Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 5, Issue. 12, December 2016, pg.143 – 149

ZDAR System: Defending Against the Unknown

Umesh Kumar Singh[1], Chanchala Joshi[2] , Suyash Kumar Singh[3]

[1] School of Engineering and Technology, Vikram University, Ujjain, M.P. India

[2] Institute of Computer Science, Vikram University Ujjain, M.P. India

[3] Institute of Engineering and Technology, Devi Ahilya Vishwavidyalaya Indore, M.P. India

umeshsingh@rediffmail.com [1], chanchala.joshi@gmail.com [2]

Abstract— Zero-day attacks are undetected through conventional signature-based defenses and hence posed a critical threat to corporate networks. They are unnoticed until a specific vulnerability is actually identified and reported. Zero-day attacks are difficult to defend against because it is mostly detected only after it has completed its course of action. Protecting networks, applications and systems from zero-day attacks is the daunting task for organization's security persons. This paper analyzed the research efforts in relation to detection of zero-day attacks. The fundamental limitations of existing approaches are the signature generation of unknown activities and the false alarming rate of anomalous behavior. To overcome these issues, this paper proposes a ZDAR (Zero-Day Attack Remedy) system for zero-day attacks analysis and detection. ZDAR system senses the organization's network and monitors the behavioral activity of zero-day exploit at each and every stage of their life cycle. The proposed approach in this paper provides a machine learning based framework to sense network traffic that detects anomalous behavior of network in order to identify the presence of zero-day exploit. The proposed framework uses supervised classification schemes for assessment of known classes with the adaptability of unsupervised classification in order to detect the new dimension of classification.

Index Terms— zero day attacks, unknown vulnerabilities, detection system, malware analysis, network security

I. INTRODUCTION

During the past few years, the rapidly growing use of network services presents the biggest challenge in protecting computing environment for being everything digital. Every day the world of digital information security faces new challenges; an incredible flood of new devices is challenging tradition methods of securing organization's network. Major software releases, introduce important new features very frequent which result in unexpected vulnerabilities [1]. Therefore, the overall security level of a network cannot be measured by simply identifying the number of known vulnerabilities present in the system. The securing network system is more than patching known vulnerabilities and deploying firewalls or IDSs. The safer network configuration has little value if it is vulnerable to zero-day attacks. Zero-day attacks pose a serious threat to the organization's network, as they can exploit unknown vulnerabilities. The vulnerabilities that are unknown could cause harm at any level of the system's security because of unavailability of patches. Also, the security risk level of unknown vulnerabilities is difficult to measure due to less predictable nature of them.

According to Symantec's Internet Threat Report of 2016 [2], there is 125% increase in targeted attacks from the year before in 2015. Also, a new zero-day vulnerability was found every week, on an average, in 2015. The zero-day vulnerabilities continue to trend upward from the last six years with 8 zero-day vulnerabilities reported in 2011, 14 zero-day vulnerabilities reported in

2012 and 23 zero-day vulnerabilities in 2013 which is doubled from the year before. In 2014, the number held relatively steady at 24. However, in 2015, an explosion in zero-day vulnerabilities reaffirms the critical role of zero-day attacks. 82 zero-day vulnerabilities were reported in 2016 up to the month of October. These estimates include only vulnerabilities that were eventually reported; the true number of zero-day vulnerabilities available to attackers could be much higher. Figure 1 shows zero-day vulnerabilities from 2011 to October 2016.

