Introduction to Network Security

Segurança em Redes de Comunicações

Mestrado em Cibersegurança

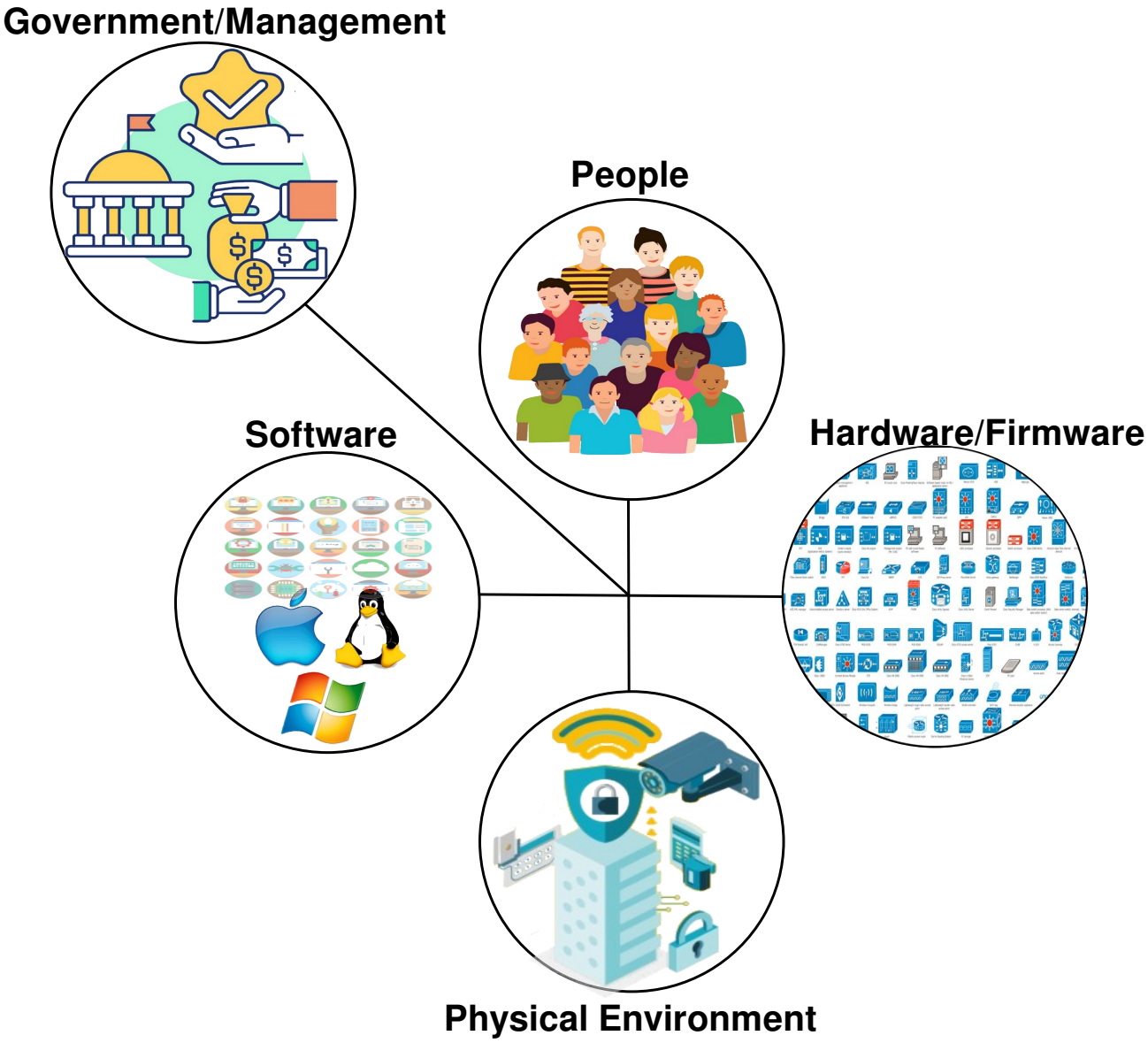
Mestrado em Engenharia de Computadores e Telemática

DETI-UA

universidade de aveiro

deti.ua.pt

Network Security Pillars



Network Operations Center (NOC)

