Data and Network Security

(Master Degree in Computer Science and Cybersecurity)

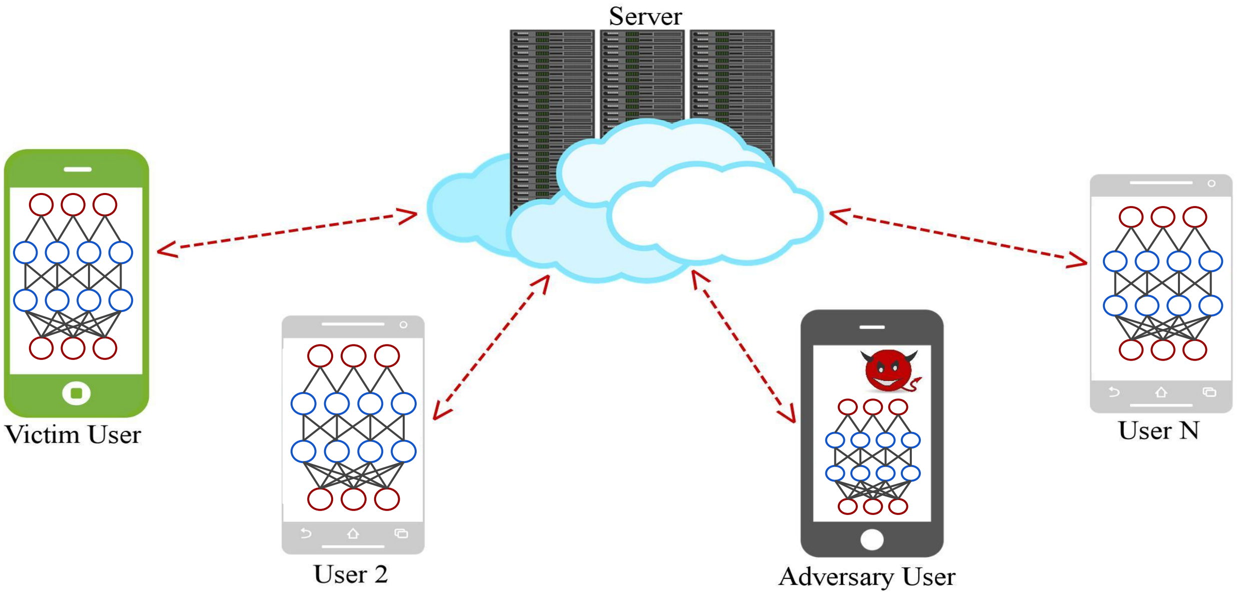
Lecture 6

SAPIENZA
UNIVERSITÀ DI ROMA

Outline for today

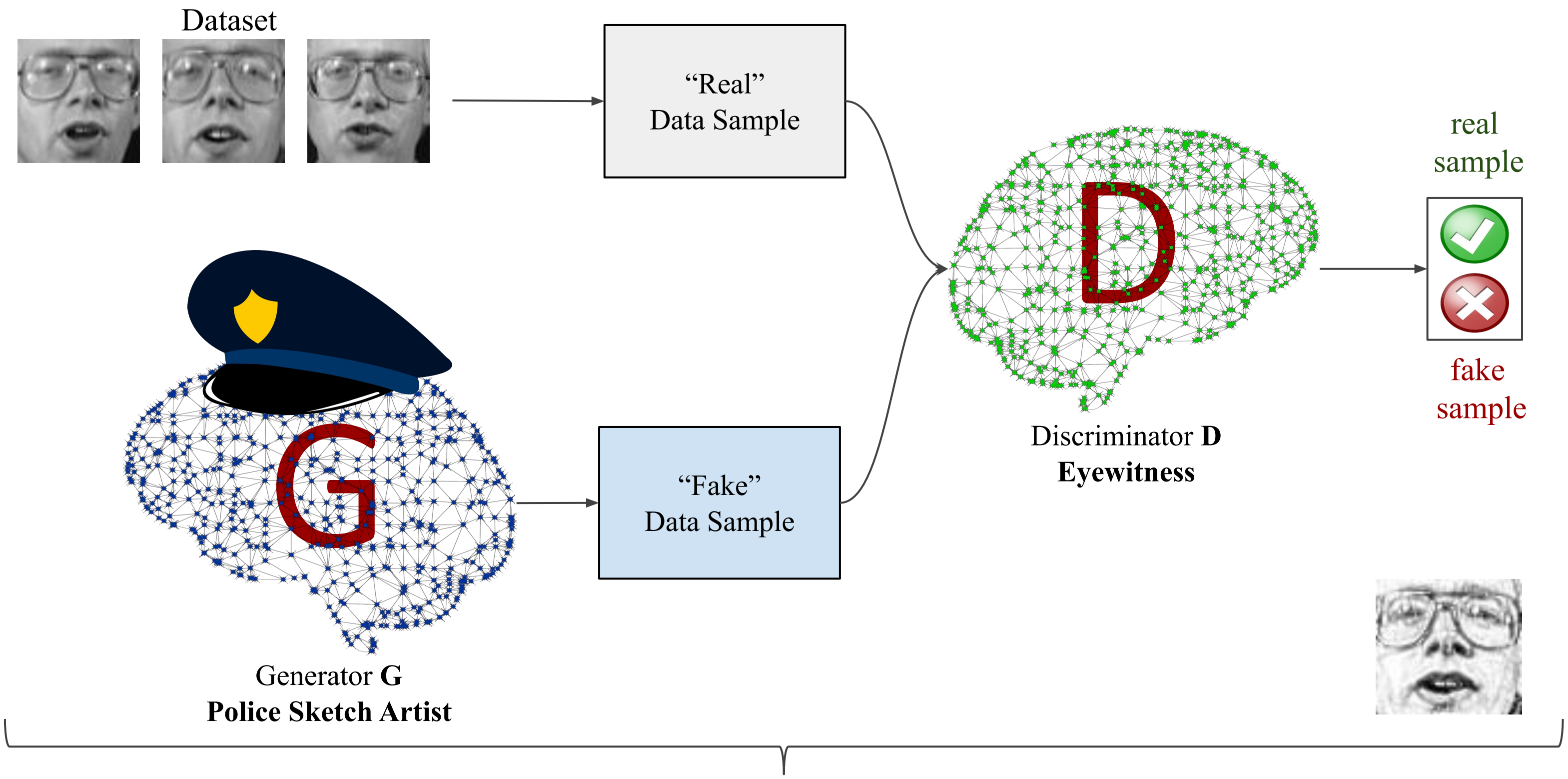
- Recap last lecture
- APTs

Collaborative Learning Scheme



Adversary's goal?
Reconstruct private samples from the dataset of the victim indirectly influencing the learning of other participants

