*IOSR Journal of Computer Engineering (IOSR-JCE)*
*e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 21, Issue 1, Ser. III (Jan - Feb 2019), PP 01-12*
*www.iosrjournals.org*

# Networks Security Assessment of Unknown Attacks

Dr. kamal Aldin Yousif
*Sadara institute – Oman -*
*Corresponding Author: kamal Aldin Yousif*

***Abstract:*** *This research is used a combination of both known and unknown attacks, Not only unknownattacks are difficult to detect and mitigate, their attack scenarios are also unpredictable, although such attack scenarios consisting of unknown attacks arepossible, they are often not taken into account when hardening the networked system because it is difficult to measure the security posture of them On theother hand, the occurrence of unknown attacks is growing rapidly [1,2]. Thus there is an urgent need for assessing the combined effects of both known and unknown attacks,unknown attacks consisting of unknown vulnerabilities, unknown devices, and unknown attack paths. This research aims to address the aforementioned problems by classifying un-known attacks, and incorporate them into the HARM.*

***Keywords:*** *HARM, unknown attacks, mitigate, attack scenarios*

Date of Submission: 01-02-2019 Date of acceptance:18-02-2019

## I. Introduction

Previous studies only dealt with known attacks and vulnerabilities in the net- worked system. Although the majority of cyber-attacks are based on exploiting only the known vulnerabilities, there are incidents that used both known and un-known attacks that caused a severe socio-economic impact upon users. Stuxnet [63] and RSA SecurID breach [2] are two well-known incidents of cyber attacksthat used a combination of both known and unknown attacks. Not only unknownattacks are difficult to detect and mitigate, their attack scenarios are also unpredictable. For example, the attack scenario of RSA SecurID breach began withphishing emails to exploit CVE-2011-0609 vulnerability, which was a zero-dayvulnerability at the time (details of the vulnerability can be looked up at the National Vulnerability Database [2]).

This research aims to address the aforementioned problems by classifying unknown attacks, and incorporate them into the HARM. Also, the severity of unknown attacks are evaluated when they are introduced in networked systems.

Lastly, two algorithms are proposed to determine mitigation strategies that minimise the effects of unknown attacks, as well as approximation algorithms to enhance the performances

## II. Problem definition

Analysis of unknown attacks by incorporating them into the hierarchical security model. Unknown attacks are classified into unknown vulnerabilities, devices, and attack paths, and security of the networked system when they are introduced is analysed based on all possible attack scenarios.

## III. Results

This goal will result inincorporation of unknown attacks into the framework of the hierarchicalsecurity model, developing new algorithms to identify significant hosts andvulnerabilities in the networked system to formulate effective mitigation strategies, and evaluation of these algorithms under various attack scenarios

## IV. Research Goals

Incorporating the Unknown attack into the hierarchical security model**.**

## V. Research methodology:

This thesis followed the scientific descriptive approach in this research, from the stage of data collection and analysis, design and implementation of programs and mathematical algorithms, processing and proving supposition.

## VI. Discussion

UnVIP are incorporated into the HARM, and the security of the networked System was analyzed taking into account various attack scenarios when unVIP areassumed. Further, new algorithms are developed to determine mitigation strategies that minimize the effects of unVIP based on identifying significant hosts andvulnerabilities in the networked system. The experimental results showed that thecombined effects of unVIP vary depending on the attack scenario. Moreover, theapproximation algorithms developed (i.e., ISHF and ISVF) can compute nearlyequivalent solutions and significantly improve the performances compared to thenaive algorithms (i.e., ISH and ISV ). However, there are limitations of solutionsproposed in this chapter, which are discussed in this section.

Although various mitigation strategies exist (e.g., as described in [4]), onlytwo unVIP mitigation strategies are considered (i.e., based on identifying significant hosts and vulnerabilities). However, it is believed that identifying significan't hosts and vulnerabilities are important intermediate steps for further networkhardening plans, because different mitigation strategies have different effects insecurity There are also various network hardening techniques (NHTs) to enhance the security (e.g., MovingTarget Defenses [4]). However, the effectiveness of deploying NHTsare not compared when unVIP are introduced in the networked system. The effect of patching vulnerabilities is taken into account, but otherNHTs are not considered, As a result, it is difficult to determine which NHTsshould be used as an unVIP mitigation strategy. Moreover, the combined effectsof NHTs to minimize the effects of unVIP have not been studied previously.

Thesecurity model does not take into account multiple NHTs, therefore it is uncertainhow the attack surface of the networked system may be changed. Therefore, otherNHTs should be incorporated into the security model and analyses the changes inthe attack surface when multiple NHTs are deployed.

System risk metric was used to analyses the security of the networked system,and also unVIP mitigation strategy algorithms are based on the results of riskanalysis. However, assessing the effectiveness of unVIP with an assumed riskvalue can be misleading, as one cannot estimate the nature of unknown attacksprecisely [6]. Therefore, it is necessary to develop various security metrics inrespect to unVIP to understand the impact of them from various aspects of securitysuch as kzd safety used in [5], or update existing metrics to measure them.

## VII. Conclusions

The volume of cyber attacks are increasing, where attackers penetrate throughby finding and exploiting vulnerabilities in the networked systems. Many of thesecurity assessments utilize only the known attacks to address flaws in the networked system, but recent cyber incidents (e.g., Stuxnet and RSA SecurID breach) showed that attackers utilize not only known attacks, but a combination of both known and unknown attacks. Only the unknown vulnerabilities are incorporated into security models in previous studies, which are analyzed with existing and/or newly developed security metrics (e.g., impact, risk, k-zero-day safety). However, these studies did not take into account the combined effects of unknown attacks.

This chapter addresses the problem of assessing the effects of combined unknown attacks in the networked system. First, unknown attacks are classified into unknown vulnerabilities, devices, and attack paths, which are incorporated into the HARM. Second, the security of networked systems with and without unVIP (taking into account both singular and combined effects) are analyzed, as well as developing two unVIP mitigation strategy algorithms that identify significant hosts and vulnerabilities to harden the networked system. Lastly, experiments were conducted, where the results showed that different unVIP attack scenarios had varying effects on the system risk. These results also showed that deploying the unVIP mitigation strategies can effectively minimize the system risk. Hence, the security effects of unVIP can be analyzed using the HARM, which can also provide effective unVIP mitigation strategies.

