ThreatMAP: Mapping Attack Plans from the Techniques, Tactics and Procedures of the MITRE ATT&CK Enterprise Framework for Plan Recognition

Emilie Coote[1], Taylor Perkins[2]

School of Computing, Queen's University, Kingston, Canada

Abstract

In this research the application of plan recognition is applied in the cybersecurity domain for the detection of anomalous behaviours indicative of cyber kill chains occuring on enterprise Information Technology (IT) networks.Cyberattacks are becoming much more frequent on enterprise networks. As the kill chains developed for cyberattacks become increasingly sophisticated, they become more and more difficult to detect, and are only alerted upon after an cyberattack has occurred. The cyber threat landscape is ever evolving and there exists a multitude of combinations of techniques and tactics that can be used to develop a cyberattack, increasing the need for automating the detection of the kill chains outlined by the Mitre Attack Enterprise Matrix. The tactics and techniques of the MITRE ATT&CK Enterprise Framework allows for the unification of network and host-based alerting, providing greater visibility on the network. By modeling the cyber kill chain it is possible to match the actions of an attacker before the network is compromised.

1. Introduction

With cyberattacks becoming more sophisticated with the implementation of defense evasion techniques by adversaries there is in increased need for methods that detect these malicious activities before a network becomes compromised.This combined with the increasing usage of the internet as more systems become connected, and more reliant on IT networks, the volume of data that must be analysed also increases. As adversarial behaviour becomes increasingly similar to normal network behaviour, cyberattacks become easier to masquerade in the flood of collected data, making traditional intrusion detection methods less effective. [1, 2, 3].

Lockheed Martin published the cyber kill chain framework that describes the stages that and adversary must take in order for a cyberattack to be successful [4]. Developed for the purpose of the identification and prevention of anomalous cyber activity, it is meant to break down the stages of a cyberattack into sections where mitigation can be put in place to stop the chain of attack. Lockheed Martin describes the seven stages of the cyber kill chain as follows, reconnaissance, weaponization, delivery, exploitation, installation, command and control, and the actions on objectives stages.

Another framework, the MITRE ATT&CK Enterprise Framework was also developed to provide an understanding of cyber threats, mapping out the common tactics and techniques utilized by adversaries during an attack [5]. This framework allows analysts to categorize adversarial behaviours based on observed techniques. The MITRE ATT&CK Enterprise Framework describes fourteen tactics, reconnaissance, resource development, initial access execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, command and control, exfiltration and impact.

Combining the knowledge of the cyber kill chain and the tactics and techniques of the MITRE ATT&CK matrix attack plans provides a description of the possible avenues of cyberattack that an advsary may take. Modeling this domain would provide a framework in which to compare enterprise IT network events for the detection of anomalous behaviours.

Plan recognition, a research area in automated planning, is a field of artificial intelligence (AI) that infers the goals of a given set of actions through the observation of behaviours. These observations can be compared to the developed plans and policies generated by the domain and problem definitions. The plan recognition model will be able to describe the set of tactics and techniques of the MITRE ATTA&CK Enterprise Framework for the purpose of detecting anomalous network behaviours. Collected observations from network and host logs found on an enterprise IT network can then be compared against the modeled anomalous behaviours to determine if there are cyber kill chains occurring.

The utilisation of plan recognition does not require any data for training, removing the need for training datasets. This approach addresses that all malicious events have to be identified. For anomaly detection techniques the models either require labeled datasets or use machine and deep learning algorithms to identify anomalous behaviours. This can be problematic when the malicious events aren't always known and therefore are not labeled. Modeling adversary behaviours addresses this concern by viewing determined behaviours in the context of the

CISC-813: Automated Planning – Final Project

deployment of a cyber kill chain rather than individual events. Determining this behaviour using the MITRE ATT&CK Enterprise Matrix provides a framework that the cyber kill chain can be compared against, and allows for different attack variations to be included for detection. Modeling adversarial behaviours also gives the model the flexibility to adapt to the changing threat landscape and does not need to be updated for each discovered attack, only when new tactics and techniques are discovered. This removes the requirement for retraining of anomaly detection models using machine and deep learning algorithms.

