IJICTR International Journal of Information & Communication Technology Research

Volume 9-Number 3-Summer 2017(7-16)

An Attack Graph Based Method for Predictive Risk Evaluation of Zero-Day Attacks

Marjan Keramati
Computer Science Department
Semnan University
Semnan, Iran
Keramati_marjan@semnan.ac.ir

Received: February 24, 2017 - Accepted: June 21, 2017

Abstract—**Performing risk assessment of computer networks is inevitable in the process of network hardening. To do efficient attack prevention, risk evaluation must be done in an accurate and quantitative manner. Such risk assessment requires thorough understanding of attack's causes or vulnerabilities and their related characteristics. But, one major problem is that, there are vulnerabilities that are known by attackers but there is no information about them in databases like NVD (National Vulnerability Database). Such vulnerabilities are referred to as unknown or zero day attacks. Existing standards like NVD ignore the effect of unknown attacks in risk assessment of computer networks. In this paper, by defining some attack graph based security metrics, we proposed an innovative method for risk evaluation of multi-step Zero-Day Attacks. Proposed method by predicting the intrinsic features of Zero-Day attacks makes their risk estimation possible. Considering the effect of Temporal features of vulnerabilities have made our approach a Dynamic Risk Estimator**

Keywords- Zero day attack; CVSS; Vulnerability; Risk Assessment; Security Metic; Network Hardening; Intrusion Prevention

I. INTRODUCTION

Intrusion Prevention is one of the main security requisites that should be done in an exact way. Being successful in this area requires evaluating the security level of each network before and after applying possible security solutions for assessing the effectiveness of each hardening approach.

Computer Network security is endangered as a result of exploiting its vulnerabilities. So, security level evaluation of computer networks is only possible by thorough understanding of its vulnerabilities and their features. By defining some security metrics which are based on the various features of vulnerabilities, the security level of each network can be measured. In the case of known vulnerabilities, such information can be extracted from Scoring Systems such as CVSS [1]. But sometimes, several months might elapse after the discovery of one vulnerability to the time of reporting its details and publishing its scores. Such vulnerabilities are referred to as zero-day vulnerabilities and have become one serious threat for computer systems. These attacks occur when, a security flaw in code is discovered and the code exploiting the flaw appears before a fix discovered or patch is available [2].

Zero -Day or Un-Known Vulnerabilities are well-known by attackers and they can easily exploit them through multi-step attacks beside known vulnerabilities by the aim of compromising the networks. But, zero-day attacks are considerably more dangerous than

known ones. The reason is that, because of the problem of insufficient information about their features, they are not usually predictable.

Note that, in some cases multi-step attacks can be modeled by security models like attack graphs. Attack graphs demonstrate possible attacks in the network and the causes of their occurrence. But, attack graphs have only qualitative description of these attacks. So, they cannot reflect the effect of applying various security solutions for network hardening. Defining model based security metrics is an alternative to solve this problem. These security metrics, makes measuring the security level of the networks possible by analyzing their attack graphs. such security metrics usually requires suitable understanding of vulnerability characteristics. Such information is only available for known vulnerabilities.

Note that, 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 [3].So, defining and utilizing model based security metrics which are independent from the vulnerabilities' characteristics can be considered as the best way for risk assessment of unknown attacks.

Some efforts like [4] have been done for risk assessment of unknown vulnerabilities. But, they have some limitations. For example, they cannot differentiate between the risk of possible zero day attacks in the network. Also, they don't consider the influence of known vulnerabilities in security evaluation of Un-Known vulnerabilities.

Note that, Computer networks have become the nerve system of enterprise information systems and critical infrastructures of human lifestyle. 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 [3].

In this paper, we regarded the above mentioned consequences of attack occurring and introduced a novel attack graph based approach for risk evaluation of zero-day attacks. The proposed approach not only considers the effect of known vulnerabilities in measuring the risk of zero-day attacks but also can differentiate between the risks of possible detectable Zero-Day Attacks in each network. Considering the tempral features of known attacks like, the likelihood of the existence of exploit tools in probability estimation, has made our system a dynamic risk estimation framework.

In this paper, Quantitative measurement of the defined security metrics has become possible by introducing a novel method for predicting the intrinsic characteristics of Zero- Day vulnerabilities.

The main usages of applying the proposed approach on real computer networks are:

- Estimating the relative effectiveness of different security solutions.
- Quantitative risk assessment of computer networks.
- Performing minimum cost network hardening in computer networks.

Note that the proposed risk assessment system is the extended version of risk assessment system which was have developed in [6]. The basic improvements of the proposed risk assessment framework over the one in [6] are:

1. This paper has a predictive attitude for the risk assessment of zero-day attacks. In order to make the predication more accurately in comparison to which has been done in [6], another novel method has been proposed that considers the behavior of all indexed vulnerabilities in anticipating the intrinsic features of the Zero-Day attack.
2. Dynamic Risk assessment of known-attack paths is now possible by the proposed method.
3. Improving the method for risk assessment of multi-step attacks is the other refinement of our paper in comparison to the last version. This improvement have been done by considering the effect of all possible attack paths associated with the vulnerability.
4. Validation of the introduced method by the aim of estimating the accuracy of the proposed approach is another significant change in comparison to before.

The remainder of this paper is organized as follows. Section II is a clear definition of Un-Known vulnerabilities by using a real network example. After a brief review of some related works in section III, the proposed method is introduced in section IV. In V and VI , VII after applying the method on two network examples, the effectiveness of the proposed method is demonstrated.