**Table 1:** Details of Hosts

| Host | OS | Applications | Vulnerability | Priv. Esc. |
|---|---|---|---|---|
| $U_1, U_2, U_3$ | MS Server 2003 SP1 | MS SQL server | CVE-2002-0721 | $g \rightarrow r$ |
| $U_4$ | Windows 7 SP1 | Basic | CVE-2014-2781 | $g \rightarrow r$ |
| $U_5$ | Redhat Enterprise Linux 6 | MySQL server | CVE-2008-0086 | $u \rightarrow r$ |
| $DS$ | MS Server 2008 SP2 | Oracle server | CVE-2012-3220 | $u \rightarrow r$ |
| $UR_{VPN}$ | MAC OS X | Basic | CVE-2014-0515 | $g \rightarrow r$ |

**An Example Networked System and Attack Scenarios**

Description of the Example Networked SystemDifferent network settings are assigned to provide a better insight of unVIPand their effect on the security. The same networked system is used as shownin Figure3, but different properties of hosts are assigned as shown in Table1 ,which also includes the information about a VPN user $UR_{V\ PN}$ (i.e., an $U_I$,assuming no restrictions on the technology used). Hosts are further divided intogroups: (i) $U_1$ , $U_2$ and $U_3$ are in a Web Server (WS) group, (ii) $U_4$ is in a User(UR) group, and (iii) U5 is in a Application Server (AS) group. The DB server isdenoted as DS, Only a single vulnerability for each host is assumed, which is toenable the attack scenario in the simplest form.

**Attack Scenarios:** Table 2 shows some of the possible attack scenarios with and without unVIPassumed in the example networked system. The table also includes the k-zero-day (kzd) safety metric (as in [6,7]),

**Table 2:** Possible Attack Scenarios

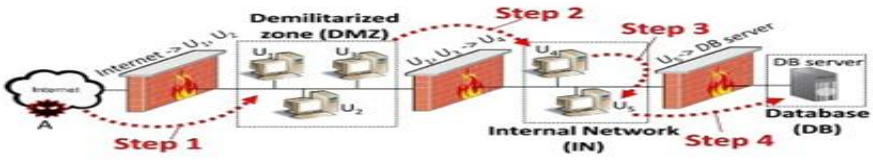
| Case | Assumption | Attack Scenario | Steps | *kzd* |
|---|---|---|---|---|
| 1 | No unVIP | $A \rightarrow WS \rightarrow UR \rightarrow AS \rightarrow DS$ | 4 | 3 |
| 2a | UV ($AS_{UV}$) | $A \rightarrow WS \rightarrow AS_{UV} \rightarrow DS$ | 3 | 3 |
| 2b | UV ($DS_{UV}$) | $A \rightarrow WS \rightarrow UR_{UV} \rightarrow DS$ | 3 | |
| 3 | UI ($UR_{VPN}$) | $A \rightarrow UR_{VPN} \rightarrow AS \rightarrow DS$ | 3 | 3 |
| 4 | UP ($UR_{VPN}$, $DS_{UV}$) | $A \rightarrow UR_{VPN} \rightarrow DS$ | 2 | 2 |

To show that it can be changed when unVIP are used in a combination,kzd safety measures the minimum number ofUVs required for the attacker to compromise the target host for a given attackscenario. These attack scenarios are illustrated in Figure 1. Those examplesshow that without any unVIP (Case 1 shown in Figure 1(a)), the attacker mustcompromise W S, UR, AS, and DS (i.e., the minimum number of exploits requiredis four). When an UV or an UI is assumed, it reduces the number of minimumsteps required by the attacker (Case 2 as shown in Figure1(b) for an UV inDS, and Case 3 as shown in Figure 1(c) for an UI in the IN subnet), However,both UVs and UIs are assumed, the attacker can exploit the UI (e.g., the VPNhost) and directly to the DS exploiting the UV (as Case 4 as shown in Figure1(d)). Moreover, the combined effects of unVIP changes the kzd safety (i.e,.from k = 3 to k = 2). Thus, these results show that (1) the combined effects ofunVIP can reduce the number of minimum exploits required, and (2) differentattack scenarios have different security effects depending on where unVIP areassumed.

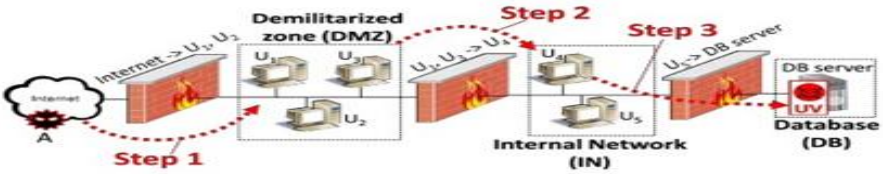
**Incorporate unVIP into the Security Model**

-2 HARM with AGs in both layers is incorporated with unVIP, which is shown in Figure 3 The upper layer remains the same as in Figure 4, but the lower layer information has changed as shown. The square box in the lower layer re-

resents the state (e.g., WS: g represents the guest privilege of W S), and the oval represents the condition (e.g., CVE-2002-0721 is a vulnerability condition that can be exploited from WS: g to gain the W S: r). For example, a u privilege is required to exploit CVE-2012-3220 in the DS to gain the r privilege.



