International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 09 | Sept -2020 ISSN: 2582-3930

Security-Aware Defense Mechanism for Advanced Persistent Threats

Ms.S. Vedavathi[1], Mr.V. Rahamthulla[2]
[1]PG Scholar, Dept. of MCA, SVIM, Tirupati,
[2] Assistant Professor, Dept. of MCA, SVIM, Tirupati, A.P.

ABSTRACT

TODAY'S security threat landscape is experiencing an accelerating evolution, which is far more dangerous than it was ten or even five years ago. Enterprises all of sizes may be overwhelmed by surging and increasingly sophisticated attacks, especially APTs with the damage and costs multiplied at a shocking rate. According to the statistics of Arbor Networks, APTs have become the number one threat on the mind of over 60% of enterprise participants, jumping ahead of DDoS attacks by 2016. As ATPs' two main intrinsic properties that distinguish from typical attacks, both advancement and persistence touch upon the diversification of attack types and methods. The former manifests stealth and uncertainty in attack path, rendering traditional signature approach targeting known attacks no longer adequate. While the latter indicates they always process through multiple stages over a long period of time, making single point detection technology lose desired effects. All of this is placing enormous pressure on enterprises to keep up the struggle and bringing forward higher request to 'security as a service' offerings. Under multiple attacker resources, defense control policy is implemented on two-stage decisions involving proportional fair resource allocation and host-attack assignment. In particular, distributed auction-based assignment algorithm is designed to capture uncertainty in the number of resolved attacks, where high-risk host-attack pairs are prioritized over others. We theoretically prove our mechanism can guarantee bounded queue backlogs, profit optimality, no underflow condition and robustness to detection errors. Simulations on real-world dataset corroborate theoretical analysis and reveal the importance of security awareness.

Keywords—Security awareness, priority-based response, APT attacks, threat intelligence, distributed auction algorithm.

INTRODUCTION

Our study highlights the intriguing role of perturbed Lyapunov optimization, where weights used for defines decision making are carefully perturbed. To accommodate host risk tolerance and avoid resource under-utilization, we develop tolerable risk admission control policy by pushing host risk levels towards certain values. By exploring temporal evolution of risk level, we formulate it as priority-aware virtual queues, which combined with attack queues, provide an integration ofhost

heterogeneity to queuing optimization. The defines control policy involving resource allocation and host-attack assignment is conducted. Such assignment issue, a minimum cost maximization flow problem in essence, is non-trivial to solve, further complicated by uncertainty in the number of resolved attacks. We construct a virtual auction market, where attack events bid for response chances provided by associated hosts. The proposed distributed auction-base assignment algorithm realizes security-aware response among hosts. All of this is placing enormous pressure on enterprises to keep up the struggle and bringing forward higher request to 'security as a service' offerings. Intelligence-driven security protection integrating detection and response capabilities would be a promising approach. Its essence lies in exploiting acquired threat intelligence(e.g., threat context, implications and motives) to facilitate response decision-making, whose realization is inseparable from the development of detection technology. An intelligent defender is more informed to identify potential risks and take decisive actions to defend against APTs. Cisco has stayed ahead of the latest threats by virtue of threat-centric security architecture. As leader in intelligence-driven security-asa-service, FireEye can identify connections between alerts,prioritize alerts and ensure intelligent and rapid response.The key problem in many security protection domains is how to efficiently allocate security resources to protect targeted hosts from potential threats. From perspective of attack defense confrontation, resource allocation problem can be cast in game-theoretic contexts. Extensive researches have been devoted to this subject. Another appealing line of research focuses on risk management. Using security paradigms like attack graphs or attack trees enables defenders assess risks based on cause-consequence relationships between network states, and further determine minimum-cost hardening measures.

RELATED WORK

We particularly identify two major challenges in defense against APTs, each of which could be addressed in this paper: Dynamic and long-lasting response: To capture APTs persistence, new requirements for attack response have been raised, undercutting the ability of traditional game models that target episodic and one-off attacks. Defenders are pressured to explore the right talent to provide dynamic and long-lasting response. Such demand is indispensable for keeping up with any change of attack-defense confrontation and maintaining proactive posture against APTs. Security-aware response: The conflict between limited defense budget and dramatic rise in attack number highlights the necessityof

security-aware response, i.e., prioritizing high-risk attacks in response. Due attention has been given to risk heterogeneity mainly on attack rate in previous works. However, which begs the questions: besides heterogeneous rate, is there any new prominent heterogeneity in host security state, especially under threat intelligence. To this end, we develop a Lyapunov-based intelligence driven defense mechanism to enable long-lasting and security aware response among risky hosts. Consider a defense system with N independent hosts, an attacker and a defender. Backed by threat intelligence, we construct an attack graph that explicitly models attack-defense confrontation. Inspired by FlipIt game, each confrontation outcome manifests itself as attack graph changes, where each player takes control over the target host by flipping it subject to a cost. From perspective of the defender, total system profit is the difference between defense utility gained from resolving attacks and defense cost incurred. We are interested in the long-term time average system profit.

