Introduction to Network and Systems Security

Aprendizagem Aplicada à Segurança

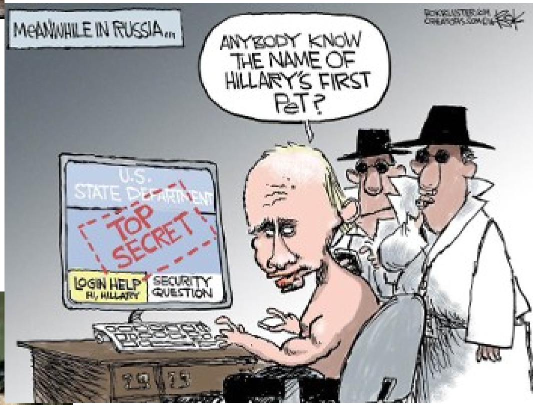
Mestrado em Cibersegurança
DETI-UA

universidade de aveiro

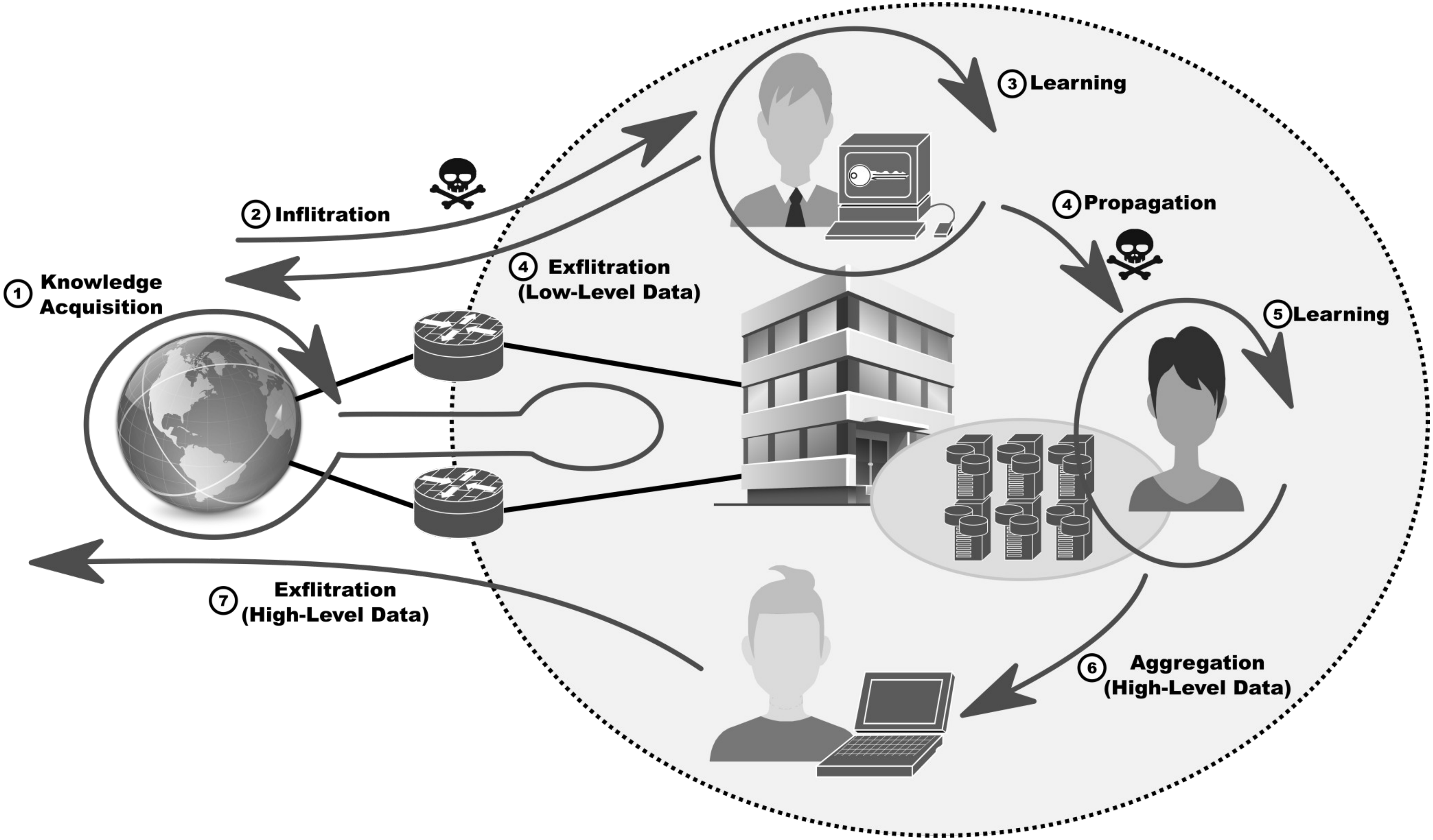
deti.ua.pt

Attacks to Networks and Systems

- 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!
- Most attacks never seen before
  - Zero-day attacks

