A Data Fusion Framework of Multi-Source Heterogeneous Network Security Situational Awareness Based on Attack Pattern

Yuangang Yao¹, Yanwei Sun¹, Zhaohui Liu¹, Xiangjie Meng¹ And Zhaohui Liu¹
¹China Information Technology Security Evaluation Center, Beijing,100000, China
¹Corresponding author’s e-mail:bravexz@163.com

Abstract. In the context of the era of big data, how to quickly and accurately detect attack events from massive amounts of heterogeneous data and form effective response on time has become the main challenge facing network security today. This paper systematically summarizes the attack behavior with both attack technology mechanisms and characteristics of the attack target, thereby constructing a scalable attack behavior model. Based on the attack behavior model, a data fusion framework of the multi-source heterogeneous network security situation is constructed. The framework normalizes multi-source heterogeneous security data into threat events with an attack pattern as the core and determine the attack state by the causal chain. Finally, the feasibility and effectiveness of the framework are verified by analyzing data in real business scenarios. This framework abstracts the multi-source heterogeneous data into an analyzable attack event, which greatly reduces the amount of data to be analyzed and improves the credibility of the network security situation data, realizing the identification of attack behaviors in the big data environment.

1. Introduction

As technology advances in 2019, so do the threats to security, including data loss or theft, cyber-attack infrastructure and so on. A security threat leads to loss or corruption of data or physical damage to the hardware and/or infrastructure. Knowing how to identify security threats is the first step in protecting computer systems. To protect computer systems from the above-mentioned security threats, an organization must have physical security control equipment, such as intrusion detection systems, firewalls, and virus sandboxes. It takes a lot of human resources to identify security threats with the massive volumes of data sets, especially from different log data sources. With the advent of the era of big data, the volume of security alert logs has gradually increased to the magnitude that manual analysis cannot be performed.

Because of the above problems, this paper proposes a data fusion framework of a multi-source heterogeneous network security situational awareness based on attack patterns. By studying the behavior characteristics of the attacker, the underlying security alarm log is abstracted into the attacker's behavior pattern to achieve the fusion of multi-source heterogeneous security logs and reduce the number of alarms.

In this paper, we investigated mechanisms of network attack and proposes a data fusion framework of a multi-source heterogeneous network security situational awareness based on attack patterns. By studying the behavior characteristics of the attacker, the underlying security alarm log is abstracted into
2. Related research

CAPEC (Common Attack Pattern Enumeration and Classification) [1] is a network attack description and classification standard first proposed by the US Department of Homeland Security in 2007 and gradually evolved into an authoritative standard for the network security industry with the participation of several research institutions. At present, the standard mainly summarizes attack patterns from two different perspectives, one is the perspective of the attack mechanism, and the other is the perspective of the attacked domain. From two different perspectives, the attack patterns form different tree structures. Each attack pattern has a certain upper-lower relationship and contains detailed information such as the summary of the attack pattern, the attack phase, the severity, the possibility of being used, the motivation, the consequences of the attack and the related vulnerability.

Xiaohong Yuan proposed to use CAPEC in security modeling [2] because CAPEC’s description of attack behaviors is biased towards technical mechanisms, which is more valuable for security researchers who analyze from a technical perspective. However, for the research on network attacks, the abstract behavior of the attacker often conforms to the behavior pattern similar to the definition of the kill-chain [3], while CAPEC lacks the abstract behavior description corresponding to the attack pattern, which is not suitable for attack behavior modeling.

ATT & CK (Adversarial Tactics, Techniques, and Common Knowledge) [4] is a knowledge base and model of cyber attacker behavior formulated by MITRE. It reflects the various stages of the attacker's life cycle and the target platform information they know. ATT & CK is useful for understanding the security risks of known attacker behavior, planning security improvements and verifying that defenses are working as expected. Analysis of the ATT & CK Matrix found that although ATT & CK constructs attack behavior cubes based on attack chain behaviors such as detection, exploitation, privilege elevation, command, and control, the attack method definitions under the same attack behavior belong to different target levels, such as AppInit DLL and Valid Accounts under privilege elevation behavior.

