Mestrado em Engenharia Informática (MEI)
Mestrado Integrado em Engenharia Informática (MiEI)

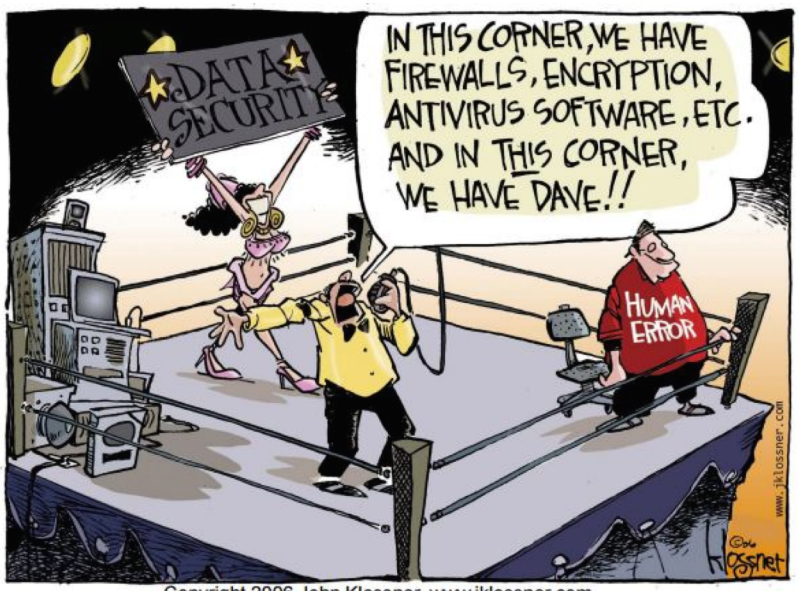
Perfil de Especialização **CSI** : Criptografia e Segurança da Informação

Engenharia de Segurança

jose.miranda@devisefutures.com

Topics

- Software Security Threats
- Categories of attacks exploiting software vulnerabilities



Copyright 2006 John Klossner, www.jklossner.com

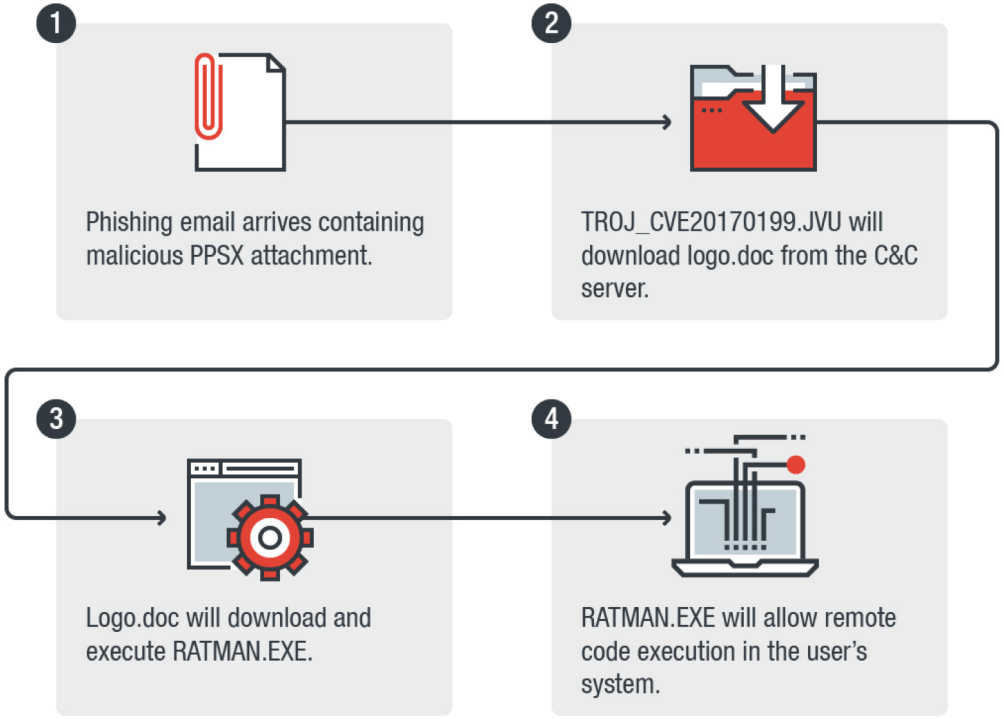
Where is the risk?

