International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 15, 2019 (Special Issue)

Design and Analysis of a Hybrid Security Framework for Zero-Day Attack

Author 1
Dehkontee Chea Cuppah
Research Scholar, Department of Computer Science and Applications,
Bangalore University, Jnanabharathi Campus,
560056, Bangalore, India.

Author 2
Ambrish G.
Guest Faculty, Department of Computer Science and Applications,
Bangalore University, Jnanabharathi Campus,
560056, Bangalore, India.

Author 3
Dr. M. Hanumanthappa
Chairperson, Department of Computer Science and Applications,
Bangalore University, Jnanabharathi Campus,
560056, Bangalore, India.

Abstract

The greatest threats against computer systems around the world come from the cyberspace in the form of cyber-attacks and the zero-day attack is one of such threats faced by computer systems around the world. A vulnerability in system firmware, software, or hardware that is still unknown to the developers or people responsible for it is known as zero-day vulnerability. A zero-day attack is an attack by hackers in which zero-day exploits are applied on a zero-day vulnerability in system firmware, software or hardware before specific security and preventive mechanisms can be identified and set for such vulnerability. This kind of attack is very challenging to defend against because those responsible for the security of such vulnerabilities are unaware of it. Zero-day attacks have been taking a serious upward surge of late and identifying such attacks in real time and quarantining it before it causes more damages to the system is a big problem that computer security personnel are faced with. This research will seek to identify ways in which zero-day attacks can be identified in real time by using a hybrid model that will be proposed. The Signature based defense technique and the Behavior based defense technique are two current security methods that have been identified and this paper will analyze these methods individually and try to find a way in which they can be combined to form a proposed hybrid model.

Keywords: Zero-day exploits, Zero-day attack, Zero-day Vulnerability, Zero-day Vulnerability.

Introduction

As the world is transitioning to a global village, the usage of network services and devices has grown rapidly over the years and such usage also comes with great security challenges. On a regular basis, computer systems face new security challenges as new devices and software are introduced into the systems and these devices or software may include unexpected vulnerabilities that widely accepted or well-known security methods may not be able to identify thus compromising the systems overall security.

Some security personnel based the security level of their system on the number of vulnerabilities they have identified and the Intrusion detection system they have in place and this action leaves their systems defenseless as the security of a system goes beyond identified vulnerabilities and having an intrusion detection system in place. A system that is susceptible to zero-day attacks cannot be considered secure. Zero-day attacks are more dangerous to a system than most attacks as it exploits unknown vulnerabilities in the system. The zero-day attack can cause grave harm throughout the system as the patches to cover the vulnerabilities being exploited are unavailable. Due to the less predictable nature of these vulnerabilities, the security risk level associated with it can be difficult to measure.

As indicated by the 2014 Internet Security Report [1] from Symantec, 2013 presented more zero-day vulnerabilities than in any earlier year and that the 23 zero-day vulnerabilities that were identified represented an increase of 61 percent when compared to 2012 and are more than the two earlier years consolidated.

In 2014, upward surge of zero-day vulnerabilities from the previous year came to a standstill as only 24 attacks (up from 23 from 2013) were reported but in the period between 2015 and October 2016, the zero-day vulnerabilities exploded greatly as a whopping 137 vulnerabilities were identified and reported.

As indicated by the 2016 Internet Threat Report [2] from Symantec. targeted attacks have increased by 125 percent from the year before 2015. Each week, on average, a new zero - day vulnerability was found in 2015

A zero-day attack is an attack by hackers in which zero-day exploits are applied on a zero-day vulnerability in system firmware, software or hardware before specific security and preventive mechanisms can be identified and set for such vulnerability.

With the current traditional security mechanisms that are in place, it is very difficult to detect zero-day attacks in real time as these mechanisms focus on already known signatures of malware and being that there are no signatures associated with zero-day attacks, they will not be detected. Exploits can go months or years before they can be identified, and this gives the attacker enough time to cause a lot of harm to the system. Using information obtained from the Zero-day danger report [3] from FireEye Security, cybercrime discovered vulnerabilities remain unknown to the public for an average of 310 days, including software vendors.

Defending against an unknown vulnerability is a very difficult task and although there are security mechanisms like antivirus, Intrusion Detection Systems and Intrusion Prevention Systems, and continuous upgrade and patching of software, it is still difficult to mitigate zero-day attacks.

Figure 1 shows the timeline of zero-day attack from the discovery of the vulnerability to the time it is patched.