Generative Adversarial Network



Dataset

"Real"
Data Sample

"Fake"
Data Sample

Discriminator **D**
Eyewitness

real
sample

fake
sample

Generator **G**
Police Sketch Artist

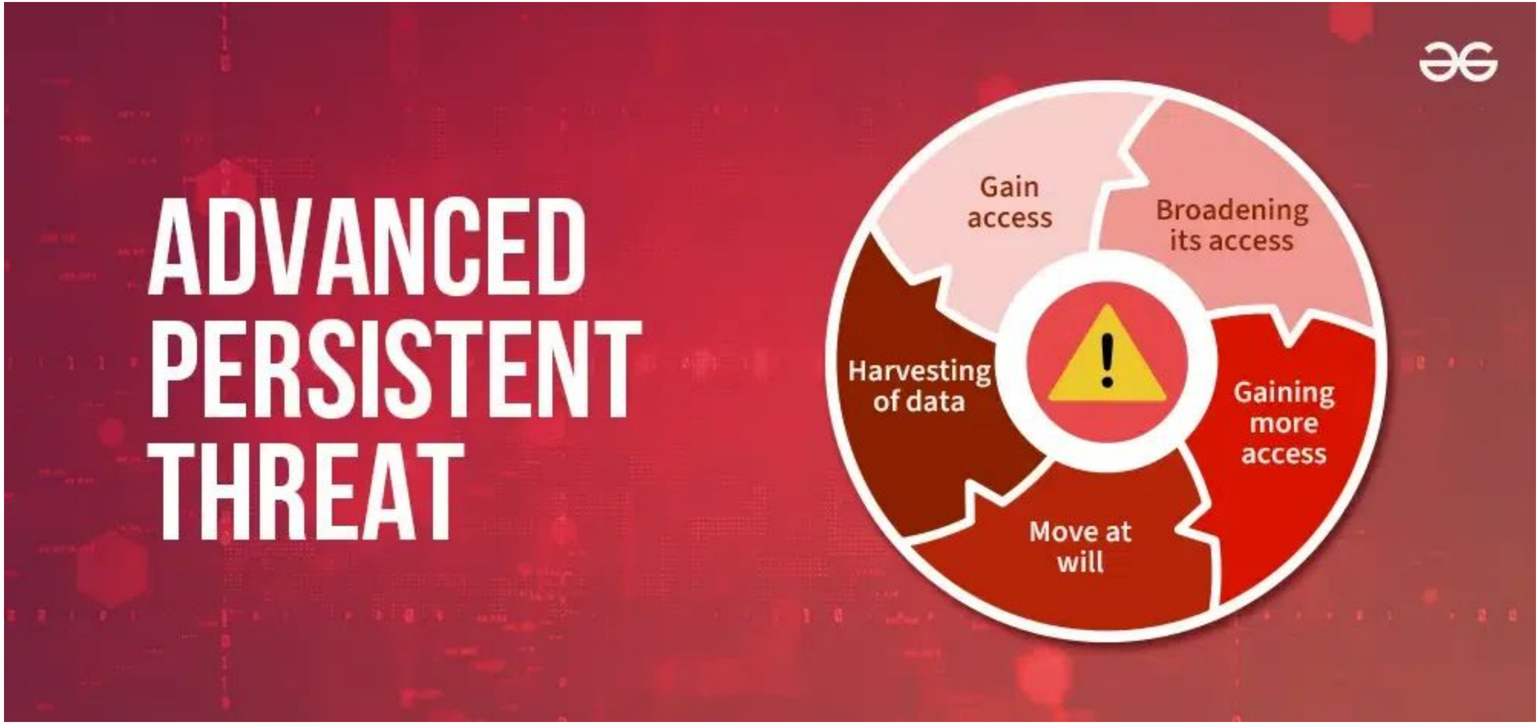
GAN Architecture

Outline for today

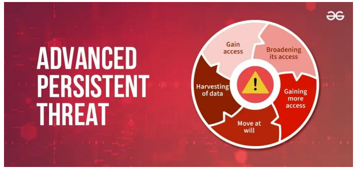
- Recap last lecture
- **APTs**

Not this...