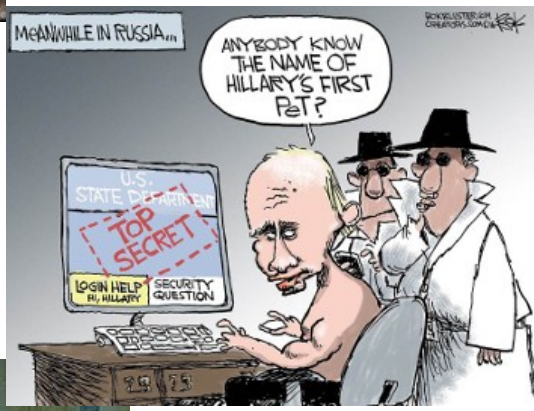
- Security competences of a NOC in an organization:
  - Network resilience and high-availability
  - Network/services segregation
  - Network devices, terminals and server/services deployment
    - Firmware/Software install, update and patch
  - Security policies deployment
    - Firewalls, IDS/IPS, etc...
  - Data acquisition
  - Threat mitigation
    - Firewall rules (by request)
    - Device isolation/deactivation
  - Forensics
    - Done after an attack
    - Gather evidences for judicial purposes
    - Gather additional data to improve future prevention/detection/response, data acquisition and threat mitigation (NDR by NOC).

Security Operations Center (SOC)

- Competences of a SOC in an organization:
  - Prevention and detection of attacks
    - Monitor network and services (with SIEM)
    - Detect vulnerabilities (with vulnerability scanning tools)
    - Detect malicious activities (with SIEM)
    - Detect anomalous behaviors (with SIEM)
      - may not be malicious!
  - Investigation
    - Analyze the suspicious activity to determine/characterize the threat
    - Evaluate how deep the threat has penetrated the network/systems
  - Response
    - Deploy counter measures based on known playbooks
    - Deploy emergency measures when threat do not match a known response playbook
  - Forensics
    - Done after an attack
    - Gather evidences for judicial purposes
    - Gather additional data to improve future prevention/detection/response, data acquisition and threat mitigation (NDR by NOC).
- Nowadays commonly operated independently of the Network Operation Center (NOC).
- Should be integrated with NOC.
  - For network/services segregation and resilience, data acquisition and threat mitigation.

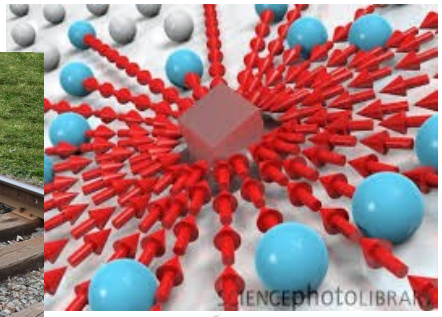
Type of Attacks (1)

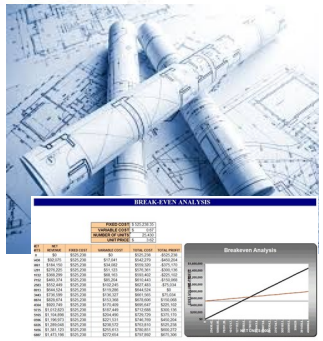
- Objectives:
  - Fun and/or hacking reputation
  - Political purposes
  - Military purposes
  - Economical purposes
  - Other?
- Technical objectives:
  - Operation disruption
  - For data interception
  - Both
    - Disruption to intercept!
    - Intercept to disrupt!



Type of Attacks (2)

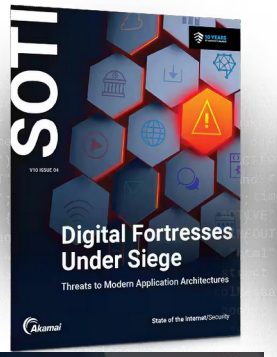
- Technical objectives:
  - Operation disruption.
    - (Distributed) Denial-of-Service.
  - Resources hijack.
    - Spam,
    - Crypt-currency mining/masternodes,
    - Platform to other attacks!
  - Data interception/stealing.
    - Personal data
      - As final goal,
      - Or as tool to achieve more value information!
    - Technical data,
      - Usually used to achieve more value information!
    - Commercial data
      - Digital objects, financial and/or engineering plans, ...
- Disruption may be used to achieve interception!
- Interception may me used to achieve disruption (operational or commercial)!

