Asian Journal of Engineering and Technology Innovation

ISSN : 2347-7385

REVIEW ARTICLE

**Received on: 01-10-2014**
**Accepted on: 10-10-2014**
**Published on: 22-10-2014**

**Mehul Das**
Dept. of computerscience Dr .D.Y. PatilInsti. Of Engg. & Tech., Pune
**Email:** ***Mehuldas3@gmail.com***
***Vikram.jaygude20@gmail.com***
***Shubtripathi13@gmail.com***
***banerjeeramnath@gmail.com***

**QR Code for Mobile users**

Conflict of Interest: None Declared

# K-Zero Day Security: Network security metric for risk measurement of unknown vulnerability

**Mehul Das, Shubham Tripathi, Vikram Jaygude, Mr. Ramnath Banerjee**
Dept. of computer science Dr .D. Y. Patil Insti. of Engg. & Tech., Pune

## ABSTRACT

By comparing the different security solution in terms of their effectiveness of solving it, network security matrix is gives the efficiency in protecting computer network. Research on security metrics has been hindered by difficulties in handling zero-day attacks exploiting unknown vulnerabilities. Security risk of unknown vulnerability is considered unmeasurable due to the less predictable nature of software flaws. This introduces a major difficulty to security metrics, since a more secure configuration would be of little value if it were equally suspecting zero-day attacks. This paper is to resolve this issue of Zero-day attacks. In this instead of ranking the unknown vulnerabilities, introduced metric counts how many such vulnerabilities would be required for compromising network assets. A larger count will indicate more security since the likelihood of having more unknown vulnerabilities applicable, available and exploitable all at the same time will be significantly lower. We will define the metric, analyze the complexity of computing the metric, devising heuristic algorithms for intractable issues, and finally implement through case studies that applying the metric to existing network security practices may generate actionable knowledge.

**Cite this article as:**
Mehul Das, ShubhamTripathi, VikramJaygude, security metric for risk measurement of unknown vulnerabilityAsian Journal of Engineering and Technology Innovation 02 (05); 2014; 05-09.

## Introduction

COMPUTER networks has become the nerve system of enterprise information systems and critical infrastructures on which our societies are highly dependent. The scale of security threats to computer networks have continued to grow same way to tackle with this. Potential consequences of a security attack have also become more and more serious as many high-profile attacks are reportedly focusing on not only computer applications but also industrial control systems at nuclear power plants and military satellites. Main difficulties in securing computer networks are the lack of methods for directly measuring the relative effectiveness of different security solutions in a network under consideration, because “one cannot improve what one can't measure.” Intrusion detection system or firewall can sometimes be obtained through lab- testing, but they are hardly aware of the real effectiveness of the solution when it is deployed in a real-world network, which can be very different from the testing environment. .Selecting and deploying a security solution still heavily rely on human experts’ experiences following a trial-and-error approach, which is a task of art, instead of a science.

Matrix method is adapted since it would enable a direct measurement and comparison of the amounts of security provided by different security solutions ,but it also has some us tackled issues like efforts on network securitble on zero-day attacks effect of unmeasurable threats is that without considering unknown vulnerabilities, a security metric will y metrics typically assign numeric scores to vulnerabilities based on known facts about vulnerabilities. This method is not applicable on zero-day attacks effect of unmeasurable threats is that without considering unknown vulnerabilities, a security metric will have questionable value at best, since it may determine a network configuration to be more secure while that configuration is in fact equally susceptible to zero-day attacks.

In this paper we propose a security metric, k-zero day safety, which will address this issue. In this instead of attempting to measure which unknown vulnerabilities are more likely to exist, we start with the worst case consideration that this is not measurable and then metric then matrix simply counts how many zero-day vulnerabilities are required to compromise a network. A larger count will indicate a relatively more secure network, since having more unknown vulnerabilities all available at the same time, applicable to the same network, and exploited by the same attacker, will be lower. We are implementing k-zero day safety metric based on an abstract model of networks and zero-day attacks. We consider the complexity of computing the metric and design heuristic algorithms addressing this complexity in special cases. Contribution of matrix approach to the best of our knowledge is that, this is among the first efforts on network security metrics that is capable of modeling the security risk of unknown zero-day attacks. Secondly the metric would bring about new opportunities to the hardening, quantitative evaluation and design of secure networks.

