Volume 5, Issue 2, February 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Detection and Prevention of Unknown Vulnerabilites on Enterprise IP Networks

Vincy Rose Chacko*
Department of Computer Science and Engineering,
St.Joseph College of Engineering, Chennai, India

M. Navaneetha Krishnan
Head of the Dept., Department of CSE,
St. Joseph College of Engineering, Chennai, India

Abstract— Computer networks have long become the backbone of Enterprise Information System. The substantial share of the security problems are still encountered in Enterprise Network. Cyber espionage can effect Ethical, Military, Political and Economic interest anywhere. To provide secure computer networks, it is necessary to measure the relative effectiveness of security solution in the network. A network security metric enable a direct measurement and comparison of the amounts of security provided by different security solutions .In this paper we propose a novel security metric Zero Day Vulnerability Prevention Framework consists of bunches of algorithms. The above framework detects and prevents unknown vulnerabilities in Enterprise IP networks. It also protects the behavior of the sessions performed by the user from the huge range of attacks. It helps in monitoring database requests and prevents the attacks. The proposed framework also implements worm and virus detection to evaluate malware from the data. The system also presents scoring to the vulnerabilities and finally it performs security analysis with the help of Topological Vulnerability Analysis (TVA) tool.

Keywords— Network Security; Enterprise IP networks; Zero day vulnerability prevention framework; Worm and virus detection; CAULDRON

I. INTRODUCTION

Cyber espionage on enterprise are politically or socially carried out mainly through the internet. Attack targets are material and corporate organization and are carried out through spread of virus dissemination, unauthorized web access, fake website stealing information. The internet has become widely complex, leaving many enterprises vulnerable to malicious attacks. Organizations are trying to protect their infrastructure against network security attacks. Every year security breaches cost companies millions of dollars in revenue, productivity and lost reputations. Enterprise networks have become vital part to the companies and governmental agencies. As they continue to grow both in size and complexity, network security has become a critical concern. An enterprise security goal is to reduce all networks and host vulnerabilities. Even a moderately-sized network can have many different attack paths which an attacker could exploit to gain unauthorized network access

Enterprises are faced with many challenges to achieve true network and application security because application vulnerabilities are on the rise, increasing network vulnerabilities and internal security breaches and information leaks. Common attacks on enterprises are Eavesdropping, IP Address spoofing, Password-based attacks, DOS and DDos attacks, Man-in–the–Middle attack, Sniffer attack and Application layer attack. The robust, time-tested set of efficient tools and techniques that have been developed to combat cyber-attacks on enterprise can provide cyber security for the field networks that is comparable to that of the most mission-critical enterprise networks in the world.

The main difficulty in securing computer networks is the absence of measuring the effectiveness of security solutions available in the given network. Indirect measurements such as firewalls are obtained; but they provide very little about the effectiveness of the security solutions when it is deployed in a real- world network. In such a case, a network security metric is used, because it would provide direct measurement of the effectiveness of the security solutions. Existing efforts provide a security metric, *k* zero day safety that simply counts how many distinct zero day vulnerabilities are required to compromise a network assets. A large count will provide more secure network. It requires tight time synchronization to detect the attacks and known geographic information to identify attacks and protect the network. It is not capable to detect attacks against routing such as worm hole, sinkhole attack and Sybil attacks. The attacker can easily create traffic collision with seemingly valid transmission drop or misdirect messages in routes.

In this paper, we propose a novel security metric, *Zero day Vulnerability Prevention Framework* to address these issues. Instead of providing how many vulnerabilities required to compromise a network, it provides varied algorithms to detect and prevent unknown vulnerabilities in Enterprise IP network. The framework provides worm and virus detection to evaluate malware from the content. The above system also assigns numerical scores to vulnerabilities based on known facts about vulnerabilities. Finally, the proposed framework conducts security analysis using topological vulnerability analysis tool CAULDRON.

II. RELATED WORK

Nayot Poolsappasit, R.Dewri and I. Ray in [1] propose a risk management framework base on Bayesian networks to quantify the chances of attacks and to develop a security mitigation and management plan. It is more compact and scalable representation. This early work use Bayesian logic to evaluate identification of assets, system vulnerability and connectivity analysis. More recently, N.Idika and B.Bhargava in [2] observes that different security metrics will provide only a partial view of security and the authors then propose a framework for grouping the metrics attack graph and decision metric based on their relative importance. Attack graph for large networks can get complex and maintains an attribute template for the graph. The size of the attribute instance can be as large as the number of machines. The combination of similar type of security metric will generate more number of graphs.