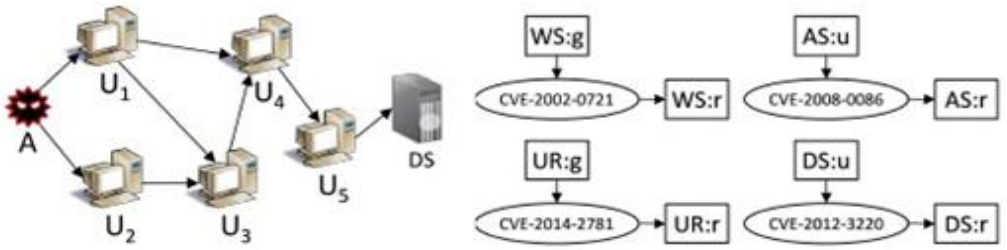

**(a) Case 1**




**(b) Case 2**


**(c) Case 3**

**Figure 1:** unVIP Attack Scenarios in the Example Networked System




(a)Upper Layer of the HARM (b) Lower Layer of the HARM

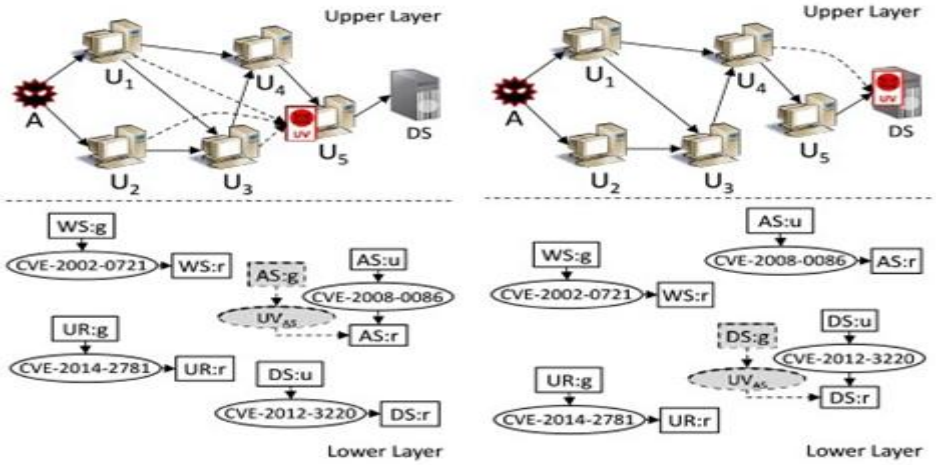
**Figure 2:** HARM of the Example Networked System

The definition of incorporating UVsinto the HARM is as follows:

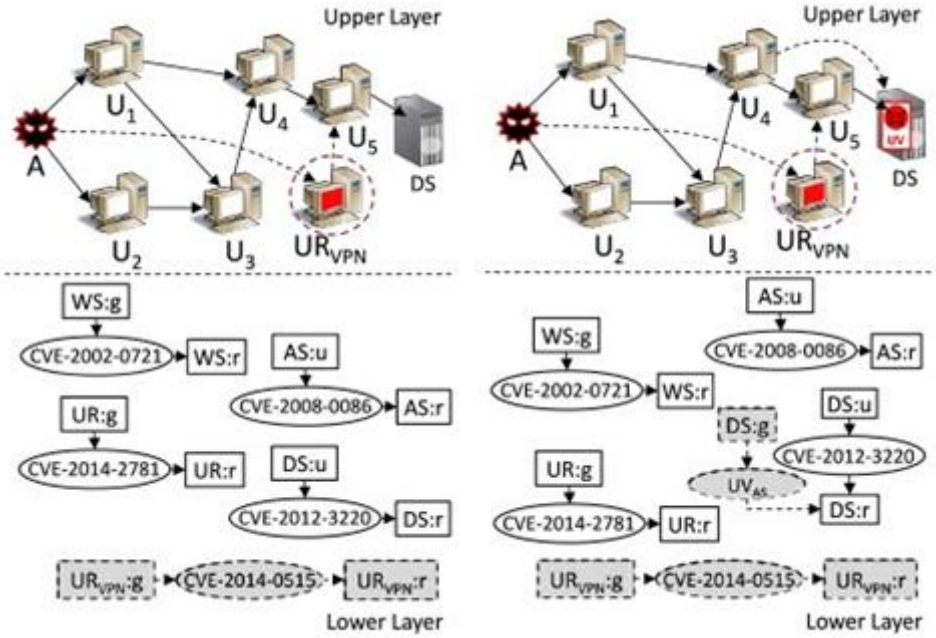
**Definition 10.** Given a HARM of a 3-tuple $H = (h, M, C)$ where $h = 2$ (as shown in Section 2.3), an UV ($uv_i$) in a node (i.e., a host) $n \in M_1$ changes the lower layer HARM to $G_n^{2*} = (N_n^{2*}, E_n^{2*})$, where $N_n^{2*} = N_n^2 \cup uv_i$ is a finite set of vulnerabilities, host states and unknown vulnerabilities, and $E_n^{2*} = (N_n^2 \times N_n^2) \cup \{(s(g), uv_i), (uv_i, s(r))\}$ is a set of edges where $s(g)$ is a guest state of the host and $s(r)$ is the root state of the host (i.e., exploiting the UV directly grants the root privilege from a guest privilege).

**Example 13. Shown in Figure 8.3(a):**
An UV assumed in AS ($uv_{AS}$ and $AS \in M_1$), a new lower layer HARM $G_{AS}^{2*} = (N_{AS}^{2*}, E_{AS}^{2*})$ is created, where $N_{AS}^{2*} = N_{AS}^2 \cup \{uv_{AS}\}$ and $E_{AS}^{2*} = E_{AS}^2 \cup \{(s(g), uv_{AS}), (uv_{AS}, s(r))\}$. UPs associated UV in AS ($up_{AS} = \{(WS, AS)\}$) (i.e., created new attack paths from WS to AS directly) creates a new upper layer $G_{AS}^{1*} = (N_{AS}^1, E_{AS}^{1*})$, where $E_{AS}^{1*} = (N^1 \times N^1) \cup \{up_{AS}\}$.

