3-17-2008

VTAC: Virtual Terrain Assisted Impact Assessment for Cyber Attacks

Brian Argauer

Rochester Institute of Technology

Shanchieh Jay Yang

Rochester Institute of Technology

Follow this and additional works at: <https://scholarworks.rit.edu/other>

Recommended Citation

Brian J. Argauer, Shanchieh Jay Yang, "VTAC: virtual terrain assisted impact assessment for cyber attacks", Proc. SPIE 6973, Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2008, 69730F (17 March 2008); doi: 10.1117/12.777291; <https://doi.org/10.1117/12.777291>

This Conference Paper is brought to you for free and open access by the Faculty & Staff Scholarship at RIT Scholar Works. It has been accepted for inclusion in Presentations and other scholarship by an authorized administrator of RIT Scholar Works. For more information, please contact ritscholarworks@rit.edu.

VTAC: Virtual Terrain Assisted Impact Assessment for Cyber Attacks

Brian J. Argauer and Shanchieh Jay Yang

Department of Computer Engineering
Rochester Institute of Technology
83 Lomb Memorial Dr., Rochester, NY, USA

ABSTRACT

Overwhelming intrusion alerts have made timely response to network security breaches a difficult task. Correlating alerts to produce a higher level view of intrusion state of a network, thus, becomes an essential element in network defense. This work proposes to analyze correlated or grouped alerts and determine their ‘impact’ to services and users of the network. A network is modeled as ‘virtual terrain’ where cyber attacks maneuver. Overlaying correlated attack tracks on virtual terrain exhibits the vulnerabilities exploited by each track and the relationships between them and different network entities. The proposed impact assessment algorithm utilizes the graph-based virtual terrain model and combines assessments of damages caused by the attacks. The combined impact scores allow to identify severely damaged network services and affected users. Several scenarios are examined to demonstrate the uses of the proposed Virtual Terrain Assisted Impact Assessment for Cyber Attacks (VTAC).

Keywords: cyber security, impact assessment, information fusion

1. INTRODUCTION

A modern day network utilizes Intrusion Detection Systems (IDSs) to provide network analysts with alerts of malicious actions. Analysts typically examine these alerts manually and are more than often overwhelmed by alert volumes, allowing attacks to slip through.¹ The task of assessing cyber attacks has gone beyond detecting, and involved tracking and correlating IDS alerts. Correlating and filtering alert messages, i.e., observables, provide traces or tracks of ongoing multistage attacks in a computer network. Building upon correlated attack tracks, this work focuses on assessing the impact caused by cyber attacks.

Assessing damage or impact caused by cyber attacks is nontrivial in that it requires associating attack actions to not only network assets but also network operations and services to the users. The Common Vulnerability Scoring System (CVSS)² provides common reference scores to determine the relative severity of damage that each vulnerability poses on the application or software. These scores form the basis, but not the final answer to cyber impact assessment. Back in 1997, Lindqvist and Jonsson,³ along with the Department of Computer Engineering at Chalmers University of Technology in Sweden, made a first attempt at correlating attack types with consequences. In their paper, they use attack technique classifications originally created from Neuman and Parker.⁴ In order to correlate attacks to consequences, they utilized 25 undergraduate students who were taking a course in applied computer security. The test facility consisted of 24 SUN ELC diskless workstations, all connected to one file-server. Each student accurately recorded their attacks and the administrators set up proper monitoring software to capture all activities and breaches. The resulting taxonomy is classified by the three traditional results of computer security: confidentiality, availability, and integrity. Breaches in these three classifications in turn result in exposure, denial of service, and erroneous output, respectively. This pioneering work has been widely cited, yet a real-time cyber attack impact assessment still does not exist today.

Other well known and more complete cyber attack taxonomies include Howard and Longstaff⁵ and Mirkovic and Reiher.⁶ Howard and Longstaff⁵ present a taxonomy that provides a timeline and structure of different attack types. They state that attackers use specific tools in order to exploit a certain vulnerability. Once the

For further inquiry, send correspondence to S. Jay Yang (E-mail: jay.yang@rit.edu, Telephone: 1 585 475 6434).

