PAPER

Security Threat Landscape

Marco Anisetti[1,*], Claudio Ardagna[1,*], Marco Cremonini[1,*], Ernesto Damiani[1,*], Jadran Sessa[1,*] and Luciana Costa[2,*]

[1]Università degli studi di Milano and [2]Telecom Italia

[*]marco.anisetti@unimi.it; claudio.ardagna@unimi.it; ernesto.damiani@unimi.it; jadran.sessa@uni; luciana.costa@telecomitalia.it

Driven by digitalization, information sharing has been experiencing exponential growth in the past few years. In turn, one's eagerness to better prepare and protect depends on the ability to change the attitude from "need to know" to "need to share". Digital technologies, most notably Artificial Intelligence (AI), have shaped decision-making, everyday communication, life, and work, hence highlighting the importance of maintaining the online economy and ensuring its prosperity. The threat landscape is continuously changing and evolving to address the evolution of the IT environment from software to IoT, via services and cloud computing. Providing an up-to-date overview of the current state of the art on threats and cybersecurity is critical to provide a picture of the status of cybersecurity and evaluate new trends in cybersecurity focusing on emerging threats and evolving attacks. CONCORDIA cybersecurity threat analysis is inspired by the different research domains and considers the following domains: (i) network-centric, (ii) system/software-centric, (iii) application/data-centric, (iv) user-centric, v) device-centric security.
Network-centric security refers to data transport as well as to the networking and the security issues associated with it. Topics range from DDoS protection, Software-Defined Networking (SDN), ad hoc networks to encrypted traffic analysis, 5G. System-centric security centers around cloud and virtualized environments, while IoT/Device-centric security centers around modern systems such as the Internet of Things (IoT)/edge and corresponding devices, both targeting topics such as middleware, secure OS, and security by design, Malware analysis, systems security validation, detection of zero-days, and recognizing service dependencies are specifically addressed. Data-centric security addresses issues concerned with management, analysis, protection, and visualization of data at all layers of a given system/environment, focusing on modern Big Data environments. Application-centric security addresses issues related to the security of applications, like modern services and their management. User-centric security addresses issues like privacy, social networks, fake news and identity management. The above domains apply to any environments ranging from traditional distributed IT systems to devices that produce raw data, such as embedded systems, sensors, IoT devices, drones, and the associated security-centric issues, such as IoT security, via service-based systems, such as, service-oriented architecture, cloud, microservices.

Terminology

The cybersecurity threat reporting follows well-known standards defined by main standardization bodies such as ISO and NIST. Our methodology to identify threats follows the definitions in the last version of ISO 27001 presented in 2013.[1] We consider a classification based on the identification of assets and threats. Please notice that the last revision of ISO 27001 presented in 2013 allows identifying risks using any methodology. In addition, in the process of developing on evolving threats and emerging attacks, our work will be based on two additional ISO standards that have a strong connection with ISO/IEC 27001:2013: ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls and ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management.
To improve the rigorousness and soundness of our approach, we also consider relevant NIST standards such as: i) NIST SP 800-53

Compiled on: July 21, 2020.
Draft manuscript prepared by the author.

[1] ISO/IEC 27001 Edition 2013 https://www.iso.org/standard/54534.html

Rev. 4 NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, ii) NIST SPECIAL PUBLICATION 1800-5 IT Asset Management, enhancing visibility for security analysts, which leads to better asset utilization and security.
Threat reporting is usually based on three pillars as follows.[2]

- **Asset:** something that has value to the organization. An asset extends beyond physical goods or hardware, and includes software, information, people, and reputation.
- **Threat:** the potential cause of an incident that may result in a breach of information security or compromise business operations.
- **Vulnerability:** a weakness of a control or asset. Another similar but more complete definition by NIST is: vulnerability is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.[3]

For instance, a digital repository, a certain subnet of the corporate network, a networked device, as well as the company brand and the workforce, can all be considered as assets possibly subject to risks and to protect. Examples of relevant threats and vulnerabilities are then listed as follows.

- EXAMPLE 1. The threat can be a disk failure. A related vulnerability is that there is no backup of the repository (availability is not guaranteed).
- EXAMPLE 2. The threat can be a malware propagation and the related vulnerability is that the anti-virus program is not blocking it, that is, malware signatures are out-of-date or incomplete (issues of confidentiality, integrity, and availability).
- EXAMPLE 3. The threat can be an unauthorized access. The vulnerability is the access control scheme that is not correctly enforced or has been ill-defined (loss of confidentiality, integrity, and availability).

As another example, an asset can be a human resource, for example a system administrator.

- EXAMPLE 4. The threat can be the unavailability of this person and the related vulnerability is that there is no replacement for this position and important maintenance cannot be done (potential loss of availability).
- EXAMPLE 5. The threat can consist of configuration errors made by the system administrator. The vulnerability is the malfunctioning of a system or the diminished security protection (issues in confidentiality, integrity. and availability)

In the following of this section, for each of the six domains of interest, we analyze assets and threats, reporting on some recent attacks. For the sake of readability, we will not discuss specific vulnerabilities at the basis of identified attacks. Also, to make our discussion consistent, where possible, we will refer to the threat group/threat nomenclature proposed by the ENISA threat taxonomy.[4]

Cybersecurity Threat Map

This section attempts to provide a cybersecurity threat map that summarizes the mapping between identified threat groups, threats, and the domains network, system, device/IoT, data, application, user, which will be then detailed in the following sections. The given overview provides such a mapping and specifies the threat numbering format. As an example, threat T2 "Denial of Service" in threat group TG4 "Nefarious Activity/Abuse" of domain D1 "Device/IoT" is referenced in the text as T1.4.2.

Device/IoT-Centric Security

Internet of Things (IoT) can be defined as "the networked interconnection of everyday objects, equipped with ubiquitous intelligence" [1]. IoT, edge computing, and smart devices are changing the environment in many ways, including smart transportation, sustainable mobility, smart cities, e-health, smart vehicles, and UAVs, just to name the few. The exponential growth of connected devices (from minuscule sensors to bigger machines), which, according to Intel[5] are expected to reach 200 billion by 2020, is revolutionizing current IT systems. The existence of billions of resource-constrained devices connected to the Internet introduces fundamental risks that can threaten users' life and personal sphere.

Device/IoT assets can be categorized by different classes as follows:

- **Data** – IoT and devices are the main source of data but, they do not have data as main assets since they stream data almost in real time. However, in case of edge or while in transit (e.g., passing to gateways), data become an important asset for this domain also considering the OWASP principle of IoT security related to the "Data aggregation",[6] which can reveal sensitive patterns.
- **Infrastructure** – It comprises communication protocols (e.g. MQTT, ZigBee), communication devices like routers, gateway, but also power supply units and batteries.
- **Devices** – It is the essence of this category and refers to sensors, actuators, as well as firmware driving them. It includes also devices that serve the purposes of aggregating data (e.g., in edge systems) and managing sensors/actuators, as well as

[2] ISO/IEC 27001 Edition 2005 https://www.iso.org/standard/42103.html

[3] Guide for Conducting Risk Assessments, NIST SP 800-30, September 2012, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[4] See https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/at$_{d}ownload/file$

[5] A guide to Internet of Things Infographic https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html

[6] Principles of IoT Security https://www.owasp.org/index.php/Principles$_{o}f_{I}oT_{S}ecurity$

embedded systems in general.

- **Platform and backend** – It refers to IoT backend in cloud. It is part of IoT since it is fundamental for the operation and has a great impact on security. For the sake of clarity, it is discussed in details in Domain 3 "System-centric security".
- **Decision making** – It regards the transformation of the acquired data into actions on the actuators or models. It can be computed on the edge. Similarly, to the platform and backend, we refer to Domain 4 "Data-centric security" for more details.
- **Management** – It includes, when available, device management services like device usage, battery status, and the like, as well as update management, network setup and statistics, and applications and diagnostics.
- **Security and privacy techniques** – It refers to all security techniques that are the target for an attacker. These represent the interesting components that would result in unauthorised data disclosure and leakage, if compromised. In IoT environment they can be spread from device interface to gateways and Cloud backend.
- **Roles** – Introduced by the NIST Big Data Public Working Group, this category includes human resources and related assets.

Cybersecurity threat map for Device/IoT-Centric Security can be summarized as follows:

- TG1.1: Unintentional damage/loss of information or IT assets: This group includes all threats causing unintentional damage including safety and information leakage or sharing due to human errors.
  - T1.1.1: Information leakage/sharing due to human errors
  - T1.1.2: Inadequate design and planning or incorrect adaptation
- TG1.2: Interception and unauthorised acquisition: This group includes threats introduced by alteration/manipulation of the communications between two parties. This TG, depending on the circumstances of the incident, could, also, be linked to TG5.
  - T1.2.1: Interception of information
  - T1.2.2: Unauthorized acquisition of information
- TG1.3: Intentional physical damage: in IoT the physical access to the devices that are spread in a potential uncontrolled environment is more serious than in another domain.
  - T1.3.1: Device modification
  - T1.3.2: Extraction of private information
- TG1.4: Nefarious activity/abuse: This group includes threats coming from nefarious activities. It requires active attacks targeting the infrastructure of the victim, including the installation or use of malicious tools and software.
  - T1.4.1: Identity fraud
  - T1.4.2: Denial of service
  - T1.4.3: Malicious code/software/activity
  - T1.4.4: Misuse of assurance tools
  - T1.4.5: Failures of the business process
  - T1.4.6: Code execution and injection (unsecured APIs)
- TG1.5: Legal: This group provides for threats resulting from violation of laws and/or regulations, such as the inappropriate use of Intellectual Property Rights, the misuse of personal data, the necessity to comply with judiciary decisions dictated with the rule of law.
  - T1.5.1: Violation of laws or regulations
- TG1.6: Organisational threats: This group includes threats to the organizational sphere.
  - T1.6.1: Skill shortage

Figure 1 shows the relation between Assets and threats for the IoT/Device domain.

Network-Centric Security

Traditional network environments are characterized by well-defined perimeters and trusted domains. Networks have been initially designed to create internal segments separated from the external world by using a fixed perimeter. The internal network was deemed trustworthy, whereas the external was considered potentially hostile. Perimeter devices, such as firewalls and intrusion detection systems, have been the traditional technologies used to secure the network.

A network asset is an asset that is part of a network. To provide a service, network assets are interconnected to each other. If a network asset is removed, the system or service may not function to full capacity. Also, network infrastructure can be considered as an asset, since it provides all hardware and software resources part of the network, enabling network connectivity, communication, operations and management of an enterprise network. An infrastructure asset provides the communication path and services between users, processes, applications, services, and external networks like the Internet. Network infrastructure devices include routers, firewalls, switches, servers, load-balancers, intrusion detection systems, domain name systems, and storage area networks.

The introduction of virtualization technology drives the digital transformation of the network, slightly changing the asset definition. The network functions virtualization concept virtualizes the majority of elements/assets of a network. In this way,

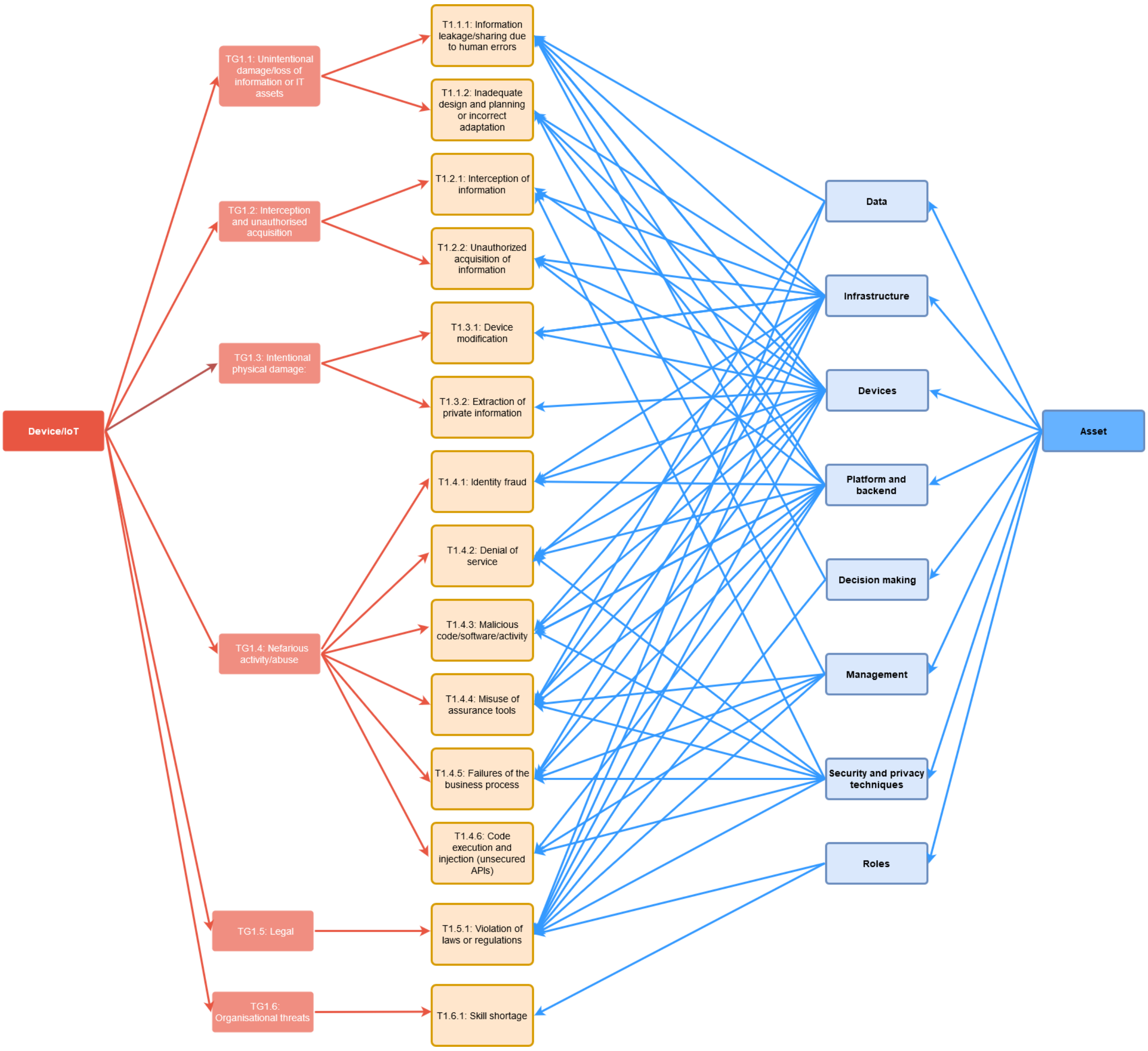
Device/IoT
TG1.1: Unintentional damage/loss of information or IT assets
TG1.2: Interception and unauthorised acquisition
TG1.3: Intentional physical damage:
TG1.4: Nefarious activity/abuse
TG1.5: Legal
TG1.6: Organisational threats
T1.1.1: Information leakage/sharing due to human errors
T1.1.2: Inadequate design and planning or incorrect adaptation
T1.2.1: Interception of information
T1.2.2: Unauthorized acquisition of information
T1.3.1: Device modification
T1.3.2: Extraction of private information
T1.4.1: Identity fraud
T1.4.2: Denial of service
T1.4.3: Malicious code/software/activity
T1.4.4: Misuse of assurance tools
T1.4.5: Failures of the business process
T1.4.6: Code execution and injection (unsecured APIs)
T1.5.1: Violation of laws or regulations
T1.6.1: Skill shortage
Data
Infrastructure
Devices
Platform and backend
Decision making
Management
Security and privacy techniques
Roles
Asset

Figure 1. Device/IoT-Centric Security: threats and assets

entire classes of network node functions can be set up as building blocks that can be connected to create overall telecommunication networks referred to as “network slice”. Network slicing is an approach proposed with the advent of 5G to allow a single network to support services with completely different operational parameters and policies. The network is viewed as an asset pool of physical resources and virtual network functions (VNFs), connectivity, bandwidth, and computational capabilities. A network ‘slice’ combines these assets to form a virtual network. Different network slices will have different operational parameters and hence a different combination of assets. The slices may share network assets or may have assets specifically allocated to them, depending on the service policies.
In this context, it is not easy to provide a network asset taxonomy. However, a possible way to categorize network assets can be to group them based on their role, derived from the functions provided by the assets or network elements. For this purpose, in this deliverable the network has been divided into subdomains and network assets have been categorized accordingly to their provided functions (and inspired from ENISA).[7]

- **Access network.** It connects individual devices to other parts of a core network through radio or fixed connections.
- **Core network.** It is the part of the network that offers services to the devices/customers who are interconnected by the access network. The core network also provides the gateway to other networks.
- **Infrastructure network/area network.** It includes hardware and software resources of an entire network that enable network connectivity, mobility management, network operation and management.
- **Peering points.** They support the communications between the subscribers of one provider and the subscribers of another provider. We consider in this group also the IPX (Internet Provider Exchange) roaming network.

Since some type of endpoint devices can also be considered as network assets a further group has been added to take them into account.

- **Endpoint network.** It includes systems/devices that communicates back and forth with the network to which they are connected. IoT devices are an example of assets in this category. This asset type is included here because in some settings the network provider retains some control (and responsibility) over these assets.

Cybersecurity threat map for Network-Centric Security can be summarized as follows:

- TG2.1: Unintentional damage/loss of information on IT assets: this group includes all threats causing unintentional information leakage or sharing due to human errors.
  * T2.1.1: Erroneous use or administration of devices and systems
- TG2.2: Interception and unauthorised acquisition: this group includes any attack, passive or active, where the attacker attempts to listen, intercept or re-route traffic/data. An example of this would be man-in-the-middle attacks. This group also includes manipulation attacks where the attacker attempts to alter or interfere with data in transit, in particular with signalling messages and routing information.
  * T2.2.1: Signaling traffic interception
  * T2.2.2: Data session hijacking
  * T2.2.3: Traffic eavesdropping
  * T2.2.4: Traffic redirection
- TG2.3: Nefarious activity/abuse: this group includes threats coming from nefarious activities. It requires active attacks targeting the network infrastructure of the victim.
  * T2.3.1: The exploitation of software bug
  * T2.3.2: Manipulation of hardware and firmware
  * T2.3.3: Malicious code/software/activity
  * T2.3.4: Remote activities (execution)
  * T2.3.5: Malicious code - Signaling amplification attacks
- TG2.4: Organisational threats: this group includes threats to the organizational sphere.
  * T2.4.1: Failures of devices or systems
  * T2.4.2: Supply chain
  * T2.4.3: Software bug

Figure 2 shows the relation between Assets and threats for the Network domain.

[7] Guideline on Threats and Assets Technical guidance on threats and assets https://www.enisa.europa.eu/publications/technical-guideline-on-threats-and-assets

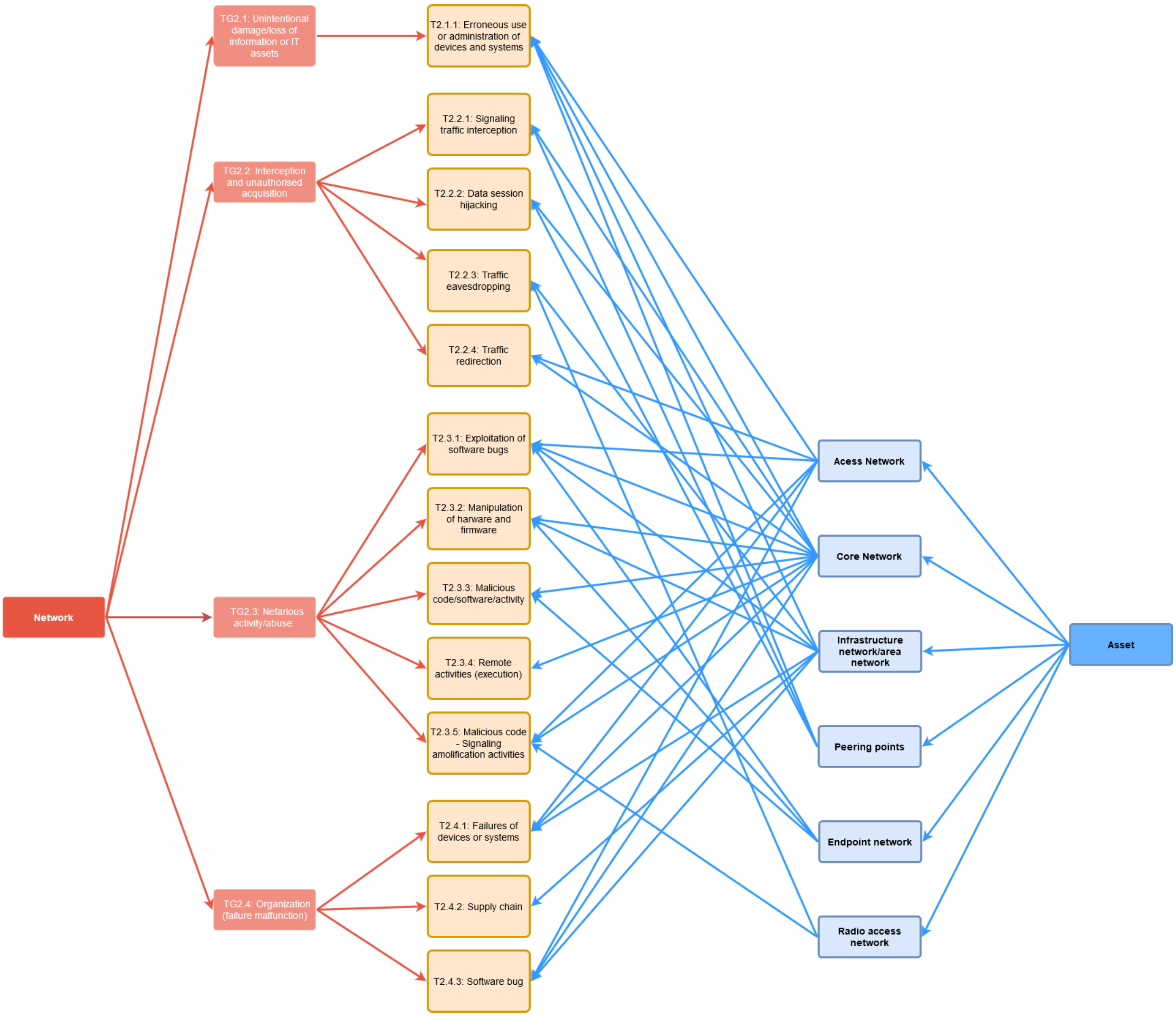
TG2.1: Unintentional damage/loss of information or IT assets
T2.1.1: Erroneous use or administration of devices and systems
T2.2.1: Signaling traffic interception
TG2.2: Interception and unauthorised acquisition
T2.2.2: Data session hijacking
T2.2.3: Traffic eavesdropping
T2.2.4: Traffic redirection
T2.3.1: Exploitation of software bugs
T2.3.2: Manipulation of harware and firmware
T2.3.3: Malicious code/software/activity
Network
TG2.3: Nefarious activity/abuse:
T2.3.4: Remote activities (execution)
T2.3.5: Malicious code - Signaling amolification activities
T2.4.1: Failures of devices or systems
TG2.4: Organization (failure malfunction)
T2.4.2: Supply chain
T2.4.3: Software bug
Acess Network
Core Network
Infrastructure network/area network
Peering points
Endpoint network
Radio access network
Asset

Figure 2. Network-Centric Security: threats and assets

System-Centric Security

The notion of system is often used as a synonym of Operating System (OS), or in general, software that enables applications to take advantage of the computation connectivity and storage capabilities of the hardware. OSs were a preferred target of a number of disruptive attacks in the past (e.g., Code Red exploiting IIS buffer overflow, Sasser attacking the Local Security Authority Subsystem Service, Snakso Linux server rootkit) owing mainly to their complexity, centrality, and role in certain crucial security features, such as authentication. Nonetheless, they will have an essential role even in the future due to the fact that OSs are increasingly immersed in a more complex environment (e.g., mobile devices, virtualized systems), where their vulnerabilities can be either exacerbated or mitigated and they can become a commodity for applications (e.g., containerization of applications).

In this context, Big Data has recently become a major trend attracting both academia, research institutions, and industries. According to IDC,[8] "revenues for Big Data and business analytics will reach $260 billion in 2020, at a CAGR of 11.9% over the 2017-19 forecast period". Today pervasive and interconnected world, where billions of resource-constrained devices are connected and people are put at the center of a continuous sensing process, results in an enormous amount of generated and collected data (estimated in 2.5 quintillions bytes of data each day [9]). The Big Data revolution fosters the so-called data-driven ecosystem where better decisions are supported by enhanced analytics and data management. Big Data are not only characterized by huge amount of data, but points to scenarios where data are diverse, come at high rates and must be proven to be trustworthy, as clarified by the 5V storyline[2]. Big Data are defined according to 5V: i) Volume (huge amount of data), ii) Velocity (high speed of data in and out), iii) Variety (several ranges of data types and sources), iv) "Veracity" (data authenticity since the quality of captured data can vary greatly and an accurate analysis depends on the veracity of data source), and v)"Value" (the potential revenue of Big Data). Big Data has been defined in different ways starting from Gartner "Big data

[8] IDC, Worldwide Semiannual Big Data and Analytics Spending Guide, 2018, https://www.idc.com/getdoc.jsp?containerId=prUS44215218

[9] Bernard Marr, How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read, May 2018, https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/363f1fcf60ba

is high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization " to McKinsey Global Institute "Big Data as data sets whose size is beyond the ability of typical database software tools to capture, store, manage and analyse."
According to ENISA's Guideline on Threats and Assets published in the context of ENISA's Security framework for Article 4 and 13a proposal, an asset is defined as "anything of value. Assets can be abstract assets (like processes or reputation), virtual assets (for instance, data), physical assets (cables, a piece of equipment), human resources, money". An item of our taxonomy is either a description of data itself, or describes assets that generate, process, store or transmit data chunks and, as such, is exposed to cyber-security threats. In addition to the ENISA Big Data Threat Landscape,[48] a major source of information for this study is the work undertaken by the NIST Big Data Public Working Group (NBD-PWG) resulting in two draft Volumes (Volume 1 about Definitions and Volume 2 about Taxonomy). Another source of information is the report "Big Data Taxonomy", issued by Cloud Security Alliance (CSA) Big Data Working Group in September 2014, where a six-dimensional taxonomy for Big Data, built around the nature of the data, is introduced.
Assets can be categorized in 5 different classes as follows:

- **Data** – It is the core class and includes all types of data from metadata, to structured, semi-structured and unstructured data, and stream of data.
- **Infrastructure** – It comprises software, hardware resources denoting both physical and virtualized devices, computing infrastructure with batch and streaming processes, and storage infrastructure with various database management systems.
- **Big Data analytics** – It includes protocols and algorithms for Big Data analysis, as well as all processing algorithms for data routing and parallelization. It points to the design and implementation of procedures, models, algorithms, as well as analytics results.
- **Security and privacy techniques** – It refers to all security techniques that are the target for an attacker. These represent the interesting components that would result in unauthorized data disclosure and leakage, if compromised. Examples are security best practice documents, cryptography algorithms and methods, information about the access control model used, and the like.
- **Roles** - Introduced by the NIST Big Data Public Working Group, it includes human resources and related assets.

Cybersecurity threat map for System-Centric Security can be summarized as follows:

- TG3.1: Unintentional damage/loss of information or IT assets: This group includes all threats causing unintentional security leakage due to human errors.
  - T3.1.1: Information leakage/sharing due to human errors
  - T3.1.2: Inadequate design and planning or incorrect adaptation
- TG3.2: Interception and unauthorised acquisition: This group includes threats introduced by alteration/manipulation of the communications between two parties (including cloud internal communication channels). This TG, depending on the circumstances of the incident, could, also, be linked to TG3.5.
  - T3.2.1: Interception of information
  - T3.2.2: Unauthorized acquisition of information (data breach)
- TG3.3: Poisoning: This group includes all the threats due to configuration/business process poisoning and aiming to alter system behaviors (i.e., at any layers).
  - T3.3.1: Configuration poisoning
  - T3.3.2: Business process poisoning
- TG3.4: Nefarious activity/abuse: This group includes threats coming from nefarious activities. It requires active attacks targeting the infrastructure at any layers like management hijacking and identity fraud.
  - T3.4.1: Identity fraud
  - T3.4.2: Denial of service
  - T3.4.3: Malicious code/software/activity
  - T3.4.4: Generation and use of rogue certificates
  - T3.4.5: Misuse of assurance tools
  - T3.4.6: Failures of the business process
  - T3.4.7: Code execution and injection (unsecured APIs)
- TG3.5: Legal: This group provides for threats resulting from violation of laws and/or regulations, such as the inappropriate use of Intellectual Property Rights, the misuse of personal data, the necessity to comply with judiciary decisions dictated with the rule of law. Section 4 of the present document will discuss aspects of this TG identified.
  - T3.5.1: Violation of laws or regulations
- TG3.6: Organisational threats: This group includes threats to the organizational sphere.
  - T3.6.1: Skill shortage
  - T3.6.2: Malicious insider

Figure 3 shows the relation between Assets and threats for the System domain.

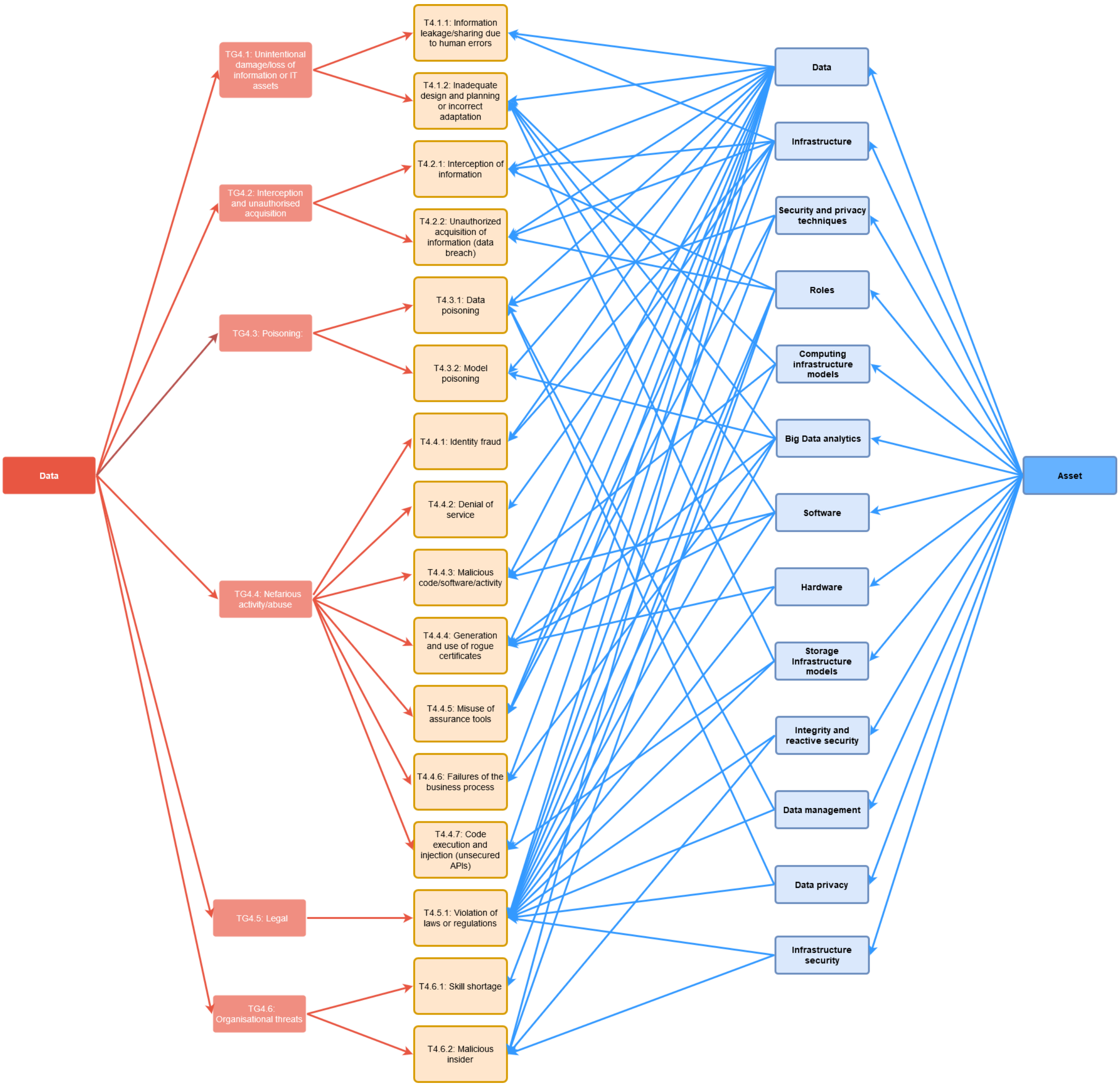
TG4.1: Unintentional damage/loss of information or IT assets
TG4.2: Interception and unauthorised acquisition
TG4.3: Poisoning:
Data
TG4.4: Nefarious activity/abuse
TG4.5: Legal
TG4.6: Organisational threats
T4.1.1: Information leakage/sharing due to human errors
T4.1.2: Inadequate design and planning or incorrect adaptation
T4.2.1: Interception of information
T4.2.2: Unauthorized acquisition of information (data breach)
T4.3.1: Data poisoning
T4.3.2: Model poisoning
T4.4.1: Identity fraud
T4.4.2: Denial of service
T4.4.3: Malicious code/software/activity
T4.4.4: Generation and use of rogue certificates
T4.4.5: Misuse of assurance tools
T4.4.6: Failures of the business process
T4.4.7: Code execution and injection (unsecured APIs)
T4.5.1: Violation of laws or regulations
T4.6.1: Skill shortage
T4.6.2: Malicious insider
Data
Infrastructure
Security and privacy techniques
Roles
Computing infrastructure models
Big Data analytics
Software
Hardware
Storage infrastructure models
Integrity and reactive security
Data management
Data privacy
Infrastructure security
Asset

Figure 3. System-Centric Security: threats and assets

Data-Centric Security

The ability of sharing, managing, distributing, and accessing data quickly and remotely are at the basis of the digital revolution that started several decades ago. The role of data in today's technology is even more important, having entered the so-called, data-driven economy. Data management and inference based on them are fundamental for any enterprise, from micro to large. Moreover, data management allows enterprises to stay competitive in the evolving global market. The data domain observed important changes at all layers of an IT chain: i) data layer: from data to big data, ii) database layer: from SQL to NoSQL, iii) platform layer: from the data warehouse and DBMS to Big Data platforms, iv) analytics layer: from data mining to machine learning and artificial intelligence. For instance, data mining focuses on discovering unknown patterns and relationships in large data sets, while machine learning aims to discover patterns in data, by learning patterns parameters directly from data. In this context, Big Data has recently become a major trend attracting both academia, research institutions, and industries. According to IDC,[10] "revenues for Big Data and business analytics will reach $260 billion in 2020, at a CAGR of 11.9% over the 2017-19 forecast period". Today pervasive and interconnected world, where billions of resource-constrained devices are connected and people are put at the center of a continuous sensing process, results in an enormous amount of generated

[10] IDC, Worldwide Semiannual Big Data and Analytics Spending Guide, 2018, https://www.idc.com/getdoc.jsp?containerId=prUS44215218

and collected data (estimated in 2.5 quintillions bytes of data each day [11]). The Big Data revolution fosters the so-called data-driven ecosystem where better decisions are supported by enhanced analytics and data management. Big Data are not only characterized by huge amount of data, but points to scenarios where data are diverse, come at high rates and must be proven to be trustworthy, as clarified by the 5V storyline[2]. Big Data are defined according to 5V: i) Volume (huge amount of data), ii) Velocity (high speed of data in and out), iii) Variety (several ranges of data types and sources), iv) "Veracity" (data authenticity since the quality of captured data can vary greatly and an accurate analysis depends on the veracity of data source), and v)“Value” (the potential revenue of Big Data). Big Data has been defined in different ways starting from Gartner "Big data is high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization ” to McKinsey Global Institute "Big Data as data sets whose size is beyond the ability of typical database software tools to capture, store, manage and analyse.“
According to ENISA’s Guideline on Threats and Assets published in the context of ENISA’s Security framework for Article 4 and 13a proposal, an asset is defined as “anything of value. Assets can be abstract assets (like processes or reputation), virtual assets (for instance, data), physical assets (cables, a piece of equipment), human resources, money”. An item of our taxonomy is either a description of data itself, or describes assets that generate, process, store or transmit data chunks and, as such, is exposed to cyber-security threats. In addition to the ENISA Big Data Threat Landscape,[48] a major source of information for this study is the work undertaken by the NIST Big Data Public Working Group (NBD-PWG) resulting in two draft Volumes (Volume 1 about Definitions and Volume 2 about Taxonomy). Another source of information is the report “Big Data Taxonomy”, issued by Cloud Security Alliance (CSA) Big Data Working Group in September 2014, where a six-dimensional taxonomy for Big Data, built around the nature of the data, is introduced.
Assets can be categorized in 5 different classes as follows:

- **Data** – It is the core class and includes all types of data from metadata, to structured, semi-structured and unstructured data, and stream of data.
- **Infrastructure** – It comprises software, hardware resources denoting both physical and virtualized devices, computing infrastructure with batch and streaming processes, and storage infrastructure with various database management systems.
- **Big Data analytics** – It includes protocols and algorithms for Big Data analysis, as well as all processing algorithms for data routing and parallelization. It points to the design and implementation of procedures, models, algorithms, as well as analytics results.
- **Security and privacy techniques** – It refers to all security techniques that are the target for an attacker. These represent the interesting components that would result in unauthorized data disclosure and leakage, if compromised. Examples are security best practice documents, cryptography algorithms and methods, information about the access control model used, and the like.
- **Roles** - Introduced by the NIST Big Data Public Working Group, it includes human resources and related assets.