In this paper we introduce ThreatMAP, the application of planning recognition for the detection of malicious activities as described by the MITRE ATT&CK Enterprise Matrix. The representation of the matrix is programmed in Planning Domain Definition Language (PDDL) and the observation file is generated from enterprise network data.

1.1. Cyber Kill Chains

A cyber kill chain is a framework that is used to define the seven stages that a cyberattack must achieve in order to be considered successful.

1. The first stage, **Reconnaissance** is where the attacker will gather information on the target network, this includes identifying available systems, possible vulnerabilities, and potential points of entries. Methods to achieve this phase would include active scanning, gathering host information, including active accounts, operating system information, and services avaliable on the network.
2. The next stage is **Weaponization**, where the attacker will develop attacks using strategies including building custom malware or leveraging prebuilt frameworks. These attacks are based on the information gained in the reconnaissance stage, and may include techniques such as building phishing emails.
3. The next stage is the **Delivery** of the weaponized payload, with the goal of getting the developed attack onto a targeted computer. This can be done through phishing emails, infected USB keys, and the exploitation of publicly facing applications.
4. After the delivery of the payload, **Exploitation** can occur of the target system. This includes actions such as installation of backdoors, exploiting available services, and user initiated execution.
5. After the target has been exploited, it is important to establish Persistence on the system, this is where **Installation** takes place. This includes the installation of of additional malware to allow maintain control of the system, the addition of user accounts, creating scheduled tasks, as well as privilege escalation.
6. Once persistence is gained through installation, **Command and Control** of the system can occur. This is when the attacked has a connection onto the system and can continue to execute actions on the system, including lateral movement. This leads into the final stage, actions on Objective.
7. With **Actions on Objective**s the attacker has full control of the system, or even the network at large, and can carry out any malicious activities including exfiltration,manipulation, ransomware, even system or network wide disruptions.

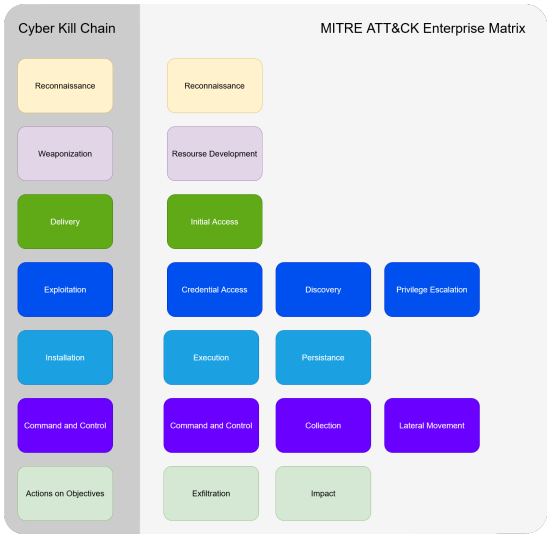

Figure 1: Mapping of the Cyber Kill Chain to The MITRE ATT&CK Enterprise Matrix

The MITRE ATT&CK Enterprise Matrix further breaks the cyber kill chain into fourteen tactics, each having a number of associated techniques. In 1 the fourteen tactics have been mapped out to the seven stages of the cyber kill chain, nothing that defence evasion does not fall under any one category as it is a technique that can be used at any time after the exploitation state has been reached.

1.2. Intrusion Detection

There are generally two methods used for intrusion detection for enterprise networks, signature based and anomaly detection. Signature based detection is used when an exploit or cyberattack has distinguishable features and rules can be created. Alerts for the enterprise network would be generated when a given signature is

detected in the data. One major drawback for signature detection is the delay of the signatures being written and databases being updated. With signature detection the exploit must first be known and a signature written, unlike with anomaly detection. Anomaly detection methods including AI are used in order to distinguish benign enterprise network events from those that are malicious. Anomaly detection does not require that the parameters of a cyberattack are known, however, it must be considered where there are enterprise network events that individually they would be considered normal operations, however combined with other events would indicate the occurrence of a cyber kill chain. This can sometimes be a difficult differentiation to make, even when using machine and deep learning techniques.