vulnerability is exploited, the attackers use it to perform an action on a specified target in order to attain an unauthorized result, and finally complete their objective. The entire process from start to finish is classified as an incident. Executing a specific action on a target is referred to as the event, and from using the tool until the attacker gets the unauthorized result is specified as the attack. This list of actions and unauthorized results can potentially be used to categorize, at the highest level, the network attack techniques, and the consequences of a successful attack. The objectives of the overall incident are at a much higher level than impact assessment will actually assess. Each of the elements in both the attack technique and consequence groups can be divided into smaller partitions based on particular attacks. For example, Mirkovic and Reiher⁶ delve into Distributed Denial of Service (DDoS) attacks. Their taxonomy specifies possible ways a DDoS attack can be executed, and the different results that it can have. It shows that a DDoS attack can be classified by the degree of automation, how it exploits the weakness, source address validity, attack rate, and persistence of agent set. The results of a DDoS attack can be classified by victim type and impact on the victim. For instance, a DDoS attack may affect only a host, or possibly the entire network. The way it affects the host may be degrading, in which it uses up parts of its victim's resources, or flat out disruptive, in which recoverability levels differ. Recovery levels should be an important characteristic to look at when determining the impact. These taxonomies are great reference models, but do not provide a mapping at the intrusion alert level, which is needed for impact assessment at a much smaller time scale.

Examining the problem from a different perspective leads to the review of work on vulnerability trees and attack graphs. Vidalis and Jones⁷ proposed the use of a vulnerability tree to identify the types of attacks an attacker could perform to accomplish a goal. Their model requires a separate vulnerability tree for each possible goal, which could be potentially numerous. Philips and Swiler⁸ suggested the use of a Bayesian network to model the vulnerabilities for risk analysis. Their model assumes acyclic graphs, which implies that bi-directional connections between hosts must be modeled in separate acyclic graphs. Massicotte, Couture, Briand, and Labiche⁹ discussed ways of introducing contextual information to cross examine with reported IDS alerts and, thus, reduce false positives. Their experiences suggested that contextual information may be derived by utilizing Snort,¹⁰ Nessus,¹¹ and Bugtraq.¹² They also suggest that a network be modeled as objects because network components are inherently modular and each component has sub-components that follow the same behavior. Our virtual terrain model, developed independently of Massicotte's work, shares some similar ideas, yet provides additional network connectivity, user, privilege, and asset criticality information for impact assessment.

'Impact assessment' is proposed to be part of the alert correlation process as suggested by Valeur, Vigna, Kruegel, and Kemmerer.¹³ They use the impact analysis component to, "determine the impact of the detected attacks on the operation of the network being monitored and on the assets that are targeted by the malicious activity." The following information sets are used: a service asset database, service heartbeat monitors, service dependencies, and service importance with respect to the overall network. The heartbeat of each monitored service is associated with observed attack actions based on explicit dependency definitions.

Porras, Fong, and Valdes¹⁴ discuss M-Correlator, a mission-impact-based approach for alert prioritization and aggregation. They mention the problem of merging and analyzing alert information from the growing number of network monitoring devices. Given the topology and mission of a network, M-Correlator's goal is to rank and consolidate incoming alerts based on the degree of threat they pose to the network. They make use of topology vetting, priority mapping, and incident ranking to assess the impact these alerts can have on the network mission and the probability of them being successful. The priority component takes into account the mission of the network by specifying critical incident types and critical computing and data assets, services, and administrative or untrusted user accounts. Porras, *et al.*, use a classification system for alerts, which can be ranked with interest levels specified by an analyst.

Our work is parallel to Valeur, *et al.*'s work and Porras, *et al.*'s work, but with an emphasis on determining the impact of correlated attacks on network assets, services, operations, missions, and users. We propose the use of virtual terrain which contains hierarchical dependency definitions, so that CVSS scores can be readily used and no explicit dependency needs to be defined between an alert to a seemingly unrelated service. Information about the network configurations, assets importance, etc. is without a doubt needed for impact assessment; our contribution lies in the formal, organized, and efficient methodology for this challenging task.

2. VIRTUAL TERRAIN ASSISTED CYBER IMPACT ASSESSMENT

2.1 Preliminaries

Let H , S , U , and N be the set of hosts, services, users, and subnets (including the entire network), respectively. The set of hosts include individual hosts, routers, servers, host clusters and server farms. A single entity is defined in virtual terrain (VT)* for a set of hosts or servers if they are configured identically and with the same access privileges. The set S contains the *types* of services offered in the entire network. An enterprise network typically offers the same type of services, e.g., FTP or SMTP, in different subnets. The different service instances are denoted as $r \in R$. If there is exactly one instance for each service type, then $R \equiv S$. For any pair of sets X and Y , the notation $X(y)$ denotes a subset of X deduced with $y \in Y$. For example, $R(h)$ means the set of service instances offered in the host node h , $S(r)$ deduces the service type of the service instance r , $N(h)$ returns the subnet where h resides, and $U(h)$ determines the set of users who have access to h . The associations between different elements in different sets is defined in the VT with directional arcs.