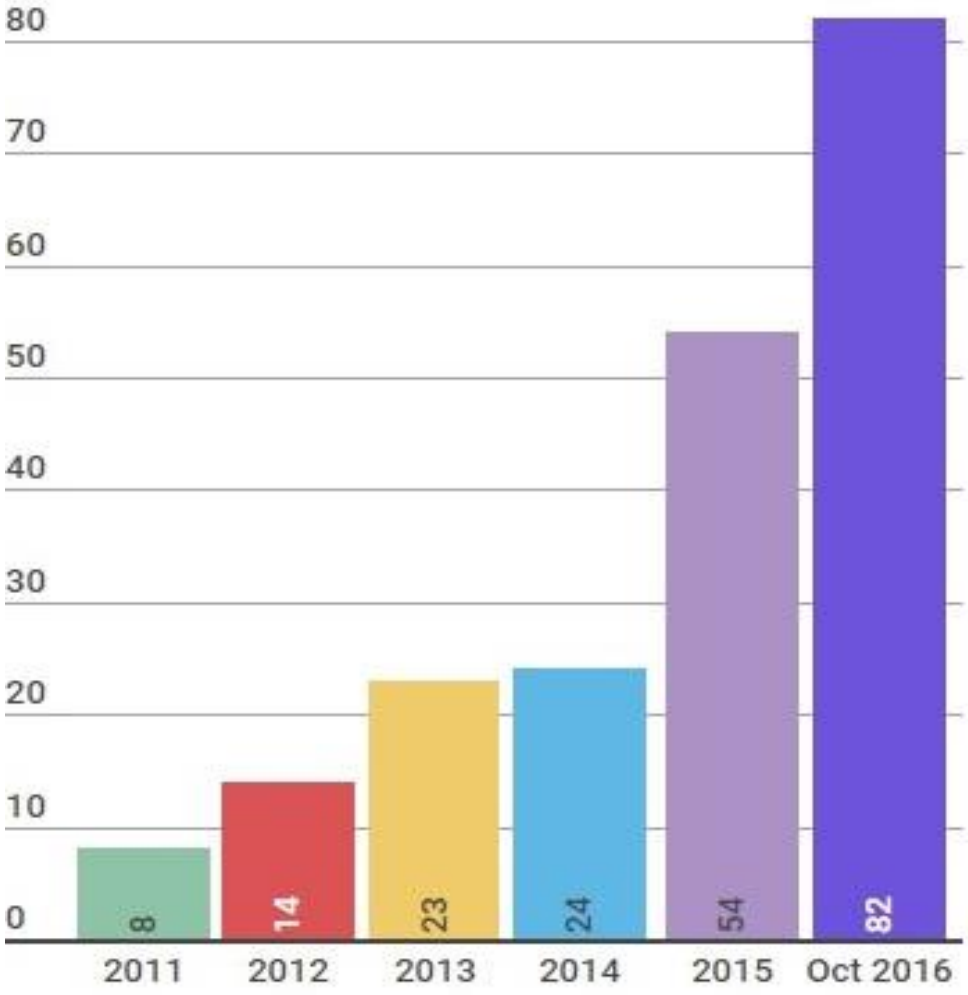

Fig1. 2011 – 2016 Zero- Day Vulnerabilities

Zero-day attacks are the attacks against system flaws that are unknown and have no patch or fix [3, 4]. With traditional defenses it is extremely difficult to detect zero-day attacks because traditional security approaches focus on malware signatures, this information is unknown in the case of zero-day attacks. Attackers are extraordinarily skilled, and their malware can go undetected on systems for months or even years which gives them plenty of time to cause irreparable harm [5, 6]. So, dealing with unknown vulnerabilities is clearly a challenging task. although there are many effective solutions like IDS/IPS, firewalls, antivirus, software upgrading and patching for tackling known attacks [8], but zero-day attacks are known to be difficult to mitigate due to the lack of information. Discovering unknown vulnerabilities and figuring out how to exploit them is clearly a challenging task. Figure 2 shows the timeline of zero-day vulnerability from discovery to patch.

Fig2. Zero-Day Timeline from discovery to patch

Zero-day vulnerabilities are the most harmful among of all the hazards confronting organization's computing environment. They exposed system's flaws to the attacker before a patch is available. Zero-day vulnerabilities are unknown but sometimes software vendor knows about the flaw but has not yet issued a fix. According to FireEye report [7], vulnerabilities discovered by cybercriminals remain unknown to the public, including vendors of the software, for an average of 310 days.