II. MOTIVATING EXAMPLE

In this section, the concept of Zero-Day Attacks is demonstrated more clearly by reviewing one well-known network example which is used in [5] for the same purpose.

Fig. 1 shows a simple network configuration including three hosts. Host 0 is the user's machine used to launch attacks, whereas host 1 and host 2 are machines within the perimeter of the enterprise network we are seeking to protect. Host1 provides an HTTP service (http) and a secure shell service (ssh), whereas host 2 provides only ssh. The firewall allows traffic to and from host 1, but only connections originated from host 2. In this example, we assume, the main security concern is over the root privilege on host 2. Clearly, if all the services are free of known vulnerabilities, a vulnerability scanner or attack graph will both lead to the same conclusion, that is, the network is secure (an attacker on host 0 can never obtain the root privilege on host 2), and no additional network hardening effort is necessary. However, we may reach a different

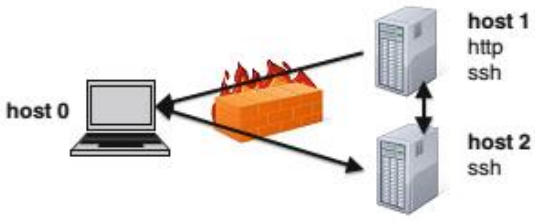

Figure 1. Illustrating Example [5].

conclusion by hypothesizing the presence of zero-day vulnerabilities and considering how many distinct zero-day exploits the network can resist [5].

The zero-day attack graph of this example is depicted in Fig. 2, where each triple inside an oval denotes a zero-day exploit and a pair denotes a condition. In this attack graph, we can observe three sequences of zero-day exploits leading to root (2). First, an attacker on host 0 can exploit a zero-day vulnerability in the firewall (e.g., a weak password in its Web-based remote administration interface) to re-establish the blocked connection to host 2 and then exploit ssh on host 2. Also, the attacker can exploit a zero-day vulnerability in either http or ssh on host 1 to obtain the user privilege. then, using host 1 as a stepping stone, the attacker can further exploit a zero-day vulnerability in ssh on host 2 to reach root(2). Since this last sequence (ssh on host 1 and then ssh on host 2) involves one zero-day vulnerability in the ssh service on both hosts, this network can resist at most one zero-day attack. Contrary to the previous belief that further hardening this network is not necessary, this zero-day attack graph shows that further hardening may be indeed for improving the security. For example, suppose we limit accesses to the ssh service on host 1 using a personal firewall or iptables rules, such that an arbitrary host 0 cannot reach this service from the Internet. We can then imagine that, the new attack graph will only include sequences of at least two different zero-day vulnerabilities (e.g., the attacker must first exploit the personal firewall or iptables rules before exploiting ssh on host 1). This seemingly unnecessary hardening effort thus can help the network resist one more zero-day attack [5].

Reference [4], proposed a security metric for measuring the risk of zero-day vulnerabilities for a computer network. This security metric that is called k-zero-day safety is based on the minimum number of distinct zero-day vulnerabilities that are needed to compromise a given network asset. The more the the amount of the mentioned security metric the less the security level of the network. Because, it will be less likely to have a large number of different unknown vulnerabilities all available at the same time, applicable to the same network, and exploitable by the same attacker.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 will be significantly smaller.

In the above example, the amount of K-Zero safety metric before applying the hardening policy (limiting accesses to the ssh service on host 1) is one and after limiting the access to host 1, this metric increases to two. This example clearly shows that, increment in K-Zero safety metric reflects the network security level improvement.

In this paper we used the mentioned security metric to define some other model based security metrics for Risk Assessment of Zero-Day Vulnerabilities.

III. RELATED WORKS

Numerous works have been done in the field of vulnerability risk assessment, improving network security, network hardening, and defining security metrics. In this section a brief review of some more related ones are provided.

Vulnerability Risk Assessment

Recently many standard efforts have been done for risk assessment of known vulnerabilities and software weaknesses. Common Vulnerability Scoring System (CVSS) [1] as a vulnerability scoring system and the Common Weakness Scoring System (CWSS) [6] as a system for software weakness scoring are two well-known examples.

Both CVSS and CWSS measure the relative severity of individual vulnerabilities in isolation and do not consider the relationship between vulnerabilities in the process of risk assessment. As the most important challenge with these scoring systems, it is worthy to mention their inability in risk assessment of multi-step attacks. So, defining attack graph based security metrics as a tool for estimating the risk of multi-step attacks has become an important requirement.

On the other hand, CVSS and CWSS can be considered as a practical foundation for security metrics. This is because, they provide security analysts and vendors standard ways for assigning numerical scores to known vulnerabilities which are already available in public vulnerability databases, such as the National Vulnerability Database (NVD) [8].

Security Metrics

There are points that should be considered in defining security metrics. According to [7], Good metrics can be measured consistently, are inexpensive to collect, expressed numerically, have units of measure, and have specific context. The National Institute of Standards and Technology (NIST) [10] describe security metric implementation process and principles for establishing a security baseline [11].

In [12] a metric was proposed for assessing the network security. It is called attack resistance and show the complexity of exploiting that attack.