Each host node $h \in H$ contains a set of service instances $R(h)$, and each service instance $r \in R(h)$ contains a set of exposures $E(r)$. The exposures are the vulnerabilities of the corresponding service and shall match to IDS alerts in VT. The mapping is done by referring to Nessus¹¹ scans, Common Vulnerabilities and Exposures (CVE) dictionary,¹⁶ and IDSs. For work reported in this paper, we consider only a subset of Snort¹⁰ alerts. In addition, each host nodes may contain an *allowed* or *denied* list, which will be referred to as the firewall list for convenience. This firewall list may contains IPs, port numbers, and/or protocols, and will be particularly comprehensive if the host node is a router. The physical connectivity of host nodes are defined in VT, and the firewall rules are checked against the attributes in IDS alerts to determine the logical connectivity.

Based on the above definitions, the following subsections define the impact scores for the hosts (I_H), the services (I_S), the users (I_U), and the subnets or the entire network (I_N). In the absence of absolute definition of ‘impact,’ all impact scores are defined with respect to the total loss of the entity being assessed, and are normalized to a value between 0 and 1. A weight or criticality of each sub-component with respect to an entity, therefore, is defined.

2.2 Impact Scores

Host Impact: *The potential damage done to a host with respect to its services and their importance to the host.*

The impact to a host $h \in H$ depends on the services running and the asserted exposures, $E^*(r, t)$, of each service r due to the attack actions observed up to time t . For each service instance $r \in R(h)$ on the host h , the asserted exposure scores, α_e , $e \in E^*(r, t)$, can be derived based on CVSS² and normalized in $[0, 1]$. The maximum of the asserted exposure scores is defined to be α_r , representing the maximum damage imposed to the service instance r .

$$\alpha_r = \max_{e \in E^*(r, t)} (\alpha_e) \quad (1)$$

The impact score for a host is the average of α_r scores weighted by the respective service criticality ($c(r, h)$). Note that $c(r, h)$ is defined to represent the importance of the service instance r to its host h .

$$I_H(h) = \frac{\sum_{r \in R(h)} c(r, h) \cdot \alpha_r}{\sum_{r \in R(h)} c(r, h)}; \quad (2)$$

Service Impact: *How potentially compromised a particular service is across the entire network.*

To calculate the impact score for a service type $s \in S$, every instance of a given service running in different hosts on the network is analyzed. For each instance $r : S(r) = s$, the same rule is used as in (1) to get α_r . Similar to the definition of I_H , I_S is a weighted average of α_r but with weights $c(r, s)$, which represents the criticality of the service instance r to the overall service s .

$$I_S(s) = \frac{\sum_{r \in R(s)} c(r, s) \cdot \alpha_r}{\sum_{r \in R(s)} c(r, s)}; \quad (3)$$

*Only a brief discussion on VT is provided in this paper. The readers may refer to Holsopple *et al.*¹⁵ for a detailed discussion on VT.

User Impact: *The potential effect to each user's use of the hosts under attack.*

There are different interpretations in assessing cyber attacks to users. One interpretation is to assess whether a user privilege on different machines has been compromised. This, however, requires host-based IDS to report privilege information on attack actions. Accurately reporting this information is not as easy as it seems and this work does not utilize such information. Alternatively, user impact can be thought as the level of confidence a user can still use the machines he or she has accounts on. In realizing this notion, $I_U(u)$ is defined as a weighted average of $I_H(h)$ for $h \in H(u)$ with weights $c(h, u)$.

$$I_U(u) = \frac{\sum_{h \in H(u)} (c(h, u) \cdot I_H(h))}{\sum_{h \in H(u)} c(h, u)}; \quad (4)$$

Network Impact: *The potential damage on a subnet or the entire network.*

The network impact score will allow an analyst to monitor the health of a subset or of the entire network. Intuitively, the calculation may be an aggregation of I_H , I_S , or I_U within the subset or the entire network. Consider the target $n \in N$ and a set of weights with respect to this target. The impact score $I_N(n)$ can be defined as follows for $X = H, S, U$.

$$I_N(n) = \frac{\sum_{x \in X(n)} (c(x, n) \cdot I_X(x))}{\sum_{x \in X(n)} c(x, n)}; \quad (5)$$

All of the impact scores can be determined for one or many attack tracks. This allows for a ranking of attack tracks in terms of their impact to different parts of the network. In fact, network analysts may focus on the most affected part of the network (e.g., subnet, services, or users) and trace the multistage attacks that cause the damage.