A. Terminology Used for Defining the Concepts

- *Vulnerability*: Vulnerability is a weakness or bug in a software program that might be used by attackers or cyber-criminals to execute unauthorized code on a network system.
- *Exploit*: An exploit triggers the vulnerability and executes a malicious action inside the vulnerable application without knowledge of the attacked user.
- *Zero-Day attack*: A Zero-Day attack is an exploit for vulnerability for which no patch is readily available and vendor may or may not be aware, it can even infect the most up-to-date system.
- *Zero-Day Vulnerability*: An unpatched vulnerability, the term "zero-day" denotes that developers had zero days to fix the vulnerability.
- *Alarm*: An alert which indicates that a system is or being attacked.
- *True Positive*: Number of correctly identified malicious code.
- *False Positive*: Number of incorrectly identified trusted code as malicious code. Alarm is generated when there is no actual attack.
- *False Negative*: Number of incorrectly rejected malicious code. Detector fails to detect actual attack and no alarm is generated while the system is under attack.
- *Noise*: Data or interference that can trigger a false positive.

Zero-day exploits require additional security defenses in order to protect network system; the traditional defenses are powerless against them. This paper described the zero-day attacks challenges, zero-day exploit identification and detection techniques and proposes a new approach to identify the zero-day attack.

This paper analyzed the dangers of zero-day attacks and proposed ZDAR (Zero-Day Attack Remedy) System to detect and rank unknown vulnerabilities. To detect unknown vulnerabilities the proposed ZDAR system involved various advanced techniques, such as polymorphic worm recognition, traffic monitoring, signature generation and attack validation. Finally, the proposed system recommends some practical steps to reduce the risks of zero-day attacks.

II. LITERATURE REVIEW

Zero day attack exploits zero-day vulnerability without any signature [9]. It takes advantage of a malware before a patch has been created. That means, for zero-day vulnerability no patch is readily available, also vendor may or may not be aware of it. The name “zero-day” shows that it occurs before the vulnerability is known; the term "zero-day" denotes that developers have had zero days to fix the vulnerability. A zero-day attack exploits a vulnerability that has not been disclosed publicly, including vendor of software, therefore, almost no defense mechanism available against zero-day attack. The anti-virus products cannot detect the attack through signature-based scanning and because the vulnerability is unknown, the affected software cannot be patched [10]. These unpatched vulnerabilities are free pass for attackers to any target they want to attack. All these facts range the market value of new vulnerability in $5000 to $250,000 [11].

According to Kaur & Singh [1] the most dangerous attacks that are harder to detect are polymorphic worms which show distinct behaviors and worms pose a serious threat to the Internet security. These worms rapidly propagated and increasingly threaten the Internet hosts and services by exploiting unknown vulnerabilities also they can change their own representations on each new infection. The same have many signatures hence their fingerprinting generation is very difficult task.

Rathor et al. [12] analyzed the log files using log correlation to detect the zero attack using attack graph. However, by nature of zero day attack, they cannot be predicted and hence remedial measures cannot be planned in advance. In the field of vulnerability categorization Joshi et al. [13] evaluates some of the prominent taxonomies, this assessment is helpful for proper categorization of vulnerabilities presents in network system environment and proposed a five dimensional approach for vulnerabilities categorization [14] with attack vector, defense, methodology used for vulnerability exploitation, impact of vulnerability on to the system, and the target of attack. There are many vulnerability scanners available for identification and assessment of vulnerabilities. Selection of these vulnerability scanners plays an important role in network security management [15,16]. However, these vulnerability scanners could not idetifiy zero-day attacks due to less predictable nature of zero-day attacks. Zhichun Li [17] proposed a fast, noise-tolerant and attack-resilient network-based automated signature generation system Hamsa, for polymorphic worms; which allowed to make analytical attack-resilience guarantees for the signature generation algorithm.