Cybersecurity threat map for Data-Centric Security can be summarized as follows:

- TG4.1: Unintentional damage/loss of information or IT assets: This group includes all threats causing unintentional information leakage or sharing due to human errors.

  * T4.1.1: Information leakage/sharing due to human errors
  * T4.1.2: Inadequate design and planning or incorrect adaptation

- TG4.2: Interception and unauthorised acquisition: This group includes threats introduced by alteration/manipulation of the communications between two parties. This TG, depending on the circumstances of the incident, could, also, be linked to TG4.5.

  * T4.2.1: Interception of information
  * T4.2.2: Unauthorized acquisition of information (data breach)

- TG4.3: Poisoning: This group includes all threats due to data/model poisoning and aiming to picture a scenario that not adhere to reality.

  * T4.3.1: Data poisoning
  * T4.3.2: Model poisoning

- TG4.4: Nefarious activity/abuse: This group includes threats coming from nefarious activities. It requires active attacks targeting the infrastructure of the victim, including the installation or use of malicious tools and software.

  * T4.4.1: Identity fraud
  * T4.4.2: Denial of service
  * T4.4.3: Malicious code/software/activity
  * T4.4.4: Generation and use of rogue certificates
  * T4.4.5: Misuse of assurance tools
  * T4.4.6: Failures of the business process
  * T4.4.7: Code execution and injection (unsecured APIs)

[11] Bernard Marr, How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read, May 2018, https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/363f1fcf60ba

- TG5: Legal: This group includes threats due to violation of laws or regulations, the breach of legislation, the failure to meet contractual requirements, the unauthorized use of Intellectual Property resources, the abuse of personal data, the necessity to obey judiciary decisions and court orders.
  * T4.5.1: Violation of laws or regulations
- TG6: Organisational threats: This group includes threats to the organizational sphere.
  * T4.6.1: Skill shortage
  * T4.6.2: Malicious Insider

Figure 4 shows the relation between Assets and threats for the Data domain.

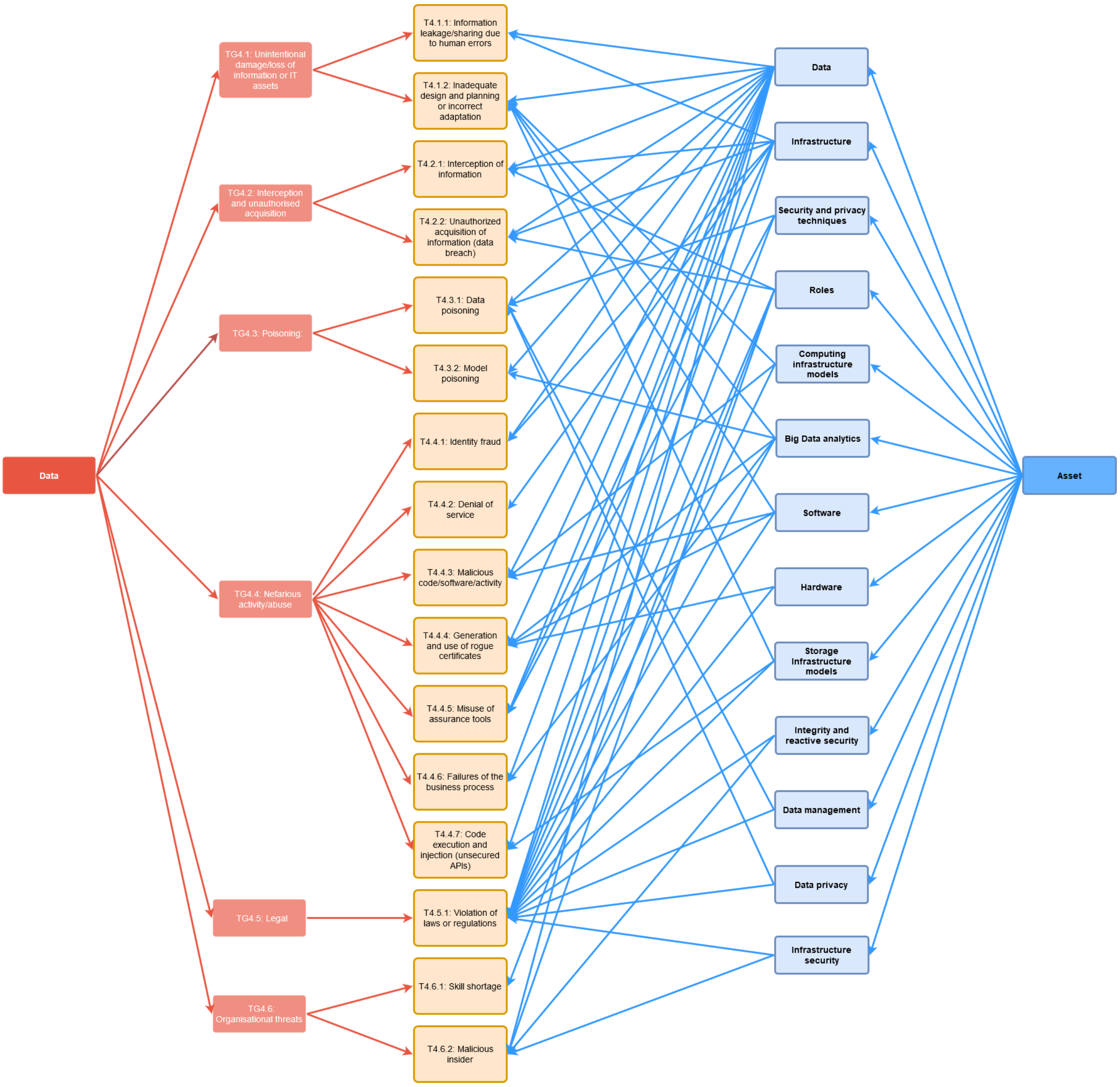
Data
TG4.1: Unintentional damage/loss of information or IT assets
TG4.2: Interception and unauthorised acquisition
TG4.3: Poisoning
TG4.4: Nefarious activity/abuse
TG4.5: Legal
TG4.6: Organisational threats
T4.1.1: Information leakage/sharing due to human errors
T4.1.2: Inadequate design and planning or incorrect adaptation
T4.2.1: Interception of information
T4.2.2: Unauthorized acquisition of information (data breach)
T4.3.1: Data poisoning
T4.3.2: Model poisoning
T4.4.1: Identity fraud
T4.4.2: Denial of service
T4.4.3: Malicious code/software/activity
T4.4.4: Generation and use of rogue certificates
T4.4.5: Misuse of assurance tools
T4.4.6: Failures of the business process
T4.4.7: Code execution and injection (unsecured APIs)
T4.5.1: Violation of laws or regulations
T4.6.1: Skill shortage
T4.6.2: Malicious insider
Data
Infrastructure
Security and privacy techniques
Roles
Computing infrastructure models
Big Data analytics
Software
Hardware
Storage infrastructure models
Integrity and reactive security
Data management
Data privacy
Infrastructure security
Asset

Figure 4. Data-Centric Security: threats and assets

Application-Centric Security

Application is denoted as a program or group of programs designed for end-users. There are numerous examples of applications used in everyday life, including word processing, spreadsheet, accounting, web browser, email client, file viewer applications among many others. Applications can be either bundled with the OS or published separately as proprietary or open-source. Current IT systems are heavily based on applications/services composed at run time.

According to OWASP TOP 10 2017[12], risk and threats are continuously evolving as the fundamental technology and architecture of application change. For instance, the advent of microservice architectures, which replaces monolithic applications, come with specific security challenges. The increasing trend in moving functionalities from server side to client side are changing the pace of security assessment and protection. In addition to the OWASP TOP 10 2017, a major source of information for this study is the work undertaken by the SANS institute resulting in CWE/SANS TOP 25 Most Dangerous Software Errors.[13] Assets can be categorized in 5 different classes as follows:

- **Data** – It includes all types of application data and metadata.
- **Interfaces** – Platform and APIs.
- **Security techniques** – It refers to all security techniques that are the target for an attacker. These represent the interesting components that would result in application breaches, if compromised. Examples are security best practice documents, cryptography algorithms and methods, information about the access control model used, and the like.
- **Roles** - Introduced by the NIST Big Data Public Working Group, it includes human resources and related assets.

Cybersecurity threat map for Application-Centric Security can be summarized as follows:

- TG5.1: Unintentional damage: This group includes all threats causing application malfunctioning or loss of confidentiality/integrity/availability due to human errors.
  * T5.1.1: Security misconfiguration
- TG5.2: Interception and unauthorised acquisition: This group includes threats introduced by alteration/manipulation of the communications between two parties. This TG, depending on the circumstances of the incident, could, also, be linked to TG5.4.
  * T5.2.1: Interception of information
  * T5.2.2: Sensitive data exposure
- TG5.3: Nefarious activity/abuse: This group includes threats coming from nefarious activities. It requires active attacks targeting the platform of the victim, as well as public interfaces of the hosting platform and applications.
  * T5.3.1: Broken authentication and access control
  * T5.3.2: Denial of service
  * T5.3.3: Code execution and injection (unsecured APIs)
  * T5.3.4: Insufficient logging and monitoring
  * T5.3.5: Untrusted composition
- TG5.4: Legal: This group provides for threats resulting from violations of laws and/or regulations, such as the inappropriate use of Intellectual Property Rights, the misuse of personal data, the necessity to comply with judiciary decisions dictated with the rule of law.
  * T5.4.1: Violation of laws or regulations
- TG5.5: Organisational threats: This group includes threats to the organizational sphere.
  * T5.5.1: Malicious Insider

Figure 5 shows the relation between Assets and threats for the Application domain.

[12] OWASP Top 10 -2017 The Ten Most Critical Web Application Security Risks https://www.owasp.org/images/7/72/OWASP$_{T}op_{1}0 - 2017_{(}en).pdf.pdf$

[13] CWE/SANS TOP 25 Most Dangerous Software Errors https://www.sans.org/top25-software-errors

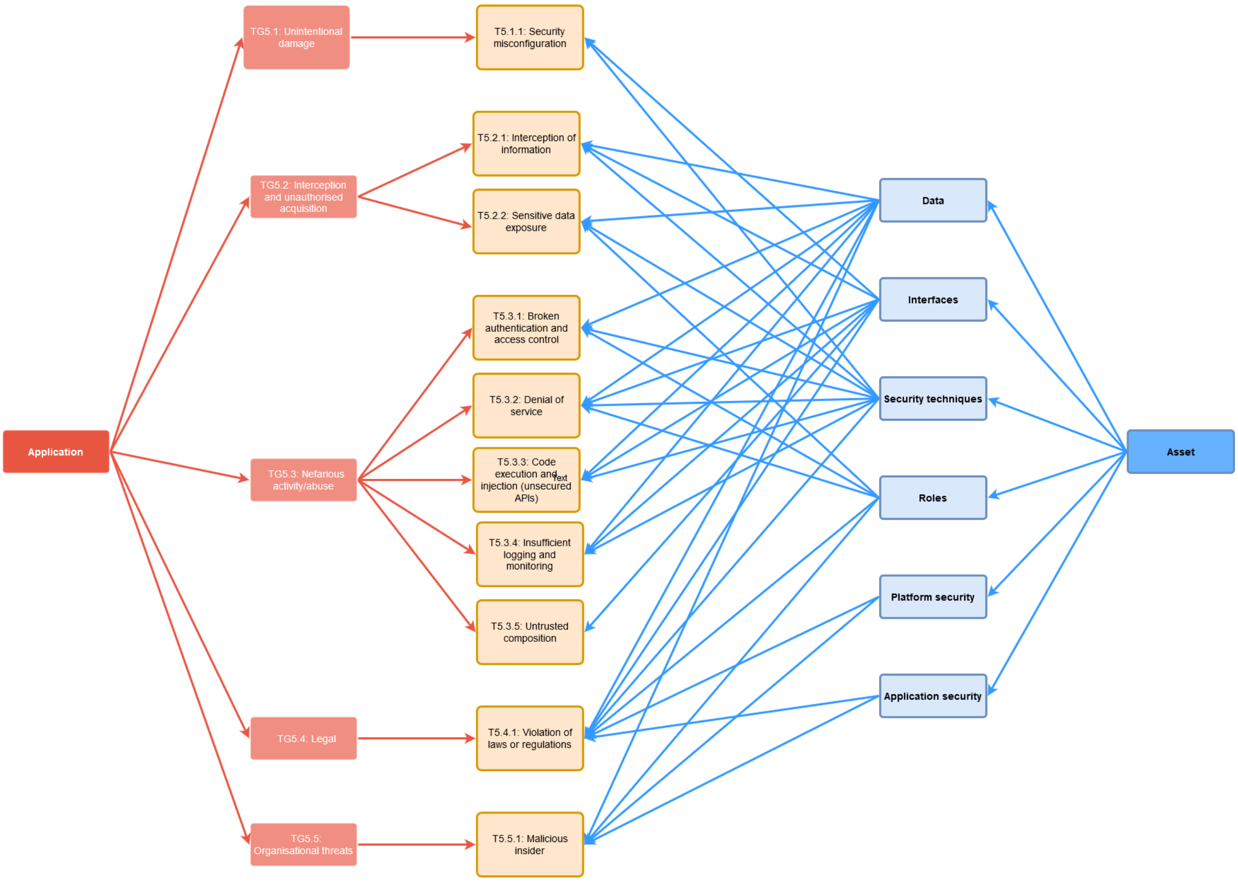
TG5.1: Unintentional damage
T5.1.1: Security misconfiguration
T5.2.1: Interception of information
TG5.2: Interception and unauthorised acquisition
T5.2.2: Sensitive data exposure
T5.3.1: Broken authentication and access control
T5.3.2: Denial of service
Application
TG5.3: Nefarious activity/abuse
T5.3.3: Code execution and injection (unsecured APIs)
Text
T5.3.4: Insufficient logging and monitoring
T5.3.5: Untrusted composition
TG5.4: Legal
T5.4.1: Violation of laws or regulations
TG5.5: Organisational threats
T5.5.1: Malicious insider
Data
Interfaces
Security techniques
Roles
Platform security
Application security
Asset

Figure 5. Application-Centric Security: threats and assets

User-Centric Security

The term *user* refers to a person using information technologies in a professional context. In general, users may have the double role of perpetrator of a threat (e.g., a threat is carried out by human actions) or victims (e.g., individuals are the asset targeted by a threat). In certain cases, there is not a clear-cut distinction between the User-centric domain and other domains, especially considering that users as perpetrators of security violations are necessarily considered in other domains too, and several semi-automated attack vectors, such as botnets, are operated by humans. Furthermore, humans are responsible for all kinds of cybercrimes, in the end, even social bots used in frauds have been designed by humans and provide illicit benefits to some humans. For most security incidents, the consequences are likely to impact humans (systems experiencing downtime, malicious applications, compromised IoT networks).
Assets can be categorized into 3 different classes as follows:

- **Internal/affiliated** – This class groups asset categories that typically reflect the roles of individuals in the company. The four categories have clear distinct features: whether or not they are mostly victim of targeted attacks, the odds to be involved in security incidents or to be responsible of insider threats and so on.
- **External** – External assets are both individuals and legal person, and represents the stakeholders not included in company's operations and processes. They are the customers and the suppliers, and those representing different interests, like the owners/shareholders, legal authorities and agencies, and the local community and country.
- **Intangible** – With this last class, we include two important intangible assets (i.e., neither referred to internal nor external assets), namely the financial market and the public opinion. Both are meta-entities that exert an important role for a company and could possibly be influenced by the consequence of a security incidents.

Cybersecurity threat map for User-Centric Security can be summarized as follows:

- TG6.1: Human errors: This group includes all threats causing unintentional information leakage or sharing due to human errors.

  * T6.1.1: Mishandling of physical assets
  * T6.1.2: Misconfiguration of systems
  * T6.1.3: Loss of CIA on data assets
  * T6.1.4: The legal, reputational, and financial cost

- TG6.2: Privacy breaches: This group includes all threats causing privacy breaches.
  * T6.2.1: Profiling and discriminatory practices
  * T6.2.2: Illegal acquisition of information
- TG6.3: Cybercrime: This group includes all threats due to data/model poisoning and aiming to picture a scenario that not adhere to reality.
  * T6.3.1: Organized criminal groups' activity
  * T6.3.2: State-sponsored organizations' activity
  * T6.3.3: Malicious employees or partners' activity
- TG6.4: Media amplification effects: This group includes threats coming from nefarious activities. It requires active attacks targeting the infrastructure of the victim, including the installation or use of malicious tools and software.
  * T6.4.1: Misinformation/disinformation campaigns
  * T6.4.2: Smearing campaigns/market manipulation
  * T6.4.3: Social responsibility/ethics-related incidents
- TG6.5: Organisational threats: This group includes threats to the organizational sphere.
  * T6.5.1: Skill shortage/undefined cybersecurity curricula
  * T6.5.2: Business misalignment/shift of priorities

Figure 6 shows the relation between Assets and threats for the User domain.

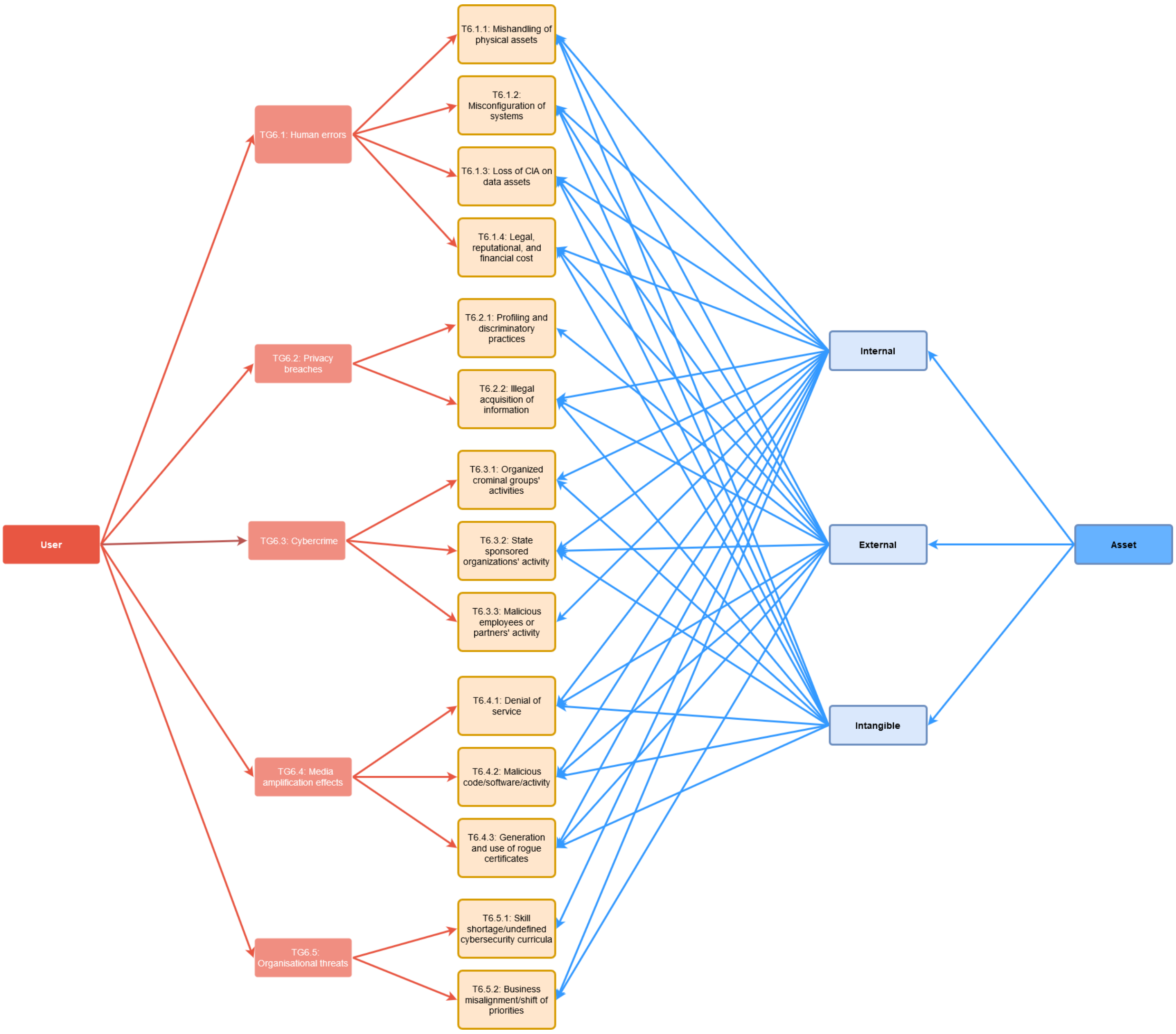
T6.1.1: Mishandling of physical assets
T6.1.2: Misconfiguration of systems
TG6.1: Human errors
T6.1.3: Loss of CIA on data assets
T6.1.4: Legal, reputational, and financial cost
T6.2.1: Profiling and discriminatory practices
Internal
TG6.2: Privacy breaches
T6.2.2: Illegal acquisition of information
T6.3.1: Organized crominal groups' activities
User
TG6.3: Cybercrime
T6.3.2: State sponsored organizations' activity
External
Asset
T6.3.3: Malicious employees or partners' activity
T6.4.1: Denial of service
Intangible
TG6.4: Media amplification effects
T6.4.2: Malicious code/software/activity
T6.4.3: Generation and use of rogue certificates
T6.5.1: Skill shortage/undefined cybersecurity curricula
TG6.5: Organisational threats
T6.5.2: Business misalignment/shift of priorities

Figure 6. User-Centric Security: threats and assets

From the given overview, it emerges that threats groups are quite horizontal to the different domains. Some differences still exist due to the peculiarities of each area. Also, threats in the area of data and users are cross-domain due to the fact that often data represent the target of an attack, while users are often seen both as a target and as a threat agent.

Key Takeaways

The following summarizes the most important findings, as a key takeaway, emerging from the threat landscape.

- **Endemic persistent threats.** + traditional threats, like software bugs, malware, and DoS, which span all over the ICT domains, from OS to networking and applications, are becoming persistent and endemic. Even old vulnerabilities can revive in the context of a new domain not mature enough to consider security as first class requirement. Even advanced architectures must be designed to face security threats, like in the case of 5G services, virtualized operating systems, and layered systems, where a number of countermeasures are used to limit their impact (e.g., sandboxing, isolation). Persistent threats are increasingly exploiting new possibilities given by new assets, platforms, and application domains. For instance, DoS is evolving towards targeting mobile devices and sensors, by speeding up battery consumption, instead of inducing service failures. Mobile devices are becoming a suitable target vector due, for instance, to poor security skills of the users. For instance, stealthy multimedia files can be used to carry out the attack, unrecognized by inexperienced users, instead of more traditional DoS flooding techniques[3].
  Interested domains: All.
- **Balance security and domain-specific constraints.** Not all the domains can adopt the same security countermeasures to deal with cybersecurity risks. There is the need to find a good trade-off between the security level to be achieved, also, as set forth by the associated legal and economic requirements. On one hand, the economic impacts of cybersecurity on the different actors and stakeholders can have important consequences. The assessment of cybersecurity efficiency in terms of economic investments in cyber-ecosystems becomes fundamental to analyze security from a strictly economic point of view, considering that often critically important systems or components have their investments in related security activities neglected. For instance, in IoT, there is an ongoing discussion on the adoption of lightweight cryptography for embedded devices in order to find a balance between security and cost constraints.[14] Such a reduced cryptography protection quality is not feasible in other domains, where security breaches and data leakages are likely to have severe impacts and a number of persistent threats still exists. The European Regulatory framework provides the basis to respond to cybersecurity threats, also, by allowing in the longer terms the related capacity building across sectors. However, the rapid development of current architectures and infrastructures render it challenging for existing regulations to remain effective for newly introduced regulations to be sufficiently future proof. Nevertheless, the European Regulators have been taking prompt action by amending existing regulations as, for instance, the ePrivacy Directive and by announcing initiatives such as the announcement by the European Commission of new legislation focusing on artificial intelligence.
  Interested domains: All
- **Physical access and insider threats.** Having physical access to assets is a serious insider-related threat and often permits to easily bypass security protections (e.g., in the IoT domain). In general, insider threats are difficult to mitigate, both when an access to critical information with high privileges is granted by software components and when an access is granted to humans/employees. In the latter case, there is the additional difficulty of predicting human behavior and intentions. For the future, it is a common belief that these threats might become even more insidious, especially when human-based (Netwrix 2018 Cloud Security Report indicates that 58% of companies attribute security breaches to insiders). This trend will be further exacerbated in the IoT context thanks to the distributed nature that makes easier to hide the insider activities. Huge effort will be put in the future to identify anomalous human behavior in conjunction to insider threats.
  Interested domains: All
- **Relation between security and safety.** ICT is nowadays permeating every sector and impacts people everyday life. It is nowadays clear that there is an increasing connection between cybersecurity and safety, and this will be more and more exacerbated in the future. The impact of IoT cybersecurity on safety for instance is crucial and current trends in adoption of IoT in critical environments such as automotive and UAVs will increase it tremendously. Another scenario where safety is connected with IoT security is health. There is an increasing adoption of IoT devices in hospitals and at the same time very low awareness about the security impact of having critical devices connected to the Internet. In this scenario, there is also a critical privacy concern to be addressed since in most cases hospital infrastructures, even if certified for HIPAA, are not ready to host IoT ecosystems that most of the times share the same networking segment as the rest of the hospital system.
  Interested domains: Device/IoT, System
- **User profiling.** The need of profiling users has a long history in ICT and was grounded on the need of control. It emerges more concretely when linked to business profits. Profiling is also one of the preliminary stages to carry out a cyber attack and to gain an advantage. The profiling capabilities (e.g., using social engineering) will be more and more exploited in the future for attacks preparation and for targeted spam/phishing campaigns. The success of smart home IoT devices is enlarging the perimeter exploitable for profiling purposes. Alexa and Google home, to name the ones with the largest user base, are fully connected and powerful devices having as one of their main goals to profile the users. They are also perceived as ubiquitous devices, and this lower the transparency of the interaction with them, increasing the risk due to low awareness. This type of devices is also connected to a powerful AI that will constitute in the future a new target for an attacker having the objective to lead the IoT to take a wrong decision (e.g., to not recognize a specific face as the one of a criminal).
  Interested domains: Device/IoT, Data, User

[14] The Debate Over How to Encrypt the Internet of Things https://www.wired.com/story/lightweight-encryption-internet-of-things/amp

- **Diffusion of Ultra-Wideband networks.** The network is obviously the primary attack vector. The more the network is powerful, the more the attack vector is critical. With the adoption of 5G, network slicing will offer differentiated services over the whole network, opening the possibility to provide networking infrastructure as a service. New threats will be introduced from the adoption of network slicing in the context of verticals. Such threats are related to data leakage between multiple virtual environments or slices, bad slice isolation that can result in security resources exhaustion in other slices. Low latency of 5G could allow better coordination among zombies in a DDoS attack scenario and to exploit protocol leakages connected to performances. In the context of IoT, the capillary diffusion enabled by 5G will allow, for instance, an attacker to focus on a specific area covered by a slice, where a large number of compromised devices can interfere with the cellular connectivity leading to a new generation of better localized DDoS.
  Interested domains: Device/IoT, Network
- **Decentralization and computation capability at the edge.** Edge computing is migrating functionality to the edge and with them also security concerns. Some of these concerns shift from a powerful and protected environment to a less powerful and less protected one. This shift needs to be carried out very carefully to provide functionalities without impacting the security features. Edge computing is adopted in many contexts including new incoming ultra wide band networking services. For instance, the access network domain will be impacted by the support of Mobile Edge Computing (MEC) that provides enhanced functionality at the edge of the network. Some sensitive functions currently performed in the physically and logically separated core are likely to be moved closer to the edge of the network, requiring relevant security controls to be moved too.
  Interested domains: Network, Application
- **Increased software and services embedded in networking.** Nowadays, software is increasingly permeating networking, bringing more functionalities and flexibility, but also enlarging attack surfaces. Software Defined Networks (SDN) and Network Functions Virtualisation (NFV) technologies are moving the traditional network architecture built on specialised hardware and software to virtualized network functions. The consequence is an increased exposure to third-party suppliers and importance of robust patch management procedures. 5G will be based on this ecosystem of networking services. Any software vulnerability will become more significant in this context. In the report about the EU coordinated risk assessment of the cybersecurity of 5G networks,[15] published on 9 October 2019, core network functions of the 5G network are underlined as critical because affecting the core network may compromise the confidentiality, availability, and integrity of all network services. Also, management systems and supporting services are considered critical assets since they control important network elements and can therefore be used to conduct malicious activity, such as sabotage and espionage. Moreover, the loss of availability or integrity of these systems and services can disrupt a significant portion of 5G network functionalities.
  Interested domains: Network
- **Artificial Intelligence as a booster of cybersecurity attacks.** The adoption of Artificial Intelligence and Machine Learning techniques can substantially expand the attack surface of every domain, permitting to discover vulnerabilities both in software components and in business process logic[4]. Artificial intelligence and machine learning techniques are at the basis of many business decisions and the success of the inferences based on them can result in a huge (economic) value. For these same reasons, they become targets of attacks by cyber criminals. On one side, data poisoning become a huge driver towards more complex attacks. On the other side, model poisoning aims to poison the source of training data in order to fake the learning algorithm in considering a malicious behavior as a normal one. In this context, adversarial machine learning had a huge boost and become a hot research topic, while computation architectures, such as Big data platforms, are enabling these threats on a large scale. An example of how powerful the AI is becoming thanks to the amount of data currently available and the computation capability of the distributed architecture is the current increasing trend of the deepfake.[16] Differently from the past, attackers are targeting person's reputation to gain an advantage and to play a scam (e.g., artificial intelligence-generated voice deepfake).
  Interested domains: System, Data, User
- **Social Media and Social Networks Threats.** Social media and social networks represent another source of emerging cybersecurity threat for the user-centered domain. The raise of social bots, that is, automatic software agents disguised as humans, is widely debated, for example in connection with the adoption of Artificial Intelligence methods able to replace humans interacting over social media. However, social bots might become a problem for cybersecurity too, for example in the case of phishing[5], for the spread of disinformation [6][7], or political propaganda[8]. In general, social bots for social media[9] and Artificial Intelligence for software tools involved in decision processes [10][11] are widely considered as both a remarkable opportunity and possibly an insidious threat for people, in both cases a challenge for future systems, organizations, and institutions[12].
  Interested domains: System, Data, User
- **Layered and Virtualized Systems.** Current systems are based on several software layers, often including a virtualization layer. In layered systems, the security of the upper layers relies on the security of the lower ones, forming a chain where each layer can be the weakest one. The trend is to increase the level of sharing and the density of the multitenancy, exacerbating the impact of most of the threats. In addition, weaknesses of traditional systems based on specific OSs will be inherited as well in the context of each layer. Specific threats for the layer protection mechanisms are evolving starting from virtualization and containment escape to cross layer hijacking. In general, containment, isolation, and sandboxing mechanisms will expose vulnerabilities in the future and their exploitation are normally associated to a very high-risk score.
  Interested domains: System, Network
- **Misconfigurations of security mechanisms and lack of transparency.** Given the complex multi-layer nature of current