The research on network security metrics has attracted much attention. In another early work, D.balzarotti, M.Monga and S. Sicari [5] propose a Cooke's classical method that will find previously unknown vulnerability in the software. An attack tree marked with abstract exploitability and hazard is passed to find sequences of attacks that corresponds to the easiest paths followed by potential attackers, and the amount of minimum effort needed along such paths is used as a security metric. In another similar work C.Phillips and L.Swiller [6] propose a graph based approach that analyses network vulnerability. It requires an input database of common attacks, specific network configuration and attacker profile. The length of shortest attack paths in terms of the number of exploits, conditions or both is taken as security metric for measuring the amount of security of networks. The main limitation of those early work lies in that they generally do not consider the relative security or likelihood of vulnerabilities.

Most of the existing works focus on developing security metric for known vulnerabilities in a network. Sommestad & Holm in [3] propose a vulnerability dependency graph that emphasizes the possible dependencies. There are no other approaches to access the risk and damage values. It specifies the effort on estimating the effort required for developing new exploits. Mc Queen, Boyer and M.Chaffin in [4] specifies an empirical study on the total number of zero day vulnerabilities available on a single day based on existing facts about vulnerabilities. Wang, Noel and Jajodia in [7] proposed a method that views vulnerability as a Boolean variable and derive a logic proposition.

III. PROPOSED ALGORITHM

Here we present a zero day vulnerability prevention framework to detect and prevent vulnerabilities in enterprise IP network. This novel framework uses varied algorithms and techniques to accomplish the goal of enterprise network. First, it finds all possible routes and selects the shortest among them based on Zeroday_shortest Algorithm. And then we find vulnerabilities in the network using Trust Aware Detection technique. The proposed approach also implements worm and virus detection to evaluate malware from the data.

Modelling Zero Day Vulnerability Prevention Framework

A. Zero day Shortest Algorithm

The Zero day_ Shortest Algorithm finds the shortest path from a source to all destinations in a directed graph. During this process it will also determine a spanning tree for the graph. Finding the shortest path in a network is a commonly encountered problem. A network can be modelled by a graph. Routers are represented by nodes. Physical links between routers are represented by edges. Attached computers are used. Each edge is assigned a weight representing the overall time that it takes to process the request and response to the client. The total cost of a path is the sum of the weights of the edges. The problem is to find the least-weight path. At the first iteration, the algorithm finds the closest node from the source node which must be a neighbour of the source node. At the second iteration, the algorithm finds the second-closest node from the source node. This node must be a neighbour of either the source node or the closest node found in the first iteration. At the third iteration, the algorithm finds the third-closest node from the source node. This node must be a neighbour of either the source node or one of the first two closest nodes. The process continues. At the k-th iteration, the algorithm finds the first k closest nodes from the source node.

Procedure Zeroday_Shortest
Input: Source, assets
Output: Assets with a non negative real number
Method:
Let wt[source] := 0
For each node v in G
If v ≠ source
wt[v] := infinity
Previous[v] := undefined
Add v to Q
While Q is not empty
u: = node in Q with min wt[u]
Remove u from Q
For each neighbour v of u
Alt: = wt[u] + length (u, v)
If alt < wt[v]
wt [v] := alt, Previous[v]:= u


```
Return wt [], previous []
```

Figure1. Determining the shortest path

B. Zero day Framework Encryption Algorithm

Zero day vulnerability prevention framework that uses AES for authenticating the request.AES is a symmetric block cipher. Framework uses this for verifying whether the request comes from the valid client or not. The valid server connection is only possible through the abstract request. The request would be encrypted using one key and decrypted by the framework using the same key.

C. Trust Aware Detection Technique

Trust Aware Detection Technique (TADT) encourages the framework to detect and prevent vulnerabilities in the network. Though only those legal neighboring nodes of an attacker might have correctly identified the adversary. Our design TADT proves effective against those harmful attacks developed out of identity deception. This technique an be implemented by the framework with low overhead. This TADT technique can be integrated into existing routing protocols with the least effort, thus producing secure and efficient fully-functional protocols.