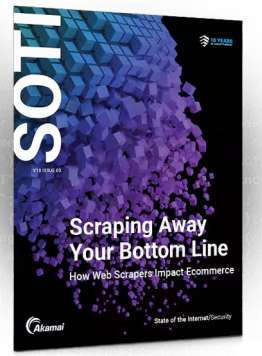


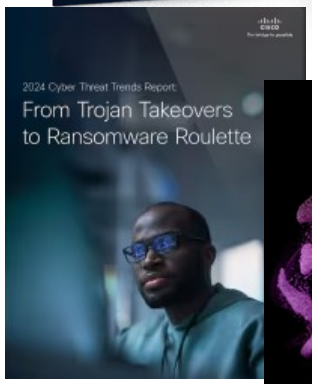


Security Reports

- Akamai State of the Internet Reports
- Cisco Cyber Threat Trends Report
- Checkpoint Cybersecurity report
- Deloitte Cyber Threat Trends report
- Fortinet Application Security Report
- Cloudflare State of Application Security
- Paloalto The State of OT Security
- Paloalto Incident Response
- NSA Cybersecurity Year in Review







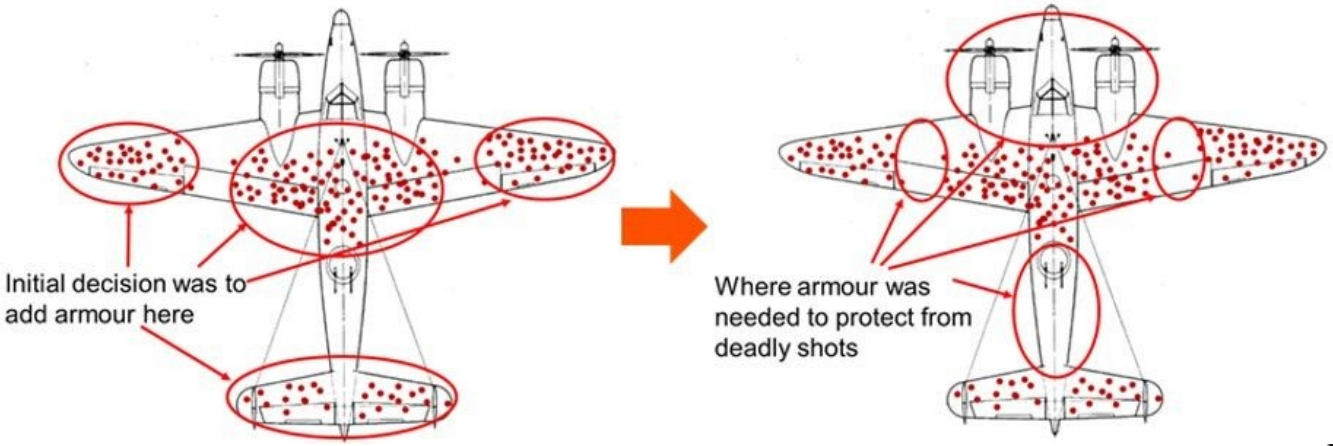
universidade de aveiro

More on Security Reports

- Identify threats with solutions, recommend to implement known solutions and good practices.
- “Hint” to the existence of many unknown threats:
  - Actors.
  - Technological (zero-day)
  - Levels
    - Network and software.
- Commercial frameworks design to (try to) solve unknown threats.
  - No concrete results or analysis of performance!

Observation Bias

- Data is captured and analyzed in a way that confirms pre-existing observations and beliefs.
  - Other data is not considered.
- This impacts how data is collected, analyzed, and acted upon in cybersecurity.
  - Limit data collection and analysis.
  - Solutions only to visible problems.
  - Unknown threats remain hidden and unsolved!
- Only visible attacks (successful or not) are considered relevant.
- **Unseen/stealth attacks are not considered!**
- WW2 planes ana