**Example 14. Shown in Figure 8.3(b):**
An UV assumed in DS ($uv_{DS}$ and $DS \in U$), a new lower layer HARM $G_{DS}^{2*} = (N_{DS}^{2*}, E_{DS}^{2*})$ is created, where $N_{DS}^{2*} = V_{DS}^2 \cup \{uv_{DS}\}$ and $E_{DS}^{2*} = E_{DS}^2 \cup \{(s(g), uv_{DS}), (uv_{DS}, s(r))\}$. UPs associated UV in DS ($up_{AS} = \{(UR, DS)\}$) (i.e., created new attack paths from UR to DS directly) creates a new upper layer $G_{DS}^{1*} = (N_{DS}^1, E_{DS}^{1*})$, where $E_{DS}^{1*} = (N^1 \times N^1) \cup \{up_{DS}\}$.




(a) An UV is assumed in AS (b) An UV is assumed in DS




(c) An UI is assumed in AS (d) UPs are assumed as a result of an UV in DS and UI in the IN Subnet

**Figure 9.3:** Incorporating unVIP in the HARM

**Example 2. Shown in Figure 3 (d):**

(a) An UV assumed in DS ($uv_{DS}$ and $DS \in U$), a new lower layer HARM $G^{2*}_{DS} = (N^{2*}_{DS}, E^{2*}_{DS})$ is created, where $N^{2*}_{DS} = N^{2}_{DS} \cup \{uv_{DS}\}$ and $E^{2*}_{DS} = E^{2}_{DS} \cup \{(s(g), uv_{DS}), (uv_{DS}, s(r))\}$.

(b) An UI in AS ($ui_{VPN}$) creates a new upper layer $G^{1*} = (N^{1*}, E^{1*})$, where $N^{1*} = N^{1} \cup \{ui_{VPN}\}$, and $E^{1*} = (N^{1} \times N^{1}) \cup \{(A, UR_{VPN}), (UR_{VPN}, AS)\}$. The corresponding lower layer, $ui_{VPN} \leftrightarrow G^{2}_{ui_{VPN}}$, is also created with the given information in Table 8.1.

(c) UPs associated with UV in DS and UI in AS ($up_{DS} = \{(A, UR_{VPN}), (UR_{VPN}, AS), (UR, DS)\}$) creates a new upper layer $G^{1\#}_{DS} = (N^{1\#}, E^{1\#})$, where $E^{1\#} = E^{1*} \cup up_{DS}$.

Various attack scenarios are taken into account (as shown in Table 2), wherethese scenarios are modeled using the HARM as shown in Figure 3, Newlyadded components are represented by dotted lines (e.g., dotted lines in the upperlayer representing new attack paths, dotted red circles representing a new device,and dotted ovals with shades in the lower layer representing new vulnerabilities).

Figures 3(a) and 3(b) show that placement of UVs changes the attack sce-nario, respectively. Figure 3(c) shows that assuming UIs can also create new attack paths. Figure 3(d) shows the most increased number of new attack paths(by nine), which implies that combined effects of unVIP can be more severe incomparison to individual unVIP assumed in the example networked system.

$$\begin{aligned} R_{system} &= \sum_{i \in path} PR_i \\ &= \sum (PR_{\{U_1,U_4,U_5,DS\}}, PR_{\{U_1,U_3,U_4,U_5,DS\}}, PR_{\{U_2,U_3,U_4,U_5,DS\}}) \\ &= 110 \end{aligned} \tag{1}$$

**Table 3:** System Risk with Two UVs

| UVs in | No. of Attack Paths | System Risk |
|---|---|---|
| None | 3 | 110 |
| WS only | 3 | 160 |
| UR only | 4 | 180 |
| AS only | 6 | 260 |
| DS only | 6 | 295 |
| WS and UR | 4 | 240 |
| WS and AS | 6 | 340 |
| WS and DS | 6 | 395 |
| UR and AS | 8 | 400 |
| UR and DS | 8 | 460 |
| AS and DS | 9 | 510 |

procedureAnalyse _ unV IP(N)
1. for i = 1 . . . |N| do
2. for d∈ S|S ⊆ N do
3. Evaluate Security
4. end for
5. end for
6. end procedure

Figure 4: Pseudo code to Analyse all unVIP Scenarios

**unVIP Mitigation Strategies**

These sections showedthat depending on where unVIP are assumed, the effects of them vary (e.g., system risks as shown in Table 3). Therefore, it is important to identify the mostsignificant network components (e.g., hosts), and harden them to minimize theeffects of unVIP, In this Section, methods to mitigate unVIP are described bymeans of: (i) identifying and hardening significant hosts to minimize the effectsof unVIP (shown above), and (ii) identifying and patching significantvulnerabilities to minimize the system risk when unVIP are assumed (shown above).

**All Possible Attack Scenarios**

Analysis of all possible attack scenarios is taken into account with unVIP assumed in the networked system, which is shown by a pseudo-code in Figure3,The pseudo-code is used to compute significant hosts and vulnerabilities later l represents the assumed number of UVs, d representsthe assumed UI in a subnet S, and N represents the networked system. Combinations of hosts are computed to consider all possible attack scenarios with a givenvalue l (e.g., with |UV | = 2, UVs are assumed for every pair of hosts).

**Identification of Significant Hosts**

An algorithm is developed to identify significant hosts by evaluating all possible attack scenarios and ranking the occurrence of each host in all possible attackpaths.

***1:procedure Identify_ Significant _Hosts( f , l, d, N)***
***2:N ← N ∪d***
***3:UV = {uv$_1$ , uv$_2$ , . . . uv$_l$ }***
***4:for UV *∈ N | UV *⊆ UV do***
***5:Analyse N$^{VU*}$***
***6:Compute host occurrence score(h)***
***7:end for***
***8:Return {h$_{max}$∈ N ∩ f | score(h$_m$ax) > score(hi ), i = 0 . . . |N ∩ f |, i≠ max}***
***9 :end procedure***

Figure 5: Identifying Significant Hosts Algorithm There are various mitigation techniques available to minimize the effects of unVIP when significant hosts are identified, such as increasing the diversity ofservices, strengthening isolation techniques, enforcing more strict access controlpolicies, and patching known vulnerabilities (as described in [8]), the initialsecurity analysis of unVIP above showed various effects of unVIP

in thenetworked system, To harden the networked system accordingly, it is important toidentify and deploy mitigation techniques on significant hosts in respect to attackscenarios developed from unVIP assumed.