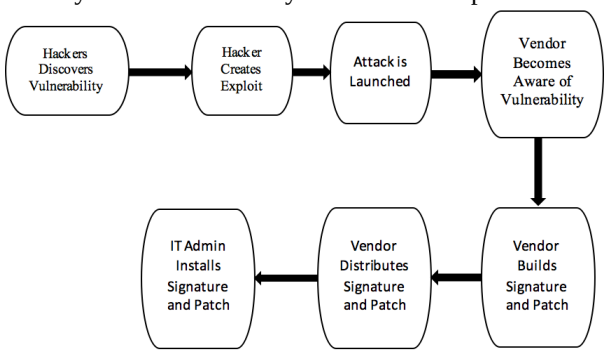

Figure 1: Zero-Day attack Timeline

With most current security mechanism being powerless against the zero-day exploit, this research paper will analyze danger associated with zero-day attacks and propose a hybrid model that will not only seek to identify zero-day attacks but also defend against it in real time. This proposed model will use the behavior-based detection technique and the signature-based detection technique to detect vulnerabilities that are known and unknown. Lastly, the paper will make a recommendation on some practical steps that should be followed to reduce the occurrence of zero-day attacks.

Definition of terms

i. Zero-day attack: an attack by hackers in which zero-day exploits are applied on a zero-day vulnerability in system firmware, software or hardware before specific security and preventive mechanisms can be identified and set for such vulnerability.

ii. Zero-day exploit: an exploit that is meant to trigger a zero-day vulnerability to gain access to a target system.

iii. Zero-day Vulnerability: a vulnerability in system firmware, software, or hardware that is still unknown to the developers or people responsible for it.

Literature Review

An attack that exploits the unknown vulnerability in a system is called zero-day attack. It takes advantage of this identified vulnerability before a patch can be developed by the vendor. The most dangerous attacks that are more difficult to detect, according to Kaur & Singh [4], are polymorphic worms that show distinct behaviors and worms pose a serious threat to network security. These worms have been rapidly propagating and increasingly threatening Internet hosts and services by exploiting unknown vulnerabilities, and on each new infection they can also change their own representations.

As it relates to the categorization of vulnerabilities, Joshi et al. [5] evaluates some of the prominent taxonomies and this assessment helps to properly categorize the vulnerabilities present in the network system environment and proposes a five - dimensional vulnerability categorization approach [6] with vector attack, defense, vulnerability exploitation methodology, vulnerability impact on the system, and the target of attack. For the identification and assessment of vulnerabilities, there are a lot of tools available and the selection of any one of those tools is important in the security of a network but the downside to these tools is that they don't detect zero-day vulnerabilities as these vulnerabilities are not known yet.

Zhichun Li et al [7] proposed for polymorphic worms an attack – resilient, noise - tolerant and fast network - based automated signature generation system called Hamsa; which enables the signature generation algorithm to provide analytical assault resilience guarantees.

CURRENT DEFENSES AGAINST ZERO-DAY ATTACKS

All networks that are connected to the have a common threat of zero-day attacks. Some of the reasons behind these attacks are stealing confidential information, disruption of activities on the system or monitoring the target's network. In this section, some of the major defense techniques that are currently being used to defend against zero-day attacks by organizations will be analyzed in-depth.

Security personnel and researchers have broadly classified these techniques into four (4) categories namely Statistical-based technique, Signature-based technique, Behavior-based technique, and Hybrid Technique.

1. Statistical-based technique
   The statistical-based technique retains a log of all past zero-day exploits that are known, and it uses information from this log to create profiles that generate new parameters to detect attacks. In simpler terms, this technique determines which network traffic or activities to allow based on its past profile and which traffic or activities to block. To do this, it must first determine which traffic is normal and which traffic is suspicious. Network traffic is matched against the log to verify if suspicious traffic is on it or not. The log must be updated regularly to record all suspicious traffic and the longer it is used on a network, the more effective and accurate it becomes as it would have fully understood the traffic flow of a network thus enabling it to determine normal activities and suspicious activities [8]. The downside to this technique is that profiles that are created from information on the log are static and cannot detect zero-day attacks in real time if such an attack has not been saved on the log.

2. Signature-based technique
   The signature-based technique is mostly used in software packages for antivirus to defend a network or system from malicious attacks in the form of worms or Trojan horse. The signature library must be updated constantly with newly identified virus signatures and for each time a new virus infection is detected or identified, the signature of such virus is stored on the signature database and this signature can now be matched against traffic coming into the network. The signature-based detection technique is sub-divided into three categories [4] namely vulnerability-driven signatures, content-based signature, and semantic-based signatures. The downside to this technique is that the signature of the attack or payload needs to be in the signature library before the system can detect it and with zero-day attacks not having known signatures, this technique is not effective in defending against such attacks.