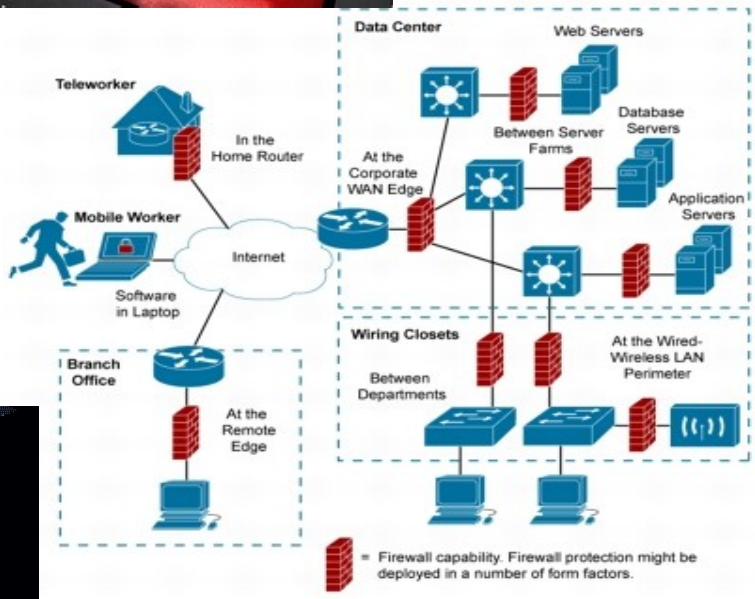


Cyber-Physical Security (non-network)

- General Security
  - Doors, Locks, Alarms, Personal, Sensors, etc...
- Human train for internal and external interaction.
- Access and movement policies
  - Inside premises and near-premises.
- Environment control redundancy and monitoring
  - Temperature, AC, Humidity, Sound, Smoke, etc...
- Power redundancy and monitoring
- Radio awareness (spectrum monitoring) and suppressors (Faraday cages)
- ...

Traditional Defenses

- Vulnerability patching.
- Firewalls
  - Centralized.
  - Distributed.
- Intrusion Prevention and Detection Systems (IDS/IPS).
- Antivirus.



- **All rely on previous knowledge of the threat and/or problem!**

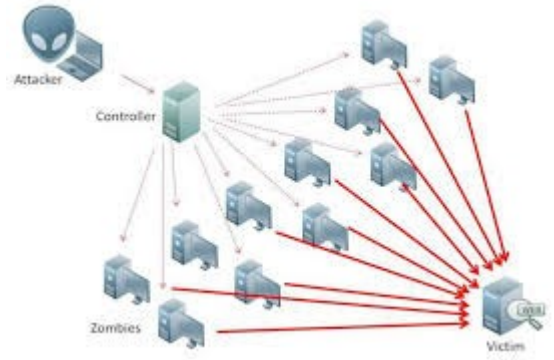
Advanced Persistent Threats

- When an attacker uses sophisticated methods.
- Focuses on specific organizations, exploring **new vulnerabilities** with **new tools**.
  - Usually previously tested with known security tools and systems.
- The attacker presence within the network have long-term goals.
- The objective is to steal, disrupt or both.
  - Large impact goals!
- Activity is stealth
  - Learns licit behaviors,
  - Perform mimic attacks,
  - Adjusts tactics based on defenses.
- May use multiple attack vectors and communication channels.
  - Alternative communication technologies (Bluetooth, Zigbee, LoRa, etc…).
  - Licit services as C&C and exfiltration vectors (DNS, Webservices, Cloud services, etc…).