**Naive Algorithm**

The algorithm, Identify Significant Hosts (ISH), to identify significant hosts is shown in Figure 3, f is a filter expression that allows users to input hosts to be filtered from the result, l is the number of UVs, d is the subnet containing the UI, and N is the networked system. This algorithm is processed in line 4 in the pseudo-code shown in Figure 4 (i.e., a function call at line 4). Line 4 in ISH specifies all possible host combinations of UVs assumed in the networked system,and the security of a given state is evaluated along with the occurrence of hosts. score(h) computes the number of occurrences a host appears in all possible attackpaths for the given state of the networked system, The returned result (i.e., line 8in ISH) is the host with the most occurrences in all attack scenarios (i.e., the mostutilized host in any attack scenarios with unVIP in the networked system).

***1:procedure Identify _Significant _Hosts Fast( f , l, d, N)***
***2:*** $N \leftarrow N \cup d$
***3:*** $UV = \{uv_1, uv_2, \ldots uv_l\}$
***4:*** $h_j \in N^* \mid N^* \subseteq N, |N^*| = |UV|$
***5:while*** $|N^*| > 1$ ***do***
***6:remove*** $h_{min} \in N^* \mid c(h_{min}) < c(h_j)$
***7:end while***
***8:Return*** $\{h_{max} \in N \cap f \mid c(h_{max}) > c(hi),\ 1 \geq i \geq |N \cap f|,\ i \neq max\}$
***9 :end procedure***

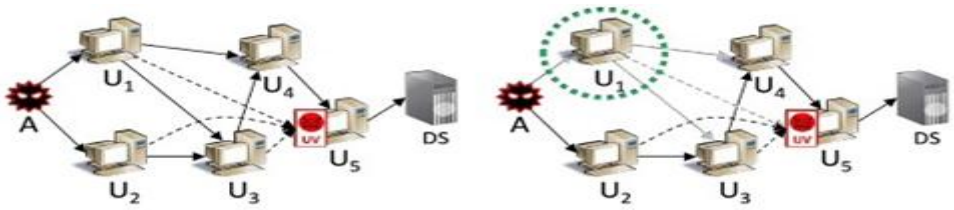
Figure 6: Identifying Significant Hosts Approximation Algorithm

**Table 4:** Significant Hosts of the Example Networked System

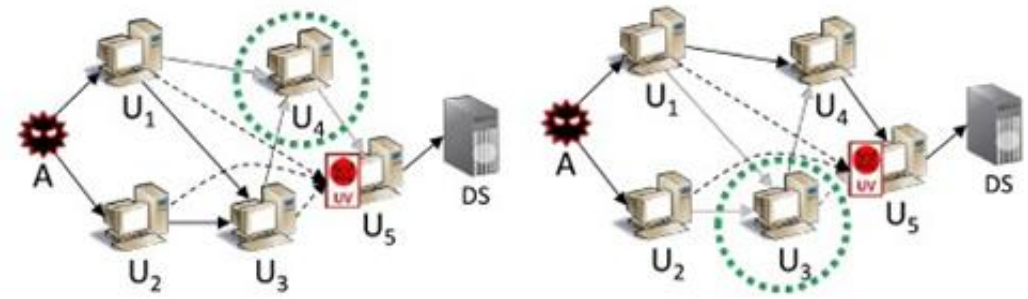
| | | Significance (1=Most, 6=Least) | | | | | |
|---|---|---|---|---|---|---|---|
| UI | | 1 | 2 | 3 | 4 | 5 | 6 |
| None | *ISH* | $U_5$ | *DS* | $U_3$ | $U_4$ | $U_1$ | $U_2$ |
| | *ISHF* | ***DS*** | $U_5$ | $U_3$ | $U_4$ | $U_2$ | $U_1$ |
| DMZ | *ISH* | $U_5$ | *DS* | $U_3$ | $U_4$ | $U_2$ | $U_1$ |
| | *ISHF* | ***DS*** | $U_5$ | $U_4$ | $U_3$ | $U_2$ | $U_1$ |
| IN | *ISH* | $U_5$ | $U_3$ | *DS* | $U_4$ | $U_1$ | $U_2$ |
| | *ISHF* | ***DS*** | $U_5$ | $U_3$ | $U_1$ | $U_4$ | $U_2$ |
| DB | *ISH* | $U_5$ | $U_3$ | *DS* | $U_4$ | $U_2$ | $U_1$ |
| | *ISHF* | ***DS*** | $U_5$ | $U_4$ | $U_3$ | $U_2$ | $U_1$ |

**Effectiveness of Identifying Significant Hosts**

Figure 7 shows the effectiveness of identifying significant hosts in compar- ison to randomly selecting hosts to harden. An UV is assumed in AS group (i.e., an UV in U5 ), and hardening a host disables the attack path through the hard- ened host (which are highlighted by green dotted circles), The most significant host to harden can be computed using the ISH, which in this example case is U5 followed by DS as shown in Table 4, but hardening either one of them would disable all possible attack paths. Hence, the next important host is hardened to show the difference of security analysis, which is host U3, When U3 is hardened (shown in Figure 7(d)), the system risk is reduced from 260 down to 105, which is more than the half of the system risk without hardening any hosts. The same effect is observed when other randomly chosen hosts are hardened (as shown in Figures 7(b) and 7(c)). However, both of these resulted in higher system risk in comparison to hardening the significant host U3.




(a) No Hardening. The System Risk is 260. (b) Hardening $U_1$ . The System Risk is 133.




(c) Hardening $U_4$ . The System Risk is 160.(d) Hardening $U_3$ . The System Risk is 103.

**Figure 7:** Security Analysis after Hardening a Host in the Networked System

**Identification of Significant Vulnerabilities**

This section shows the computation of identifying significant vulnerabilitiesknown in the networked system when unVIP are assumed. Similarly as shown above ,an algorithm is developed to compute all possible attack scenarios to analysesthe significance of patching vulnerabilities, and evaluate the effectiveness of it.

