

Introduction to Network Security

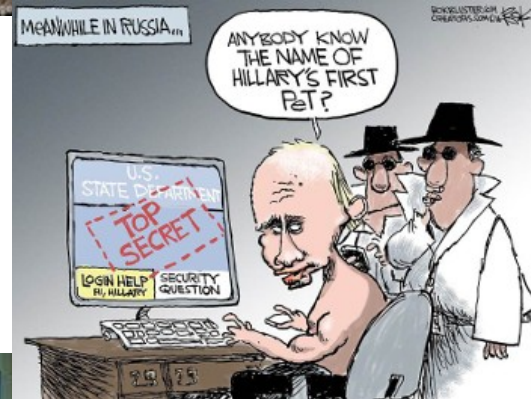
Segurança em Redes de Comunicações
Mestrado em Cibersegurança
DETI-UA

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,

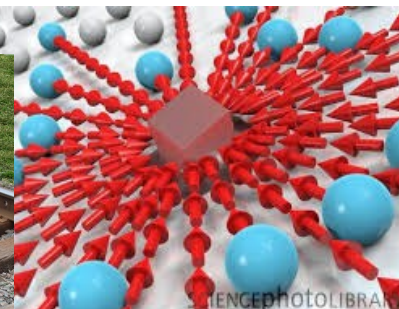
- Usually used to achieve more value information!

- ➔ Commercial data

- Digital objects, financial and/or engineering plans, ...

- Disruption may be used to achieve interception!

- Interception may be used to achieve disruption (operational or commercial)!



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

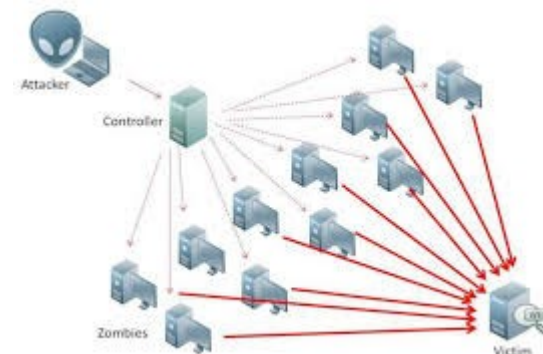
• Denial o service by physical signal jamming