Hahn and Adam built a network security analysis framework based on the attack chain model [5] for assessing the risks of network attacks, while Lyndsey Franklin chose to use ATT & CK to build a threat analysis workflow [6]. Lynn divided attack behaviors into three categories in "Ontology Based APT Attack Behavior Analysis in Cloud Computing" [7]: host-based attack behaviors, network-based attack behaviors, and malicious code behaviors. Lee M [8] established the correspondence between API functions and attack behavior. The characteristics of the attack behavior cannot be obtained by associating the API function with the attack behavior. Therefore, it is also impossible to perform feature attribute and behavior correlation analysis based on the constructed attack behavior.

Li [9] assumes possible targets in the network based on important asset information in the network and constructs a layered attack path map. The probability of each hypothetical attack intent target is calculated by calculation, and the true attack intent and the most likely attack path of the attacker are obtained.

Mishra [10] proposed a model, which will work in real-time to analyze suspicious activities and detect the intrusion automatically. The proposed model will also analyze the alarms to detect attacks and give an automatic response to prevent in real-time. Processes were compared with original log events with tempered log events and the difference was found.

Woo S [11] described the attack behavior as an atomic action similar to MACE [12] and abstracted it as an attack behavior through a set of action sequences. However, the description of actions such as
simple access, file transfer, etc. The action lacks a description of the attack mechanism and cannot achieve behavior-based reasoning prediction.

Jianwei Zhuge [13] proposed an attack planning identification algorithm. The algorithm establishes the association between attacks through state abstraction of attack actions, thereby realizing early warning of attacks.

Musa [14] presents an effective model of depicting the devices and the data flow that efficiently identifies the weakest nodes along with the concerned vulnerability's origin. The complexity of the attack graph using MulVal has been greatly reduced using the proposed approach of using the risk and CVSS base score as evaluation criteria.

Based on the attribute attack graph, Cui [15] proposed the probabilistic attack graph model, which is generated by adding various factors that affect network security. The model uses security equipment performance data, common vulnerability scoring system data, etc. to calculate prior probability, finally obtains the network security index, and carries on the exploratory analysis.

Kotenko [16] suggests a framework for cyber attack modeling and impact assessment. It is supposed that the common approach to attack modeling and impact assessment is based on representing malefactors' behavior, generating attack graphs, calculating security metrics and providing risk analysis procedures.

REINECKE [17] assumes a computing device may: generate, using an attack model that specifies the behavior of a particular attack on a computing system. The hypothesis specifying, for a particular state of the particular attack, at least one attack action. Using the hypothesis, to identify at least one analytics function for determining whether at least one attack action specified by the hypothesis occurred on the computing system.

Pal [18] uses Computerized methods and systems to determine an entry point or source of an attack on an endpoint, such as a machine, e.g., a computer, node of a network, system or the like. These computerized methods and systems utilize an attack execution/attack or start the root, to build an attack tree, which shows the attack on the endpoint and the damage caused by the attack, as it propagates through the machine, network, system.

Through the above research papers, it is found that the analysis and identification of network attacks are mainly carried out through probabilistic models. These methods have low attack recognition accuracy and cannot handle multi-source heterogeneous data. According to the characteristic that network attacks have an obvious causal logic relationship, this paper extracts the characteristics of network attacks and establishes an attack identification framework. The framework recognizes attack behavior through rich feature matching, which effectively reduces the amount of data and improves recognition accuracy.

3. A data fusion framework based on attack pattern
The data fusion framework based on attack mode proposed in this paper transforms network attacks into structured, standardized knowledge for representation, and uses first-order logical predicates to describe the relationship between network attacks, to analyze security events with mathematical models. The framework identifies the single-time behavior of the attacker from a large number of low-level alarm information, correlates different attack actions and extracts the attack intention through causal chain reasoning. It can effectively find complex network attacks under large-scale data.

This chapter introduces the definition of attack patterns, framework design, and fusion information processing.

3.1. Attack pattern definition
The idea of data fusion based on attack behavior modeling is derived from the classic description model in automatic programming problems-STRIPS [19] (Standford Research Institute Problem Solver) model. This model uses the relationship between attack actions to correlate to achieve early warning of network attacks.
The effectiveness of the model depends on the accurate modeling of a single attack action. By studying the above-mentioned multiple attack behavior modeling methods and attack classification criteria, a complete description of a single attack behavior should include the following three dimensions:

- Characteristics of the attack target. Most attacks on the network are launched against specific platforms, showing strong correlation characteristics of the target, such as the eternal blue vulnerability attack against specific versions of the windows.
- Attack mechanism. Including technical means, timing characteristics, severity, prerequisites and resource requirements.
- Attack intention. Reflect the attacker's mind, a single attack may contain multiple attack intentions and results.