For the security assessment, changes in the system risk are taken into accountwhen patching known vulnerabilities. However, other security metrics can also beused (e.g., probability of an attack and mitigation costs).

**Naive Algorithm**

Figure 8 shows the algorithm, Identify Significant Vuls (ISV), to identify significant vulnerabilities, where it is used in conjunction with the pseudo-code (inline 4) shown in Figure 3, The variables have the same implications as shown Previously(apart from the filter expression, f , where it filters vulnerabilities specifiedby users), and vi ∈ N ∩ f is a set of all known vulnerabilities vi in the networkedsystem N. Steps from 7 to 9 in ISV patches the known vulnerability and calculate

***1 :procedure Identify _Significant _Vuls( f , l, d, N)***
***2: N ← N ∪d***
***3: UV = {uv$_1$ , uv$_2$ , . . . uv$_l$ }***
***4: for UV *∈ N | UV *⊆ UV do***
***5: for v$_i$∈ N ∩ f do***
***6: Patch v$_i$***
***7: score(v$_i$) ← score(v$_i$ ) + ΔR$_{system}$***
***8: Unpatchv$_i$***
***9: end for***
***10 :end for***
***11:Return {v$_{max}$∈ N ∩ f | score(v$_m$ ax) > score(v$_i$ ), i = 0 . . . |N ∩ f |, i≠ max}***
***12:end procedure***

Figure 8: Identifying Significant Vulnerabilities Algorithm the differences in the system risk. Then, step 11 returns the vulnerability withthe most reduction in system risk. ISV computes all possible host combinationsto take into account all possible attack scenarios. Thus, the algorithm has anexponential computational complexity.

***1: procedure Identify_ Significant_ Vuls _Fast( f , l, d, N)***
***2: N ← N ∪d***
***3: UV = {uv$_1$ , uv$_2$ , . . . uv$_l$ }***
***4: V = {v$_1$ , v$_2$ , . . . v$_m$ }***
***5: h $_j$∈ N * | N *⊆ N, |N * | = |UV |, max(∑ c(h $_j$ ))***
***6: for v$_i$∈ N ∩ f do***
***7: Patch v$_i$***
***8: score(v$_i$) ← score(v$_i$ ) + ΔR$_{system}$***
***9: Unpatchv$_i$***
***10: end for***
***11:Return {max(score(v$_{min}$)) ∈ N ∩ f | score(v$_{min}$) > score(v$_i$ ), 1 ≥ i ≥ |N∩***
***f |, i≠ max{***
***12 :end procedure***

Figure 9: Identifying Known Vulnerabilities Approximation Algorithm

**Table 5:** Arbitrarily Assumed Vulnerabilities

| Vulnerabilities | Impact Values | Assigned Hosts |
|---|---|---|
| $V_A$ | 4 | WS, UR |
| $V_B$ | 3 | WS |
| $V_C$ | 6 | WS, AS |
| $V_D$ | 5 | UR, DS |
| $V_E$ | 7 | UR |
| $V_F$ | 8 | AS |
| $V_G$ | 2 | AS |
| $V_H$ | 10 | DS |

**Table 6:** Significant Vulnerabilities of the Example Networked System

| | | Significance (1=Most, 6=Least) | | | | | |
|---|---|---|---|---|---|---|---|
| UI | | 1 | 2 | 3 | 4 | 5 | 6 |
| None | *ISV* | $V_C$ | $V_F$ | $V_E$ | $V_D$ | $V_B$ | $V_A$ |
| | *ISVF* | $V_C$ | $V_F$ | $V_E$ | $V_D$ | $V_B$ | $V_A$ |
| DMZ | *ISV* | $V_C$ | $V_F$ | $V_E$ | $V_D$ | $V_B$ | $V_A$ |
| | *ISVF* | $V_C$ | $V_F$ | $V_E$ | $V_D$ | $V_B$ | $V_A$ |
| IN | *ISV* | $V_C$ | $V_F$ | $V_E$ | $V_D$ | $V_B$ | $V_A$ |
| | *ISVF* | $V_C$ | $V_F$ | $V_E$ | $V_D$ | $V_B$ | $V_A$ |
| DB | *ISV* | $V_C$ | **$V_E$** | **$V_F$** | $V_D$ | $V_B$ | $V_A$ |
| | *ISVF* | $V_C$ | **$V_F$** | **$V_E$** | $V_D$ | $V_B$ | $V_A$ |

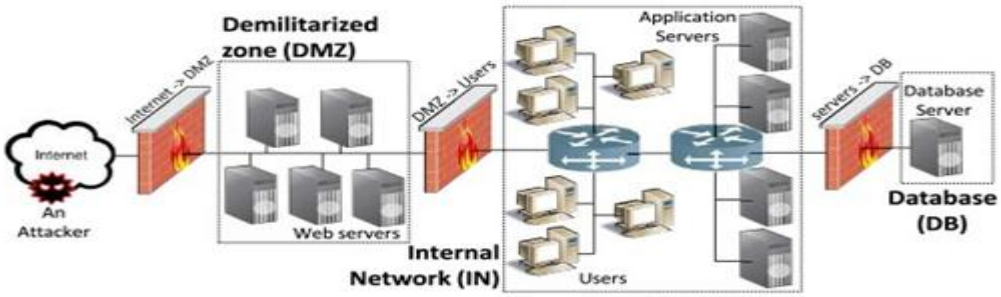



**Figure 10:** The Networked System for Simulations

**Experimental Results**

In this section, comprehensive security analyses are conducted, which showshow security of the networked system changes with respect to various attack scenarios assuming unVIP above. Further, the accuracy and performancebetween mitigation strategy algorithms are compared (i.e., naive algorithms ISHand ISV , and approximation algorithms ISHF and ISV F) as shown above. Thenetworked system for simulations (as shown in Figure 10) is assumed with vulnerabilities in Table 5.