2.3 Logical and Illogical Attacks

In determining the impact scores, VTAC does more than blindly processing the incoming correlated alerts. Since alerts are grouped with others that potentially belong to the same sequence of multistage attack, VTAC can determine whether a step is 'illogical' based on the prior steps in the same sequence and the attributes defined in VT, such as the firewall rules. An attack step is illogical if the corresponding alert contains conflicting attributes to the VT definition. There are a few possible reasons for illogical steps: (1) the alert is a false positive, (2) the VT definition is wrong or not updated, (3) there are coordinated attacks or wrongly correlated alerts, and (4) it is a new attack and wrongly categorized to a known alert message. Determining the root cause for the problem is out of the scope of this paper. VTAC will merely identify the illogical steps and leave it to the analysts to determine whether to process these steps in determining the impact scores. Figure 1 shows the algorithm VTAC uses to determine the illogical steps.

3. TEST NETWORK ILLUSTRATED

To examine and validate the performance of the virtual terrain and impact assessment algorithms, a test network is created. Ideally, this network would represent a real-world enterprise network. Valeur, Vigna, Kruegel, and Kemmerer¹³ discuss that there is a lack of example networks with full configurations needed to provide impact assessment. They also mention the lack of attack data for evaluating impact assessment systems. After thorough discussions with network security specialists and IT personnel, a mock network was created and configured to the best of our knowledge. Attack scenarios are created from IDS alerts to simulate different types of attacks. These scenarios are assumed to be output from an alert correlator such as INFERD.^{17, 18}

```

Boolean logicalAttack = false;
List validAttackPorts = {};
PortInfo givenPort = port/protocol from alert;
List<PortInfo> exposurePorts = {};

if ( dst exists && dst.hasExposure(alertSig) ) {
  if ( !givenPort.isEmpty() ) {
    validAttackPorts = givenPort ∩ exposure.getPorts();
  } else {
    validAttackPorts = exposure.getPorts();
  }

  validAttackPorts = validAttackPorts ∩ (ports ∉ dst.getBannedList(src));

  path = spanningTree(src, dst);
  pathRules = getFirewallRules( path );

  validAttackPorts = validAttackPorts ∩ pathRules;

  if ( !validAttackPorts.isEmpty() ) {
    logicalAttack = true;
  }
}

```

Figure 1. Pseudo-code for determining logical vs. illogical attack steps.

3.1 Network Configuration

Figure 2 shows the terrain information associated with the test network. It was designed using a layered network approach, with each successive layer capable of having choke points to restrict traffic flow. Typically on a layered network, traffic is limited flowing down the network, but is free to travel up the network. By creating servers or demilitarized zone (DMZ) subnets ‘out-of-band,’ it prevents traffic that is flowing up and out of the network from accessing the servers. Each router has been configured for specific traffic flow patterns on a neighbor-to-neighbor basis. Services running on each machine were taken into consideration for the configuration.

The 192.168.1.X subnet provides public services to external users, which include an external web server, a mail server, and an FTP server. Subnet 192.168.3.X includes all of the internal services, including an internal web server, an SQL server, a domain controller, and a file server. The internal web server is one that can be accessed network wide and functions as this network’s intranet. The centralized domain controller is the point of authentication for most of the network, and the main file server serves as a data repository for some of the departments. Each server has at least some of the necessary remote services running on the machine required to provide that service. Figure 2 shows the users, including administrators, next to the departments or servers they have access to.

There are four departments in the network. Each of them has a different configuration and plays a unique role. Table 1 summarizes the key service accessibility of each department. Each department contains a cluster of workstations, which may or may not have access to the centralized domain controller and file server. Among the four, Department C is relatively tightly secured with its own internal file server and domain controller, so there is no need for file or authentication traffic to be allowed through to its department. On the contrary, Department D is relatively less secured, since it requires access to and from the main domain controller and file server, thus permitting file and authentication traffic. Department B, though has its own file server, also allow access from both main servers, while Department A only permit traffic from the main domain server. The firewall settings in routers and servers are configured accordingly.

