Security Visualization: Cyber Security Storm Map and Event Correlation

Denise Ferebee
Computer Science
University of Memphis
Memphis, TN 38152
dferebee@memphis.edu

Dipankar Dasgupta
Computer Science
University of Memphis
Memphis, TN 38152
dasgupta@memphis.edu

Michael Scmidt
Art
University of Memphis
Memphis, TN 38152
mschmidt@memphis.edu

Qishi Wu
Computer Science
University of Memphis
Memphis, TN 38152
qishiwu@memphis.edu

***Abstract*— Efficient visualization of cyber incidents is the key in securing increasing complex information infrastructure. Extrapolating security-related information from data from multiple sources can be a daunting task for organizations to maintain safe and secure operating environment. However, meaningful visualizations can significantly improve decision-making quality and help security administrators in taking rapid response. The purpose of this work is to explore this possibility by building on previously gained knowledge and understanding of weather maps used in meteorology, assessing the gaps, and applying various techniques and matrices to quantify the impacts of cyber incidences in an efficient way.**

Keywords-information visualization; cyber security; event correlation; random matrix theory

I. Introduction

Electronic devices from eReaders, to smartphones like the iPhone [1], are now peppering our lives. Each device is either connected via wi-fi or a cellular connection. These new devices require methods to monitor and handle security breaches. These breaches generally cause large amounts of data to be collected. In an area of technology where time is of the essence, this is a hindrance to the impact analysis of the breach/event.

Once data is collected and analyzed, it is typically shared between business/government organizations for further impact studies. These organizations make decisions in reference to legal, financial, and operating requirements. Thus, the information has to be consumable by a diverse audience. This audience's decisions affect many services that companies and government organizations provide. Because much of the data is at a device level, this adds another hindrance to the impact analysis of the breach/event. Many of the consumers of the data do not want to know that a server was down for hours because of a virus. They want to know how does this affect their e-commerce applications, organizational brand, legal implications, and financial bottom line. Thus, they need to understand how these services are affected by a server's inaccessibility.

Many organizations are global and services reside in multiple locations and security information consumers need to understand how these locations are affected by a breach/event. Global locations can affect each other thus leading to a need to correlate breaches/events between them.

There are a number of factors in determining the impact of a security breach/event. They consist of the following:

- Large data volume from security mechanism
- Time and specialized skills needed to analyze the data
- Abstracting the data for general information consumption
- Teamwork (i.e. coordination, cooperation, requirement sharing, etc.) between Information Technology and Business organizations
- Correlating the breaches/events to temporally and spatially at a service level

For the purposes of this document, we will cover two major areas: providing the data in a multi-audience consumable manner via security visualization, and an event correlation that takes into account temporal and spatial aspects in order to correlate the events to business/organization services. The sections of this document will consist of the following: related work, proposed event correlation, proposed visualization, implementation details, and future work.

II. Related Work

In this section will be covered security mechanisms, standards/best practices/guidelines that are used to bridge communication and deal with requirement gathering, visualization aspects, and event correlation.

A. *Security Mechanism*

A statement of what is and is not allowed is a security policy [2]. A method, tool or procedure for enforcing a security policy is a security mechanism [2].

Many security mechanisms protect the changing environments referenced in the introduction section (e.g. firewalls, application/business methods, policies, etc.) [3], [4]. When a compromise occurs, there is a large volume of

Identify applicable sponsor/s here. *(sponsors)*

www.manaraa.com

monitoring data. Granted, there are tools that are able to analyze this data from a specific domain (i.e. switch, server, firewall, mobile device, etc.). Each of these mechanisms has its own logging and alerting methods requiring some form of maintenance by an administrator, developer or security engineer. The main goals of security mechanisms are as follows:

- **Prevention:** the failure of an attack
- **Detection:** determining if an attack is occurring
- **Recovery:** either stopping an attack and assessing and repairing the damage or continuing to function normally even though an attack is underway [3], [4]

Security mechanisms alone cannot adequately determine the extent of the impact of a security breach because Information Security involves more than just Information Technology (IT). It also involves "the business". Therefore, the two sides have to continually work together to determine "How well the business is doing". "Well" in this aspect references whether the business is suffering due to a security breach and "how is it suffering". In order to determine the effects of a security breach, the first step is to determine which business organizations and components are involved. Thus, a Business Impact Analysis (BIA) should be performed. The purpose for this is to determine mission-critical business processes, IT processes, and resources that are affected by the breach [1], [5], [6], [7]. Hence, let us explore some of the standards and best practices/guidelines that help to define and support this effort.

