Automating reasoning with ATT&CK?

Jonathan M Spring, Rawan Al-Shaer

FloCon, Jan 8, 2020

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM19-1296

Introduction

MITRE ATT&CK is made up of **TTP** (Tactics, Techniques, Procedures)

- They are low-level descriptions of adversarial actions (Eg. T1193 Spearphishing Attachment, T1112 Modify Registry, T1056 Input Capture).
- The community is interested in using ATT&CK for detection, prediction, forensics, and threat hunting because it provides behavioral observables for detecting attacks.

Our goal:

- Characterize ATT&CK's structure and usefulness for automated detection, etc.; especially of their APT dataset.

TTPs in MITRE ATT&CK Framework

Phases

PRE-ATT&CK

Priority Definition
- Planning, Direction

Target Selection
Information Gathering
- Technical, People, Organizational

Weakness Identification
- Technical, People, Organizational

Adversary OpSec
Establish & Maintain Infrastructure
Persona Development
Build Capabilities
Test Capabilities
Stage Capabilities

Enterprise ATT&CK

Tactics

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control
Impact

12 Tactics

Techniques

Spearphishing
PowerShell
DLL injection
Based64 encoding
C2 Encryption
Process injection
Launch Daemon
Modify registry
Input Capture
File Obfuscation
Exfiltration over C2

244 Techniques

Challenges

MITRE ATT&CK TTPs are not *correlated* at the technique level

MITRE ATT&CK techniques are not *ordered temporally*

- A kill-chain ordered set of techniques would be, for example:

1. Account Discovery
2. [weaponization]
3. Spearphishing Attachment
4. User Execution
5. Bypass User Account Control
6. Automated Collection, Data Compressed
7. Exfiltration over C2 Channel

Attacks and Campaigns

ATT&CK merges (unhelpfully, we think) the concept of attack with that of campaign

This is true even though it uses the kill chain as a semi-organizational concept

In the kill chain, an attack is a single exploitation attempt

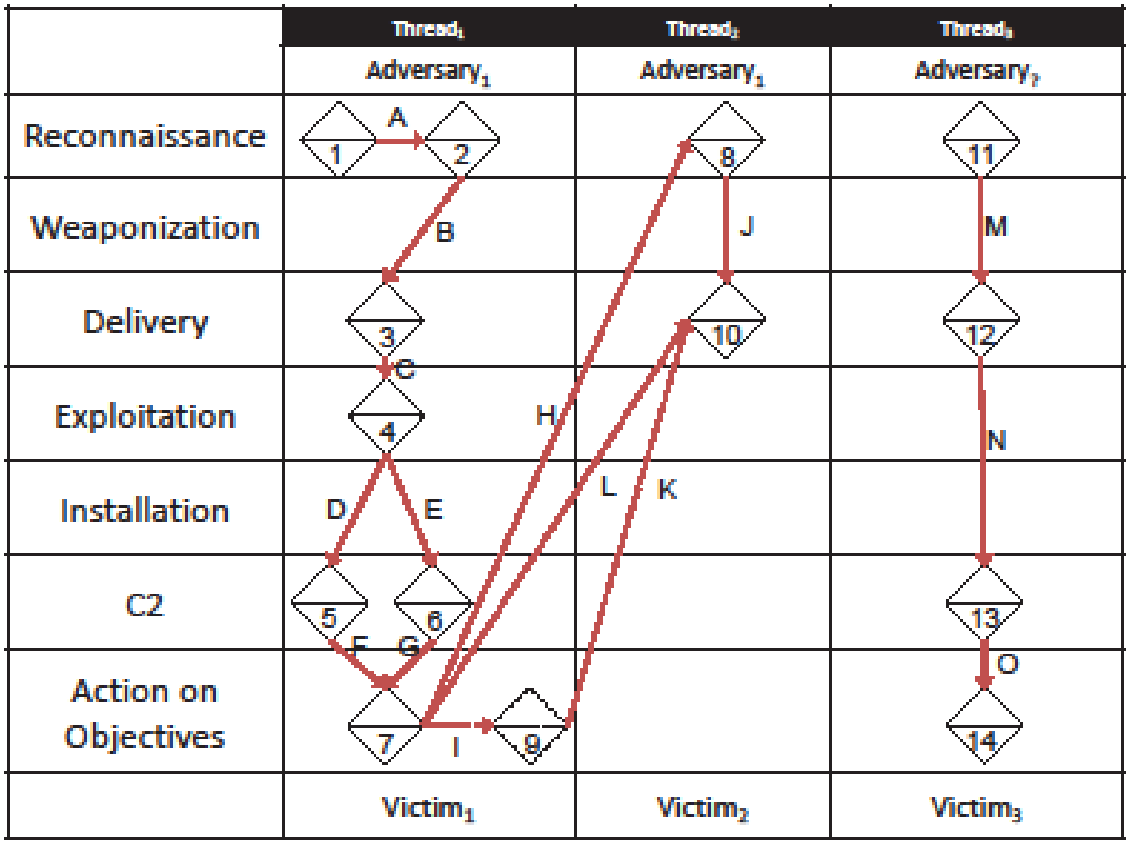
Campaigns are a series of planned or interrelated attacks

The kill chain and diamond model are not perfect, but they are useful mental models to organize general knowledge in security

- See Spring JM, Illari P. Building general knowledge of mechanisms in information security. Philosophy & Technology. 2018 Sep 17:1-33.