Figure 2. Test network showing machine services and user accounts

Department	Authentication		File System		Other Access			
	Main	Internal	Main	Internal	Mail	FTP	Int. Web	Internet
A	✓	-	-	✓	✓	✓	✓	✓
B	✓	-	✓	✓	✓	✓	✓	✓
C	-	✓	-	✓	✓	-	✓	✓
D	✓	-	✓	-	✓	✓	✓	✓

Table 1. Summary of department configurations.

3.2 Populating the VT Model

The test network created does not physically exist, therefore, Nessus, NMap, or other scanners could not be used. The network characteristics were manually entered into the virtual terrain schema. The machine, service, and account criticality values along with the exposure damage values were arbitrarily assigned. Values were decided in a reasonable manner with respect to the mission of network infrastructure. For example, servers are generally given higher values of $c(h, \text{entire-net})$ because they play a more important role to the overall network. Depending on the type of service and its location (main or department specific server), the criticality could also be affected. Service criticality values ($c(r, h)$) were determined by the importance of the service is to each respective machine. The FTP service is obviously more important to an FTP server than a telnet or remote media service on the server. The criticality of machines to normal users ($c(h, u)$) were determined based on the values given in Table 2. The $c(h, u)$ values for Administrators are similar to that for the normal user, except that a high criticality is assigned for the machines that the administrator is directly responsible for.

Machine Type	$c(h, u)$ for normal users
Domain Controller	0.8
File Server	0.5
FTP Server	0.1
Mail Server	0.3
Workstation	1.0

Table 2. The values used for $c(h, u)$ for normal users u .

At the time of this work, the CVSS scores were not available for all the service vulnerabilities defined in the test network. Thus, exposure scores (α_e) were populated with respect to the type of attack they are associated with. Table 3 shows the damage scores assigned to each exposure according to its type. Notice that the impact score definitions from Section 2.2 do not take into account privilege level. The fact that exposure scores differs according to privilege levels shall help differentiate the threat posed due to access gained by the attacker.

Type of Attack	Exposure Score (α_e)
Reconnaissance	0
User Level Intrusion	4
System Level Intrusion	7
Privilege Escalation	7
Goal (e.g., backdoor, DoS)	10
Miscellaneous	1

Table 3. Summary of populating exposure damage scores

4. RESULTS AND DISCUSSION

Using the test network discussed in Section 3, a set of scenarios are tested to examine the uses of the proposed impact assessment framework. Due to length constraints, three attack scenarios are discussed in this section to demonstrate how VTAC would perform (1) when processing illogical versus logical attack steps, (2) under different department configurations, and (3) in the presence of insider attacks.

4.1 Logical vs. Illogical Attacks

The first scenario shown in this paper was created to experiment with illogical attack steps. This scenario was run twice, first not allowing illogical steps to be processed and a second one allowing them to be. Table 4 shows the attack steps with Steps 9-12 being the illogical ones.

This attack scenario starts with exploiting the external web server and then attempts to gain access to the internal server domain. Once obtaining access to the main DC, the attack continues to attack Department C's servers. Department C's configuration does not allow these servers to be accessed from outside of the department, thus they are labeled illogical. After this, Department C's servers become stepping stones to allow the attack propagate further into the network. Note that this is indicative that Steps 9-12, though illogical, could actually be true positives. Following these attacks, the attacker returns to the internal web server and continues to exploit other areas of the network.

Figures 3 and 4 shows the I_H scores for different machines in the entire network with the illogical steps not processed and processed, respectively. Notice that there are no changes in I_H 's for Department C's domain controller and file server when Steps 9-12 are not processed and they elevate when the illogical steps are processed. This verifies that VTAC can automatically distinguish illogical steps from logical ones and process them if users elect to do so. Because these illogical steps are likely to be true positives (unless missing/wrong alerts or wrong alert correlations), processing them to determine the true impact scores at the later stage is important. Comparing Figures 3 and 4 shows no difference in I_H 's after Steps 9-12. This is because the other machines attacked after that do not reside in Department C. Other impact scores may be affected even after Steps 9-12. For example, both the NetBIOS service and the entire network impact scores are affected as shown in Figure 5.

Figure 3. Host impact scores for Scenario 3, illogical attack not processed.

Figure 4. Host impact scores for scenario 3, illogical attack processed.

Figure 5. Impact scores for NetBIOS service and the entire network with and without processing illogical steps.