[15] EU-wide coordinated risk assessment of 5G networks security https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

[16] A Voice Deepfake Was Used To Scam A CEO Out Of $243,000 https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/114964a22241

architectures, misconfigurations and in general issues due to the lack of transparency are largely considered as among those with the most severe impact. According to CSA, misconfigurations and inadequate controls will become increasingly problematic especially in cloud environments, as well as weaknesses in authentication, lack-of-control, and visibility, while more traditional threats to confidentiality based on malicious code are becoming less important for cloud and virtualization.
Interested domains: System

- **Business process compromise.** BPC traditional threats are becoming more and more diffuse nowadays for business process implemented in the cloud. This is possible also due to the advanced AI capabilities of an attacker to improve BPC-based attacks. Such attacks are able, for instance, to exploit behavioral information via shadow IT, which is increasing due to the plethora of services that are becoming part of daily activities of employees. The current lack of insurance tools capable to mitigate this behavioral-oriented threat should be addressed in the future.
  Interested domains: System, Network
- **Human errors.** One notable trend is that human interactions with machines, and in particular the proportion of workers whose place of work is strongly intertwined with IT technologies, has increased fast in the last decade, as clearly analysed by the European Agency for Safety and Health at Work[13]. A human mistake is more likely than in the past to be the possible cause for failures in machine-controlled processes, a broad category that includes cybersecurity incidents. The reason is in the more frequent presence of human-machine interfaces in business processes as well as in the increasing complexity of digital-physical interactions in workplaces. Often, it could turn out to be mostly (i) a problem of business procedures, (ii) employees under the pressure of a tight schedule or with conflicting requirements between security and productivity, or (iii) even a consolidated usage of a technology, not aligned with original specification, that the company has tolerated (or promoted) along many years[14]. The healthcare is a sector that presents sensible user-centered threats and is often mentioned as one mostly endangered by emerging cybersecurity threats[15]. Not only healthcare personal information of patients is leaked or mismanaged, a type of security incident that hardly could be called "emerging"[157], but also medical devices are considered at risk and increasingly exposed to cybersecurity threats[16].
  Interested domains: All
- **Skill shortage and configuration errors.** Today, single and not-expert users are directly involved in complex business processes and can influence them. Configuration errors are therefore increasing as never seen before, introducing a huge amount of new opportunities for cyber criminals to affect the CIA (Confidentiality, Integrity, Availability) properties of systems and users. For instance, security misconfigurations such as wrong access policies, weak passwords, unpatched systems, and the like, make the overall environment unsecure. Personal data of the users can be stolen and sold on the black market. Entire systems can be hijacked and remotely controlled, while specific sensors/devices put offline by exhausting their resources. Portion of the whole system can be compromised to launch more complex attacks (e.g., Mirai botnet).
  This complexity is even exacerbated when the architecture requires interdisciplinary competences in order to be used like in case of Big Data architecture. Privacy implications of Big data processing are connected with the computation architecture, as well as with the algorithms, models, and learning peculiarities. The increase in system and platform complexity does not find a counterpart in the skills and competences, resulting in an important lack of data scientists able to properly manage such new technologies. Human errors in system configurations are still at the forefront of the issues driving new and old attacks.
  Interested domains: All
- **Data breaches.** The fundamental role assumed by data in every aspect of our life makes attacks that aim to data breach and leak increasing.[17] In this context, traditional attacks like phishing and (D)DoS are reviving a new boost and mainly target the CIA triad of data. Given the potential huge revenue for attackers stealing data, targeted phishing attacks and malwares have been presented in the last few years. For example, phishing attacks are not aiming at big numbers of compromised users, but rather they target rich individuals, people with access to financial accounts or sensitive business data, or even public authorities that handle PII related data.[17] As another example, malwares mostly target data and in particular unauthorized data wiping, modification, access. They count 30% of all data breaches incidents.[18]
  Moreover, the EU General Data Protection Regulation (GDPR) that became applicable as of May 2018 introduced a series of novelties, including the mandatory reporting of data breaches to the competent authorities, provided that certain requirements are met. Today, a data breach or leakage can become a new weapon in the cybercriminal hands, which will increase the number of extortion attacks with the threat of GDPR penalties deriving from data disclosure. Note that the reporting of security incidents to competent authorities is, also, dictated under then Directive on the Security of the Networks and Information Systems (NIS Directive) that was to be transposed to the national legal orders of the Member States by May 2018.
  Interested domains: All
- **Applications and software everywhere.** As applications are spreading at all layers of ICT systems, attacks targeting them are spreading as well. Malware attacks continue to rule the roost, particularly targeting cloud (and IoT) applications. Ransomware are still strong in this area and difficult to challenge by national law enforcement agencies alone. Mobile malware is growing exponentially since 2017, following the increase in the use of mobile systems, such as mobile banking that is overtaking online banking.[19] In this context, it is quite likely that a growth and development of mobile malware targeting users and applications will be observed.
  Interested domains: Application
- **Complexity of the application deployment environment.** Traditionally, the application deployment environment is considered quite stable. It is handled as a landing platform for the application development. Nowadays, the complexity and

[17] WP2018 O.1.2.1 - ENISA Threat Landscape 2018 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/

[18] 2018 Verizon Data Breach Investigations Report, https://www.researchgate.net/publication/324455350$_{2}018_{V}erizon_{D}ata_{B}reach_{I}nvestigations_{R}eport$

[19] Europol, Internet Organised Crime Threat Assessment (IOCTA), Strategic, policy and tactical updates on the fight against cybercrime https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf

dynamics of the surrounding environment are changing this scenario. The increase in platform complexity and the proliferation of many (third-party) libraries open the door to new attacks (e.g., privilege escalation, hijacking, code execution) that threaten not only the platform itself, but also the users relying on it.
Interested domains: Application

- **Service miniaturization.** The advent of microservice architecture has increased the revenue for enterprises and supported new businesses, at the same time neglecting non-functional properties such as security and privacy. This scenario represents one of the most important challenges to be faced in the next years. The miniaturization of services but also of devices (IoT sensors), as well as the pervasive and continuous involvement of humans in the functioning loop have resulted in an environment with an unprecedented level of risk.
  Interested domains: Application, Device/IoT, System
- **Cyber-physical systems as enablers of next-generation attacks to users.** Cyber-physical systems have brought changes to several aspects of daily life, like in electrical power grids, oil and natural gas distribution, transportation systems, healthcare devices, household appliances, and many more. They clearly could show a relevant user-centered component, either for their development and maintenance, or the consequences of their operation. As often is the case with emerging technologies, they are often riddled with security vulnerabilities that could easily become threats to users and individuals[17].
  Interested domains: Human, Device/IoT, System

The following list represents an overview of the identified key takeaways and their corresponding domains:

Table 1. Key takeaways: Summary

Key Takeaways	Interested Domains
Endemic persistent threats	All
Balance security and domain-specific constraints	All
Relation between security and safety	All
Physical access and insider threats	Device/IoT, System
User Profiling	Device/IoT, Data, User
Diffusion of Ultra Wideband networks	Device/IoT, Network
Decentralization and computation capability at the edge	Network, Application
Increased software and services embedded in networking	Network
Artificial Intelligence as a booster of cybersecurity attacks	System, Data, User
Social Media and Social Networks Threats	System, Data, User
Layered and Virtualized Systems	System, Network
Misconfigurations of security mechanisms and lack of transparency	System
Business process compromise	System, Network
Human errors	All
Skill shortage and configuration errors	All
Data Breaches	All
Applications and software everywhere	Application
Complexity of the application deployment environment	Application
Service miniaturization	Application, Device/IoT, System
Cyber-physical systems as enablers of next-generation attacks to users	Device/IoT, System, User

Conclusions

Due to the digitalization and emerging trends brought with it, that have permeated into every aspect of the everyday's life and gained importance in ensuring the prosperity of the economy, information sharing has been seeing a steady growth in the past decade. Therefore, there has been an ever-increasing requirement to better prepare and protect which comes with a necessity to shift the attitude to "need to share". Consequently, the threat landscape has been rapidly transforming to adhere to the evolution of software, IoT, services and cloud computing. In order to get a clear view of the current state-of-the-art cybersecurity, attacks and threats, there is a necessity to have an up-to-date overview of the nascent threats and attacks. Based on the state-of-the-art literature findings, CONCORDIA cybersecurity threat analysis attempts to accomplish this objective by considering six research domains, including: i) IoT/device-centric, ii) network-centric, iii) system-centric, iv) data-centric, v) application-centric, vi) user-centric, and identifying cybersecurity threats and assets related to every domain. The report further classifies each identified threat group to the corresponding subcategories and provides summary for each. Ultimately, a list of 20 key findings emerging from a threat landscape is outlined, and each of the key findings is thoroughly described. Most importantly, the identified key findings are mapped with the related domains. Appendix section of the whitepaper provides readers with more information about each of the identified domains, as well as about each of the classified threats

Appendix

In the following we present a more detailed discussion about threats for each of the identified domains.

Device/IoT-Centric Security

The exponential growth of connected devices (from minuscule sensors to bigger machines), which, according to Intel[5] are expected to reach 200 billion by 2020, is revolutionizing current IT systems. Smart transportation, sustainable mobility, smart cities, e-health, smart vehicles, UAVs, and many more are just some examples of domains where IoT, edge computing, and smart devices are changing the environment. The existence of billions of resource-constrained devices connected to the Internet introduces fundamental risks that can threaten users' life and personal sphere. Current environments are so pervasive and ubiquitous that users just become another component of the system.

Threats

We discuss the threats that can be mapped to the Device/IoT asset taxonomy. In general, the IoT scenario revolutionizes the concept of security, which becomes even more critical than before. Security protection must consider millions of devices that are under control of external entities, freshness and integrity of data that are produced by these devices, and heterogeneous environments and contexts that co-exist in the same IoT environment[18]. Trend Micro, a cybersecurity solutions provider, stated that the IoT has become a primary target for cybercriminals. The SonicWall 2019 report shows that IoT malware increased 55% and threats related to encryption spiked 76% compared to the 2018.[20] This trend leads to an increment in budget for security in IoT. According to Gartner,[21] the IoT security in IoT budget will reach $3.1 billion in 2021. Concerning attack vectors in IoT, according to F-Secure Attack Landscape H1 2019, the Telnet protocol is the one mostly used among the TCP-based ones while the UPnP is the top exploit among the UDP ones.[22] Given the peculiarity of IoT devices, which are in many cases outdated embedded systems, F-Secure estimated half a billion IoT devices vulnerable to 10-year-old vulnerabilities.
Even considering the heterogeneous nature of the assets belonging to the Device/IoT domain, the IETF definition of threat, namely, "a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm", is general enough to cover with all the IoT threats. IoT has a specific peculiarity: the strong link between security leakages and safety. ITU-T in its report Y.4806 underlines this link identifying a list of threats that are capable to affect safety. OWASP identifies in the 2018 the top 10 IoT security threats where weakness of passwords, network services and interfaces are identified as the top three threats.
We remark that Botnet is a security concern typically involving IoT but not very often targeting IoT itself. Botnets normally exploit IoT vulnerabilities to infect the devices. Initially, IoT botnets were grounded on manual physical malicious activities on the devices (TG1.3) or on exploiting the access control weaknesses and default passwords (T1.1.1). Later attackers focused on protocol weaknesses (TG1.2) vulnerabilities in general (TG1.4) and diffusion via malware. Recent botnets adopt hybrid approaches to infect the devices therefore they can be associated to different threats. In the following, we associate specific botnet of threat groups considering the principal threat type used to establish the botnet. In addition, proxy threats are common where a compromised device is used as a proxy to launch attacks hiding the identity of the attacker. In this case, no infection is needed, just the reuse existing functionality.

Threat Group TG1.1: Unintentional damage/loss of information or IT assets

Threat T1.1.1: Information leakage/sharing due to human errors

Human errors are among the most critical threats in today complex environment. These threats are accidental, meaning that they are not intentionally posed by humans, and are due to misconfiguration, clerical errors, misapplication of valid rules and knowledge-based mistakes. In IoT, most errors are related to poor/absent patch management, the adoption of weak passwords or failure to update default ones, as well as to wrong authorization configurations. Device authentication or device authorisation may need a non-trivial human intervention since Internet objects ("things") usually do not have apriori knowledge about their ecosystem. The well-known lack of specialized IoT cybersecurity competences (even when only simple, "basic hygiene" security is needed) plays an important role in increasing the errors at this level (see Threat T1.6.1).
Assets: It refers almost to every asset groups. More in details it refers to "Data", "Device", "Infrastructure", "Platform and backend", "Decision making".

Threat T1.1.2: Inadequate design and planning or incorrect adaptation

[20] SonicWall Mid-Year update report

[21] Gartner Says Worldwide IoT Security Spending Will Reach $1.5 Billion in 2018 https://www.gartner.com/en/newsroom/press-releases/2018-03-21-gartner-says-worldwide-iot-security-spending-will-reach-1-point-5-billion-in-2018

[22] ATTACK LANDSCAPE H1 2019 https://s3-eu-central-1.amazonaws.com/evermade-fsecure-assets/wp-content/uploads/2019/09/12093807/2019$_{a}ttack_{l}andscape_{r}eport.pdf$

IoT devices rely on software that might contain severe bugs due to wrong design choices and absence of a reliable adaptation/update strategy to fix such errors. This makes the devices vulnerable to many different types of attacks from buffer overflow to lack of authentication (well-known, easy-to-guess, hardcoded password for device configuration). This can be considered one of the most important security threats, and in many cases, it is exploited to generate botnet attacks. IoT still misses an effective adaptation planning strategy to cope with this type of threats. This threat is therefore strongly connected with TG1.3.
Assets: “Device”, “Infrastructure”, “Platform and backend”, “Management”.

Threat Group TG1.2: Interception and unauthorised acquisition

Threat T1.2.1: Interception of information

This threat considers an attacker intercepting a communication between two communicating parties. In IoT network, not all the communication channel is sufficiently protected, for instance if keying material, security parameters, or configuration settings are exchanged in clear or if weak or unsuitable/vulnerable cryptographic algorithms are used. Related attacks include man-in-the-middle, communication protocol and session hijacking, or message replay. The man-in-the-middle attack rely on the fact that both the commissioning and operational phases may be vulnerable. In IoT, it is normally assumed that no third parties can eavesdrop during the execution of key materials exchange protocol (i.e., communication in clear form). IoT communication protocol hijacking takes advantage of the possibility to “sniff” the traffic and then uses aggressive techniques like forcing disconnection or reset. In case of session hijacking, attack activities are oriented to act as a legitimate host/device to steal, modify or delete transmitted data. In addition, device authentication or device authorization may be nontrivial or need human intervention (see Unintentional damage / loss of information or IT assets threat group), since devices usually do not have a priori knowledge about the rest of the ecosystem or completely automatic mechanisms to differentiate legitimate and illegitimate devices (see physical threat group). An attacker with low privileges can misuse additional flaws in the implemented authentication and authorization mechanisms of a device to gain more privileged access to the device itself obtaining elevation of privilege.
Another attack that fits the IoT domain is the "harvest and decrypt" attack in which an attacker can start to harvest (store) encrypted data today and decrypt it years later, once a quantum computer is available (e.g., VENONA project[23]). This is linked to the fact that many IoT devices remain operational for a decade or even longer, and during this time, digital signatures used to sign software updates might become obsolete, making the secure update of IoT devices challenging. Reply attack uses a valid data transmission maliciously by repeatedly sending it or delaying it, in order to manipulate or crash the targeted device.
Assets: “Device”, “Infrastructure”, “Security mechanisms”.

Threat T1.2.2: Unauthorised acquisition of information

IoT networks can be spoofed, altered, or replayed, to create routing loops, attract/repel network traffic, extend/ shorten source routes, to name but a few. As an example, via sybil attack an attacker can present multiple networking level identities to other devices in the network.
In addition, IoT can be subject to disclosure of sensitive data, intentionally or unintentionally, to unauthorised parties. Confidential data may be captured by attackers from individual devices, during transit, or from the backend, local storage, edge nodes (information acquisition via physical access is described in TG1.3). Privacy must be also considered, for instance, when the sensor is transmitting sensible data like health-related data and when device location tracking provided by the device poses a privacy risk to users. This threat shares most of the attack strategies with Networking Domain. In the following, we describe some of them showing a clear connection with IoT environment where nodes can be manipulated/added more easily.
Assets: “Device”, “Infrastructure”, “Platform and backend”.

Threat Group TG1.3: Intentional physical damage

Threat T1.3.1: Device modification

Having physical access to the IoT device allows a non-trusted factory to clone the physical characteristics, firmware/software and security configuration of a device. Deployed devices might also be compromised and their software reverse-engineered, allowing for cloning. Cloned devices may be sold cheaply in the market and can contain functional modifications including backdoors. Alternatively, a genuine device may be substituted with a variant or clone during transportation, commissioning or in operation. Another substitution is a firmware level substitution that is less expensive and less easy to discover that physical cloning or replacement. In some cases, this substitution occurs in the framework of a patching or upgrading, and it may or may not requires physical access (we include this type of attacks in this threat

[23] VENONA https://www.nsa.gov/news-features/declassified-documents/venona/

for simplicity even if they can be obtained without full physical access). Other attacks that refer to this threat are device replication, camouflage, malicious device/node injection, to name but a few.
Assets: "Device", "Infrastructure".

Threat T1.3.2: Extraction of private information

IoT devices are often physically unprotected. This allows physical attacks to extract private information such as keys, data from sensors (for example, healthcare status of a user), configuration parameters (for example, the Wi-Fi key), or proprietary algorithms (for example, the algorithm performing some data analytics task).
Assets: "Device".

Threat Group TG1.4: Nefarious activity/abuse

Threat T1.4.1: Identity fraud

Identity fraud in IoT primarily refers to both weak user/admin credentials and authentication, which is a quite diffuse threat for IoT (at the top of the OWASP top Ten), and identity spoofing, which involves authentication protocol leakages in IoT, for instance, at device bootstrapping time. Poor credential management such as weak password choices or lack of multi-factor authentication for user and administrative interfaces of devices, gateways or back-ends, is a common vulnerability in many information systems and even exacerbated in IoT due to the limitations at device side. Passwords/credentials are in most of the cases guessable, weak and hardcoded at firmware level. Identity fraud in IoT can be obtained due to weakness of the identity provisioning protocols that can be spoofed.
Assets: "Device", "Infrastructure", "Platform and backend".

Threat T1.4.2: Denial of service

Traditional (Distributed) Denial of Service is a major threat for IoT where devices, being resource-constrained, are more susceptible to denial of services. It aims to threaten components availability by exhausting their resources, causing performance decrease, loss of data, service outages, on one side, but also potential safety issue, on the other side. In addition, compromised devices themselves are often used to disrupt the operation of other networks or systems via a Distributed DoS (DDoS) attack (see TG physical). Here we consider DoS that targets IoT not generated by IoT devices.
Assets: "Device", "Infrastructure", "Security mechanisms", "Platform and backend".

Threat T1.4.3: Malicious code/software/activity

This class of threats usually targets all ICT stack and the aforementioned 6 domains. They aim to distribute and execute malicious code/software or execute malicious activities. These threats usually involve malware, exploit kits, worms, trojans, and exploit backdoors and trapdoors, as well as developer errors/weaknesses. Devices can be infected with such malicious programs due to vulnerabilities in software or firmware, that are much more diffuse that in other domain due to the difficulties in keeping an IoT device updated. An IoT specific threat that is difficult to discover, is the counterfeit device since it cannot be easily distinguished from the original. These devices usually have backdoors and can be used to conduct attacks on other ICT systems in the environment in most of the cases botnet type of attacks.
Assets: "Device", "Infrastructure", "Security mechanisms", "Platform and backend".

Threat T1.4.4: Misuse of assurance tools

Assurance is the way to gain justifiable confidence that a system will consistently demonstrate one or more security properties, and operationally behave as expected, despite failures and attacks [19]. Assurance is based on audit, certification, and compliance tools and techniques [20][21]. The manipulation of such tools and techniques can result in scenarios where the malicious behavior of attackers is masqueraded and is not discovered. Assurance information is necessary to ensure the security of the system during its entire lifecycle from its design to its operation. It is also necessary due guarantee compliance and regulation. In IoT environment the adoption of assurance is even more crucial due to the need to cope with the lack of security mechanisms at the peripheries.
Assets: "Data", "Device", "Platform and backend", "Infrastructure", "Security mechanisms", "Management".

Threat T1.4.5: Failures of business process

Poorly designed business processes can damage or cause loss of assets. IoT can be part of a complex system handling sensible data, like in case of health or industrial application. Threats to confidentiality of sensor data (e.g., wrong delivery through untrusted gateways) and integrity of sensor data (e.g., the use of temporal local tamperable data store) can have high impact.
Assets: "Device", "Platform and backend", "Infrastructure", "Security mechanisms", "Management".

Threat T1.4.6: Code execution and injection (unsecure APIs)

IoT applications are built on web services models and in many cases each device offers APIs can then become a target of attack, and be vulnerable to well-known attacks, such as the Open Web Application Security Project (OWASP) Top Ten list.[24] This threat is listed as the third mostly risky in the OWASP Top 10 IoT due to the fact that i) IoT offers poor administrative interfaces and ii) due to budget restrictions, IoT vendors do not dedicate much budget on its security and testing. In particular, code execution (e.g., XSS) and injection (e.g., SQL injection) are critical attacks that can increase risks.
Assets: "Platform and backend", "Security mechanisms", "Management".

Threat Group TG1.5: Legal

Threat T1.5.1: Violation of laws or regulations

The management of legal aspects impacts IoT system and can represent a threat to the system itself. As mentioned earlier the legislation landscape on IoT is quite complex, and IoT systems potentially involve devices produces under different legislations and regulations. Violations of laws or regulations, the breach of legislation, the failure to meet contractual requirements, the unauthorized use of Intellectual Property resources, the abuse of personal data, the necessity to obey judiciary decisions and court orders are examples of threats. Also, the lack of cyber-regulations in countries with high concentration of hacker groups is having an impact with these regards. In January of 2018, Cyber Security Research Institute report into the Internet of Things sponsored by F-Secure stated that IoT represents a considerable threat to consumers, due to inadequate regulations regarding its security and use.[25] In some scenarios the situation is even more complex due to the ubiquitous nature of IoT sensors. For instance, Google was forced to announce in early 2018 that its Nest Security system included a microphone that was not disclosed to consumers.[26]
Assets: All assets.

Threat Group TG1.6: Organisational threats

Threat T1.6.1: Skill shortage

A possible shortage of skilled IoT cybersecurity experts is one of the main threats to IoT. Another aspect is the lack of security awareness at management level.[27] This threat has a strong link to threat group TG1 "Unintentional damage / loss of information or IT assets". The F-Secure chief, Mikko Hypponen declared in 2017 that "many IoT device vendors have little to no experience in building internet-connected devices," and "they build IoT devices to be cheap and to work, but not to be secure."[28]
Assets: "Roles".

Network-Centric Security

Traditional network environments are characterized by well-defined perimeters and trusted domains. Networks have been initially designed to create internal segments separated from the external world by using a fixed perimeter. The internal network was deemed trustworthy, whereas the external was considered potentially hostile. Perimeter devices, such as firewalls and intrusion detection systems, have been the traditional technologies used to secure the network.

Threats

In this section, we discuss the threats that can be mapped to the network asset taxonomy. The threats reported here are not exhaustive but representative of the matters covered. Most of them are related to mobile network considering the network evolution toward 5G and the fixed-mobile network convergence. This section provides an overview of the main relevant security issues. Most of them are already known and under the attention of different standardization bodies, security working groups, and an alliance that is working on them by providing guidelines and countermeasures as well as configurations hardening. However, despite such actions, some of these attacks are still ongoing. This is in part motivated by the availability of open-source attack tools.
For several years now, vulnerable network assets have been exploited as preferred targets. Malicious cyber actors often target

[24] Many common vulnerability exposures for Big Data components, such as Hadoop, are reported in specialized Websites, see for example https://cve.mitre.org and https://www.cvedetails.com

[25] PINNING DOWN THE IOT https://fsecurepressglobal.files.wordpress.com/2018/01/f-secure$_{p}inning - down - the - iot.pdf$

[26] Users alarmed by undisclosed microphone in Nest Security System https://arstechnica.com/gadgets/2019/02/googles-nest-security-system-shipped-with-a-secret-microphone/

[27] See https://www.justice.gov/usao-ndca/pr/sunnyvale-based-network-security-company-agrees-pay-545000-resolve-false-claims-act

[28] Should You Fear the IoT$_{R}eaper?https : //blog.f - secure.com/should - you - fear - the - iot_{r}eaper/$

network devices, and, once on the device, they can remain there undetected for long periods. After an incident, where administrators and security professionals perform forensic analysis and recover control, a malicious cyber actor with persistent access on network devices can reattack the recently cleaned hosts. The adoption of a Security Assurance process that covers the entire life cycle management starting from secure design, secure development, secure deployment, security monitoring, and security management is necessary to counteract these attacks. There are also cases where attackers do not need to compromise their intended target directly but can achieve their aim by compromising the supply chain where it is least secure. In the last years, there was, in fact, an increase in breaches caused by vulnerable software. Any given software stack can contain many sources of components and libraries in differing versions, increasing the need to assess, test, and patch carefully. This potential threat highlights the importance of managing the supply chain.

Another source of well-known network breaches is the use of legacy protocols. Signaling exchange is required to establish and maintain a communication channel or session on telecommunication networks as well as allocate resources and manage networks. For example, a 2/3G network uses SS7 (Signalling System 7) and SIGTRAN (SIGnalling Transport) while 4G relies on Diameter; all generations use SIP (Session IP) and GTP (GPRS Tunnel Protocol). Many fundamental services, such as short messaging service (SMS), are managed by these protocols. Many of these signaling protocols are outdated and have been implemented under a trust model that assumed well-behaved mobile operators without the need to deploy strong security controls. In addition, another type of attack vector comes from flaw in the specifications. The paper in [19] is an example of vulnerabilities discovered during a careful analysis of LTE access network protocol specifications and a demonstration of how those vulnerabilities can be exploited using open source LTE software stack and low cost hardware. The paper in [20] demonstrates instead the usefulness of adopting formal verification tool to automatically check whether the desired security properties are satisfied or if instead the defined protocols/procedures suffer from ambiguity or under-specification.

To complete our overview of the attack scenario, another vector comes from poor configuration of network nodes as highlighted in [21]. In the following section, the most relevant network threats are reported according to their respective categories.[29][30]

Threat Group TG2.1: Unintentional damage/loss of information on IT assets

Threat T2.1.1: Erroneous use or administration of devices and systems

Attacks or human-errors are exploited to gain unauthorised privileged access to a system, which can lead to the installation of other malicious content or backdoors or even physical access to the devices. It is used as part of an attack, regardless of whether the target is a single system/asset or a whole network or facility.
Assets: “Core Network”, “Access Network”, “Infrastructure Network/Area Network”, “Peering Points”.

Threat Group TG2.2: Interception and unauthorized acquisition

Threat T2.2.1: Signaling traffic interception

Most signaling protocols are dated and implemented in an insecure way. Some of them have not been designed with any security features. SS7 (Signaling System 7) and Diameter are signaling protocols used in mobile networks. It is widely known that these signaling protocols have no security defenses built in and have several severe security weaknesses, which can be exploited by attackers in many ways. SS7 is used to exchange information among different elements of the same network or between roaming partner networks (e.g., call routing, roaming information, features available to subscriber). Diameter is the replacement of SS7 for the 4G mobile network. An adversary could exploit signaling system vulnerabilities to redirect calls or text messages (SMS) to a phone number under the attacker’s control.
Assets: “Core Network”, “Peering Points”. The exploitation of SS7 design weaknesses to obtain a victim’s location, harvest their messages, and listen in on calls was demonstrated in 2014.[31] Other examples are the demonstration in [32] and [33]. O2 in Germany confirmed that some customers in Germany have had their accounts drained by attackers that used SS7 to intercept and redirect mTANs to their own phones.[34] In [35], an attempted Data interception attacks using SS7 was reported.

Threat T2.2.2: Data session hijacking

[29] Mobile Telecommunications Security Threat Landscape, GSMA, January 2019 https://www.gsma.com/aboutus/resources/mobile-telecommunications-security-threat-landscape

[30] Threat Landscape 2018, ENISA https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape

[31] White hats do an NSA, figure out LIVE PHONE TRACKING via protocol vuln https://www.theregister.co.uk/2014/12/26/ss7$_a$*ttacks/*

[32] Tobias Engel, “SS7: Locate. Track. Manipulate”, 2014, https://imsicatcher.info/article/ss7-locate-track-manipulate/

[33] “SS7 Attack Discovery” , Positive Technologies, 2016 https://www.ptsecurity.com/upload/corporate/ww-en/products/documents/ss7/PT-TAD-Product-Brief-eng.pdf

[34] Schwachstelle im Mobilfunknetz: Kriminelle Hacker räumen Konten leer https://www.sueddeutsche.de/digital/it-sicherheit-schwachstelle-im-mobilfunknetz-kriminelle-hacker-raeumen-konten-leer-1.3486504

[35] Tunnel Vision : Malicious data interception via SS7 https://www.adaptivemobile.com/blog/malicious-data-interception-via-ss7

Session Hijacking is an attack which is basically used to gain an unauthorized access between an authorized session connection. For example the GPRS Tunnelling Protocol (GTP) allows mobile subscribers to maintain a data connection for Internet access while on the move. GTP manages tunnels for transporting IP packets throughout the core network to the internet. GTP comprises three parts—control plane (GTP-C), user plane (GTP-U) and charging (GTP-C). Since there is no authentication and encryption supported in GTP-U messages themselves, several attacks to GTP-U might be possible. An attack via the GRX global roaming exchange network can be conducted by employees of almost any mobile operator as well as by external attackers who have access to the operator's infrastructure. Such an attacker might be able to craft GTP-U messages and send them to the network to trigger answer messages and thus get information (e.g. about network topology), or just send malicious messages to the network. This may involve guessing a valid TEID (Tunnel Endpoint Identifiers), hijacking a TEID, unless the endpoints use non-predictable TEIDs.

Other common hijacking attacks exploited the vulnerabilities of Border Gateway Protocol (BGP). They are documented for instance in IETF's RFC 4272 "BGP Security Vulnerabilities Analysis", which was published in 2006. BGP fundamental vulnerabilities related to the lack of a mechanism to protect integrity and authenticity of messages in peer-to-peer communications. Also, the lack of a mechanism to validate the authority of an AS (Autonomous system) to announce prefixes or relay route information. Finally, BGP has no mechanism to validate the authenticity of the path attributes in prefix announcements. These security vulnerabilities can be exploited by an adversary to perform BGP hijacking, when the adversary claims to be the origin of prefixes of another network. The result of this attack is that the traffic is forwarded to the wrong destination. This attack can be used to intercept, alter, or disrupt Internet traffic.

Assets: "Core Network", "Peering Points".

Threat T2.2.3: Traffic eavesdropping

An eavesdropping attack is possible if the traffic is not protected, e.g. user-plane traffic is not encrypted at the radio access level or if vulnerable/weak crypto algorithms are used. Eavesdropping is also possible by exploiting lack of protection on the backhaul link that connect radio access network to core network. In 4G networks the backhaul is composed of IP-based control elements and interfaces, making it vulnerable to IP-based attacks. In addition, eavesdropping can be possible also by exploiting the lack of mutual authentication between the radio access node and the core network, or the lack of prevention against IP-based attacks, or the lack of encryption of data and signaling traffic. If the backhauling link is not encrypted, then user security context information such as part of the currently used keying material will be revealed to an eavesdropper. Also, the user plane traffic would be available to eavesdroppers in the clear. The impact of eavesdropping depends on what traffic is affected. Eavesdropping control plane traffic can be more critical as it may reveal information to the attacker that allows him to mount further attacks.

Assets: "Radio Access Network", "Infrastructure Network/Area Network".

Threat T2.2.4: Traffic redirection

Redirection of data can be accomplished at different levels. On local networks IPv4 ARP spoofing, ipv6 router advertisement or automatic proxy discovery can be exploited. At the internet level DNS spoofing is widely used to point legitimate hostnames to fake servers. Ultimately, redirection of data can be possible by data manipulation that can be especially performed if data is not integrity protected. **Assets:** "Access Network", "Core Network".