This...

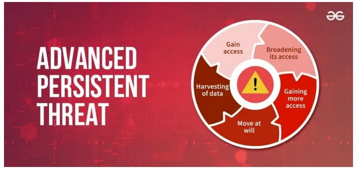

ADVANCED PERSISTENT THREAT
Gain access
Broadening its access
Gaining more access
Move at will
Harvesting of data

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:

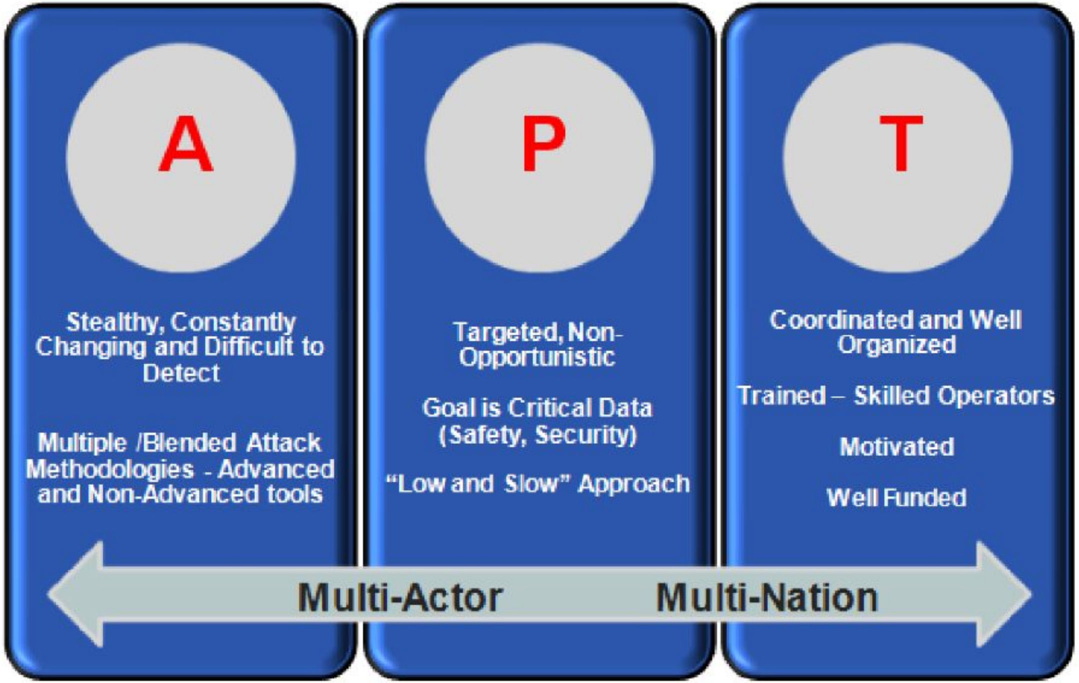
- short-lived
- indiscriminate

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



A

Stealthy, Constantly Changing and Difficult to Detect

Multiple /Blended Attack Methodologies - Advanced and Non-Advanced tools

P

Targeted, Non-Opportunistic

Goal is Critical Data (Safety, Security)