Step	Description	Source IP	Dest IP	P#/Pro	Alert Signature
1	Scan Ext. Web Server	140.203.195.48	192.168.1.2	80/tcp	WEB-MISC http directory traversal
2	Attack Ext. Web Server	140.203.195.48	192.168.1.2	80/tcp	WEB-IIS .asa HTTP hdr buf overflow att.
3	Scan FTP Server	192.168.1.2	192.168.1.4	21/tcp	FTP adm scan
4	Attack FTP Server	192.168.1.2	192.168.1.4	21/tcp	FTP ADMw0rm ftp login attempt
5	Compromise Int. Web Server	192.168.1.2	192.168.3.3	80/tcp	WEB-IIS .asa HTTP hdr buf overflow att.
6	Get info about Main DC	192.168.3.3	192.168.3.2	/	DNS named version attempt
7	Attack Main DC	192.168.3.3	192.168.3.2	/	DNS EXPLOIT named overflow attempt
8	Attack Main DC Again	192.168.3.3	192.168.3.2	/	RPC status GHBN format string attack
9*	Recon on Dep-C DC	192.168.3.3	192.168.30.2	/	DNS zone transfer TCP
10*	Attack Dep-C DC	192.168.3.3	192.168.30.2	/	DNS EXPLOIT named 8.2-to-8.21
11*	Access Dep-C File Server	192.168.3.3	192.168.30.3	/	NETBIOS SMB ADMIN\$access
12*	Attack Dep-C File Server	192.168.3.3	192.168.30.3	/	NETBIOS DOS RFPoison
13	Attack Dep-C Cluster	192.168.30.3	192.168.31.100	/	DOS Real Audio Server
14	Attack Dep-B Cluster SSH	192.168.30.2	192.168.20.100	/	SCAN SSH Version map attempt
15	Attack Dep-B Cluster SSH	192.168.30.2	192.168.20.100	/	EXPLOIT ssh CRC32 overflow
16	Scan Dep-B File Server	192.168.20.100	192.168.20.2	/	NETBIOS SMB Strup Flder access att.
17	Gain access Dep-B File Server	192.168.20.100	192.168.20.2	/	NETBIOS SMB C\$ access
18	Attack Dep-B File Server	192.168.20.100	192.168.20.2	/	NETBIOS DOS RFPoison
19	Attack Dep-B File Server	192.168.3.3	192.168.20.2	/	NETBIOS DOS RFPoison
20	Scan SSH on Dep-A Cluster	192.168.20.2	192.168.11.100	/	SCAN SSH Version map attempt
21	Attack Dep-A Cluster SSH	192.168.20.2	192.168.11.100	/	EXPLOIT ssh CRC32 overflow
22	Attack Dep-A File Server	192.168.11.100	192.168.10.2	/	NETBIOS DOS RFPoison

Table 4. Attack Scenario 1: Logical vs. Illogical (steps with *).

4.2 Identical Attack Sequence on Individual Departments

This scenario was created to demonstrate how different subnet configurations can affect impact scores given the same sequence of attack actions. The same attack actions, as shown in Table 5, are executed four times but with steps 15-17 targeting on different department clusters. Table 5 shows the attack actions targeted for Department A. Each of the four departments' clusters is setup with the same telnet service to be exploited.

Step	Description	Source IP	Dest IP	P#/Pro	Alert Signature
1	Scan Ext. Web Server	140.203.195.48	192.168.1.2	80/tcp	WEB-MISC http directory traversal
2	Attack Ext. Web Server	140.203.195.48	192.168.1.2	80/tcp	WEB-IIS .asa HTTP hdr buf overflow att.
3	Attack Mail Server (POP3)	192.168.1.2	192.168.1.3	110/tcp	POP3 USER overflow attempt
4	Attack Mail Server (SMTP)	192.168.1.2	192.168.1.3	25/tcp	SMTP RCPT TO overflow
5	Attack Mail Server (SMTP)	192.168.1.2	192.168.1.3	25/tcp	SMTP exchange mime DOS
6	Scan FTP Server	192.168.1.2	192.168.1.4	21/tcp	FTP adm scan
7	Attack FTP Server	192.168.1.2	192.168.1.4	21/tcp	FTP ADMw0rm ftp login attempt
8	Compromise Int. Web Server	192.168.1.2	192.168.3.3	80/tcp	WEB-IIS .asa HTTP hdr buf overflow att.
9	Get info about Main DC	192.168.3.3	192.168.3.2	/	DNS named version attempt
10	Attack Main DC	192.168.3.3	192.168.3.2	/	DNS EXPLOIT named overflow attempt
11	Attack Main DC Again	192.168.3.3	192.168.3.2	/	RPC status GHBN format string attack
12	Attack Main File Server	192.168.3.3	192.168.3.4	445/tcp	NETBIOS nimda RICHERD20.DLL
13	Attack Main File Server	192.168.3.3	192.168.3.4	445/tcp	NETBIOS SMB trans2open buf overflow att.
14	Attack Main File Server	192.168.3.3	192.168.3.4	445/tcp	NETBIOS DOS RFPoison
15	Attack Dep-A Cluster	192.168.3.3	192.168.11.102	23/tcp	WEB-MISC telnet attempt
16	Attack Dep-A Cluster	192.168.3.3	192.168.11.102	23/tcp	TELNET EZsetup account attempt
17	Attack Dep-A Cluster	192.168.3.3	192.168.11.102	23/tcp	TELNET bsd telnet exploit response