B. Standards/Best Practices/Guidelines

What is a standard? Why do we need them? These are a series of questions that must be answered in order to justify their use. Suppose you have two businesses or agencies that need to communicate via TCP. Business A has a fiber backbone and needs to communicate with Business B that communicates via TCP by avian carrier. Hence, communication can be a problem because the two businesses are not using a similar method. Therefore, for the purposes of the this paper, we define "standards" as the a set of techniques that are agreed upon by a group of practitioners as being techniques/methods that bestow the most trust that data and processes are error free. In order to provide the most trust, business organizations and Information Technology (IT) organizations have to work together to determine the impact of a security breach on the business' financial, legal, corporate brand, and procedures.

The following are examples of standards/best practices/guidelines that provide a means of joint roles and responsibilities and impact analysis methods but most of all security requirements:

- Information Technology Infrastructure Library (ITIL): provides an approach for IT service management [8], [9], [10], [11], [12]
- Payment Card Industry Data Security Standard (PCI DSS): provides a standard for maintaining credit card data by a set of core principles and requirements [13], [14]
- International Organization for Standardization (ISO): provides a means for the business and IT to be able to speak the same language and have similar points of reference (e.g. ISO standard for Information Security) [10], [15], [16], [17]
- Business Continuity Management (BCM): defines an organization's processes of dealing with the following: identification and risk mitigation in reference to business disruption, disruptive event response, recovery and restoration of critical business functions after a disruption, and post-mortem analysis for process improvement [18]
- Business Impact Analysis: defines how a company analyzes a security breach through collaboration with IT, legal, finance, and other organizations that have a stake [7], [19], [10], [11]

The procedures and defined requirements introduced in the fore mentioned list provides the basis for the security mechanisms that are needed to ensure trust. Therefore, security requirements and mechanism needs come from both the business and IT. Please refer to Figure 2: Proposed Methodology to show how all of these components fit together.

C. Information Visualization

This section will cover the some basic information visualization methodology and a general overview of some of the current security visualizations. These components can be used in providing consumable information.

1) Visualization Methodology

When it comes to visualization, there are techniques in reference to environment, display, color, lightness, visual attention, patterns, etc. [8]. Before any of these techniques are applied, we first need to understand the user of the visualization and their needs. Thus, we are profiling our users as shown in Figure **1**: Concept Map. First, we need to understand what the current process is for understanding and correlating the data. Next, profile the data, the information need, and the purpose or how the information is used. Finally, we profile the new user profile/process by examining the input data location and context, the workflow (i.e. visualization workflow), user roles and identities, the agenda when the visualization will be used, and the value of the information provided.

The MS-Guidelines, MS-Process, MS-Taxonomy can be beneficial to this process [9]. MS-Guidelines are organized by leveraging the MS-Taxonomy that defines six main classes with-in the multi-sensory design space [9]. These classes include visual display, auditory display, haptic display, spatial metaphors, direct metaphors, and temporal metaphors. Spatial metaphors refer to the concepts of space perception. Direct metaphors refer to how an individual's senses detect information. Temporal metaphors refer the perception of events over time. These concepts are beneficial in helping to profile users by providing base concepts that can be used to capture requirements of how the user will or can interact with the visualized data.

المنارة للاستشارات
www.manaraa.com

In addition, Colin Ware's "Information Visualization Perception for Design" provides a basis for designing visualizations that take into account the cognitive psychology aspect, data characteristics, and suggests types of visualizations and components that enhance the user's experience.