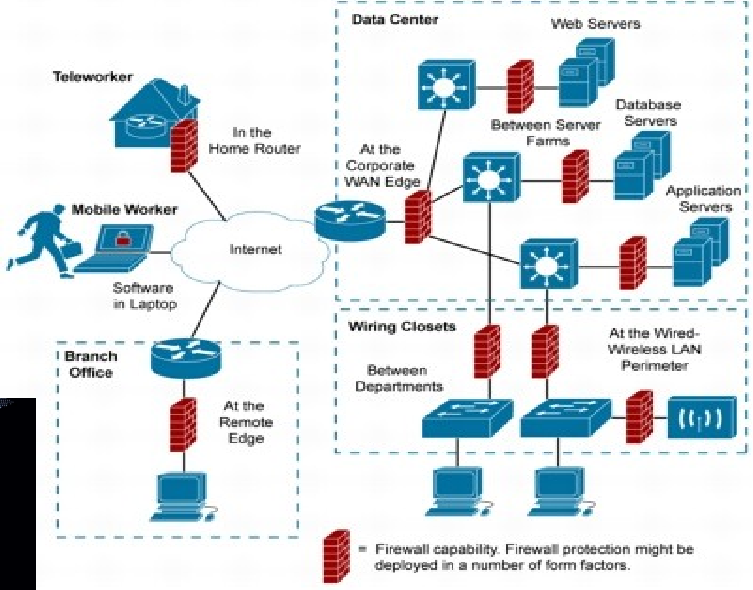


Attack Phases



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 Awareness.

Awareness

- **Direct** Awareness
  - By direct observation.
- **Indirect** Awareness
  - By analysis of reactions to events.
- Awareness **by Correlation**
  - Joint analysis of multiple sources of data to detect hidden patterns and relations.
  - Big Data Problem.
- Awareness **by Prediction**
  - Detection of patterns over time.
  - Black Swan Problem!
- Its all an **Inference**, **Validation**, **Correction** loop.

Cyber Situational Awareness (1)

- Ability to effectively **Acquire Data** by **Monitoring** networks and systems to:
  - Optimize services,
  - Detect and counter-act anomalous activity/events.
- **Analyze/Process** data to know and characterize
  - Network entities,
    - An entity should be understood as a person, a group, a terminal, a server, an application, etc...
  - Data flows,
  - Services and users perception of service.

Cyber Situational Awareness (2)

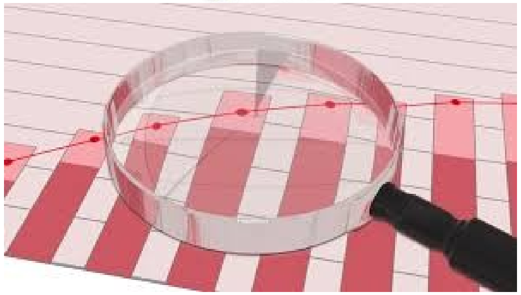
- All data sources are acceptable.
  - Never assume data irrelevance!
- Data may be:
  - Quantitative.
    - Allows for statistical analysis and may serve as machine learning training input.
    - e.g., number of packets, number of flows, number of contacted machines, etc...
  - Qualitative.
    - Can be transformed to quantitative data by counting techniques and statistical characterization
    - e.g., error message X, address Y contacted, packet of type Z, etc...

Cyber Situational Awareness (3)

- Time is relevant.
  - History is relevant.
  - Relative and absolute.
  - An event occurs in a specific time instant, and it is part of a sequence of events.
- Timescale(s) of analysis must:
  - Include the target characteristics,
  - Allow the perception of the event in time for a response.
- Data may be re-scaled for multiple analysis purposes.

Cyber Awareness Steps

- Data acquisition.
- Data processing.
  - Creation of time sequences with different counting intervals (minimum timescales).
  - Creation of time sequences with different statistical metrics (larger timescales).



- Creation of entities’ behavior profiles and objects’ data patterns.
  - Usually time dependent.

- Classification of entities’ behaviors and/or objects’ data patterns.
  - Identification/classification.
  - Anomaly detection.
  - Rogue agent or manipulated/forged data object.