Threat Group TG2.3: Nefarious activity/abuse

Threat T2.3.1: Exploitation of software bugs

The more the network environment will be software-defined, virtualized and transferred on general commodity hardware equipment, the more such environment could be exposed to vulnerabilities due to software bugs and poor configuration. Already today every year thousands[36] of software bugs impacts network devices such as routers, servers, databases or other functional elements of the networks. This type of threat also includes network failures when several systems fail to connect or to work together.

Through software bugs it is possible to attack the vulnerable device or the entire infrastructure causing, for instance, DoS, frauds, and other issues. To help customer to manage such situations, many network manufacturers such as Cisco, Juniper, Ericsson, Huawei set up specific PSIRT (Product Security Incident Response Team) Services, aimed to collect, analyse, and provide patches related to their products and finally to help their customers to address the possible issues suggesting related solutions.

Assets: "Access Network", "Core Network", "Infrastructure Network/Area Network", "Endpoint Network".

Threat T2.3.2: Manipulation of hardware and firmware

Attacks against hardware and firmware are especially appealing to attackers. Once they have compromised the firmware, they can safely persist on the device and evade the security measures applied at OS, application or software levels. Since the malicious code lives within the firmware of physical components, the threat can easily survive a complete reimaging

[36] See https://www.cvedetails.com/vulnerabilities-by-types.php

of the system or even replacement of the hard drive(s). This sort of persistent attack would typically occur as a second stage of malware infection. Once a system is initially compromised, malware could then look for vulnerabilities in the firmware and missing device protections that could allow malicious code to be implanted in the firmware itself. This threat clearly points also to Device/ IoT-centric security.
Assets: "Core Network", "Infrastructure Network/Area Network", "Endpoint Network".

Threat T2.3.3: Malicious code/software/activity

Malware is any piece of software written with the intent of damaging devices, stealing data, or causing a damage. Viruses, Trojans, and recently crypto-miners and ransomware are among the different kinds of malware. Although the primary target for the malware is traditionally to "infect" a device (fixed or mobile), malware is one of the main threats against network infrastructures (e.g. the control plane), and it will be even more dangerous with the emerging networks softwarization. When devices are considered, this threat is strongly connected to threat T1.4.3 in Device/IoT-centric security.
Assets: "Core Network", "Endpoint Network".

Threat T2.3.4: Remote activities (execution)

Remote activities can take a variety of forms, but in general refer to the process by which an agent can exploit a network vulnerability to run, for example, arbitrary code on a targeted machine or system.
Assets: "Core Network".

Threat T2.3.5: Malicious code - Signaling amplification attacks

Mobile networks do not have enough radio resources to provide service to every single customer at the same time. The scarcity of bandwidth requires advanced techniques to reuse idle resources in an efficient manner. The RRC protocol stack reassigns radio resources from a given user when the connection goes idle for a few seconds. When an inactivity timer expires, the radio bearer between the mobile device and the core network is closed and those resources become available to be reassigned to another UE. At this stage, the UE moves from connected to idle state. Each instance of bearer disconnection and setup involves a significant number of control messages exchanged among nodes within the EPC (Evolved Packet Core). DNS amplification is another example of attack that massively exploit open recursive DNS servers mainly for performing bandwidth consumption (DDoS attacks). The amplification effect lies in the fact that DNS response messages may be substantially larger than DNS query messages.
Assets: "Access Network", "Radio Access Network“, "Core Network".

Threat Group TG2.4: Organization (failure malfunction)

Threat T2.4.1: Failures of devices or systems

System failures includes the incidents caused by failures of a system, for example hardware failures, software failures or errors in procedures or policies. An example is a software bug in a system like an HLR that suddenly stops its operation and consequently prevents al subscribers from connecting. This threat clearly points also to Device/IoT.
Assets: "Access Network", "Core Network", "Infrastructure Network/Area Network".

Threat T2.4.2: Supply chain

A supply chain threat refers to the compromise of an asset, for instance, a software provider's infrastructure and commercial software, with the aim to indirectly damage a certain target (e.g., the software provider's clients). This type of attack is typically used as a first step out of a series of attacks. More concisely, it is used as a stepping stone for further exploitation, once foothold is gained to the target system or systems. Attackers do not need to compromise their intended target directly but, in many cases, can achieve their aim by compromising the supply chain where it is least secure. This potential threat highlights the importance of managing the supply chain holistically and driving out or mitigating insecure elements.
Assets: "Infrastructure Network".

Threat T2.4.3: Software bug

A security bug is a software bug that can be exploited to gain unauthorized access or privileges on a computer system. Software bugs could have an impact on ICT systems, such as routers, servers, databases, and in this way impact networks or services. This type of threat also includes complex failures like network failures when several systems fail to connect or otherwise work together.
Assets: "Access Network", "Core Network", "Infrastructure Network/Area Network".

System-Centric Security

The notion of system in ICT is notably so generic to be suitable to denote almost everything that is based on software components. The system is widely used as a synonym of Operating System (OS), or in general, software that enables applications to take advantage of the computation connectivity and storage capabilities of the hardware. Due to their centrality, their role in some crucial security features (e.g., authentication), and their complexity, OSs were a preferred target of many disruptive attacks in the past (e.g., Code Red exploiting IIS buffer overflow, Sasser attacking the Local Security Authority Subsystem Service, Snakso Linux server rootkit). Nonetheless, they will have a fundamental role even in the future due to the fact that OSs are increasingly immersed in a more complex environment (e.g., mobile devices, virtualized systems), where their vulnerabilities can be either exacerbated or mitigated and they can become a commodity for applications (e.g., containerization of applications). Linux OS, for instance, is deeply involved in complex environments such as IoT.

Threats

In this section, we discuss the threats that can be mapped to the modern system asset taxonomy. CSA in its "Top Threats to Cloud Computing: The Egregious 11" of 2019, surveyed industry experts on security issues in the cloud industry in order to rate 11 salient threats, risks, and vulnerabilities. The most prominent outcome is that compared to the previous CSA report, traditional cloud security issues under the responsibility of cloud service providers (CSPs), such as the denial of service, shared technology vulnerabilities and CSP data loss and system vulnerabilities are no more ranked as important for the Cloud user perspective. This suggests a maturation of the cloud user understanding of the cloud, on one side, but should not lower the attention on such threats from the CSP perspective. It is interesting to note that the top threats reported are more in the area of potential control plane weaknesses and limited cloud visibility. Misconfiguration and inadequate change control, for instance, are ranked at position number two. Misconfiguration is the leading cause of data breaches in the cloud. Also, the absence of automatic proactive change control is perceived as another risky weakness.

Threat Group TG3.1: Unintentional damage/loss of information or IT assets

Threat T3.1.1: Information leakage/sharing due to human errors

Human errors are among the most critical threats in today ICT environment. These threats are accidental, meaning that they are not intentionally posed by humans, and are due to misconfiguration, clerical errors (for example pressing the wrong button), misapplication of valid rules (poor patch management, weak passwords), and knowledge-based mistakes (software upgrades and crashes).

According to IBM X-Force Threat Intelligence Index of 2018,[37] misconfigured cloud servers, networked backup incidents and other improperly configured systems were responsible for the exposure of more than 2 billion records, or nearly 70% of the total number of compromised records tracked by X-Force in 2017. In the 2019 report, IBM reported that publicly disclosed misconfiguration incidents increased 20% year-over-year. Human errors at virtualization level can be even more dangerous and complex to be identified (e.g., wrong VM images management/cloning).

Examples of attack at virtualization level are available in Threat T3.1.2. They are related to wrong internal processes, but similarly they can be obtained due to human errors in configuring them or as human mistakes.

Assets: "Data", "Infrastructure".

Threat T3.1.2: Inadequate design and planning or incorrect adaptation

Inadequate design and deployment, including its adaptation, of a modern cloud-based system can result in threats to managed data. As an example, migration to the cloud requires a careful design and planning to preserve security during and immediately after the migration. This means the implementation of appropriate security architecture to withstand cyber attacks. Unfortunately, this process is still not well perceived by the company leading to a series of security incidents. The main reason is that organizations implement a "lift-and-shift" cloud migration, simply porting their existing IT stack and security controls to a cloud environment. Similarly, weak control plane while designing a full cloud solution may cause severe issues. In virtualized environments, several processes can be affected by intrinsic vulnerabilities due to their peculiarities. For instance, migrations are needed for balancing the workload, but open security issues while migration is in progress. Other virtualization-specific processes that can be affected are VM rollback and VM cloning.

This threat refers to business process design and shows some similarity to business process failure threat T3.3.2 and business process poisoning threat T3.3.2, but it is due to unintentionally wrong design. If the process refers to moving, cloning, or copying VM files, then it can be linked to unauthorised acquisition of information threat T3.2.2 as well. Due to this connection, some of the following attacks can be considered as examples also for other threats.

Assets: "Middleware", "Management", "Infrastructure".

Threat Group TG3.2: Interception and unauthorised acquisition

[37] IBM X-Force Threat Intelligence Index https://www.ibm.com/security/data-breach/threat-intelligence

Threat T3.2.1: Interception of information

It considers an attacker intercepting a communication between two communicating links. Inter-node communication with cloud components is often unsecured by the default configuration, it is possible to hijack a user session or gain unauthorized access to services in social networks, and communication protocol flaws can result in data breach.
Cloud Stacks software distributions (for example Open Stack) do not always use protocols for data confidentiality and integrity between communicating applications (e.g., TLS and SSL) and are not always configured properly (e.g., changing default passwords). In addition, this effect is further exacerbated in complex layered environment based on virtualization environments because they permit cross-inspection of various tenant's data flow, as well as topology inference that could serve to set up several attacks. Meltdown and Spectre, for instance, are two CPU-level vulnerabilities that can be exploited to create a side channel focused on deducing the content of computer memory. These vulnerabilities can be exploited even in virtualized environments, leading to an even more serious security risk, given the sharing of physical resources among multiple tenants.
VM network traffic sniffing/spoofing are among the most critical threats in virtualization. Privilege domain processes like management interface can intercept all network traffic before it gets to the unprivileged user domain. The network traffic of a particular VM can be sniffed to read the communication or to perform traditional MITM attacks. Even if extremely difficult (i.e., the target and the attacker must be executed on the same core), virtualization permits a more low-level interception of information at cache level (both L2 and L1) due to the sharing of the same hardware resources. For instance, a side-channel attack on L2 cache.
Assets: "Network", "Compute Nodes", "Management Server/Console", "Access Control/Authorisation".

Threat T3.2.2: Unauthorised acquisition of information (data breach)

Unauthorised acquisition of data following data breaches is an important threat,[38]. However, in cloud/virtualized environment data breaches have some peculiarities that is worth to be discussed in this threat. In virtual/cloud environments, where physical resources are shared between tenants, there may be a set of behaviors that result in the unauthorized acquisition of information. For instance, exposure via scavenging in virtualized environments is even more serious[22] than in physical systems. In general, the physical sharing of virtualization or the logical sharing of the cloud enhance the severity of accessing to unauthorized data.
Assets: "Data".

Threat Group TG3.3: Poisoning

Threat T3.3.1: Configuration poisoning

Configuration poisoning is a serious threat in complex environments such as cloud and virtualized data centers.[39] It is sometimes called deliberate/intentional misconfiguration. It is very difficult to detect and shares similar impact as unintentional misconfiguration. In most of the cases, it implies a malicious insider. F5 Labs researchers study the breaches due to intentional insecurity and the growth rate from 2017 to 2018 was an alarming 200%. [39] For instance, one poisoning activity can be related to modification of firewalling service (i.e., web Application Firewall) configuration, to avoid deep packet inspection on certain port. Several configuration poisoning activities targeted the audit mechanisms or cloud console monitoring system to hide the attacker activities (e.g., the log system poisoning).[40]
Configuration poisoning shares technical similarities with misconfigurations due to human errors, but it differs from it for the fact that poisoning is intentional, and it brings in most of the cases to an invalid configuration that provides an advantage for the attacker.
On the other hand, misconfiguration (mistake) is not intentional, but still difficult to be discovered yet less difficult than the intentional ones. Configuration poisoning can be either the effect of an external attack or of a malicious insider attack. For this reason, it has a strong link with other threats of TG3.4. Poison objective can be focused to produce a configuration that exposes the server to attacks. However, since intentional, the type of configuration modification is much more complex to be detected that misconfiguration, mainly due to the fact that the attacker wants to hide herself as well as to hide the fact that something is not well configured.
Assets: "Middleware", "Management", "Infrastructure", "Security Mechanisms".

Threat T3.3.2: Business process poisoning

It refers to what is also called business process compromise (BPC), an attack that silently alters parts of specific business processes, or machines facilitating these processes, to generate significant monetary profit for the attackers. Accord-

[38] Europol, Internet Organised Crime Threat Assessment (IOCTA), Strategic, policy and tactical updates on the fight against cybercrime https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf

[39] Intentionally Insecure: Poor Security Practices in the Cloud https://www.f5.com/labs/articles/cisotociso/intentionally-insecure-poor-security-practices-in-the-cloud

[40] Hybrid Cloud Security Best Practices Focus On The Five C's: Console, Configuration, Connectivity, Cloud Data, And Containers https://cyberdefense.orange.com/wp-content/uploads/sites/9/2019/09/forrester$_{r}$eport$_{h}$ybrid$_{c}$loud$_{s}$ecurity.pdf

ing to Trend Micro, 43% of surveyed organizations have been impacted by a BPC.[41] In most of the cases, the business process is implemented at application level, but it can also be associated with internal cloud or virtualization business process related to automatic or programmable activities. In case of VM relocation, for instance, to handle load balancing, the target location server can be altered to a weaker configuration where memory copy protection can be disabled.

This threat is connected with inadequate design and planning or incorrect adaptation threat T3.1.2, but with the difference that this is an intentional alteration of working business process. It is therefore also connected with malicious insider threat T3.6.2 that can more easily alter business process from inside. In addition, in many cases, it is obtained via poisoning of configurations of the business process T3.3.1. In cloud and virtualization, most of these alterations are malicious alterations of business process configurations.

Assets: “Middleware”, “Management”, “Infrastructure”, “Security Mechanisms”.

Threat Group TG3.4: Nefarious activity/abuse

Threat 3.4.1: Identity fraud

In modern systems, identity handling may be more difficult due to the more complex and stratified hierarchical administration of privileges of the different layers down to the virtual one. As an example, at the virtual network level, when aggregating virtual networks into a federation, issues of role segregation and policy conflicts may arise, providing room for identity fraud. Moreover, the dynamics of adding and removing entities may be used by malicious entities to gain a new identity, for example, through inconsistencies in the migration process. Replay attacks are also facilitated by shared communication channels, which can be exploited at the virtual router level by replying to old control messages[23]. Concerning repudiation, the disposable nature of VMs, providing log features and the rollback procedures typical of virtualized environments, may have a strong impact on the non-repudiation of actions registered via logging[24]. Cloud adoption introduces multiple changes to traditional internal system management practices related to identity and access management (IAM). IAM must be able to scale and support immediate de-provisioning of access to resources.It must be automated and integrated in the cloud environment. In addition, IAM becoming increasingly interconnected for instance due to federation. In such environment, password theft is even more severe (e.g., network lateral movement attack such as “pass the hash”). In case of legacy system password strength, rotation must be verified since they are still among the mostly common cases of leakages. Similarly, in case of management of cryptographic keys, the handling of keys lifecycle, creation distribution and deletion, as a fundamental role to reduce breaches. In the cloud also hijacking of cloud service and subscriptions accounts is riskier due to the peculiarity of the Cloud model itself, where data and application reside in the cloud services.

Assets: “Middleware”, “Management”, “Security Mechanisms”.

Threat T3.4.2: Denial of service

Traditional DDoS is among the main threats to complex systems. They aim to threaten components availability at any of the layer by exhausting their resources, causing performance decrease, loss of data, service outages, on one side, and data availability, on the other side.

In layered environments based on virtualization, this disruption is exacerbated due to the sharing of resources. For instance, physical resource overloading may cause degradation of a virtual network’s performance, leading to disruption in communications, especially when the resources are in the same area as the underlying network. We note that this may happen: i) unintentionally during the system’s lifecycle (difficult to predict) or ii) maliciously in case of coordinated attacks.

Virtualized environments seek to cope with this severe class of threats by adopting isolation solutions and by promoting fair distribution of resources among all virtualized entities (network entities included). However, these approaches are difficult to implement due to the intrinsic characteristics of virtualized systems that share computing resources and distribute them (possibly on demand) at runtime.

Assets: “Middleware”, “Infrastructure”, “Security Mechanisms”.

Threat T3.4.3: Malicious code/software/activity

This class of threats usually targets all ICT stack and the six domains addressed in this deliverable. They aim to distribute and execute malicious code/software or execute malicious activities. These threats usually involve malware, exploit kits, worms and Trojans. They exploit backdoors and trapdoors, as well as developers’ errors/weaknesses. Malicious attackers can host malware on cloud services. Cloud services that host malware can seem more legitimate because the malware uses the CSP’s domain and can use cloud-sharing tools to further propagate itself. Hyper-jacking is a special type of malicious activity that affects hypervisors in virtualized environment. The target is to violate the integrity of the hypervisor to get control over it. Other malicious activities are the VM hopping that allows to jump from a VM to another on the same physical server and VM escape that takes advantages from isolation failures between hypervisor and the VM to gain control of the hypervisor and VMs. Malware-infected VM/container images can be deployed in the

[41] Half of management teams lack awareness about BPC despite increased attacks https://www.helpnetsecurity.com/2018/12/07/business-process-compromise/

relative repositories of images to be used by an attacker when launched on a trusted infrastructure leading to serious security issues.
Assets: "Middleware", "Security Mechanisms", "Virtual File Format".

Threat T3.4.4: Generation and use of rogue certificates

This class of threats usually target all ICT stack and the 6 domains in this deliverable. Certificates are largely used in cloud to make the service working in a trustful ecosystem.
Assets: "Middleware", "Management", "Infrastructure", "Security Mechanisms".
Attacks: This threat is usually at the basis of other more complex attacks as discussed in the previous threats. As an example, BIG-IP and BIG-IQ do not properly regenerate certificates and keys when deploying VM image on AWS, Azure or Verizon cloud service, which makes multiple instances to share the same certificates and keys. It causes the disruption of services eventually leading to information leak (CVE-2016-2084).

Threat T3.4.5: Misuse of assurance tools

Assurance is the way to gain justifiable confidence that IT systems will consistently demonstrate one or more security properties, and operationally behave as expected, despite failures and attacks[25]. Assurance is based on audit, certification, and compliance tools and techniques. The manipulation of such tools and techniques can result in scenarios where the malicious behaviour of attackers is masqueraded and is not discovered. Assurance information is necessary to ensure the security of the system during its entire lifecycle from its design to its operation. It is also necessary to guarantee compliance and regulation. This is valid through all the domains but especially for cloud and virtualization is quite crucial due to the intrinsic lack of transparency [26][27].
Assets: "Data", "Middleware", "Management", "Infrastructure", "Security Mechanisms".

Threat T3.4.6: Failures of business process

According to ENISA taxonomy, improper business processes can damage or cause loss of assets. In the cloud environment, one of the main causes of this type of threat is the limited cloud usage visibility. There can be two behaviours, un-sanctioned app usage and sanctioned app misuse, which refer to internal company regulations and processes that are not satisfied completely. In case of un-sanctioned app use, employees can use cloud application without any specific permission, any support for the corporate leading to what is called shadow IT.[42] This behaviour is risky when implies insecure cloud services that do not meet the corporate guidelines. IBM recently found that one out of three employees at Fortune 1000 companies regularly use cloud-based SaaS apps that have not been explicitly approved by their internal IT departments.[43]
An example of shadow IT that causes much more issues than what it was supposed to solve, was the adoption of chat room service for managing a post attack scenario on a big company. The chat room allows an attacker to learn sensible information about the company due to an unknown vulnerability that was used without alerting the security department.[44]
For the sanctioned app misuse, it is very complex to be detected but still very dangerous and can be connected to external threat actors that impersonalise legitimate internal user. An example of app misuse that is a violation of the company policy is to do a backup on a personal SaaS service.
This threat relates to the lack of security governance/awareness and with the need of having users' behavioural analysis for compliance with company policies.
Assets: "Virtual machine", "Platforms", "Infrastructure".

Threat T3.4.7: Code execution and injection (unsecure APIs)

At virtualization level, it is possible to execute code on hypervisor from a malicious VM via memory modification (heap memory) of hypervisor or to compromise the management interface via its web application exploiting CSS and SQL injection. Cloud applications are built on web services models; APIs can then become a target of attack, and be vulnerable to well-known attacks, such as the Open Web Application Security Project (OWASP) Top Ten list[25]. In particular, code execution (e.g., XSS) and injection (e.g., SQL injection) are critical classes of attacks that can increase risks. Cloud computing strongly relies on software user interfaces (UIs) and APIs to allow customers to manage and interact with cloud services. The security and availability of general cloud services are dependent on the security of these APIs. They are exposed at the perimeter and therefore very likely to be attacked. An increasing emphasis was dedicated to how to handle API keys as they are largely used in cloud services.[45]
More specifically for the cloud, CSA identified a meta-structure (i.e., the protocols and mechanisms that provide the interface between the infrastructure layer and the other layers) and an appli-structure (i.e., the applications deployed in the cloud and the underlying application services used to build them) failures as related to the APIs that ignore their existence, for instance, when APIs still use just username and password ignoring the other more advanced offered

[42] Gartner predicts that by 2020, one-third of all successful security attacks will come through shadow IT systems.
[43] Bring shadow IT into the light: Discover, assess, approve and educate https://www.ibm.com/information-technology/bring-shadow-it-light-discover-assess-approve-and-educate-0
[44] Shadow IT: Every Company's 3 Hidden Security Risks https://www.darkreading.com/endpoint/shadow-it-every-companys-3-hidden-security-risks/a/d-id/1332454
[45] Insecure API Implementations Threaten Cloud https://www.darkreading.com/cloud/insecure-api-implementations-threaten-cloud/d/d-id/1137550

security features. Similarly, to mitigate appli-structure failures, in 2019, Apple restricted iOS app providers to do screen recording as a means of analytics. Glassbox is one of the most famous application that was blocked due to this Apple policy.
Assets: “Middleware”, “Virtual machine”, and “Platforms”.

Threat Group TG3.5: Legal

Threat T3.5.1: Violation of laws or regulations data

Occurrence of a breach of EU and national laws. Depending on the exact form of EU law, certain regulations (e.g. GDPR) are directly applicable across EU Member States, while those in the form of Directive (e.g. NIS Directive) become applicable as soon as they are transposed in the national legal orders of the Member States. Note that in the occurrence of a breach of law affected individuals and organizations may seek for remedies both in the national courts, as well as before the European Court of Justice.
Assets: All assets.

Threat Group TG3.6: Organisational threats

Threat T3.6.1: Skill shortage

A possible shortage of skilled system administrators and managers is one of the main threats to complex systems. Lack of skill for virtualized environments, as well as the lack of technical competences on a specific cloud ecosystem, may have a tremendous impact on the entire cloud system. These sectors even if are somehow related to sysadmin area requires specific competences to be acquired to maintain security under control. This threat has a strong link to threat group TG3.1 “Unintentional damage / loss of information or IT assets”.
Assets: “Roles”.

Threat T3.6.2: Malicious insider

Insider threats can be distinguished in unintentional or malicious insiders. Unlike external threat actors, insiders do not have to penetrate firewalls, VPNs and other security defences at the perimeter. Insiders operate within a company’s security circle of trust, where they have direct access to resources. This makes this type of threat very complex to counteract. The Netwrix 2018 Cloud Security Report indicates that 58% of companies attribute security breaches to insiders, including negligence.[46] Being in this privileged position, the insider can be the vector of many other threats, like the ones relative to poisoning TG3.3, but also to nefarious activities TG3.4.
Assets: “Data”, “Middleware”, “Management”, “Infrastructure”, “Security Mechanisms”.

[46] Cloud Security Risks and Concerns in 2018 https://blog.netwrix.com/2018/01/23/cloud-security-risks-and-concerns-in-2018/

Data-Centric Security

The ability of sharing, managing, distributing, and accessing data quickly and remotely are at the basis of the digital revolution that started several decades ago. The role of data in today's technology is even more important, having entered the so-called, data-driven economy. Data management and inference based on them are fundamental for any enterprise, from micro to large, to make value and compete in the global market, and replaced the central role that was usually owned by communication means. The data domain observed important changes at all layers of an IT chain: i) data layer: from data to big data, ii) database layer: from SQL to NoSQL, iii) platform layer: from the data warehouse and DBMS to Big Data platforms, iv) analytics layer: from data mining to machine learning and artificial intelligence. For instance, data mining focuses on discovering unknown patterns and relationships in large data sets. Machine learning aims to discover patterns in data, by learning patterns parameters directly from data; it is composed of a training step and the algorithm is not programmed to manage such patterns. It builds and keeps the model of system behavior. Artificial intelligence mimics human intelligence and tries to reason on data to produce new knowledge.

Threats

We discuss the threats that can be mapped to the (Big) Data asset taxonomy. In general, threats, such as network outage or malfunctions of the supporting infrastructure, may heavily affect Big Data. In fact, since Big Data has millions of data items and each item may be stored in a separate physical location, this architecture leads to a heavier reliance on the interconnections between servers. Also, physical attacks (deliberate and intentional), natural and environmental disasters, and failures/malfunction (e.g. malfunction of the ICT supporting infrastructure), since their effects are strongly mitigated by the intrinsic redundancy of Big Data, though Big Data owners deploying their systems in private clouds or other on-premise infrastructure should take these attacks under serious consideration.
Data are compromised at huge rates, more than 25 million records compromised in the first semester of 2018,[17] with an increased cost of 6.4% in 2018. Social media counts the top amount of breached records, while healthcare leads the number of incidents. The average cost of a data breach raised to $3.9 million, while the average number of breached records by country was 25,575, with a cost per lost records of 150$ and time to identify and contain a breach 279 days.[47]

According to ENISA Big Data Threat Landscape,[48] a threat to a Big Data asset can be considered as "any circumstance or event that affects, often simultaneously, big volumes of data and/or data in various sources and of various types and/or data of great value". It can be further divided in Big Data breach when "a digital information asset is stolen by attackers by breaking into the ICT systems or networks where it is held/transported" and Big Data Leak "the (total or partial) accidental disclosure of a Big Data asset at a certain stage of its lifecycle due to inadequate design, improper software adaptation or when a business process fails". A Big Data Breach involves a malicious attacker behavior resulting in an unauthorized access, while a Big Data Leak involves an honest-but-curious attacker or an observer.

Threat Group TG4.1: Unintentional damage / loss of information or IT assets

Threat T4.1.1: Information leakage/sharing due to human errors

Human errors are among the most critical threats in today complex environments.[17][47][49] These errors cause accidental threats, meaning that they are not intentionally posed by humans, and are due to misconfiguration, clerical errors (for example pressing the wrong button), misapplication of valid rules (poor patch management, weak passwords), and knowledge-based mistakes (software upgrades and crashes).
Assets: "Data", "Infrastructure".

Threat T4.1.2: Inadequate design and planning or incorrect adaptation

Inadequate design and deployment, including its adaptation, of a Big Data platform can result in threats to managed data. For example, data replications, though is often seen as countermeasure to threat T4.4.2, could also represent an attack driver, in case (one of) these replicas (storage nodes) are weak or simply increase the probability of data disclosure and data leaks. As another example, the use of an encrypted storage communicating in a network exchanging data in clear could result in a data leak scenario. The design and deployment of the Big Data platform can then represent a source of threats if not deeply tested and verified. One additional threat related to the design is the lack of scalability of some tools. This threat is also connected to Threat T4.4.2 (Denial of Service)
Assets: "Data", "Big Data analytics", "Software", "Computing Infrastructure models“, "Storage Infrastructure models".

[47] Ponemon Institute's Cost of a Data Breach Report 2019
[48] Big Data Threat Landscape, ENISA, January 2016, https://www.enisa.europa.eu/publications/bigdata-threat-landscape/at$_d$*ownload/fullReport*
[49] Information Leakage, http://projects.webappsec.org/w/page/13246936/Information%20Leakage, 2018.

Threat Group TG4.2: Interception and unauthorised acquisition

Threat T4.2.1: Interception of information

It considers an attacker intercepting a communication between two communicating parties. It is possible to hijack a user session or gain unauthorized access to services in social networks, and communication protocol flaws can result in data breaches. Big Data software distributions (for example Hadoop, Cassandra, MongoDB, Couchbase) do not always use protocols for data confidentiality and integrity between communicating applications (e.g., TLS and SSL) and are not always configured properly (e.g., changing default passwords).
Assets: "Data", "Roles", "Infrastructure".

Threat T4.2.2: Unauthorised acquisition of information (data breach)

Unauthorised acquisition of data following data breaches is also an important threat,[38] and considers incidents resulting in a compromise or loss of data. In addition, GDPR in Europe is predicted to increase the number of extortion attacks. Attackers will try to extort money with the threat of GDPR penalties deriving from data disclosure.[50]
Assets: "Data", "Roles", "Infrastructure".

Threat Group TG4.3: Poisoning

Threat T4.3.1: Data poisoning

The increasing development of systems that take decisions on the basis of collected data, as well as inferences based on them, make the trustworthiness of data critical. Data poisoning then becomes a fundamental threat to all system building their processes and activities on data. Data integrity is not the only property to protect and guarantee. Data provenance, non-repudiation, and accountability should also be provided.
Assets: "Data", "Security and privacy techniques", "Data management", "Data privacy".

Threat T4.3.2: Model poisoning

It aims to poison the machine learning models, by poisoning data (Threat T4.3.1) used for the training of the model. The idea is that if an attacker can poison the data used for training, the resulting model will represent a behavior different from the real and correct behavior of the target system.
Assets: "Data", "Data Analytics".

Threat Group TG4.4: Nefarious activity/abuse

Threat T4.4.1: Identity fraud

Identity fraud is the leading type of data breaches.[17] Access credentials are in fact among the most critical data managed by Big Data platforms. They are used to access personal accounts possibly containing highly sensitive information such as credit card numbers, payment and billing details. Personal data are often coupled with profiling data such as user preferences, habits. These data are often used for impersonation fraud, creating big opportunities for identity thieves.[51] In this context, where social networking is in everyday life, social engineering raises back its importance and becomes a basis for new attacks.
Assets: "Data", "Infrastructure".

Threat T4.4.2: Denial of service

Traditional (Distributed) Denial of Service is among the main threats for complex Big Data platforms. They aim to threaten components availability by exhausting their resources, causing performance decrease, loss of data, service outages, on one side, and data availability, on the other side.
Assets: "Infrastructure".

Threat T4.4.3: Malicious code/software/activity

[50] Trend Micro Security Predictions for 2018: Paradigm Shifts https://www.trendmicro.com/vinfo/my/security/news/threat-landscape/2018-trend-micro-security-predictions-paradigm-shifts

[51] Big data creates big opportunities for identity thieves: see http://www.c4isrnet.com/story/military-tech/it/2015/01/19/big-data-identity-theft/22004695/

This class of threats usually target all ICT stack and the 6 domains in this deliverable. They aim to distribute and execute malicious code/software or execute malicious activities that target the confidentiality, integrity, and availability of data. These threats usually involve malware, exploit kits, worms, trojans, and exploit backdoors and trapdoors, as well as developer errors/weaknesses. Malicious software also targets distributed programming frameworks, which use parallel computation, and may have untrusted components.
Assets: "Data", "Software", "Computing infrastructure models".

Threat T4.4.4: Generation and use of rogue certificates

This class of threats usually target all ICT stack and the 6 domains in this deliverable. They aim to use rouge certificates to access Big Data assets and communication links, causing data leakage, data breaches, misuse of brand, and upload/download malware or force updates (see Threat T4.4.3).
Assets: "Data", "Big Data analytics", "Software", "Hardware".

Threat T4.4.5: Misuse of assurance tools

Assurance is the way to gain justifiable confidence that IT systems will consistently demonstrate one or more security properties, and operationally behave as expected, despite failures and attacks[27][16]. Assurance is based on audit, certification, and compliance tools and techniques[25]. The manipulation of such tools and techniques can result in scenarios where the malicious behavior of attackers is masqueraded and is not discovered. Assurance information is necessary to ensure the security of the system during its entire lifecycle from its design to its operation. It is also necessary to guarantee compliance to regulations.
Assets: "Security and privacy techniques", "Data", "Infrastructure".

Threat T4.4.6: Failures of business process

According to ENISA taxonomy,[52] improper business processes can damage or cause loss of assets. This class includes threats to confidentiality (e.g., wrong anonymization) and integrity of data (e.g., wrong management of replicas that can bring to scenarios of Big Data degradation, increasing the risk of inconsistent data).
Assets: "Data", "Big Data analytics".

Threat T4.4.7: Code execution and injection (unsecure APIs)

Big Data applications are built on web services models; APIs can then become a target of attack, and be vulnerable to well-known attacks, such as the Open Web Application Security Project (OWASP) Top Ten list[24]. In particular, code execution (e.g., XSS) and injection (e.g., SQL injection) are critical classes of attacks that can increase risks. Web Applications attacks and breaches often result in larger data breaches.[53]
Assets: "Data", "Storage Infrastructure models".

Threat Group TG4.5: Legal

Threat T4.5.1: Violation of laws or regulations

The poor management of legal aspects pertinent to Big Data system can be considered as a threat to the system itself. In this respect, the GDPR and the Free Flow of Non-Personal Data Regulation, for instance, dictate -among others- how organizations are expected to handle personal data, who is ultimately responsible for the protection of personal data in the context of complex supply chains, what are the associated obligations concerning mixed data sets of both personal and non-personal data and how to mitigate risks (e.g. for profiling).
Assets: All assets.

Threat Group TG4.6: Organisational threats

Threat T4.6.1: Skill shortage

A possible shortage of skilled data scientists and managers is one of the main threats to Big Data.[54] This threat has a strong link to threat group TG4.1 "Unintentional damage/loss of information or IT assets".

