Poster: M^2ASK : A Correlation-Based Multi-Step Attack Scenario Detection Framework Using MITRE ATT&CK Mapping

Qiaoran Meng
National University of Singapore
Singapore, Singapore
e0492494@e.nus.edu

Nay Oo
NCS Cyber Special Ops-R&D
Singapore, Singapore
nay.oo@ncs.com.sg

Yuning Jiang
National University of Singapore
Singapore, Singapore
yuning_j@nus.edu.sg

Hoon Wei Lim
NCS Cyber Special Ops-R&D
Singapore, Singapore
hoonwei.lim@ncs.com.sg

Biplab Sikdar
National University of Singapore
Singapore, Singapore
bsikdar@nus.edu.sg

Abstract

Traditional Network Intrusion Detection Systems (NIDS) often generate large volumes of alerts with redundancies and false positives, incapable of correlating detected attack actions. This adds difficulty for security analysts to construct a comprehensive understanding of multi-step attacks. To address these limitations, we present a novel MITRE-based Multi-step Attack Scenario Construction (M^2ASK) algorithm that enhances cyber threat intelligence (CTI) by integrating MITRE ATT&CK tactic and technique mapping, facilitating the interpretation of multi-step attacks and informing response strategies. Our approach processes alert data from NIDSs, transforming it into a network communication graph. Graph-based correlation techniques are employed, combined with MITRE ATT&CK and Cyber Kill Chain stage profiling to construct comprehensive network attack scenarios. Our key contributions include: (1) the development of a Cyber Kill Chain based model for constructing attack scenarios; (2) the alert correlation approach based on MITRE ATT&CK tagging of attack actions.

CCS Concepts

• **Computing methodologies** → **Machine learning algorithms**; • **Security and privacy** → *Intrusion detection systems*; • **Networks** → *Network security*.

Keywords

Multi-Step Attack; Alert Correlation; MITRE ATT&CK

ACM Reference Format:
Qiaoran Meng, Nay Oo, Yuning Jiang, Hoon Wei Lim, and Biplab Sikdar. 2024. Poster: M^2ASK : A Correlation-Based Multi-Step Attack Scenario Detection Framework Using MITRE ATT&CK Mapping. In *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24), October 14–18, 2024, Salt Lake City, UT, USA.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3658644.3691392

1 Introduction

Multi-step attacks, characterised by multiple coordinated attack actions, have been on the rise in cyber intrusions. However, traditional NIDSs primarily focus on detecting single-step attacks and struggle to correlate alerts or construct complete attack scenarios. To address these limitations and enhance attack detection capabilities, researchers have leveraged the rich features of NIDS alerts to conduct feature study and similarity-based alert correlation for attack identification [1, 4, 6, 10]. Attack scenarios are typically constructed through various single-step attack action linking strategies from correlated alerts based on various attack models. However, a notable gap exists in the utilization of detailed attack models based on established cyber attack frameworks, as observed in the general attack stage models for attack scenario construction outlined in [1, 10]. The generated attack scenarios have the actionability and interpretability yet to be improved by leveraging CTI support and alert semantic analysis.

This poster introduces a novel algorithm designed to construct comprehensive network attack scenarios in network systems, significantly enhancing CTI. Our proposed algorithm aims to enhance the logic and explainability of attack scenario identification by the development of MITRE ATT&CK tactics and techniques [8] multi-class categorization model and Lockheed Martin Cyber Kill Chain [3] based attack model. We employ a correlation-based approach combined with MITRE ATT&CK and Cyber Kill Chain profiling to construct the multi-step attack scenarios, subsequently identifying and ranking potential attack paths for each attack. We summarize the key contributions of our paper as follows:

- We developed an ensemble-based approach to tag MITRE ATT&CK tactics and techniques on network meta-alerts, thereby facilitating effective correlation.
- We proposed a Cyber Kill Chain based attack model for attack scenario construction, significantly enhancing the interpretability of multi-step attacks and informing response strategies to cyber threats.

2 Algorithm Design

In this section, we outline the design of the proposed M^2ASK algorithm to precisely identify multi-step attack scenarios with CTI enhancement. The key stages of the algorithm are illustrated in Figure 1. The inputs to the algorithm are the network alerts collected

CCS '24, October 14–18, 2024, Salt Lake City, UT, USA.

