Concordia Workshop – CS Consultant

Learning Objectives - Threats

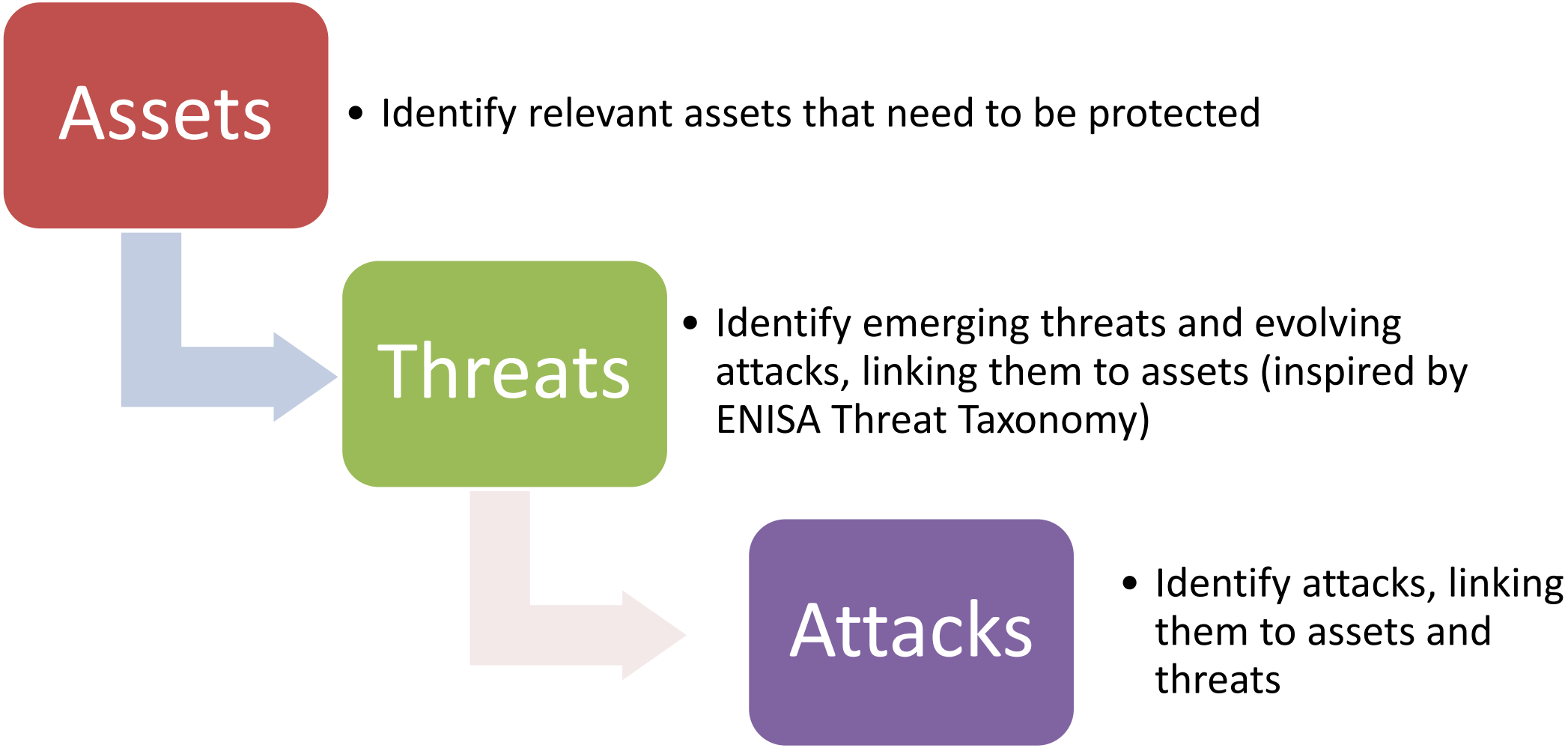
Marco Anisetti, Università degli Studi di Milano

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830927.

Cybersecurity threat analysis

- Overview of emerging threats and evolving attacks based on existing reports/documents (e.g., ENISA threat report)
- Evaluate the **new trends in cybersecurity from a technical perspective**
  - provides an overview of the current state of the art on threats and cybersecurity in the domains of interest of CONCORDIA
- **Identify future and emerging threats** in six domains of interest: (i) network-centric, (ii) system-centric, (iii) application-centric, (iv) data-centric, (v) IoT/device-centric, (vi) user-centric security

