ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Comparison of Different Security Solutions for Finding Vulnerabilities

M.Anusha
M.Tech Student,
Department of CSE,
Sree Rama institute of Technology and Science,
Kuppenakuntla, Penuballi, Khammam,TS India.

B.R.M Reddy
Assistant Professor,
Department of CSE,
Sree Rama institute of Technology and Science,
Kuppenakuntla, Penuballi, Khammam,TS India.

ABSTRACT:

By enabling a direct comparison of different security solutions with respect to their relative effectiveness, a network security metric may provide quantifiable evidences to assist security practitioners in securing computer networks. However, research onsecurity metrics has been hindered by difficulties in handling zero-day attacks exploiting unknown vulnerabilities. In fact, the security risk of unknown vulnerabilities has been considered as something unmeasurable due to the less predictable nature of software flaws.This causes a major difficulty to security metrics, because a more secure configuration would be of little value if it were equally susceptible to zero-day attacks.

In this paper, we propose a novel security metric, k-zero day safety, to address this issue. Instead of attempting to rank unknown vulnerabilities, our metric counts how many such vulnerabilities would be required for compromising network assets; a larger count implies more security because the likelihood of having more unknown vulnerabilities available,applicable, and exploitable all at the same time will be significantly lower. We formally define the metric, analyze the complexity of computing the metric, devise heuristic algorithms for intractable cases, and finally demonstrate through case studies that applying the metric to existing network security practices may generate actionable knowledge.

Index Terms:

Security metrics, network security, attack graph, network hardening

INTRODUCTION:

COMPUTER networks have long become the nerve system of enterprise information systems and critical infrastructures on which our societies are increasingly dependent.However, the scale and severity of security threats to computer networks have continued to grow at an ever increasing pace. Potential consequences of a security attack have also become more and more serious as many high-profile attacks are reportedly targeting not only computer applications but also industrial control systems at nuclear power plants, implanted heart defibrillators, and military satellites.One of the main difficulties in securing computer networks is the lack of means for directly measuring the relative effectiveness of different security solutions in a given network, because “you cannot improve what you cannot measure.” Indirect measurements, such as the falsepositive and negative rates of an intrusion detection system or firewall, may sometimes be obtained through laboratory testing, but they typically say very little about the actual effectiveness of the solution when it is deployed in a real-world network, which may be very different from the testing environment. In practice, choosing and deploying a security solution still heavily rely on human experts’ experiences following a trial-and-error approach, which renders those tasks an art, instead of a science.

Existing System:

In such a context, a network security metric is desirable because it would enable a direct measurement and comparison of the amounts of security provided by different security solutions.

Existing efforts on network security metrics typically assign numeric scores to vulnerabilities based on known facts about vulnerabilities.However, such a methodology is no longer applicable when we consider zero-day attacks. In fact, a popular criticism of past efforts on security metrics is that they cannot deal with unknown vulnerabilities, which are generally believed to be unmeasurable [21]. Unfortunately, without considering unknown vulnerabilities, a security metric will only have questionable value at best, because it may determine a network configuration to be more secure while that configuration is in fact equally susceptible to zero-day attacks. We, thus, fall into the agnosticism that security is not quantifiable until we can fix all potential security flaws but by then we certainly do not need security metric at all [21].

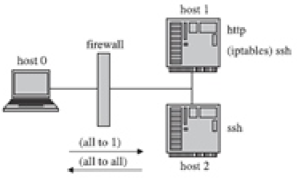


Fig. 1. An example network.

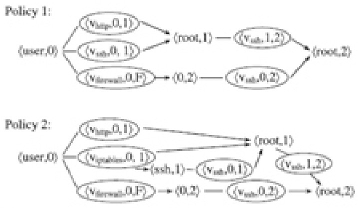


Fig. 2. Sequences of zero-day attacks.

Proposed System:

In this paper, we propose a novel network security metric, k-zero day safety, to address this issue. Roughly speaking, instead of attempting to measure which unknown vulnerabilities are more likely to exist, we start with the worst case assumption that this is not measurable.Our metric then simply counts how many zero-day vulnerabilities are required to compromise a network asset.

A larger count will indicate a relatively more secure network, because the likelihood of having more unknown vulnerabilities all available at the same time, applicable to the same network, and exploitable by the same attacker, will be lower. We will formally define the k-zero day safety metric based on an abstract model of networks and zero-day attacks. We analyze the complexity of computing the metric and design heuristic algorithms for addressing this complexity in special cases.

We demonstrate the usefulness of the metric by applying it to the evaluation of existing practices in network hardening through a series of case studies.The contribution of this work is twofold. First, to the best of our knowledge, this is among the first efforts on network security metrics that is capable of modeling the security risk of unknown zero-day attacks. Second, we believe the metric would bring about new opportunities to the quantitative evaluation, hardening, and design of secure networks.