It significantly reduces negative impacts from these attackers. It is also energy-efficient with acceptable overhead. It incorporates the trustworthiness of nodes into routing decisions and allows a node to circumvent an adversary misdirecting considerable traffic with a forged identity attained through replaying. It identifies such intruders that misdirect noticeable network traffic by their low trustworthiness and routes data through paths circumventing those intruders to achieve satisfactory throughput. TADT is also energy-efficient, highly scalable, and well adaptable. The above technique enables a node to keep track of the trustworthiness of its neighbors and thus to select a reliable route and put in the routing table. Not only does TADT circumvent those malicious nodes misusing other nodes' identities to misdirect network traffic, but also accomplishes energy usage properly.

D. Zero day Worm and Virus Detection Algorithm

Worms are widely regarded to be major security threat. Active worms spread in an automated fashion.Anti-virus are the popular tool to combat worms. It used pattern based technology to detect worms. However the high spreading speed of worm is less effective in anti-virus. Moreover, anti-virus cannot detect unknown internet worm automatically because it uses signature in detecting worms. Anti-virus compares the file structure of the worms with the signatures stored in its database. If they are matched, then the file is considered as infected by the worm. This required the anti-virus database to be frequently updated, so that it can detect new worms. This is the main reason why anti-virus cannot detect most of unknown internet worm automatically. Beside antivirus, firewalls and routers can be used to detect worm. Signature and block based worm detection, occurs only after the worm already spread. The worm generates an IP address and uses that IP address to communicate to potential victim, when the IP address is unused. The proposed Worm and Virus Detection Algorithm is used to detect the malwares from the data. This algorithm used for the file that has a huge size. It performs searching based on the three attributes, file type, file size and file content. It will check the worms in the file randomly. It is the major advantage of getting the worms from the content. The number of comparisons are performed any number of times in the specified algorithm. This will be more applicable to the user to detect the malware from the content very accurately. If there is any match in location then it will return an integer value. This will specify that file is virus affected or not. The algorithm is energy-efficient, highly scalable, and well adaptable and also accomplishes time usage.

```
Procedure Zero day _Worm and Virus Detection
Input: File to Check
Output: An integer Value
Method:
Let M be the length of input file
Let N be the length of original File
Let first be the one random number (1 to M)
Let Second be the another random number (1 to N)
While first< second
Let s1 be the substring of the input file
Let s2 be the substring of the original file
If s1 equals to s2
Return False
Else
Return True
```

Figure2.Detecting the malware from the data

E. Common Vulnerability Scoring System (CVSS)

CVSS is a vulnerability scoring system designed to provide an open and standardized method for rating the vulnerabilities. The proposed framework uses CVSS version 2 calculators to provide scores to the vulnerabilities. Base score is used to calculate the temporal score and the temporal score is used to calculate environmental score. Base

represents the intrinsic and fundamental characteristics of vulnerability that are constant over time and user environments. Temporal **r**epresents the characteristics of vulnerability that change over time but not among user environments. Environmental represents the characteristics of vulnerability that are relevant and unique to a particular user's environment.

F. Vulnerability Analysis using CAULDRON

This evaluates the proposed model with the existing techniques. During evaluation, security metric lies in the lack of necessary benchmark data such an evaluation would require both data and details of the networks including node configurations. One viable approach would be integrated with the proposed model as an added feature to existing vulnerability analysis tool, such as CAULDRON to evaluate its practical effectiveness and to fine-tune the model. Proposed System security analysis done by Topological Vulnerability tool (TVA)-CAULDRON. CAULDRON (Cyber-attack modelling, analysis and Visualization) supports both offensive and defensive applications. CAULDRON places Vulnerabilities and their protective measures within context of overall network security by modelling their interdependencies via attack graphs. The Analysis of attack graphs provides alternative sets of protective measures that guarantee safety of critical system. It is a Topological Vulnerability tool approach consist of Network Capture Builds a model of the network in relevant term security attributes, Vulnerability Database ,Exploit specifications ,Graph engine, Interactive visual analysis of attack Graphs, and optimal counter measures.