ADVANCED PERSISTENTTHREAT

Persistent is specially designed to serve long time, it stealth itself that means it kills-itself to hide from anti- virus or scanners and regenerate until goal reached. Attacks are unauthorized activities with malicious intent using specially crafted code or techniques.

Threats are classified into 6 steps they are given below:

SCOPE

In defense against APTs, each of which could be addressed in this paper: Dynamic and long-lasting response: To capture APTs persistence, new requirements for attack response have been raised, undercutting the ability of traditional game models that target episodic and one-off attacks. Defenders are pressured to explore the right talent to provide dynamic and long-lasting response. Such demand is indispensable for keeping up with any change of attack-defense confrontation and maintaining proactive posture against APTs. Security-aware response: The conflict between limited defense budget and dramatic rise in attack number highlights the necessity of security-aware response, i.e., prioritizing high risk attacks in response. Due attention has been given to risk heterogeneity mainly on attack rate in previous works. However, which begs the questions: besides heterogeneous rate, is there any new prominent heterogeneity in host security state, especially under threat intelligence. To this end, we develop a Lyapunov-based intelligence driven defense mechanism to enable long-lasting and security aware response among risky hosts. Consider a defense system withN

independent hosts, an attacker and a defender. Backed by threat intelligence, we construct an attack graph that explicitly models attack-defense confrontation. Inspired by FlipIt game, each confrontation outcome manifests itself as attack graph changes, where each player takes control over the target host by flipping it subject to a cost. From perspective of the defender, total system profit is the difference between defense utility gained from resolving attacks and defense cost incurred. We are interested in the long-term time average system profit.

DEFENSE SYSTEM FOR ADVANCED PERSISTENT THREAT

Today's security threat landscape is experiencing an accelerating evolution, which is far more dangerous than it, was ten or even five years ago. According to the statistics, Advanced Persistent Threats (APTs) have become the number one threat on the mind of over 60% of enterprise participants, jumping ahead of DDoS attacks. In existing system Intelligence-driven security protection system has been applied. Which integrates detection and response capabilities as a promising approach? Intelligence-driven security protection integrating detection and response capabilities would be a promising approach. Its essence lies in exploiting acquired threat intelligence (e.g., threat context, implications and motives) to facilitate response decision-making, whose realization is inseparable from the development of detection technology. An intelligent defender is more informed to identify potential risks and take decisive actions to defend against APTs. With joint efforts of industry and academia, dramatic improvements in intelligent driven protection have been made. Cisco has stayed ahead of the latest threats by virtue of threat-centric security architecture. As leader in intelligence-driven security-as a-service, FireEye can identify connections between alerts, prioritize alerts and ensure intelligent and rapid response. The concept of defense in depth originates from the military discipline. Defense in depth aims to stop or defend the intruders attack. In a computer network defense in depth not only intercepts intruder's attacks on the network, but also provides time for a system auditor or administrator to identify the origin of problem and defends so that the chances of attackers invasion reduces and increases the attackers risk of detection, Defense in depth strategy continuously monitors the cloud and slows the attacker's progress and provides the time to the defender but not totally provides security it acts as security barrier, it provides intrusion detection and protection system, virus protection and removal system, whale phishing detection

and blocking system for secured electronic mails, malicious site filtering system for blocking malicious files download,vulner ability identification and patches to remedy, audit log analysis and finally USB-Media Management.

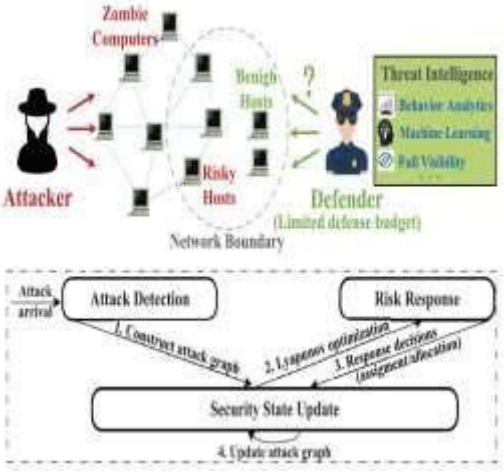
Virtualization in cloud computing is minimizes risk by

Figure 1. Advanced Persistent Threat Défense System.

enhancing security through centralized IT management, easily update service packs and patches, easily restore servers/desktops. The virtual machine manager that manages the life cycle of virtual machines on a single node is called hypervisor,then ewriskareaish ypervisor itself; it is the prime target of intruder. All assets such as network, hardware and software should be managed; identity and access management is the primary security measure towards thecloud security that means right individuals should be accessed right resource at right time for right reason.