- ◆ Pure disruption, or

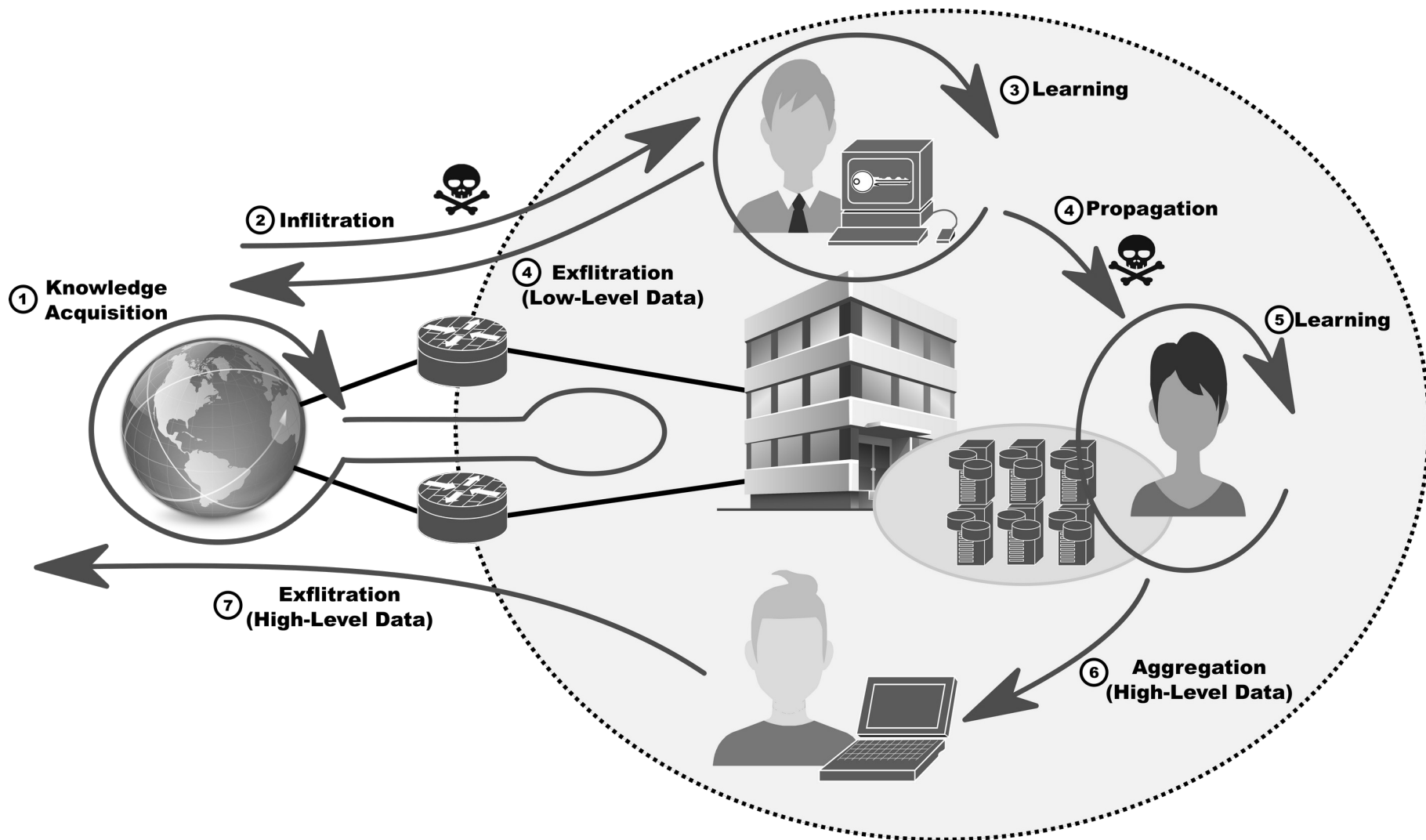
- ◆ Disruption to activate secondary channels (more easily compromised).

- ◆ Solution

- Detect, localized source and physically neutralize.



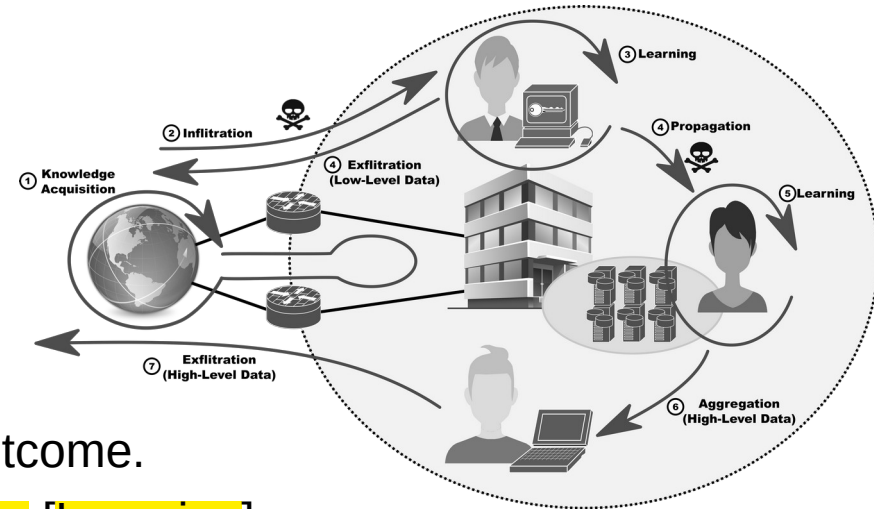
Attacks Phases



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 **transferred** 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

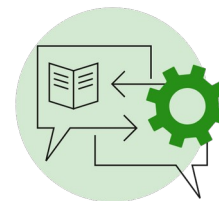
- ◆ Applications
- ◆ Frameworks/API
- ◆ Protocols
- ◆ Operating systems
 - Kernel, kernel modules, drivers, and base applications.
 - Configurations!
- ◆ Low level code
 - CPU microcode, firmware, and BIOS/UEFI.