[52] Confidentiality, Integrity, Availability (CIA)
[53] 2019 Global Threat Intelligence Report https://www.nttsecurity.com/gtir
[54] See for example reports from McKinsey http://www.mckinsey.com/features/big$_d$ata and from the Financial Times http://www.ft.com/cms/s/0/953ff95a-6045-11e4-88d1-00144feabdc0.htmlaxzz3ntU3lM00

Assets: “Roles”.

Threat T4.6.2: Malicious insider

Insider threats are among the most critical security threats, and can involve unintentional or malicious insiders[55]. The view that insider attacks may inflict larger damages than outside attackers is widely shared [28][55][56][57]. Their impact is also increasing due to the fact that, on one side, no effective security solutions exist for this threat and, on the other side, the value of data is increasing exponentially. Insiders are in fact authorized users with legitimate access to sensitive/confidential documents, possibly knowing existing vulnerabilities[55]. Malicious insiders have therefore multiple incentives to carry out an attack that ranges from revenge to revenue when sensitive data are at their disposal.
Assets: “Roles”, “Data”, “Infrastructure Security”, “Integrity and Reactive Security”

Application-Centric Security

This section describes an overview of assets in Domain 5 on application-centric security. It includes an overview of assets and threats that span the full spectrum of applications. Major sources of information for this study are OWASP[58] and SANS[59] reports. It is important to note that this section does not consider applications providing functionalities for infrastructure/system/network management.

Threats

In this section, we discuss the threats that can be mapped to the application asset taxonomy. Our review was driven by the OWASP and SANS generic risk assessment. In general terms, threats, such as injection and application malfunctioning, may strongly affect IT in general. In fact, current IT systems are heavily based on applications/services composed at run time and therefore exposed to attacks and breaches. Also, attacks to hosting platforms (deliberate and intentional), failures/malfunctions (e.g. malfunction of the ICT supporting platform) can be important sources of risk. We introduce the major characteristics of the threat taxonomy, with a special focus on cyber-security threats; that is, threats applying to information and communication technology assets. We also consider threats not related to ICT and caused by humans during their activities.
A threat to application assets can be considered as “any circumstance or event that affects, often simultaneously, services and applications distributed over the Web”.

Threat Group TG5.1: Unintentional damage

Threat T5.1.1: Security Misconfiguration

Security misconfiguration is one of the most exploited threats. Cyber attackers often try to exploit unpatched software, use default accounts, or unused pages to gain unauthorized access to systems. The problem can target systems at any layers and give the attacker the possibility of compromising the system and bypassing access control checks. This threat is related to threats in other domains: Threat T4.1.1 and Threat T4.1.2 in Data-Centric Security Threat T3.1.1 in System-centric Security, Threat T1.1.1 in Device/IoT-Centric Security.
Assets: “Interfaces”, “Security Techniques”.

Threat Group TG5.2: Interception and unauthorised acquisition

Threat T5.2.1: Interception of information

Interception of information is another important threat that plague the application domain. This threat is horizontal and target all domains involving weaknesses in network communications, system components and devices, data exchange, and users’ activities. In this domain, interception of information is mainly due to weaknesses and flaws in the protocols for communication encryption (e.g., SSL). This threat is related to threats in other domains: Threat T4.1.1, Threat T4.2.1, and Threat T4.2.2 in Data-Centric Security, threat T3.2.1 in System-Centric Security , Threat T1.2.1 in Device/IoT-Centric Security.

[55] IPACSO Project, Innovation Framework for ICT Security,Available: https://ipacso.eu/
[56] R. F. Trzeciak. 2017. SEI Cyber Minute: Insider Threats, http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=496626
[57] PWC. 2017. Global Economic Crime Survey 2016: US Results. https://www.pwc.com/us/en/forensic-services/economic-crime-survey-us-supplement.html.
[58] OWASP™ Foundation - the free and open software security community, https://www.owasp.org/index.php/Main$_{page}$
[59] SANS Institute, https://www.sans.org/

Assets: “Data”, “Interfaces”, “Security Techniques”.

Threat T5.2.2: Sensitive data exposure

Sensitive data exposure is a major plague for applications and is often the results of misconfigurations or weak security protection. Many web applications and APIs do not properly protect sensitive data.[12] Rather than trying to decrypt an encrypted communication, cyber attackers try to intercept it, steal keys, access clear text.[12] The most common weaknesses concern, not surprisingly, the store/exchange of sensitive data in plain text, as well as how crypto is employed (e.g., weak key generation and management, weak algorithm). This threat results in common sensitive data leakage and breach both for data in transit and at rest. This threat is related to threats in other domains: Threats T4.1.1, T4.2.1, T4.2.2, T4.4.4 in Data-Centric Security, as well as T5.1.1 and T5.1.2 in this section.
Assets: “Data”, “Security Techniques”, “Roles”.

Threat Group TG5.3: Nefarious activity/abuse

Threat T5.3.1: Broken authentication and access control

Broken authentication and access control allow an attacker to compromise an application and often the entire system hosting it. As a consequence, a bug in the application functions implementing authentication and session management, as well as access control, result in catastrophic consequences, allowing attackers to compromise passwords, keys, or session tokens, assume other users’ identities.[12] Restrictions on authorizations are also not properly enforced. Access control weaknesses are similar and permit unauthorized operations affecting confidentiality and integrity of data and applications.
Assets: “Data”, “Security Techniques”, “Roles”.

Threat T5.3.2: Denial of service

Denial of service has been extensively discussed in both device/IoT-, network-, system-, and data-centric security. One of the main targets of denial of service is applications for a variety of reasons, economic, political, ideological, and the like. This threat is related to threats in other domains.
Assets: “Data”, “Interfaces”, “Security Techniques”, “Roles”.

Threat T5.3.3: Code execution and injection (unsecure APIs)

Code execution and injection are common threats to applications. Unsecure APIs are supporting criminals in their malicious activities since the advent of the Internet and are increasing in importance since the advent of distributed services. This threat is related to threats in other domains: Threat T4.4.2 in Data-Centric Security, Threat T3.4.3 in System-Centric Security, and Threat T1.4.3 in Device/IoT-Centric Security.
Assets: “Data”, “Interfaces”, “Security Techniques”.

Threat T5.3.4: Insufficient logging and monitoring

This threat supports criminals in going undetected. It reduces the performance of intrusion detection and attack identification, decreasing the response and remediation effectiveness.[12]
Assets: “Data”, “Interfaces”, “Security Techniques”.

Threat T5.3.5: Untrusted composition

This threat subsumes many other threats in this deliverable focusing specifically on composite services. Composite services in fact orchestrate atomic services to provide advanced functionalities. This composition, however, introduces new risks that go beyond the risks of atomic service[16][29]. First of all, composite services could result in a compromise due to combined information they have access to. Then, the composition of strong atomic services does not result in a strong composite service. Afterwards, the strength of a composite service is the strength of the weakest atomic service. Finally, multiple communications and storages need to be protected at time.
Assets: “Interfaces”.

Threat Group TG5.4: Legal

Threat T5.4.1: Violation of laws or regulations

Taking, also, into account the discussion above on violation of applicable laws, it can be argued the most relevant laws, in this case, are the GDPR and the Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS). National laws of Member States can certainly apply, but those are, essentially, left

outside the scope of this deliverable.
Assets: All assets.

Threat Group TG5.5: Organisational threats

Threat T5.5.1: Malicious insider

The insider threats are among the most critical security threats to be faced, and can be distinguished in unintentional or malicious insiders[55] It is quite shared the view that insider attacks may inflict larger damages than outside attackers[28].[55][56][57] Their impact is also increasing due to the fact that, on one side, no effective security solutions exist for this threat and, on the other side, the value of data is increasing exponentially. Insiders are in fact authorized users with legitimate access to sensitive/confidential documents, possibly knowing existing vulnerabilities[55]. Malicious insiders have therefore multiple incentives to carry out an attack that ranges from revenge to revenue when sensitive data are at their disposal.
Assets: "Roles", "Data", "Platform Security", "Application Security".

User-Centric Security

This section describes an overview of assets in Domain 6 on User-centric security. Here the term users refers to human users of information technologies in a professional context. We do not include software systems mimicking human users (e.g., bots, autonomous agents) and also, in the classification of security threats and attack samples, we exclude home users engaging in recreational personal usage of information technologies. Rather, we specifically categorize assets according to a typical industrial scenario and, equally, threats as perceived from a company's perspective. In general, users may have the double role of perpetrator of a threat (e.g., a threat is carried out by human actions) or victims (e.g., individuals are the asset targeted by a threat). Therefore, what should be reasonably included in the user-centric security domain? Individuals as perpetrators or as victims? There is not a clear-cut answer, especially considering that users as perpetrators of security violations are necessarily considered in other domains too, and several semi-automated attack vectors, such as botnets, are operated by humans. Furthermore, humans are responsible for all kinds of cybercrimes, in the end, even social bots used in frauds have been designed by humans and provide illicit benefits to some humans. The same for humans as victims. For most security incidents, the consequences are likely to impact humans. Systems experiencing downtime, malicious applications, compromised IoT networks likely have a negative impact on human activities. Therefore, some more stringent criteria should be adopted.

Threats

In this section, we discuss the threats that can be mapped to the User asset taxonomy previously presented. Before introducing the major characteristics of the threat taxonomy, a note of caution should be presented because the User domain, of all the cybersecurity domains, is the more recent to be considered as a primary domain of concern and, for this reason, and also for the non-technical nature of many related aspects, its scope is still somehow debated or sometimes ambiguously defined.For example, still few years ago, the Health Information Trust Alliance stated that "cybersecurity does not address non-malicious human threat actors, such as a well-meaning but misguided employee."[60] This means that, still recently and, at least, for a relevant organization in one of the key industrial sector, human errors were largely out of the scope of cybersecurity. This would be unconceivable with respect to current cybersecurity analyses, after the User domain has been elevated at the same level of traditional cybersecurity domains such as Systems, Networks, or Data.
On the other side, it is not uncommon today to encounter articles on online cybersecurity-related magazines and in surveys making claims such as "malicious insiders and human error to be the two top cybersecurity threats".[61] These claims, together with the utterly misleading logical fallacy of considering users (or the human factor) as threats (as well as the too often repeated analogy, in technical circles, between users and the weakest link in a chain), grossly overstate and confound threats connected with the User domain, with the aim of shifting the attention of organizations and professionals to the newest hype. Click-baiting editorial styles or commercial interests are likely part of the motivations for such a poor information, but a general lack of understanding and experience with studies on human errors and user behaviour connected to IT technologies is equally an important factor.
However, these anecdotes should remind of the fact that the boundaries and the threats of the User domain are still to be regarded as, to some extent, subjective and not yet well established.
More thoroughly conceived and articulated analyses have appeared in recent years raising the attention to the human factor in cybersecurity. For example, NIST, through the Federal Information System Security Educators' Association (FISSEA), has concluded that human errors and negligence often play an important role in chain of events leading to data breaches. Also,

[60] WhiteHouse,The Cost of Malicious Cyber Activity to the U.S. Economy,2018, Available: https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

[61] Human Factor is a Persistent Cybersecurity Threat, Survey Says. Security Magazine, August 2019. https://www.securitymagazine.com/articles/90734-human-factor-is-a-persistent-cybersecurity-threat-survey-says

security risk management and business operations are often disconnected functions, resulting in a poorly coordinated process management.[62] The Verizon Data Breach Investigation Report (DBIR), a respected annual survey, for the current 2019 edition confirms that the category Miscellaneous Errors, while not among the most relevant for security incidents (i.e., security events not resulting in data breaches, such as Denial of Services), it is instead one of the lost likely pattern for data breaches. Interestingly, other categories that could be partially referred to the User domain, such as Privilege Misuse (e.g., employees using their system and data access privileges outside their job duties) and Cyber-Espionage (e.g., this threat category often adopt deceitful techniques to target specific employees or make use of unfaithful insiders), are relevant. Such results hardly represent a surprise, in fact their relevance is a fact from years.

Many have debated about the importance of the organization for cybersecurity and, to this regard, the expression Human-centered security has been used. Holz et al.[30] have presented a detailed research agenda aimed at reorganizing industrial processes of cybersecurity around the role of individuals in all their form, as software developers, IT integrators, system administrators, and end users. Many others, for instance ENISA[63], Corradini and Nardelli [31], and Safa et. al. [22] have addressed the security threats related to users focusing on the perceived need of more and better training of the workforce. The lack of adequate training programs and curricula for cybersecurity professionals as one of the main reason for the gap in available workforce is widely debated worldwide and the subject of several proposals[32][33][23].

Regarding cybercrimes, the User domain is more specifically concerned with identifying whom is responsible, which characteristics they exhibit, and their main motivations and pattern of activity. Two large profiles have emerged in recent years: criminal organizations and state-sponsored groups; the former mainly responsible of financially motivated crimes, the latter mainly driven by cyber-espionage and data breaches. Criminal groups exploit vulnerabilities in existing technologies, as well as the features offered by new technologies, engaging in the traditional arms race with law enforcement and companies' prevention and mitigation solutions. State-sponsored attacks are often framed with reference to cyberwarfare[24][34]. Despite that reference could be reasonable in certain situations and for specific contexts, however, it often confounds the analysis by focusing more specifically on geopolitical and military issues than on more operational and business-related threats[35]. State-sponsored attacks are mostly related to cyber-espionage; thus, they represent a lucrative activity for the perpetrators and, often, a severe competitive loss for the victims[36][37][38]. Therefore, they should probably be more conveniently framed with respect to international market competition and the protection of strategic investments.

Finally, we mention two classes of threats that still are not commonly included in cybersecurity threat taxonomies: threats to a company's market share and threats from amplification effects on media. Analyses of the economic and financial consequences of a security breach have been studied from long[25][26][27][39]. However, it is still an issue that has not entered the mainstream in cybersecurity and requires more and better detailed analyses. In some cases, the actual negative effects, especially long term effects, have been questioned, on the basis of the complex and non-linear cause-effect relationships governing stock prices[40][41][42]. The amplification effect of media, traditional or online, with respect to risks and threats is a well-known effect that is still largely ignored in cybersecurity threat taxonomies. On the opposite, it is important to consider, at least as one of the new threat sources to put on a watch list. Episodes where the social amplification of risks, driven by the media, have had relevant effects are discussed in the literature[2][43][44][45].

In summary, a threat to User assets can be considered as "any circumstance or event that produces adverse effects primarily on individuals as part of an organization or as stakeholders. The threat should be carried out through digital means, either voluntarily (attack/cybercrime) or involuntarily (human error)".

Threat Group TG6.1: Human errors

Threat T6.1.1: Mishandling of physical assets

Physical assets like laptops and disposable data storage are often lost or stolen. In most cases, this event has moderate effects, if any, but it happened that in few circumstances it resulted in severe consequences. This is a typical threat caused by human errors.
Assets: All assets.

Threat T6.1.2: Misconfiguration of systems

System misconfiguration is probably the most typical example of human error. All types of systems are systematically misconfigured, often resulting in small failures, sometimes representing one of the major causes of cyber risks, as witnessed by all security surveys.
Assets: All assets.

Threat T6.1.3: Loss of CIA on data assets

This threat generally refers to data breaches and data leaks, so it mostly refers to the Data domain. However, it often has an undoubtedly human component that makes it worth to be included in the User domain, too. Access privileges are often misused, credentials are managed improperly, and trust is given to someone impersonating someone else or exploiting employees' good faith.
Assets: All assets.

[62] Cybersecurity – the Human Factor: Prioritizing People Solutions to improve the cyber resiliency of the Federal workforce. FISSEA. 2017. https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017$_W$*itkowski*$_B$*enczik*$_J$*arrin*$_W$*alker*$_M$*aterials*$_F$*inal.pdf*

[63] ENISA, Cyber Security Culture in organisations. February 2018. https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

Threat T6.1.4: Legal, reputational, and financial cost

A security incident may have effects that go well beyond the technical domain and production processes. Intangible goods, such as the brand reputation, the financial solidity of the company, and the trustworthiness of the management could suffer some consequences that might be addressed outside the technical competences and mostly by the financial direction, marketing, and the highest company management levels.

Assets: All assets.

Threat Group TG6.2: Privacy breaches

Threat T6.2.1: Profiling and discriminatory practices

In recent years, the US Federal Trade Commission FTC) has actively monitored data brokers practices and its reports have shed a light on such a crucial while elusive industrial segment of the digital society with enormous implications on online privacy. The conclusion of the FTC is disheartened: “In the nearly two decades since the Commission first began to examine data brokers, little progress has been made to improve transparency and choice”. In Europe, GDPR has introduced severe limitations and fines for commercial profiling, however, it does not seem to have stopped the practice of profiling web users for advertising purposes. Other discriminatory practices have been conjectured for Internet giants like Google[64] and Facebook[65].

Assets: “External”.

Threat T6.2.2: Illegal acquisition of information

Illegal acquisition of data may happen as a consequence of hacking, of malware exfiltrating information, or of data breaches. is also an important threat, and considers incidents resulting in a compromise or loss of data. This threat represents the typical domain of privacy. Users could be both targets and actors for this threat, depending on their role. The issue has been debated and analysed extensively and has evident cross-domain aspects. Several comprehensive reports and survey are available[46][47], as well as specific professional skills and profiles.

Assets: All assets.

Threat Group TG6.3: Cybercrime

Threat T6.3.1: Organized criminal groups’ activity

As mentioned before, the threat from organized criminal groups has been clearly recognized in analyses produced in recent years as those mostly related to financial gain. The use of malware, botnet, ransomware, and hacking is often related to criminal organizations, which are moving online for their illegal activity. Dark web markets selling illegal goods, private encrypted online chat, and other online forums are new ways for organized criminal groups to extend their business.

Assets: “Internal”, “Intangible”.

Threat T6.3.2: State-sponsored organizations’ activity

Similar to the previous threat, we have already presented the threat connected to state-sponsored organizations as the one mostly related to cyber-espionage. Market competition in key sectors of the economy, such as advanced technology, energy, and innovative manufacturing techniques, has always suffered of industrial espionage. The diffusion of online services and networked systems as enormously increased the possibilities for those willing to access to proprietary data.

Assets: All assets.

Threat T6.3.3: Malicious employees or partners’ activity

Threats from insiders have been extensively debated in the last two decades, at least, with alternate emphasis. In some years, the threat from malicious employees reached the hype on specialized press, with someone even claiming that it had exceeded the dangers from outside an organization. More pragmatic studies and surveys, such as Verizon DIBIR, have instead confirmed that despite some fluctuation in the reported cases, the proportion between breaches originated from the inside and those from the outside remained close to the classical 20-80 proportion. Therefore, it never happened a sort of explosion of internal attacks. What is instead true is that inside attackers are likely to exploit better information and higher privileges, increasing the odds of severe consequences.

Assets: “Internal”.

Threat Group TG6.4: Media amplification effects

[64] David Shepardson and Bryan Pietsch, U.S. states launch antitrust probe of Google, advertising in focus. Reuters, September 2019. https://www.reuters.com/article/us-tech-antitrust-probe/u-s-states-launch-antitrust-probe-of-google-advertising-in-focus-idUSKCN1VU107

[65] Katie Paul and Akanksha Rana, U.S. charges Facebook with racial discrimination in targeted housing ads. Reuters, March 2019. https://www.reuters.com/article/us-facebook-advertisers/hud-charges-facebook-with-housing-discrimination-in-targeted-ads-on-its-platform-idUSKCN1R91E8

Threat T6.4.1: Misinformation/disinformation campaigns

This threat group is the less common in cybersecurity threat taxonomies and wants to consider the relevance that media (social and online media, in particular) have in spreading information and amplifying the effect of news in the public opinion, which does not just include laymen, but professionals, business partners, potential customers and investors, and the authorities, too.
Assets: All assets.

Threat T6.4.2: Smear campaigns/market manipulation

Similar to the previous threat, in this case we account for the possibility that a smear campaign is directed towards a company or some representative figures with the aim of manipulating the market, for instance the stock price or a market opportunity.
Assets: All assets.

Threat T6.4.3: Social responsibility/ethics-related incidents

Ethics has been under the spotlight in the last few years, mostly for questionable activities of companies of the so-called "shared economy" and the potential consequences of AI-driven decision technologies. This represents a new cybersecurity threat for organizations, which might be attacked by crafting an incident based on ethical problems. Combined with previous threats regarding online media, the ethics-related issues represent a new form of social responsibility for companies, that should be carefully considered because a negative press or public opinion campaign might have severe consequence on business.
Assets: All assets.

Threat Group TG6.5: Organizational threats

Threat T6.5.1: Skill shortage/undefined cybersecurity curricula

We have previously introduced and discussed about this threat. Skill shortage in cybersecurity is a problem regularly debated in cybersecurity conferences and professional events, because it regards the majority of organizations. New initiatives to standardize academic curricula exist, together with a trend towards professionalization of the role of cybersecurity experts [33][66]. However, it is still not clear and certainly far from a large agreement what should be the core skills of a cybersecurity expert and how to have a larger and better prepared workforce.
Assets: "Internal".

Threat T6.5.2: Business misalignment/shift of priorities

This represent the typical domain of eGovernment, where one of the main goals is to keep a constant alignment between IT and business goals and between IT processes and the corporate strategy. Similarly, a governance of corporate cybersecurity is needed and should be more mature than the present situation.
Assets: "Internal" and "External".

Main Attacks

The scope of this appendix is to present major attacks that affected each of our domains of interest. The attacks are grouped based on the main exploited threats.

Attacks related to Device/IoT-Centric Security

In the following, the main attacks affecting the Device/IoT domain are reported.

- **Threat T1.1.1: Information leakage/sharing due to human errors:** In medical sector IoT applications are very critical as also pointed out by Choi et al.[48] that showed how data breach in hospital can impact on the 30-day mortality rate. According to Jiang et al.[49] most breaches in hospitals were triggered by employee mistakes or unauthorized disclosures. Given the nature of the information, the impact on privacy is of paramount importance. In some cases, sensor channels are protected, but the aggregation nodes at the edge were not. Employee mistakes can reveal them or generate a weakness that can potentially reveal them[49]. Installation phase is also critical in IoT since in most of the cases it the only moment where human intervention can activate security features or configure secure connections with the rest of the network. It can be complex to remediate to a human error at this phase.
- **Threat T1.1.2: Inadequate design and planning or incorrect adaptation:** Many attacks partially involve this threat to trigger another one, like in the case of botnets. Examples of security attacks generated by an inadequate design are the ones that involves CloudPets' toys, that are designed without considering any Bluetooth security features, so that everyone within range can connect to them, and send and receive commands and data.[67] Given the nature of these devices, adaptation and fixing

[66] CyBok, The Cyber Security Body Of Knowledge. Version 1.0, October 2019. https://www.cybok.org/
[67] How This Internet of Things Stuffed Animal Can Be Remotely Turned Into a Spy Device https://www.vice.com/en$_u$s/article/qkm48b/how − this − internet − of − things − teddy − bear − can − be − remotely − turned − into − a − spy − device

strategy are almost not applicable. One example of wrong design of IoT device deployment is the one related to the device of refrigeration/heating-ventilation and air-conditioning of HVAC vendor that has remote access to monitor the environmental temperature. These devices were used in 2015 to generate data breach on a retail's network. More than the vulnerabilities of the devices, the problem was the decision of having such devices on the same network with POS services.[68] Similar issues are quite common in medical facilities that uses IoT devices for their specific capabilities without having network segmentation of them from other devices. The result is that any local device can end up having a global impact.[69]

- **Threat T1.2.1: Interception of information:** Recently Amazon Smart Ring IoT devices was discovered by BitDefender to be vulnerable to password interception since they handle the exchange of the WiFi password in plain text format over an http channel.[70] A security vulnerability in BMW's Connected Drive system allowed researchers to unlock the vehicles affected without the car keys. The researchers were able to impersonate BMW servers and send, over the public cellular network, remote unlocking instructions to vehicles. The problem was fixed adding HTTPS encryption to the connection and ensures that the car only accepts connections from a server with the correct security certificate. More recently VPNFilter similarly to BlackEnergy malware intercepted communication from SCADA systems used in manufacturing and the maintenance of infrastructure to sniff out credentials attacking routers.[71]
- **Threat T1.2.2: Unauthorised acquisition of information:** Some traditional networking attacks can have a role in IoT given the vulnerabilities of networking devices currently used in IoT environment. For instance, the sinkhole attack (or blackhole attack) is obtained via an attacker that declares himself to have a high-quality route/path allowing him to do manipulate all packets passing through it. Another type of attack to the network is the selective forwarding attack where the attacker can selectively forward/drop packets. The wormhole attack is obtained recording packets at one location in the network and tunnelling them to another location having the scope of influencing perceived network behaviour distort statistics and impacting the routing functionalities.
- **Threat T1.3.1: Device modification:** An attacker may be able to exploit firmware upgrade (requiring or not physical access) by maliciously replacing the device's firmware influencing its operational behavior. For example, an attacker can obtain a periodical report the energy consumption of a specific device could adding a piece of malicious code to the firmware. This information can be then used to infer if a home or an enterprise is active or not. In other cases, the fact that the firmware upgrade can be complex in IoT environment lead to the situation in which firmware has not been properly maintained and updated. This scenario opens to vulnerabilities that might be exploited by attackers to replace the firmware on the device remotely. For instance, the Foscam wireless cameras were vulnerable to firmware replacement allowing full camera control.[72] IoT is also exposed more than other systems to physical cloning attack. Butun et al.[50] described a number of scenarios where clone attack impacts IoT and the relative detection countermeasure.
- **Threat T1.3.2: Extraction of private information:** Park et al. focused on the attack on information on IoT Sensors including the ones requiring physical access[51]. In many cases physical access permits to bypass security protections and access to the device having the scope of tampering it to extract private information or to modify firmware to have a privileged shadow access. Additional examples are the side channel attacks on sensors data. Maiti et al. describe side channel attack on mobile keypads using smartwatches[52]. Sarkisyan et al. study PIN prediction using smartwatch motion sensor[53]. Chakraborty et al. describe optical eavesdropping on the display of a mobile device via light sensors[54].
- **Threat T1.4.1: Identity fraud:** In 2015 Moose infected a device using brute force attacks through Telnet and set up a SOCKS and HTTP proxy. In 2018, Guardzilla, an IoT camera, used the same hard-coded keys on devices as it did for its AWS storage server. This is an example of IoT threat that allows impersonification via access key of the cloud backend service.[73]
- **Threat T1.4.2: Denial of service:** In Finland, a DDoS attack took down the heating systems of at least two housing blocks in the city of Lappeenranta, leaving their residents without heating in sub-zero temperatures for more than a week.[74] Apparently the source of this attack was a Mirai botnet.
- **Threat T1.4.3: Malicious code/software/activity:** The Puerto Rican Electric Power Authority (PREPA) in 2009 suffered a series of power theft incidents related to its smart meter deployment. The attack was quite complex and exploited different threats. For instance, it requires physical access (TG1.3), and it probably implies malicious insiders that understand the hardware functionalities. The main exploited vulnerability was discovered later in 2010 and was injection of false data mainly at installation phase.[75] This is considered a serious security issue for IoT devices especially in correlation with malicious insider. IoT is also the preferred target for Botnet based malware. Recently a new variant of Gafgyt malware targets small office and home routers exploiting well known vulnerabilities. It is in competition with JenX botnet and in case of double infection they are programmed to disable each other.[76] Jeep Cherokees was discovered to be vulnerable to an attacker that may be miles away yet capable of sending commands through the Jeep's entertainment system to its dashboard functions, steering, brakes, and transmission.[77] IoT_Reaper, also known as "the Reaper," is variant of Mirai Linux that utilizes at least ten old and well-known vulnerabilities in IoT. Given the difficulties in updating IoT even old vulnerabilities can be very effective. Recently cryptominers start considering IoT devices, more for the fact that they are quite easy to tamper than for their computational power even if devices such as Alexa and mobile phones (android OS via ADB.Miner) have non-negligible computational capabilities. More recently, these

[68] IoT Hack Connected To Target Breach https://www.mocana.com/blog/2014/02/05/iot-hack-connected-target-breach

[69] Health care's huge cybersecurity problem https://www.theverge.com/2019/4/4/18293817/cybersecurity-hospitals-health-care-scan-simulation

[70] Ring Video Doorbell Pro Under the Scope https://labs.bitdefender.com/2019/11/ring-video-doorbell-pro-under-the-scope/

[71] VPNFilter: New Router Malware with Destructive Capabilities https://www.symantec.com/blogs/threat-intelligence/vpnfilter-iot-malware

[72] How A Creep Hacked A Baby Monitor To Say Lewd Things To A 2-Year-Old https://www.forbes.com/sites/kashmirhill/2013/08/13/how-a-creep-hacked-a-baby-monitor-to-say-lewd-things-to-a-2-year-old/

[73] Security flaws let anyone snoop on Guardzilla smart camera video recordings https://techcrunch.com/2018/12/27/guardzilla-security-camera-flaws/

[74] DDoS Attack Takes Down Central Heating System Amidst Winter In Finland https://thehackernews.com/2016/11/heating-system-hacked.html

[75] Puerto Rico smart meters believed to have been hacked – and such hacks likely to spread https://www.smart-energy.com/regional-news/north-america/puerto-rico-smart-meters-believed-to-have-been-hacked-and-such-hacks-likely-to-spread/

[76] This aggressive IoT malware is forcing Wi-Fi routers to join its botnet army https://www.zdnet.com/article/this-aggressive-iot-malware-is-forcing-wi-fi-routers-to-join-its-botnet-army/

[77] Hackers Remotely Kill a Jeep on the Highway—With Me in It https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

types of malware used blockchain-based DNS to make them more difficult to track, like Fbot.

- **Threat T1.4.4: Misuse of assurance tools:** Given the IoT peculiarities such assurance tool is in most of the cases not implemented but there is a non-negligible effort in order to have them in place in the near future. Therefore, more attacks will become available in the future.
- **Threat T1.4.5: Failures of business process:** Examples of business process failures are the ones that imply poorly-designed technical workflows like for instance save sensor data in multiple copies and in a not protected location or keep them locally even after having transferred them. Other failures refer to business-specific processes where IoT devices are manufactured with non-reliable or non-security components and the manufacturing process has no requirements on assurance which is a supply chain vulnerability. According to TrapX most of the healthcare organizations are vulnerable to medical device hijacking also called "medjacking", which in many cases imply failures on the business process connected with sensors or on the procurement process.[78]
- **Threat T1.4.6: Code execution and injection (unsecure APIs):** SQL injections are bigger danger to the IoT than traditional networks. They are in many cases at the basis of most of the Botnet since SQL injection can lead to privilege escalation quite straightforward. In many cases the target is a smartphone that controls devices like in the cases of the XSS and SQL injection of Belkin devices and WeMo app.[79] Recently Carlo Gavazzi SmartHouse version 6.5.33 was discovered to suffer from cross site request forgery along with both reflective and persistent XSS vulnerabilities.[80]
- **Threat T1.5.1: Violation of laws or regulations Threat T1.6.1: Skill shortage:** No recent attacks have been reported.

Attacks related to Network-Centric Security

The following presents the major attacks that affected each of our domains of interest. The attacks are grouped based on the main exploited threat.