Cyber Vulnerability	Company	Product	Associated Malware	CVSS	Recorded Future Risk Score
CVE-2018-8174	Microsoft	Internet Explorer	Fallout Exploit Kit, KaiXin Exploit Kit, LCG Kit Exploit Kit, Magnitude Exploit Kit, RIG Exploit Kit, Trickbot, Underminer Exploit Kit	7.6	89
CVE-2018-4878	Adobe	Flash Player	Fallout Exploit Kit, GreenFlash Exploit Kit, Hermes Ransomware, Sundown Exploit Kit, Threadkit Exploit Kit	7.5	89
CVE-2017-11882	Microsoft	Office	AgentTesla, Andromeda, BONDUPDATER, HAWKEYE, LCG Kit, Loki, POWRUNNER, QuasarRAT, REMCOS RAT, ThreadKit Exploit Kit	9.3	99
CVE-2017-8750	Microsoft	Office	Formbook, Loki, QuasarRAT	7.6	89
CVE-2017-0199	Microsoft	Office	DMShell++, njRAT, Pony, QuasarRAT, REMCOS RAT, SHUTTERSPEED, Silent Doc Exploit Kit, Threadkit Exploit Kit	9.3	99
CVE-2016-0189	Microsoft	Internet Explorer	Grandsoft Exploit Kit, KaiXin Exploit Kit, Magnitude Exploit Kit, RIG Exploit Kit, Underminer Exploit Kit	7.6	89
CVE-2017-8570	Microsoft	Office	Formbook, QuasarRAT, Sisfader RAT, Threadkit Exploit Kit, Trickbot	9.3	99
CVE-2018-8373	Microsoft	Internet Explorer	Quasar RAT	7.6	89
CVE-2012-0158	Microsoft	Office	Silent Doc Exploit, PlugX	9.3	89
CVE-2015-1805	Google	Android	AndroRAT	7.2	89

Top Vulnerabilities in 2018 – https://go.recordedfuture.com/hubfs/reports/cta-2019-0319.pdf

Where is the risk?

- CVE-2017-0199



Trend Micro – https://blog.trendmicro.com/trendlabs-security-intelligence/cve-2017-0199-new-malware-abuses-powerpoint-slide-show/

Where is the risk?

February 2019. State-sponsored hackers were caught in the early stages of gaining access to computer systems at the Australian Federal Parliament

February 2019. European aerospace company Airbus reveals it was targeted by Chinese hackers who stole the personal and IT identification information of some of its European employees

February 2019. Norwegian software firm Visma revealed that it had been targeted by hackers from the Chinese Ministry of State Security who were attempting to steal trade secrets from the firm's clients

January 2019. Hackers associated with the Russian intelligence services were found to have targeted the Center for Strategic and International Studies

