CASCADES: Modeling and Simulation of Cyber Attacker Behaviors for Network Threat Analysis

[1]Stephen Moskal, [2]Michael Kuhl, [1]Shanchieh Jay Yang
[1]Department of Computer Engineering, [2]Department of Industrial Systems and Engineering
Rochester Institute of Technology, Rochester, New York 14623
{sfm5015, mekeie, jay.yang}@rit.edu

I. Introduction

Recent high-profile data breaches has caused a shift in the cyber security field to focus more on prevention of cyber attacks as opposed to detection of threats. Security assessments of enterprise computer networks by the use of vulnerability assessment tools and penetration tests are now common and in most cases a requirement. Despite these prevention techniques, recent data breaches are causing billions of dollars of losses to companies as current techniques are not capable of exposing all issues in a network. The complexity of this problem is the result of the size a network and the sheer number of configurations possible along with the diverse skills and attack preferences of the adversaries. Static network analysis that uses attack graphs, *e.g.,* [1], [2], [3], [4] exhaustively exposes attack paths but struggles to provide realistic attack scenario representation because only vulnerability data is used. Game Theory ([5], [6]) and Agent-based ([7], [8]) modeling techniques were applied to this application to capture how the attacker interacts with the network but where not flexible in the types of attacks that could be modeled. Simulation has been applied to the cyber domain ([8], [9], [10]) and is a promising technique, however due to the complexity of the problem it is difficult to achieve realistic simulations. This work expands on [10] by developing a cyber attack simulator that identifies key aspects of computer networks and cyber attack behaviors to provide a realistic simulation while reducing the model complexity.

CASCADES (Cyber Attack Scenario and Network Defense Simulator) is a cyber attack scenario simulation platform that exposes the relationship and dependency of the cyber attacker's behaviors to the physical network configuration. By modeling both the network and the attacker it is possible to understand how an attacker effects a network but also how a network configuration effects the attacker's progress given an attack scenario. CASCADES employs a knowledge-based behavior model [11] representing the capabilities, opportunities, intent, and preferences of the individual attacker to aid in the understanding of the key information the attacker needed to make decisions as the attack progresses. By representing the attacker based on the knowledge developed throughout an attack and how the attacker uses that information along with the integration of the Cyber Attack Kill Chain, CASCADES provides the capability of representing a wide variety of attackers while still maintaining realistic attack scenarios. This allows the generation of many attack graphs while maintaining accuracy along with understanding the interplay between the attacker and the defender without requiring an expert to configure. Preliminary results of CASCADES shows both the types of attackers play a large role in how resilient an network is to an attack but also the effects of how a misconfigured network has on the attacker's progress.

II. Context Models for Simulation

CASCADES is a multithreaded model-driven cyber attack simulator built off the previous efforts of MASS in [10]. CASCADES uses 4 major context models: Virtual Terrain (VT), the Vulnerability Database, Attacker Behavior Model (ABM), Intent Module. The VT is the description of the physical network consisting of routers, machines, and the connections between them. This also contains the services that are installed on the machines which describes the vulnerabilities. All vulnerability data is stored in the Vulnerability Database which is a preparatory database consisting of data from NVD, MITRE, Snort, etc.

A critical component of CASCADES is the ABM which houses the logic to select the actions performed by the attacker. The ABM uses the network knowledge gained from performing reconnaissance or previously attempted attack actions to influence the type of attack the attacker may choose along with the preference the attacker may have on certain types of targets or actions. Tightly coupled with the ABM, the intent module describes the goals or the intentions of the attacker for the simulation. The intent can be described as generically to attack a certain type of machine (*e.g.,* customer information database) or strictly "if... then" intentions to provide more robust and reactionary intents. Other context models are also defined in CASCADES including: moving target defenses (MTD), intrusion detection systems (IDS), and the noise generator (generates normal network traffic). Figure 1 shows the overall system architecture of CASCADES.

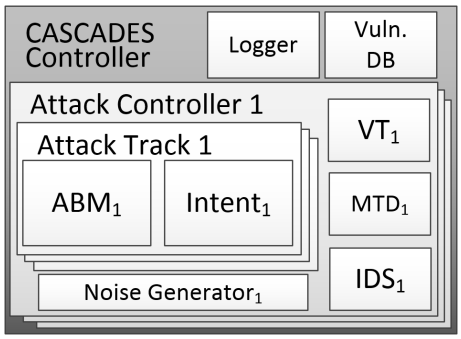

Fig. 1: The overall CASCADES system architecture

III. Experiments and Analysis

A test network is set up with 16 machines modeled with key aspects commonly found in enterprise networks like DMZ's, guest networks, administrative machines, and high security subnets. For these simulations, the intent of the attacker was to exfiltrate information contained on the backup server located in the deepest part of the network. For these experiments, three different types of attackers were modeled: an amateur, an expert, and a random attacker. The amateur attacker has a limited skill set, is not concerned with being caught, and gives up easily upon failure. The expert attacker is methodical in the types of targets they choose and uses stealthy attack actions. Whereas the random attacker is a brute force attacker that literally randomly selects actions which is used as a worst case baseline. For comparison, the three attackers are simulated on the base network as well as a misconfigured network with a firewall misconfiguration exposing a secured machine to the internet to demonstrate how the network configuration effects the attacker's progress. Each case and attacker is simulated 1000 times to measure the variance between simulations. Figure 2 shows an example of a single simulated step of an attack path using the CASCADES UI.

