Data and Network Security

(Master Degree in Computer Science and Cybersecurity)

Lecture 5

SAPIENZA
UNIVERSITÀ DI ROMA

Outline for today

- Recap last lecture
- Advanced persistent threats - Detection

Advanced Persistent Threats

Sophisticated, targeted cyberattack in which an unauthorized entity gains access to a network and remains undetected for an extended period of time.

Advanced Persistent Threats

Sophisticated, targeted cyberattack in which an unauthorized entity gains access to a network and remains undetected for an extended period of time.

- **APT attacks are characterized by:**
  - advanced tactics,
  - stealthy infiltration methods,
  - persistent presence within the targeted network.

APTs vs. Common attacks

Opportunistic (common) attacks:

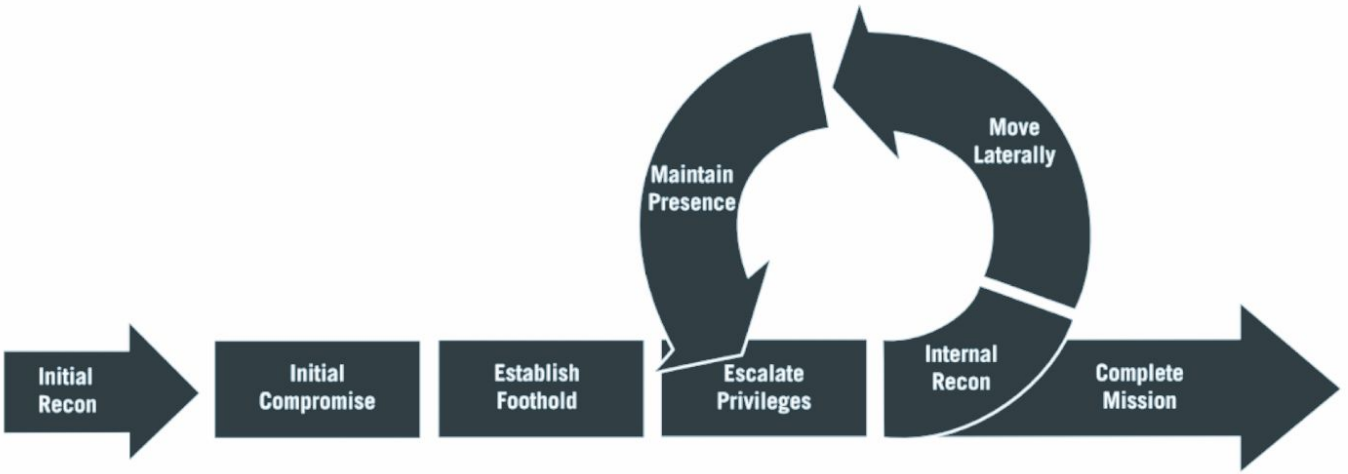
- short-lived
- indiscriminate

APTs vs. Common attacks

APT attacks:

- Carefully planned,
- Well-funded,
- Tailored to target high-value assets, such as sensitive data, intellectual property, or strategic information.

APT - Life Cycle



Why APTs?

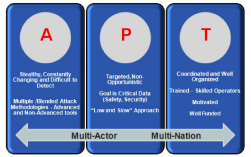
- Economic espionage
- Political espionage
- Ideological motivations

Why APTs?

- **Economic espionage**

  Seek to steal valuable intellectual property, trade secrets, or proprietary information from targeted organizations.

Why APTs?



- **Political espionage**

  Nation-state actors may target government agencies, diplomatic organizations, political parties, or foreign entities to gain insights into:
  - geopolitical developments,
  - national security strategies,
  - diplomatic matters (e.g negotiations).
  - …

Why APTs?

- **Ideological motivations**

  Groups or individuals with specific ideological agendas may target organizations or entities that they perceive as adversaries or opponents to advance their ideological goals or raise awareness about social or political issues.

Detecting APTs

To counteract this threat, an entity/organization needs to put some active defense mechanisms in place.

Detecting APTs

To counteract this threat, an entity/organization needs to put some active defense mechanisms in place.

- **Cyber Threat Hunting**
  - Process that is put in place in order to tackle (hunt) this kind of sophisticated threat.

Cyber Threat Hunting

Cyber Threat Hunting

Process that is put in place in order to tackle (hunt) this kind of sophisticated threat.

- **User/Entity behaviour analytics**
- **Other intelligence resources**

Cyber Threat Hunting

Cyber Threat Hunting

Process that is put in place in order to tackle (hunt) this kind of sophisticated threat.