“Intelligent” Defenses

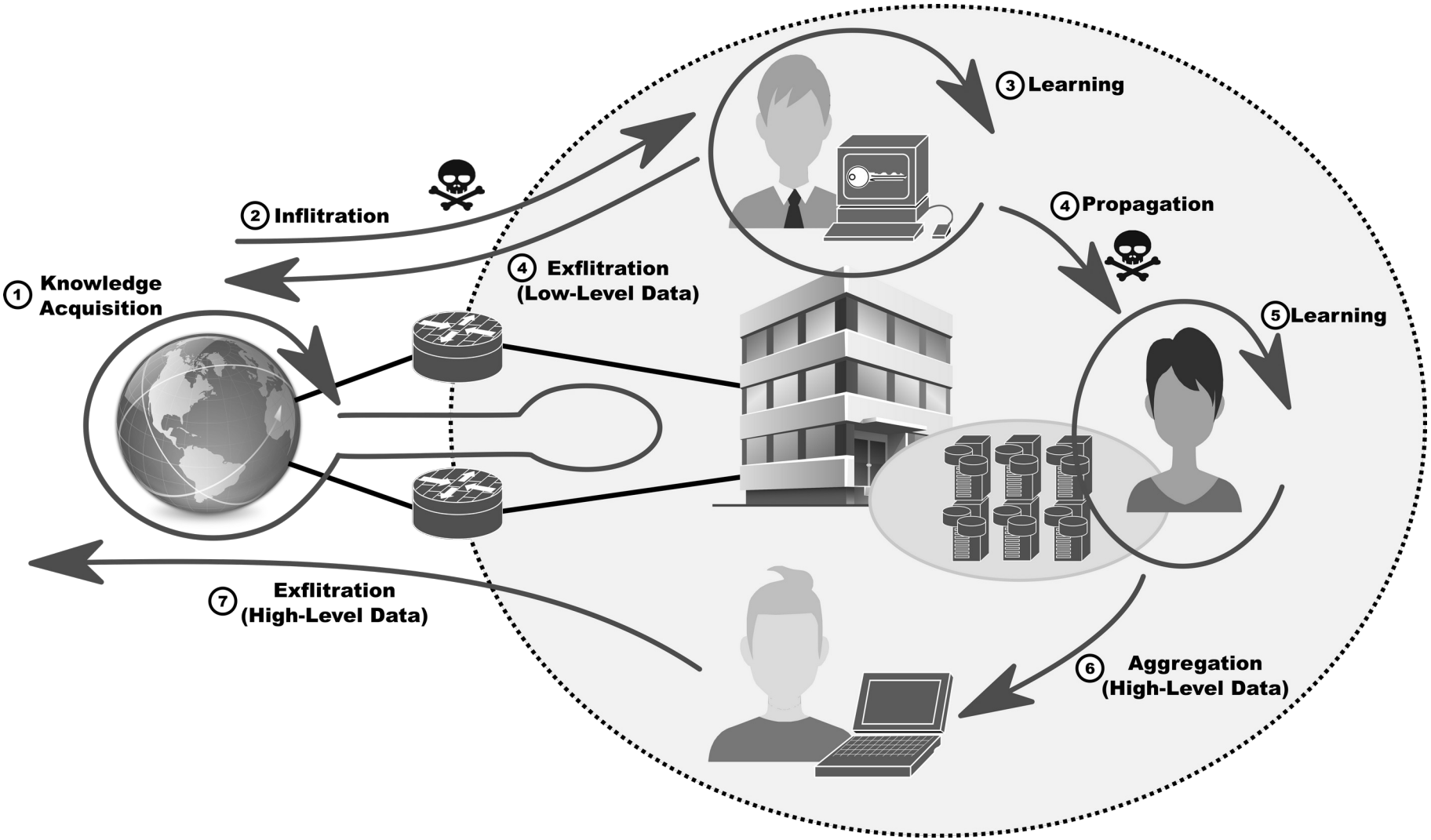
- Detection of unknown threats and/or problems.
  - In time to deploy counter-measures.
- Application of Big Data and Data Science techniques to network ans systems monitoring data.
- Some traditional solutions start to incorporate AI into their equipment
  - E.g., Palo Alto Network Firewalls, Cisco Appliances, …
- Still limited to manufacturer based solutions and localized data.
- Still limited in scope.
  - Obvious threats vs. Stealth threats.
- Optimal deployment requires an overall network and systems knowledge.
  - Network and Systems (Cyber) Situational Awareness.