• Hardware

- ◆ Physical **tempering**
- ◆ Physical **emissions**
 - Electromagnetic emissions, sound, ...
- ◆ Power instability, Electromagnetic Pulses (EMP), etc ...

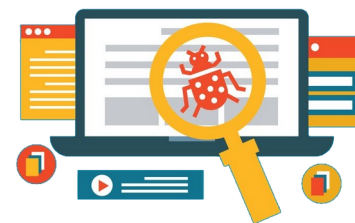
• Known vs. unknown

- ◆ CVE
- ◆ IDS/IPS and antivirus databases



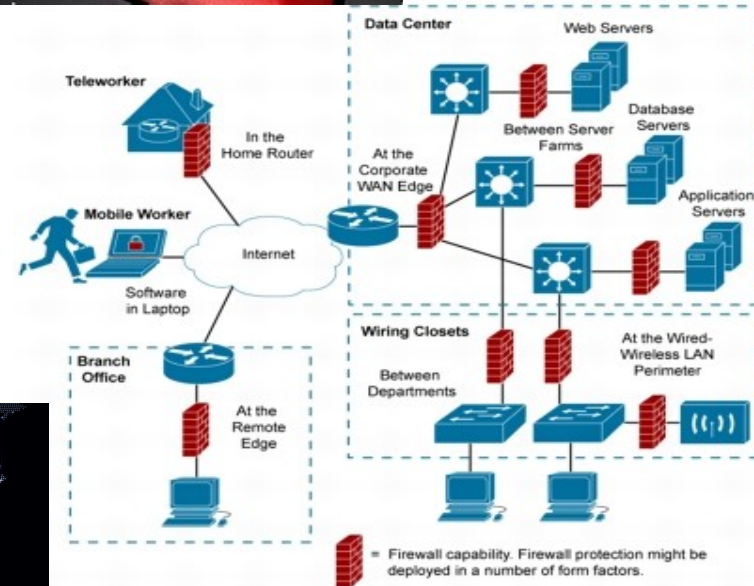
CVE

Common Vulnerabilities and Exposures



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 and 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.



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.
 - ...



Security Metrics/KPI

- Access management

- ◆ How many users have administrative access, and how often is used.
- ◆ Shared passwords between staff.

- Preparedness

- ◆ Percentage of devices fully patched and up to date.

- Days to patch

- ◆ Average time between patch availability and deployment.

- Unidentified devices

- ◆ Illicitly deployed devices.
- ◆ BYoD policy, legacy devices, unlisted devices, IoT devices, etc...

- Security devices average/maximum load per time period.

- Intrusion attempts

- ◆ Amount of detected and undetected attempts (in real time or after off-line auditing).

- Cost per incident

- ◆ Includes staff overtime, external support, investigation costs, employee productivity loss, loss of communication, service failure, etc...

- Mean Time Between Failures (MTBF)

- ◆ Average time between failures (hardware and/or software).
- ◆ General or per device/service.

- Mean Time to Recovery (MTTR)

- ◆ Average time between failure and recovery (hardware and/or software).

- Mean Time to Detect (MTTD)

- ◆ Average time between intrusion and detection.

- Mean Time to Acknowledge (MTTA)

- ◆ Average time between detection and start of countermeasures deployment.

- Mean Time to Contain (MTTC)

- ◆ Average time between start of countermeasures deployment and complete mitigation.

- Mean Time to Resolve (MTTR)

- ◆ MTTA+MTTC