2) Security Visualizations

Current security visualizations consist of but are not limited to the following types: simple charts, histograms, scatter plots, parallel coordinates, maps, treemaps, three-dimensional views, etc. Visualization also has a human factor aspect. Therefore, providing a meaningful visualization requires having a good understanding of the user, the problem, and the information to be conveyed [3], [5].

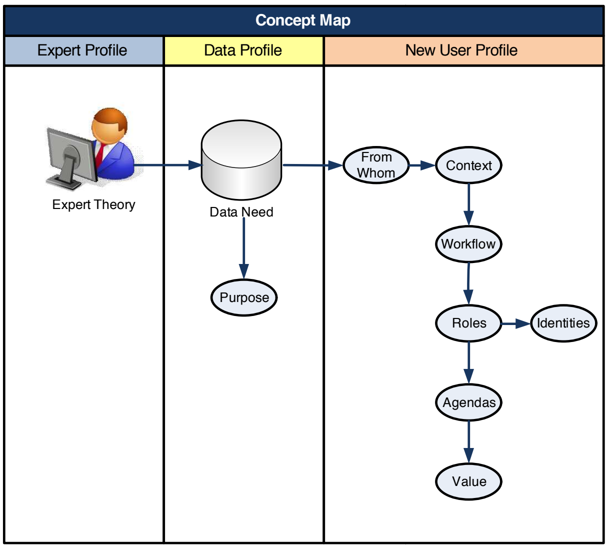


Figure 1: Concept Map

VisAlert is a visualization tool that integrates log and alert files into an intuitive visualization that is a mix between a topology map and concentric circles around the outside similar to a ring chart. This visualization shows alert type by color-coding, a larger node size to show more alerts, and a larger beam indicating persistence [23].

REFLEX is a solution where user, application, source, and destination are visualized using parallel-coordinates in order to show the relationships between the occurring events [24].

D. Event Correlation

Because businesses/organizations offer services, data has to be abstracted from the device level (i.e. firewalls, applications, servers, routers, etc.) to the service level in order to make the information more relevant to the consumer (i.e. business/organization information user). Therefore, this section will cover the device level data, event correlation using Random Matrix Theory (RMT) and vulnerability classification using the Common Vulnerability Scoring System (CVSS).

1) Data

The average security professional or systems administrator looks at many applications in order to understand what is happening at a particular security mechanism. The data can span the following:

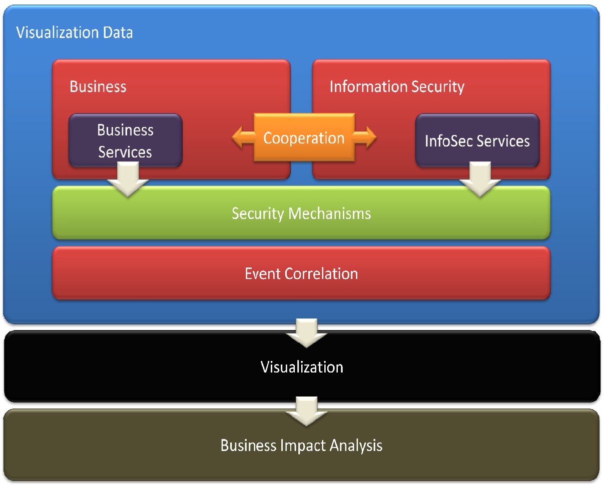
- **System performance:** CPU, memory, disk, network utilization
- **Business rules:** Users with a particular access level get access to particular pieces of data, encryption requirements, and data storage requirements
- **Infrastructure requirements:** firewalls, encryption, routers, switches, etc.
- **Application requirements:** authentication, database access, encryption, and data storage

Because security data comes from a myriad of mechanisms, it takes a considerable amount of time for analysis. In addition, many of the information consumers want/need to understand the big picture. [2], [25]

2) CVSS:

A lot of the guess work is being taken out determining the severity of a vulnerability for a mechanism. This is being done via the CVSS. Vendors of the mechanisms submit a vulnerability alert based on three aspects: a base metric group, temporal metric group, and an environmental metric group [26]. The base metric group captures how a vulnerability is accessed, whether or not extra conditions are needed for exploitation, how it affects an IT device/component and the degree of loss [26]. The temporal metric group captures the exploitability, remediation level, and report confidence changes over time. The environmental metric group captures the characteristics of vulnerability in accordance/association with an IT environment. The metric group consists of collateral damage potential, target distribution, confidentiality requirements, integrity requirements, and availability requirements. The environmental group scoring is completely IT organization subjective and how the organization feels vulnerabilities affect their environment based on their own understanding and domain knowledge [26].