“Low and Slow” Approach

T

Coordinated and Well Organized

Trained – Skilled Operators

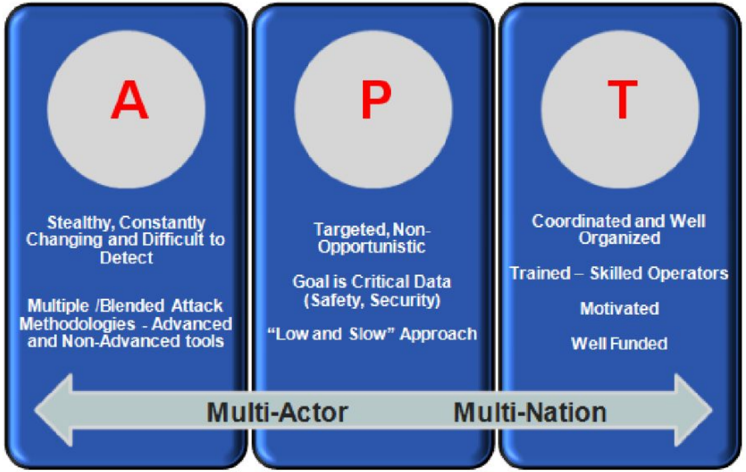
Motivated

Well Funded

Multi-Actor Multi-Nation

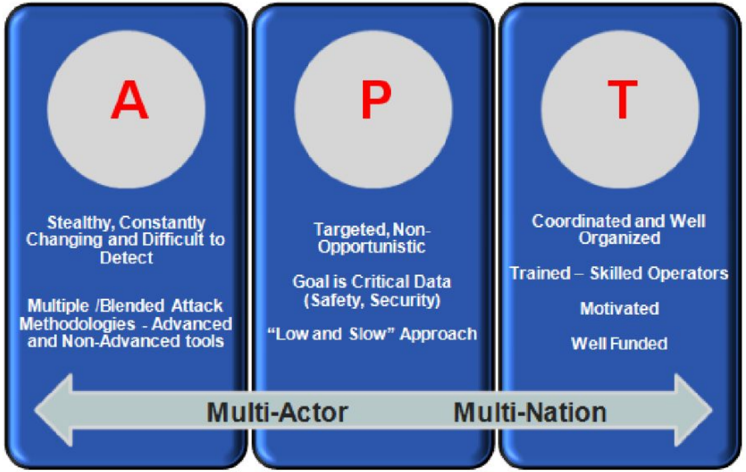
ADVANCED

The attack team has significant levels of expertise and significant resources, allowing the use of multiple and elaborated different attack vectors.


A
Stealthy, Constantly Changing and Difficult to Detect
Multiple /Blended Attack Methodologies - Advanced and Non-Advanced tools
P
Targeted, Non-Opportunistic
Goal is Critical Data (Safety, Security)
"Low and Slow" Approach
T
Coordinated and Well Organized
Trained – Skilled Operators
Motivated
Well Funded
Multi-Actor
Multi-Nation

PERSISTENT

The attack team operates in order to remain present and undetected within the organization as long as possible



A

Stealthy, Constantly Changing and Difficult to Detect

Multiple /Blended Attack Methodologies - Advanced and Non-Advanced tools

P

Targeted, Non-Opportunistic

Goal is Critical Data (Safety, Security)

"Low and Slow" Approach

T

Coordinated and Well Organized

Trained – Skilled Operators

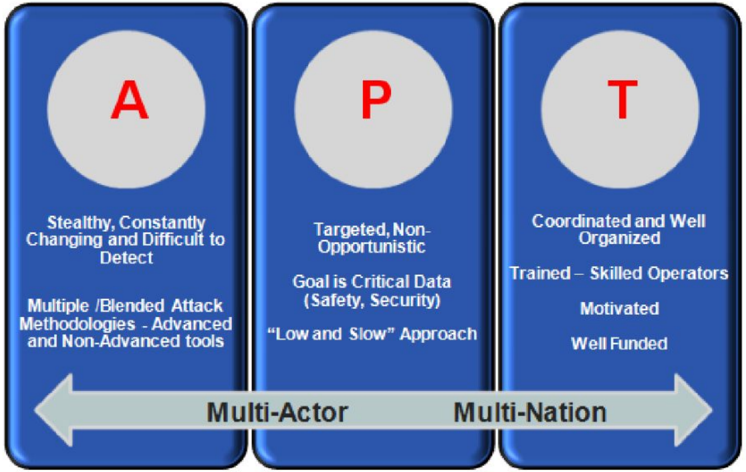
Motivated

Well Funded

Multi-Actor Multi-Nation

THREAT

Potential to adversely impact organizational operations, their assets, or individuals.



A

Stealthy, Constantly Changing and Difficult to Detect

Multiple /Blended Attack Methodologies - Advanced and Non-Advanced tools

P

Targeted, Non-Opportunistic

Goal is Critical Data (Safety, Security)