- **User/Entity behaviour analytics**
- **Other intelligence resources**

***non-conventional sophisticated techniques need to be employed due to the fact that this is no common threat, it spans in time and keeps evolving.**

Know-How

Understanding such complex attacks requires a lot of knowledge in order to design and develop strategies and defense mechanisms.

What we need is a knowledge framework that will assist us in developing a set of semantic indicators.

- **Define and understand the context of the attack.**
- **Initiate the appropriate countermeasure.**

Semantic indicators

Semantic indicators are clues or signals within a set of data that provide insights into the **meaning**, **context**, or **intent** behind the information. These indicators help users interpret and understand the content more accurately.

Threat intelligence analysis to identify:

- **patterns,**
- **trends,**
- **anomalies**

that may indicate malicious activity or suspicious behavior.

MITRE ATT&CK

Curated knowledge base and framework that categorizes the tactics, techniques, and procedures used by adversaries during cyber attacks.

Developed by MITRE Corporation, a nonprofit organization that operates federally funded research and development centers, ATT&CK provides a comprehensive taxonomy of cyber threats based on real-world observations and expert analysis.

MITRE ATT&CK

Curated knowledge base and framework that categorizes the tactics, techniques, and procedures used by adversaries during cyber attacks.

Developed by MITRE Corporation, a nonprofit organization that operates federally funded research and development centers, ATT&CK provides a comprehensive taxonomy of cyber threats based on real-world observations and expert analysis.

Started in 2013 with the purpose of documenting common tactics, techniques and procedures against Windows enterprise networks and nowadays it spans almost all main enterprise solutions and also provides mitigations strategies.

MITRE ATT&CK - The TTP trio

Tactics, Techniques and Procedures

MITRE ATT&CK - The TTP trio

Tactics

Tactics represent the high-level objectives or goals that adversaries aim to achieve during a cyber attack. They describe the strategies employed by attackers to accomplish their mission.

Example:

- **gaining initial access to a target network,**
- **establishing persistence,**
- **escalating privileges,**
- **exfiltrating data,**
- **disrupting operations.**

Tactics serve as the primary categories for organizing and classifying adversary behavior.

MITRE ATT&CK - The TTP trio

Techniques

Techniques are the specific methods or procedures used by adversaries to achieve each tactic. They describe the step-by-step actions taken by attackers to accomplish their objectives.

Example:

Techniques under the "initial access" tactic may include:

- **phishing emails,**
- **exploiting software vulnerabilities,**
- **leveraging stolen credentials to gain entry into a target network**

MITRE ATT&CK - The TTP trio

Procedures (sub-techniques)
Variations or specific implementations of techniques that further refine the behaviors observed in cyber attacks.
They provide additional granularity and detail to techniques, allowing for more precise analysis and detection of adversary activity. Procedures describe specific ways in which techniques are executed or customized by attackers to suit their objectives or adapt to the target environment.

Example:
A procedure under the "exploitation of remote services" technique may involve exploiting a specific vulnerability in a web server software to gain unauthorized access.

APTs nature

Rely on subtle and slow operations and as such **traditional detection techniques** might fail.

What is needed?

APTs rely on subtle and slow operations.

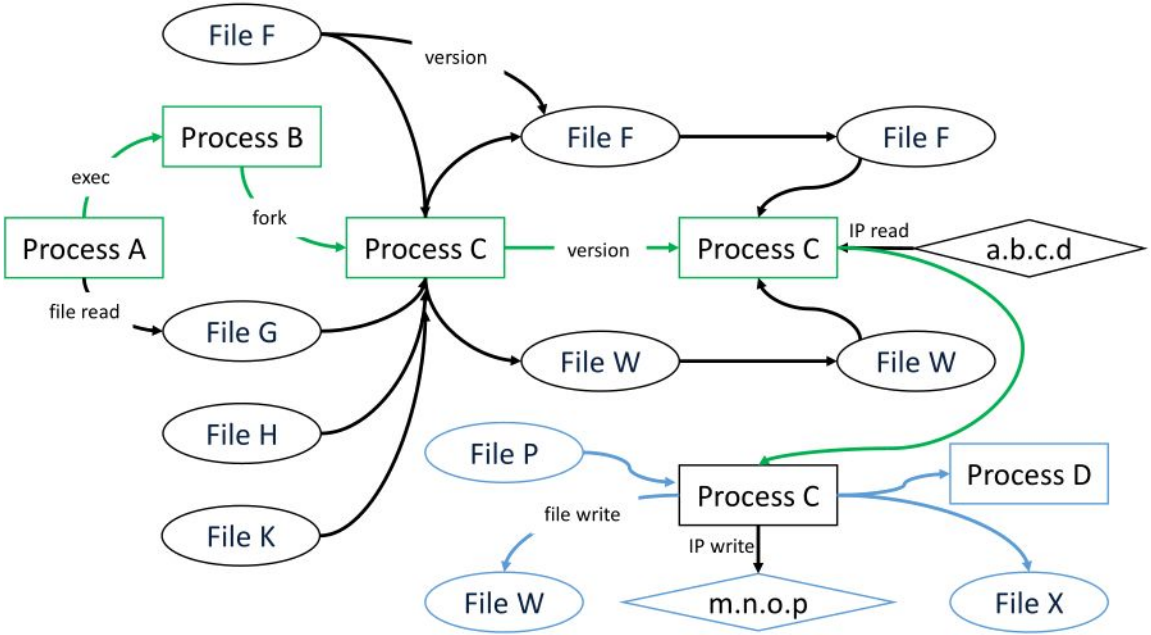
This brings a lot of challenges for a detection technique because:

- **Real time operation**
- **Able to focus on context**
- **Need to capture relation (cause-event) between (long-term) activities**
- **Low false positive rate**
- **Possibly detect attacks without prior knowledge**

What is needed? Provenance

What is needed? Provenance

Provenance Graphs: Represent system execution as a Directed Acyclic Graph that describes information flow and causality (edges) between kernel objects (vertices, e.g., processes, files, sockets).

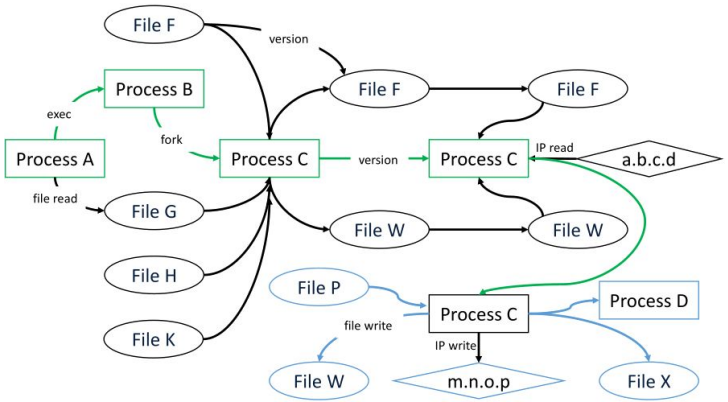


Provenance Graphs

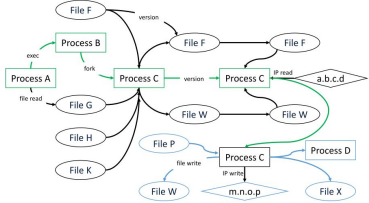
Provenance Graphs: Represent system execution as a Directed Acyclic Graph that describes information flow and causality (edges) between kernel objects (vertices, e.g., processes, files, sockets).

Provenance Graphs:

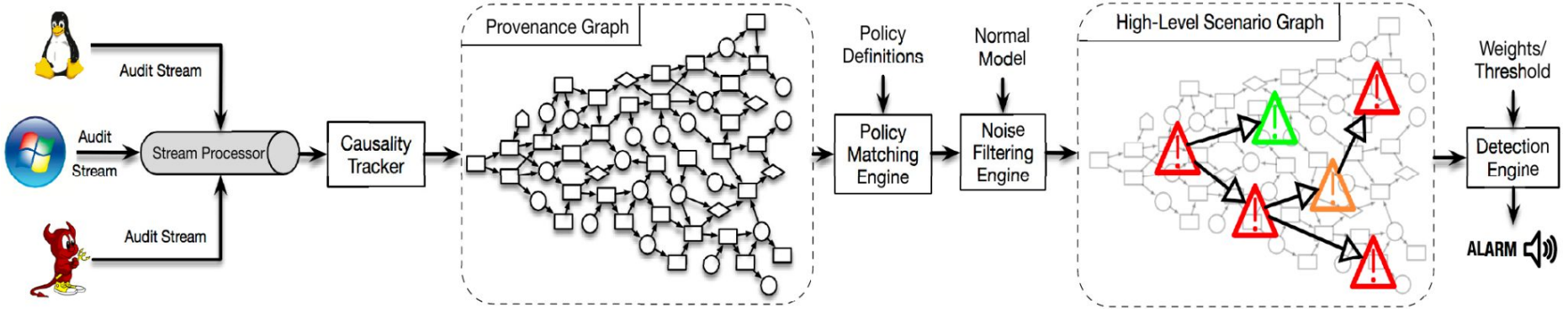
- Enable long term behaviour monitoring and eventually detection due to the connection of casually-related events in the data provenance graph.
- Provide information-rich context that can be used to better distinguish between benign/malicious events.