ACM ISBN 979-8-4007-0636-3/24/10
https://doi.org/10.1145/3658644.3691392

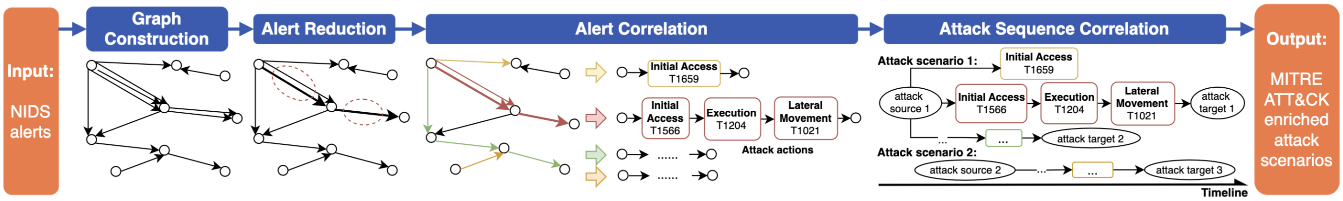

Figure 1: Block diagram of the multi-step attack detection algorithm M^2ASK.

from NIDSs in the network system. These alerts are first transformed by graph construction module to a directional network communication graph, where nodes represent network hosts and edges indicate alert communications between hosts. Considering the noisy nature of network alerts, we then perform alert reduction to collate overlapping low-level alerts into meta-alerts and reconstruct the network graph. Alert correlation is performed on the meta-alert graph to generate all possible attack sequences based on MITRE ATT&CK mapping and Cyber Kill Chain attack model. In the next module, the attack sequences are merged by considering temporal and causality relationships between attack stages, forming comprehensive attack scenarios with MITRE ATT&CK labels.

2.1 Alert Reduction

Considering the high information overlapping between alerts, this module is designed to combine duplicates into meta-alerts to condense the alerts. We propose a pairwise alert collation technique to combine the similar alerts between the same pair of network hosts, which are likely to be triggered by the same attack or benign activity. The conditions for collating alerts to meta-alert depend on the alert *timestamp* and *description* attributes. Specifically, for the alerts with the same source and destination hosts, the collation can only be performed if: 1) the time difference between their timestamps is within a small threshold, 2) the alert descriptions are highly similar. After the alerts are divided by time window, alert descriptions within each time window are transformed to numerical vectors by the UMBC cybersecurity specific word-to-vector model [5] and clustered by DBSCAN. Each alert cluster with similar descriptions within the time window threshold is transformed to one single meta-alert with updated attributes. A network meta-alert graph is then reconstructed using all meta-alerts generated.

2.2 Alert Correlation

Leveraging the network meta-alert graph, we apply our Cyber Kill Chain based attack model to perform alert correlation for attack sequence generation. We define an attack action as an atomic attack from a source to a destination host with $start\_time$, end_time, Cyber Kill Chain $stage$, MITRE ATT&CK $tactic$ and $technique$ features. An attack sequence is defined as a directed graph of attack action nodes and two network host nodes, namely $attack\_source$ and $attack\_target$. It represents an attacker network trace of correlated attack actions based on our attack model. Under the MITRE ATT&CK framework, adversaries employ distinct tactics, each corresponding to specific attack objectives, during different attack steps. We define an attack model following the Lockheed Martin Cyber Kill Chain stages, with a heuristic mapping from MITRE ATT&CK enterprise network tactics to Cyber Kill Chain stages.

The first step of the alert correlation module is to identify all network communication paths, which can be signs of the network attack propagation, from the meta-alert graph. A network path is denoted by $P = (L, E)$, where $L = [V_1, V_2, ..., V_n]$ represents a sequence of network hosts and E represents the edges between all pairs of adjacent network hosts following chronological order. Next, we perform the mapping from each meta-alert along the extracted network paths to MITRE ATT&CK tactics and techniques. The mapping task is conceptualized as a text classification problem of the meta-alert $description$ field containing detailed textual alert descriptions. We leverage a majority voting based classification ensemble to learn text patterns and identify the MITRE ATT&CK mappings for each meta-alert. Using our heuristic mapping, the corresponding attack stages can then be determined.

Subsequently, for each network path with MITRE ATT&CK mapped meta-alerts, we identify attack actions as groups of meta-alerts sharing the same source and destination hosts, attack stage, and MITRE ATT&CK tactic and technique. These identified attack actions are then transformed into attack sequences using Algorithm 1. The $SameHostPrecedence$ function orders attack actions in A_i first by attack $stage$ and then chronologically by $start\_time$. The $GetRelation$ function determines the relationship between a new attack action a and the latest action a_l in the current attack sequence AS based on the three types of relationships defined in Definition 1, thus deciding the placement of a in AS.