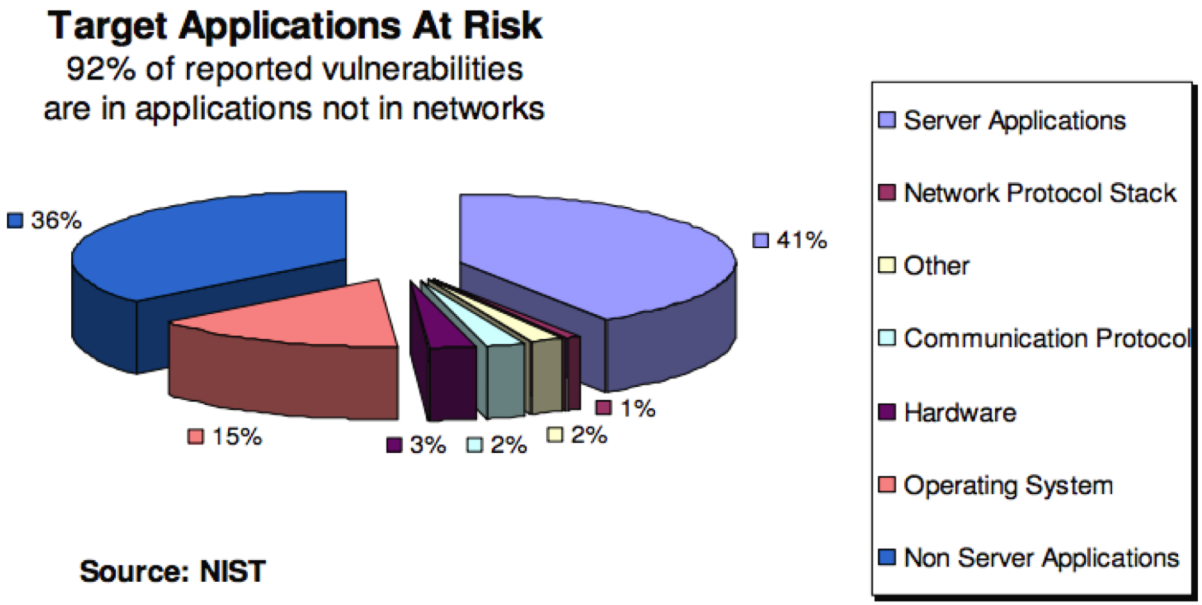
January 2019. The U.S. Department of Justice announced an operation to disrupt a North Korean botnet that had been used to target companies in the media, aerospace, financial, and critical infrastructure sectors.

January 2019. Former U.S. intelligence personnel were revealed to be working for the UAE to help the country hack into the phones of activists, diplomats, and foreign government officials