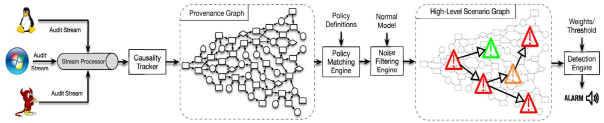
Approaches relying on provenance graphs



Aim: Generation or a high-level graph that represents the attacker actions and thus makes it easier to spot and mitigate (possibly in real-time).

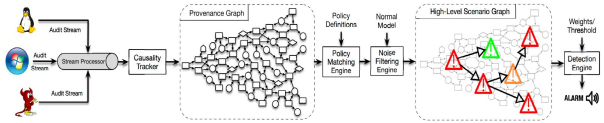


Steps



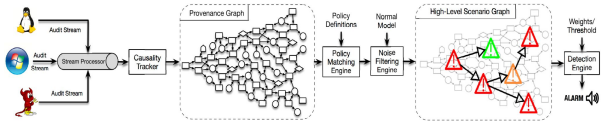
- **Alert generation**
  - Map low-level events to generate semantically close alerts to the attackers behaviour (in our case to TTPs)

Steps



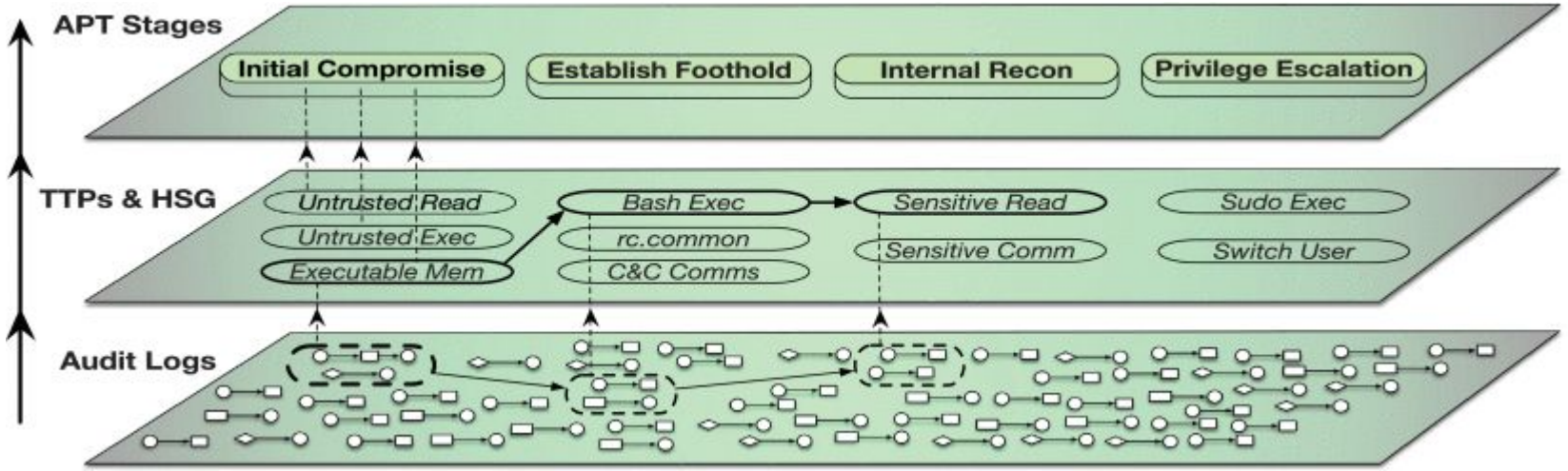
- **Alert generation**
  - Map low-level events to generate semantically close alerts to the attackers behaviour (in our case to TTPs)
- **Alert Correlation**
  - Take into account the flow of information between files/processes to generate a high-level scenario graph (HSG) where nodes correspond to TTPs and edges represent information flows between entities consisted in the TTPs

Steps



- **Alert generation**
  - Map low level events to generate semantically close alerts to the attackers behaviour (in our case to TTPs)
- **Alert Correlation**
  - Take into account the flow of information between files/processes to generate a high-level scenario graph (HSG) where nodes correspond to TTPs and edges represent information flows between entities consisted in the TTPs
- **Attack detection and HSG presentation**
  - Use the HSG to compute a “threat score” and raise an alarm if a predefined threshold is surpassed. The HSG is also presented to the cyber-analyst team for further processing.

Mapping the information



Utilize Mitre ATT&CK framework to map low-level system events to an intermediate high-level representation that can be then easily mapped to an APT campaigns' phases.

Reading Material

1. Advanced Persistent Threats: Link-1, Link-2
2. Provenance based APT detection: Link-1, Link-2