Definition 1. Two attack actions a_i and a_j has the relationship:
1) Parallel: $a_i.src = a_j.src$, $a_i.dst = a_j.dst$ and $a_i.stage = a_j.stage$.
2) Parent-child: $a_i.src = a_j.src$, $a_i.dst = a_j.dst$, $a_i.stage < a_j.stage$, $a_i.start\_time < a_j.start\_time$ OR $a_i.dst = a_j.src$, $a_i.stage$ not before Exploitation stage, $a_i.start\_time < a_j.start\_time$.
3) None: conditions 1) and 2) are both not satisfied.

2.3 Attack Sequence Correlation

The attack sequences derived from respective network paths may represent different attempts within the same multi-step attack. Thus, they are considered partial attack scenarios. These sequences are merged into attack scenarios by correlating their constituent attack actions. We consider two possible merging scenarios. The first scenario, *shared attack action*, merges sequences that share the same attack action node into a new sequence by the shared node. For the second scenario, *parent-child attack actions*, two attack actions from different attack sequences have a parent-child relationship. A directed edge is added from the parent action to the child attack

```
Algorithm 1: Transformation to Attack Sequence
  Input: Set of attack actions $A$, network path
         $P = ([V_1, ..., V_n], E)$
  Output: List of attack sequences $L_{as}$
  while $A \neq \emptyset$ do
      Initialize attack sequence $AS$ and latest attack action $a_l$;
      for $i \in [1, n-1]$ do
          $A_i \longleftarrow \{a | a \in A, a.src = V_i, a.dst = V_{i+1}\}$;
          Sort $A_i$ in ascending order by $SameHostPrecedence$;
          for each $a \in A_i$ do
              Set $AS.attack\_source \longleftarrow V_i$ if AS is empty;
              Relationship $r \longleftarrow GetRelation(a, a_l)$;
              if $r = parallel$ then
                  Add $a$ as the child of $a_l$'s parent node;
                  Set $a_l \longleftarrow a$, remove $a$ from $A$;
              else if $r = parent - child$ then
                  Add $a$ as the child of $a_l$;
                  Set $a_l \longleftarrow a$, remove $a$ from $A$;
      Set $AS.attack\_target \longleftarrow a_l.dst$, add $AS$ to $L_{as}$;
```

action to link the attack sequences together. After merging, the final outputs are attack scenarios enriched with MITRE ATT&CK information, enhancing CTI for defense.

3 Preliminary Results

We evaluated the algorithm performance by a case study of the first scenario in the IDS2012 dataset [7]. The attack scenario, titled *infiltrating the network from inside*, involves six attack steps. the attacker initially gained access to host A by malicious email attachment, then compromised B to perform SQL injection attack on the web server C. The raw network packet capture data from the day of the attack was processed by SecurityOnion [2], an open-source security information and event management (SIEM) tool, to generate network alerts. We trained the MITRE ATT&CK mapping model using a subset of the Emerging Threat Open Suricata 5.0 rule set [9] containing alert messages, MITRE ATT&CK tactics and techniques. The trained model achieved F1 scores of 93.4% and 98.4% respectively for tactic and technique categorization, and was subsequently integrated into the algorithm. The attack scenario graph generated by M^2ASK from these alerts is simplified and drawn in Figure 2. Utilizing our correlation strategy, which incorporates both chronological and causality relationships, the graph clearly illustrates the attacker's sequential network attack actions from the initial compromise of host A to the final SQL injection attack on C. Each attack action is tagged with source and destination hosts, an alert message and MITRE ATT&CK labels. Additionally, the Cyber Kill Chain stages of network attack steps can be extracted from the attack scenario. This comprehensive tagging greatly enhances threat intelligence, providing critical information for incident response.

4 Conclusion

In conclusion, this paper addresses the limitations observed in NIDSs concerning alert correlation and multi-step attack detection. Recognizing the gap in current literature regarding CTI-enriched attack models, we propose a novel multi-step attack detection algorithm M^2ASK. The algorithm efficiently consolidates large volume of NIDS alerts into meta-alerts through signature-based alert reduction. Leveraging an ensemble MITRE ATT&CK mapping model, we extract single-step attack actions enriched with MITRE ATT&CK tactics and techniques. Our defined attack model integrates the Cyber Kill Chain framework, serving as a robust foundation for constructing attack scenarios based on attack action correlation.