IV. SYSTEM DESIGN

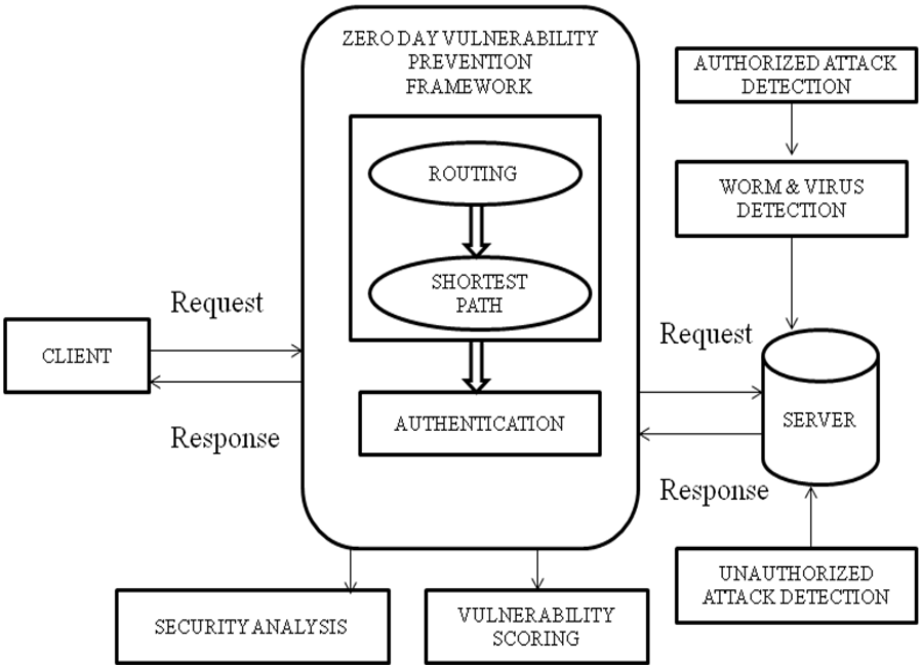

Figure3. System Architecture

Figure 3 demonstrates the system design. Client gives request to the server. A valid server connection is only possible through the session value. The session value is encrypted and decrypted for authentication. It will provide more security. The system defines a zero day vulnerability prevention framework that detects and prevents vulnerabilities on Enterprise IP network. This will identify the entire possible path that client connects to the destination and put it in the routing table. From the routing table it will find the shortest path based on the weights calculate on each node. Then it provides peer connection to the appropriate sever. Thus the framework detects both authorized & unauthorized attacks. Unauthorized attack includes the client trying to connect without session or with different session .In such cases, the framework that prevents the attack by blocking particular IP and put it in a blacklist. The authorized attack will include the SQL Injection attack and prevention, File uploading attack. These attacks are detected and prevented by using Trust Aware Detection Techniques. This system mainly concentrated on the worm and virus detection by zero day worm and virus detection Algorithm. It will detect the malwares from the data. It will provide scoring to the vulnerabilities by integrating the framework with CVSS. Finally it implements the security analysis with the help of CAULDRON tool and fine tune the framework performance.

A. Route Filtering and Path Identification

The zero day vulnerability prevention framework first calculates the weight on the each node. It evaluates whether the client is valid or not. The valid server connection is possible through the abstract session value. It then find the entire possible paths that client connects to the server. The entire possible path will be placed in the routing table. From the specified paths in the routing table, it will identify the shortest path based on the weight assigned in each node. It is the overall time that it takes to process the request and response to the client.

B. Authentication and Unauthorized Attack

The proposed framework verifies each client whether authenticated or not. A valid server connection is only possible through the abstract session value. This session value is appended with the request to the server. Abstract session is a status value that will be encrypted. At the destination server it will be decrypted by the framework and connects to the server. This abstract session provides more security to the server connection. There will be a chance of unauthorized attack. It may be in the form request without abstract value and request having different abstract values or invalid abstract. The framework detects the unauthorized attacks based on trust aware detection technique by blocking the client from future access and put that into the blacklist.