"Low and Slow" Approach

T

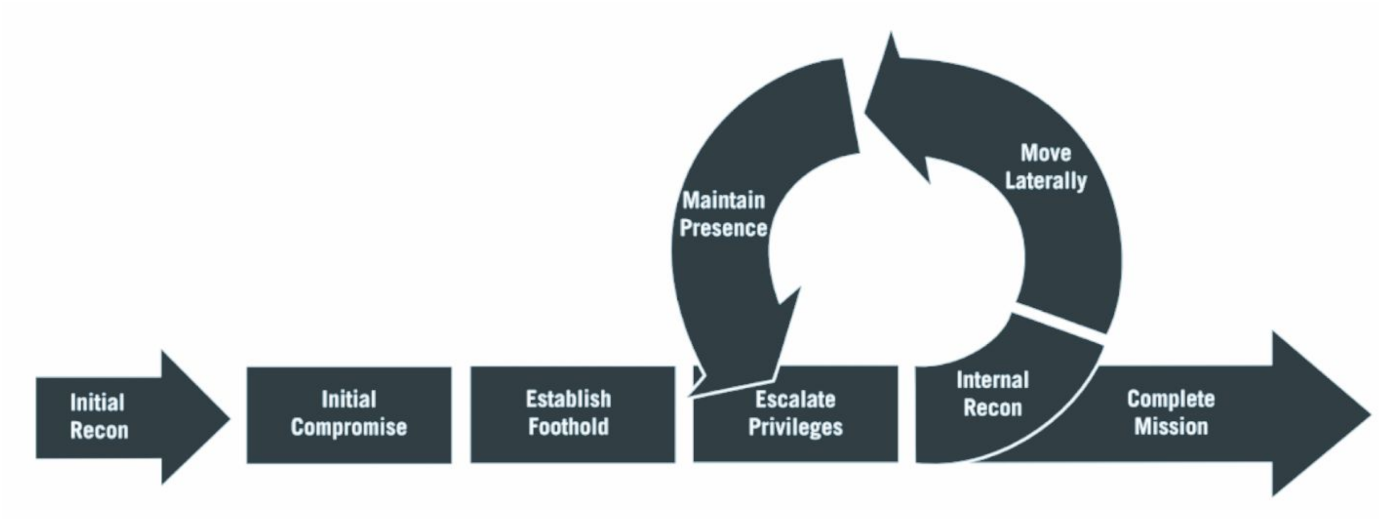
Coordinated and Well Organized

Trained – Skilled Operators

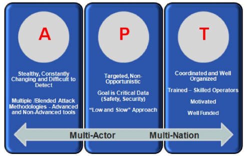
Motivated

Well Funded

APT - Life Cycle



Why APTs?



A

Stealthy, Constantly Changing and Difficult to Detect

Multiple /Blended Attack Methodologies - Advanced and Non-Advanced tools

P

Targeted, Non-Opportunistic

Goal is Critical Data (Safety, Security)

"Low and Slow" Approach

T

Coordinated and Well Organized

Trained – Skilled Operators

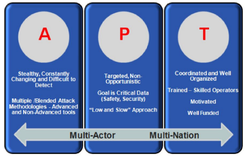
Motivated

Well Funded

Multi-Actor Multi-Nation

- Economic espionage
- Political espionage
- Ideological motivations

Why APTs?



A

Stealthy, Constantly Changing and Difficult to Detect

Multiple /Blended Attack Methodologies - Advanced and Non-Advanced tools

P

Targeted, Non-Opportunistic

Goal is Critical Data (Safety, Security)

"Low and Slow" Approach

T

Coordinated and Well Organized

Trained – Skilled Operators

Motivated

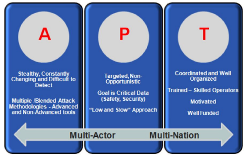
Well Funded

Multi-Actor Multi-Nation

- **Economic espionage**

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

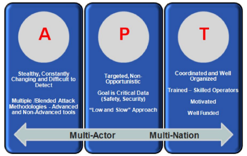
Why APTs?


A
Stealthy, Constantly Changing and Difficult to Detect
Multiple /Blended Attack Methodologies - Advanced and Non-Advanced tools
P
Targeted, Non-Opportunistic
Goal is Critical Data (Safety, Security)
"Low and Slow" Approach
T
Coordinated and Well Organized
Trained – Skilled Operators
Motivated
Well Funded
Multi-Actor
Multi-Nation

- **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?



A

Stealthy, Constantly Changing and Difficult to Detect

Multiple /Blended Attack Methodologies - Advanced and Non-Advanced tools

P

Targeted, Non-Opportunistic

Goal is Critical Data (Safety, Security)

"Low and Slow" Approach

T

Coordinated and Well Organized

Trained – Skilled Operators

Motivated

Well Funded

Multi-Actor Multi-Nation

- **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 (Adversarial Tactics, Techniques, and Common Knowledge)

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.