**Motivation:**

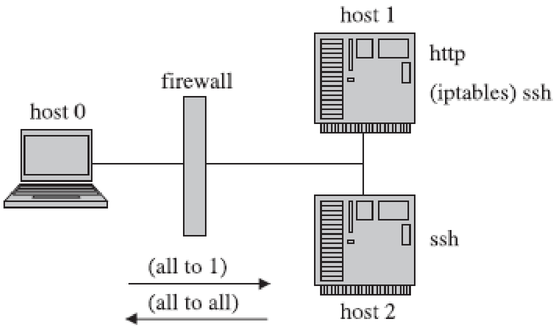

Fig. 1. An example network.

Fig. 1 shows an example where host 1 and host 2 comprise Of internal network. Firewall permits all the outbound Connection requests but it blocks all the inbound requests to host 2. The main security concern here is whether any Of the attacker on host 0 can obtain root privileges on host 2. If we assumed all the services to be free of the known Vulnerabilities, then a vulnerability scanner or an attack graph will draw exactly same conclusion that this network has secure attackers on host 0 hence cannot obtain the root privilege on host 2.

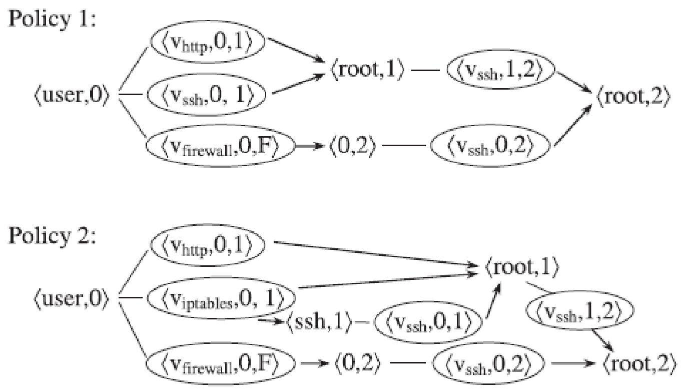

Fig. 2. Sequences of zero-day attacks.

Consider the following two iptables policies:

Policy 1. The iptables rules are left in a default configuration that accepts all the given requests.. Policy 2. The iptables rules are configured which allows specific IPs, excluding host 0, to gain access to the sshservice. Clearly, the network is already secure, policy 1 is preferred due to its simplicity (no special iptables rules are needed to be configured by the administrator) and functionality (any external host can connect to the ssh service on host 1). However, a different conclusion can be drawn if you compare the two policies with respect to the network's resistance to zero-day vulnerabilities. Specifically, policy 1. Under policy 1, where each triple indicates an exploit vulnerability, source host, destination host and a pair indicates a host condition, it illustrates three possible ideas for compromising host 2:

a. The attacker attacking host 0 exploits zero-day vulnerability in the HTTP service on host 1 and then use it as a stepping stone to exploit another zero-day vulnerability in the secure shell service on host 2.

b. He exploits zero-day vulnerability in the secure shell service on both of the hosts i.e host 1 and host 2.

c. He exploited zero-day vulnerability in the firewall (e.g., a default password) to circumvent the traffic blocking it before it compromises host 2. The first and third case require two different and separate zero-day vulnerabilities, whereas the second requires one zero-day vulnerability (in the secure shell service). Therefore, the network may be compromised with at least one zero-day attack under policy 1.

2. Under policy 2, the second case is different:

a. The same as 1a.

b. The attacker can exploit zero-day vulnerability to circumvent the given iptables rules before exploiting the secured shell service on both hosts i.e. host 1 and host 2.

c. The same as 1c.

The three cases now require two different zero-day vulnerabilities. The network can, hence, be compromised with at least two zero-day attacks according to policy 2.