The most dangerous zero-day exploits driven by downloads, in which an exploited Web page results malware attack in system [18]. These kinds of attacks exploit Web browser’s vulnerabilities or third-party browser plug-ins. So far, some of the most hazardous zero-day exploits that play critical role in lucrative targeted attacks are Hydraq Trojan [19], Stuxnet [20], Duqu [21] and Flamer [22]. Hydraq Trojan designed to steal information from several companies. Stuxnet, vanished the Iranian nuclear program in 2010, contained four zero-day exploits never before seen. It is known as malware of the century and U.S. and Israeli government agencies are suspected of having created Stuxnet. Duqu, identified as the most sophisticated malware ever

seen, appeared in 2012 [23], used against the security firm and many other targets worldwide. An unknown high level programming language used to develop some part of Duqu malware and it exploits zero-day Windows kernel vulnerabilities. Flame malware discovered by Kaspersky Lab in 2012, exploits zero-day vulnerabilities in Microsoft Windows. These zero-day attacks are most difficult to defend because after attack only the data get available for analysis [24].

III. TRADITIONAL DEFENSES AGAINST ZERO-DAY ATTACKS

Any organization connected to the internet has one common threat of zero-day attacks. The purposes of these attacks are, sensing confidential information, monitoring target's operations, theft of commercial information and system disruption. This section analyzed the research efforts done in direction of defense against zero-day exploit. The primary goal of defense techniques is to identify the exploit as close as possible to the time of exploitation, to eliminate or minimize the damage caused by the attack [25]. The research community has broadly classified the defense techniques against zero-day exploits as statistical-based, signature-based, behavior-based, and hybrid techniques [1].

A. Statistical-based

Statistical-based attack detection techniques maintain the log of past exploits that are now known. With this historical log, attack profile is created to generate new parameters for new attacks detection. This technique determines the normal activities and detects the activities which are to be blocked. As the log is updated by historical activities, the longer any system utilizing this technique, the more accurate it is at learning or determining normal activities [26]. Statistical-based techniques build attack profiles from historical data, which are static in nature; therefore they are not able to adopt the dynamic behavior of network environment. So, these techniques can't be used for detection of malware in real time.

B. Signature-based

For detection of polymorphic worms, signature-based techniques are used to identify their new representations on each new infection. There are basically 3 categories of signature-based detection techniques [1]: content-based signatures, semantic-based signatures and vulnerability-driven signatures. These techniques are generally used by virus software vendors who will compile a library of different malware signatures [1]. These libraries are constantly being updated for newly identified signatures of newly exploited vulnerabilities. Signature-based techniques are often used in virus software packages to defend against malicious payloads from malware to worms.

C. Behavior-based

These techniques rely on the ability to predict the flow of network traffic [1]. Their goal is to predict the future behavior of network system in order to resist the anomalous behavior. The prediction of future behavior is done by machine learning approach through the current and past interactions with the web server, server or victim machine [27]. Behavior-based techniques determine the essential characteristics of worms which do not require the examination of payload byte patterns [1]

Intrusion detection and intrusion prevention signatures integrate these defense techniques. These signatures need to have two basic qualities [1], "First, they should have a high detection rate; i.e., they should not miss real attacks. Second, they should generate few false alarms". The goal of any techniques used by an organization should be to detect in real time the existence of a zero-day exploit and prevent damage and proliferation of the zero-day exploit.

D. Hybrid-based

Hybrid-based techniques combine heuristics with various combinations of the three previous techniques which are statistical-based, signature-based, and behavior-based techniques. Using a hybrid model technique will overcome a weakness in any single technique [1].

IV. RECENT ZERO-DAY VULNERABILITIES BY CATEGORY

Zero-day attacks pose one of the most serious threats to the organization's network, as they can exploit unknown vulnerabilities. The unknown vulnerabilities could cause harm at any level of the system's security, because the security risk of unknown vulnerabilities can't be measure due to less predictable nature of them [7]. Table 1 represents the sample list of recent zero-day vulnerabilities by category. The recently discovered zero-day attacks reflect that cyber-attacks are becoming more sophisticated and better at bypassing organizational defenses, so it has become crucial to detect zero-day attacks.