The definition of an attack pattern in this paper is based on these three dimensions, and the three-level structure attack pattern shown in figure 1 is constructed.

The definition of target features refers to the Common Platform Enumeration (CPE) [20], and targets are divided into three types: applications and services, operating systems, and hardware systems, which are uniquely identified by combining vendors and version numbers. The attack mechanism and attack intention are combined with the modeling methods in CAPEC and ATT & CK.

According to the definition of the attack pattern, its mathematical symbol represents the following triplet form:

\[ \text{Attack Pattern}_m = \{ \text{Target}_i, \ \text{Technology}_j, \ \text{Status}_k \} \]  

(1)

\( \text{Attack Pattern} \) represents the attack pattern.
\( \text{Target}_i \) represents a set of attack targets.
\( \text{Technology}_j \) represents attack mechanism characteristics.
\( \text{Status}_k \) represents a set of attack intentions.

Take SSH brute force as an example:
- Type of the attack target: ssh service
- Technical means: brute force
- Timing characteristics: short-time high intensity
- Attack phase: reconnaissance
- Consequences: obtaining permissions or information collection

60 attack patterns have been defined and some of them are shown in table 1.
Table 1. Some of attack patterns.

| Attack phase          | Target Characteristics       | Attack intent           |
|-----------------------|------------------------------|-------------------------|
| SSH brute force       | reconnaissance               | Service: SSH            |
| WebLogic deserialization | exploitation       | Middleware: WebLogic   |
| SQL injection         | exploitation                 | Application             |

3.2. Data fusion framework of multi-source heterogeneous

The difficulty of multi-source heterogeneous situational data fusion lies in:
- The log data collected by different security vendors and devices are inconsistent in describing network attacks.
- The description of the same situational information is inconsistent.

This paper intends to use the attack pattern as the key factor in describing the network attack and integrates three sources of heterogeneous situation data to extract and describe the abstract attack intention. The framework is shown in figure 2.

![Data fusion framework](image)

The framework is divided into the data layer, event layer, and status layer. The event layer uses data feature extraction to perform attack pattern correlation matching to form a single attack action. The state layer uses context attack semantics and causal chains to achieve attack scenario restoration and attack prediction. The framework data processing flow is as follows:

3.2.1. Feature extraction of multi-source heterogeneous network situation data.

According to the attack pattern defined in this paper, three main types of information: target characteristics, attack mechanism, and attack intention in network attack situation data need to be extracted. By establishing a mapping relationship between the normalized attack situation data field and the unknown attack situation data field, the target, mechanism, and intention information of the attack situation are extracted.
3.2.2. Association of attack patterns

This paper has defined 60 types of attack patterns, which match target characteristics, attack mechanisms and attack intents one by one. If the existing attack patterns are met, this attack situation is classified as corresponding attack behavior. The matching process is shown in figure 3.

![Figure 3. Attack pattern matching flowchart.](image)

If the extracted attack features cannot match the existing attack pattern or there are too few features that cannot match the existing attack pattern, a single attack feature will match the corresponding standard specification. In the case of only the characteristics of the attack mechanism, the keywords of the attack mechanism match CAPEC or ATT & CK; in the case of only the attack intention or target characteristics, it matches CVE or CWE (Common Vulnerability Enumeration) [21] to complete the classification of attack patterns.

Take the extraction of target characteristics and attack intentions of unknown attacks as examples. The CVE number information in the attack situation data is used to extract the target platform information and attack hazard information. Besides, the CVE has a unique mapping in the CWE to correlate CAPEC. Combine the targets, mechanisms, and hazard characteristics extracted from the CVE to determine the division of unknown attack modes, shown in figure 4.

![Figure 4. Unknown attack pattern matching example.](image)
3.2.3. **Normalization of attack situation data**

After the attack pattern association matching is completed, the situation data forms a triple-paradigm structure of the entity-attack mode-entity. Taking the attack mode as the core, it has a normalized data structure with a complete attack mechanism, target characteristics, and attack intention, and still retains the basic information in the attack situation data-attack source IP, targets IP, attack source port number, target port number, etc.

At the same time, for the general information lacking in attack situation data, such as IP geographic information, the data is expanded and dimensioned while normalizing, forming rich text situation data using security analysis.