In [13] an attack graph based metric was introduced for risk evaluation of the attacks in the network. This metric evaluates network security based on the length of the existing attack paths in the network that reflects the attacker's effort and diversity of vulnerabilities in the network as an indicator for amount of knowledge that attacker requires. The main problem with this

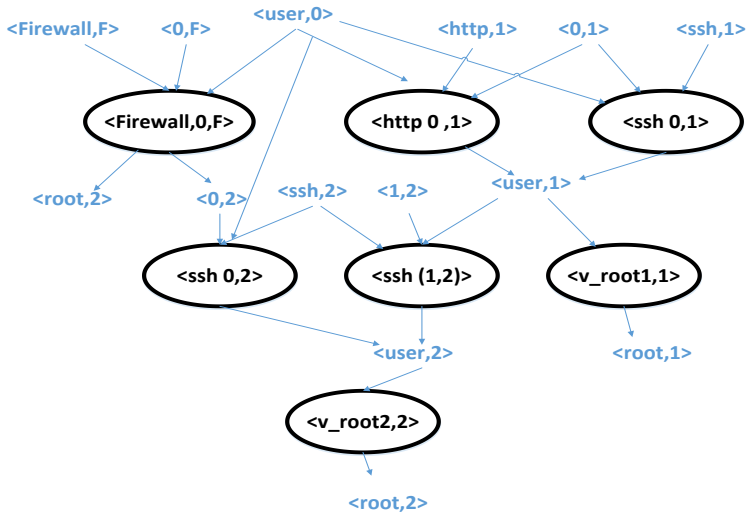

Figure 2. Zero Day Attack Graph of Fig. 1[5].

metric is that it neglects the interdependencies between vulnerabilities.

In [14] some novel attack path security metrics are proposed that measure the security of considered network. Also they suggested an efficient approach for combining these security metrics that compare the security of two different networks. The main problem with [14] is that, in assessing network security, they ignored the inherent features of the vulnerabilities and it seems that their definition of security metrics is based on one simple assumption that, vulnerabilities are inherently similar and in general it is not true. Because, differences in the natures of vulnerabilities may change the probability of their exploiting.

In [15] a valuable CVSS based approach is proposed that has tried to rank each vulnerability by efficiently considering the relationship between vulnerabilities in the network

Attack Graphs

Modeling network security is one of the most important fields in network security. One of the modeling tools is attack graph. Numerous efforts have been done for generating attack graphs like [17].
Attack graphs are efficient tools for demonstrating possible ways for the attacker to intrude his goal. On the other hand, it can specify what vulnerabilities and with which sequence can be exploited by an attacker to reach his aim. By one view, attack graphs can be divided into two groups. State based and compact attack graphs [14, 19]. In state based attack graphs, despite of possible attacks, beneficial information about the status of the network is also demonstrated. Such as all services that are executed on each host, accessibility of each user on each host, etc. But the disadvantage is that generating such graphs are so time consuming because their generation complexity is exponential in terms of number of hosts in the network and their vulnerabilities. As a result, compact or exploit-based attack graphs has been introduced. These graphs can be generated in polynomial time. So in many usages like [13, 19] and in our study, we selected compact attack graph for defining security metrics. In these attack graphs, there are two types of nodes, exploits and conditions. Exploits are exploited vulnerabilities and conditions are required conditions for exploiting vulnerabilities and consequences of exploiting them in the network. Example of such graphs is shown in Fig.1.in this figure, exploits are shown with rounded boxes and conditions are depicted by labels on edges.

Minimum Cost Network Hardening

Efforts like [19] [20] are examples of researches in minimum cost network hardening. Proposed methods are based on attack graph and they try to find the best result by traversing it. But finding the optimal solution scales exponentially with the size of the attack graph [21]. [21] is one of the most efficient efforts in this area as it proposed a methodology that can find a near optimal solution in linear time. [22] is the collection of the authors achievements in performing minimum cost network hardening. the main shortcoming with [19], [20], [21] is their inability for measuring the amount of security improvement for each optimal solution. So by using these approaches, performing cost-benefit tradeoff will be impossible.

Zero Day Attacks Risk Assessment of Zero Day Attacks

Reference [5], proposed a set of polynomial approaches for measuring the level of k-zero day safety of each network by analyzing its vulnerabilities. Authors in [22] introduced an approach for measuring a network's mean time-to-compromise by considering both known and zero day attacks. It first devises models of the mean time for discovering and exploiting individual vulnerabilities. Then, it employs Bayesian networks to derive the overall mean time-to-compromise by aggregating the results of individual vulnerabilities.
As it is said before, the main problem with the existing methods for risk assessmnet of Zero-Day vulnerabilities is that, they do not consider the effect of known vulnerabilities in risk assessment of zero-day attacks. Also, they cannot discriminate between the risk of existent zero day vulnerabilities in the network.

This paper is a method for risk assessment of zero-day vulnerabilities that assigns the risk of each vulnerability separately by considering the effect of Known ones in each network.

IV. PROPOSED METHOD

Intrinsic Characteristics of each known vulnerability are available in Vulnerability Data Bases like NVD [8]. So, Risk Assessment of attacks that are composed of known vulnerabilities can be possible.

But, in the case of Zero-Day Attacks that there is no enough information about their features, Risk evaluation have become a serious challenge. So, it should be performed in a way that is independent from the vulnerability characteristics as much as possible.

In this paper, the method for Risk Assessment of Zero Day Attacks has been defined based on some Attack Graph Based Security Metrics that can be measured quantitatively by the analysis of the network's attack Graph.