Cloud computing security can be provided by using cryptographic techniques that is fully homomorphic encryption. and decryption. Fully homomorphic encryption is implemented on working on a virtual platform as a Cloud server, a VPN network that links the Cloud with the customer, and then simulating using cloud simtool.Security of cloud computing is based on onion layer security using fully homomorphic encryption concept of security which is to enable and provides confidentiality of data. Is concerned with protecting data at transit or at rest; also, by preventing unauthorized dis- closures and data continuous layered base monitoring and defense system is developed using defense in depth forAPT.

ARCHITECTURE



Consider the general intelligence-driven defense system consisting of two agents and N independent end hosts containing valuable data that need to be

protected. The agent who wants to attack the network to achieve some specific goals is called the attacker, while the other agent who tries to defend hosts and minimize attack effects is called the defender. To avoid being trapped, the attacker usually uses multiple zombie computers to launch attacks simultaneously. Suppose one zombie computer carries out only one attack1.For a zombie computer launching multiple attacks, we treat it as multiple zombie computers. Backed by threat intelligence, the defender first identifies potential risky zombie computers and infected hosts, and then determines when and which hosts to secure under limited defense budget. Such practiceactually constitutes the essence of intelligence-driven defense.Specifically, "intelligence" refers to the threat information acquired by the practical anomaly detection system, as shown in Section IV, while "driven" suggests that our priority-based response policy designed later highly depends on detection results. Our main contributions are highlighted.

EXPERIMENTAL ANALYSIS TO APT DEFENSE SYSTEM

Cloud Sim Tool Kit plays a great role in modeling and simulating cloud environment. Virtualization is capable of associating system/software and physical hardware on which it is running. It can be used at servers, storage, networkand enables resource sharing and utilization. A Virtual Cloud Environment is modeled by, database, user-interface and application logic, so that users are able to access and deploy applications from anywhere in controlled environment where we can replicate results based on hypothesis. It also provides capability to do experimentation.

Steps involved in defense in depth and auditing cloud for continuous monitoring to secured data storage are:

1. KeyGeneration
2. TagGeneration
3. DataIntegrity
4. Periodic SamplingBatchAudit
5. Audit forDynamicOperations

CONCLUSION

A Lyapunov-based intelligence-driven security aware defense mechanism against APTs. we develop tolerable risk admission control policy to accommodate host risk tolerance, and further implement security-aware defense control policy, where high-risk host attack pairs are prioritized over others. Simulations based on real-world dataset validate the effectiveness of our mechanism.

FUTUREENHANCEMENTS

As a future work, It is not suitable for large scale Networks so in future we can extend it. Due to resource constraints we are developed this for small scale

Networks. The major advantage of our work over it is to integrate detection into defense strategy making, and capture intelligent defender's ability to acquire threat knowledge, which are vital to enabling high response efficiency. All of this is producing new challenges for defense mechanism design.

REFERENCES

[1] T. F. Yen, A. Oprea, K. Ovariole, T. Leatham, W. Robertson, etal., "Beehive: Large-scale Log Analysis for Detecting Suspicious Activity in Enterprise Networks," in Proc. of ACM ACSAC, Dec. 2013.

[2] K. Veeramachaneni, I. Arnaldo, A. Cuesta-Infante, V. Korrapati,C. Basils and K. Li, "AI2: Training A Big Data Machine to Defend," in Proc. of IEEE International Conference on Big Data Security, Apr. 2016.

[3] Cisco White Paper, "Cisco 2014 Annual Security Report,"2014.

[4] FireEye Datasheet, "insight Threat Intelligence,"2017.

[5] W. Tong and S. Zhong, "A Unified Resource Allocation Framework for Defending Against Pollution Attacks in Wireless Network Coding Systems," IEEE Transactions on Information Forensics and Security,vol. 11, no. 10, pp. 2255-2267, Oct. 2016.

ABOUT AUTHORS:

[1]**Ms.S. Vedavathi** is currently pursuing MCA in Sree Vidyanikethan Institute of Management, Tirupati, Andhra Pradesh, India.

[2]**Mr. V. Rahamthulla,** Assistant Professor in Dept.of MCA, Sree Vidyanikethan Institute of Management, Tirupati, Andhra Pradesh, India.