3.2.4. **Correlation of attack action status based on the causal chain**

The state layer derives the association of the attack action and the attack state based on the single attack and the causal relationship formed by the event layer. The related mathematical logic reasoning is as follows:

Assume that $apa_i$ and $apa_j$ are abstract attack actions that occur in time slice $i$ and time slice $j$, A causal chain between attack actions $apa_i$ and $apa_j$ is expressed as $apa_i \rightarrow apa_j$, if and only if:

$$\exists p \mid \text{postcondition}\_\text{path}(apa_i, p) \cap \text{precondition}\_\text{path}(p, apa_j) \quad (2)$$

The consequence state $p$ of $apa_i$ is the prerequisite state of $apa_j$, then between $apa_i$ and $apa_j$ includes a plurality of abstract relations associated with state $p$.

At the same time, it is assumed that specific attack actions $ap_i$ and $ap_j$, and corresponding abstract actions $apa_i$ and $apa_j$ exist, thereby deriving the association of specific attack actions.

$$\exists ap_i, ap_j \mid \text{abstraction}\_\text{path}(apa_i, ap_i) \cap \text{abstraction}\_\text{path}(apa_j, ap_j) \Rightarrow ap_i \rightarrow ap_j \quad (3)$$

If and only if the following conditions are met, there is a causal chain relationship $apa_i \rightarrow g_j$ between the abstract attack action $apa_i$ and the target state $g_j$.

$$\exists apa_i \mid \text{abstraction}\_\text{path}(apa_i, ap_i) \cap \text{precondition}\_\text{path}(apa_i, g_j) \cap \text{description}\_\text{edge}(p, g_j) \quad (4)$$

3.3. **Multidimensional analysis of attack patterns**

The normalized network attack situation data formed with the attack mode as the core fusion contains the behavior characteristics of the attacker. By defining and establishing the pre-relationship and post-relationship of atomic-level attack behavior, the behavior pattern of the attacker is mined, and an analytical model based on behavior characteristics is constructed.

This paper combines a single attack behavior analysis and multi-dimensional attack behavior correlation to form a composite attack behavior analysis model.

3.3.1. **Analysis of single attack behavior.**

A single attack behavior analysis uses a certain attribute in the attack event as a fulcrum, such as the number of attacks, the duration of the attack, the source and destination IP geography, and the industry to which the IP belongs. At the same time, associated threat intelligence is used to judge the credibility of the attack event.

For example, the density attributes of attack behaviors are extracted from the fused situation data, focusing on high-duration and high-density types of events, such as SSH brute force attacks, FTP brute force attacks, etc. By filtering long or high-frequency event characteristics greatly reduce the workload of analysts. The specific method is to pay attention to the duration of the security event and the attack.
frequency of the security event. Comparing the custom-set duration and intensity baseline, three different types of events can be generated: high duration low-frequency attack events, high duration high-frequency attacks, and low duration high-frequency attacks.

Secondly, the geographic attributes of the source and destination IPs are extracted from the fused situation data, and a geographic location baseline is formed based on historical alerts or normal access behavior. The events in which the geographic information of the source address or the destination address matches the characteristics of the outliers are extracted.

After the security event is generated, the inference model links the threat intelligence to judge each attribute of the generated event. The judged attributes include, but are not limited to, the attack source IP, the attacked IP, the URL information involved in the event, the host information and the file hash value.

Annotate events based on threat intelligence hits, such as malicious scan sources, brute force crack sources, zombie hosts, malicious sites, etc.

3.3.2. Compound behavior analysis

Compound attack behavior analysis is based on Lockheed Martin's kill-chain theory, which divides attacks into seven different stages: reconnaissance, weaponization, delivery, exploitation, command and control, execution, and maintenance, as shown in figure 5.

![Figure 5. Seven stages of the kill chain.](image)

According to the sequence of events and the kill chain stage, various events for the same target IP will be aggregated together, and the capture stage will identify whether the attack chain has been captured. There are currently three types of kill chain:

- Being attacked but not yet captured. This type of kill-chain contains events in at least two different stages and does not include events in the command and control, execution and maintenance stages. This type indicates that the target asset is under attack but not invaded.
- Suspected to be compromised. This type of kill-chain contains at least two events at different stages, and at least one command and control, execution and maintenance events. This type indicates that the detected event during the capture phase is related to the target asset and it is determined that it may be controlled by the attacker.
- Single-stage multi-type attack. The kill-chain contains only events in a single attack chain phase, but there are more than two types of attack patterns. It shows that the target asset has suffered multiple types of attack patterns at the same time, but is not controlled by the attacker.