Risk Of vulnerability V_i can be assessed with (1) with multiplying the probability of exploiting it by the amount of damage exploiting it will impose on security parameters of the network [23].

$$Risk\ (V_i) = Probability\ (V_i) \times Impact\ (V_i) \quad (1)$$

Note that, Zero Day Attacks can be modeled by attack graphs like the one described in section II. So, in order to do risk assessment, we defined our security metrics based on attack graphs to be easily measurable. These security metrics are introduced in two below subsections

A. *Probability Estimation of Zero-Day Attacks*

In this paper, some security metrics are defined for probability estimation. These security metrics are inspired from the K-Zero-Day Safety security metric which is used by [4]. Proposed security metrics are:

- **K-Zero-Day Safety of a Zero-Day Vulnerability:**
  This security metric indicates the minimum number of Zero-day vulnerabilities that are required for exploiting each Un-known Vulnerability. The more this security metric for each vulnerability, the less the probability of exploiting it.
- **Length of the K-Zero-Day Path**
  The sequence of vulnerabilities that includes one or more Zero-Day vulnerabilities for exploiting each vulnerability is called the K-Zero-Day Path. This path may consist of both known and Zero-Day Vulnerabilities.
  The more the length of this path, the more effort the attacker should make for reaching the goal, so the lower the probability of exploiting each Vulnerability.
- **Exploitability of K-Zero-Day Path**
  Different vulnerabilities have different levels of difficulty for exploiting. We regarded this issue and defined a security metric for assessing the exploitability level of each attack path.

Security Metric in (2) indicates the exploitability of each attack path (Sequences of vulnerabilities that can help the attacker to reach his/her goal in the attack graph.).

in (2) we have below parameters:

- ✓ PL is the length of the K-Zero-Dat path consisting of both known and Zero-Day Vulnerabilities.
- ✓ $IExp\ (V_i)$ is the Intrinsic Probability of exploiting vulnerability V_i.
- ✓ $DExp\ (V_i)$ is the Dynamic Probability of exploiting vulnerability V_i

$$Exploit(Path) = \frac{1}{PL} \times \sum_{i=1}^{PL} IExp\ (V_i) \times DExp\ (V_i)\ . \quad (2)$$

The probability of exploiting each vulnerability is calculated by (3).security metrics in (3) are:

- ✓ KZS is the K-Zero-Day Safety of the vul defined earlier.
- ✓ $KPath$ implies K-Zero-Day Path.

$$Prob\ (vul) = \frac{1}{PL} \times \frac{1}{KZS} \times \frac{Exploit(KPath)}{10} \quad . \quad (3)$$

(3), calculates the probability of exploiting each attack path which lead to exploiting vulnerability vul.

Note that in each network, there is usually more than one attack path that leads the attacker to exploit a vulnerability. So, for each possible attack path, we calculate (3) and pick the maximum one as the probability of exploiting that vulnerability.

Quantifying the Proposed Risk Metrics

As we mentioned earlier, According to [9], Good metrics can be measured consistently, are inexpensive to collect, expressed numerically, have units of measure, and have specific context. So, for a security metric to be used practically in Risk assessment of real networks, it is a must to define it in a way to be quantifiable.

By considering such necessity, defining security metric in (2) , (3)was done in such a way to be quantified by attack graph analysis and extracting vulnerability related information from CVSS.

Involved security metrics in (2), (3) and the way of quantifying them are as below:

- ✓ PL: The length of each attack path can be determined by attack graph analysis in polynomial time.(generation and analysis of compact attack graphs is done in polynomial time. [13, 19])
- ✓ KZS : This metric can be measured by analyzing the attack graph in polynomial time too.
- ✓ $IExp\ (V_i)$. for known vulnerabilities this security metric is available in CVSS(named Exploitability) and reflects the difficulty level of exploiting it based on the vulnerability's intrinsic features. The higher this parameter, for each vulnerability the easier exploiting it and the probability of exploiting goes higher.

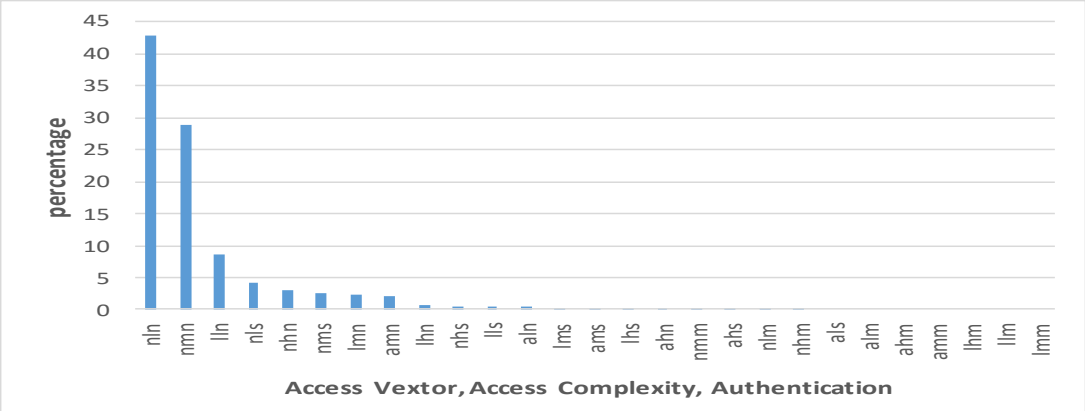

Figure 3. Exploitability parameters for the indexed vulnerabilities between 1988 and 2016.