Using plan recognition would combine the two methods. The resultant model of this research provides the possible plans and policies that can be built from the Mitre ATT&CK Enterprise Matrix, thereby providing a signature. It is also not limited by the need of updating signatures as new attacks become available. Defining the possible actions that are available would build plans that adapt to the evolving threat landscape. The MITRE ATT&CK Enterprise Framework also incorporates both network and host-based events. The correlation of these events gives better insight into what is occurring on the network.

1.3. Automated Planning and Goal Recognition

Automated planning leverages algorithms that aim to develop strategies that result in solutions to specified problems. It is commonly used in areas such as event scheduling and path optimization. Automated planning requires a domain to be modeled, and a problem to be described in order to produce plans. The domain is comprised of a set of actions made up of predicates. These predicates can be applied to a number of variables to enable to modeling of a given domain.

Rameriz et al. defines planning recognition of the determination of a goal given a set of observed actions [6]. Plan recognition is a field of automated planning where possible goals are given based on a provided set of observables in an observation file. An observation is a predicate corresponding to achieved actions. The observables in this research are a list of observed events occurring on a given network. The application of plan recognition is to determine whether observations found in the obervation file matches the a plan provided by the plan recognition model, if so the plan would be a valid plan in the given domain.

2. A Planning Model for Detecting Cyber Kill Chains

This paper proposes the implementation of ThreatMAP, an automated planning to model cyber kill chains as described by the MITRE ATT&CK Enterprise Matrix for plan recognition. This solution addresses the delay found using cyberattack signatures, and gives context to independently occurring events that may be part of a cyber kill chain. ThreatMAP is also flexible and can easily be updated when new techniques and tactics are discovered. The goal of this research is to develop a model that can be used to detect occurring cyber kill chains in enterprise network data and would alert analysts to cyberattack before any data is compromised. This is achieved by using the model to determine if an observable plan matches one of the possible plans contained within the model.

2.1. States

Each state in the ThreatMAP model is represented as a one of the tactics from the MITRE ATT&CK Enterprise Matrix. There are fourteen tactics described by this matrix, each one in represented in this research. This states are divided into categories based on the stages of the cyber kill chain.

The tactics first had to be mapped to the cyber kill chain. This allows the definition of allowed movements between the tactics as described in the cyber kill chain. This mapping is described in 1. The adversary will only need to reach one tactic for each of the stages of the cyber kill chain, however it is possible that an adversary will reach multiple tactics under a given cyber kill chain state. This provides a more realistic representation of an adversary moving through a network during cyber attack.

Defense evasion is not covered by the cyber kill chain, however this tactic describes techniques that are used to evade detection once the adversary has gained access to the system. This is a state that can be reached from any one of the installation, command and control, and actions on objectives states.

2.2. Actions

The actions in this planning domain are the techniques found under the tactics of the MITRE ATT&CK matrix. They describe the transitions between each state, represented by the techniques outlined for each tactic of the MITRE ATT&CK Enterprise Matrix. For the purpose of this research we implemented a limit on the number of techniques to model for each tactic, choosing the ones that would be the most common.

For each state in the model, there are a number of actions that could occur in order to transition to the next

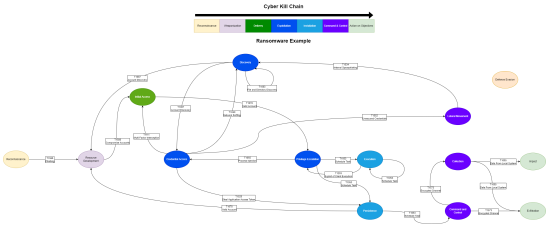

Figure 2: State Graph for Ransomware Attack based on the MITRE ATT&CK Matrix

state. Not all outcomes for each action are deterministic, there are techniques in the MITRE ATT&CK Enterprise Matrix when attempted technique are not successful and will either have the adversary remain in a current state, or move back to a previous state. An example of this can be seen in technique t1598 for phishing [7].