Table 5. Attack Scenario 2: Departmental Attacks.

Figure 6 shows the I_N for each department as the almost-identical attack sequence is executed for it. Departments A, B, and D all have similar impact scores and patterns, while Department C experiences the least impact when it gets to the later stage of the multistage attack. Department C sees least impact because it uses its own authentication and file servers and does not allow access from the FTP server. Therefore, attacks on the FTP server, main file server, and main DC do not affect Department C. Also, although Department C has the telnet service on its cluster, the attack is illogical, because the router does not permit telnet traffic to pass through from the internal servers domain. The impact scores are slightly different among Departments A, B, and D, depending on the servers they allow access. When the main file server is attacked (steps 12-14), Department B and D's impact scores change, but Department A's does not. This is because Department A does not permit traffic from the main file server. Overall, Department D sees highest impact as expected.

This experiment demonstrates that VTAC allows to differentiate cyber attack's impact to subnets with different configurations. This can be used as an online tool for analysts to focus on high impact attacks and departments, as well as an offline tool to analyze individual department configurations.

Figure 6. Individual department impact scores for Department Attacks.

4.3 Insider Attacks

This experiment concerns attack sequences originated from internal machines. These attacks may be executed by disgruntled employees, employees coerced into helping a hacker, a hacker physically gaining access to an inside machine, or possibly from an employee snooping around or showing off their hacking capabilities. Table 6 shows the progression of an insider attack originated from the host cluster in Department C.

Step	Description	Source IP	Dest IP	P#/Pro	Alert Signature
1	Attack Dep-C DC	192.168.31.104	192.168.30.2	53/tcp	DNS named version attempt
2	Attack Dep-C DC	192.168.31.104	192.168.30.2	53/tcp	DNS EXPLOIT named overflow attempt
3	Attack Dep-C File Server	192.168.31.104	192.168.30.3	139/tcp	NETBIOS SMB C\$ access
4	Attack Dep-C File Server	192.168.31.104	192.168.30.3	139/tcp	NETBIOS SMB ADMIN\$access
5	Attack Dep-B Cluster	192.168.31.104	192.168.20.102	22/tcp	SCAN SSH Version map attempt
6	Attack Dep-B Cluster	192.168.31.104	192.168.20.102	22/tcp	ATTACK-RESPONSE success gobbles ssh explt
7	Attack Main DC	192.168.20.102	192.168.3.2	135/tcp	RPC mountd TCP exportall request
8	Attack Main DC	192.168.20.102	192.168.3.2	53/tcp	DNS EXPLOIT named 8.2-to-8.21

Table 6. Attack Scenario 3: Insider Attack.

Figures 7 and 8 show the impact scores for all the hosts and users in the entire network. A few signs can be noticed to indicate about the insider attack. Note that the first few attack steps exhibit an unusual pattern in I_H 's and I_U 's. First, the first affected machines are internal to a department instead of the external or internal servers - see Figure 7. Second, the global Administrator's I_U does not spike while Admin-C's elevates - see Figure 8. Obviously the $I_N(\text{Dep-C})$ will show an elevated score - not shown in this paper due to space limitations.

Also notice Steps 5-8 in this insider attack scenario. The attack expands beyond Department C and reaches Department B and then the main servers. Notice that the user Kate has access to both Departments C and B, and, thus, the main servers. The fact that the impact scores rise first within Department C (a very secured subnet), then those in Department B, followed by the main servers, hints that Kate or Kate's account could be the one initiating the insider attack. Observing the patterns of impact scores generated by VTAC can be also indicative to and help trace insider attacks.