But for Zero –Day Vulnerabilities, such information is not available. So, we extracted the Exploitability sub-score for all indexed vulnerabilities (1988-2016) from CVSS to follow the behavior of known vulnerabilities in risk estimation of un-known vulnerabilities. results is shown in Fig .3

Exploitability sub-score consists of three parameters (Access Vector, Access Complexity and Authentication).These parameters are shown in TABLE I. 27 different patterns can be possible by these three parameters. CVSS Calculator assigns one numeric score for each of these 27 parameters.

Fig .3 demonstrates the percentage of each possible 27 patterns among the extracted vulnerabilities.Based on the information in Fig .3, we calculated the weighted Average of the reported 27 patterns in (4) as a prediction of the Exploitability parameter of each Zero-Day Vulnerability and used it as quantitative measure for $IExp\ (V_i)$.

$$IExp\ (V_{Zero-Day}) = \sum_{i=1}^{27} percentage\ (pattern_i) \times Numeric - Score\ (pattern_i) \quad (4)$$

Applying (4) on the information in Fig .3 results in 8.03. So, for each zero-day vulnerability, we assign 8.03 to its $IExp$ metric.

- ✓ $DExp\ (V_i)$: in this paper, we considered the Dynamic Probability of exploiting vulnerability V_i as the probability of introducing exploits that can be evaluated by the Pareto distribution in (5). Parameters for the best match with real data are shown too. In (5), x is the age of the vulnerability that is calculated by counting the days between the date of the first disclosure and the date the CVSS Scoring is conducted (for example Today) [24].

$$F(x) = 1 - \left(\frac{k}{x}\right)^{\alpha}. \quad (5)$$
$$k = 0.00161\ ,\quad \alpha = 0.260$$

TABLE I. POSSIBLE VALUES FOR SOME CVSS SUB-SCORES.

Access Vector	Access Complexity	Authentication	I_C, I_I, I_A
Local (l)	High (h)	Multiple (m)	None (n)
Adjacent Network (a)	Medium (m)	Single (s)	Partial (p)
Network (n)	Low (l)	None (n)	Complete (c)

Note that, for Zero-Day Vulnerabilities $DExp\ (V_i)$ is 1. This is because of the nature of such vulnerabilities that, exploit tools are available for them before their exposure.

In this paper, we also introduced a security metric in (6) for the probability estimation of exploiting attack paths which does not consist of Zero-Day vulnerabilities

$$Prob\ (path) = \frac{1}{PL} \times \frac{Exploit(Path)}{10} \quad (6)$$

B. *Impact Estimation*

In CVSS, for each known vulnerability there is a parameter Impact that reflects the consequence of exploiting the vulnerability on Confidentiality, Integrity and availability of the network. Three sub-parameters of Impact parameter is shown in TABLE I.

for un-known (Zero-Day) vulnerabilities, such information is not available. consequently, we tried to analyze the nature of indexed vulnerabilities in order to predicate and estimate the Impact of these vulnerabilities.

To reach this goal, we extracted the Impac for all known vulnerabilities (1988-2016) to follow the behavior of known vulnerabilities in risk estimation of un-known vulnerabilities. The results are shown in Fig. 4. calculating the weighted Average of the reported 27 possible patterns of Impact sub-parameter in (7) results in 6.8. as a results we consider the Impact of exploiting each Zero-day vulnerability equal to 6.8.

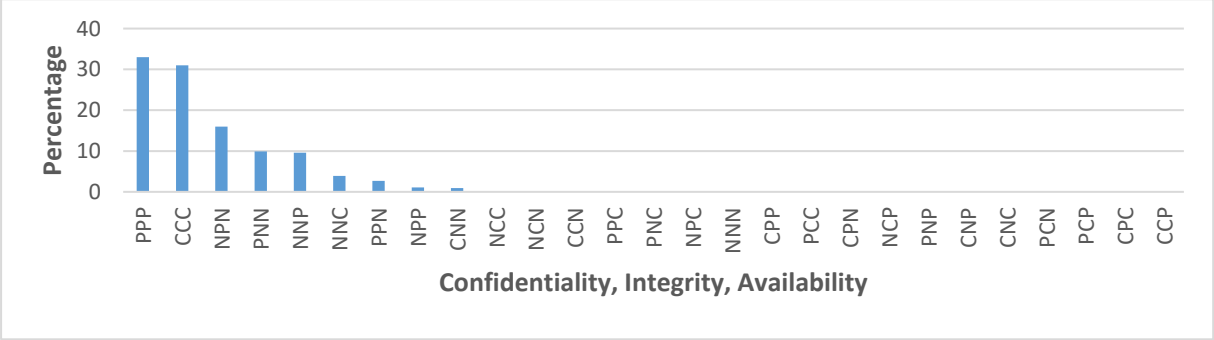

Figure 4. Percentage of possible combination of Impact parametrs for the indexed vulnerabilities between 1988 and 2016

$$Impact\left(V_{Zero-Day}\right) = \sum_{i=1}^{27} percentage\ (pattern_i) \times Numeric - Score\ (pattern_i) \quad (7)$$

But, as exploiting each Zero-Day vulnerability like the other ones occurs as a result of exploiting other vulnerabilities, we considered the Impact of each Zero-Day vulnerability to be equal to the Impact of its associated K-Zero-Dat path .