3. Behavior-based technique
   The behavior-based technique tries to predict how the traffic on a network flow. The aim of this is to predict the network behavior in order to detect and prevent an anomalous behavior of network traffic on the network. The prediction done by the behavior-based technique can be achieved with the help of a machine learning approach that analyses current and past network activities on the victim machine, web server or server [9]. This is the only technique that can determine the major characteristics of viruses or worms by examining the byte patterns of the payload [4].

4. Hybrid-based technique
   The hybrid-based technique can be obtained from the combination of any of the three above-listed defense techniques. The aim of combination either two or all the above-listed techniques is to use the strengths of one to overcome the weaknesses of the other [4].
   This research paper will focus more on this technique.

1.2 RECENTLY IDENTIFIED ZERO-DAY VULNERABILITIES

A zero-day attack is one of the biggest threats to network systems around the world and some of the recently identified zero-day attacks have served as a wakeup call that these attacks are now getting more sophisticated and can easily bypass network defenses thus making the detection and prevention of zero-day attacks in real time very crucial [10].

Some of the zero-day vulnerabilities that were detected in recent years were mostly done by FireEye [11] and the ones they identified were:

Vulnerabilities
CVE-2017-8759-SOAP WSDL parser code injection
CVE-2017-0261-EPS “restore” Use-After-Free
CVE-2017-0262-Type Confusion in EPS
CVE-2017-0263-win32k!xxxDestroyWindow Use-After-Free
CVE-2017-0199: In the Wild Attacks Leveraging HTA Handler
CVE-2016-4117 Flash Zero-day Exploited in the Wild
CVE-2016-0167 Microsoft Windows Zero-Day Local Privilege Escalation
CVE-2016-1019 Security Advisory for Adobe Flash Player
CVE-2015-6585 Hangul Word Processor
CVE-2015-2545 MS Office, CVE-2015-2546 MS Windows
Adobe Flash Zero-Day: CVE-2015-3113
CVE-2015-1641
CVE-2015-2424
CVE-2015-1701
CVE-2015-1671
CVE-2014-0322
Internet Explorer 9 through 11 Exploit: CVE-2014-1776
CVE-2014-4148
CVE-2014-4113
CVE-2014-0502
CVE-2014-4114

Table 1: Recently Identified Zero-day Vulnerabilities

Proposed Hybrid Model

Zero-day attacks can be carryout from the time the vulnerability is identified and exploited to the time the vendor develop a patch to secure the vulnerability and counter the attack. The length of time such an attack may last for cannot really be determined as it is difficult to determine when the vulnerability was first identified.

The proposed framework will combine both the signature-based technique and the behaviour-based technique. It will be used to monitor the traffic flow coming into the network to determine whether such traffic contains malicious threats or not.

Figure 2 shows the proposed system architecture and it will consist of six (6) main components: A Packet acquisition module, Packet extraction, and disassembly module, analysis and evaluation module, signature generation, signature matching, and behaviour analysis.

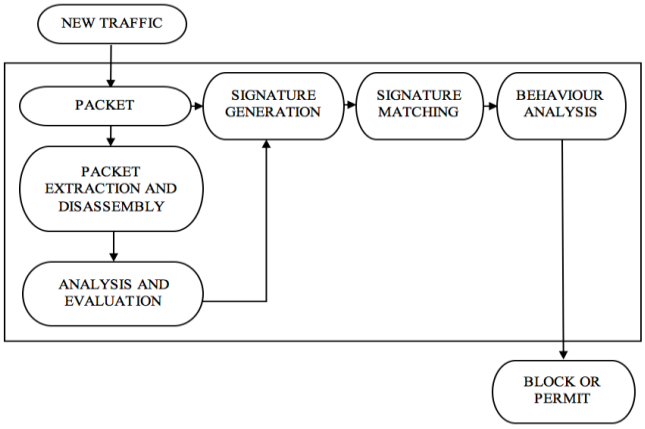

Figure 2: Signature-Behaviour based hybrid technique

Once new traffic flows into the network, the packet acquisition module will collate all packet belong to the same flow and forward it to the extraction and disassembly module. Once it gets to this module, individual packets will be extracted and disassembled and forwarded to the Analysis and Evaluation module. This module will use an Intrusion Detection System/Intrusion Prevention System to perform a deep packet inspection to identify any malware in the packets. Once this is done, the packets will be reassembled and forwarded for signature generation. Once generated, the signature will then be matched against the signature database and if it does not match any signature in the database, the traffic will then be forwarded to the behaviour analysis module for traffic flow analysis by using Hidden Markov Model machine learning approach. If no anomaly is detected in the traffic, it will then be permitted to enter the network but if an anomaly is detected no matter how small, the traffic will be blocked from entering the network.