TODO: Include code example

There are also techniques in the MITRE ATT&CK Enterprise Matrix that may contain a number of subtechniques, such as the case for technique t1586 for compromising accounts [8]. There are a number ways for this action to be successful in our implementation, and dependant on the method used to compromise the account the resulting predicates may differ.

TODO: Include code example

The state transitions are determined through valid transitions determined by the cyber kill chain framework. An example of a valid attack graph is featured in 2 where a ransomware kill chain is modeled.

2.3. Types

An enterprise network has a number of users and systems on their network, all of which may be vulnerable to cyberattack and need to be included in the modeling as parameters. There are many different parameters that can be utilized within the actions not limited to the users and the systems, the status of the network, the account access, and the position of the adversary also need to be included. These are all modeled as objects and have corresponding predicates.

2.4. Implementation - Under Construction

ThreatMAP is a Fully Observable Non Deterministic (FOND) representation programmed in PDDL. The domain is a FOND representation as we have a set of described techniques from the MITRE ATT&CK Enterprise Matrix that are modeled as actions, determining this domain to be fully observable. There are also actions where there are multiple outcomes, also making the domain non deterministic.

The way in which this model is implemented is through describing the variables found on an enterprise network, including the systems, user accounts, and any associated vulnerabilities that may be present. The status of the cyberattack must also be tracked, this includes any obtained information that an adversary discovers on the network, for example if the adversary has obtained root credentials.

TODO: Include Predicates

2.4.1. Domain

The domain describes the predicates and actions for this problem space. We include a number of predicates that describe the state of the environment, including determining the stage of the cyber kill chain, the user access, and if the users or computers on the network are exploitable.

The actions for ThreatMAP are also described in the domain. This includes the techniques selected from the MITRE ATT&CK Enterprise Matrix modeled as actions.

2.4.2. Problem

The problem is described using the variables on the enterprise network as objects, this includes the states of the MITRE ATT&CK Enterprise Matrix, users, computers, and the adversary. Each of these objects described in the problem is assigned a type.

The initial state is also defined. For this problem the initial state is that the given adversary is at s1, the reconnaissance state. The valid movement between the states, otherwise known as the stages of the cyber kill chain, are also described as depicted in 2. Finally the goal is described, this is that the adversary has reached one of the two goal states, infiltration or impact.

3. Evaluation - Under Constrution

The aim in this research is to build a model that represents the valid transitions of the tactics of the MITRE ATT&CK Enterprise Matrix. In order to achieve this aim the following must be achieved

- Each MITRE Tactic is described as a State
- Each MITRE Technique is described as a valid Action
- Correctly translating movement between states with fluents
- Accurately modeling a cyber kill chain as a resultant policy
- A FOND model that can be used for detection of occurring cyber kill chains

The validity of the model can be evaluated through observations dervied from network data during the completion of a cyber kill chain. These observation files

representing known cyber kill chains can be developed and used to determine the ability of the defined model to detect possible cyber kill chains.

4. Related Work

Plan recognition as planning is used in a number of domains. The work of Ramirez et al. outlines the possible application of plan recognition as planning [6]. In this work the determination of plans for a given problem is explored. Ramirez et al. do not aim to find the optimal solution for a given problem, but a valid plan.

The application of plan recognition to the cybersecurity field has been approached previously. The work of Amos-Binks et al. outlines the application of plan recognition to attack graphs [1]. In this work a network attack is modeled and plan based security metrics are explored, including the percentage that the plan is complete, the minimum remaining path length (MRPL) that shortest possible path to the described goal, and the identification of a choke point, which identifies areas where intervention could prevent the continuation of the cyberattack.

An early work by Geib et Al. explores the utilization of probabilistic planning in plan recognition to replace IDS [9]. In this work a probability model is proposed, modeling the actions that an adversary takes to achieve a goal, however there are limitations including the inability to model evasion techniques, and that the model is capable of representing a single adversary on the network.

Planning recognition has also been applied to Wireless Local Area Network (WLAN) data in a similar way in the work of Chen et al [3]. WLAN data encompasses 802.11 radio packets and wireless device information. Their aim is to detect one of four types of attacks, Denial of Service (DoS), Media Access Contro (MAC) spoofing, Main in the Middle (MITM), or Wi-Fi Protected Access (WPA) attack. Plan recognition techniques are used to predict the type of occurring attacks based on the behaviour of the devices on the network.