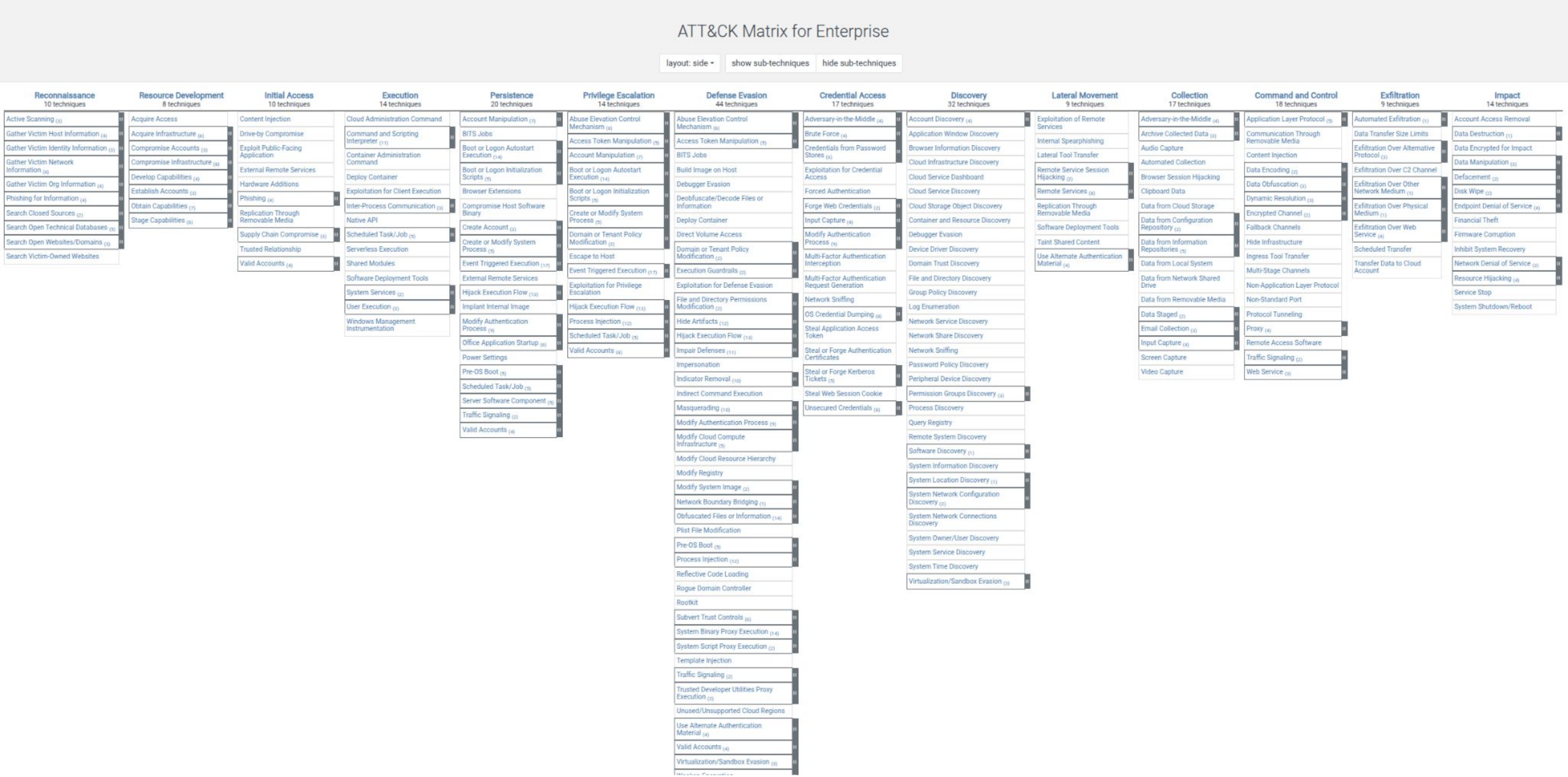
MITRE ATT&CK

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



ATT&CK Matrix for Enterprise

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 44 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (5)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (11)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (1)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Create or Modify System Process (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Domain or Tenant Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (5)	Escape to Host	Direct Volume Access	Modify Authentication Process (9)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Scheduled Transfer	Financial Theft
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (17)	Event Triggered Execution (17)	Domain or Tenant Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (5)	Hide Infrastructure	Transfer Data to Cloud Account	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (2)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Ingress Tool Transfer		Inhibit System Recovery
			Software Deployment Tools	Hijack Execution Flow (13)	Hijack Execution Flow (13)	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels		Network Denial of Service (2)
			System Services (2)	Implant Internal Image	Process Injection (12)	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	File and Directory Discovery		Data from Removable Media	Non-Application Layer Protocol		Resource Hijacking (4)
			User Execution (3)	Modify Authentication Process (9)	Scheduled Task/Job (5)	Hide Artifacts (12)	Steal Application Access Token	Group Policy Discovery		Data Staged (2)	Non-Standard Port		Service Stop
			Windows Management Instrumentation	Office Application Startup (6)	Valid Accounts (4)	Hijack Execution Flow (13)	Steal or Forge Authentication Certificates	Log Enumeration		Email Collection (3)	Protocol Tunneling		System Shutdown/Reboot
				Power Settings		Impair Defenses (11)	Steal or Forge Kerberos Tickets (5)	Network Service Discovery		Input Capture (4)	Proxy (4)		
				Pre-OS Boot (5)		Impersonation	Steal Web Session Cookie	Network Share Discovery		Screen Capture	Remote Access Software		
				Scheduled Task/Job (5)		Indicator Removal (10)	Unsecured Credentials (8)	Network Sniffing		Video Capture	Traffic Signaling (2)		
				Server Software Component (5)		Indirect Command Execution		Password Policy Discovery			Web Service (3)		
				Traffic Signaling (2)		Masquerading (10)		Peripheral Device Discovery					
				Valid Accounts (4)		Modify Authentication Process (9)		Permission Groups Discovery (3)					
						Modify Cloud Compute Infrastructure (5)		Process Discovery					
						Modify Cloud Resource Hierarchy		Query Registry					
						Modify Registry		Remote System Discovery					
						Modify System Image (2)		Software Discovery (1)					
						Network Boundary Bridging (1)		System Information Discovery					
						Obfuscated Files or Information (14)		System Location Discovery (1)					
						Plist File Modification		System Network Configuration Discovery (2)					
						Pre-OS Boot (5)		System Network Connections Discovery					
						Process Injection (12)		System Owner/User Discovery					
						Reflective Code Loading		System Service Discovery					
						Rogue Domain Controller		System Time Discovery					
						Rootkit		Virtualization/Sandbox Evasion (3)					
						Subvert Trust Controls (6)							
						System Binary Proxy Execution (14)							
						System Script Proxy Execution (2)							
						Template Injection							
						Traffic Signaling (2)							
						Trusted Developer Utilities Proxy Execution (3)							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material (4)							
						Valid Accounts (4)							
						Virtualization/Sandbox Evasion (3)							
						Weaken Encryption							

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.