In this paper, the Impact of each attack path is estimated by calculating the Arithmetic Average for the Impact parameter of the path's involved vulnerabilities.

Also, we considered the Impact of each K-Zero-Day path to be the mean of its involved vulnerabilities.

Now it is possible to use (1) for risk assessment of Zero-Day attacks. In the Next section, the results of applying our method on two network example are shown.

V. EXPERIMENTAL RESULTS

The results of risk assessment for two network examples are shown in two below sub sections.

A. *The First Network Example*

Reference [22] used the network in Fig. 5 for illustrating the concept of Zero-Day Attacks. Here, the risk of Zero-Day Vulnerabilities of this network is evaluated by the proposed approach.

In this network, file transfer protocol (ftp) service on host 1 has a vulnerability (CVE-2001-0886). Also, the remote shell service (rsh) is another vulnerability (CVE-1999-1450); a buffer overflow vulnerability (CVE-2010-3814) is present on host 2. In addition, a secure shell service (ssh) which is free from any known vulnerability is running on both hosts. For simplicity, it is assumed that the firewall cannot be compromised. Exploitability parameter of the mentioned known vulnerabilities are shown in TABLE II.

Suppose, the main security concern is to prevent gaining root privilege on host 2. Fig. 6 depicts, what may happen in this network. each predicate inside an oval indicates an exploit vulnerability (source host, destination host) (shaded ovals represent zero day exploits), each predicate in plaintext is a security-related condition condition(host), condition(host1, host2), or the connectivity(source host, destination host). An exploit can be executed only if, all of its pre-conditions are satisfied. A condition may either be initially satisfied (e.g.,(0,1)), or be the post-condition of an exploit (e.g.,user(1)).

Required parameters for Risk Assessment of Zero-Day Vulnerabilities in this network are shown in Table III.

Exploitability Sub-Score of the Known vulnerabilities were extracted from CVSS. Note that,the current Version of CVSS Calculator is v2. But the Exploitability and Impact sub-scores are also available in v3 [1]. So, our risk assessment method can be extended easily to be compatible with the CVSS Calculator v3 too.

The Exploitability and Impact parameters of Zero-Day vulnerabilities are considered to be 8.03 , 6.8 respectively by interpretations in section IV.

This example shows the ability of the proposed method in risk assessment of un-known vulnerabilities by considering the effect of the known ones, that is an improvement over the existing approachs.

B. *Second Network Example*

Risk assessment of zero-day vulnerabilities was also done for the illustrating network example in Fig .1 esults are shown in TABLE IV.

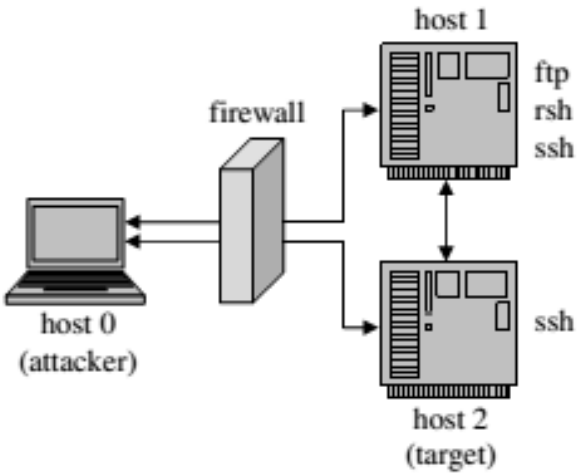

Figure 5. The First Network Example [22]

TABLE II. EXPLOITABILITY SUB-SCORE OF KNOWN VULNERABILITIES FOR THE NETWORK IN FIG 5.

Vulnerability	Exploitability Sub-Score	Impact
CVE-2001-0886	3.9	6.4
CVE-1999-1450	10	6.4
CVE-2010-3814	8.6	6.4

VI. VALIDATING THE PROPOSED APPROACH

One way to validate the accuracy of the available methods for risk assessment of Zero-Day Vulnerabilities is to compare the Risk Assessment results before and after the disclosure of the Zero-Day Vulnerability.

In this paper, there is a predictive perspective for risk estimation of Zero-Day Attacks. We did this prediction by trying to follow the behavior of known vulnerabilities. So, In order to evaluate the accuracy of this prediction, for the network in Fig. 5, we did risk assessment before and after disclosure of Zero-Day vulnerability in ssh service.

The results are shown in Table V.

CVSS considers below qualitative levels for possible vulnerability's quantitative risk level:

- 0 <Risk <4 : qualification degree=low
- 4 <=Risk <7 : qualification degree=medium
- 7 <=Risk =<10 : qualification degree=high

Note that, the risk of the zero-day vulnerabilities of ssh service in Fig. 5 (ssh(0,1), ssh(0,2) ,ssh(1,2)) remained in the same qualitative risk level before and after disclosure. so, there is no false negative (change to higher qualitative levels) nor false positive (change to lower qualitative levels) in the risk measurement done by our approach.

Risk assessment after disclosure in the present approach is done by defined security metric in (6).Another important point is that, as generation and analysis of compact attack graphs is done in plynomial time [13], the introduced method can be used for risk assessment of Zero-Day Attacks in real world.

