Security Threat Landscape

Authors:

Marco Anisetti, ***Università degli studi di Milano***

Claudio Ardagna, ***Università degli studi di Milano***

Marco Cremonini, ***Università degli studi di Milano***

Ernesto Damiani, ***Università degli studi di Milano***

Jadran Sessa, ***Università degli studi di Milano***

Luciana Costa, ***Telecom Italia***

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 the transportation of data 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 below follows well-known standards in the field from the 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 newer 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 base 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 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 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 can be considered as an asset. 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 virus propagation and the related vulnerability is that the anti-virus program is not blocking it, that is, virus patterns are not updated or incomplete (issues of confidentiality, integrity, and availability).
- EXAMPLE 3. The threat can be unauthorized access. The vulnerability is the access control scheme that is not working (loss in 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 (potential loss of availability).
- EXAMPLE 5. The threat can be given by the configuration errors made by the system administrator. The vulnerability is the malfunctioning of a system or diminished security protection (issues in confidentiality, integrity. and availability).

In the following of this section, for each of the 6 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

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

- TG1.1: Unintentional damage/loss of information or IT assets
  - T1.1.1: Information leakage/sharing due to human errors
  - T1.1.2: Inadequate design and planning or incorrect adaptation
- TG1.2: Interception and unauthorized acquisition
  - T1.2.1: Interception of information
  - T1.2.2: Unauthorized acquisition of information
- TG1.3: Intentional Physical Damage
  - T1.3.1: Device modification
  - T1.3.2: Extraction of private information
- TG1.4: Nefarious activity/abuse
  - 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
  - T1.5.1: Violation of laws or regulations
- TG1.6: Organizational threats
  - T1.6.1: Skill shortage

Network-Centric Security

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

- TG2.1: Unintentional damage/loss of information or IT assets
  - T2.1.1: Erroneous use or administration of devices and systems
- TG2.2: Interception and unauthorized acquisition
  - 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
  - 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: Organizational (failure malfunction)
  - T2.4.1: Failures of devices or systems
  - T2.4.2: Supply chain
  - T2.4.3: Software bug

System-Centric Security

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

- TG3.1: Unintentional damage/loss of information or IT assets
  - T3.1.1: Information leakage/sharing due to human errors
  - T3.1.2: Inadequate design and planning or incorrect adaptation
- TG3.2: Interception and unauthorized acquisition
  - T3.2.1: Interception of information
  - T3.2.2: Unauthorized acquisition of information (data breach)
- TG3.3: Poisoning
  - T3.3.1: Configuration poisoning
  - T3.3.2: Business process poisoning
- TG3.4: Nefarious activity/abuse
  - 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
  - T3.5.1: Violation of laws or regulations
- TG3.6: Organizational threats
  - T3.6.1: Skill shortage
  - T3.6.2: Malicious insider

Data-Centric Security

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

- TG4.1: Unintentional damage/loss of information or IT assets
  - T4.1.1: Information leakage/sharing due to human errors
  - T4.1.2: Inadequate design and planning or incorrect adaptation
- TG4.2: Interception and unauthorized acquisition
  - T4.2.1: Interception of information
  - T4.2.2: Unauthorized acquisition of information (data breach)
- TG4.3: Poisoning
  - T4.3.1: Data poisoning
  - T4.3.2: Model poisoning
- TG4.4: Nefarious activity/abuse
  - 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)
- TG5: Legal
  - T4.5.1: Violation of laws or regulations
- TG6: Organizational threats
  - T4.6.1: Skill shortage
  - T4.6.2: Malicious Insider

Application-Centric Security

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

- TG5.1: Unintentional damage
  - T5.1.1: Security misconfiguration
- TG5.2: Interception and unauthorized acquisition
  - T5.2.1: Interception of information
  - T5.2.2: Sensitive data exposure
- TG5.3: Nefarious activity/abuse
  - 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
  - T5.4.1: Violation of laws or regulations
- TG5.5: Organizational threats
  - T5.5.1: Malicious Insider

User-Centric Security

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

- TG6.1: 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
  - T6.2.1: Profiling and discriminatory practices
  - T6.2.2: Illegal acquisition of information
- TG6.3: Cybercrime
  - 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
  - T6.4.1: Misinformation/disinformation campaigns
  - T6.4.2: Smearing campaigns/market manipulation
  - T6.4.3: Social responsibility/ethics-related incidents
- TG6.5: Organizational threats
  - T6.5.1: Skill shortage/undefined cybersecurity curricula
  - T6.5.2: Business misalignment/shift of priorities

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.

Cybersecurity Top Findings & Key Takeaways

---

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

[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_download/file