The objective of this model is to detect anomalities and isolate all malicious content to prevent it from entering the network. This can only be achieved with the help of a machine learning based malware detection which will be placed in the behaviour analysis module.

Benefits of the Signature-Behavior based Hybrid Model

- It strengthens the the signature-based technique and the behaviour-based technique by combining the advantages of the both techniques to minimize the disadvantages of each technique.
- This technique will be able to detect zero-day attacks in real-time and will also be able to manage it before major harm is done.

Conclusion

All networks or software may have vulnerabilities, but the ones hackers target are ones that are widely used or that will cause great impact. The weakest link to any network system is through humans and most of the vulnerabilities that have been identified have either been in Adobe Flash or Internet Explorer and these platforms are frequented mostly by employees of organizations. Maintaining a secure network is difficult as networks are dynamic and have lots of uncertainties, therefore organizations should continuously seek new methods to defend their network in order to prevent hackers from exploiting vulnerabilities in the system. The proposed Signature-Behaviour based hybrid technique will thoroughly scrutinize any packet before allowing it into the network in real-time using machine learning approach to identify the attacks and does not require prior knowledge of the attack. Packets will be broken down and be analysed individually and if an anomaly is detected no matter how small, the entire traffic will be denied from entering the system/network.

Conflict of Interest

The authors declare that there is no conflict of interest as it relates to this paper.

Acknowledgment

It is a great pleasure to express my gratitude to all those who inspired and helped me in completing this paper.
I would like to express my immense gratitude to **Dr. Hanumanthappa M,** Chairperson of the Department of Computer Science and Applications, Bangalore University, for his valuable assistance and co-operation.
It is pleasure to thank **Ambrish G.** who has given me ideas and guidance during the duration of the research**.**
It is also pleasure to express my gratitude to all **Teaching and Non- Teaching staff** members of Department of Computer Science and Applications for their encouragement and providing valuable requirements.
With a deep sense of indebtedness I convey my heartiest thanks to **my parents** who have taken effort and given me such an opportunity to acquire knowledge and gain experience in my life. As well as **my friends** who have helped for this accomplished task.

References

[1] Symantec Corporation, "Internet security threat report" Retrieved from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_ v19_21291018.en-us.pdf, 2014

[2] Symantec Internet Security Threat Report, Internet Report Volume 21, APRIL 2016.

[3] FireEye Security, "ZERO-DAY DANGER: A Survey of Zero-Day Attacks and What They Say About the Traditional Security Model‖ ", 2015.

[4] Kaur, Ratinder.; Singh, Maninder., "Efficient hybrid technique for detecting zero-day polymorphic worms," Advance Computing Conference (IACC), 2014 IEEE International, pp.95-100, 21-22 Feb. 2014.

[5] Joshi, Chanchala; Singh, Umesh Kumar; Tarey, Kapil, "A Review on Taxonomies of Attacks and Vulnerability in Computer and Network System". International Journal of Advanced Research in Computer Science and Software Engineering (IJRCSSE) Volume 5, Issue 1, January 2015, pp 742-747.

[6] Joshi, Chancala; Singh, Umesh Kumar "ADMIT- A Five-Dimensional Approach towards Standardization of Network and Computer Attack Taxonomies". International Journal of Computer Application (IJCA, 0975 – 8887), Volume 100, Issue 5, August 2014, pp 30-36

[7] Li, Zhichun; Sanghi, Manan; Chen, Yan; Kao, Ming-Yang; Chavez, Brian, "Hamsa: Fast Signature Generation for Zero-day Polymorphic Worms with Provable Attack Resilience", Proceedings of the 2006 IEEE Symposium on Security and Privacy (S&P'06).

[8] Albanese, Massimiliano; Jajodia, Sushil; Noel, Steven, "A time-efficient approach to cost-effective network hardening using attack graphs" in Proceedings of DSN'12, 2012, pp. 1– 12.

[9] Alosefer, Yaser; Rana, Omer F., "Predicting client-side attacks via behavior analysis using honeypot data," Next Generation Web Services Practices (NWeSP), 2011 7th International Conference on Next Generation Web Services Practices, pp.31,36, 19-21 Oct. 2011.

[10] Hammarberg, David, "The Best Defenses against Zero-day Exploits for Various-sized Organizations", Retrieved from https://www.sans.org/reading-room/whitepapers/bestprac/defenses-zero-day-exploits-various-sized-organizations-35562, 2014.

[11] FireEye Security, "Recent Zero-Day Exploits". Retrieved from: https://www.fireeye.com/current-threats/recent-zero-day-attacks.html