The CVSS provides a common vulnerability classification that many security devices and applications vendors use to characterize an issue. Therefore, this takes some of the legwork out of analyzing device/mechanism level data. This gives us a standard for classifying our security data.



المنارة للاستشارات
www.manaraa.com

Figure 2: Proposed Methodology

3) *Random Matrix Theory*

In previous research, we hypothesized that we could apply the universal properties of RMT to the sensor/security mechanism data of cyber security. The sensor data in this process was based on the number of occurrence (i.e. how many times CPU utilization, network utilization/availability, memory utilization, etc. was over a particular percentage during a period of time). A correlation threshold was determined by constructing a network of profiles using RMT. Next, the correlation matrix was denoised based on the following two characteristics of symmetric matrices [27], [28], [29]:

1. The nearest neighbor spacing distribution (NNSD) of eigenvalues follows Wigner surmise of Gaussian Orthogonal Ensembles (GOE) if a correlation between nearest-neighbor eigenvalues exists
2. The NNSD conforms to a Poisson distribution if there is no such correlation [27], [28], [29].

The transition between the two distributions were used as a threshold to construct an event indicator network where the nodes represent event indicators and the edges represent the correlations between all pairs of indicators with weights equal to correlation coefficients. Then, a correlation network is constructed using the original correlation matrix where the only edges that are kept are the ones that are higher than the threshold. Thus, a graphical representation is produced of a security event under the current security breach [27], [28], [29].

New correlation networks are compared to classified networks stored in a database. The comparison is made of two sets of nodes and edges where the edges are classified in the following manner [27], [28], [29]:

- *Shared Internal (SI):* The subset of internal edges that are shared by both networks such that the vertices also exist in both networks.
- *Non-shared (NS):* The subset of edges that are not shared by are connected to shared nodes
- *Bridging (BR):* The subset of edges that connect shared and non-shared.
- *External (EX):* The subset of edges that connect to nodes in the non-shared edges

Similarity is calculated based on the relationships of the shared internal, non-shared, and bridging edges and nodes.

III. Proposed Event Correlation

One of the major factors not considered in our previous research of event correlation using RMT was location. We are going to work under the premise of business and IT services because this will allow us to abstract the devices up to a service offering (i.e. many devices make up a service). In addition, many companies/organizations reside globally and therefore, their services reside globally. Thus, we must take into a account that service locations and service offerings can affect other locations and offerings.

From our previous work, we observed correlations from security sensor/mechanism indicators. Indicators consisted of memory utilization, CPU utilization, login failures, etc. as referenced in the Related Work section. We have chosen to use CVSS because security device, software, and network device manufactures have standardized their vulnerabilities references in this manner.

The data has been expanded from a matrix *M* to a set of matrices L_n where n is the number of business/organization locations. We reference each location L_n geospatially (i.e. by latitude and longitude). Each row in L_n is a CVSS vulnerability V_i where *I* is the number of different types of vulnerabilities that occurred at a location L_n. Each column in L_n is a time stamp T_j where *J* is the number of time intervals.

We evaluated applying the previous correlation method to the newly expanded data. However, we realized that we would have information loss in reference to location and the correlation of vulnerabilities between locations. In this approach, we will have a set of matrices D_p where *P* is the number of matrices in the set which will be two. D_1 is the matrix where each row is CVSS vulnerability V_i and each column is a time interval T_j. D_2 is the matrix where each row is a CVSS vulnerability V_i and each column is the number of occurrences at a location $L_{n.}$. The purpose of D_2 is to be the basis of a correlation between vulnerabilities and locations (i.e. vulnerabilities occurring at one location can affect other locations and we are using this to capture that information).

