An Intelligence-Driven Security-Aware Defense Appliance for Advanced Persistent Threats

D Gayathri[1], Ms.P. Sukanya[2]
[1]PG Scholar, Dept. of MCA, Sietk, Puttur,
[2] Assistant Professor, Dept. of MCA, Sietk, Puttur, A.P.

ABSTRACT

Combined with many different attack forms, advanced persistent threats (APTs) are becoming a major threat to cyber security. Existing security protection works typically either focus on one-shot case, or separate detection from response decisions. Such practices lead to tractable analysis, but miss key inherent APTs persistence and risk heterogeneity. To this end, we propose a Lyapunov-based security-aware defense mechanism backed by threat intelligence, where robust defense strategy making is based on acquired heterogeneity knowledge. By exploring temporal evolution of risk level, we introduce priority aware virtual queues, which together with attack queues, enablesecurity -aware response among hosts. Specifically, a long-term time average profit maximization problem is formulated. We first develop risk admission control policy to accommodate hosts' risk tolerance and response capacity. 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—APT attacks, threat intelligence, security awareness, priority-based response, distributed auction algorithm.

INTRODUCTION

TODAY'S security threat landscape is experiencing an accelerating evolution, which is far more dangerous thanit was ten or even five years ago. Enterprises all of sizes may be over whelmed 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 andun certainty 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. 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-asa-service, Fire Eye 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, providing insights on effective defense decision-making through mutual strategic behaviour analysis. 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

Security management is the process of which security controls are implement and security managers are subject to control.

1. Establish controls, classify data and determine which controls apply, assign responsibilities
2. Implement Controls:
   - Block and scan E-mail file attachments

- Lock Down application before a file is downloaded and it should be scanned perfectly to stop APT
- Continuous monitoring of cloud using vulnerability testing tools
- Periodic testing and scanning to control APT

Defense in depth is the security approach layered one layer on other as known as onion model of security most commonly adopted in cloud computing. Where each layer is deployed with some activity such as Security Event Monitoring, Network Security System, Data Loss Prevention and Recovery System, Forensics Analysis, Email Security, Web Security, Intrusion Detection and Prevention System, Protection system from Risks, Threat sand Attacks. A fundamental duty of intrusion detection is audit records, i.e., records of ongoing activities of the users that form a vital input for intrusion detection. But therewillbesomeoverlapsbetweenthebehavioroflegitimateusersandintruders.Cloudsecurityconcernswith anti-virus, identity management, access management and data loss prevention.

Authentication is a primary security service; the most common used procedure is verification of username and password; it is the processes of verifying who you are? Is that you say who you are? And Authorization is the processes of giving boundaries that is how much you can be accessed. Auditing consists of examination based on previous history place. Audit data is recorded in audit log files, continuous monitoring and auditing procedures should be followed based on intelligence system.

Intrusion detection system is used to detect the outside attacks; it is a monitoring system that monitors network or system activities to identify malicious activities or policy violations and produces reports to a management station. IDS are in two types they are Network Intrusion Detection System and Host Based Intrusion Detection System. Intrusion Detection and Prevention System is primarily focussing on the identifying risks, threats and attacks, audits log records information, violated security policies are determined and prevents network based, host based, wireless and data storage risks, threat sand attacks. Detections are Signature based, anomaly based and stateful protocol analysis. Where in Signature based, which compares known threat signatures to observed events to identify malwares. Anomaly based, which compares definitions of what activity is considered normal against observed events to identify significant deviations.

ADVANCED PERSISTENT THREAT

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:

Reconnaissance

Gathering of information about the target, looking for Specific areas that can be focused on to achieve long-term compromise with the minimal amount of energy or effort. This usually involves finding an individual that can be targeted to be used in intrusion.

Instrusion

Determining and finding some way to the organization to establish a foot hold. This usually does not require exploitation and is most commonly achieved by convincing a user to open an attachment or click on a link they are not supposed to open.