The attacker's behavior pattern preference is found by aggregating the composite behavior sequence in the result and the expert chain decision tree is used to make the multi-layer decisions on the kill-chain. Prioritize high-threat kill-chains to improve the efficiency of operation and maintenance analysts.

4. Analysis of operating results

Multi-source heterogeneous network security situational awareness data fusion framework based on attack patterns is tested by accessing three different types of probe device traffic in actual business scenarios. The daily processing log volume reaches 1 million and the running time exceeds one month. Three different types of high-confidence threat events were found in the data and the entire attack process was restored.

According to the description of the attack patterns in the three different types of traffic probes, which have been matched with 60 predefined attack pattern characteristics, the three types of heterogeneous original situation data are effectively normalized into security events based on the attack pattern.
on the kill-chain model, the attack state with context semantics is extracted from the normalized security events to form a kill chain and the multi-source heterogeneous network situation data is aggregated.

From the actual results of the framework, the 24 million original situation data is normalized into 630,000 fusion event data, and 14,000 attack scene data are constructed with a data compression ratio of 1714:1, as shown in figure 6, which effectively reduces the amount of analysis by analysts.

Analyzing from the framework event layer, the three types of raw situational data are fused into six types of events (including buffer overflow, injection, worm, Trojan, scanning, brute force cracking), as shown in figure 7.

It can be found in figure 7 that the event layer is mainly brute force and scan events. Operation and maintenance personnel can strengthen the blocking of detection sources such as scanning and brute force. The framework extracts high-value single-attribute analysis events such as long-term high-intensity attacks, overseas attacks and Trojan horse file transfers for single attributes such as geographic information and frequency at the event layer. These events account for about 15% of the total number of events at the fusion layer. It can also reduce the workload of the analyst, as shown in figure 8.
Figure 8. Event type statistics of event layer.

From the analysis of the statistical results of the framework state layer, as shown in Figure 9, the reconnaissance status event accounted for 81%, followed by the command and control phase. Operation and maintenance personnel can give priority to further research and judgment of events in the exploitation, command and control and delivery phases, which account for 19%, effectively improving analysis efficiency.

Figure 9. Status layer statistics.

According to the causal chain and kill chain model, three high-threat state events were found from the situation data, and the corresponding attack intentions were analyzed through the association of abstract actions, as shown in Table 2.

| Kill-chain conclusion      | Attack intention                                  |
|----------------------------|---------------------------------------------------|
| 1  Mining Trojan           | Unauthorized access and resource abuse            |
| 2  Trojan implant through webshell | Unauthorized access and control                  |
3. Trojan implant through SQL injection  Data tampering and destruction

By dividing the stages of the kill chain of the incident, the intrusion behavior is restored. Take the mining Trojan as an example, the attacker first implants the Monero coin mining program (delivery phase), and then the mining program connects the mining pool to perform the mining action (command and control phase). The behavior of the remote control phase is consistent with the kill chain judgment. Therefore, it is inferred that the target machine is infected with a mining Trojan.

5. Conclusions and prospects
This paper proposes a multi-source heterogeneous network security situational awareness data fusion framework based on the attack pattern. Through the test of actual business scenarios, it effectively fuses multi-source heterogeneous security log data into 60 predefined attack patterns. The normalized situation data formed by the framework can support reasoning based on attack behaviors and discover highly credible security threat events. The framework innovatively transforms the objects of security analysis from the original security log association to the analysis of the attacker's behavior characteristics, effectively compressing the data analysis magnitude in the big data environment.

The data fusion framework mainly solves the security data fusion and threat identification issues under the big data architecture. The framework fuses heterogeneous situational data into normalized attack behavior characteristics through feature matching. Compared with traditional original log correlation, this method effectively fuses original logs representing the same behavior and uses attack behavior analysis to replace original log analysis which reduces the workload of analysts. Besides, based on the causal chain and attack chain models, the aggregation of attack behaviors against specific target assets, and effective identification of high-threat events through the reduction of the attack process.