Each set of matrices D_p will be used to create two correlation networks $C_{n.}$. The set of networks C_n represents a security event/storm. The correlation matrix C_1 is created based on our original research and will characterize the storm at a location L_n. The correlation matrix C_2 will be created based on our original research. However, it will only be used to determine what other locations might be involved or affecting the current security storm.

IV. Proposed Visualization

In this section, we will cover an overview of the visualization approach. This will entail details of the overall holistic view and application general application features.

A. *Holistic View of Security*

For purposes of this paper, we will define a holistic security view as a view that looks at the business and IT services as a whole. We will not be focusing solely on devices to determine the impact of a security breach, but the services and locations that those devices form in order to provide a top-level view that will provide consumable information for a diverse audience. We propose to use a weather map view.

How will a weather map view provide a holistic view of security events? First, we abstract the network components by service and then by location. Therefore, there is no end-user information overload. A drill-down from location shows each business or IT service that is available at that location. Building on this metadata allows for additional meaning to be added when an event occurs because the security visualization can potentially show the spread of virus propagation, one view may show propagation rate, recovery rate as the patches or

المنارة للاستشارات

www.manaraa.com

antivirus mitigations has started. The main purpose for this visualization is to provide data analysis assistance for decision support purposes (i.e. to show emerging relationships that typically go unnoticed because the data cannot observed as a whole or because of sheer volume).

B. Features

What features will the visualization provide? There will be three views of the data provided: 1) the location view as shown in Figure 3: Location View with Services, 2) the storm map view as shown in Figure 5: Security Storm Map for Example Scenario, and 3) the service view. First is the location view. The location view shows the connected locations and the security vulnerabilities that are occurring. The storm map view will start with a set of physical locations illustrating how each site connects to another site. From each location, the user will be able to drill down and see the business and IT services that are available at that location. This provides a similarity between our security weather/storm map and a meteorological weather map. In a meteorological weather map like Doppler radar icons in reference to high and low fronts, hurricanes and snowstorms are visible and intuitive. Therefore, we would like to take a similar approach with security storms. The collection of icons will be used as a legend to describe the types of security storms. The user will be able to select nodes in order to obtain additional information such as detailed description of the events and severity that are occurring via a popup window.

From the service view, the user is able to see devices that make up the services. They can drill down to see the devices connected to each service and the events that are occurring. This gives the network or security engineer the ability to see which portions of the network are plagued by events and determine based on business need. This additional metadata can be used to narrow down the steps for risk mitigation.

The users will be provided a preferences panel, a security-warning panel, and a security event simulation panel. These components will allow a user to customize their view so that they can see the information relevant for their needs. They will be allowed to turn the icons off and on for various types of events from the view layout. The history form of the preferences panel will allow the users to select a date and time in order to view historical events and see their progression to better understand the event propagation. This feature provides a similar element of a meteorological weather map by showing security storm progression.

V. IMPLEMENTATION DETAILS

In the previous sections, we have discussed ways of creating a security visualization storm map and event correlation. In this section, we will cover how we marry the event correlation with the security visualization.