- **Threat T2.1.1: Erroneous use or administration of devices and systems:** A human error caused a mobile internet outage for millions of users. Due to a human error (wrong software configuration) during the migration of the packet gateway, clients of one operator were not able to use mobile data. Mobile switches were affected by this incident. A rollback was successfully executed to resolve the issue.[81] Misconfigured, Open DNS Servers has been used in Record-Breaking DDoS Attack. The attackers abused improperly configured or default-state DNS servers, also known as open DNS resolvers.[82]
- **Threat T2.2.1: Signaling traffic interception:** An attacker by simply having a signaling network access (e.g. by simply renting a global title on the market) can sent crafted messages to retrieve location information of the network node on which a target subscriber is connected. An attacker can alter current subscriber's location and profile to receive mobile terminating or mobile originating calls, SMS, or data traffic. Hostile SS7 Update Location enables subscriber SMS interception by simulating a fake MSC which will then receive the SMS for this targeted subscriber. Interception of SMS messages could enable adversaries to obtain authentication codes used for multi-factor authentication. In [83] SS7 has been exploited to intercept two-factor authentication codes sent to online banking customers, allowing them to empty their accounts. The exploitation of SS7 design weaknesses to obtain a victim's location, harvest their messages, and listen in on calls was demonstrated in 2014.[84] Other examples are the demonstration in [85] and [86]. O2 in Germany confirmed that some customers in Germany have had their accounts drained by attackers that used SS7 to intercept and redirect mTANs to their own phones.[87] In [88], an attempted Data interception attacks using SS7 was reported.
- **Threat T2.2.2: Data session hijacking:** A data session hijacking was achieved by performing GTP attacks.[89] In 2014, attackers hijacked a portion of online traffic from a set of 19 ISPs, with the goal of stealing cryptocurrency from a group of users.[90] In April 2017, Rostelecom, a Russian SP, leaked dozens of routes pertaining to IP addresses that belong to major financial services firms. The Russian ISP 'originated' 137 prefixes, 37 of which belong to financial, e-commerce, and payment services, like Mastercard, Visa, Forti, Alfabank. For 7 minutes, global traffic to these services was redirected via the Rostelecom network.[91] In 2018, a BGP hijack was used to divert traffic to Google from subscribers living in the west of the USA, via Russia, to China, allegedly intentionally and for espionage purposes.[92]
- **Threat T2.2.3: Traffic eavesdropping:** To conduct such an attack, attackers would need to have the proper equipment to capture and store the radio communication between the cellular mobile device and the base station. False Base Station (FBS), Rogue

[78] Medjacking: The newest healthcare risk? https://www.healthcareitnews.com/news/medjacking-newest-healthcare-risk

[79] Assessing the Severity of SQL Injection Threats to IoT Security https://www.smartdatacollective.com/assessing-severity-sql-injection-threats-iot-security/

[80] Carlo Gavazzi SmartHouse 6.5.33 XSS / Cross Site Request Forgery https://packetstormsecurity.com/files/155508/ZSL-2019-5543.txt

[81] Annual Report Telecom Security Incidents 2018 https://www.enisa.europa.eu/publications/annual-report-telecom-security-incidents-2018

[82] Misconfigured, Open DNS Servers Used In Record-Breaking DDoS Attack https://www.darkreading.com/attacks-breaches/misconfigured-open-dns-servers-used-in-record-breaking-ddos-attack/d/d-id/1139433

[83] After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts https://www.theregister.co.uk/2017/05/03/hackers$_{f}ire_{u}p_{s}s7_{f}law$/

[84] White hats do an NSA, figure out LIVE PHONE TRACKING via protocol vuln https://www.theregister.co.uk/2014/12/26/ss7$_{a}ttacks$/

[85] Tobias Engel, "SS7: Locate. Track. Manipulate", 2014, https://imsicatcher.info/article/ss7-locate-track-manipulate/

[86] "SS7 Attack Discovery" , Positive Technologies, 2016 https://www.ptsecurity.com/upload/corporate/ww-en/products/documents/ss7/PT-TAD-Product-Brief-eng.pdf

[87] Schwachstelle im Mobilfunknetz: Kriminelle Hacker räumen Konten leer https://www.sueddeutsche.de/digital/it-sicherheit-schwachstelle-im-mobilfunknetz-kriminelle-hacker-raeumen-konten-leer-1.3486504

[88] Tunnel Vision : Malicious data interception via SS7 https://www.adaptivemobile.com/blog/malicious-data-interception-via-ss7

[89] HITB2014AMS – Day 2 – On Her Majesty's Secret Service: GRX A Spy Agency https://www.corelan.be/index.php/2014/05/30/hitb2014ams-day-2-on-her-majestys-secret-service-grx-a-spy-agency/

[90] Hacker Redirects Traffic From 19 Internet Providers to Steal Bitcoins https://www.wired.com/2014/08/isp-bitcoin-theft/

[91] Rostelecom Route Leak Targets E-Commerce Services https://blog.thousandeyes.com/rostelecom-route-leak-targets-ecommerce-services

[92] OK Google, why was your web traffic hijacked and routed through China, Russia today? https://www.theregister.co.uk/2018/11/13/google$_{r}ussia_{r}outing$/

Base Station (RBS), International Mobile Subscriber Identifier (IMSI) Catcher or Stingray can be used for traffic eavesdropping (passive and active) by exploiting security weaknesses in mobile networks. With mobile network evolution from 2G until 5G more security features have been added. However, the use of fake base station remains still possible and this issue is under discussion within the 3GPP SA3 to define a possible way to detect fake base station. The security enhancements provided with 5G network limit the type of information that can be gathered by using a fake base station. At least until 4G by using fake base station it is possible to retrieve the user IMSI, because device authenticates itself via its unique subscriber identity. This means that the fake BS can request the IMSI and gets it. 5G specifications provide the necessary mechanisms for protecting a user privacy and the subscriber's identity should have to be encrypted to prevent attacks from fake base station. Moreover, even in the current 5G there are some identification information transmitted from the device which are still unencrypted. This data can be captured by a fake BS and used to determine the class of devices, some hardware components, models and operating system. The info can be useful for attackers if they are looking for a specific custom device. An attacker can change the category of the target device so that the base station only provides 2G/3G connections. This will make the device vulnerable to other attacks specific to 2G/3G. In passive attacks, the false base station records and analyses the mobile radio signal of legitimate connections between the operator network and the targeted mobiles. The attacker can decode the network identifier of the targeted mobiles and possibly decrypt the communication content if it was encrypted using a vulnerable cipher algorithm. In an active attacker, the attacker is on the path of the communication between a targeted mobile and the legitimate network with a false base station used in a man-in-the-middle setup. The false base station impersonates the radio signal of a legitimate mobile network and forces the mobile device to connect to it by using a higher power signal. In the meantime, the false base station connects to the legitimate network by impersonating the targeted mobile. In 3G network, a false base station can relay the network authentication signaling to the intercepted mobile and ask the network to use either no security or vulnerable security algorithms. Examples of broken 2G cryptographic algorithms are A5/1 and A5/2. In addition, using a rogue base station broadcasting at a high-power level, an attacker can force a user to downgrade to either GSM or UMTS. For example, using a fake BS once IMSI of a target user has been obtained it could be possible to modify the 4G SDR based network code to degrade the 4G service completely forcing the device to look for another cell in the 3G frequencies or 2G[93]. Another way to perform downgrade attacks are reported in the paper "Practical attacks against privacy and availability in 4G/LTE mobile communications"[18]. Recently at the DefCon Security Conference in Las Vegas 2019, a team of researchers from Blackberry displayed how the calls can be hacked by cyber criminals.[94]

- **Threat T2.2.4: Traffic redirection:** An active domain name system (DNS) redirect attack, referred to as aLTEr has been recently demonstrated by researchers from Ruhr-Universität Bochum and New York University Abu Dhabi.[95] It allows an attacker to perform man-in-the-middle attacks to intercept communications and redirect the victim to malicious websites using DNS spoofing. This attack works by taking advantage of a design flaw within the LTE network: the data link layer (or layer 2) of the LTE network is encrypted with AES-CTR but it is not integrity-protected. This means an attacker can modify the bits even within an encrypted data packet, which later decrypts to a related plaintext. As a result, the attacker is posing as a cell tower to the victim, while pretending to be a subscriber to the real network.
- **Threat T2.3.1: Exploitation of software bugs:** Many attacks based on vulnerability exploitation have been reported against core and access networks. A massive attack was launched toward the end of 2016, main target was Deutsche Telekom Access Network and its Infrastructures. A cyber-attack that infected nearly one million routers used to access Deutsche Telekom Internet service was part of a campaign targeting web-connected devices around the globe.[96] The devices were vulnerable Customer Premises Equipment (CPE), and according to the telecommunications company, impacted customers were unable to connect to the Internet. Software vulnerabilities are also used to penetrate the network infrastructures by APT (Advanced Persistent Threat).[97] As described by Cybereason, the "Soft cell" operation started by exploiting a vulnerability in an unpatched IIS publicly-facing server from which the attackers gathered information about the network and propagated across the network. Recently it was also identified the Simjacker attack which exploit a vulnerability of a SIM Card technology, called S@T Browser. The key issue with the S@T Browser technology is that its default security does not require any authentication, and as a result the attacker is able to execute functionality on the SIM card with the aim to 'take over' the mobile phone to retrieve and perform sensitive commands. The location information of thousands of devices was obtained over time without the knowledge or consent of the targeted mobile phone users.[98]
- **Threat T2.3.2: Manipulation of hardware and firmware:** The Meltdown and Spectre vulnerabilities introduced the world to the power of hardware-level weaknesses.[99] The recently discovered LoJax[100] malware and the Hacking Team UEFI Rootkit are two of the most well-known examples of firmware attacks. In both examples, the malware targeted the system's UEFI firmware. These attacks took advantage of specific vulnerabilities and many other vulnerabilities have been discovered over the past few years in UEFI and related components. However, in some cases attackers do not need to exploit a vulnerability at all to install their malicious implants. Older systems and even some recent servers lack basic protections like signed firmware updates. These attacks can apply to virtually any devices that can be compromised with malware. While malware represents a common attack vector, research has shown that firmware can also be exploited remotely. This attack vector has a lot to do with the growing set of networking options found within UEFI components themselves. The standard UEFI codebase now includes a rich

[93] Israel Accused of Planting Mysterious Spy Devices Near the White House http://fakebts.com/author/pedro/
[94] Hackers Could Decrypt Your GSM Phone Calls https://www.wired.com/story/gsm-decrypt-calls
[95] Protecting against the latest LTE network attacks https://blogs.cisco.com/security/protecting-against-the-latest-lte-network-attacks
[96] New Mirai Variant Targets Routers, Knocks 900,000 Offline https://threatpost.com/new-mirai-variant-targets-routers-knocks-900000-offline/122155/
[97] Operation Soft Cell: A Worldwide Campaign Against Telecommunications Providers https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers
[98] New Simjacker vulnerability exploited by surveillance companies for espionage operation https://simjacker.com/
[99] Spectre and Meltdown explained: A comprehensive guide for professionals https://www.techrepublic.com/article/spectre-and-meltdown-explained-a-comprehensive-guide-for-professionals/
[100] LoJax: First UEFI rootkit found in the wild, courtesy of the Sednit group https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/

set of network capabilities for Ethernet, WiFi, and even Bluetooth that allow the firmware to communicate remotely and even perform a full HTTP boot from a remote server across the Internet. Eclypsium researchers found that in some cases the update over the Internet functionality was downloaded unverified and in the clear. The host would try to contact a remote update server using plain HTTP without SSL or any verification. This means that simple man-in-the-middle or other redirection techniques (e.g. DNS/ARP/route poisoning) could be used to modify the response returned to the client and exploit the vulnerability. As a result, the research showed that one could remotely deliver malicious code resulting in buffer overflows and arbitrary code execution just by checking if a newer version of the firmware exists.[101]

- **Threat T2.3.3: Malicious code/software/activity:** One of the most important technology in the network environment is the Software Define Network (SDN). SDN technology aims to replace the physical network by using a decoupled Data plane-Control plane architecture controlled by software. Although no specific malware attack has been already public announced, ETSI Security experts published the "ETSI GS NFV-SEC 003: Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance", where malware is indicated as one of the main threat vectors. Also, Academia and independent researchers are investigating the topic. As an example of such investigations, in 2016, during the Black Hat event, it was presented a paper "attacking SDN infrastructure: are we ready for the next-gen networking?".[102] The paper describes how malware can attack and damage SDN infrastructures. Two uses case have been presented: the first one shows how to infect the SDN Control Plane at Build-time and the second one how to infect the SDN Control plane at run time. Another example of malware spread that impacted the network functions was Wannacry, a ransomware crypto-worm that targeted computers running the Microsoft Windows operating system on May 2017. Once installed in a computer, thanks to its worm behaviour, it had the capabilities to spread into the local networks compromising the functionality of the network. Telefonica was impacted by this attack[103]. Malware spread can impact also the endpoint network asset. As a recent example, during June 2019 a new variant of malware was detected which aim to wipe the firmware of IoT devices in attacks reminiscent of the old BrickerBot malware that destroyed millions of devices back in 2017. This new variant is named Silex, it works by trashing an IoT device's storage, dropping firewall rules, removing the network configuration, and then halting the device.[104]
- **Threat T2.3.4: Remote activities (execution):** In 2018 Hackers targeted mobile phone networks around the world aiming to obtain CDR records.[97] The threat actor was attempting to steal all data stored in the active directory, compromising every single username and password in the organization, along with other personally identifiable information, billing data, call detail records, credentials, email servers, geo-location of users, and more. The attack began with a web shell running on a vulnerable, publicly-facing server, from which the attackers gathered information about the network and propagated across the network. The threat actor attempted to compromise critical assets, such as database servers, billing servers, and the active directory. The hackers created privileged accounts to easily regain access later, and in one case even set up a VPN connection to easily tunnel back into the network.
- **Threat T2.3.5: Malicious code - Signaling amplification attacks:** An attack consists of malicious users who take advantage of the signaling overhead required to setup and release dedicated bearers to overload the signaling plane by repeatedly triggering dedicated bearers' requests. A botnet of infected mobile devices could be used to generate a signaling amplification attack by forcing each terminal to constantly establish and release IP connections with an external server[55]. A piece of malware could also trigger mobile phones to reboot at the same time, thereby potentially overloading the Evolved Packet Core (EPC) with registrations once they come back up. It is also necessary to consider that, Home Subscriber Server (HSS) is also involved in a significant number of signaling processes at the EPC; thus, can as well suffer from signalling amplification attack. Such saturation of the EPC could potentially also occur legitimately due to the overwhelming amount of traffic and frequent reconnections of billions of Machine to Machine (M2M) nodes. Amplification attacks exploiting Network Transfer Protocol (NTP) and DNS signalling are reported in [105].
- **Threat T2.4.1: Failures of devices or systems:** A system failure caused a mobile internet, telephony and SMS outage for thousands of users. A software bug occurred in the SPR (Subscriber Profile Repository) server. Following the repeated instability of the equipment, the signalling traffic increased and the STP (Signalling Transfer Point) platforms became overloaded. As a result, end users had difficulties to access mobile internet services as well as voice and SMS services. The vendor responded by fully restoring the functionality of the SPR equipment. To stop the avalanche of signalling messages, the 3G and 4G networks were partially shut off and all subscribers were located on the 2G network.[81] A system failure caused a mobile internet outage for millions of users. A software bug occurred in the Internal system component Software Deployment Manager (SDM) leading to the degradation of user authorization for mobile data and mobile voice. As a result, end users had difficulties to access mobile services, both voice and data. Also, customers abroad were affected (roaming services). Mobile switches and mobile user registers were affected by this bug. The provider removed the obstacles in accessing the services and for the prevention of similar incidents in the future, a mitigation plan was created in collaboration with software vendors.[106] System failure caused disruption in, both mobile and fixed, telephony and internet services as well SMS/MMS services, affecting millions of users. Outage of several network components used for delivering DSL in the subscriber access network resulted in the disruption of mobile and fixed telephony and internet access. The provider responded by raising the capacity of the remaining network components. A subsequent software upgrade resolved the issue completely.[106]
- **Threat T2.4.2: Supply chain:** In 2018, several examples of supply chain attacks have been identified, including tampering

[101] Remote UEFI Attacks https://eclypsium.com/2018/08/27/uefi-remote-attacks/

[102] ATTACKING SDN INFRASTRUCTURE: ARE WE READY FOR THE NEXT-GEN NETWORKING? https://www.blackhat.com/docs/us-16/materials/us-16-Yoon-Attacking-SDN-Infrastructure-Are-We-Ready-For-The-Next-Gen-Networking.pdf

[103] What is the WannaCry Ransomware Attack? https://www.upguard.com/blog/wannacry

[104] New Silex malware is bricking IoT devices, has scary plans https://www.zdnet.com/article/new-silex-malware-is-bricking-iot-devices-has-scary-plans/

[105] See https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/

[106] Annual Report Telecom Security Incidents 2017 – enisa, https://www.enisa.europa.eu/publications/annual-report-telecom-security-incidents-2017/at$_d$*ownload/fullReport*

with chipsets[107] and vulnerabilities in AMD processors.[108] A recent case of "supply chain attacks" is the "NotPetya" malware. It spreads to systems that had a specific accounting software installed. The investigation of the incident revealed that the threat actor behind the attack compromised the infrastructure of the software provider, tampered the software, and pushed the tampered version of the software to the provider's clients as a legitimate software update. The software update essentially installed the "NotPetya" malware on the victim-machines. Another case is a backdoor dubbed ShadowPad. It was injected into a network management software suite and was pushed through a software update to the respective systems that had the software installed. The attack was spotted when a company using the software observed suspicious domain name lookup requests. Such a backdoor could potentially allow the threat actor behind the attack to load malware on the victim systems and/or exfiltrate data.[109]

- **Threat T2.4.3: Software bug:** Multiple vulnerabilities were found by security researchers in 4G routers manufactured by several companies, with the flaws exposing users to information leaks and command execution attacks.[110]

Attacks related to System-Centric Security

In the following, the main attacks affecting the System domain are reported.

- **Threat T3.1.1: Information leakage/sharing due to human errors:** Information leakage due to misconfiguration has been reported in many studies in literature and by CSA as one of the major sources of security issues. In 2017, a misconfigured AWS Simple Storage Service (S3) cloud storage bucket exposed detailed and private data[111]. In 2018, a server misconfiguration (public access) exposed the Elasticsearch database owned by Exactis to a massive breach containing highly personal data.[112] Again, in 2018, a misconfigured rsync server for backup permitted unauthenticated data transfer to any rsync client exposing, Level One Robotics customers' data (including Volkswagen, Chrysler).[113] Another famous example refers to Verizon customer accounts data beaches due to misconfiguration of S3 buckets. Other human errors can lead to system outage like in the case of the famous AWS employ error that took server offline.[114] AWS said that it has not had to fully reboot these S3 systems for several years, and the program has grown extensively since then, causing the restart to take longer than expected.
- **Threat T3.1.2: Inadequate design and planning or incorrect adaptation:** Examples of inadequate planning refers to the lack of controls on backups, and data cloning for internal management processes. Accenture inadvertently left a massive store of private data across four unsecured Amazon S3 buckets, exposing highly sensitive passwords and secret decryption keys. S3 buckets contained data that could be downloaded without a password by anyone just knowing the web addresses of the server.[115] Similarly, data that belong to Honda Connect App were exposed online. Researchers form Kromtech Security Center discovered the data stored on two unsecured, publicly accessible and unprotected Amazon AWS S3 Buckets.[116] In 2018, more than 120 million unique identification numbers issued by the Brazilian Federal Reserve to Brazilian citizens were exposed on unprotected S3 Bucket.[117] The problem was that the server was treated as accessible web server, while it should be protected. In 2019, Voipo, a Voice over Internet Protocol (VoIP) telecom company, exposed millions of unencrypted customer call logs and credentials on an Elasticsearch database.[118] The problem was again inadequate planning since it was declared that the server exposed was a development server having no security features enabled. Migration process can be also considered a source of serious threats for visualization, where migration is normally handled automatically for the sake of dynamic load balancing. During live migration, an attacker at malicious hypervisor may falsely advertise available resources to migrate the compromised VM to the trusted hypervisor. This is a malicious activity exploiting a wrongly designed migration process. Other examples refer to VM rollback. For instance, while restoring a VM from a snapshot to a previous state, the security features enabled in the actual state can be disabled. VM rollback can be exploited by an attacker even using a brute-force approach [19]. VM cloning can be used to copy and move a VM without revealing to the user that the VM has been cloned in multiple instances. VM cloning can be also executed for the legitimate scope of backup. In this case the backup location must be secured for intromission or copy even not intentional. Another example of wrongly designed process is the one related to Apache CloudStack (version before 4.5.2), which does not properly preserve VNC passwords when migrating KVM virtual machines (CVE-2015-3252), exposing to attacks at credential level.
- **Threat T3.2.1: Interception of information:** Attacks aiming to intercept data exchanged in internal or external communications involving the system at every level have been proposed in the past. At cloud level most of the attacks refer to applications deployed on the cloud. Considering virtualization layer, the recent foreshadow vulnerability (CVE-2018-3646) that affects XenServer allows an attacker to create a speculative side channel and steal data in VMRAM from other non-trusted VMs on the same physical server. Other attacks can exploit the cold boot of VM memory snapshot to capture sensible data or read the

[107] Security researcher claims Via C3 x86 CPUs contain hidden 'God mode' https://www.computing.co.uk/ctg/news/3060992/security-researcher-claims-via-c3-x86-cpus-contain-hidden-god-mode

[108] 13 flaws found in AMD processors, AMD given little warning https://www.networkworld.com/article/3262976/security/13-flaws-found-in-amd-processors-amd-given-little-warning.html

[109] ShadowPad: How Attackers hide Backdoor in Software used by Hundreds of Large Companies around the World https://www.kaspersky.com/about/press-releases/2017$_s$*hadowpad − how − attackers − hide − backdoor − in − software − used − by − hundreds − of − large − companies − around − the − world*

[110] 4G Router Vulnerabilities Lets Attackers Take Full Control https://www.bleepingcomputer.com/news/security/4g-router-vulnerabilities-let-attackers-take-full-control/

[111] See https://www.forbes.com/sites/thomasbrewster/2017/12/19/120m-american-household

[112] See https://www.wired.com/story/exactis-database-leak-340-millionrecords/

[113] See https://www.upguard.com/breaches/short-circuit-how-a-robotics-vendor-exposed-confidential-data-for-majormanufacturing-companies

[114] See Amazon explains big AWS outage, says employee error took servers offline, promises changes https://www.geekwire.com/2017/amazon-explains-massive-aws-outage-says-employee-error-took-servers-offline-promises-changes/

[115] See https://www.zdnet.com/article/accenture-left-a-huge-trove-of-clientpasswords-on-exposed-servers/

[116] Personal data of over 50,000 Honda Connect App leaked https://www.hackread.com/personal-data-of-over-50000-honda-connect-app-leaked/

[117] Exposed S3 bucket compromises 120 million Brazilian citizens https://www.scmagazine.com/home/security-news/exposed-s3-bucket-compromises-120-million-brazilian-citizens/

[118] See https://www.zdnet.com/article/voipo-database-exposed-millions-of-calland-sms-logs-system-data/

memory exchanged by different VMs [56]. Zhang at al.[57] used Prime+Probe technique on L2 cache to detect co-location on Xen. Monitoring L1 cache timing, Zhang et al.[58] extracted the ElGamal secret key that is used for GNU Privacy Guard decryption performed in another VM, while Weiß et al.[59] extracted AES keys of a VM running on an ARM Cortex-A8 processor. Irazoqui et al.[60] demonstrated a side-channel attack to recover AES keys in Xen and VMWare. Yarom at al.[61] used a flush and reload approach to observe shared pages of Intel X86 processor to extract private keys across multiprocessor and multicore running VMs. A related technique called Prime+Probe was adopted by Inci et al.[62] to monitor L3 cache in order to extract noisy data from Amazon E2 VM and use it to obtain RSA encryption key. Other approaches try to setup a covert-channel attack. Maurice et al.[63] used the same Prime+Probe approach for LLC-based covert channel. Xiao et al.[64] presented a memory deduplication-based covert-channel attack which is faster than L2 cache-based attacks. Another type of attack is the rowhammer attack across VMs exploiting memory de-duplication to obtain, for instance, a side channel and a covert channel[65]. Most of the above attacks use malicious actions or malware as vectors to exploit the vulnerability.

- **Threat T3.2.2: Unauthorised acquisition of information (data breach):** In general data breach is the main goal of an attack and therefore most of the attacks can be related to data breach. A famous example that refers to a cloud service is the Dropbox data breach in 2014[119] that permitted the discovery of private file transfer links. More recently, another data breach targeted Amazon Black Friday, where details about amazon e-commerce was exposed.[120] The famous VENOM vulnerability (CVE-2015-3456) at virtualization layer that affects Qemu can potentially lead to data breach as well. It allows an attacker to break out a VM, execute code on a host machine, and access all the other VMs on the host. A potential data breach was also reported as connected to VMware and Dell EMC storage as a service technology and a trio of critical vulnerabilities (CVE-2017-15548, CVE-2017-15549, and CVE-2017-15550). A set of potential data breaches are related to attacks on VM images focused on extracting data from the VM image file at rest. Similar to this, but more sophisticated, is the VM data remanence attack. Data remanence was experimented by Albelooshi at al.[66] to see if physical representation of digital data remains on the physical device even after its removal.
- **Threat T3.3.1: Configuration poisoning:** The case of Capital One attack is an example of multiple deliberate configuration poisoning of both firewall and S3 bucket to expose data.[121] In 2017 National Credit Federation exposed its customers data due to an intentional poisoning of AWS S3 bucket configured for public access under a subdomain. As a side note, the company did not react immediately to this potential breach due to the difficulties of updating device firmware. In 2019, Ascension, a data and analytics company, database was exposed on a publicly accessible elastic search database apparently due to a poisoned backup process. Again in 2019, a massive government data set belonging to the Oklahoma Department of Securities (ODS) was left unsecured on a storage server (based on an open access rsync) exposing millions of sensitive files.[122]
- **Threat T3.3.2: Business process poisoning:** A famous example of BPC attack was the one of Bangladesh Central Bank, which resulted in losses of up to US$81 million poisoning the SWIFT protocol for money transfer using a piggybacking approach. This is more at application level, but similar concepts can be exploited at cloud/virtualization level. Considering the cloud environment, the business process implementation in cloud is a preferred target for compromising since it is much less visible than a normal business process and the attacker activities can be more complex to detect. Another example refers to VM relocation. It can be exploited explicitly poisoning the process to target a malicious server, where memory snapshot is enabled[67]. Other examples in threat T3.1.2 that are relative to inadequate design and planning or incorrect adaptation can be exploited also via ad hoc poisoning of cloud/virtualization processes.
- **Threat 3.4.1: Identity fraud:** In virtualized environments, privilege escalation can be even more dangerous than in a physical environments because of multitenancy and the hierarchical structure of administrator privileges. In addition, VMM is a crucial target for usurpation-based misappropriation, due to its role in virtualization, as well as to the presence of vulnerabilities that allow guest-OS users the potential to execute arbitrary code on the host OS.[123] Timehop had a data breach due to compromised admin credentials that were used to enter their Cloud.[124] Deloitte experienced a major data breach due to weak identity, credential and access management or its Azure account in 2017. More recently, in 2018, a German student hacked data protected by weak passwords.[125] Generally speaking, 2017 was the year of the rise of cloud account-targeted campaigns, in particular for Microsoft Office 365 accounts. Another example of account hijacking was presented as a PoC in 2018. It was based on compromises of Microsoft live accounts via subdomain hijacking.[126]
- **Threat T3.4.2: Denial of service:** Both on cloud and virtualization the main scope of the attacker is to exploit the sharing of resources. In virtualization, examples of attacks are the ones that focused on the hypervisor crash. A VM may corrupt the hypervisor memory and cause the hypervisor to crash leading to DoS (CVE-2018-7542 on Xen via NULL pointer dereference).[127] Resource starvation can be exploited to violate the availability of the hypervisor via uncontrolled resource allocation[68]. In cloud, the concept is very similar due to the idea to share services among different users and tenants. However, some DoS attacks in cloud also target the API exposed by the different cloud layers. Yeh et al.[69] presented a multi-resource DoS attack on cloud VM migration schemes.
- **Threat T3.4.3: Malicious code/software/activity:** The Zepto variant of the Locky ransomware spreads via cloud services such

[119] Dropbox and Box leak files in security through obscurity nightmare https://www.techrepublic.com/article/dropbox-and-box-leak-files-in-security-through-obscurity-nightmare/

[120] Amazon hit with major data breach days before Black Friday https://www.theguardian.com/technology/2018/nov/21/amazon-hit-with-major-data-breach-days-before-black-friday

[121] Capital One Data Breach Impacts 100 Million Customers https://divvycloud.com/capital-one-data-breach/

[122] Unprotected Government Server Exposes Years of FBI Investigations https://thehackernews.com/2019/01/oklahoma-fbi-data-leak.html

[123] Common Vulnerabilities and Exposures (2012) CVE-2012-2450. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2450.

[124] Timehop discloses July 4 data breach affecting 21 million https://techcrunch.com/2018/07/09/timehop-discloses-july-4-data-breach-affecting-21-million/

[125] German Man Confesses to Hacking Politicians' Data, Officials Say https://www.nytimes.com/2019/01/08/world/europe/germany-hacking-arrest.html

[126] PoC Exploit Compromises Microsoft Live Accounts via Subdomain Hijacking https://threatpost.com/poc-exploit-compromises-microsoft-live-accounts-via-subdomain-hijacking/138719/

[127] A Methodology for Determining Forensic Data Requirements for Detecting Hypervisor Attacks https://pdfs.semanticscholar.org/4e09/697e99b107f11f90ca-563160d4be95bb90c2.pdf

as Microsoft OneDrive, Google Drive and Box by sharing a malicious file with potential victims. Similarly, CloudSquirrel attack establishes a connection with its command and control hosted in Dropbox. Historical examples of hyperjacking are the SubVirt[70] that installs a hypervisor below the host OS and controls the VM and the Blue Pill[71] that exploits hardware extensions in the virtualization enabled CPUs and runs an infected system into a VM. In the work of Jasti et al.[72], VM hoping has been demonstrated by maliciously gaining an access to different VMs.

- **Threat T3.4.4: Generation and use of rogue certificates:** This threat is usually at the basis of other more complex attacks as discussed in the previous threats. As an example, BIG-IP and BIG-IQ do not properly regenerate certificates and keys when deploying VM image on AWS, Azure or Verizon cloud service, which makes multiple instances to share the same certificates and keys. It causes the disruption of services eventually leading to information leak (CVE-2016-2084).
- **Threat T3.4.5: Misuse of assurance tools:** The complexity of the current cloud systems makes the poisoning of assurance tools critical to cover unauthorized access to large amounts of personally identifiable data. No recent attacks have been reported.
- **Threat T3.4.6: Failures of business process:** In general, there are a number of attacks that exploit shadow IT. Some of them rely with the usage of apps installed on mobile devices or on free services used by one or more company employee, for instance, to fulfil a temporal need. In many of the cases, these services are used just few times and then forgotten, without taking care of updates and new security issues discovered. Reports on attacks exploiting shadow IT are not frequent, since they are not easy to be discovered; however, every attack that is caused by an employee using a vulnerable service against company regulations in terms of adoption of abnormal usage can be considered relevant to this threat. NormShield reports on breaches caused by third parties. This can be considered as a superset of the Shadow IT based attacks including also app misuse in some cases.
- **Threat T3.4.7: Code execution and injection (unsecure APIs):** A famous attack dates back to 2010. An Amazon cross-site scripting (XSS) bug enabled credential theft. Another famous attack was the one of US Internal Revenue Service (IRS) in 2015, which exposed a great amount of record via a vulnerable API ("Get Transcript"). More recently, a vulnerability of Facebook API was exploited resulting in the generation of an access token that had the permissions of the Facebook mobile app, not for the viewer, but for the other Facebook user. This also links back to account hijacking. Considering virtualization level, and specifically the management interface injection vulnerability can be exploited. For example, CSS vulnerability (CVE-2012-5050) in VMware vCenter Operations before 5.0.x allows remote attackers to inject arbitrary web script to take control of vCenter". The Iago attack[73] is an example of virtualization level API call from kernel perspective. Supposing to have a malicious kernel, it can make an application to act against its interests by communicating with it, since applications generally do not check return values from the kernel.
- **Threat T3.5.1: Violation of laws or regulations data**
- **Threat T3.6.1: Skill shortage:** Examples of attacks that ground on skill shortage can be found in TG3.1. The main problem is the wrong "lift-and-shift" approach in moving traditional ICT to the cloud, where missing skills play a significant role.
- **Threat T3.6.2: Malicious insider:** A famous example of malicious insider was the 2018 Tesla saboteur. The sabotage included the use of false usernames to make changes to the code used in the Tesla Manufacturing Operation System Cloud, as well as exporting large amounts of highly sensitive data to unknown third parties. Another example of malicious insider that can be also linked to failure of business process was discovered in 2018 and refers to an engineer that was found guilty of stealing navy secrets via personal Dropbox account.[128] Considering virtualized environments, a compromised management interface can be used to exploit vulnerabilities by a privileged user (CVE-2016-9603, CVE-2017-2615), having the scope to attack the hypervisor like the compromising CIA, DMA attack exploiting the direct channel between hypervisor and the HW, VM sprawl attack aimed to violate the hypervisor availability. In addition, management interface can be directly accessed by a malicious insider[74][75] leading to attacks on the VMs[76].

Attacks related to Data-Centric Security

In the following, the main attacks affecting the Data domain are reported.