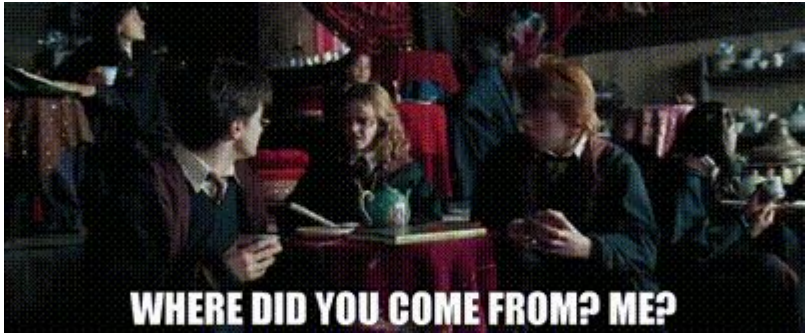
What is needed?

APTs rely on subtle and slow operations.

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

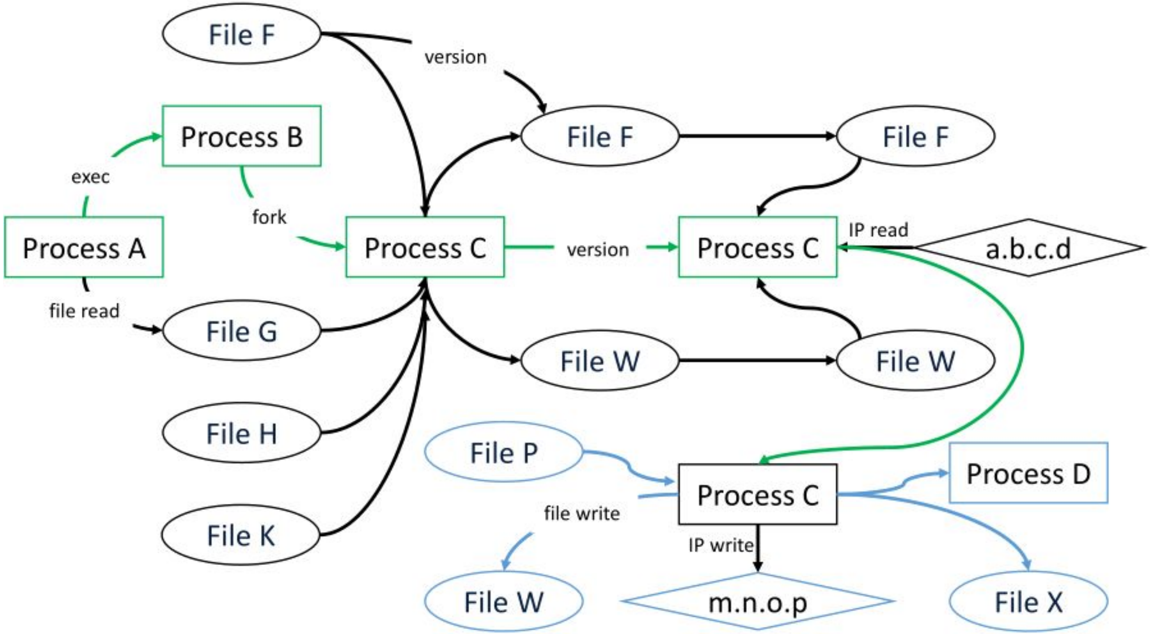
- Real time operation
- Able to focus on context
- Need to capture relation (cause-event) between (long-term) activities
- Low false positive rate
- Possibly detect attacks without prior knowledge

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).



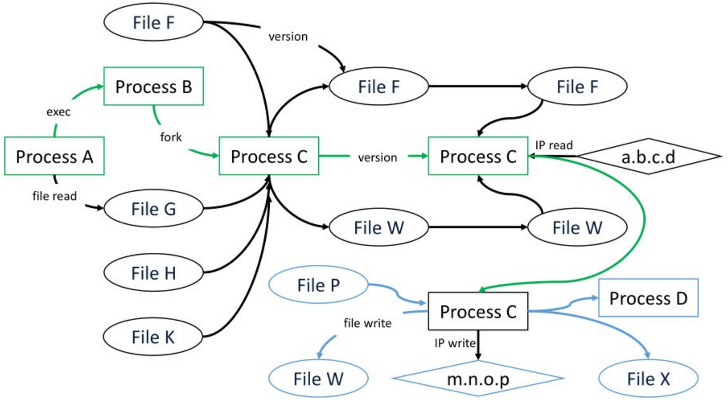
Provenance Graphs

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).

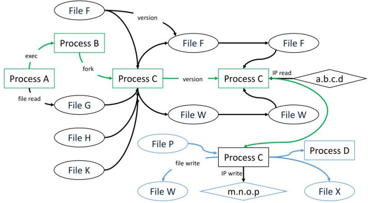
Provenance Graphs:

- Enable long term behaviour monitoring and eventually detection due to the connection of casually-related events in the data provenance graph.

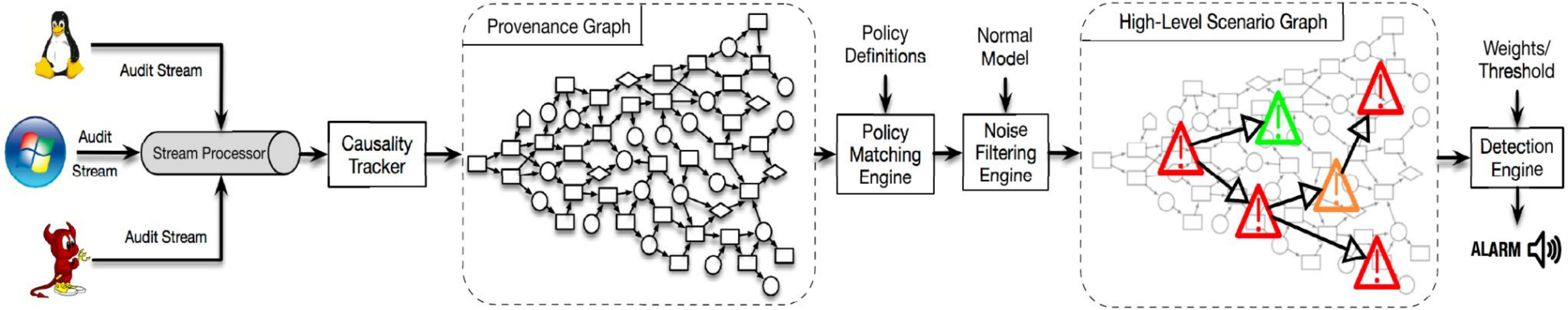
- Provide information-rich context that can be used to better distinguish between benign/malicious events.



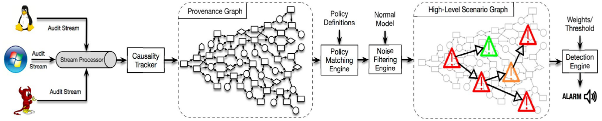
Approaches relying on provenance graphs



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).

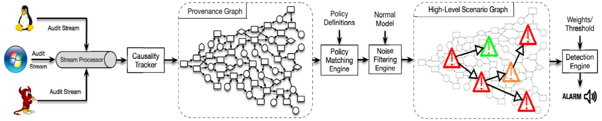


Steps



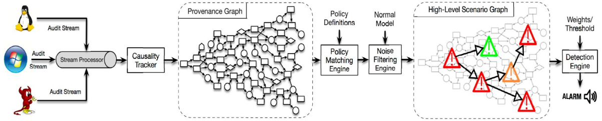
- **Alert generation**
  - Map low-level events to generate semantically close alerts to the attackers behaviour (in our case to TTPs)

Steps



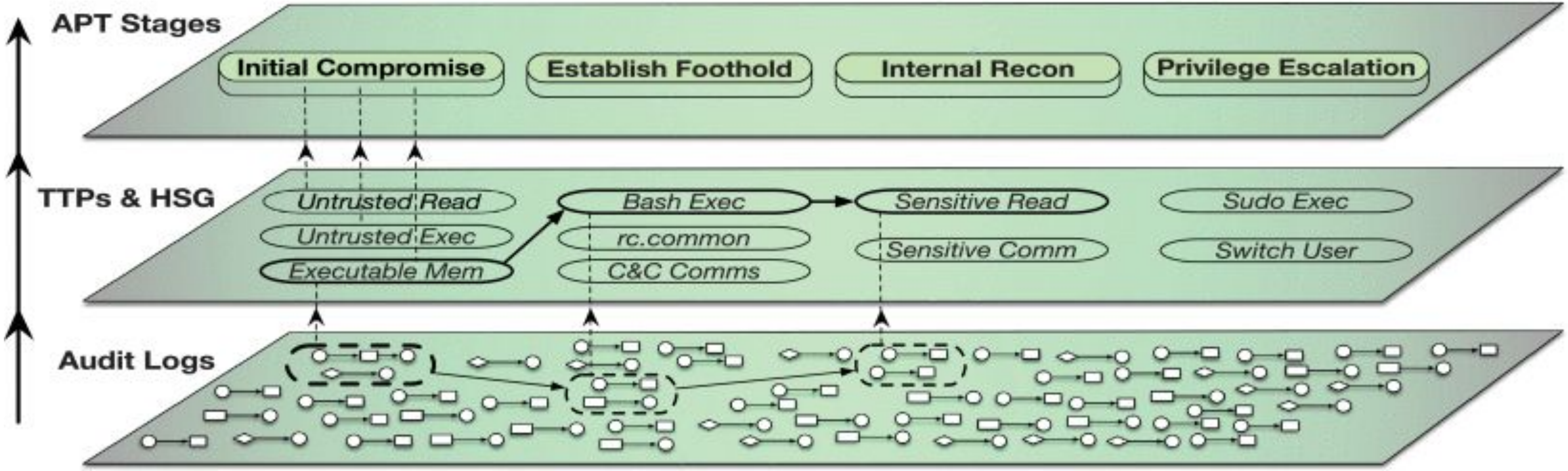
- Alert generation
  - Map low-level events to generate semantically close alerts to the attackers behaviour (in our case to TTPs)
- Alert Correlation
  - Take into account the flow of information between files/processes to generate a high-level scenario graph (HSG) where nodes correspond to TTPs and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