Motivating Example:

Fig. 1 shows a toy example in which hosts 1 and 2 comprise the internal network. The firewall allows all outbound connection requests but blocks inbound requests to host 2.Assume the main security concern here is whether any attacker on host 0 can obtain the root privilege on host 2.Clearly, if we assume all the services to be free of known vulnerabilities, then a vulnerability scanner or attack graph will both draw the same conclusion that this network is secure attackers on host 0 cannot obtain the root privilege on host 2.Now, consider the following two iptables policies: Policy 1. The iptables rules are left in a default configuration that accepts all requests. Policy 2. The iptables rules are configured to only allow specific IPs, excluding host 0, to access the ssh service.Clearly, because the network is already secure, policy 1 will be preferable due to its simplicity (no special iptables rules need to be configured by the administrator) and functionality (any external host may connect to the ssh service on host 1).However, a different conclusion can be drawn if we compare the above two policies with respect to the network's resistance to potential zero-day vulnerabilities. Specifically, 1. Under policy 1, the upper diagram in Fig. 2 (where each triple indicates an exploit hvulnerability, source host, destination hosti and a pair indicates a condition hcondition, hosti) illustrates three possible ways for compromising host 2:a. The attacker on host 0 exploits a zero-day vulnerability in the HTTP service on host 1 and then uses it as a stepping stone to exploit another zero-day vulnerability in the secure shell service on host 2. b. He/She exploits a zero-day vulnerability in the secure shell service on both hosts 1 and 2.c. He/She exploits a zero-day vulnerability in the firewall (e.g., a default password) to circumvent the traffic blocking before compromising host 2. The above first and third cases require two different zero-day vulnerabilities, whereas the second only requires one zero-day vulnerability (in the secure shell service).

Therefore, the network can be compromised with at least one zero-day attack under policy 1. 2. Under policy 2, only the second case is different, as illustrated in the lower diagram in Fig. 2: a. The same as the above 1a. b. The attacker exploits a zero-day vulnerability to circumvent the iptables rules before exploiting the secure shell service on both hosts 1 and 2. c. The same as the above 1c. All three cases now require two different zero-day vulnerabilities. The network can, thus, be compromised with at least two zero-day attacks under policy 2.Considering 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 the likelihood of having a larger number of distinct zero-day vulnerabilities all available at the 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, our metric will not depend on any specific statistical model, considering the process of finding vulnerabilities is believed to be chaotic). To revisit the above example, the network can be regarded as more secure under policy 2 than under policy 1 because the former requires more (two) zero-day attacks to be compromised.The key observation here is that considering a network's resistance to potential zero-day vulnerabilities may assist in ranking the relative security of different network configurations, which may be otherwise indistinguishable under existing vulnerability analysis or attack graph-based techniques.The remainder of this paper will build upon this key observation and address remaining issues.

RELATED WORK:

Standardization efforts. There exist numerous standardization efforts on security metrics, such as the Common Vulnerability Scoring System (CVSS) [24] and, more recently, the Common Weakness Scoring System (CWSS) [37]. The former focuses on ranking known vulnerabilities, whereas the latter on software weaknesses. Both CVSS and CWSS measure the relative severity of individual vulnerabilities in isolation and do not address their overall impact. On the other hand, these efforts form a practical foundation for research on security metrics, as they provide security analysts and vendors standard ways for assigning numerical scores to known vulnerabilities that are already and the time to compromise of a system [11]. In our recent vulnerabilities [22], a report on the popularity of zero-day vulnerabilities vulnerabilities are available).

A recent effort ranks different applications in the same system by how serious the services) are H ! 2S and privileges privð:Þ : H ! 2P , and . the that their exploitation requires a network connection between the source and destination hosts, a remotely accessible service on the destination host, and existing privilege on the source host. In addition, exploiting such a vulnerability can potentially yield any privilege on the destination host. Those assumptions are formalized as the first type of zero-day exploits in Definition 2. The second type of zero-day exploits in the definition represent privilege escalation following the exploitation of services.Definition 2 (Zero-day exploit). Given a network, for each remote service s, we define a zero-day vulnerability vs such that the zero-day exploit hvs; h; h0i has three econditions, hs; h0i (existence of service), hh; h0i (connectivity), and hp; hi (attacker's existing privilege); it has one postcondition hps; h0i where ps is the privilege of service s on h0. for each privilege p, we define a zero-day vulnerability vp such that the preconditions of the zero-day exploit hvp; h; hi include the privileges of remote services on h, and the postcondition is hp; hi.Now that we have defined zero-day exploits, it is straightforward to extend a traditional attack graph with zero-day exploits. Specifically, a zero-day attack graph is simply a directed graph composed of both zero-day and known exploits, with edges pointing from preconditions to corresponding exploits and from exploits to their postconditions.