- **Threat T4.1.1: Information leakage/sharing due to human errors:** Information leakage due to misconfiguration has been reported in many studies in literature. BinaryEdge[129] showed how erroneous system misconfigurations led to weaknesses in Redis, MongoDB, Memcache and ElasticSearch. The same study comments how very often these technologies are meant to be installed in private environments, providing weak default security configurations (e.g., no authentication or encryption), privileging performance. Other attacks have been reported with unauthorized sharing of sensitive and confidential information.[130] The data breach targeting Equifax[38] in 2017 was one of the widest breaches ever. Hackers took advantage from a well-known bug that was exploited due to the fact that the Equifax system was not up-to-date. The hackers stolen names, birthdates, Social Security numbers, addresses, and driver license numbers for 145.5 million Americans plus approximately 200,000 credit card numbers, and affected more than 100 million credit users worldwide.[131] Targeted phishing attacks are rapidly increasing and are relevant for both data and user domains.[17] Cyber criminals target rich individuals and top-management people that have access to sensitive data, as well as public authorities that handle personal identifiable information.[132][133] Also, a shift from

[128] Engineer Found Guilty of Stealing Navy Secrets via Dropbox Account https://www.bleepingcomputer.com/news/legal/engineer-found-guilty-of-stealing-navy-secrets-via-dropbox-account/

[129] Data, Technologies and Security - Part 1 http://blog.binaryedge.io/2015/08/10/data-technologies-and-security-part-1/

[130] Dropbox Security Bug Made Passwords Optional For Four Hours, http://techcrunch.com/2011/06/20/dropbox-security-bug-made-passwords-optional-for-four-hours/

[131] Data Breach https://www.malwarebytes.com/data-breach/

[132] Malwarebytes LABS, Cybercrime tactics and techniques: Q2 2018 https://resources.malwarebytes.com/files/2018/07/Malwarebytes$_C$*ybercrime – Tactics – and – Techniques – Q2 – 2018.pdf*

[133] KrebsOnSecurity, The Year Targeted Phishing Went Mainstream, https://krebsonsecurity.com/2018/08/the-year-targeted-phishing-went-mainstream/

consumer to enterprise targets has been observed and driven by profit.[38][17] Business email compromise (BEC) scams[134] is a financial fraud also called CEO fraud that aims to reduce the effort of a phishing attack. Before sending an attack, the cyber-criminals identify the preferred victim in the business (e.g., someone from the finance department), and send a fraudulent email, impersonating the CEO or CFO. PIR Bank in Russia lost $920,000 due to an outdated, unsupported cisco router that was used as a trojan horse to reach the core of the bank.[135] A similar issue happened to British Airways, where an outdated version of Modernizr Javascript library was exploited to steal customer data.[136] MongoDB, a major open source NoSQL database, was the target of different attacks. In 2015,[137] three students from University of Saarland in Germany at the Centre for IT Security found that the default installation of MongoDB running at TCP port 27017 was freely available for read and write operations. More recently, in 2017, hackers have wiped more than 26k MongoDB again exploiting its default configuration permitting connections from the Internet.[138] A rise in attacks to Hadoop components, such as Hadoop YARN, Redis, and ActiveMQ has been observed. The goals of these attacks can be different, from cryptomining to ransomware and data wiping.[139][140][141] A company affiliated to FedEx was breached due to an unsecure Amazon S3 server and resulted in data exposed on the internet.[17] Similarly, data from 221 LA County was accidentally exposed due to a misconfigured S3 cloud server.[17]

- **Threat T4.1.2: Inadequate design and planning or incorrect adaptation:** It has been shown how the replication approach taken by Hadoop framework can backfire:[142] a corrupted application could destroy all replicas. Damiani[77] claims that Hadoop redundancy could even be a non-linear risk booster for Big Data leakages. Also, Aditham[78] shows how the design of the Hadoop Distributed File System (HDFS) could introduce security problems. HDFS, which is the basis of many storage systems, originally, cannot tolerate the failure of Namenode, as proved in real scenarios.[143] Finally, NIST reported a scenario where digital rights management (DRM) techniques were not built to scale and caused system failures.[144][145] In 2017, Amazon AWS and, in particular, its S3 storage, suffered a major outage.[146][147] This outage was due to the fact that to fix a performance problem an incorrect command was sent causing this unexpected disruption. After this command was set, an unpredictable sequence of cascading events caused the big denial of service. Apache Ambari erroneously stored sensitive data on disk in temporary files on the Ambari server host.[148] These files were then readable by any authenticated users. The database server of Exactis was publicly accessible and resulted in the theft of millions user records.[17][149]
- **Threat T4.2.1: Interception of information:** Attacks aiming to intercept data exchanged in internal or external communications involving the Big Data platform have been proposed in the past. Among them, we can consider hijacking and eavesdropping. Hijacking is an active attack and aims to take control of a communication and its content. Eavesdropping is a passive attack where the content of the communication is intercepted without interfering with the information flow. In 2017, the biggest data breach targeting Equifax[38] affected more than 100 million credit users worldwide and across the EU. Note that the General Data Protection Regulation (GDPR) that became applicable in May 2018 dictates the mandatory reporting of data breaches (both to affected individuals and Data Protection Authorities), provided that certain requirements are met. A vulnerability in Apache Hadoop Distributed File System (HDFS) permitted cyber criminals to remotely access sensitive information with no authentication.[150] Apache Ambari permitted cyber attackers to steal sensitive information, caused by the exposure of passwords for Hadoop credential. These passwords are stored in Ambari Agent informational log messages when the credential store feature is enabled for eligible services.[151][152]
- **Threat T4.2.2: Unauthorised acquisition of information (data breach):** Massive privacy breaches have been reported,[153][154] where administrative credentials have been used to regularly access private user information. As already mentioned, in 2017, the biggest data breach targeted Equifax65 and affected more than 100 million credit users worldwide. Data breach at Yahoo is the biggest data breach ever and involved three billion customers.[38][155]Abuse of Point of Sales (POS) terminals is another

[134] Symantec, BEC Scams Remain a Billion-Dollar Enterprise, Targeting 6K Businesses Monthly, July 2019 https://www.symantec.com/blogs/threat-intelligence/bec-scams-trends-and-themes-2019 July

[135] Data Breach Investigations Report 2019, https://enterprise.verizon.com/resources/reports/dbir/

[136] A simple fix could have saved British Airways from its £183m fine https://www.wired.co.uk/article/british-airways-data-breach-gdpr-fine

[137] 40,000 UnProtected MongoDB Databases Found on the Internet https://thehackernews.com/2015/02/mongodb-database-hacking.html

[138] More than 26,000 vulnerable MongoDB databases whacked by ransomware https://www.theinquirer.net/inquirer/news/3016752/mongodb-hack-26000-databases-whacked-by-ransomware

[139] Securonix Threat Research:Detecting Persistent Cloud Infrastructure/Hadoop/YARN Attacks Using Security Analytics:Moanacroner, XBash, and Others https://www.securonix.com/web/wp-content/uploads/2019/01/Securonix$_{T}hreat_{R}esearch_{M}oanacroner_{X}Bash.pdf$

[140] Hadoop coop thrown for loop by malware snoop n' scoop troop? Oh poop https://www.theregister.co.uk/2019/01/24/hadoop$_{m}alware_{a}ttack/$

[141] Securonix Threat Research: Detecting Persistent Cloud Infrastructure/Hadoop/YARN Attacks Using Security Analytics: Moanacroner, XBash, and Others https://www.securonix.com/securonix-threat-research-detecting-persistent-cloud-infrastructure-hadoop-yarn-attacks-using-security-analytics-moanacroner-xbash-and-others/

[142] How Your Hadoop Distribution Could Lose Your Data Forever http://www.smartdatacollective.com/michelenemschoff/193731/how-your-hadoop-distribution-could-lose-your-data-forever

[143] See "Notes by Facebook engineering" in https://www.facebook.com/notes/facebook-engineering/under-the-hood-hadoop-distributed-filesystem-reliability-with-namenode-and-avata/10150888759153920

[144] NIST Special Publication 1500-4. Use case: consumer digital media (examples: Netflix, iTunes, and others).

[145] Xiao Zhang, "A Survey of Digital Rights Management Technologies", see http://www.cse.wustl.edu/ jain/cse571-11/ftp/drm.pdf

[146] Typo blamed for Amazon's internet-crippling outage https://www.theguardian.com/technology/2017/mar/03/typo-blamed-amazon-web-services-internet-outage

[147] Amazon knocked AWS sites offline because of typo https://www.zdnet.com/article/amazon-knocked-aws-sites-offline-because-of-typo/

[148] See https://www.cvedetails.com/cve/CVE-2017-5655/

[149] Cyber Risk Outlook 2018 https://www.jbs.cam.ac.uk/fileadmin/user$_{u}pload/research/centres/risk/downloads/crs - cyber - risk - outlook - 2018.pdf$

[150] Common Vulnerabilities and Exposures https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1296

[151] Apache Ambari Hadoop credential stores information disclosure https://exchange.xforce.ibmcloud.com/vulnerabilities/146702

[152] See https://www.cvedetails.com/cve/CVE-2018-8042/

[153] "Google fires employees for breaching user privacy" in TechSpot news, (Sept 2010) in http://www.techspot.com/news/40280-google-fired-employees-for-breaching-user-privacy.html

[154] Armerding, T., The 17 biggest data breaches of the 21st century, https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html, 2018.

[155] Djurberg, J. A., Bekräftat: ddos-attack bakom tågförseningar [Confirmed: DDOS attack behind train delays], https://computersweden.idg.se/2.2683/1.690504/ddos-bakom-tagforseningar, 2017

example of unauthorised acquisition of information.[38] The terminal is manipulated to access and distribute the data of the customers, or in other cases fake companies are created to steal these data. A weakness in the "Search" capability of the Facebook platform resulted in one of the biggest data breaches where about 2.000 million users' information was exposed (including Cambridge Analytica case[156]).[17] A problem in the Twitter procedure for password handling exposed passwords in plain text.[17]

- **Threat T4.3.1: Data poisoning:** Data poisoning is often seen as a preparation activity for launching attacks (e.g., Carbanak and Cobalt malware[157]). It is at the basis of the other threats in this deliverable, as a means for hiding malicious behavior and covering malicious traces (see Threat T4.4.5), and as a way to manipulate inferences and decisions. Specific to this threat, in 2015, attacks to drug infusion pump have been reported.[158][159] Cyber criminals were able to modify the amount of drugs distributed to patients potentially causing an overdose, due to lack of authentication.
- **Threat T4.3.2: Model poisoning:** Adversarial machine learning is a technique developed in the field of machine learning that aims to fool model learning through data poisoning[79]. The goal is to provide model training with fake data that cause the trained model to make a mistake and malfunction. Zhao et al.[80] presented an overview of data poisoning attacks on multi-task relationship learning, and an approach to optimal data poisoning. Yi et al.[81] presented an adversarial machine learning approach that aims to spectrum data poisoning attack. The goal is to let an adversary falsify the spectrum sensing data in wireless communications. Li et al.[82] presented data poisoning attacks on collaborative filtering systems, where an attacker generates malicious data to avoid being detected. Zugner et al.[83] studied adversarial attacks on neural networks for graph data.
- **Threat T4.4.1: Identity fraud:** Some of the attacks based on identity fraud target the control infrastructure (and the user's system interface) where the Big Data systems is built, such as private or public clouds[84]. An attack permitting to take control over the console gives to the attacker the ability of managing the user's account including the access to stored data. Attacks of this type[160] are based on a mixture of signature wrapping and advanced XSS techniques, then privilege escalation leading to identity fraud. Last but not least, attacks often target social networks. For example, XSS vulnerabilities on Twitter have been used to push malicious and fake tweets, while Internet malware has emerged on Facebook as a means of promoting malicious profiles.[161] Social engineering attacks continue to grow with the goal of obtaining personal data, hijacking accounts, steal identities.[38] Identity fraud can also target companies. For instance, attackers can try to impersonate legitimate businesses to retrieve Point of Sales (POS) terminals that are then used to steal customer data.[38] This attack is possible since the information used to request a POS is non-confidential. The Card-not-present fraud is another example of attack that can be linked to the identify fraud.[38] Stolen credit cards are used for e-commerce shopping.
- **Threat T4.4.2: Denial of service:** A DoS attack targeted the Hadoop cluster, leading to a significant decrease of system performance and causing the loss of the targeted resource to other cloud users[85]. An attack to Amazon distributed storage was also reported, based on authenticated requests and account validation.[162] Also, attacks to social networks have been reported, such as the one exploiting some weaknesses of the Hadoop Distributed File system, to target Facebook[143]. Today, Distributed-Denial-of-Service (DDoS) attacks are distributed as a tool against private business as well as the public sector. The aims of these attacks are used financial gains, as well as ideological, political or purely malicious reasons. This type of attack is the most widespread second to malware attacks only (2017), and is increasingly becoming more accessible, low cost and low risk. Data wiping attacks target data availability by overwriting files/data with random data or by deleting them. Shamoon Malware infects a system and then wipes all its files, destroying the hard disk and making systems unusable. It was first introduced in 2012, and then reused in 2016, to attack oil and gas company Saudi Aramco in the Middle East. In 2018, the last version of the malware was used to attack the Italian oil and gas firm Saipem.[163] The new malware involves a new wiper that deletes files from infected computers before the Shamoon malware wipes the master boot record. Saipem stated that between 300 and 400 servers and up to 100 personal computers were compromised. DemBot malware[164][165] targeted Hadoop server using a YARN exploit to take control of the system and launch a DDoS attack. A similar attack used Mirai malware to exploit the same Hadoop YARN exploit and launch a devastating DDoS.[166][167]
- **Threat T4.4.3: Malicious code/software/activity:** Service spoofing (e.g., ARP spoofing) aims to masquerades an attacker identity to take a competitive advantage. Web application attacks and code injection attacks are traditional examples of attacks that often represent the starting point for more sophisticated attacks. In Big Data, malware can infect nodes to send malicious commands to other servers, worms can distribute themselves sending copies to other nodes. Backdoors or hidden functionality can simplify accesses to components and devices[86]. A malicious code attack is also reported in [86] as faulty results of the Hadoop logging data system. It uses a malicious script to let Flume streaming previously modified log data into Hcatalog [86]. MapReduce computational framework has been the target of malicious software. Untrusted mappers can in fact alter results, whose malicious activities could be difficult to identify with large amount of data.[48] Ransomware[38] is still a critical attack that aims to target availability of data; recently, we are moving from financial motivations to nation states actions. Meltdown[87]

[156] The Value of Personal Online Data https://www.enisa.europa.eu/publications/info-notes/the-value-of-personal-online-data

[157] Carbank/Cobalt A global threat to financial institutions https://www.europol.europa.eu/sites/default/files/documents/carbanakcobalt.pdf

[158] A hacker can give you a fatal overdose https://money.cnn.com/2015/06/10/technology/drug-pump-hack/

[159] Hacker Can Spend Fatal Dose to Hospital Drug Pumps https://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps

[160] US-CERT warns of guest-to-host VM escape vulnerability http://www.zdnet.com/article/us-cert-warns-of-guest-to-host-vm-escape-vulnerability/

[161] See Nine Threats Targeting Facebook Users in http://www.itbusinessedge.com/slideshows/show.aspx?c=90875

[162] ZDnet bog in http://www.zdnet.com/article/amazon-explains-its-s3-outage/

[163] Shamoon: Destructive Threat Re-Emerges with New Sting in its Tail https://www.symantec.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail

[164] DemonBot Malware Targets Apache Hadoop Servers Using Available Exploit Code https://www.tenable.com/blog/demonbot-malware-targets-apache-hadoop-servers-using-available-exploit-code

[165] New DDoS botnet goes after Hadoop enterprise servers https://www.zdnet.com/article/new-ddos-botnet-goes-after-hadoop-enterprise-servers/

[166] Mirai 'botmasters' now exploiting Hadoop flaw to target Linux servers https://www.itpro.co.uk/botnets/32427/mirai-botmasters-now-exploiting-hadoop-flaw-to-target-linux-servers

[167] Due to Misconfigured Component: DemonBot Malware Infects Multiple Apache Hadoop Servers https://hackercombat.com/due-to-misconfigured-component-demonbot-malware-infects-multiple-apache-hadoop-servers/

and Spectre[88] are new information disclosure vulnerabilities in most modern microprocessors.[135] They break the isolation between user applications and operating system, and different applications, respectively, to the aim of retrieving sensitive data in the memory of other running programs,[168] including passwords, personal photos, emails, instant messages and even business-critical documents. In 2013, the Carbanak and Cobalt malware[38] was launched targeting financial institutions. The malware took control of the servers and ATMs, impersonating customers for money transfers, inflating account balances and controlling ATMs. This attack also links to threat T4.4.1 identity fraud and threat T4.3.1 data poisoning. The gang managing this malware got arrested in 2018.

- **Threat T4.4.4: Generation and use of rogue certificates:** This threat is usually at the basis of more complex attacks as discussed in the previous threats, in particular, T4.2.1, T4.3.2, T4.4.1, T4.4.2. For instance, an increase in phishing sites using HTTPS has been observed.[17] Attackers used free certificate services like Let's Encrypt or Comodo to break the common assumption that HTTPS web sites are secure and safe.
- **Threat T4.4.5: Misuse of assurance tools:** The complexity of current data storage and databases makes poisoning of assurance tools critical to cover unauthorized access to large amounts of personally identifiable data. No recent attacks have been reported.
- **Threat T4.4.6: Failures of business process:** User re-identification is an example of weak anonymization. While data collection and aggregation use anonymization techniques, individual users can be re-identified by leveraging other Big Data data sets, often available in the public domain [89]. This scenario is put to the extreme by Big Data variety that permits to infer identity from anonymized data sets by correlating with apparently innocuous public information.[169][170][171]
- **Threat T4.4.7: Code execution and injection (unsecure APIs):** Data breaches due to unsecure APIs have been reported in the past and often targeted social networks (e.g., Facebook, Yahoo and Snapchat).[172][173] SPARQL code injection is an example of attacks to Semantic Web technologies [90]. Security flaws are rather common in Big Data languages like SPARQL, RDQL and SPARUL, mimicking the one affecting traditional and still dangerous query languages, like SQL, LDAP and XPath injection [91][174]. Hive, MongoDB and CouchDB also suffer from traditional threats such as code execution and remote SQL injection.[175][176] A big data breach was reported on India's national ID database, "Aadhaar," affecting more than 1.2 billion Indian citizens. The breach was due to an unsecured API used to check a customer's status and verify their identity.[177] Apache Hadoop YARN NodeManager Daemon has been found to be vulnerable to Zip Slip vulnerability.[178] This attack permits to inject malicious code in the jobs of other cluster users. In 2018, Alibaba Cloud Security Team discovered the first Remote Code Execution (RCE) exploit in Spark Rest API.[179] This weakness allowed to instruct the server to download and execute a remote jar file from the Darknet. A vulnerability in Apache Spark permitted an unauthenticated, remote attacker to execute arbitrary code on the master host of a targeted system.[180] This vulnerability exploits improper security restrictions and insufficient validation of user-supplied input. A vulnerability in Apache Ambari permitted to implement persistent cross-site scripting thanks to insufficient sanitization of user-supplied data.[181] A weakness in the British Airways web and mobile app caused the exposition of personal and payment data.[182]
- **Threat T4.5.1: Violation of laws or regulations**
- **Threat T4.6.1: Skill shortage:** Data analysis and management are among the most important activities in a Big Data environment. Data science skill and data scientist shortage introduce unprecedented risks.[183] Lack of skill can in fact result in wrong decisions and adaptations with catastrophic consequences on the target system (see also threat T4.1.1). The inability to properly analyse large data sets can then result in substantial loss of money, reducing productivity and innovation growth.
- **Threat T4.6.2: Malicious insider:** In the data domain, the risks introduced by insider threats are quite clear and often result in data leakage. The goal is to increase the cyber attacker revenue or to decrease the reputation of the attack target. Very famous are the cases of Edward Snowden or Chelsea Manning (the work in [92] provides the description of the most famous insider threat cases). Case studies of insider threats have been analyzed in different domains and from different angles [93]. For instance, Randazzo et al.[94] presented 23 case studies in the finance sector, while Kowalski et al.[95] 36 case studies in the government sector, involving fraud, IP theft, and sabotage of the IS/network, and combination thereof. Other works [96][97]described case studies including system administrators, programmers, and network professionals. Keeney et al.[98] also presented different cases of Sabotage using IT in critical infrastructures. Additional work has been done in [99][100][101][102] aimed to data exfiltration, IP theft, or sabotage in financial and military sectors. Unintentional insider threat was considered by [102] (phishing attacks) and [103] (unintentional denial of service).

[168] Meltdown and Spectre Vulnerabilities in modern computers leak passwords and sensitive data https://meltdownattack.com/

[169] AOL search data leak https://en.wikipedia.org/wiki/AOL$_s$*earch*$_d$*ata*$_l$*eak*

[170] See NIST Big Data Interoperability Framework: Volume 4, Security and Privacy. Use case: Web traffic analytics in retail and marketing.

[171] ENISA's report "Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics "

[172] Jaime Ryan (CA, Sr. Director) and Tyson Whitten (CA, Director of API Management) in "Takeaways from API Security Breaches" presentation and webinar (2015) reported breaches, due to unsecure APIs, for Yahoo, Snapchat and other companies, see http://transform.ca.com/API-security-breaches.html?source=AAblog

[173] See security issues for the Graph Facebook API library reported by Websegura technical blog, http://www.websegura.net/advisories/facebook-rfd-and-open-file-upload/

[174] In October 2015, presumably, an SQL injection was used to attack the servers of British telecommunications company Talk Talk's, endangering the personal details of up to four million customers. See http://www.mobilenewscwp.co.uk/2015/10/23/talktalk-hacking-scandal-expert-reaction/

[175] 50 For example Hive version 2.0 suffers from cross site scripting, code execution, and remote SQL injection vulnerabilities, see https://packetstormsecurity.com/files/132136/Hive-2.0-RC2-XSS-Code-Execution-SQL-Injection.html.

[176] MongoDB suffers injection attacks, see 212

[177] A new data leak hits Aadhaar, India's national ID database https://www.zdnet.com/article/another-data-leak-hits-india-aadhaar-biometric-database/

[178] Apache Hadoop spins cracking code injection vulnerability YARN https://www.theregister.co.uk/2018/11/23/apache$_h$*adoop*$_y$*arn*$_z$*ip*$_s$*lip*$_v$*ulnerability/*

[179] Alibaba Cloud Security Team Discovers Apache Spark Rest API Remote Code Execution (RCE) Exploit https://www.alibabacloud.com/blog/alibaba-cloud-security-team-discovers-apache-spark-rest-api-remote-code-execution-rce-exploit$_5$93865

[180] Announcement Regarding Non-Cisco Product Security Alerts https://tools.cisco.com/security/center/viewAlert.x?alertId=59176

[181] Cross-site scripting in Apache Ambari https://www.cybersecurity-help.cz/vdb/SB2019052711

[182] Customer data theft https://www.britishairways.com/en-gb/information/incident/data-theft/latest-information

[183] August LinkedIn Workforce Report: Data Science Skills are in High Demand Across Industries https://news.linkedin.com/2018/8/linkedin-workforce-report-august-2018

Attacks related to Application-Centric Security

In the following, the main attacks affecting the Application domain are reported.

- **Threat T5.1.1: Security Misconfiguration:** Default configurations are usually at the basis of security breaches. For instance, Amazon AWS S3 poorly configured access control policy allows an attacker to read and write data from a bucket.[184] Mirai IoT malware targets the devices that are usually managed by not-expert people and come with default configurations. Being such devices often available through the network using an application (GUI) with default credentials, they are the perfect target for malware like Mirai.[185] Other attacks like WannaCry, one of the most known cryptolockers, used the EternalBlue exploit, spreading the ransomware to every other unpatched computer on the network using a single vulnerable and internet-exposed system.[186] The slow patching process of companies made the cryptolocker effective even if Microsoft already released a patch. Other attacks target insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information in operating systems, frameworks, libraries, and applications.[12] Vulnerable XML processors can be used to attack XML-based web services:[12] ”Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.” In this context, well-known attacks are Billion Laughs Attack and SAML Security XML External Entity Attack.
- **Threat T5.2.1: Interception of information:** In addition to attacks presented in other domains, many attacks resulting in information interception have been reported. Advanced Persistent Malware is increasingly designed to steal SSL/TLS keys and certificates.[187] For instance, the Heartbleed Bug vulnerability of OpenSSL cryptographic software library permitted to steal sensitive information (digital keys and certificates) normally protected by SSL/TLS encryption.[188] Man-in-the-Middle (MITM) Attacks are traditional attacks where an attacker impersonates a trusted website accessing all communications. Again, steal of SSL/TLS keys and certificates facilitates such attack, and unsecured or lightly protected wireless access points are often exploited for entry. Self-signed and wildcard certificates, as well as unknown, untrusted, and forged certificate authorities are other sources of attacks.[187189] The first is at the basis of fake web sites for phishing attacks; the second results, as proven by NetCraft in 2014, fake digital certificates impersonating banks, ecommerce sites, ISPs and social networks deployed across the Internet.
- **Threat T5.2.2: Sensitive data exposure:** Attacks in this threat mainly resembles to attacks described in T5.1.1 and T5.1.2 in this section, and T4.1.1, T4.2.1, T4.2.2, T4.4.4. Attacks such as the ones to ApplePay,[190] ATM,[191] banks,[192] are facilitated by cleartext, that is, either password stored in clear or cleartext communications.
- **Threat T5.3.1: Broken authentication and access control:** Automated brute force, dictionary, and session management attacks are spread. Several Member States have reported the exploitation of Remote Desktop Protocols (RDPs) for malware infection. Cyber attackers scan specific open ports and then attempt to brute force access to the victims RDP.[38193] For instance, in 2017, up to 90 email accounts of UK Parliament were compromised thanks to a brute force attack and weak passwords. Weak and default password are at the basis of many botnets, such as Mirai IoT malware, which compromised devices by guessing weak passwords[194] to access the management application (GUI)[104][185].
- **Threat T5.3.2: Denial of service:** On one side, malware often targets components and services that result in an application DoS. For instance, Mirai malware targeted the availability of DNS to bring well-known applications down (e.g., Twitter, the Guardian, Netflix, Reddit, CNN).[185] On the other side, as already discussed in Threat T2.3.5 and T5.2.1, expired certificates can result in system outages or open a door to attacks, such as, in 2013, where Microsoft Azure experienced a worldwide outage or, in 2014, tens of thousands of payment terminals in U.S. made unavailable.
- **Threat T5.3.3: Code execution and injection (unsecure APIs):** Malware attacks have been extensively discussed in previous sections. As a summary, ransomware (e.g., WannaCry and NotPetya) attacks moved the malware attack to another level, difficult to challenge by national law enforcement agencies alone.[38] In addition, cyber attackers are turning security defences in weapons. SSL/TLS has been used to deliver malware undetected, to disrupt secured transactions, and to exfiltrate data over encrypted communication channels.[190] For example, Zeus botnet used SSL communication to upgrade the attack after the initial email infection. After the Boston Marathon bombing, a malware distributed through a spam message used SSL to report back to its command and control server.[190] Finally, mobile malware, specifically targeting mobile operating systems and mobile applications, is growing significantly since 2017, in particular mobile ransomware.[195196] Some reports indicate that this malware is active in Africa, Asia and USA, with the exception of mobile ransomware which heavily targets North America.[38] More in detail, Ransomware, spyware, bots, Adware, Potentially Unwanted Applications (PUA), Trojans, and Trojan spyware are exponentially targeting smartphones and IoT devices [3], over which modern applications are installed. PUA is

[184] AWS S3 Bucket Discovery Build your own tools with the secapps Fuzzer https://blog.websecurify.com/2017/10/aws-s3-bucket-discovery.html

[185] I Can’t Believe Mirais: Tracking the Infamous IoT Malware https://securityintelligence.com/posts/i-cant-believe-mirais-tracking-the-infamous-iot-malware-2/

[186] Two years after WannaCry, a million computers remain at risk https://techcrunch.com/2019/05/12/wannacry-two-years-on/?guccounter=1guce$_{r}eferrer_{u}s = aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8guce_{r}eferrer_{c}s = G - KKo6amjJ2OCukY1Fh6 - A$

[187] Common SSL Attacks https://www.venafi.com/education-center/ssl/common-ssl-attacks

[188] The Hearthbleed Bug http://heartbleed.com/

[189] Why SSL/TLS attacks are on the rise https://www.csoonline.com/article/3212965/why-ssl-tls-attacks-are-on-the-rise.html

[190] Wallet-snatch hack: ApplePay ’vulnerable to attack’, claim researchers https://www.theregister.co.uk/2017/07/28/applepay$_{v}uln$/

[191] ATM logic attacks: scenarios, 2018 https://www.ptsecurity.com/ww-en/analytics/atm-vulnerabilities-2018/

[192] How hackers rob banks https://www.ptsecurity.com/ww-en/analytics/banks-attacks-2018/

[193] Panda Security, PandaLabs Annual Report 2017, 2017.

[194] ’Brute force’ cyber attack on Parliament compromised up to 90 email accounts https://www.telegraph.co.uk/news/2017/06/25/brute-force-cyber-attack-parliament-compromised-90-email-accounts/

[195] TrendLabs, 2017 Annual Security Roundup: the paradox of cyber threats, 2018.

[196] Symantec, ‘Facts and figures’, Internet Security Threat Report (ISTR), 2018

the topmost Android malware detected by Quick Heal,[197] where third-party application stores are used to spread malware and exfiltrate private information of the user. Gugi is an example of a banking Trojan exploiting the security policies of Android Marshmallow [3]. GooglePlay has dozen of malicious apps[3]; for instance, Judy, which affected around 36.5 million Android users,[198] was in about 40 applications. According to [3], runtime information gathering (RIG) [105], energy-based [106], remote code execution/injection,[199] [107] hijacking,[201] privilege escalation attacks[108][109] are the most critical targeting Android devices. They are most based on vulnerabilities in (third-party) libraries and over-permissioned applications, libraries, and ad libraries [3].

- **Threat T5.3.4: Insufficient logging and monitoring:** This class of threats is usually a pre-requisite for any large attack and major incident. It virtually exploits insufficient logging and monitoring to go undetected for a while, reducing timely response (191 days on average in 2016).[13]
- **Threat T5.3.5: Untrusted composition:** Attacks related to this threat mainly target single services/applications, trying to identify the weakest link in the composition. They then resemble to attacks described in this section. No recent attacks on the composition flow and orchestrators have been reported, while different assurance solutions (e.g., [110]) have been reported to verify (e.g., certify) the strength of a service composition by verifying the strength of the single component services.
- **Threat T5.4.1: Violation of laws or regulations**
- **Threat T5.5.1: Malicious insider**

Attacks related to User-Centric Security

In the following, the main attacks affecting the User domain are reported.

- **Threat T6.1.1: Mishandling of physical assets:** The problem of mishandling of physical assets is particularly evident with the case of stolen laptops. Laptops are systematically stolen from cars, offices, and public places, as witnessed by cybersecurity surveys like the Verizon DBIR or other studies[111]. More worrisome is the fact that there already is a history of severe data breaches caused by stolen laptops[112], and affecting critical and sensitive data.[202]
- **Threat T6.1.2: Misconfiguration of systems:** Attacks due to system misconfiguration have a long history. Incidents happened for misconfigurations of BGP[113][114], DNS[115], firewalls[116], web applications[117], up to recent AWS S3 buckets[118], and many other systems. Beside the System and Application domains, the User domain is also involved because misconfigurations have often to do with situations leading users to make errors. This scenario should be accounted for and explicitly managed.
- **Threat T6.1.3: Loss of CIA on data assets:** This is a vast threat category, spanning over multiple domains and comprising almost countless attacks. Attacks on CIA regarding the User domain could be found in those cases where the human factor is key for the attack to succeed. For example, cases where a user has misused his/her access privileges[119], the case of fraudulent or mismanaged Certification Authority[120], or employees falling prey of impersonation attacks[121] or frauds, such as cases of so called CEO frauds, where CEOs (or other C-level managers) are either victims[203] or perpetrators of frauds[122].
- **Threat T6.1.4: Legal, reputational, and financial cost:** There are few examples of firms that were fined for a cybersecurity incident. For instance, in 2007, Heartland Payment Systems payed $150 million in fines and legal costs for a breach in which more than 100 million credit and debit card numbers were lost[123][204]. However, for the EU, things seem to have changed after the GDPR, which may impose severe fines, and organizations took notice [124][125]. Cybersecurity incidents causing financial and reputational costs have been analysed, especially by scholars and analysts interested in the economics of cybersecurity[126][127].
- **Threat T6.2.1: Profiling and discriminatory practices:** In 2012, the FTC published a document titled "Protecting Consumer Privacy in an Era of Rapid Change"[205] addressing the data broker sector and specifically those not regulated by the FCRA. Data brokers were categorized in those having an activity: (i) subject to the FCRA; (ii) not subject to FCRA and collecting data for marketing purpose; (iii) not subject to FCRA and collecting data for purposes other than marketing, for instance to detect frauds or locate people. Then, in 2014, a new report titled "Data Brokers - A Call for Transparency and Accountability" was published[206]. To date, it represents one of the most comprehensive analysis of the data broker industry. The characteristics of nine data brokers are described. Their names are unknown for almost everybody (i.e., Acxiom, Corelogic, Datalogix, eBureau, ID Analytics, Intelius, PeekYou, Rapleaf, and Recorded Future), but their activity has involved nearly every US consumer and many others internationally. These companies manage consumers' data - usually bought from other data brokers or from companies directly collecting them from individuals – and produce derived data for satisfying their clients business needs in terms of marketing, risk mitigation, and people search. Citizens are normally unaware and never specifically informed of their

[197] Annual threat report. 2017. Quick Heal. http://dlupdate.quickheal.com/documents/others/Quick$_{H}eal_{A}nnual_{T}hreat_{R}eport_{2}$017.pdf

[198] Jason Murdock. Judy' could be the largest malware campaign ever found on google play. 2017. International Business Times. http://www.ibtimes.co.uk/judy-could-be-largest-malware-campaign-everfound-google-play-store-1623508

[199] Android Developers Blog. Android security bulletin, October. 2017. https://source.android.com/security/bulletin/2017-10-01[200]

[201] Mohit Kumar. 2014. The hacker news. Facebook sdk vulnerability puts millions of smartphone users' accounts at risk. http://thehackernews.com/2014/07/facebook-sdkvulnerability-puts.html

[202] Jessica Davis, Data of 43,000 patients breached after theft of unencrypted laptop. Healthcare IT News, January 2018. https://www.healthcareitnews.com/news/data-43000-patients-breached-after-theft-unencrypted-laptop

[203] Jill McCabe, FBI Warns of Dramatic Increase in Business E-Mail Scams. FBI Phoenix, April 2016. https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-warns-of-dramatic-increase-in-business-e-mail-scams

[204] Danny Yadron, "Companies Wrestle With the Cost of Cybersecurity," Wall Street Journal, https://www.wsj.com/articles/no-headline-available-1393371844

[205] US Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers. March 2012. https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers

[206] US Federal Trade Commission, Data Brokers - A Call for Transparency and Accountability, Washington, DC: US Federal Trade Commission, May 2014, available at: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

personal data being used for these purposes. Data may include bankruptcy information, voting registration, consumer purchase data, web browsing activities, warranty registrations, and other from everyday online and offline activity. Data sources are heterogeneous; from publicly available blogs and social media to commercial sources, for example about the purchasing history of customers or online service registrations. Data updates are commanded by data brokers according to their cost-benefit assessment: The more frequent the update, the higher the classification accuracy and costs. For this reason, some personal data might be inaccurate even for a long time, without the individual able to know about that and about possible consequences of misalignment. Typically, data brokers compile commercial categories and group customers with similar behaviors. Such categories may look fancy to those not accustomed with advertising practices. Example of categories could be: Soccer Moms, Urban Scramble, Rural Everlastings or Thrifty Elders. Bizarre as they may sound, categories like these are useful for targeting quality buyers, as profiled citizens are dubbed by a very active online advertising company[207]. Another data broker activity is to develop models to predict behaviors. In this case, a subset of customers is specifically analysed for its purchase behavior and that knowledge is applied to predict future purchases of other customers with similar characteristics. This may also involve sensitive information like those related to health, pregnancy and medicine consumption. In particular, privacy abuses of health data have been the subject of several journalistic investigations[208][209] and scientific research[128][129], which unveiled some commercial practices that most citizens completely ignore but strongly oppose when informed. For instance, the severity of medical privacy invasion came shockingly to light in 2013 with the Congressional testimony of Pam Dixon of World Privacy Forum[210]. In that occasion, Dixon presented evidences that lists of patients suffering from mental illness to sexual dysfunctions, cancer and HIV/AIDS to name just a few examples were commonly traded. Even more outrageously, lists of rape victims were publicly advertised and sold. Opting out of data broker profiling is often impractical, at least. Since data broker typically do not interact directly with consumers, even those offering clear opt-out procedures are unlikely to be known by consumers willing to exercise their choice. Many data broker instead provide murky opt-out procedures or simply do not care of providing any. In Dixon Congressional testimony, it was mentioned that in a sample of 352 data broker, just 128 provided an opt-out procedure. In some cases, for example when consumers are profiled to calculate a credit score, it is practically impossible to be deleted from a score list. In other situations, the opt-out choice is made difficult to exercise due to clauses such as the request of a motivation to be approved or of a fee. Therefore, opting-out of data broker profiling, when permitted, is likely to be incomplete, does not imply deletion of personal data and does not involve third parties, it may be costly, hard to find and there is no guarantee that it is not just temporary.

