MITRE ATT&CK:
Climb to the top

Authors
Francesco Maria Ferazza, MSc (Royal Holloway, 2021)
Jorge Blasco Alis, ISG, Royal Holloway

Abstract

The purpose of this article is to explain what the MITRE ATT&CK framework is and how it has become the de-facto industry standard for describing cyber adversarial behaviour. The article will illustrate why it was created, why it can be considered a burgeoning cyber security ontology, and finally how it ended up being the one of the most respected and widespread frameworks. A thorough understanding of the MITRE ATT&CK framework and of its uses can be beneficial to cyber security enthusiasts and professionals at all levels: technical, managerial, and board. The article is written with such a broad audience in mind and as such won't linger on overly technical details.[a]

[a]This article is published online by Computer Weekly as part of the 2022 Royal Holloway information security thesis series https://www.computerweekly.com/ehandbook/MITRE-ATTCK-Climb-to-the-top. It is based on an MSc dissertation written as part of the MSc in Information Security at the ISG, Royal Holloway, University of London. The full thesis is published on the ISG's website at https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/isg-technical-reports/.

Introduction to the framework

The MITRE ATT&CK framework was born in 2013 as a spin-off of MITRE's Fort Meade eXperiment (FMX). FMX was a research environment used to emulate both adversarial and defender behaviours in an effort to use telemetry and behavioural analysis to improve post-compromise detection of threats. To do so, a scientifically-sound way to catalogue and document adversarial behaviour was deemed necessary. The MITRE ATT&CK framework was born to fulfil that duty. It is meant to be a curated and globally shared knowledge base of adversarial tactics, techniques, and procedures, providing a common representation of both attacks and defences to enable better threat modelling, cyber threat intelligence, adversarial emulation, and red teaming.

At a higher level, ATT&CK can be seen as a behavioural model that consists of the following core components: *tactics, techniques, softwares, procedures, adversarial groups*, and related *mitigations.* Let us briefly define what these core elements are.

Tactics are the tactical achievements an attacker aims for when performing an action. In other words, when malicious actors use techniques, the tactics are what they want to achieve.

Where tactics represent "why" an action is performed, **techniques** represent the "how". For example, exploiting a public-facing application would be a technique used to obtain the tactical goal (the tactic) of initial access.

Techniques and tactics: example

Drive-by downloads are a technique to reach the tactical objective of *initial access* to a system.

Procedures represent how specific adversaries implement the different techniques; their modus operandi and their **software** are listed. **Groups** are either threat groups, threat actors, intrusion sets, or malware families performing targeted, advanced, and persistent activity. **Mitigations** are all known controls, safeguards, and countermeasures that can be put in place to prevent techniques from being carried out successfully.

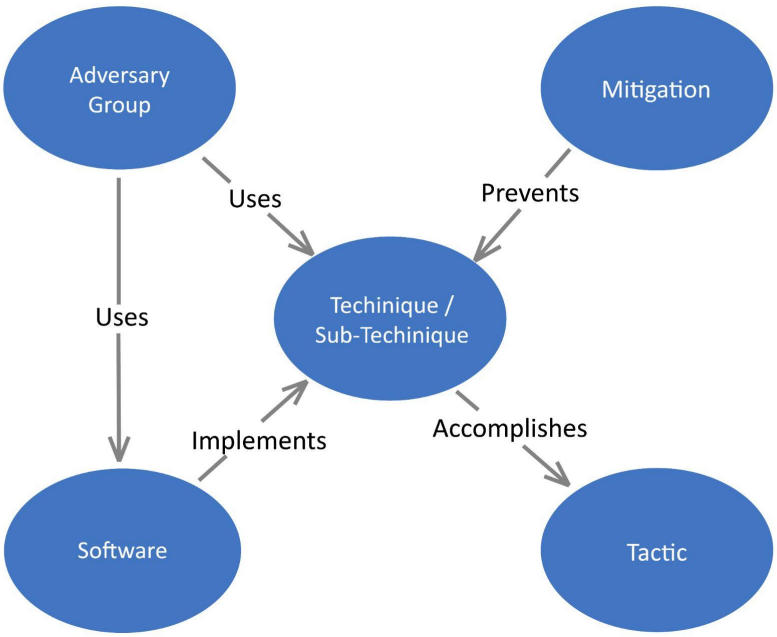

Figure 1: Relationship between the core elements.

All these core elements correlate with each other and can be used to describe adversarial behaviour during an attack or a campaign. Figure 1 gives a generic example of how these core elements correlate.

Figure 2 gives the same picture, but filled with real TTPs, actors, software, and mitigations. It shows that **group** APT28[1] uses the **software** Mimikatz to perform the **technique** of "dumping OS credentials"[2], with the **tactical** goal of "obtaining credentials access"[3], and all of this can be prevented by implementing the **mitigation** "credential access protection"[4].

The ATT&CK framework precisely defines what its core elements are, but also strictly specifies the rigid object structure they should have, what their metadata should be, and how they relate to each other.

This makes the framework different from a simple taxonomy and closer to an ontology, the first cyber security ontology. This is because while a taxonomy simply classifies its contents, an ontology specifies them and how they relate.

What makes the framework so good?

The framework has become a de facto standard in the information security industry. Information security academics, analysts, researchers, defenders, and vendors are increasingly adopting MITRE ATT&CK as their go-to framework to describe adversarial behaviour and TTPs. It is now common to see huge security firms such as CrowdStrike, Kaspersky, or FireEye releasing reports and whitepapers consistently employing MITRE ATT&CK to document their findings. Similarly, government agencies around the globe are using the framework to disseminate their security warnings and recommendations.

[1] https://attack.mitre.org/groups/G0007/
[2] https://attack.mitre.org/techniques/T1003
[3] https://attack.mitre.org/tactics/TA0006
[4] https://attack.mitre.org/mitigations/M1043

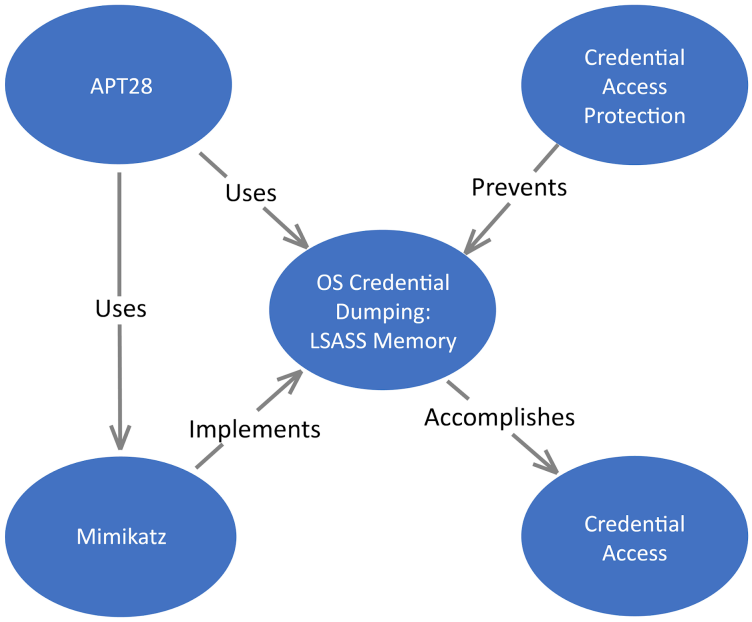

Figure 2: Relationship between the core elements with real actors.

Let us illustrate the many reasons behind this success.

It is easy to exchange and automate

MITRE ATT&CK fully supports STIX2[5], a language and serialisation format used to exchange cyber threat intelligence. First of all, this means that it is easy to exchange ATT&CK data between different organisations and actors. Sharing a bit of intelligence with STIX2 is as simple as sharing a JSON (JavaScript Object Notation) file.

Additionally, serialised data is much simpler to integrate within existing information and cyber security processes and tools. Moreover, automation, and realistic risk modelling and management can be achieved thanks to the ontology-like nature of the framework, its support of STIX2, and the application of semantic reasoners.

It can adapt to various maturity levels

The framework is extremely versatile, for it can be used by individuals and teams at both the tactical, operational, and strategic levels of organisations and at various degrees of maturity. The entry level requirements to start using it are very low.

A basic user can employ it as a simple reference and knowledge base of known TTPs, groups, and mitigations. That is as easy as browsing the ATT&CK web site[6] and searching the matrix relevant to your domain of interest (enterprise, mobile, ICS). (The links previously provided in the article point to the MITRE ATT&CK framework website and show how useful and easy to consult it can be.)

More advanced teams might use MITRE ATT&CK to create fully automated processes to analyse intrusions, understand their enemies cyber kill chains, deploy specific defences, and share their cyber threat intelligence findings with peer organisations. The sky's the limit here!

[5] https://oasis-open.github.io/cti-documentation/stix/intro.html
[6] https://attack.mitre.org/

It is open, curated, and routinely updated

One of the biggest pros of the framework is that it is completely open source, for it was designed to be a "curated and globally shared knowledge base" of adversarial behaviours. Everyone can access and query it when looking for information about a specific adversarial tactic, technique, or procedure.

The MITRE corporation even supplies a public TAXII API to do so and, furthermore, provides Python code snippets showing how simple it is to query that endpoint. Security researchers from all around the world can also contribute to the framework's knowledge base, for the MITRE group is always accepting external contributions. Techniques, sub-techniques, cyber threat intelligence, and data source contributions are the most welcome and submitting them is extremely easy.

The framework has seen many updates over the years, it started with a focus on windows enterprise systems only, and has now expanded to cover also other operative systems, mobile devices, and even ICS/SCADA environments. Major updates to the framework happen roughly twice a year.

It works well with other threat models

The MITRE ATT&CK framework is not mutually exclusive with other threat models such as Microsoft STRIDE or Lockheed Martin's Cyber Kill Chain; it can actually be employed alongside them. This is true because those models have different abstraction layers and are used to provide different services.

For example, the Cyber Kill Chain has a higher abstraction level, useful to understand high-level adversarial processes, goals, patterns, intents. However, it lacks the notions required by the defenders to describe hostile actors' tactical goals, techniques, modi operandi, procedure, and related mitigations. Those elements are better described with a mid-level abstraction model such as the MITRE ATT&CK framework with its strict relational structure and filled with the intelligence gathered from several millions of real-world, documented and catalogued, intrusions.

A scenario to better illustrate the above statement:

- A privilege escalation is being reported by the SOC of an organisation.
- Analysts using the Cyber Kill Chain can reconstruct the phases preceding the privilege escalation and can try to synthesise information about the next step of the attacker.
- However, the kill chain approach has no notion of the exact techniques and procedures used.
- Analysts will need MITRE's framework to describe the detailed adversarial behaviour and to answer questions like "What technique did the attacker use to escalate privileges? How was that technique implemented? What are the suggested mitigations?".
- In this scenario, for example, the malicious actor might have escalated privileges by Abuse of Elevation Control Mechanisms (MITRE ATT&CK technique) and more specifically by exploiting Setuid and Setgid (MITRE ATT&CK MITRE sub-technique).

In this abstraction-based representation (Figure 3), an even lower tier is possible, and that would be represented by vulnerability (or malware) databases, where specific software and code examples are found, but completely devoid of any intrusion analysis context dimension, such as TTPs, adversarial intent, etc.

Using different intrusion analysis models at different abstraction layers will grant analysts and defenders a much more comprehensive view of the threat landscape and of their adversaries' actions.

Figure 3: Abstraction

It is versatile

The MITRE ATT&CK framework can improve many information and cyber security processes within an organisation. It clearly is a tool that can be used to enhance cyber threat intelligence activities: as we have previously seen the framework supports STIX, which makes it even easier to exchange data and information and to automate certain processes of the intelligence lifecycle.

Additionally, since the MITRE ATT&CK framework contains information about real-world documented TTPs employed by actual groups, it can be used to perform better adversary emulation exercises.

As a tool to analyse intrusions and attack paths, it can be leveraged by organisations to perform better defensive gap assessments, identifying weak spots in their defences against real-world threats, with the result of prioritising the most important controls in a cost-efficient way.

Some organisations are even employing the MITRE ATT&CK framework to enhance their cyber attribution capabilities.

In order to recap the previous five points, here is a short list of the reasons that made the framework successful:

- It is easy to exchange and automate.
- It can adapt to different maturity levels.
- It is open, curated, routinely updated.
- It works well with other threat models.
- It is versatile.

Conclusion

The adoption rate within the cyber security industry of the MITRE ATT&CK framework has been steadily growing in the past years and we can expect this trend to keep growing. Every month, more

and more vendors, researchers, academics, and defenders are integrating the framework within their security processes, studies, and reports.

The pros listed previously are the main reason for this success: the MITRE ATT&CK is a global knowledge base of documented adversarial behaviours, curated by a highly reputable corporation, routinely updated, and easy to automate and interface with existing information security technologies and processes.

ATT&CK is so solid, widespread, and future-proof that it is already being used as the foundation of new information security frameworks such as D3FEND, released by MITRE in August 2021, funded and endorsed by the NSA. MITRE D3FEND is a vendor agnostic knowledge graph of all known countermeasures that can be employed to defend against the techniques and sub-techniques listed in its MITRE ATT&CK counterpart; its countermeasures are literally mapped to ATT&CK techniques.

We can expect MITRE ATT&CK to keep growing, to become a fully-fledged cyber security ontology, and to serve as the foundation of newer, just as remarkable, cyber security tools.

Biographies

Francesco Ferazza has been the Director of Operations of Ziff Davis Global Partners for the past 8 years. He is also a visiting lecturer for the Information Security distance learning MSc at the Royal Holloway, University of London and a senior cyber security analyst at “Analytica for intelligence and security studies”, an Italian think tank. Francesco loves anything that has to do with cyber threat intelligence, cyber security ontologies, Advanced Persistent Threats, FIN groups, Python and Javascript coding. In his spare time, he volunteers as a paramedic in his hometown, Milan.

Jorge Blasco obtained his PhD from University Carlos III of Madrid in 2012. His dissertation was focused in the field of information security. After obtaining his PhD, Jorge worked as an assistant lecturer in University Carlos III of Madrid. In 2014, he moved to City, University of London, where he worked until 2016 as a Research Fellow in a project about application collusion. His main research interests include mobile malware, steganography and wearable devices. Jorge joined the Information Security Group in September 2016 and was was promoted to Senior Lecturer in 2019.

Series editor: S.- L. Ng