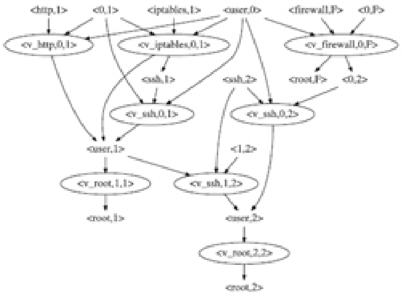


Fig. 3. An example of zero-day attack graph.

Fig. 3 shows the zero-day attack graph of our (in this special case, all exploits are zero day).In a zero-day attack graph, we use the notion of initial condition for conditions that are not postconditions of any exploit (e.g., initially satisfied conditions, or those as the result of insider attacks or user mistakes).

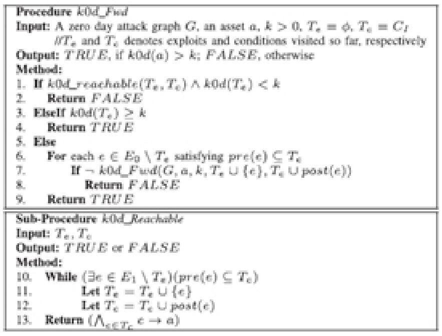
We also need the notion of attack sequence, that is, any sequence of exploits in which the preconditions of every exploit are either initial conditions, or postconditions of some preceding exploits (intuitively, this indicates an executable sequence of attacks).

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Finally, we regard a given condition a as the asset (which can be extended to multiple assets with differentvalues [41]) and use the notation seqðaÞ for any attack sequence that leads to a.

COMPUTING k-ZERO DAY SAFETY:

This section presents algorithms for computing the proposed metric. The first two algorithms have appeared in [41] and the third algorithm is a new contribution of this paper.



```
Procedure k0d_Fwd
Input: A zero day attack graph $G$, an asset $a$, $k > 0$, $T_e = \phi$, $T_c = C_I$
       //$T_e$ and $T_c$ denotes exploits and conditions visited so far, respectively
Output: $TRUE$, if $k0d(a) > k$; $FALSE$, otherwise
Method:
If $k0d\_reachable(T_e, T_c) \wedge k0d(T_e) < k$
    Return $FALSE$
ElseIf $k0d(T_e) \geq k$
    Return $TRUE$
Else
    For each $e \in E_0 \setminus T_e$ satisfying $pre(e) \subseteq T_c$
        If $\neg$ $k0d\_Fwd(G, a, k, T_e \cup \{e\}, T_c \cup post(e))$
            Return $FALSE$
    Return $TRUE$

Sub-Procedure k0d_Reachable
Input: $T_e, T_c$
Output: $TRUE$ or $FALSE$
Method:
While $(\exists e \in E_1 \setminus T_e)(pre(e) \subseteq T_c)$
        Let $T_e = T_e \cup \{e\}$
        Let $T_c = T_c \cup post(e)$
Return $(\bigwedge_{c \in T_c} c \rightarrow a)$
```

APPLYING k-ZERO DAY SAFETY:

In this section, we first demonstrate the power of our metric through applying it to network hardening. We also extend the basic metric model to define submetrics for measuring the potential of hardening options. Finally, we discuss practical issues in instantiating the model from given networks.Based on the proposed k-zero day safety metric, we can now redefine network hardening as rendering a network k-zero day safe for a larger k. Clearly, such a concept generalizes the above qualitative approaches. Specifically, under our model, those qualitative approaches essentially achieve k > 0, meaning that attacks are no longer possible with known vulnerabilities only. In contrast to those qualitative approaches, our definition can rank network hardening solutions based on the relative degree of security guarantee provided by those solutions. Such a ranking would enable us to model network hardening as various forms of optimization problems, either with k as the objective function and cost as constraints (that is, to maximize security) or vice versa.

CONCLUSIONS:

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 tocharacterize various hardening options; we also discussed in details how the abstract model may be instantiated for given networks in practice. Finally, we demonstrated how applying 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] P. Ammann, D. Wijesekera, and S. Kaushik, "Scalable, Graph- Based Network Vulnerability Analysis," Proc. Ninth ACM Conf. Computer Comm. Security (CCS '02), pp. 217-224, 2002.

[2] D. Balzarotti, M. Monga, and S. Sicari, "Assessing the Risk of Using Vulnerable Components," Proc. ACM Second Workshop Quality of Protection (QoP '05), pp. 65-78, 2005.