Table 1: Recent zero-day vulnerabilities list

Adobe/Flash	Operation Greedy Wonk	CVE-2014-0498
	Remote Code Execution	CVE-2014-0502
	Buffer Overflow	CVE-2014-0515
	Stack Based Buffer Overflow	CVE-2014-9163
	ActionScript 3 ByteArray Use After Free Remote Memory Corruption	CVE-2015-5119
	Remote Code Execution	CVE-2014-0497 CVE-2015-5123 CVE-2015-5122 CVE-2015-5119
	Operation Pawn Storm	CVE-2015-7645
Internet Explorer	Remote Code Execution	CVE-2014-1776
	Backdoor.Moudoor	CVE-2014-0322
	Memory Corruption	CVE-2014-0324
	Backdoor.Korplub	CVE-2015-2502

Given the value of these vulnerabilities, it's not surprising that a market has evolved to meet demand. In fact, at the rate that zero-day vulnerabilities are being discovered, they may become a commodity product [25]. Targeted attack groups exploit the vulnerabilities until they are publicly exposed then toss them aside for newly discovered vulnerabilities. When The Hacking Team was exposed in 2015 as having at least six zero-days in its portfolio [23], it confirmed our characterization of the hunt for zero days as being professionalized.

V. PROPOSED ZDAR (ZERO-DAY ATTACK REMEDY) SYSTEM

The zero-day attacks occur between the time period, when vulnerability is first exploited and when software vendors start to develop a counter to that attack. It is difficult to measure the duration of the time period, as it is hard to determine when the vulnerability was first discovered. Even sometimes vendors do not know if the vulnerability is being exploited when they fix it. So the vulnerability may not be recorded as a zero-day attack. However the vulnerability time period can be of several years long. According to FireEye [7], a typical zero-day attack may last for 310 days on average.

The proposed framework is visualized as a security system that monitors the network flow and deciding whether it is malicious or not. Figure 3 shows the proposed system architecture, which consists of the following six major components: data acquisition module, an intrusion detection system, information collection, feature extraction and transformation, supervised classifier, and a UI (client machine/ host/ server machine) portal.

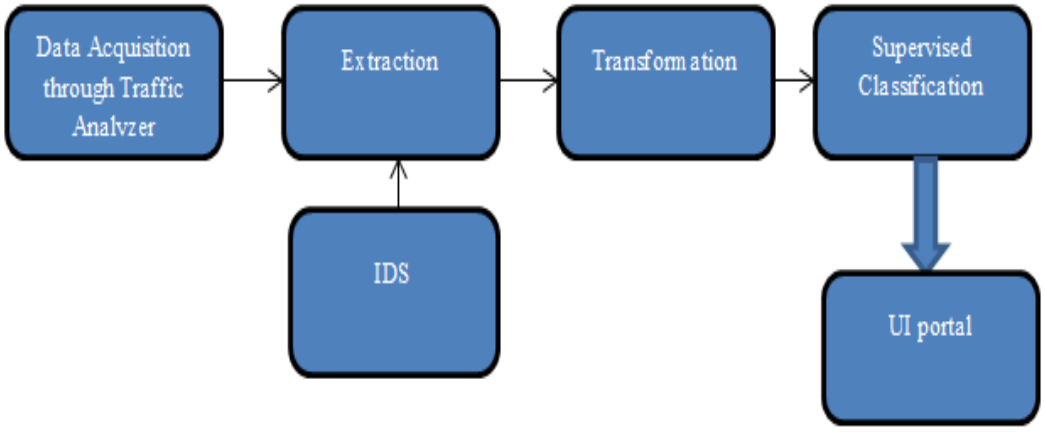

Fig 3. ZDAR (Zero-Day Attack Remedy) Framework

The data capture module is a device Traffic Analyzer (TA) which parses packets and collates packets belonging to the same flow. This module is responsible for generating all the flow-level features associated with this flow. The IDS/IPS module performs deep packet inspection and tags the flow whether it belongs to some threat. The information storage component stores all the flow features and their associated class labels. The feature extraction module extracts statistical features on a per-flow basis while the feature transformation module converts them into more robust features that will be used to build classifiers for detecting malicious flows. The classifiers are constructed in an offline fashion and are deployed to incoming network flows. The UI portal is used for reporting the emergence of new suspicious flows.