WhalePhising

It is a Technique of an attacker, most probably uses an e-mail that appears to be from a well-known individual or a multi-national company offering a job or business mail which seems to be related to you. It is from a criminal who wants to theft bank credit card details and other financial information. It is also for the company confidential information where you are working.

Exploitation

Intruder steals and extracts the critical information off the cloud in a stealthy way. At this stage the intruder establishes persistence and total control of the cloud. This is usually done by installing customized tools to create a communication in the cloud.

Back Door

Establishment of backdoor ultimately what the APT wants to be able to communicate with the network they are targeted. After initial intrusion has been accomplished.

Command and Control

An attacker wants to own the entire network and maintain for a long-term access for both current and future use. This usually requires obtaining, cracking or hijacking admin, and privileged credentials.

Advanced Persistent Threat is majorly classified into 6 types they are as follows:

1. Infected with a virus by browsing

2. Targeted e-mail attack
3. Induction via downloaded files
4. Infected with virus via a medium(USBStick)
5. Distributed Denial of Service attack and other Advanced Attacks.

❖ Common features of Advanced Persistent Attack

1. Identifies HTTP protocol or other communication protocols or ports that are used by the target organization, and performs back door communications.
2. Spreads Infection within the compromised system that infects a network within an organization and then spreads infection to systems by exploiting vulnerabilities. Infects many more computers in the network so that it can more efficiently steal the information stored in the system.
3. Simultaneous updates and spread viruses in chores with the extended capability module downloaded from the command and control server. It spreads in the system with capability of carrying out an effective attack.
4. Information gathering, attack spreads to a closed system via a USB and spreads to the open system via social engineering methods and websites.

Advanced Persistent Threat is a hot and controversial term used among security professional, it is the combination of different threats such as zero-day threats, polymorphic threats and blended threats. A zero-day threat is a cyber- attack on an OS or application vulnerability that is the attack launches to the public awareness of the vulnerability from day zero. Polymorphic threat is that morphs – continuously changes and makes impossible to detect for traditional signature-based security defenses to detect. A Blended threat employs multiple attack vectors it adopts stealthy procedures.

DEFENSE SYSTEM FOR ADVANCED PERSISTENT THREAT

Defense in depth is a protection procedure which challenges different attack methods through multi layered such as application, datastorage, weblogic, network, logical and physical layered security architecture. Multi- layered defense like onion layered is more protected compared to single defense system. 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, it also recovers the data losses and the successive effects towards the protection of cloud data storage. 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, vulnerability identification and patches to remedy, audit log analysis and finally USB-Media Management.

To protect the cloud computing environment from risks, threats and attacks, the security concerns are around the virtualization system/software/application and hardware. Virtualization in cloud computing is minimizes risk byenhancing 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 ew risk area is hypervisor 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 the cloud 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 which is based on arbitrary processing.The data and information security can be pro- vided to the confidential data to the cloud server by using cryptographic keys for 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

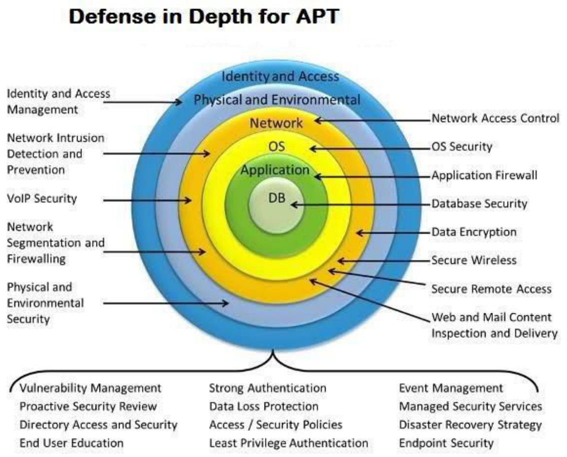
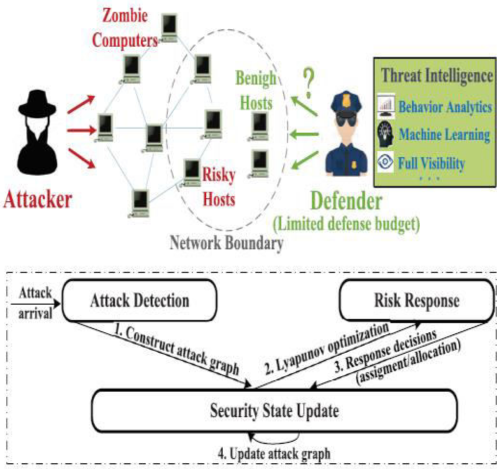