Disruption Attacks

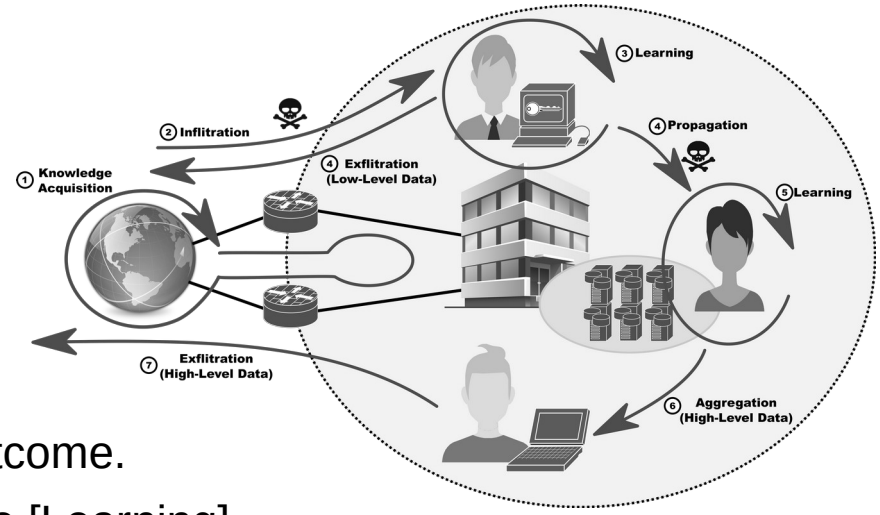


- Distributed DoS
  - Multiple slow/small devices generating traffic to a target
    - TCP vs. UDP
  - Purpose of disruption
    - By political/economical/"reputation"
    - Redirection to other service/location?
  - Solution at target
    - Load-balancers
    - For TCP, maybe its possible to survive making active (with licit client validation) session resets (server/firewalls)
      - White list solution, for completed session negotiation
    - For UDP/DNS, block requests for known external relay/redirection DNS servers (blocks attack amplification, IP target spoofing)
      - Doesn't work with large botnets and direct requests to target
  - Solution at source
    - Anomalous behaviors detection
      - Low traffic variations hard to detect
      - Time and periodicity changes are easier to detect
      - Destinations of traffic changes
      - With "really low" data rates is impossible to detect
- Denial of service by physical signal jamming
  - Pure disruption, or
  - Disruption to activate secondary channels (more easily compromised).
  - Solution
    - Detect, localized source and physically neutralize.
- Disruption of support services/utilities
  - Internet external connection, power, water, access roads, etc...

Attacks Phases



Attacks are Done Incrementally



- Escalation of goals and privileges.
  - Public knowledge opens doors to private information and access to protected domains [Infiltration].
  - The first illicit access to a protect domain may not provide a relevant outcome.
  - Attacker must acquire more knowledge [Learning].
  - The additional knowledge allows to access other secure domain zones/devices/data with increasing relevance [Propagation].
    - At any phase the attacker may require additional knowledge [Learning].
  - When a relevant outcome is acquired it must be transfered to outside of the protected domain [Exfiltration].
  - Direct exfiltration may denounce the relevant points inside of the secure domain.
    - The relevant outcome must be first transferred inside the protected domain to a less important point [Aggregation].
    - Attacker chooses a point that may be detected and lost without harm.

Technical Network Vulnerabilities

- Software
  - Applications
  - Frameworks/API
  - Protocols
  - Operating systems
    - Kernel, kernel modules, drivers, and base applications.
    - Configurations!
  - Low level code
    - CPU microcode, firmware, and BIOS/UEFI.
- Hardware
  - Physical tempering
  - Physical emissions
    - Electromagnetic emissions, sound, ...
  - Power instability, Electromagnetic Pulses (EMP), etc ...
- Known vs. unknown
  - CVE
  - IDS/IPS and antivirus databases

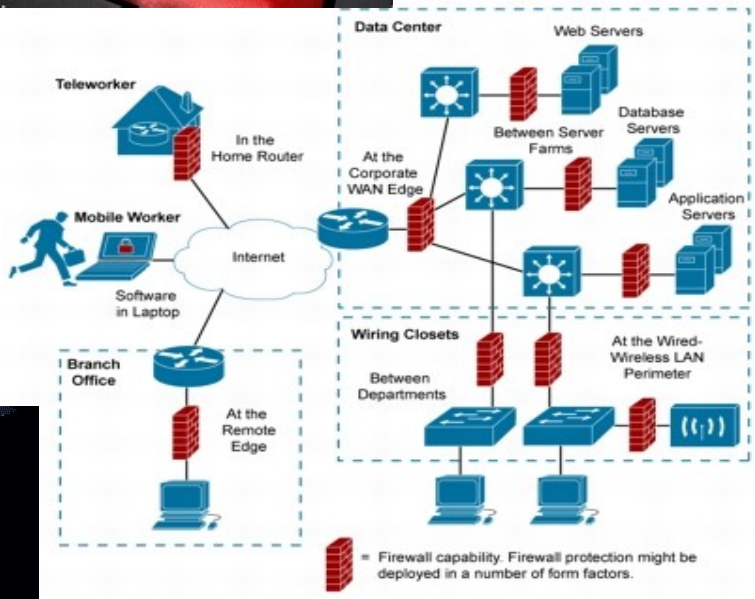
CVE

Common Vulnerabilities and Exposures

universidade de aveiro

Traditional Defenses

- Vulnerability patching.
- Firewalls
  - Centralized.
  - Distributed.
- Intrusion Prevention and Detection Systems (IDS/IPS).
- Antivirus.