The research by Amos-Binks et al, Chen et al. and Wang et al. is focused on using the alerts from network data in order to build a planning model. However these methods are limited to a subset of the possible cyberattacks, and do not leverage the host data on the network. The application of the MITRE ATT&CK Enterprise Framework allows for the unification of network and host based alerting.

Another proposed model. Plan2Defend, leverages plan recognition models in order to monitor and respond to cyberthreat on a smart grid [10]. Plan2Defend models a smart grid, and the status of the various operations occurring. The aim is to alert when anomalous behaviours are occurring on the network. A number of attacks are run against a digital twin to similar the smart grid under attack and these observations are used against Plan2Defend. The goal is to recognize the attack and respond by alerting.

5. Summary

This research will provide a plan recognition model that is capable of generalizing the method of attack based on the adversary behaviours outlined by the MITRE ATT&CK Enterprise Matrix. In this paper cyber kill chains and the MITRE ATT&CK Enterprise Framework was summarized and a brief background on planning recognition was presented. Other works utilizing planning recognition in the field of cyber security were also explored. Based on these findings the implementation of ThreatMAP was presented.

5.1. Future Work

There are a number of areas where this research can be furthered:

- Applying a probabilistic approach for each action
- Determine threshold for alerting
- Automatic generation of observation files from enterprise networks
- Automation of actions to prevent the continuation of the cyberattack

References

[1] A. Amos-Binks, J. Clark, K. Weston, M. Winters, K. Harfoush, Efficient attack plan recognition using automated planning, in: 2017 IEEE Symposium on Computers and Communications (ISCC), IEEE, Heraklion, Greece, 2017, pp. 1001–1006. URL: http://ieeexplore.ieee.org/document/8024656/. doi:10.1109/ISCC.2017.8024656.

[2] L. Wang, Z.-T. Li, J. Ma, Y.-M. Ma, A.-F. Zhang, Automatic attack plan recognition from intrusion alerts, in: Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007), IEEE, Qingdao, 2007, pp. 1170–1175. URL: https://ieeexplore.ieee.org/document/4288026/. doi:10.1109/SNPD.2007.396.

[3] G. Chen, H. Yao, Z. Wang, An Intelligent WLAN Intrusion Prevention System Based on Signature Detection and Plan Recognition, in: 2010 Second International Conference on Future Networks, IEEE, Sanya, Hainan, China, 2010, pp. 168–172. URL: http://ieeexplore.ieee.org/document/5431861/. doi:10.1109/ICFN.2010.77.

[4] Cyber Kill Chain® | Lockheed Martin, ????. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

[5] Matrix - Enterprise | MITRE ATT&CK®, ????. URL: https://attack.mitre.org/versions/v13/matrices/enterprise/.

[6] M. Ramirez, H. Geffner, Plan Recognition As Planning (????).

[7] Phishing, Technique T1566 - Enterprise | MITRE ATT&CK®, ????. URL: https://attack.mitre.org/versions/v13/techniques/T1566/.

[8] Compromise Accounts, Technique T1586 - Enterprise | MITRE ATT&CK®, ????. URL: https://attack.mitre.org/techniques/T1586/.

[9] C. Geib, R. Goldman, Plan recognition in intrusion detection systems, in: Proceedings DARPA Information Survivability Conference and Exposition II. DISCEX'01, volume 1, 2001, pp. 46–55 vol.1. doi:10.1109/DISCEX.2001.932191.

[10] T. Choi, R. K. L. Ko, T. Saha, J. Scarsbrook, A. M. Koay, S. Wang, W. Zhang, C. S. Clair, Plan2Defend: AI Planning for Cybersecurity in Smart Grids, in: 2021 IEEE PES Innovative Smart Grid Technologies - Asia (ISGT Asia), IEEE, Brisbane, Australia, 2021, pp. 1–5. URL: https://ieeexplore.ieee.org/document/9715679/. doi:10.1109/ISGTAsia49270.2021.9715679.