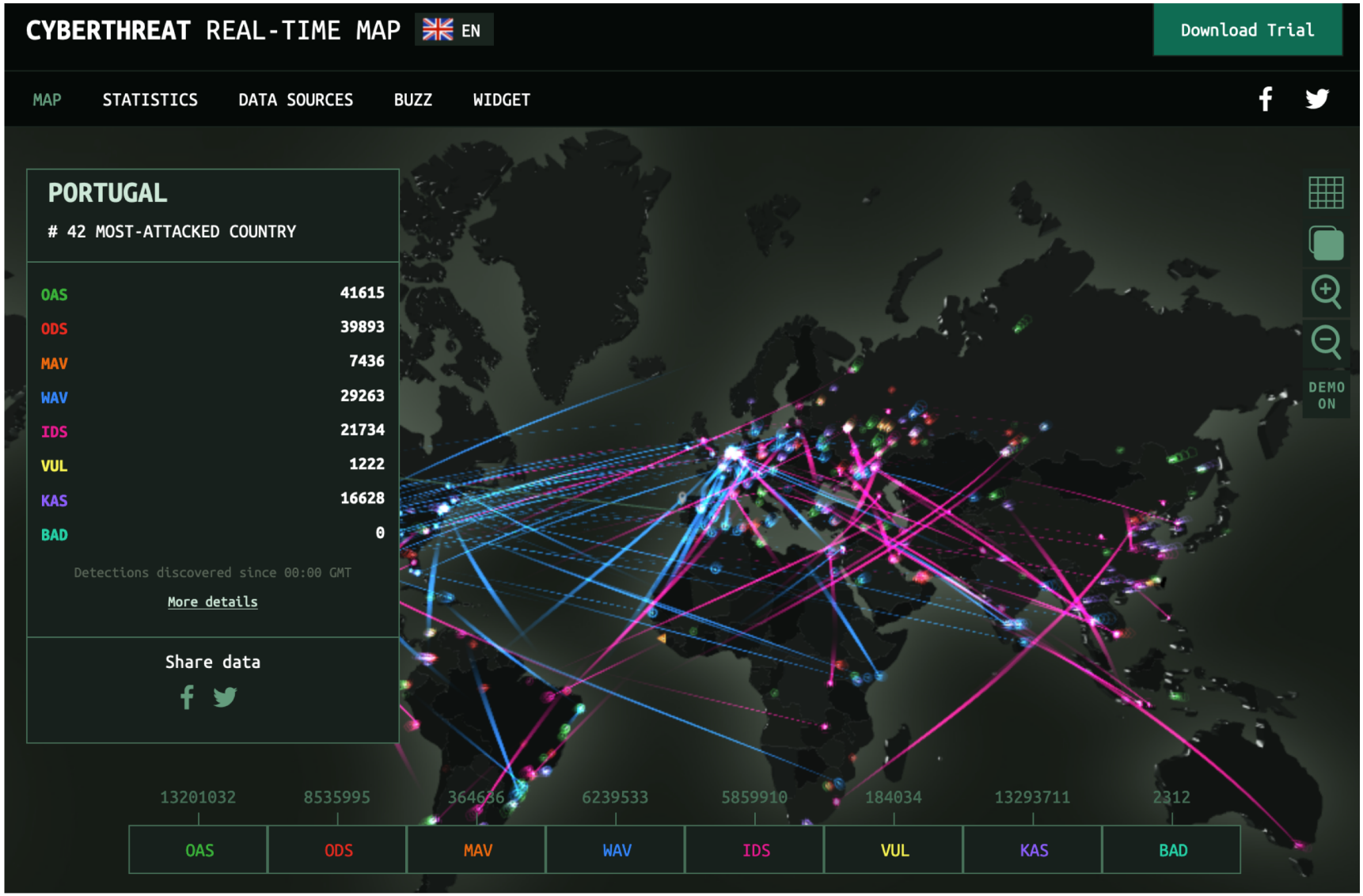
January 2019. U.S. prosecutors unsealed two indictments against Huawei and its CFO Meng Wanzhou alleging crimes ranging from wire and bank fraud to obstruction of justice and conspiracy to steal trade secrets

CSIS – https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity

What is at risk?



What is at risk?



Kaspersky Lab – https://cybermap.kaspersky.com/. (28/Abr/2019)

Software Security Threats

- A threat to a software system is any actor, agent, circumstance or event that has the potential to cause harm to that system or the data or resources to which the system accesses or allows access.
- Threats can be categorized according to their intentionality:
  - unintentional,
  - intentional but not malicious
  - malicious (attacks).
- Most software attacks exploit some vulnerability or weakness in the software.
- Threats to software are present throughout its life cycle.

Software Security Threats

Example of software threats in the development, distribution and operation phases, categorized according to their intentionality.

Threat category	Development	Distribution	Operation
Not intentional	Typing error in source code by sloppy programmer, changes the functionality of software compiled from this source code. The programmer who does not know the safe coding practices writes a C module that makes insecure calls to external libraries.	The system administrator accidentally assigns write permissions to all users to the directory in which the software is installed.	The user can perform an extremely long input because the HTML input form does not validate and truncate the excess characters.

Software Security Threats

Example of software threats in the development, distribution and operation phases, categorized according to their intentionality.

Threat category	Development	Distribution	Operation
Intentional but not malicious	To satisfy the customer's request to make performance the top priority, the programmer eliminates input validation functions that add performance overhead. The programmer pressed by management to deliver the source code within a tight deadline, does not security review the code.	The administrator assigns "root" privileges to a software program that has been deployed in such a way that it can only be run as root.	The frustrated user repeatedly inserts unusual combinations of commands in order to bypass a data input interface from the pull-down menu. The frustrated user repeatedly refreshes and resends the same input data to an application that was not designed to return a confirmation that the input data had been received.

Software Security Threats

Example of software threats in the development, distribution and operation phases, categorized according to their intentionality.