- **All rely on previous knowledge of the threat and/or problem!**

“Intelligent” Defenses

- Detection of unknown threats and/or problems.
  - In time to deploy counter-measures.
- Application of Big Data and Data Science techniques to network ans systems monitoring data.
- Some traditional solutions start to incorporate AI into their equipment
  - E.g., Palo Alto Network Firewalls, Cisco Appliances, …
- Still limited to manufacturer based solutions and localized data.
- Still limited in scope.
  - Obvious threats vs. Stealth threats.
- Optimal deployment requires an overall network and systems knowledge.
  - Network and Systems (Cyber) Situational Awareness.

Infiltration Phase

- Licit machines must be compromised to implement the different attacks phases.
  - Ideally in a privileged “zone” of the network, and/or
  - With access credentials, and/or
    - User credentials, address(es), hardware key, etc…
  - With “special” software, and/or
  - Target data.
- May include the installation of software or usage of licit vulnerable software.
- May be remotely controlled (constantly or not).
  - Command and control (C&C).
- May have autonomous (AI) bots installed to perform illicit actions.
  - When remote C&C is not possible or subject to easy detection.

Remotely by Exploiting Licit Users

- Objectives:
  - Credentials acquisition.
  - Software insertion.
  - Ramsomware.
- Vectors:
  - E-mail and social networking
    - Phishing for credentials.
    - Office macros.
    - Binaries execution.
  - Downloadable software
    - Cracks.
    - Non-certified software stores.
    - …

Remotely by Attacker Actions

- Possible when network/systems have unpatched (unresolved) vulnerabilities.
  - Limited in time.
- Possible when network/systems are poorly configured/designed
  - Less limited in time.
  - Hard to perform discovery without detection by traditional defense systems.
    - Sometimes poorly configured/designed systems are not protected by adequate systems (if any).
- Usually not done first.
- Done after acquiring some credentials/privileges from licit users.
  - Using direct connections/services.
  - Easier to hide (stealth attacks) by having reduce activity or mimicking licit usage.

Locally by Physical Interaction

- Objectives:
  - Traffic interception.
  - Local network access to exploit vulnerabilities.
  - Direct access to machine.
- Vectors:
  - Ethernet ports at public/unprotected locations
    - With VLAN separation
    - Without VLAN separation
    - Protected by 802.1X
  - Network taps at public/unprotected locations
  - Fake access points.
    - Rogue access points
  - Low security in IoT devices/network (Bluetooth, Zigbee, Thread)
  - Network devices access
    - Unprotected serial/console ports, USB ports, etc...
  - USB ports (short time access)
    - Long time objectives
      - Trojan/root kits injection.
    - Short time objectives
      - Device data acquisition (contacts, messages, sms, etc...)
  - Sitting down at a terminal or with a device!
  - Other?

Propagation Phase

- Done using a mixture of methodologies:
  - Credentials exploitation.
    - Direct usage or by using allowed applications.
  - Impersonating users and systems.
    - Similar to credential exploitation but more advanced based on acquired knowledge (licit behavior).
    - Requires time to learn and mimic licit behavior.
      - Time patterns, traffic patterns, application patterns, etc...
  - Vulnerability exploitation.
    - Inside a protected domain systems are many times considered in a secure zone.
    - Less maintained and legacy OS/applications may be required to run (no patching).
    - Broader range of vulnerabilities

Aggregation and Exfiltration Phase

- Data transferred from machine to machine.
- Internally [Aggregation] it can be done using existing channels.
- Externally [Exfiltration]
  - It can be done directly using existing channels.
    - File copy, email, file sharing, etc…
    - Can be detected.
  - It can be done hiding information within existing/allowed channels and licit communications.
    - Slower data transfer, harder (impossible?) to detect.
    - Examples:
      - Usage of steganography in photos (via social networking).
      - Usage of embed data in text and voice messages.
      - ...

Simple vs Complex Scenarios

- Small/medium network
- Large Network
- Datacenter
- Geographically distributed network