Methodology



Data-Centric Security: Threats

Threat Groups	Threats
TG1 – Unintentional damage / loss of information or IT assets	*Threat T1: Information leakage/sharing due to human errors* *Threat T2: Inadequate design and planning or incorrect adaptation*
TG2 – Interception and unauthorised acquisition	*Threat T3: Interception of information* *Threat T4: Unauthorised acquisition of information (data breach)*
TG3 – Poisoning	*Threat T5: Data Poisoning* *Threat T6: Model Poisoning*
TG4 – Nefarious Activity/Abuse	*Threat T7: Identity fraud* *Threat T8: Denial of service* *Threat T9: Malicious code / software / activity* *Threat T10: Generation and use of rogue certificates* *Threat T11: Misuse of assurance tools* *Threat T12: Failures of business process* *Threat T13: Code Execution and Injection (unsecure APIs)*
TG5 – Legal	*Threat T14: Violation of laws or regulations / Breach of legislation / Abuse of personal data*
TG6 – Organisational threats	*Threat T15: Skill shortage* *Threat T16: Malicious Insider*

Data-Centric Security: Current Trends

- **Data breaches and leaks are increasing**
- **Traditional attacks** like phishing and DDoS **are reviving a new boost** and mainly target the confidentiality, integrity, and availability of data
- **Human errors**, as well as **glitches in system configuration**, are still at the forefront of the issues and **facilitate attacks**
  - Lack of skills and competences
  - Increase in system and platform complexity
- **Target phishing and malwares are spreading**
  - Phishing attacks target rich individuals, people with access to financial accounts or sensitive business data or even public authorities that handle PII related data.
  - Malwares target data and in particular wipe, modify, access data with no authorization (30% of all data breaches incidents).

Data-Centric Security: Current Trends

- **EU General Data Protection Regulation (GDPR)** changed the fundamentals of data protection worldwide
  - **New legal requirements** of reporting data breaches
  - **Data breach or leakage can become a new weapon in the cyber criminal hands** (extortion attacks with the threat of GDPR penalties deriving from data disclosure).
- New threats and attacks
  - **Impair algorithm and infrastructure behavior** at the basis of artificial intelligence and machine learning become new targets
  - **Data poisoning** as a huge driver towards more complex attacks
  - **Model poisoning** to fake the learning algorithm in considering a malicious behavior as a normal one

Application-Centric Security: Threats

Threat Groups	Threats
TG1 – Unintentional damage / loss of information or IT assets	*Threat T1: Security Misconfiguration*
TG2 – Interception and unauthorised acquisition	*Threat T2: Interception of information* *Threat T3: Sensitive data exposure*
TG3 – Nefarious Activity/Abuse	*Threat T4: Broken Authentication and Access Control* *Threat T5: Denial of service* *Threat T6: Code Execution and Injection (unsecure APIs)* *Threat T7: Insufficient logging and monitoring* *Threat T8: Untrusted composition*
TG4 – Legal	*Threat T9: Violation of laws or regulations / Breach of legislation / Abuse of personal data*
TG5 – Organisational threats	*Threat T10: Malicious Insider*

Application-Centric Security: Current Trends

- As applications are spreading at all layers of an 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
  - Mobile malware is growing exponentially since 2017 (e.g., mobile banking)
  - DDoS are evolving targeting mobile devices and sensors, and mainly battery consumption
- 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

Application-Centric Security: Current Trends

- **Single and not-expert users are directly involved in complex business processes**
  - Configuration errors are therefore increasing as never seen before
    - E.g., 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
- **Micro-service architecture** has increased the revenue for enterprise and supported new businesses, while **neglecting non-functional properties** such as security and privacy

System-Centric Security: Threats

Threat Groups	Threats
TG1 – Unintentional damage / loss of information or IT assets	*Threat T1: Information leakage/sharing due to human errors* *Threat T2: Inadequate design and planning or incorrect adaptation*
TG2 – Interception and unauthorised acquisition	*Threat T3: Interception of information* *Threat T4: Unauthorised acquisition of information (data breach)*
TG3 – Poisoning	*Threat T5: Configuration Poisoning* *Threat T6: Business process Poisoning*
TG4 – Nefarious Activity/Abuse	*Threat T7: Identity fraud* *Threat T8: Denial of service* *Threat T9: Malicious code/software/activity* *Threat T10: Generation and use of rogue certificates* *Threat T11: Misuse of assurance tools* *Threat T12: Failures of business process* *Threat T13: Code execution and injection (unsecure APIs)*
TG5 – Organisational threats	*Threat T14: Skill shortage* *Threat T15: Malicious Insider*

System-Centric Security: Current Trends

- Current systems are based on a **number of software layers** and in most of the cases including virtualization layer
  - The security of multi-layer systems is the security of the weakest layer
  - Increasing sharing level and multitenancy exacerbate the impact of most of the threats
  - They inherit and make the weaknesses of traditional systems worse
- **Misconfigurations** and inadequate controls will become increasingly problematic in cloud environments, as well as **weaknesses on authentication and lack-of-control and visibility**
- Similarly, emerging threats are **Businness Process Compromise in cloud**, which are linked to the advanced AI capabilities of an attacker to improve BPC-based attacks