Threat category	Development	Distribution	Operation
Malicious	The programmer intentionally includes three exploitable faults and one backdoor in its source code. The integrator adds a logic bomb to an open source program.	The system installer leaves the default application password unchanged to facilitate the life of the attacker with whom he is in collusion. The system administrator intentionally configures the firewall to allow access to URLs (Uniform Resource Locators) that contain executable content.	The attacker initiates a SQL injection attack against a Web application that uses a database. The programmer sends a predefined data string to a Web application that knows that it will trigger the execution of the logic bomb it has planted in that application.

Attack categories

- Categories of attacks exploiting software vulnerabilities:
  - **Recognition Attack**
    - Helps the attacker find out more about the software and its environment so that subsequent attacks can be more effective;
    - Attackers are particularly interested in the software version information and COTS (Commercial off-the-shelf) and OSS (Open-source software) components of the environment, as this information reveals whether the software / environment includes components with known vulnerabilities that may be explored.
  - **Attack Facilitator**
    - Type of attacks that facilitate the realization of other attacks;
    - Examples: attacks that exploit buffer overflow to execute malicious code; attacks to increase privileges.
  - **Disclosure Attack**
    - Reveal data that should not be seen by the attacker (compromise of confidentiality).
  - **Corruption attack**
    - Adulterate and corrupt the software to change its mode of operation (compromise of integrity).
  - **Sabotage attack**
    - Causes the software to fail or prevents it from being accessed by its users;
    - Also known as a "denial of service" (compromise of availability).
  - **Malicious code attack**
    - Inserts malicious logic into the software, triggers the execution of malicious code already embedded in the software, or malicious delivery / execution in the software execution environment.

STRIDE threat list

The STRIDE-based threat list is useful for identifying threats from the point of view of attackers' goals.

Threat Type	Example	Security control
Spoofing	An action that has the purpose of accessing and using, in an illegal way, the credentials of another user, such as *username* and *password*.	Authentication
Tampering	An action that aims at malicious modification / modification of persistent data (for example, in a database), and the change of data in transit between two computers in an open network (eg the Internet).	Integrity
Repudiation	An action that has as purpose to carry out illegal operations in a system that does not have mechanisms to track the prohibited operations.	Non-repudiation
Information disclosure	An action that is intended to read a file that by someone withou access rights, or to read data in transit.	Confidentiality
Denial of service	An action that is intended to deny access to valid users (for example, by making a web server temporarily unavailable or unusable).	Availability
Elevation of privilege	An action that has the objective of obtaining privileged access to resources, in order to access the information unduly or to compromise the system.	Authorization

STRIDE threat list

Based on each type of STRIDE threat, it is possible to identify threat mitigation techniques that can be used to mitigate each concrete threat identified.

Threat Type	Threat mitigation techniques	Security control
Spoofing	1. Appropriate Authentication 2. Protect data / secret information 3. Do not store secrets	Authentication
Tampering	1. Appropriate Authorization 2. Hashes 3. MACs 4. Digital signatures 5. Protocols inviolable / resistant to attacks	Integrity
Repudiation	1. Digital signatures 2. Timestamps 3. Audit logs	Non-repudiation
Information disclosure		Confidentiality
Denial of service		Availability
Elevation of privilege		Authorization

jose.miranda@devisefutures.com

STRIDE threat list

Based on each type of STRIDE threat, it is possible to identify threat mitigation techniques that can be used to mitigate each concrete threat identified.

Threat Type	Threat mitigation techniques	Security control
Spoofing		Authentication
Tampering		Integrity
Repudiation		Non-repudiation
Information disclosure	1. Authorization 2. Advanced privacy protocols 3. Encryption 4. Protect secrets 5. Do not store secrets	Confidentiality
Denial of service	1. Appropriate Authentication 2. Appropriate Authorization 3. Filter 4. Throttling / Control 5. Service quality	Availability
Elevation of privilege	1. Run with minimal privileges	Authorization

Work sheet

- Analyze https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity.