TAG CYBER

MAPPING CVE RECORDS TO THE ATT&CK FRAMEWORK

DR. EDWARD G. AMOROSO
DR. PAULO SHAKARIAN

The enterprise security benefit of mapping common vulnerabilities and exposures (CVEs) to the offensive tactics included in the MITRE ATT&CK framework is explained. On-going mapping work at CYR3CON is used to exemplify the process and its usefulness for cyber practitioners.

INTRODUCTION

One of the most useful methods in modern cybersecurity risk management involves keeping an accurate and detailed record of the threats, vulnerabilities, and attack methods that are applicable to the enterprise application, computing, and networking environments. Within an organization, this is performed in the context of a *vulnerability management* (VM) program, usually in conjunction with a locally supported cyber risk registry.

To assist with this important security task, which is especially challenging if only because of the enormous number of potential vulnerabilities and attack methods, research teams have tried to create frameworks and public repositories that can serve as a base for enterprise protection efforts. The MITRE organization has been particularly helpful in this regard, publishing useful models that are applied in practice today around the world.

Two especially meaningful such resources from the MITRE team are the *Common Vulnerabilities and Exposures* (CVE) list of known vulnerabilities,[1] and the *MITRE ATT&CK* framework,[2] which lists and organizes known tactics and techniques used by offensive cyber attackers. Both of these frameworks are well-known globally and are used frequently by cyber security practitioners and commercial vendors to help guide their day-to-day work.

The relationship between the CVE list and the ATT&CK framework is less well-known, however, which is unfortunate since the two resources can and should be used

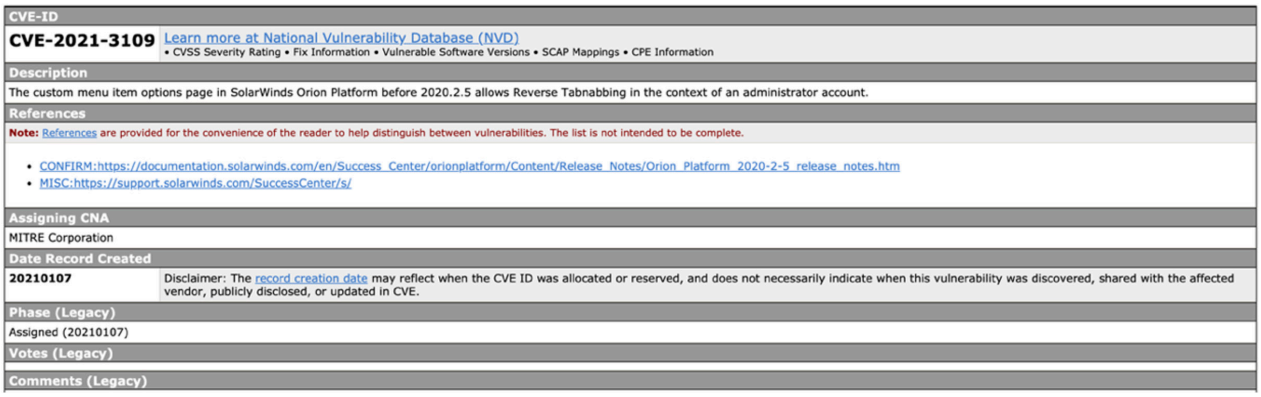
in coordination. In this report, we outline how such a mapping might be done by practitioners and vendors. We also offer a case study from CYR3CON[3], a commercial security vendor, which uses this type of mapping to help prioritize which vulnerabilities should be addressed in a given security program.

COMMON VULNERABILITIES AND EXPOSURES (CVE)

The CVE Program was created by MITRE in 1999 to help identify, define, and organize publicly disclosed cyber security vulnerabilities. Designated partner organizations agree to publish CVE records to ensure reasonably consistent descriptions of the vulnerabilities that are relevant to practitioners. The approach helps security teams coordinate how they should prioritize vulnerabilities for mitigation. The CVE database is free for use and download.[4]

The primary contribution of CVE is the standardization of cyber vulnerability and exposure descriptions. Having common CVE identifiers eases the problem of dealing with multiple sources (e.g., security information and event management (SIEM) platform, endpoint security) all referring to the same security issue, but with different descriptions and terminology. CVE normalizes these disparate references, which improves the sharing of security data across platforms, tools, and services.

Interestingly, the way CVE works is that it links together existing cyber vulnerability databases. That is, CVE records contain standard identifier information along with a brief description to related vulnerability advisories. A separate database called the US National Vulnerability Database (NVD) is used to provide more detailed information such as mitigation guidance, priority scoring, and other useful data. Below is a sample CVE record related to the recent SolarWinds incident.



CVE-ID

CVE-2021-3109 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

The custom menu item options page in SolarWinds Orion Platform before 2020.2.5 allows Reverse Tabnabbing in the context of an administrator account.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:https://documentation.solarwinds.com/en/Success_Center/orionplatform/Content/Release_Notes/Orion_Platform_2020-2-5_release_notes.htm
- MISC:https://support.solarwinds.com/SuccessCenter/s/

Assigning CNA

MITRE Corporation

Date Record Created

20210107 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20210107)

Votes (Legacy)

Comments (Legacy)

FIGURE 1. CVE Record Related to SolarWinds Incident

As one might expect, considerable debate has occurred about the respective pros and cons of exposing vulnerabilities so publicly. Hackers and nation state actors, for example, gain access to the same cyber security exposure data as the defenders, and this can have consequences. The general consensus, however, has been that sharing this data produces more benefits than risks – and the process has thus continued to grow in application and use.

MITRE ATT&CK

According to MITRE, ATT&CK is a *globally accessible knowledge base of adversary tactics and techniques* based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.[6] The framework includes over five hundred techniques, and each is associated with one or more of fourteen tactics, which correspond to different phases of an adversary attack.

Practitioners view the MITRE ATT&CK framework as consisting of an extensive knowledge base of adversary tactics and techniques used by cyber attackers. The framework is designed as a foundational base for defenders to build protections based on threat models from real-world observations. In practice, MITRE ATT&CK has been used effectively by enterprise security teams, as well as cyber security vendors building commercial products.

Unlike the CVE framework, MITRE ATT&CK does not reference reported vulnerabilities in specific products. Instead, it provides a more general overview of tactics and techniques – and this helps to broaden its applicability across a range of different scenarios. Endpoint security vendors, in particular, have used the framework to compare their relative performance in dealing with a standard set of tactics from the ATT&CK framework.[7]

FIGURE 2. MITRE ATT&CK Framework

The ATT&CK model can be viewed as providing an atomic view of the various components that make up offensive attacks and larger campaigns. The model organizes these atomic components into categories that correspond roughly to a typical offensive campaign. As such, the elements of the model are ripe for analysis, mapping, and other analysis tasks. In the next section, we outline how specific tactics might be mapped to vulnerabilities, and how this might be done using ATT&CK and CVE.

MAPPING STRATEGIES

The goal of any mapping strategy for security frameworks is to provide useful insights either for practitioners trying to disrupt adversaries or for vendors trying to build better security platforms. In either case, however, no one mapping methodology will cover every case. Nevertheless, we offer here some commentary on the great benefits of trying to make the connection – and we follow this up with a case study from a commercial vendor.

Mapping attack tactics to vulnerabilities introduces a more granular step in connecting vulnerabilities to attacks, not unlike related threat modeling work in place for many years.[8] Generally, the goal of any mapping is to support abstraction, where some concept (e.g., attack campaign) is represented in terms of its underlying components (e.g., vulnerabilities). The textbook view of such mapping starts with assets, maps to threats, extends to vulnerabilities, and then expands to attacks.[9]

HOW ATT&CK RELATES TO VULNERABILITY MANAGEMENT

MITRE ATT&CK is used by threat intelligence analysts in the SOC. The techniques included in the framework are aligned with behaviors observed in system logs and network traffic. ATT&CK allows

analysts to determine whether various patterns are associated with certain behaviors or threat groups. For example, an analyst can map network data from a SIEM to ATT&CK techniques, and to then create a chart showing which threat actors use those techniques. This method can provide a decision maker with insights into which threat actors may be conducting initial reconnaissance on the enterprise.

One area where different ATT&CK elements often differ is in their mapping to the physical world. For example, ATT&CK technique T1200 (Hardware Additions) involves an adversary introducing "computer accessories, computers, or networking hardware into a system or network that can be used as a vector to gain access." This has clear physical-world implications, whereas T1068 (Exploitation for Privilege Escalation) does not involve the physical world.

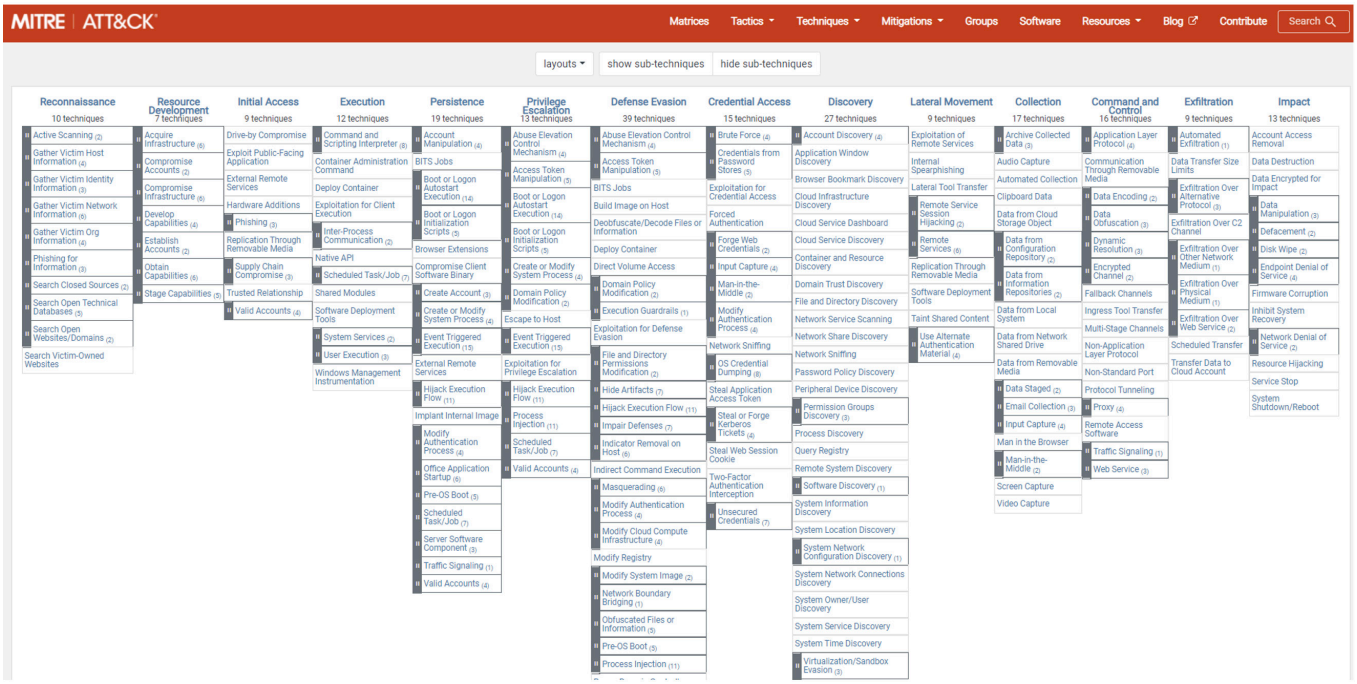


FIGURE 3. Screenshot of ATT&CK Listing Techniques Used and Associated Tactics

ALIGNING ATT&CK WITH CVES

In contrast to the ATT&CK framework, the Common Vulnerability Enumeration (CVE) system was created to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. As of the time of this writing, there are over 150,000 CVEs each associated with one or more pieces of software enumerated by a related taxonomy called the Common Platform Enumeration (CPE) system. In Q1 of 2021 there were about 4,419 published CVEs and an additional 9,455 reserved CVEs.

Today, there has been much work to map patterns of behavior from system logs and network traffic to the MITRE ATT&CK framework. Additionally, an increasing number of reports have been written about attacks that directly reference ATT&CK technique numbers. This is a good trend for defenders because a common taxonomy helps us analyze adversary actions using automated techniques spanning from database query visualization to advanced artificial intelligence.

There are some practical limitations to the use of ATT&CK, however. For example, mapping system log data and network traffic data to ATT&CK techniques will only cover a subset of the techniques. For example, tactic T1588.005 (Obtain Capabilities) deals with an attacker obtaining an exploit, which

occurs prior to even launching an attack. For this reason, the tactic cannot be directly associated with observables in system logs or network traffic.

Additionally, certain vulnerabilities can enable multiple techniques. For example, MITRE identifies many techniques as requiring privilege escalation in the ATT&CK framework and also identifies privilege escalation provided by certain vulnerabilities in the CVE framework. There are other examples of techniques directly enabled by vulnerabilities such as T1498 (Network Denial of Service) and T1212 (Exploitation for Credential Access).

CONSIDERATIONS IN ALIGNING CVES AND ATT&CK TECHNIQUES

Our discussion above focused on alignment of CVEs with ATT&CK techniques. In this section, we identify three practical considerations (identified in our own case study mapping work) that must be kept in mind when aligning the two paradigms.

- ***Not All MITRE ATT&CK Techniques Should Align to CVEs :*** Most MITRE ATT&CK techniques will have nothing to do with vulnerabilities. As part of the CYR3CON mapping (described below), the number of ATT&CK techniques associated with vulnerabilities was found to be roughly 25%. As techniques are chained together, however, it is possible to disrupt attacks involving non-vulnerability related techniques through remediation of CVEs. Thus, while most techniques will not be directly related to vulnerabilities, they remain relevant to the overall analysis.
- ***NIST/MITRE information about CVEs is not sufficient to align with ATT&CK :*** While the CVE standard contains metadata about vulnerabilities (such as software applicability), it does not contain all the information needed to provide the greatest insight into the relationship. An example is that often the CVE number for the vulnerability will be registered, but the standard information from NIST will not be available. Similarly, vulnerabilities might allow for the execution of techniques not enumerated in the CVE system, but that *are* classified in ATT&CK. In these cases, multi-sourced intelligence helps ensure useful alignment.
- ***Manual analysis for alignment will not scale :*** The CYR3CON mapping included data from vulnerability scans of tens of thousands of vulnerabilities, and each of these vulnerabilities was available for mapping to several of the hundreds of ATT&CK techniques. With thousands of new vulnerability disclosures each month, manual methods for alignment will not scale. Data science and machine learning methods become very important in such alignments as a result.Alerting the data owner of access or edit attempts.

CASE STUDY: USING CYR3CON INTELLIGENCE TO GENERATE ATTACK SEQUENCES

We've discussed how mapping ATT&CK techniques to CVEs can help vulnerability management teams disrupt sequences of techniques taken by attackers. Now, we take a step back to look at how such sequences can be generated in the context of a case study mapping at CYR3CON with the goal of generating attack sequences for improved intelligence.

Specifically, CYR3CON conducted a pilot involving analysis of over 700 security reports that each described adversarial techniques. The analysis associated those reports with the corresponding techniques. Using information about the techniques, such as applicable MITRE ATT&CK, computing platform, and required privileges, CYR3CON created a directed graph where two ATT&CK techniques are linked together with an arrow if the use of one was reported to proceed another. A subset of the resulting graph is shown in Figure 4 below.

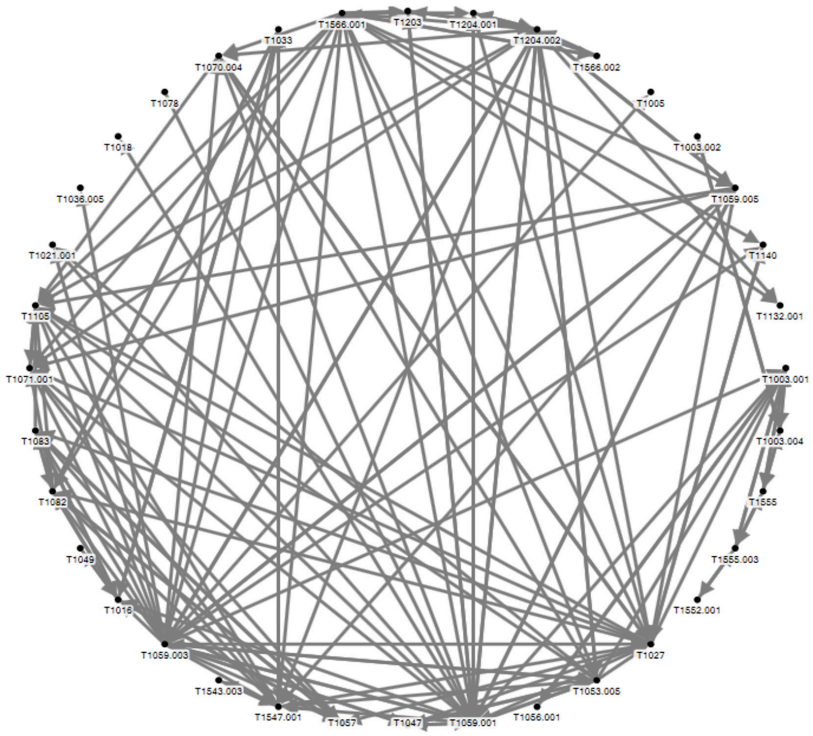


FIGURE 4. MITRE ATT&CK Directed Graph Mapping Visualization

Such mapped information enables various analytic approaches. For example, if ATT&CK techniques are observed by the SOC, or if they are available to an attacker due to an un-mitigated vulnerability, the relationships shown in the above visualization can be instantiated to that situation, representing what hackers previously had available to them. In addition, upon instantiation for a specific situation, the above representation can be unrolled to produce a list of possible sequences that an attacker can use. These, in turn, can further be analyzed through automated means for disruption.

Disrupting Attack Sequences

The CYR3CON mapping of relationships among ATT&CK techniques provided insights, based on historical reporting, into which ATT&CK techniques normally proceeded each other and/or used in tandem with each other. The resulting construct is what data scientists refer to as a graph, which is not the type that show the relationship between an X and Y variable, but rather a depiction of relationships.

As mentioned above, relationships can be unrolled, which means that potential attacker patterns can be observed in an automated way. With this level of understanding, one can look at how such patterns can be disrupted. Further, by mapping CVEs to ATT&CK techniques, analysts can understand which CVEs can play a potential role in an ATT&CK chain. As part of the CYR3CON mapping effort, attacker sequences were unrolled and examined to determine which vulnerabilities can be remediated to disrupt such attach chains. The below figure shows an example from our experiment.

Example output from CYR3CON attack sequence disruption experiment:

```
The following sequences can be disrupted by remediating
CVE-2017-10271:
T1059.001-PowerShell, T1203-Exploitation for Client Execution,
T1204.002-Malicious File, T1053.005-Scheduled Task
T1059.001-PowerShell, T1203-Exploitation for Client Execution,
T1204.002-Malicious File, T1059.003-Windows Command Shell,
T1047-Windows Management Instrumentation, T1053.005-Scheduled
Task
T1059.001-PowerShell, T1203-Exploitation for Client Execution,
T1204.002-Malicious File, T1059.005-Visual Basic,
T1059.003-Windows Command Shell, T1053.005-Scheduled Task
```

FIGURE 5. Example Output from CYR3CON Mapping

Note that the attacker had multiple sequences available to him in this case that could potentially involve exploitation of the above-named CVE. A defender, for example, can also identify all potential attacker sequences available based on a vulnerability scan and work to remediate vulnerabilities that are involved with attack sequences they wish to disrupt. Using techniques like identification of predicted exploits can narrow such a list further.

HOLISTIC ATTACK DISRUPTION: OPS AND VM

Throughout this article, we've looked at both the MITRE ATT&CK and CVE frameworks, discussed how CVEs could map to ATT&CK techniques, shown how attacker sequences could be derived, and outlined how such sequences can inform a vulnerability management program to strategically remediate CVEs to disrupt attacker activities. However, the disruption of attacker sequences can also require vulnerability remediation – and this exposes a strength in the ATT&CK taxonomy – namely, that one can map CVEs along with operational data to ATT&CK techniques. By looking at what is available to an attacker, security teams can examine a variety of options to disrupt a given attack sequence.

Suppose, for example, that foreign hackers are suspected of launching attacks against a domestic enterprise. Using ATT&CK, analysts can map all sequences of techniques known to be used by these attackers. They can look at how to disrupt the sequences based on a full arsenal of security tools. For example, patching certain vulnerabilities might deny a portion of these sequences, with some vulnerabilities be non-remediated due to dependencies with legacy software. In these systems, analysts can resort to disrupting different portions of the attack sequence, such as taking steps to avoid privilege escalation through additional authentication techniques, blocking ports, or even isolating systems.

Ultimately, the defensive goal is to stop attackers before their attacks can start. Whether the defensive action deals with patching vulnerabilities or taking a more SOC-oriented action becomes a secondary management concern, because in either way the threat can be blocked. This holistic approach to cyber security leads to a better unity of effort across enterprise teams, and results in a more proactive, threat-centric, automated approach.

ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.

ABOUT CYR3CON

CYR3CON provides the only machine learning threat intelligence platform that predicts and prioritizes the latest cyber threats, enabling CISO's to better understand the threat landscape, gain knowledge about malicious hacker behavior, and identify emerging attacks against enterprises. CYR3CON's underlying algorithms are also the only offering validated through years of academic research, peer reviewed publication, and government backed grants. For more information, please visit https://www.cyr3con.ai/.

[1] Information on the CVE program is available here: https://cve.mitre.org/.

[2] Information on the MITRE ATT&CK program is available here: https://attack.mitre.org/.

[3] Founded by Dr. Paulo Shakarian, Arizona-based CYR3CON uses machine learning to derive useful cyber threat and vulnerability intelligence from hacker networks to help enterprise teams properly prioritize their security controls.

[4] Download of the CVE database is available here: https://cve.mitre.org/data/downloads/index.html.

[6] These two sentence quotes from MITRE are taken from the heading on this website: https://attack.mitre.org/.

[7] Here is a typical report outlining the results of such MITRE testing of endpoint security products: https://www.mitre.org/news/press-releases/mitre-releases-results-of-evaluations-of-21-cybersecurity-products.

[8] Many salient aspects of threat modeling, including attack trees, were invented by this author and are referenced in https://en.wikipedia.org/wiki/Threat_model.

[9] First introduced in this early 1993 computer security textbook by the author: https://www.amazon.com/Fundamentals-Computer-Security-Technology-Amoroso/dp/0131089293.