Consider the fact that each zero-day attack has only a limited lifetime (before the vulnerability is disclosed and fixed), it is reasonable to assume that a large number of distinct zero-day vulnerabilities that is available during same time in this particular network will be significantly smaller (the probability will decrease exponentially if the occurrences of different vulnerabilities

can be regarded as independent events; however, the metric will not be dependent on any specific statistical model considering the process to find vulnerabilities is believed to be very chaotic). To revisit the given example, the network is regarded as more secure under policy 2 as compared to policy 1 because the former requires more (two) zero-da attacks to be compromised.

The crucial observation is that considering a network's resistance to zero-day vulnerabilities can assist in the relative security of various network configurations, which is otherwise indistinguishable under the existing vulnerability analysis and attack on graph-based techniques.

The remainder of this paper is build upon this important observation and address the remaining issues.

## Related work

Standardization efforts. There exits multiple standardization efforts on security metrics, like the Common Vulnerability Scoring System (CVSS) and, recently, the Common Weakness Scoring System (CWSS) . Former focuses on software weaknesses as vulnerability. CVSS & CWSS do not address their overall impact of vulnerability. These efforts form a foundation for research on security metrics, as they provide standard ways for assigning numerical scores to known vulnerabilities that are already available in public vulnerability databases, similar to the National Vulnerability Database.

Network security metrics. In an early work, a metric is proposed as the time and efforts required by potential dversaries on the basis of a Markov model of attack stages. In another early work, parameters considered a security metric for measuring the amount of security of networks were , the length of shortest attack paths, in number of exploits, conditions, or both .Main disadvantage of those early work lies in that they generally don’t take the relative severity of vulnerabilities under consideration .Later Compromise Percentage Metric (NCP) was proposed which shows the percentage of network assets that may be compromised by attackers. Now in recent work Page Rank Algorithm is introduced in that it basically indicates the percentage of network assets that may be compromised by attackers and for that assumption made is that the attackers would progress along different paths in an attack graph in a random fashion. An another research work replaces attack trees with more advanced attack graphs and replace its attack paths with attack scenarios. A mean time-to-compromise metric is also proposed based on the predator state-space model (SSM) used in the biological sciences it defines the average time required for compromising networks, the metric provides rich semantics than other abstract metrics. Main drawback of this work is in an oversimplified model of network intrusions and differences between vulnerabilities.

More recently authors found that matrix proposed provides partial view of security , and they proposed a framework for grouping such metrics based on their relative importance . A more recent research proposes a risk management framework using Bayesian networks for quantifying the chances of attacks and for developing a security mitigation and management plans.

Zero-day attack. These are attacks that exploits a previously unknown vulnerability in a computer application, one that developer have not had time to address & patch are called as Zero – data because programmer has Zero day to fix the flaws . The thing included in our work is that if statistical information about zero-day vulnerabilities, like the total number of such vulnerabilities, can be obtained or predicted based on such empirical studies, then such information can definitely be incorporated in our metric, for eg. a larger k is needed when more zero-day vulnerabilities are available . A recent research ranks different applications in the same system by how serious the effect would be if there exists a single zero-day vulnerability in those applications. Security metrics in other areas. Security metrics have been proposed in fields other than network security. In software security, the attack surface metric measures that how a software is vulnerable to attacks based on the degree of exposure Our focuses on ranking, rather than quantifying, security threats at network and system level essentially allow us to work with weaker assumptions that actually stem from such immeasurability results . Study of privacy metrics has seen significant successes, which clearly indicates the large impact of developing suitable security metrics on related researches.

The proposed paper is incorporating zero-day vulnerabilities.

**Future Work**

All zero-day vulnerabilities are regarded as equally likely due to their common immeasurability, where as in some cases safe assumptions can be made .Assigning different weights and probabilities to different (types of) zero-day vulnerabilities would be a extension to our proposed model. scope of our proposed metric is limited by the three basic considerations about zero-day vulnerabilities and those are the existence of network connectivity, vulnerable services on destination host, and initial privilege on source host .Make the broaden the scope by accommodating other types of attacks is an important future work .