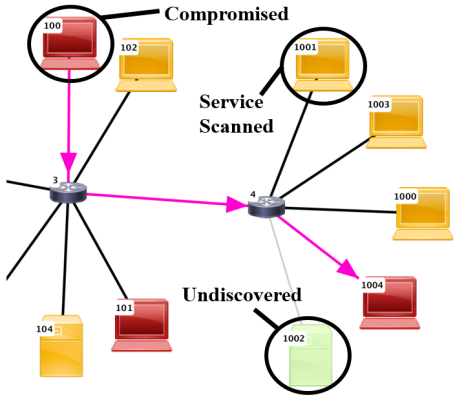

Fig. 2: A partial simulated attack path on a network showing the state of the affected machines.

Table I shows the number of actions taken to achieve the intent and the failure rate (percent of time the attacker failed to achieve their intent) for both of the networks and the three attackers. In the case of the base network, both the amateur and expert attacker took the same average amount of steps to complete their intent. This is due to the amateur attacker having the necessary skills to penetrate the network along with the network being small enough that the amateur could find the goal machine. However, the amateur failed to achieve their intent 17.8% of the time on the base network compared to the 1.8% of the expert. When analyzing the misconfigured network the number of actions performed for both the expert and the random attacker decreased significantly while the amateur increased slightly. This is because the amateur did not have the skills to successfully take advantage of this newly introduced security hole in the network. It can also be seen that with this misconfiguration the naive random attacker is approaching the average number of steps that the amateur attacker, which is concerning from an analysis perspective because even the brute force case is performing well incomparison.

TABLE I: Simulation statistics for both network types and the three attackers.

Network Config.		Amateur	Expert	Random
Base	Avg. Steps	27.5	27.6	47.4
	Failure Rate	17.8	1.8	0
Error	Avg. Steps	28.8	20.4	33.5
	Failure Rate	15.5	1.2	0

IV. Lessons Learned & Conclusions

The test example shown in this abstract demonstrates the capability to analyze various different types of attackers in different situations by evaluating the knowledge the attacker gains throughout an attack scenario. CASCADES has additional capabilities such as exposing critical weaknesses in a network based on the frequency of attacks on a particular machine or the frequency a service or vulnerability is attempted and a fully functional UI for analysis of attacks. We learned that by modeling the attacker's decisions based off of the knowledge gained throughout an attack and applying a Cyber Attack Kill Chain to the simulation, simulation is viable and promising approach to network threat analysis. The results of this work also emphasized the complexity of a cyber attack and what makes each cyber attacker different from one another. From this work we have a better understanding of what are the parameters needed to represent cyber attacker behaviors and knowledge and we can refine and add new parameters to better model behaviors which then provides better analysis of network threat resilience.

References

[1] S. Jha, O. Sheyner, and J. Wing, "Two formal analyses of attack graphs," in *Proceedings of 2002 15th IEEE Computer Security Foundations Workshop]*. IEEE, 2002, pp. 49–63.

[2] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing, "Automated generation and analysis of attack graphs," in *Proceedings of 2002 IEEE Symposium on Security and Privacy*. IEEE, 2002, pp. 273–284.

[3] I. Kotenko and E. Doynikova, "Security assessment of computer networks based on attack graphs and security events," in *Proceedings of ICT-EurAsia*, 2014, pp. 462–471.

[4] ——, "The capec based generator of attack scenarios for network security evaluation," in *Proceedings of 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, vol. 1. IEEE, 2015, pp. 436–441.

[5] B. Wang, J. Cai, S. Zhang, and J. Li, "A network security assessment model based on attack-defense game theory," in *Proceedings of 2010 International Conference on Computer Application and System Modeling (ICCASM)*, vol. 3. IEEE, 2010, pp. V3–639.

[6] K. Chung, C. A. Kamhoua, K. A. Kwiat, Z. T. Kalbarczyk, and R. K. Iyer, "Game theory with learning for cyber security monitoring," in *Proceedings of 2016 IEEE 17th International Symposium on High Assurance Systems Engineering (HASE)*. IEEE, 2016, pp. 1–8.

[7] I. Kotenko, "Agent-based modeling and simulation of cyber-warfare between malefactors and security agents in internet," in *Proceedings of 19th European Simulation Multiconference "Simulation in wider Europe"*, 2005.

[8] D. Grunewald, M. Lützenberger, J. Chinnow, R. Bye, K. Bsufka, and S. Albayrak, "Agent-based network security simulation," in *Proceedings of The 10th International Conference on Autonomous Agents and Multiagent Systems-Volume 3*. International Foundation for Autonomous Agents and Multiagent Systems, 2011, pp. 1325–1326.

[9] S. Moskal, D. Kreider, L. Hays, B. Wheeler, S. J. Yang, and M. Kuhl, "Simulating attack behaviors in enterprise networks," in *Proceedings of 2013 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2013, pp. 359–360.

[10] S. Moskal, B. Wheeler, D. Kreider, M. E. Kuhl, and S. J. Yang, "Context model fusion for multistage network attack simulation," in *Proceedings of Military Communications Conference (MILCOM), 2014 IEEE*. IEEE, 2014, pp. 158–163.

[11] S. Moskal, "Knowledge-based decision making for simulating cyber attack behaviors," Master's thesis, Rochester Institute of Technology, 2016.