Diamond model and Campaigns

The diamond model for campaigns includes some things that ATT&CK does not



Sergio Caltagirone, Andrew Pendergast, Christopher Betz. The Diamond Model of Intrusion Analysis. 2014

Does it matter that ATT&CK is missing this temporal structure?

In short, yes.

At least, if you want to understand the relationship between MITRE's APT data sets and the techniques they use, temporal kill-chain structure helps

Helps how?

If you use machine learning methods to cluster related or frequently co-occuring techniques, then *sequential pattern mining* (kill chain guides sequencing) is better than any of:

- Partitioned Clustering
  - Finding the optimal K clusters
  - K means clustering
  - PAM clustering
  - Fuzzy Analysis clustering
  - Cluster Validation
- Hierarchical Clustering
  - Finding the optimal K clusters
  - Agglomerative clustering
  - Divisive clustering

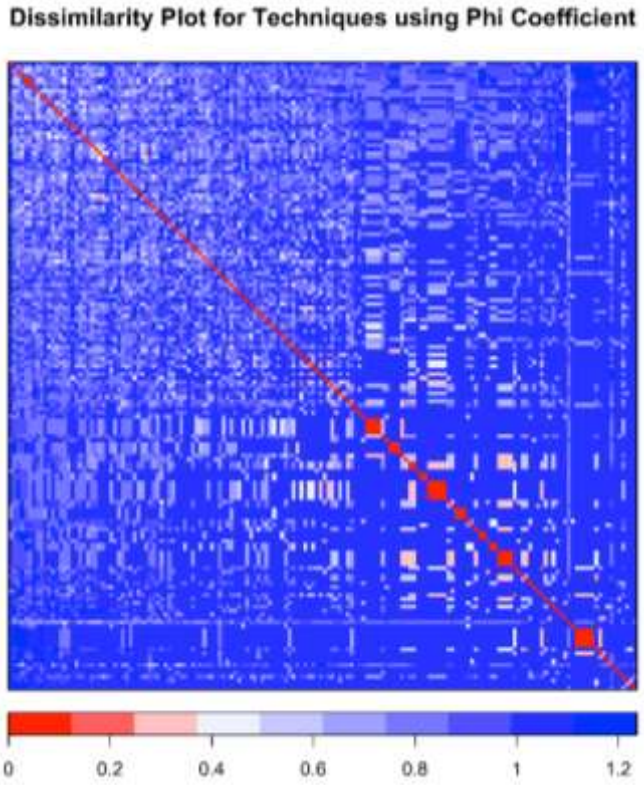
(Paper on this due out soon)

For intuition behind this result, consider clustering coefficient of APT data set

Hopkins Statistic: assess the clustering tendency of a dataset by measuring the probability that a given dataset is generated by a uniform distribution – tests the spatial randomness of the data

- Interpretability:
  - **H = 0.5**: The data set contains no meaningful clusters
  - **H ≅ 1**: The data set contains meaningful clusters
  - **H ≅ 0**: The data set is regularly spaced (neither clustered nor random)

Using Phi Coefficient : **H = 0.6**



Sequential Pattern Mining

- After temporally ordering observed attacks, sequential pattern mining created technique rules based on which techniques often showed a temporal order
- **SPADE (Sequential Pattern Discovery using Equivalence Classes) Algorithm:**
  1. Find the most frequent single length sequence
  2. Observe the two-type temporal sequences (A occurs before B) and two-element item groupings (A and B are often seen together)
  3. Based on the most frequent length-two outputs, then move on to finding three-element sequences and three element item groupings
  4. Continues until no longer finds frequent outputs
- Confidence: likelihood that the sequential rule A → B actually occurs among transactions containing item set A, under the constraint that item set A is before B. High confidence implies a high likelihood that B occurs in a future sequence
- Extracted **19** technique rules with confidence of 0.5 or higher

Why should we care about related techniques?

To automate reasoning in incident analysis, it would help to know what adversary actions are most likely to look for, given what the analyst has seen already

ATT&CK could provide this, but without temporal structure it doesn't

If we had it clear and formalized, we could use it in formal, automated reasoning

- See Spring JM, Pym D. Towards Scientific Incident Response. International Conference on Decision and Game Theory for Security 2018 Oct 29 (pp. 398-417). Springer.

Automated reasoning with ATT&CK?

Not yet

But we could make progress on automating incident and campaign analysis with some careful improvements

The target for automation is probably improving automated evidence collection and data discovery in a SIEM, so that an analyst can review incidents, and not alerts.

Other problems with techniques in ATT&CK

Some techniques are subsets of others. For example:

- Scripting
- Powershell
- Bash scripting

There do not seem to be guidelines on when an analyst tags an intrusion with the more general or more specific option

The unified cyberspace ontology (UCO) tries to be a bit more rigorous about these relationships, but it does not have the same level of input from practitioners.

Summary

The case studies captured in ATT&CK are valuable information for incident analysis

The ATT&CK structure is not currently amenable to automated reasoning

Two most important things to make it so:

- Restore the temporal relationships between the techniques (as in the Diamond Model)
- Make hierarchy or subset relationships between techniques explicit

Thanks! Questions?

jspring __ cert.org