Defense in Depth for APT
Identity and Access Management
Network Intrusion Detection and Prevention
VoIP Security
Network Segmentation and Firewalling
Physical and Environmental Security
Identity and Access
Physical and Environmental
Network
OS
Application
DB
Network Access Control
OS Security
Application Firewall
Database Security
Data Encryption
Secure Wireless
Secure Remote Access
Web and Mail Content Inspection and Delivery
Vulnerability Management
Proactive Security Review
Directory Access and Security
End User Education
Strong Authentication
Data Loss Protection
Access / Security Policies
Least Privilege Authentication
Event Management
Managed Security Services
Disaster Recovery Strategy
Endpoint Security

Figure 1. Advanced Persistent Threat Défense System.

customer, and then simulating using cloud sim tool.Security of cloud computing is based on onion layer security using fully homo morphic 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- closure sand data losses.To secure clouds from malicious attack small wares and steal thviruse sa 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 itas multiple zombie computers. Backed by threat intelligence,the defender first identifies potential risky zombie computersand infected hosts, and then determines when and whichhosts to secure under limited defense budget. Such practiceactually constitutes the essence of intelligence-driven defense.Specifically, "intelligence" refers to the threat informationacquired by the practical anomaly detection system, as shownin Section IV, while "driven" suggests that our priority-basedresponse 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, network and enables resource sharing and utilization. A Virtual Cloud Environment is modeled by using data center'scapabilities as a network of virtual services which includes hardware, database, user-interface andapplication logic , so that users are able to access and deploy applications from anywhere in the Internet driven by Simulation tools open up the possibility of evaluating the practical assumption in a controlled environment where we can replicate results based on hypothesis. CloudSim has capabilities to do experimentation on risks, threats and attacks on cloud computing infrastructure and application services. 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 Sampling BatchAudit
5. Audit for DynamicOperations

CONCLUSION

We provide a Lyapunov-based intelligence-driven security aware defense mechanism against APTs. Backed by threa tintelligence, 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.

FUTURE ENHANCEMENTS

As a future work, it would be worth while to further extend our mechanism to large-scale networks.Under resource constraints, Zhang et al. proposed a two-player game model for defending against APTs with asymmetric feedback structure, where attacker can fully observe target states while largely hiding its actions from defender.The major advantage of our work over it is to integrate detection into defense strategy making, and capture intelligentdefender's ability to acquire threat knowledge, which are vitalto enabling high response efficiency. All of this is producingnew challenges for defense mechanism design.

REFERENCES

[1] Cisco White Paper, “Cisco 2017 Annual Security Report,” 2017.

[2] ISACA White Paper, “2015 Advanced Persistent Threat Awareness-ThirdAnnual,”
2015.

[3] Arbor Networks White Paper, “12th Worldwide Infrastructure Security Report,” 2017.

[4] Advanced Persistent Threat. Available: https://en.wikipedia.org/wiki/Advanced persistent threat.

[5] Cloud Security Alliance, Big Data Working Group, “Big Data Analyticsfor Security Intelligence,” Sept. 2013.

ABOUT AUTHORS:

[1]**Ms.D. Gayathri** is currently pursuing MCA in Siddharth Institute of Engineering & Technology, Puttur, Andhra Pradesh, India.

[2]**Ms P. Sukanya,** Assistant Professor in Dept. of MCA, Siddharth Institute of Engineering & Technology, Puttur, Andhra Pradesh, India.