**ACKNOWLEDGMENTS**

We are grateful to our teacher guide and project coordinator for the guidance they gave us in preparing this paper successfully.

| **S.NO** | **PAPER** | **CONFERENCE** | **1.Advantages**<br>**2.Disadvantages** |
|---|---|---|---|
| 1 | Scalable, Graph-Based Network Vulnerability Analysis | Proc. Ninth ACM Conf.ComputerComm. Security (CCS ’02), pp. 217-224, 2002. | 1.The model will be more suitable for application to the evaluation of penetration attacks launched by human attackers<br>2.In a zero-day attack graph, known vulnerabilities only affect the metric value through serving as a shortcut for attackers to bypass zero-day exploits. The relative severity of differentknown vulnerabilities is not taken intoconsideration in the metric. |
| 2 | Validating and Restoring Defense in Depth Using Attack Graphs,” | Proc. IEEE Conf. Military Comm. (MILCOM’ 06), 2006 | 1.An important future work is to broaden the scope by accommodating other types of attacks (e.g., a time bomb which requires no network connection).<br>2.a.They do not directly support trust relationship |

| | | | |
|---|---|---|---|
| | | | attacks where an attacker obtains a prerequisite for another attack (e.g. a password) from one host and then uses this prerequisite to compromise another remote host.<br>b.They also do not directly model situations where an attacker compromises a firewall and changes the firewall rules, because this changes the network reachability. |
| 3 | Quality of Protection: Measuring the Unmeasurable | Proc. ACM Second Workshop Quality Protection (QoP '06) | 1.This survey will provide a bettwr understanding of the different directions in which research has been done on this topic and how techniques developed in one area can be applied in domains for which they were not intended to begin wth.<br>2.Instantiating the metric model may involve uncertain input information (e.g., the possibility of Insider attacks). |
| 4 | MeasuringNetwork Security Using Dynamic Bayesian Network | Proc.Fourth ACM Workshop Quality of Protection (QoP '08), 2008 | 1.a.Produces stochastic classifiers<br>can be combined with utility functions to make optimal decisions<br>b.Easy to incorporate causal knowledge<br>resulting probabilities are easy to interpret<br>c.Very simple learning algorithms<br>if all variables are observed in training data<br>2.a.Fixed sized hypothesis space<br>may underfit or overfit the data<br>may not contain any good classifiers if prior knowledge is wrong<br>b.Harder to handle continuous features |
| | | | |
| 5 | Modeling Modern Network Attacks and Countermeasures UsingAttack Graphs," | Proc. Ann. Computer Security Applications Conf.(ACSAC )pp. 117-126, 2009. | 1. It is used to detect and mitigate compromised machines and provide security with less resource consumption.<br>2.One vulnerabilities may cause another vulnerabilities to be exploit simultaneously and leads to security problem. |

**Conclusion:**

In this paper, we have proposed the k-zero day safety as a novel network security metric, discussed its computation and application, and demonstrated its power in practical scenarios. Specifically, we formally defined the k-zero day safety model and showed that the metric satisfied the required algebraic properties of a metric function. We then studied the complexity of computing the metric and proposed efficient algorithms for determining the metric value. Next, we applied the proposed metric to the practical issue of network hardening and extended the metric to characterize various hardening options; we also discussed in details how the abstract model may be instantiated for given networks in practice. Finally, we demonstrated howapplying the proposed metric may lead to interesting and sometimes surprising results through a series of case studies; we also discussed how the metric may potentially be applicable to SCADA security.

**REFERENCES**

1. Greenberg, "Shopping for Zero-Days: A Price List for Hackers 'Secret Software Exploits," Forbes, Mar. 2012.
2. H. Holm, M. Ekstedt, and D. Andersson, "Empirical Analysis of System-Level Vulnerability Metrics through Actual Attacks,"IEEE Trans. Dependable Secure Computing, vol. 9, no. 6, pp. 825837,Nov. 2012.
3. L. Wang, T. Islam, T. Long, A. Singhal, and S. Jajodia, "An AttackGraph-Based Probabilistic Security Metric ,"Proc. 22nd Ann. IFIPWG 11.3 Working Conf. Data and Applications Security, 2008.
4. L. Wang, S. Jajodia, A. Singhal, and S. Noel, "k-Zero Day Safety: Measuring the Security Risk of Networks against Unknown Attacks," Proc. 15th European Conf. Research Computer Security(ESORICS '10), pp. 573-587, 2010.