C Authorized Attack Detection and Prevention

The biggest threats are security attacks from people within the organization. While external attacks are extremely important and critical, internal attacks should not be overlooked. The zero day vulnerability prevention framework thus detects an authorized attack also. They may include activities like SQL injection attacks, file uploading attacks. It is possible for attackers to provide a username containing SQL meta-characters that subvert the intended function of the SQL statements. When a client wants to get the details, that when it connects to the server, weight and all details these types of attacks occurs. Consider the case admin`or`1`=`1. This allows an attacker to log in to the data, since OR expression is always true. Using the above technique attackers can inject other SQL commands which could extract modify or delete data within the database. Trust aware detection technique that detects such kinds of attacks and prevents by using prepared statements that helps in defending against SQL injection and move the IP to blacklist. File uploading attacks occurred during uploading files. The attacker uploads the files that virus affected. It will go for the Google search and collects all the files that are suspected to virus with same name. It will extend the database error files by adding the new searched Google items. Trust aware detection technique that detects the attacks and prevents based on the file name and blocks that IP.

D. Worm and Virus Detection

It evaluates malwares from the content. Worms and viruses are self-replicating programs. It uses network to send copies of itself to other systems invisibly without user authorization. Zero day worm and virus detection algorithm is used to find worm and virus based on the file type, size and content. Three parameters are used for evaluating the malwares from the content. It compares the size of the file and type of the file. Then it compares the content randomly. The comparison round is determined by the authenticated person. If it detects any match, it will detect the file as an un-trusted one. Otherwise, it will be a trusted file. The un-trusted file will be moved to the database black list.

E .Vulnerability Scoring

It gives scores to the vulnerabilities based on their extremity. The zero day vulnerability prevention framework that assigns scores to the vulnerabilities by integrating it with common vulnerability scoring system. It identifies and assesses vulnerabilities across many disparate hardware and software platforms. They need to prioritize above vulnerabilities and remediate those that pose the greatest risk. CVSS is composed of three metric groups Base, Temporal, and Environmental, consisting of a set of metrics. Base represents the intrinsic and fundamental characteristics of vulnerability that are constant over time and user environments. Temporal represents the characteristics of vulnerability that change over time but not among user environments. Environmental represents the characteristics of vulnerability that are relevant and unique to a particular user's environment. The purpose of the CVSS base group is to define and communicate the fundamental characteristics of vulnerabilities. This main approach to characterizing vulnerabilities provides users with a clear and intuitive representation of vulnerability. CVSS offers the following benefits, standardized vulnerability Scores, Contextual Scoring and Open framework.

F. Security Analysis

CAULDRON is a next generation predictive tool for enterprise information security. It gives the transformation of raw security data that allow users to proactively prepare for potential attacks on enterprises, manage the vulnerability risks and have real-time situational awareness. It does three things aggregate data, correlate the data against known vulnerability datasets and visualization .It begins with Network capture that builds a model of the network, in terms of relevant security attributes. It represents data collection for a network to be defined according to vulnerability database and exploit conditions. All these inputs together to build an environmental model for multi-step attack graph simulation. Vulnerability Database it is comprehensive repository of reported vulnerabilities .The Graph engine uses the environmental model for multi-step attack graph through the networks, for a given user-defined attack scenario. The system then provides capabilities for interactive visual analysis of attack graphs.

V. DISCUSSIONS

The main objective is to detect and prevent unknown vulnerabilities on enterprise IP network using zero day vulnerability prevention framework. It prevents both authorized and unauthorized attacks by implementing Trust Aware Detection technique. Thus the framework will be the best to prevent these attacks in the enterprise IP network. The above framework provides an efficient peer communication in a large network. It can applied to various types of industries such as Defence, Information Technology, Research and Development which have large network. The proposed novel framework detects and prevents various attacks on Enterprise IP Networks.

VI. RESULTS

A. Prevention of Targeted attacks

Cyber attacks that are geared at particular organizations and services to obtain private, technical and other intellectual assets are prevented by *Zero day Vulnerabilities Prevention frame work.*

B. Worm and Virus Prevention

A kind of targeted attack geared at particular entity and carried out continuously and persistently using a variety of means in order to gain access to the target. It mainly prevents the attacks against users attach malicious program.