**Security Analysis**

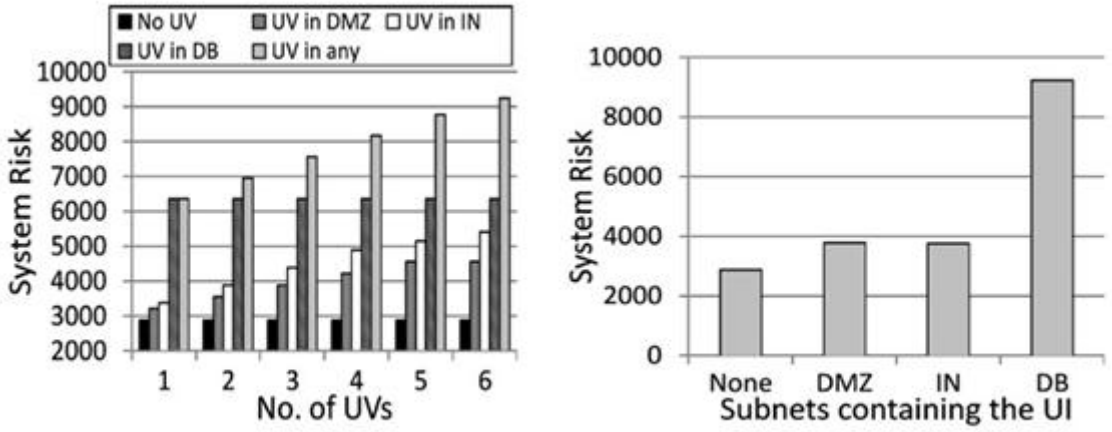
Only UVs and Only UIs in the Networked System: Figure 11 shows the security analysis of the networked system with only UVs or only UIs assumed inthe networked system. Figure 11(a) shows only UVs assumed in the networkedsystem. UPs created as a result of UVs are also taken into account. It shows thatthe system risk varies based on where UVs are assumed in the networked system)e.g., an UV in the DB subnet

resulted in a higher system risk than an UV in theDMZ subnet). An UV in the DB increased the system risk the most (which is thesubnet that contained the target host), where the system risk is increased more thandouble the amount when no UVs are assumed. If subnets not containing the targethost (i.e., DS) are taken into account, UVs in the IN subnet has higher system riskwhen compared to UVs in the DMZ subnet. As the number of UVs grows, systemrisks for all attack scenarios have increased linearly. In the case of UVs in the DBsubnet, increasing the number of UVs did not affect the system risk since therewas only a single host.

Figure 11(b) shows only an UI assumed in the networked system (with Upscreated as a result of an UI), where the VPN host with a single UV is taken intoaccount as the UI. It shows that assuming an UI in the DB subnet increases thesystem risk the most, followed by an UI in the DMZ and IN subnets. Also, thenumber of attack paths has increased from 120 to 270 when an UI is assumedin the DB subnet compared to no UIs, which resulted in more than triple theamount of system risk compared to no UIs. The number of attack paths when anUI is assumed in the DMZ and IN subnets are 144 and 145 respectively, but theincrease in system risk was higher with an UI in the DMZ subnet (i.e., less numberof attack paths with higher system risk). Therefore, the increase in system risk isnot linearly proportional to the number of attack paths.

unVIP in only the IN Subnet: Different effects of unVIP assumed only in

the IN subnet are shown in Figure 13, It shows that an attack scenario withoutunVIP has a constant system risk with respect to the number of UVs, as well asthe attack scenario with only an UI assumed (i.e., these two attack scenarios arenot affected by the number of UVs). In the case of UVs assumed, increasing thenumber of UVs almost linearly increases the system risk. The combined effectsof UVs and an UI in the IN subnet showed the highest system risk.




(a) (b)

**Figure 11:** Security Analysis of the Networked System with only UV/UI

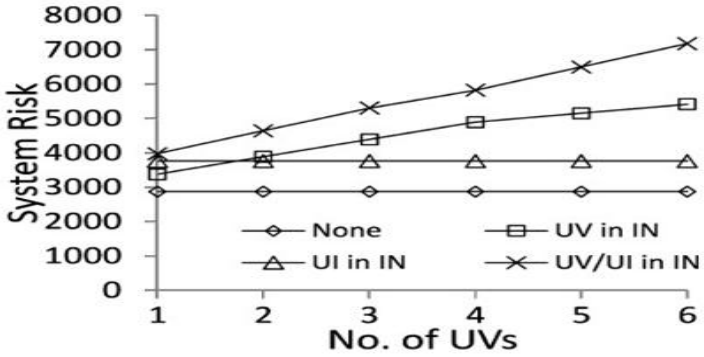
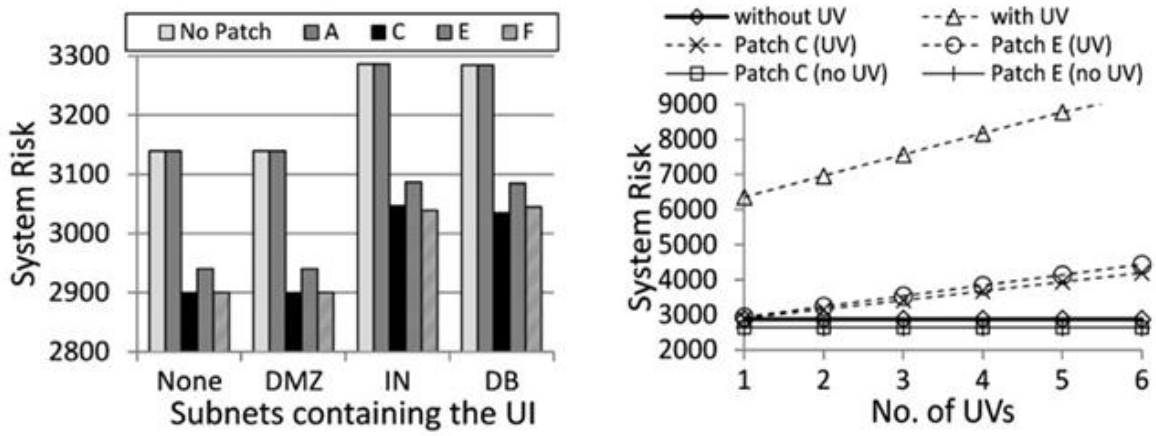



**Figure 12:** UNVIP assumed only in the IN Subnet

Patching Different Vulnerabilities in the Networked System: Figure 13 shows the effect of patching vulnerabilities in the networked system with unVIPassumed in the networked system. Figure 13(a) shows the effect of patchingdifferent vulnerabilities. One UV in the DB subnet is assumed with an UI in various subnets. Patching some vulnerabilities does not affect the system risk (e.g,.when patching vulnerability VA , no changes in system risk is observed). Also,patching different vulnerabilities have different changes in the system risk,

Forexample, patching vulnerabilities VC or VF minimizes the system risk. However,patching vulnerability VE can also reduce the system risk, but it does not decreasethe system risk as much as patching vulnerabilities VC or VF.