I. COMPARING THE PROPOSED APPROACH WITH SIMILAR SCORING SYSTEM

Standard Systems

Existing standards like CVSS Only Score Known vulnerabilities and do not provide security analysts with Zero-Day attacks related information.

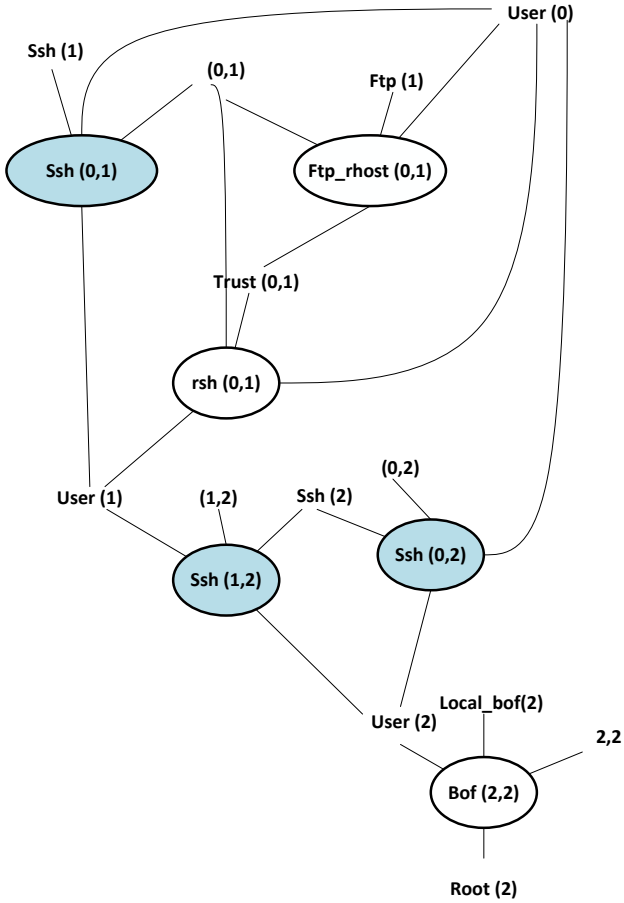

Figure 6. Attack Graph of the First Network Example in Fig 5[22]

TABLE III. RISK ASSESSMENT OF THE NETWORK IN FIG 5.

	KZS	PL	$Exploit(KPath)$	$Impact$	$Prob$	$Risk$
Ssh(0,1)	1	1	8.03	6.8	1	6.8
Ssh (1,2)	1	3	9.21567	5.366667	0.307189	1.64858
Ssh (0,2)	1	1	8.03	6.8	1	6.8

TABLE IV. RISK ASSESSMENT OF THE NETWORK IN FIG 1.

	KZS	PL	$Exploit(KPath)$	$Impact$	$Prob$	$Risk$
Firewall (0,1)	1	1	10	6.4	1	6.4
htp (0,1)	1	1	10	6.4	1	6.4
Ssh (0,1)	1	1	10	6.4	1	6.4
Ssh (0,2)	2	2	10	6.4	0.25	1.6
Ssh (1,2)	2	2	10	6.4	0.25	1.6

TABLE V. VALIDATING PERFORMED RISK ASSESSMENT FOR FIG 5 BY THE PROPOSED APPROACH.

	Risk **(before disclosure)**	**CVE after Disclosure**	***Risk*** **(after disclosure)**
Ssh(0,1)	6.8(medium)	CVE-2012-5975	4.3(medium)
Ssh (1,2)	1.64858(low)	CVE-2012-5975	2.016993(low)
Ssh (0,2)	6.8(medium)	CVE-2012-5975	4.3(medium)

Non-Standard Systems

Some efforts like [4] have been done in assessing the risk of unknown vulnerabilities. But, they have some limitations. For example, they cannot differentiate between the risk of possible zero day attacks in the network. Also, they don't consider the influence of known vulnerabilities in security evaluation of Un-Known vulnerabilities.

The proposed approach not only considers the effect of known vulnerabilities in measuring the risk of zero-day attacks but also can differentiate between the risks of possible detectable Zero-Day Attacks in each network

II. CONCLUSION AND FUTURE WORKS

Zero-Day Vulnerabilities can be considered as one of the most interesting points for attackers. Such vulnerabilities are those which are only known by the attackers and there is no enough information about them in Vulnerability databases like NVD.

Un-Known attacks often remain hidden from the view point of the security analysts. So, despite of taking preventive solutions, the network remain vulnerable to the wide range of attacks.

In this paper, some model based security metrics are proposed for risk assessment of Un-Known or Zero-Day vulnerabilities. Quantifying the proposed security metrics have become possible by introducing a method for predicting the intinsinc features of the vulnerabilities by observing the behavior of all indexed known vulnerabilities (1988-2016)

The introduced method has considerable improvements over the previous works as it can differentiate between the separate Zero-Day Attacks in each network.

Also, it can perform risk assessment of Un-known attacks by considering the effect of known vulnerabilities in the network. This idea makes risk estimation of multi-step attacks possible.

On the other hand, considering the the likelihood of the existence of exploit tools in probability estimation, has made our system a dynamic risk estimation framework.

In the future we are going to improve our method in terms of accuracy by using mathematical methods for predicting the severity of vulnerabilities in the case of insufficient information about the intrinsic features of vulnerabilities.