The goal of proposed framework is to detect and isolate malicious flows from the network traffic and further classify them as a specific type of the known malware, variations of the known malware or as a new (unknown) malware. To achieve this, we develop a machine-learning based malware detection and classification framework by sensing organization's network traffic features. Our proposed framework integrates the accuracy of supervised classification on known classes with the adaptability of unsupervised learning for new malware detection.

VI. CONCLUSION

Vulnerabilities appear in almost every organization, but the most attractive to targeted attackers is software that is widely used [28]. Most of the vulnerabilities are discovered in software such as Internet Explorer and Adobe Flash, which are used frequently by a large number of consumers and professionals. After discovery, the zero-day attacks are quickly added to attackers' toolkits and exploited. This paper presents a malware detection approach based on features derived from network flow characteristics. The proposed approach addresses, the supervised learning techniques and identify flows of known and unknown malware with very high precision.

Networks are dynamic in behavior with uncertainties, so new method should regularly be sought to prevent malicious attackers from exploiting unknown vulnerabilities. This paper proposes an efficient approach to detect zero-day attacks using feature extraction and transformation by sensing suspicious network connections which do not match known attack signatures at run-time. The feature transformation module discovered the suspicious connections which differentiate between the behavior of known attacks and anomalous activities. The anomaly detection technique is used to discover anomalies and thus to identify the zero-day attack types using an assigned anomaly score. The proposed method is effective and efficient in detecting zero-day attacks than the typical statistical based anomaly detection techniques.

ACKNOWLEDGEMENT

The authors are thankful to MP Council of Science and Technology, Bhopal, for providing support and financial grant for the research work.

REFERENCES

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

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

[3] Kaur, R.; Singh, M., "Automatic Evaluation and Signature Generation Technique for Thwarting Zero-Day Attacks", Second International Conference, SNDS 2014, India, pp 298-309, March 13-14, 2014.

[4] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.

[5] Y. Yang, S. Zhu, and G. Cao, "Improving sensor network immunity under worm attacks: a software diversity approach," in Proceedings of the 9th ACM international symposium on Mobile ad hoc networking and computing. ACM, 2008, pp. 149–158.

[6] J. Caballero, T. Kampouris, D. Song, and J. Wang, "Would diversity really increase the robustness of the routing infrastructure against software defects?" in Proceedings of the Network and Distributed System Security Symposium, 2008.

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

[8] L. Wang, M. Zhang, S. Jajodia, A. Singhal, and M. Albanese, "Modeling network diversity for evaluating the robustness of networks against zeroday attacks," in Proceedings of ESORICS'14, 2014, pp. 494–511.

[9] A. AlEroud, G. Karabatis, "Toward Zero-day Attack Identification Using Linear Data Transformation Techniques", IEEE 7th International Conference on Software Security and Reliability, pp 161-168, 18 - 20 Jun 2013.

[10] T. Leinster and C. Cobbold, "Measuring diversity: the importance of species similarity," Ecology, vol. 93, no. 3, pp. 477–489, 2012.

[11] L. Bilge, T. Dumitras, "Before we knew it: an empirical study of zero-day attacks in the real world", CCS '12 Proceedings of the 2012 ACM conference on Computer and communications security, pp 833-844, Raleigh, North Carolina, USA — October 16 - 18, 2012.