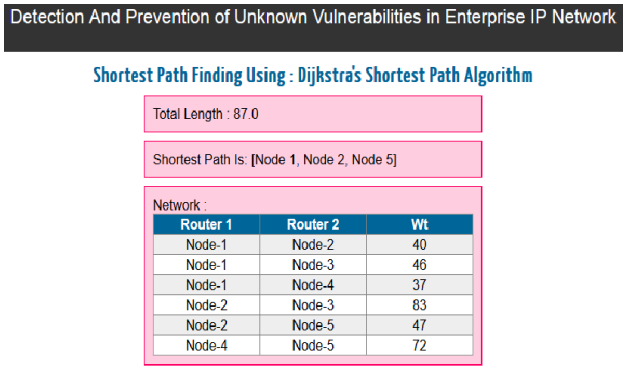

Figure4. Shortest path

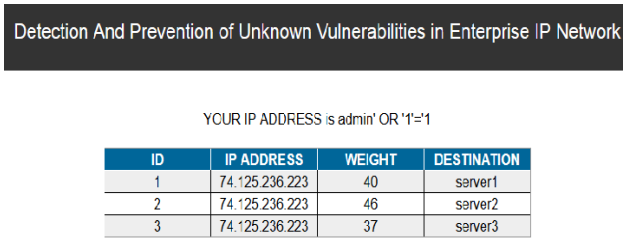

Figure5. Authorized Attack

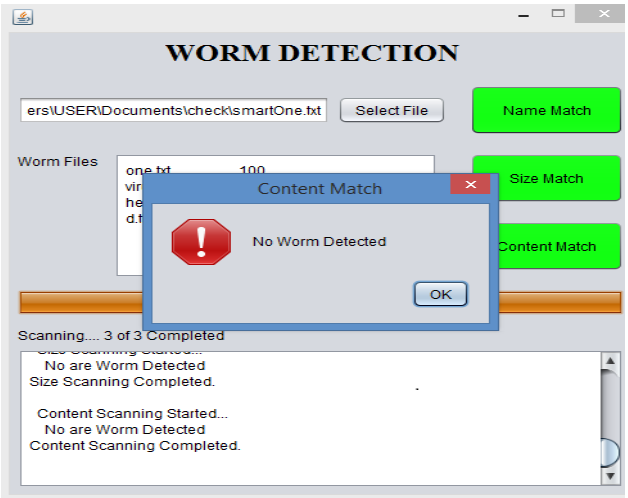

Figure 6.Worm and virus Prevention

VII. CONCLUSION

In this paper we have proposed the *Zero Day Vulnerability Prevention Framework* to detect the unknown vulnerabilities which first identifies the node status whether the node is active or dead and whether it comprised with attacker's activity. Here, it is proposed trust aware detection techniques to prevent the attack and provide secure connection from clients to server. This design also prevents attacker's activity during data transmission. At that time it blocks the path and selects the secure path for data transmission. Next, it applied a worm and virus detection to evaluate malicious software from data. Finally, the system conducted an experiment with CAULDRON tools and realized that this proposed Zero Day Vulnerability Prevention Framework and routing aware techniques together provides an efficient and secure network for data transmission.

There are several interesting areas for further research. The first is how the penetration testing can be applied to zero day vulnerability prevention frameworks in enterprise networks. The second is to broaden the scope by accommodating other types of attacks which requires no network connection.

REFERENCES

[1] 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

[2] T. Sommestad, H. Holm, and M. Ekstedt, "Effort Estimates for Vulnerability Discovery Projects," Proc. 45th Hawaii Int'l Conf.System Sciences (HICSS '12), pp. 5564-5573, 2012

[3] N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs," IEEE Trans.Dependable Secure Computing, vol. 9, no. 1, pp. 61-74, Jan. 2012

[4] M. Shahzad, M. Shafiq, and A. Liu, "A Large Scale Exploratory Analysis of Software Vulnerability Life Cycles," Proc. 34th Int'lConf. Software Eng. (ICSE '12), 2012

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

[6] 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.

[7] L. Wang, S. Noel, and S. Jajodia, "Minimum-Cost Network Hardening Using Attack Graphs," Computer Comm., vol. 29,no. 18, pp. 3812-3824, 2006

[8] J.W.P. Manadhata, "An Attack Surface Metric," Technical Report CMU-CS-05-155, Carnegie Mellon University, 2005

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

[10] 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.

[11] C. Phillips and L. Swiler, "A Graph-Based System for Network- Vulnerability Analysis," Proc. New Security Paradigms Workshop (NSPW '98), 1998.

[12] M. McQueen, T. McQueen, W. Boyer, and M. Chaffin, "Empirical Estimates and Observations of 0Day Vulnerabilities," Proc. Hawai Int'l Conf. System Sciences, pp. 1-12, 2009.