REFERENCES

[1] http://www.first.org/cvss/ (accessed December, 13, 2016)

[2] Ghani, H. & Luna, J. & Khelil, A. & Alkadri, N. & Suri, N "Predictive Vulnerability Scoring in the Context of Insufficient Information Availability. In Proc. of The IEEE International Conference on Risks and Security of Internet and Systems (CRiSIS), 2013, PP.1-8.

[3] *J. McHugh. Quality of protection: Measuring the unmeasurable? In Proceedings of the 2nd ACM QoP, pages 1–2, 2006*

[4] Wang, L. & Jajodia, S. & Singhal, A. & Noel S. k-zero day safety: measuring the security risk of networks against unknown attacks. *Proc. 15th European Conf. Research Computer Security*, 2010, pp. 573–587.

[5] Albanese, M. & Jajodia, S. & Singhal, A. & Wang, L. An Efficient Framework for Evaluating the Risk of Zero-Day Vulnerabilities. In E-Business and Telecommunications, Springer, 2014, PP. 322-340.

[6] M. Keramati, "An attack graph based procedure for risk estimation of zero-day attacks," *2016 8th International Symposium on Telecommunications (IST)*, Tehran, 2016, pp. 723-728.

[7] http://cwe.mitre.org/cwss/, (accessed May, 25, 2016)

[8] http://www.nvd.org, /, (accessed May, 25, 2016)

[9] Jaquith., Security Metrics: Replacing Fear, Uncertainty, and Doubt. Addison Wesley Publication, 2007.

[10] http://www.nist.gov/computer-security-portal.cfm, (accessed May, 25, 2016)

[11] M. Swanson, N. Bartol, J. Sabato, et al., "Security Metrics Guide for Information Technology Systems", Technical Report 800-55, National Institute of Standards and Technology, 2003

[12] L. Wang, A. Singhal, S. Jajodia, "Measuring the Overall Security of Network Congurations using Attack Graphs", Proceedings of the Data and Applications Security, Springer-Verlag, pp. 98-112, 2007

[13] C. Feng, D. Liu, J. Su, Y. Zhang, "A Scalable Approach to Analyzing Network Security using Compact Attack Graphs", Journal of Networks, pp. 543-550, 2010.

[14] N. Idika, B. Bhargava, "Extending Attack Graph-based Security Metricsand Aggregating Their Application", IEEE Transactions On DependableAnd Secure Computing, pp. 1-12, 2010.

[15] Pengsu Cheng, Lingyu Wang, Sushil Jajodia, Anoop Singhal, "Aggregating CVSS base scores for semantics-rich network security metrics,"Proc. 31st International Symposium on Reliable Distributed Systems (SRDS 2012), Irvine, California, October 8-11, 2012.

[16] Sheyner, Oleg Mikhail. "Scenario Graphs and Attack Graphs."PhDThesis Submitted to School of Computer Science, Computer Science Department, Carnegie Mellon University, 2007.

[17] Sheyner, O., Wing, J.: Tools for Generating and Analyzing Attack Graphs. In: Proc. ofWorkshop on Formal Methods for Comp. and Objects, pp. 344–371 (2004)

[18] Islam, T., and Lingyu Wang. "A Huristic Approach to Minimum Cost Network Hardening Using Attack Graphs."

NewTechnologies, Mobility and Security. IEEE, 2008. 1-5..

[19] Noel, Steven, Sushil Jajodia, Brian O'Berry, and Michael Jacobs."Efficient Minimum-Cost Network Hardening Via Exploit Dependency Graphs." 19th Annual Computer Security Applications Conference. IEEE Computer Society, 2003. 86-92.

[20] M. Albanese, S. Jajodia, and S. Noel, “Time-Efficient and Cost-Effective Network Hardening Using Attack Graphs,” in Proceedings of the 42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2012), Boston, Massachusetts, USA, June 25-28, 2012.

[21] Lingyu Wang • Massimiliano Albanese Sushil Jajodia,” Network Hardening, An Automated Approach to Improving Network Security”,Springer,2014

[22] Nzoukou, W & Wang, L & Jajodia, S & Singhal, A, A unified framework for measuring a network's mean time-to-compromise. Proc. 32nd Int'l. Symp. on Reliable Distributed Systems (SRDS).2013, pp. 215-224.

[23] Joh, H. & Malaiya, Y. K. Defining and Assessing Quantitative Security Risk Measures Using Vulnerability Lifecycle and CVSS Metrics. Proc. Int. Conference on Security and Management. 2011, pp. 10-16.

[24] Frei, S. & May, S. & Fiedler, U. & Plattner, B. (2006). Large-scale vulnerability analysis. LSAD ’06: Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense, 2006, pp. 131–138.

Marjan Keramati received both her undergraduate and graduate degrees in Computer System Architecture from Iran University of Science and Technology. Currently, she is Faculty Member in Semnan University, Department of Computer Science. Also, she is Editorial Board Member in the International Journal of Cases on Information Technology (USA). Besides, she is the member of National and Technical Commission of Standard Codification and has registered one National Standard in the field of network security in 2017. Publishing papers in International Journals and Conferences, Journal paper reviewing in various prestigious International Journals and being both Scientific and Executive Committee members in International Conferences are the other examples of her academic activities. Her research Interests include: Risk Evaluation, Security Metrics, Security Modeling ,Vulnerability Analysis, Cloud Computing Security, Intrusion Prevention Systems, Intrusion Response Systems.