[3] S.M. Bellovin, "On the Brittleness of Software and the Infeasibility of Security Metrics," IEEE Security and Privacy, vol. 4, no. 4, p. 96, July/Aug. 2006.

[4] M. Dacier, "Towards Quantitative Evaluation of Computer Security," PhD thesis, Institut Nat'l Polytechnique de Toulouse, 1994.

[5] E.W. Dijkstra, "A Note on Two Problems in Connection with Graphs," Numerische Mathematik, vol. 1, pp. 269-271, 1959.

[6] J. Doob, Measure Theory. Springer-Verlag, 1994.

[7] C. Dwork, "Differential Privacy," Proc. 33rd Int'l Colloquium Automata, Languages and Programming (ICALP '06), vol. 2, pp. 1- 12, 2006.

[8] N. Falliere, L.O. Murchu, and E. Chien, "W32.Stuxnet Dossier," Symantec Security Response, 2011.

[9] M. Frigault, L. Wang, A. Singhal, and S. Jajodia, "Measuring Network Security Using Dynamic Bayesian

Network," Proc. Fourth ACM Workshop Quality of Protection (QoP '08), 2008.

[10] A. Greenberg, "Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits," Forbes, Mar. 2012.

[11] 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. 825- 837, Nov. 2012.

[12] J. Homer, X. Ou, and D. Schmidt, "A Sound And PracticalApproach to Quantifying Security Risk in Enterprise Networks,"technical report, Kansas State Univ., 2009.

[13] N. Idika and B. Bhargava, "Extending Attack Graph-Based SecurityMetrics and Aggregating Their Application," IEEE Trans. Dependableand Secure Computing, vol. 9, no. 1, pp. 75-85, Jan./Feb. 2012.

[14] K. Ingols, M. Chu, R. Lippmann, S. Webster, and S. Boyer,"Modeling Modern Network Attacks and Countermeasures UsingAttack Graphs," Proc. Ann. Computer Security Applications Conf.(ACSAC '09), pp. 117-126, 2009.

[15] S. Jajodia, S. Noel, and B. O'Berry, "Topological Analysis ofNetwork Attack Vulnerability," Managing Cyber Threats: Issues,Approaches and Challenges, V. Kumar, J. Srivastava, and A.Lazarevic, eds., Kluwer Academic, 2003.

[16] A. Jaquith, Security Merics: Replacing Fear Uncertainity and Doubt.Addison Wesley, 2007.

[17] S. Jha, O. Sheyner, and J. Wing, "Two Formal Analysis ofAttack Graph," Proc. 15th Computer Security Foundation Workshop(CSFW' 02), 2002.

[18] D. Leversage and E. Byres, "Estimating a System's Mean Time-to-Compromise," IEEE Security and Privacy, vol. 6, no. 1, pp. 52-60,Jan./Feb. 2008.

[19] W. Li and R.B. Vaughn, "Cluster Security Research Involving the Modeling of Network Exploitations Using Exploitation Graphs," Proc. IEEE Sixth Int'l Symp. Cluster Computing and Grid (CCGRID '06), p. 26, 2006.

[20] R. Lippmann, K. Ingols, C. Scott, K. Piwowarski, K. Kratkiewicz,M. Artz, and R. Cunningham, "Validating and Restoring Defensein Depth Using Attack Graphs," Proc. IEEE Conf. Military Comm.(MILCOM' 06), pp. 981-990, 2006.

[21] J. McHugh, "Quality of Protection: Measuring the Unmeasurable?"Proc. ACM Second Workshop Quality Protection (QoP '06),pp. 1-2, 2006..

22th Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques(Eurocrypt '05), pp. 457-473, 2005.

[23] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "SecureAttribute-Based Systems," Proc. 13th ACM Conf. Computer andComm. Security (CCS '06), pp. 99-112, 2006.

[24] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-BasedEncryption for Fine-Grained Access Control of Encrypted Data,"Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06),pp. 89-98, 2006.

Author's:

M.Anusha is a student of Sree Rama Institute of Technology & Science, Kuppenakuntla,Penuballi, Khammam, TS,India.Presently she is Pursuing her M.Tech (CSE) from this collegeHer area of interests includes Information Security, Cloud Computing, Data Communication & Networks.

Mr. B.R.M.Redy is an efficient teacher, received M.Tech from JNTU Hyderabad is working as an Assistant Professor in Department of C.S.E, Sree Rama Institute of Technology & Science, Kuppenakuntla, Penuballi, Khammam, AP,India. He has published many papers in both National & International Journals. His area of Interest includes Data Communications & Networks, Information security, Database Management Systems, Computer rganization, C Programming and other advances in Computer Applications