Figure 13(b) shows the changes in system risk when the number of UVs is increased, and the effectiveness of patching a significant vulnerability, which inthis attack scenario is vulnerability VC , When there are no UVs, patching vulnerabilities VC or VE does not have a significant effect decreasing the system risk. Onthe other hand, assuming UVs increased the system risk rapidly (e.g., more thantriple for |UV | = 6), but patching vulnerabilities VC or VE reduces the system risksignificantly, Also patching vulnerability VC is more effective (e.g., minimizes the system risk) compared to patching vulnerability VE when UVs are assumed inthe networked system. The simulation result shows that it is important to identifysignificant vulnerabilities to minimize the system risk.




(a) (b)

**Figure 13:** Effect of Patching Vulnerabilities in the Networked System

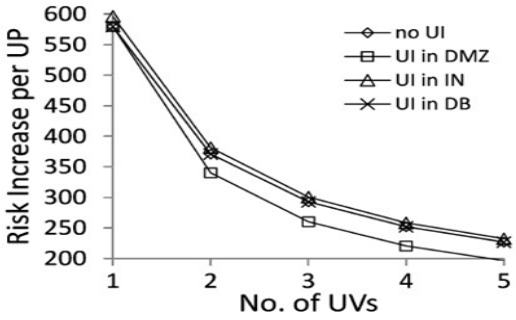



**Figure 14:** UVs in Respect to the System Risk

## References:

[1]. WU, Y., FOO, B., MAO, Y., BAGCHI, S., AND SPAFFORD, E. Automated Adaptive Intrusion Containment in Systems of Interacting Services. Computer Networks 51, 5 (Apr. 2007), 1334–1360.

[2]. XIE, A., CAI, Z., TANG, C., HU, J., AND CHEN, Z. Evaluating NetworkSecurityWithTwo-LayerAttackGraphs. InProc.ofthe25thAnnual Computer Security Applications Conference (ACSAC2009)(2009), pp.127 –136.

[3]. XIE, P., LI, J., OU, X., LIU, P., AND LEVY, R. UsingBayesianNetworks for Cyber Security Analysis. In Proc. of IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2010) (June 2010), pp. 211–220.

[4]. YACKOSKI, J., LI, J., DELOACH, S., AND OU, X. Mission-orientedMoving Target Defense Based on Cryptographically Strong Network Dynamics. InProc.ofthe8thAnnualCyberSecurityandInformationIntelligence Research Workshop (CSIIRW 2013) (New York, NY, USA, 2013), ACM, pp. 57:1–57:4.

[5]. YAGER, R. OWA Trees and Their Role in Security Modeling using Attack Trees. Information Sciences 176, 20 (2006), 2933–2959.

[6]. YUAN, E., MALEK, S., SCHMERL, B., GARLAN, D., AND GENNARI, J. Architecture-Based Self-Protecting Software Systems. In Proc. of the 9th InternationalACMSigsoftConferenceontheQualityofSoftwareArchitectures (QoSA 2013) (2013), pp. 33–42.

[7]. ZHANG, Y., LI, M., BAI, K., YU, M., AND ZANG, W. Incentive Compatible Moving Target Defense against VM-Colocation Attacks in Clouds. In Information Security and Privacy Research, D.Gritzalis, S.Furnell, and M.Theoharidou, Eds., vol.376 of IFIP Advances in Information and Communication Technology. Springer Berlin Heidelberg, 2012, pp. 388–399.

[8]. ZHANG, Z., AND WANG, S. Boosting Logical Attack Graph for Efficient Security Control. In Proc. of the 7th International Conference on Availability, Reliability and Security (ARES 2012) (Aug 2012), pp. 218–223.

[9]. ZHANG, Z., WANG, S., AND KADOBAYASHI, Y. Exploring attack graph for cost-benefit security hardening: A probabilistic approach. Computers & Security (2012).
[10]. ZHU, Y., HU, H., AHN, G., HUANG, D., AND WANG, S. Towards temporal access control in cloud computing. In Proc. of Annual IEEE International Conference on Computer Communications (INFOCOM 2012) (2012), pp. 2576–2580.
[11]. ZHUANG, R., ZHANG, S., BARDAS, A., DELOACH, S., OU, X., AND SINGHAL, A. Investigating the Application of Moving Target Defenses to NetworkSecurity. InProc.ofthe6thInternationalSymposiumonResilient Control Systems (ISRCS 2013) (2013), pp. 162–169.
[12]. ZHUANG, R., ZHANG, S., DELOACH, S., OU, X., AND SINGHAL, A. Simulation-based Approaches to Studying Effectiveness of Moving-Target Network Defense. In Proc. of National Symposium on Moving Target Research (2012).
[13]. ZONOUZ, S., KHURANA, H., SANDERS, W., AND YARDLEY, T. RRE: A Game-theoretic Intrusion Response and Recovery Engine. In Proc. of the 39th IEEE/IFIP International Conference on Dependable Systems Networks (DSN 2009) (2009), pp. 439–448.

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

Dr. Kamal Aldin Yousif. " Networks Security Assessment of Unknown Attacks" IOSR Journal of Computer Engineering (IOSR-JCE) 21.1 (2019): 01-12.