[12] M. Rathor, D. M. Dakhane, "Predicting Unknown Vulnerabilies in Network Using K- zero Day Safety Technique", International Journal of Advanced Research in Computer Science and Software Engineering 5 (4), pp. 221-224, April- 2015.

[13] C. Joshi, U.K. Singh, "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.

[14] C. Joshi, U.K. Singh, "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
[15] C. Joshi and U. Singh, "Analysis of Vulnerability Scanners in Quest of Current Information Security Landscape" International Journal of Computer Application (IJCA, 0975 – 8887), Volume 145 No 2, pp. 1-7, July 2016.
[16] C. Joshi, and U. K Singh, "Performance Evaluation of Web Application Security Scanners for More Effective Defense" International Journal of Scientific and Research Publications (IJSRP), Volume 6, Issue 6, pp 660-667, June 2016, ISSN 2250-3153.
[17] Z. Li, M. Sanghi, Y. Chen, "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).
[18] M. Frigault, L. Wang, A. Singhal, and S. Jajodia, "Measuring network security using dynamic bayesian network," in Proceedings of 4th ACM QoP, 2008.
[19] A. Lelli. (2010, Jan.) The trojan. hydraq incident: Analysis of the aurora 0-day exploit, Available: http://www.symantec.com/connect/blogs/trojanhydraq-incidentanalysis-aurora-0-day-exploit
[20] N. Falliere, L. O. Murchu, and E. Chien.(2011, Feb.) W32.stuxnet dossier, Available: http://www.h4ckr.us/library/Documents/ICSEvents/Stuxnet%20Dossier%20(Symantec)%20v1.4.pdf
[21] Symantec. (2011, Nov.) W32.duqu the precursor to the next stuxnet, Available: http://www.symantec.com/content/en/us/enterprise/media/s ecurity response/whitepapers/w32 duqu the precursor to the next stuxnet.pdf
[22] R. Goyal and P. Watters, "Obfuscation of stuxnet and flame malware," in Proc. 3rd Int. Conf. on Applied Informatics and Computing Theory, pp. 150–154, Barcelona, Oct. 2012.
[23] "McAfee Labs 2017 Threats Predictions", Intel Security, November 2016.
[24] P. Ammann, D. Wijesekera, and S. Kaushik, "Scalable, graph-based network vulnerability analysis," in Proceedings of ACM CCS'02, 2002.
[25] D. Hammarberg, "The Best Defenses against Zero-day Exploits for Various-sized Organizations", SANS Institute InfoSec Reading Room, September 21st 2014.
[26] M. Albanese, S. Jajodia, and S. Noel, "A time-efficient approach to cost-effective network hardening using attack graphs," in Proceedings of DSN'12, 2012, pp. 1–12.
[27] Y. Alosefer, O.F. Rana, "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.
[28] I. Kim, K. Kim, "A Case Study of Unknown Attack Detection against Zero-day Worm in the HoneyNet Environment", 11th International Conference on Advanced Communication Technology (ICACT), pp 1715-1720, 15 - 18 Feb 2009.

Authors Profile

Umesh Kumar Singh (M'16) received his Doctor of Philosophy (Ph.D.) in Computer Science from Devi Ahilya University, Indore(MP)-India. He is currently Associate Professor of Computer Science and Director in School of Engineering & Technology, Vikram University, Ujjain(MP)-India. He has authored 6 books and his about 100 research papers are published in national and international journals of repute. He was awarded Young Scientist Award by M.P. council of Science and Technology, Bhopal in 1997. He is reviewer of various International Journals and member of various conference committees. His research interest includes Computer Networks, Network Security, Internet & Web Technology, Client-Server Computing and IT based education.

Chanchala Joshi received her Master of Science in Computer Science and Master of Philosophy in Computer Science from Vikram University, Ujjain(MP)-India. She is currently Ph.D. Student and Junior Research Fellow in Institute of Computer Science, Vikram University, Ujjain(MP)-India. Her research interest includes network security, security measurement and risk analysis.