5. CONCLUSION AND FUTURE WORK

This work addresses the need for an efficient and real-time impact assessment system for cyber attacks. VTAC utilizes a graph-based virtual terrain model to assess correlated attack's impact to hosts, services, users, and subnets in a network. A scoring scheme is developed to determine the relative damage caused by the attacks to the different entities in the network. The scoring scheme goes beyond assessing individual hosts and based on individual alerts. VTAC provides analysts various views of the attacked network and examines the situation on a per correlated attack track basis. A test network with sufficient configuration information is developed along

Figure 7. Host impact scores for Insider Attack.

Figure 8. User impact scores for Insider Attack.

with numerous attack scenarios. A subset of the scenarios are presented. The demonstrated results show that VTAC is capable of processing illogical steps, analyzing impact to different departments with varying levels of security configurations, and identifying and tracing insider attacks. The developed framework and tool will be essential for timely response to cyber attacks. Future work includes incorporating cross-examination of impact caused by different attack tracks. Other scoring schemes will be developed and analyzed. Finally, populating virtual terrain information automatically as much as possible will be crucial to achieving the full potential of VTAC.

ACKNOWLEDGMENTS

The authors would like to thank Jared Holsopple of CUBRC for providing valuable input to the design of VTAC, and Jon Claudius and Stephen Byers for their expert insight into network configurations. This work is funded through the National Center for Multisource Information Fusion (NCMIF) grant under the technical supervision of AFRL/IFEA.

REFERENCES

1. T. Bass, "Intrusion detection systems and multisensor data fusion," *Communications of the ACM* **43**, April 2000.
2. Forum of Incident Response and Security Teams (FIRST), "A complete guide to the common vulnerability scoring system." <http://www.first.org/cvss/cvss-guide.html>, 2007.
3. U. Lindqvist and E. Jonsson, "How to systematically classify computer security intrusions," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 154–163, (Oakland, CA, USA), 1997.
4. P. G. Neumann and D. B. Parker, "A summary of computer misuse techniques," in *Proceedings of the 12th National Computer Security Conference*, pp. 396–407, (Baltimore, Maryland, USA), Oct. 10-13 1989.
5. J. Howard and T. Longstaff, "A common language for computer security incidents," 1998.
6. J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *Computer Communication Review* **34**(2), pp. 39–53, 2004.
7. S. Vidalis and A. Jones, "Using vulnerability trees for decision making in threat assessment," tech. rep., University of Glamorgan, School of Computing, Wales, UK, June 2003.
8. C. Phillips and L. P. Swiler, "A graph-based system for network-vulnerability analysis," in *Proceedings of the 1998 workshop for new security paradigms*, pp. 71 – 79, (New York, NY, USA), 1998.
9. F. Massicotte, M. Couture, L. Briand, and Y. Labiche, "Context-based intrusion detection using snort, nessus and bugtraq databases," in *Proceedings of the Third Annual Conference on Privacy, Security and Trust*, (Fredericton), October 2005.
10. Sourcefire, "Snort: an open source network intrusion prevention and detection system." <http://www.snort.org>, 2007.
11. T. N. S. Inc., "Nessus vulnerability scanner." <http://www.nessus.org/>, 2007.
12. S. Focus, "Bugtraq vulnerability database." <http://www.securityfocus.org/bid>, 2006.
13. F. Valeur, G. Vigna, C. Kruegel, and R. A. Kemmerer, "A comprehensive approach to intrusion detection alert correlation," *IEEE Transactions on Dependable and Secure Computing* **1**, pp. 146 – 169, July-Sep 2004.
14. P. Porras, M. Fong, and A. Valdes, "A mission-impact-based approach to infosec alarm correlation," in *Recent Advances in Intrusion Detection. 5th International Symposium, RAID 2002. Proceedings (Lecture Notes in Computer Science Vo.2516)*, pp. 95 – 114, (Zurich, Switzerland), 2002.
15. J. Holsopple, B. Argauer, and S. J. Yang, "Virtual terrain: a common representation of a computer network," in *Proceedings of SPIE, Defense and Security Symposium*, March 2008.
16. Mitre, "Common vulnerabilities and exposures (CVE dictionary)." <http://cve.mitre.org>, 2007.
17. M. Sudit, A. Stotz, and M. Holender, "Situational awareness of a coordinated cyber attack," in *Proceedings of SPIE, Defense and Security Symposium*, pp. 114–129, March 2005.
18. M. Sudit, A. Stotz, M. Holender, W. Tagliaferri, and K. Canarelli, "Measuring situation awareness and resolving inherent high-level fusion obstacles," in *Proceedings of SPIE, Defense and Security Symposium*, **6242**, April 2006.