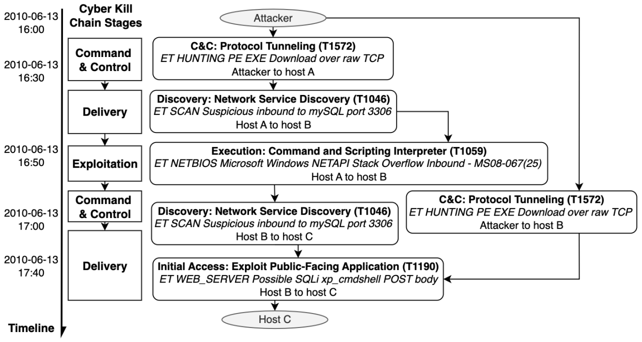
2010-06-13
16:00
Cyber Kill
Chain Stages
Attacker
2010-06-13
16:30
Command
& Control
C&C: Protocol Tunneling (T1572)
ET HUNTING PE EXE Download over raw TCP
Attacker to host A
Delivery
Discovery: Network Service Discovery (T1046)
ET SCAN Suspicious inbound to mySQL port 3306
Host A to host B
2010-06-13
16:50
Exploitation
Execution: Command and Scripting Interpreter (T1059)
ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067(25)
Host A to host B
Command
& Control
C&C: Protocol Tunneling (T1572)
ET HUNTING PE EXE Download over raw TCP
Attacker to host B
2010-06-13
17:00
Discovery: Network Service Discovery (T1046)
ET SCAN Suspicious inbound to mySQL port 3306
Host B to host C
2010-06-13
17:40
Delivery
Initial Access: Exploit Public-Facing Application (T1190)
ET WEB_SERVER Possible SQLi xp_cmdshell POST body
Host B to host C
Host C
Timeline

Figure 2: Simplified attack scenario graph of IDS2012 dataset attack scenario 1.

Acknowledgments

This work was funded by the NUS-NCS Joint Laboratory for Cyber Security (grant no. A-0008542-00-00).

References

[1] Steffen Haas and Mathias Fischer. 2019. On the alert correlation process for the detection of multi-step attacks and a graph-based realization. *ACM SIGAPP Applied Computing Review* 19, 1 (2019), 5–19. https://doi.org/10.1145/3325061.3325062

[2] Ross Heenan and Naghmeh Moradpoor. 2016. Introduction to Security Onion. http://researchrepository.napier.ac.uk/Output/461935

[3] Eric M Hutchins, Michael J Cloppert, Rohan M Amin, et al. 2011. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research* 1, 1 (2011), 80.

[4] Azqa Nadeem, Sicco Verwer, Stephen Moskal, and Shanchieh Jay Yang. 2022. Alert-Driven Attack Graph Generation Using S-PDFA. *IEEE Transactions on Dependable and Secure Computing* 19, 2 (2022), 731–746. https://doi.org/10.1109/TDSC.2021.3117348

[5] Ankur Padia, Arpita Roy, Taneeya Satyapanich, Francis Ferraro, Shimei Pan, Youngja Park, Anupam Joshi, and Tim Finin. 2018. UMBC at SemEval-2018 Task 8: Understanding Text about Malware. In *Proceedings of the 12th International Workshop on Semantic Evaluation*, Marianna Apidianaki, Saif M. Mohammad, Jonathan May, Ekaterina Shutova, Steven Bethard, and Marine Carpuat (Eds.). Association for Computational Linguistics, New Orleans, Louisiana, 878–884. https://doi.org/10.18653/v1/S18-1142

[6] Ali Ahmadian Ramaki, Morteza Amini, and Reza Ebrahimi Atani. 2015. RTECA: Real time episode correlation algorithm for multi-step attack scenarios detection. *Computers & Security* 49 (2015), 206–219.

[7] Ali Shiravi, Hadi Shiravi, Mahbod Tavallaee, and Ali A. Ghorbani. 2012. Toward developing a systematic approach to generate benchmark datasets for intrusion detection. *Computers & Security* 31, 3 (2012), 357–374. https://doi.org/10.1016/j.cose.2011.12.012

[8] Blake E Strom, Andy Applebaum, Doug P Miller, Kathryn C Nickels, Adam G Pennington, and Cody B Thomas. 2018. MITRE ATT&CK: Design and philosophy. In *Technical report*. The MITRE Corporation.

[9] Emerging Threats. 2023. *Emerging Threats Open Suricata 5.0 Rules Database.* Proofpoint Inc. https://rules.emergingthreats.net/open/suricata-5.0/

[10] Xiaoyu Wang, Xiaorui Gong, Lei Yu, and Jian Liu. 2021. MAAC: Novel Alert Correlation Method To Detect Multi-step Attack. In *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. 726–733. https://doi.org/10.1109/TrustCom53373.2021.00106