- **Threat T6.2.2: Illegal acquisition of information:** Data has always been the target of attacks[211]. Now they are often reported at great length by the press and might represent a major incident for a company, Cambridge Analytica[212] and Equifax [130] are just two of the most noticeable examples. With respect to the User domain, the illegal acquisition of information may have unforeseen consequences on a company's operations. From damaging the brand reputation to costs for litigations and liabilities, the loss of trustworthiness, scapegoating and career damages, and so forth. A data breach is not only a threat for data and data owners, but it might trigger a cascade of consequences on the organization's processes and personnel.
- **Threat T6.3.1: Organized criminal groups' activity:** Attacks perpetrated by organized criminals are almost countless. From petty crimes to large frauds. Europol publishes one of the leading reports providing with plenty of information[38]. In the current issue, one of the key messages is that still criminals mostly target data. Europol, too, insists on the need to counteract criminal groups by considering the big picture and adopting a holistic approach consisting in analysing single vulnerabilities but also the system perspective, technologies and organizational processes, tools and people.
- **Threat T6.3.2: State-sponsored organizations' activity:** Political, geostrategic, and business tensions arose in recent years among several countries worldwide leading to a wave of state-sponsored attacks. It has become common to talk about state-sponsored organizations engaged in hostile activities against organizations in other countries. Stuxnet, often dubiously dubbed as "the first act of cyberwar", was one of the first episodes of clear state-sponsored attack[131]. After that episode, state-sponsored attacks seem to have escalated, becoming common and motivated by vary different reasons [37][132][133][134].
- **Threat T6.3.3: Malicious employees or partners' activity:** As we reminded, it is way too easy to overhype the dangers posed by disloyal insiders and oversell stereotypes like the "disgruntled employee" or the "treacherous sysadmin". On the other side, it is true that cases of cybercrimes made by employees are countless. For example, the US Department of Homeland Security has published a long list of references to insider threats analyses, showing the many ways an employee may become the responsible of a cybercrime[135][213].
- **Threat T6.4.1: Misinformation/disinformation campaigns:** A misinformation or disinformation campaign (the difference laying in the intentionality of the campaign) targeting a company might inflict not negligible damages on brand reputation and trustfulness, which would require public relation efforts to be mitigated. Evidences of this are still murky and opinionated, but at least we can observe that the problem is growing and has already put pressure on some companies.[214][215] With regard

[207] Rubicon Project. The Advertising Automation Cloud, 2016, available at: https://rubiconproject.com/

[208] L. Beckett. Everything We Know About What Data Brokers Know About You, Pro Publica, 2014, available at: https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you

[209] A. Tanner. How Data Brokers Make Money Off Your Medical Records, Scientific American, 2016, available at: http://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/

[210] P. Dixon. Congressional Testimony: What Information Do Data Brokers Have on Consumers?, World Privacy Forum, 2013, available at: https://www.worldprivacyforum.org/2013/12/testimony-what-information-do-data-brokers-have-on-consumers/

[211] Juliana De Groot, The History of Data Breaches. Digital Guardian's Blog, October 2019. https://digitalguardian.com/blog/history-data-breaches

[212] Cadwalladr, C., Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian, 17, 22.

[213] Department of Homeland Security, Insider Threat - Cyber. DHS National Cybersecurity and Communications Integration Center, 2019. https://www.dhs.gov/cisa/insider-threat-cyber

[214] Mike Isaac, Facebook Finds New Disinformation Campaigns and Braces for 2020 Torrent. The New York Times, October 21, 2019. https://www.nytimes.com/2019/10/21/technology/facebook-disinformation-russia-iran.html

[215] Shelly Banjo, Facebook, Twitter and the Digital Disinformation Mess. The Washington Post, October 2, 2019. https://www.washingtonpost.com/business/facebook-twitter-and-the-digital-disinformation-mess/2019/10/01/53334c08-e4b4-11e9-b0a6-3d03721b85ef$_{s}tory.html$

to software tools developed to assists in misinformation campaigns [136], the massive surge of social bots (i.e., software bots employed in social media and mimicking legitimate journalists or just common social media users) is one of the most relevant phenomena and has attracted a great deal of interest and analyses [7][137]. According to some estimates, on Twitter, social bots represent between 5 to 15% of users and are responsible for misinformation campaigns, phishing attacks, election and market manipulation[216] and, in most cases, are organized in social bot networks centrally coordinated, an approach that closely mirrors the commandcontrol scheme of botnets exploited for electronic crime[138][139]. Many research efforts are ongoing with the goal of detecting social bots from legitimate human users, with the subject of social bot detection as one of the most active in the area of social media security [140][141][142][143].

- **Threat T6.4.2: Smear campaigns/market manipulation:** This is still more a theoretical case than a real threat, but nevertheless the growing influence of online media and social networks provide the means for new forms of classical pump-and-dump schemes. Example of politically motivated smear campaign abound[144]. The shift to a business threat is certainly possible in the future[145]. With respect to software tool employed in smear campaigns and market manipulation operations, we forward to the previous discussion regarding social bots, because they represent a general family of software tools and coordination mechanisms largely employed in malicious activity on social media.
- **Threat T6.4.3: Social responsibility/ethics-related incidents:** IT companies accused of unethical behavior[146] and that have suffered for the consequences of having behaved (or the perception of) unethical are not rare in history[147]. Interestingly, cases of modern Internet-based, technology intensive companies that are reported to engage in unethical behavior seem rampant. Sometimes, the bad reputation gained has triggered boycotts by customers. Uber, for example, has been recently often accused of unethical activities and its reputation has clearly suffered for that[148]. The sharing economy, as a whole, has been studied as possibly facilitating unethical activities[149].
- **Threat T6.5.1: Skill shortage/undefined cybersecurity curricula:** No recent attacks have been reported.
- **Threat T6.5.2: Business misalignment/shift of priorities:** Many companies still struggle with deciding the right position in the organigram of the responsible of cybersecurity, being either the CSO (Chief Security Officer) or the CISO (Chief Information Security Officer), or even the more recent CRO (Chief Risk Officer)[217][218]. The organizational weakness of the cybersecurity function in many companies is also one of the reasons for the common shift of priority of cybersecurity, that sees drastic budget reduction as soon as the company is in need of review budgets[150].

References

1. Xia F, Yang LT, Wang L, Vinel A. Internet of things. International journal of communication systems 2012;25(9):1101.
2. Scherer CW, Cho H. A social network contagion theory of risk perception. Risk Analysis: An International Journal 2003;23(2):261–267.
3. Bhat P, Dutta K. A survey on various threats and current state of security in android platform. ACM Computing Surveys (CSUR) 2019;52(1):1–35.
4. Hussain S, Chowdhury O, Mehnaz S, Bertino E. LTEInspector: A systematic approach for adversarial testing of 4G LTE. In: Network and Distributed Systems Security (NDSS) Symposium 2018; 2018. .
5. Shafahi M, Kempers L, Afsarmanesh H. Phishing through social bots on Twitter. In: 2016 IEEE International Conference on Big Data (Big Data) IEEE; 2016. p. 3703–3712.
6. Shao C, Ciampaglia GL, Varol O, Flammini A, Menczer F. The spread of fake news by social bots. arXiv preprint arXiv:170707592 2017;96:104.
7. Shao C, Ciampaglia GL, Varol O, Yang KC, Flammini A, Menczer F. The spread of low-credibility content by social bots. Nature communications 2018;9(1):1–9.
8. Bessi A, Ferrara E. Social bots distort the 2016 US Presidential election online discussion. First Monday 2016;21(11-7).
9. Brachten F, Mirbabaie M, Stieglitz S, Berger O, Bludau S, Schrickel K. Threat or opportunity?-examining social bots in social media crisis communication. arXiv preprint arXiv:181009159 2018;.
10. Nowak A, Lukowicz P, Horodecki P. Assessing Artificial Intelligence for Humanity: Will AI be the Our Biggest Ever Advance? or the Biggest Threat [Opinion]. IEEE Technology and Society Magazine 2018;37(4):26–34.
11. Duan Y, Edwards JS, Dwivedi YK. Artificial intelligence for decision making in the era of Big Data–evolution, challenges and research agenda. International Journal of Information Management 2019;48:63–71.
12. Helbing D, Frey BS, Gigerenzer G, Hafen E, Hagner M, Hofstetter Y, et al. Will democracy survive big data and artificial intelligence? In: Towards digital enlightenment Springer; 2019.p. 73–98.
13. Flaspöler E, Hauke A, Pappachan P, Reinert D, Bleyer T, Henke N, et al. The human machine interface as an emerging risk. EU-OSHA (European Agency for Safety and Health at Work) Luxemburgo 2009;.
14. Ciborra C. The labyrinths of information: Challenging the wisdom of systems: Challenging the wisdom of systems. OUP Oxford; 2002.
15. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care 2017;25(1):1–10.
16. Sametinger J, Rozenblit J, Lysecky R, Ott P. Security challenges for medical devices. Communications of the ACM 2015;58(4):74–82.
17. Humayed A, Lin J, Li F, Luo B. Cyber-physical systems security—A survey. IEEE Internet of Things Journal 2017;4(6):1802–1831.

[216] Cloudflare Inc. What is a Social Media Bot?, Cloudflare, 2020., available at: https://www.cloudflare.com/learning/bots/what-is-a-social-media-bot/

[217] Westby JR. Governance of enterprise security: CyLab 2012 report. Pittsburgh, PA. 2012. http://www.fbiic.gov/public/2010/jul/cylab-governance-2010.pdf

[218] Data Security Council of India. "Developing a Framework to Improve Critical Infrastructure Cybersecurity." https://www.nist.gov/document/040813dscipdf

18. Ardagna CA, Asal R, Damiani E, Vu QH. From security to assurance in the cloud: A survey. ACM Computing Surveys (CSUR) 2015;48(1):1–50.
19. Armbrust M, Fox A, Griffith R, Joseph AD, Katz RH, Konwinski A, et al. Above the Clouds: A Berkeley View of Cloud Computing 2009;.
20. Mell P, Grance T, et al. The NIST definition of cloud computing 2011;.
21. Chandna S, Singh R, Akhtar F. Data scavenging threat in cloud computing. International Journal of Advances In Computer Science and Cloud Computing 2014;2(2):106–111.
22. Safa NS, Von Solms R, Futcher L. Human aspects of information security in organisations. Computer Fraud & Security 2016;2016(2):15–18.
23. Aldawood H, Skinner G. Challenges of implementing training and awareness programs targeting cyber security social engineering. In: 2019 Cybersecurity and Cyberforensics Conference (CCC) IEEE; 2019. p. 111–117.
24. Courtney M. States of cyber-warfare. Engineering & Technology 2017;12(3):22–25.
25. Garg A, Curtis J, Halper H. Quantifying the financial impact of IT security breaches. Information Management & Computer Security 2003;.
26. Gal-Or E, Ghose A. The economic consequences of sharing security information. In: Economics of information security Springer; 2004.p. 95–104.
27. Chai S, Kim M, Rao HR. Firms' information security investment decisions: Stock market evidence of investors' behavior. Decision Support Systems 2011;50(4):651–661.
28. Brzoska M, Bossong R, van Um E. Security Economics in the European Context: Implications of the EUSECON Project. Economics of Security Working Paper; 2011.
29. Moore T. The economics of cybersecurity: Principles and policy options. International Journal of Critical Infrastructure Protection 2010;3(3-4):103–117.
30. Holz T, Pohlmann N, Bodden E, Smith M, Hoffmann J, Human-Centered Systems Security: IT-Sicherheit von Menschen für Menschen. Verfügbar unter: https://www. ptj. de/lw_resource/datapool/_items/item_7794 . . . ; 2016.
31. Corradini I, Nardelli E. Building organizational risk culture in cyber security: the role of human factors. In: International Conference on Applied Human Factors and Ergonomics Springer; 2018. p. 193–202.
32. Vieane A, Funke G, Gutzwiller R, Mancuso V, Sawyer B, Wickens C. Addressing human factors gaps in cyber defense. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 60 SAGE Publications Sage CA: Los Angeles, CA; 2016. p. 770–773.
33. Rashid A, Danezis G, Chivers H, Lupu E, Martin A, Lewis M, et al. Scoping the cyber security body of knowledge. IEEE Security & Privacy 2018;16(3):96–102.
34. Hughes R. NATO and Cyber Defence. Atlantisch Perspectief 2009;33.
35. Yoo CS. Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures. Cyberwar: Law and Ethics for Virtual Conflicts (Jens David Ohlin, Kevin Govern, Claire Finkelstein, eds, 2015) 2015;p. 15–3.
36. Everett C. The lucrative world of cyber-espionage. Computer Fraud & Security 2009;2009(7):5–7.
37. Watkins B. The impact of cyber attacks on the private sector. Briefing Paper, Association for International Affair 2014;12.
38. Bressler MS, Bressler L. Protecting your company's intellectual property assets from cyber-espionage. Journal of Legal, Ethical and Regulatory Issues 2015;18(1):21.
39. Gordon LA, Loeb MP, Zhou L. The impact of information security breaches: Has there been a downward shift in costs? Journal of Computer Security 2011;19(1):33–56.
40. Richardson V, Watson MW, Smith RE. Much Ado about Nothing: The (Lack of) Economic Impact of Data Privacy Breaches. Journal of Information Systems 2019;.
41. He Z, Frost T, Pinsker R. The Impact of Reported Cybersecurity Breaches on Firm Innovation. Journal of Information Systems 2019;.
42. Rosati P, Cummins M, Deeney P, Gogolin F, van der Werff L, Lynn T. The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. International Review of Financial Analysis 2017;49:146–154.
43. Bakir V. Media and risk: old and new research directions. Journal of risk research 2010;13(1):5–18.
44. Chung IJ. Social amplification of risk in the Internet environment. Risk Analysis: An International Journal 2011;31(12):1883–1896.
45. Gharibi W, Shaabi M. Cyber threats in social networking websites. arXiv preprint arXiv:12022420 2012;.
46. Toch E, Bettini C, Shmueli E, Radaelli L, Lanzi A, Riboni D, et al. The privacy implications of cyber security systems: A technological survey. ACM Computing Surveys (CSUR) 2018;51(2):1–27.
47. Ye H, Cheng X, Yuan M, Xu L, Gao J, Cheng C. A survey of security and privacy in big data. In: 2016 16th international symposium on communications and information technologies (iscit) IEEE; 2016. p. 268–272.
48. Choi SJ, Johnson ME. Do Hospital Data Breaches Reduce Patient Care Quality? arXiv preprint arXiv:190402058 2019;.
49. Jiang JX, Bai G. Evaluation of causes of protected health information breaches. JAMA internal medicine 2019;179(2):265–267.
50. Butun I, Österberg P, Song H. Security of the internet of things: vulnerabilities, attacks and countermeasures. IEEE Communications Surveys & Tutorials 2019;.
51. Park M, Oh H, Lee K. Security risk measurement for information leakage in IoT-based smart homes from a situational awareness perspective. Sensors 2019;19(9):2148.
52. Maiti A, Jadliwala M, He J, Bilogrevic I. Side-channel inference attacks on mobile keypads using smartwatches. IEEE Transactions on Mobile Computing 2018;17(9):2180–2194.
53. Sarkisyan A, Debbiny R, Nahapetian A. WristSnoop: Smartphone PINs prediction using smartwatch motion sensors. In: 2015 IEEE international workshop on information forensics and security (WIFS) IEEE; 2015. p. 1–6.
54. Chakraborty S, Ouyang W, Srivastava M. LightSpy: Optical eavesdropping on displays using light sensors on mobile devices. In: 2017 IEEE International Conference on Big Data (Big Data) IEEE; 2017. p. 2980–2989.
55. Shaik A, Borgaonkar R, Asokan N, Niemi V, Seifert JP. Practical attacks against privacy and availability in 4G/LTE mobile communication systems. arXiv preprint arXiv:151007563 2015;.

56. Rocha F, Gross T, Van Moorsel A. Defense-in-depth against malicious insiders in the cloud. In: 2013 IEEE International Conference on Cloud Engineering (IC2E) IEEE; 2013. p. 88–97.
57. Zhang Y, Juels A, Oprea A, Reiter MK. Homealone: Co-residency detection in the cloud via side-channel analysis. In: 2011 IEEE symposium on security and privacy IEEE; 2011. p. 313–328.
58. Zhang Y, Juels A, Reiter MK, Ristenpart T. Cross-VM side channels and their use to extract private keys. In: Proceedings of the 2012 ACM conference on Computer and communications security; 2012. p. 305–316.
59. Weiß M, Heinz B, Stumpf F. A cache timing attack on AES in virtualization environments. In: International Conference on Financial Cryptography and Data Security Springer; 2012. p. 314–328.
60. Irazoqui G, Inci MS, Eisenbarth T, Sunar B. Fine grain cross-vm attacks on xen and vmware. In: 2014 IEEE Fourth International Conference on Big Data and Cloud Computing IEEE; 2014. p. 737–744.
61. Yarom Y, Falkner K. FLUSH+ RELOAD: a high resolution, low noise, L3 cache side-channel attack. In: 23rd {USENIX} Security Symposium ({USENIX} Security 14); 2014. p. 719–732.
62. Inci MS, Gülmezoglu B, Apecechea GI, Eisenbarth T, Sunar B. Seriously, get off my cloud! Cross-VM RSA Key Recovery in a Public Cloud. IACR Cryptology ePrint Archive 2015;2015(1-15).
63. Maurice C, Neumann C, Heen O, Francillon A. C5: cross-cores cache covert channel. In: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment Springer; 2015. p. 46–64.
64. Xiao J, Xu Z, Huang H, Wang H. A covert channel construction in a virtualized environment. In: Proceedings of the 2012 ACM conference on Computer and communications security; 2012. p. 1040–1042.
65. Pessl P, Gruss D, Maurice C, Schwarz M, Mangard S. {DRAMA}: Exploiting {DRAM} addressing for cross-cpu attacks. In: 25th {USENIX} Security Symposium ({USENIX} Security 16); 2016. p. 565–581.
66. Albelooshi B, Salah K, Martin T, Damiani E. Experimental proof: Data remanence in cloud VMs. In: 2015 IEEE 8th International Conference on Cloud Computing IEEE; 2015. p. 1017–1020.
67. Shafieian S, Zulkernine M, Haque A. Attacks in public clouds: Can they hinder the rise of the cloud? In: Cloud Computing Springer; 2014.p. 3–22.
68. Shi L, Wu Y, Xia Y, Dautenhahn N, Chen H, Zang B, et al. Deconstructing Xen. In: NDSS; 2017. .
69. Yeh JR, Hsiao HC, Pang AC. Migrant attack: A multi-resource dos attack on cloud virtual machine migration schemes. In: 2016 11th Asia Joint Conference on Information Security (AsiaJCIS) IEEE; 2016. p. 92–99.
70. King ST, Chen PM. SubVirt: Implementing malware with virtual machines. In: 2006 IEEE Symposium on Security and Privacy (S&P'06) IEEE; 2006. p. 14–pp.
71. Desnos A, Filiol É, Lefou I. Detecting (and creating!) a HVM rootkit (aka BluePill-like). Journal in computer virology 2011;7(1):23–49.
72. Jasti A, Shah P, Nagaraj R, Pendse R. Security in multi-tenancy cloud. In: 44th Annual 2010 IEEE International Carnahan Conference on Security Technology IEEE; 2010. p. 35–41.
73. Checkoway S, Shacham H. Iago attacks: why the system call API is a bad untrusted RPC interface. ACM SIGARCH Computer Architecture News 2013;41(1):253–264.
74. Kandias M, Virvilis N, Gritzalis D. The insider threat in cloud computing. In: International Workshop on Critical Information Infrastructures Security Springer; 2011. p. 93–103.
75. Rocha F, Correia M. Lucy in the sky without diamonds: Stealing confidential data in the cloud. In: 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W) IEEE; 2011. p. 129–134.
76. Li C, Raghunathan A, Jha NK. Secure virtual machine execution under an untrusted management OS. In: 2010 IEEE 3rd International Conference on Cloud Computing IEEE; 2010. p. 172–179.
77. Damiani E. Toward big data risk analysis. In: 2015 IEEE International Conference on Big Data (Big Data) IEEE; 2015. p. 1905–1909.
78. Aditham S, Ranganathan N. A novel framework for mitigating insider attacks in big data systems. In: 2015 IEEE International Conference on Big Data (Big Data) IEEE; 2015. p. 1876–1885.
79. Meng H, Thing VL, Cheng Y, Dai Z, Zhang L. A survey of Android exploits in the wild. Computers & Security 2018;76:71–91.
80. Zhao M, An B, Yu Y, Liu S, Pan SJ. Data poisoning attacks on multi-task relationship learning. In: Thirty-Second AAAI Conference on Artificial Intelligence; 2018. .
81. Shi Y, Erpek T, Sagduyu YE, Li JH. Spectrum data poisoning with adversarial deep learning. In: MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM) IEEE; 2018. p. 407–412.
82. Li B, Wang Y, Singh A, Vorobeychik Y. Data poisoning attacks on factorization-based collaborative filtering. In: Advances in neural information processing systems; 2016. p. 1885–1893.
83. Zügner D, Akbarnejad A, Günnemann S. Adversarial attacks on neural networks for graph data. In: Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining; 2018. p. 2847–2856.
84. Somorovsky J, Heiderich M, Jensen M, Schwenk J, Gruschka N, Lo Iacono L. All your clouds are belong to us: security analysis of cloud management interfaces. In: Proceedings of the 3rd ACM workshop on Cloud computing security workshop; 2011. p. 3–14.
85. Huang J, Nicol DM, Campbell RH. Denial-of-service threat to Hadoop/YARN clusters with multi-tenancy. In: 2014 IEEE International Congress on Big Data IEEE; 2014. p. 48–55.
86. Osawaru ER, AH RA. A Highlight of Security Challenges in Big Data. Int J Inform Syst Eng 2014;2(1):2289–2265.
87. Lipp M, Schwarz M, Gruss D, Prescher T, Haas W, Fogh A, et al. Meltdown: Reading kernel memory from user space. In: 27th {USENIX} Security Symposium ({USENIX} Security 18); 2018. p. 973–990.
88. Kocher P, Horn J, Fogh A, Genkin D, Gruss D, Haas W, et al. Spectre attacks: Exploiting speculative execution. In: 2019 IEEE Symposium on Security and Privacy (SP) IEEE; 2019. p. 1–19.
89. De Capitani Di Vimercati S, Foresti S, Livraga G, Samarati P. Data privacy: definitions and techniques. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 2012;20(06):793–817.
90. Orduña P, Almeida A, Aguilera U, Laiseca X, López-de Ipiña D, Goiri AG. Identifying security issues in the semantic web: Injection attacks in the semantic query languages. Actas de las VI Jornadas Cientifico-Tecnicas en Servicios Web y SOA

2010;51:4529–4542.

91. Ben Mustapha N, Zghal HB, Aufaure MA, Ben Ghezala H. Enhancing semantic search using case-based modular ontology. In: Proceedings of the 2010 ACM symposium on applied computing; 2010. p. 1438–1439.
92. Collins M. Common sense guide to mitigating insider threats. CARNEGIE-MELLON UNIV PITTSBURGH PA PITTSBURGH United States; 2016.
93. Homoliak I, Toffalini F, Guarnizo J, Elovici Y, Ochoa M. Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. ACM Computing Surveys (CSUR) 2019;52(2):1–40.
94. Randazzo MR, Keeney M, Kowalski E, Cappelli D, Moore A. Insider threat study: Illicit cyber activity in the banking and finance sector. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST; 2005.
95. Kowalski E, Conway T, Keverline S, Williams M, Cappelli D, Willke B, et al. Insider threat study: Illicit cyber activity in the government sector. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST; 2008.
96. Fischer LF. Characterizing information systems insider offenders. In: Proceedings of the 45th Annual Conference of the International Military Testing Association Citeseer; 2003. p. 03–06.
97. Shaw E, Ruby KG, Post JM. The insider threat to information systems. Security Awareness Bulletin 1998;2(98):1–10.
98. Keeney M, Kowalski E, Cappelli D, Moore A, Shimeall T, Rogers S. Insider threat study: Computer system sabotage in critical infrastructure sectors. National Threat Assessment Ctr Washington Dc; 2005.
99. Magklaras GB, Furnell S. Insider threat prediction tool: Evaluating the probability of IT misuse. Computers & Security 2001;21(1):62–73.
100. Jabbour G, Menascé D. Stopping the insider threat: The case for implementing autonomic defense mechanisms in computing systems. In: Proceedings of the International Conference of Information Security and Privacy; 2009. .
101. Bishop M, Engle S, Peisert S, Whalen S, Gates C. Case studies of an insider framework. In: 2009 42nd Hawaii International Conference on System Sciences IEEE; 2009. p. 1–10.
102. Probst CW, Hunker J. The risk of risk analysis and its relation to the economics of insider threats. In: Economics of information security and privacy Springer; 2010.p. 279–299.
103. Predd J, Pfleeger SL, Hunker J, Bulford C. Insiders behaving badly. IEEE Security & Privacy 2008;6(4):66–70.
104. Anisetti M, Asal R, Ardagna CA, Comi L, Damiani E, Gaudenzi F. A Knowledge-Based IoT Security Checker. In: European Conference on Parallel Processing Springer; 2018. p. 299–311.
105. Zhang N, Yuan K, Naveed M, Zhou X, Wang X. Leave me alone: App-level protection against runtime information gathering on android. In: 2015 IEEE Symposium on Security and Privacy IEEE; 2015. p. 915–930.
106. Fiore U, Palmieri F, Castiglione A, Loia V, De Santis A. Multimedia-based battery drain attacks for android devices. In: 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC) IEEE; 2014. p. 145–150.
107. Poeplau S, Fratantonio Y, Bianchi A, Kruegel C, Vigna G. Execute this! analyzing unsafe and malicious dynamic code loading in android applications. In: NDSS, vol. 14; 2014. p. 23–26.
108. Hardy N. The Confused Deputy: (or why capabilities might have been invented). ACM SIGOPS Operating Systems Review 1988;22(4):36–38.
109. Schlegel R, Zhang K, Zhou Xy, Intwala M, Kapadia A, Wang X. Soundcomber: A Stealthy and Context-Aware Sound Trojan for Smartphones. In: NDSS, vol. 11; 2011. p. 17–33.
110. Anisetti M, Ardagna C, Damiani E, Polegri G. Test-based security certification of composite services. ACM Transactions on the Web (TWEB) 2018;13(1):1–43.
111. Johnson SD, Bowers KJ, Gamman L, Mamerow L, Warne A. Theft of Customers' Personal Property in Cafés and Bars. Problem-Oriented Guides for Police 2010;60.
112. Wakeling SG, Hannay P, Baig Z. A review of data breaches and losses that occurred from laptops that were stolen or otherwise misplaced in 2015 and 2016 2017;.
113. Mahajan R, Wetherall D, Anderson T. Understanding BGP misconfiguration. ACM SIGCOMM Computer Communication Review 2002;32(4):3–16.
114. Nordström O, Dovrolis C. Beware of BGP attacks. ACM SIGCOMM Computer Communication Review 2004;34(2):1–8.
115. Pappas V, Wessels D, Massey D, Lu S, Terzis A, Zhang L. Impact of configuration errors on DNS robustness. IEEE Journal on Selected Areas in Communications 2009;27(3):275–290.
116. Cuppens F, Cuppens-Boulahia N, Garcia-Alfaro J. Detection and removal of firewall misconfiguration. In: Proceedings of the 2005 IASTED International Conference on Communication, Network and Information Security, vol. 1; 2005. p. 154–162.
117. Eshete B, Villafiorita A, Weldemariam K. Early detection of security misconfiguration vulnerabilities in web applications. In: 2011 Sixth International Conference on Availability, Reliability and Security IEEE; 2011. p. 169–174.
118. Continella A, Polino M, Pogliani M, Zanero S. There's a Hole in that Bucket! A Large-scale Analysis of Misconfigured S3 Buckets. In: Proceedings of the 34th Annual Computer Security Applications Conference; 2018. p. 702–711.
119. Schultz EE. A framework for understanding and predicting insider attacks. Computers & Security 2002;21(6):526–531.
120. Turner P, Polk W, Barker E. Preparing for and Responding to Certification Authority Compromise and Fraudulent Certificate Issuance. National Institute of Standards and Technology; 2012.
121. Danev B, Luecken H, Capkun S, El Defrawy K. Attacks on physical-layer identification. In: Proceedings of the third ACM conference on Wireless network security; 2010. p. 89–98.
122. Khanna V, Kim EH, Lu Y. CEO connectedness and corporate fraud. The Journal of Finance 2015;70(3):1203–1252.
123. Etzioni A. The private sector: A reluctant partner in cybersecurity. Geo J Int'l Aff 2014;15:69.
124. Tobin P, McKeever M, Blackledge J, Whittington M, Duncan B. UK Financial Institutions Stand to Lose Billions in GDPR Fines: How can They Mitigate This? In: The British Accounting and Finance Association Scottish Area Group Conference, BAFA, Ed., Aberd; 2017. .
125. Voigt P, von dem Bussche A. Enforcement and Fines Under the GDPR. In: The EU General Data Protection Regulation (GDPR) Springer; 2017.p. 201–217.
126. Lesk M. Cybersecurity and economics. IEEE Security & Privacy 2011;9(6):76–79.
127. Cordes JJ. An overview of the economics of cybersecurity and cybersecurity policy. CSPRI Report 2011;p. 1–18.

128. Kaplan B. Selling health data: de-identification, privacy, and speech. Cambridge Quarterly of Healthcare Ethics 2015;24(3):256–271.
129. Huesch M, Ong M, Richman BD. Could data broker information threaten physician prescribing and professional behavior? CESR-Schaeffer Working Paper 2015;(2015-009).
130. Berghel H. Equifax and the latest round of identity theft roulette. Computer 2017;50(12):72–76.
131. Langner R. Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy 2011;9(3):49–51.
132. Bronk C, Tikk-Ringas E. The cyber attack on Saudi Aramco. Survival 2013;55(2):81–96.
133. Joubert V, Five years after Estonia's cyberattacks: Lessons learned for NATO? Research Paper no. 76. Rome, Italy: Research Division, NATO Defense College; 2012.
134. Brenner JF. Eyes wide shut: The growing threat of cyber attacks on industrial control systems. Bulletin of the atomic scientists 2013;69(5):15–20.
135. Silowash GJ, Cappelli DM, Moore AP, Trzeciak RF, Shimeall T, Flynn L. Common sense guide to mitigating insider threats 2012;.
136. Wang P, Angarita R, Renna I. Is this the era of misinformation yet: combining social bots and fake news to deceive the masses. In: Companion Proceedings of the The Web Conference 2018; 2018. p. 1557–1561.
137. Ferrara E, Varol O, Davis C, Menczer F, Flammini A. The rise of social bots. Communications of the ACM 2016;59(7):96–104.
138. Boshmaf Y, Muslukhov I, Beznosov K, Ripeanu M. The socialbot network: when bots socialize for fame and money. In: Proceedings of the 27th annual computer security applications conference; 2011. p. 93–102.
139. Shao C, Hui PM, Wang L, Jiang X, Flammini A, Menczer F, et al. Anatomy of an online misinformation network. PloS one 2018;13(4):e0196087.
140. Davis CA, Varol O, Ferrara E, Flammini A, Menczer F. Botornot: A system to evaluate social bots. In: Proceedings of the 25th international conference companion on world wide web; 2016. p. 273–274.
141. Cai C, Li L, Zengi D. Behavior enhanced deep bot detection in social media. In: 2017 IEEE International Conference on Intelligence and Security Informatics (ISI) IEEE; 2017. p. 128–130.
142. Kudugunta S, Ferrara E. Deep neural networks for bot detection. Information Sciences 2018;467:312–322.
143. Cresci S, Petrocchi M, Spognardi A, Tognazzi S. Better safe than sorry: an adversarial approach to improve social bot detection. In: Proceedings of the 10th ACM Conference on Web Science; 2019. p. 47–56.
144. Sandıkcı Ö, Ekici A. Politically motivated brand rejection. Journal of Business Research 2009;62(2):208–217.
145. Angel JJ, McCabe DM. The business ethics of short selling and naked short selling. Journal of Business Ethics 2009;85(1):239–249.
146. McCormick DW, Spee JC. IBM and Germany 1922–1941. Organization Management Journal 2008;5(4):214–223.
147. Rao SM, Hamilton JB. The effect of published reports of unethical conduct on stock prices. Journal of Business Ethics 1996;15(12):1321–1330.
148. Chee FM. An Uber ethical dilemma: examining the social issues at stake. Journal of Information, Communication and Ethics in Society 2018;.
149. Ahsan M. Entrepreneurship and ethics in the sharing economy: A critical perspective. Journal of Business Ethics 2018;p. 1–15.
150. Srinidhi B, Yan J, Tayi GK. Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. Decision Support Systems 2015;75:49–62.