Network-Centric Security: Threats

Threat Groups	Threats
TG1 – Unintentional damage / loss of information or IT assets	*Threat T1: Erroneous use or administration of devices and systems*
TG2 – Interception and unauthorised acquisition	*Threat T2: Signaling traffic interception* *Threat T3: Data session hijacking* *Threat T4: Traffic eavesdropping* *Threat T5: Traffic redirection*
TG3 – Nefarious Activity/Abuse	*Threat T6: Exploitation of software bugs* *Threat T7: Manipulation of hardware and firmware* *Threat T8: Malicious code/software/activity* *Threat T9: Remote activities (execution)* *Threat T10: Malicious code - Signaling amplification attacks*
TG4 – Organisational (failure malfunction)	*Threat T11: Failures of devices or systems* *Threat T12: Supply chain* *Threat T13: Software bugs*

Network-Centric Security: Current Trends

- Network environments are **more and more dynamic**, expanding the network perimeters and requiring multiple layers of defence to mitigate vulnerabilities
- **Everything connected to a network becomes a target**
  - Attack surfaces include traditional servers, as well as IoT devices and network assets in all 5 domains
- Criminals have **more entry points** than ever before
- New emerging risk factors and threats exploiting the adoption of new network technologies such as 5G, Network Functions, Resource Exhaustion, and many others
- Mobile malware and attacks

User-Centric Security: Threats

Threat Groups	Threats
TG1 – Human Errors	*Threat T1: Mishandling of physical assets* *Threat T2: Misconfiguration of systems* *Threat T3: Loss of CIA on data assets* *Threat T4: Legal, reputational, and financial cost*
TG2 – Privacy breach	*Threat T5: Profiling and discriminatory practices* *Threat T6: Illegal acquisition of information*
TG3 – Cybercrime	*Threat T7: Organized criminal groups' activity* *Threat T8: State-sponsored organizations' activity* *Threat T9: Malicious employees or partners' activity*
TG4 – Media amplification effects	*Threat T10: Misinformation/disinformation campaigns* *Threat T11: Smearing campaigns/market manipulation* *Threat T12: Social responsibility/ethics-related incidents*
TG5 – Organisational threats	*Threat T9: Skill shortage/undefined cybersecurity curricula* *Business misalignment/shift of priorities*

User-Centric Security: Current Trends

- With the advent of IoT, **users become just another component of complex systems**
  - Their involvement is increasingly pervasive
  - Complex systems/applications based on data sensed by users devices
  - The trustworthiness of data become fundamental
- **Users become target of attacks**
  - Fake news, fake social accounts, and deep fake to manipulate and altering perception of reality
  - Reputation attacks targeting the reputation of the users through impersonation/fake news
  - Attacks to smart devices and smart homes, making users source of untrustworthy data

Device/IoT Security: Threats

Threat Groups	Threats
TG1 – Unintentional damage / loss of information or IT assets	*Threat T1: Information leakage/sharing due to human errors* *Threat T2: Inadequate design and planning or incorrect adaptation*
TG2 – Interception and unauthorised acquisition	*Threat T3: Interception of information* *Threat T4: Unauthorised acquisition of information (data breach)*
TG3 – Intentional Physical Damage	*Threat T5: Device modification* *Threat T6: Extraction of private information*
TG4 – Nefarious Activity/Abuse	*Threat T7: Identity fraud* *Threat T8: Denial of service* *Threat T9: Malicious code / software / activity* *Threat T10: Misuse of assurance tools* *Threat T11: Failures of business process* *Threat T12: Code Execution and Injection (unsecure APIs)*
TG5 – Legal	*Threat T14: Violation of laws or regulations / Breach of legislation / Abuse of personal data*
TG6 – Organisational threats	*Threat T15: Skill shortage*

Device/IoT Security: Current Trends

- IoT enlarges the perimeter of the system
  - devices with very basic security capabilities
- Adoption of **lightweight cryptography for embedded devices** in order to find a balance between security and cost constraints
- **Physical access to IoT** device will be exploited also in the future as bridge to generate malicious insider-based threats
- One emergency that is already underlined but will be exacerbated in the future is the **strict relation between IoT security and safety**
- Adoption of smart home devices such as Alexa, Google home
  - AI capabilities
- With the advent of 5G, **the diffusion of IoT will receive a tremendous boost** exacerbating the actual concerns and opening to new ones.

Summary of Top Findings & Key Takeaways

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

http://sesar.di.unimi.it/cybersecurity-top-findings/

Contact

Research Institute CODE
Carl-Wery-Straße 22
81739 Munich
Germany

contact@concordia-h2020.eu

Follow us

www.concordia-h2020.eu

www.twitter.com/concordiah2020

www.facebook.com/concordia.eu

www.linkedin.com/in/concordia-h2020