The current matching is mainly based on fuzzy matching by related standards and specifications. The matching result is usually an abstract attack pattern. This level of attack pattern lacks detailed target characteristics, attack mechanisms, and attack intentions, which can support high-level reasoning. The next step is to study natural language understanding and knowledge maps to achieve highly accurate matching of attack patterns.

Acknowledgments
This work was supported by the National Key R&D Program of China(N0.2018YFB0804703).

References
[1] MITRE.(2019) Common Attack Pattern Enumeration and Classification (CAPEC). http://capec.mitre.org/.
[2] Yuan, X. , Nuakoh, E. B. , Beal, J. S. , & Yu, H. . (2014). Retrieving relevant capec attack patterns for secure software development.
[3] Lockheed Martin.(2019) Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.
[4] MITRE.(2019) ATT&CK. https://attack.mitre.org/.
[5] Hahn, A. , Thomas, R. K. , Lozano, I. , & Cardenas, A. . (2015). A multi-layered and kill-chain based security analysis framework for cyber-physical systems. International Journal of Critical Infrastructure Protection, 11(Complete), S187454821500061X.
[6] Franklin, L. , Pirrung, M. , Blaha, L. , Dowling, M. , & Feng, M. . (2017). Toward a visualization-supported workflow for cyber alert management using threat models and human-centered design. Visualization for Cyber Security. IEEE.
[7] Choi, J. , Choi, C. , Lynn, H. M. , & Kim, P. . (2016). Ontology Based APT Attack Behavior Analysis in Cloud Computing. International Conference on Broadband & Wireless Computing. IEEE.
[8] Lee, Mungyu, Choi, Junho, Choi, Chang, & Kim, Pankoo. (2017). 14th ieee annual consumer communications & networking conference (ccnc) - las vegas, nv (2017.1.8-2017.1.11) 2017 14th ieee annual consumer communications & networking conference (ccnc) - apt attack behavior pattern mining using the fp-growth a. 1-4.

[9] Li, S., Zhu, M., & Qiu, Y. (2018, November). Attack Intent Analysis Method Based on Attack Path Graph. In Proceedings of the 8th International Conference on Communication and Network Security (pp. 27-31). ACM.

[10] Mishra, V. P., Shukla, B., & Bansal, A. (2019). Analysis of alarms to prevent the organizations network in real-time using process mining approach. Cluster Computing, 22(3), 7023-7030.

[11] Woo, S., On, J., & Lee, M. (2013). Behavior Ontology: A Framework to Detect Attack Patterns for Security. Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on. IEEE Computer Society.

[12] MITRE.(2019) Malware Attribute Enumeration and Characterization (MAECTM). https://maecproject.github.io/.

[13] ZHUUGE Jian-Wei. (2006). A network attack plan recognition algorithm based on the extended goal graph. Chinese Journal of Computers, 29(8), 1356-1366.

[14] Musa, T., Yeo, K. C., Azam, S., Shanmugam, B., Karim, A., De Boer, F., ... & Faisal, F. (2019, January). Analysis of Complex Networks for Security Issues using Attack Graph. In 2019 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-6). IEEE.

[15] Cui, Y., Li, J., Zhao, W., & Luan, C. (2019). Research on Network Security Quantitative Model Based on Probabilistic Attack Graph. In ITM Web of Conferences (Vol. 24, p. 02003). EDP Sciences.

[16] Kotenko, I., & Chechulin, A. (2013, June). A cyber attack modeling and impact assessment framework. In 2013 5th International Conference on Cyber Conflict (CYCON 2013) (pp. 1-24). IEEE.

[17] REINECKE, P., Mont, M. C., & Beresna, Y. (2019). U.S. Patent No. 10,262,132. Washington, DC: U.S. Patent and Trademark Office.

[18] Pal, A., Arzi, L., & Leiderfarb, T. (2019). Method and system for modeling all operations and executions of an attack and malicious process. U.S. Patent No. 10,440,036. Washington, DC: U.S. Patent and Trademark Office.

[19] Fikes, R. E., & Nilsson, N. J. (1971). Strips: a new approach to the application of theorem proving to problem solving. Artificial Intelligence, 2(3-4), 189-208.

[20] MITRE.(2014) Common Platform Enumeration(CPE). https://cpe.mitre.org/.

[21] MITRE.(2019) Common Weakness Enumeration(CWE). https://cwe.mitre.org/.