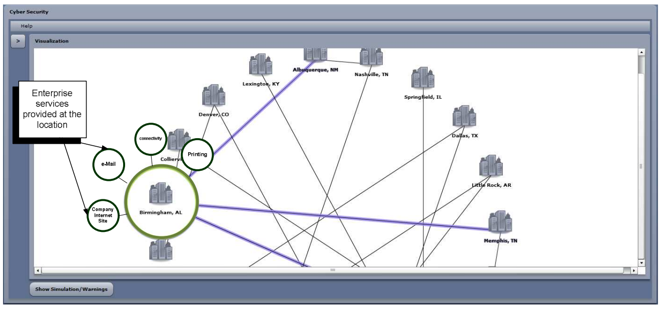
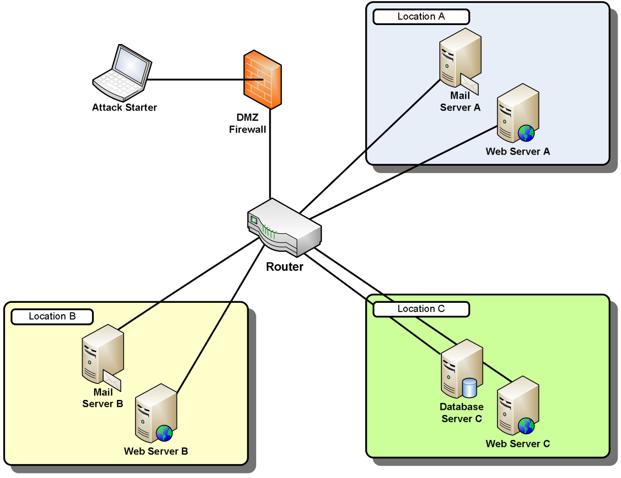

Cyber Security

Figure 3: Location View with Services

To show this marriage of methods, we are going to work through a sample scenario from Advanced Cyber Attack Modeling, Analysis, and Visualization Report (ACAMAV) as a base [30]. In the ACAMAV report, there was one network location and one mail server and one web server. In our example, we have expanded it to 3 locations in order to show the relationship between locations that share business or IT services. The sample scenario network is shown in Figure 4: Sample Scenario Network **Layout**. There will be three server locations Location A as Memphis, TN, Location B as Birmingham, AL, and Location C as Little Rock, AR.



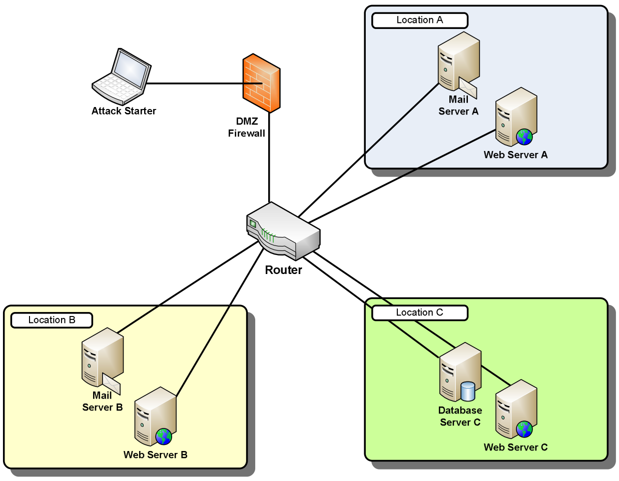


Figure 4: Sample Scenario Network Layout

www.manaraa.com

Web Server A and Web Server B are both running a vulnerable version of Microsoft Internet Information Server (IIS), which is reachable from outside the firewall. Both mail servers A and B are not secured properly. Both Web Server A and Web Server B have the following vulnerabilities [30]:

- CVE-2001-0333 - CVSS v2 Base Score:7.5 [26]
- CVE-2001-0507 - CVSS v2 Base Score:7.2 [26]
- CVE-2000-0884 - CVSS v2 Base Score:7.5 [26]
- CVE-1999-1011 - CVSS v2 Base Score:10.0 [26]

In Figure 5: Security Storm Map for Example Scenario, we show Location A – Memphis, TN and Location B – Birmingham, AL. Each has a cloud the represents that there is a problem. Color defines the level of the event severity. The lightning's colors are defined as the following:

- Yellow – the largest percentage of events have a low CVSS v2 Base Score
- Orange – the largest percentage of events have a medium CVSS v2 Base Score
- Red – the largest percentage of events have a high CVSS v2 Base Score

In our case, all of the vulnerabilities have a high base score. Therefore, the lightning is red inferring that they require immediate attention.

If the largest percentage of event types is split between two groups, we will go with the group with the highest severity. Next, there are lines between locations that have a correlation between the vulnerabilities that are occurring. The line size depicts the amount/number of correlations. In Figure 5: Security Storm Map for Example Scenario, the Memphis and Birmingham locations currently have only four vulnerabilities and they are affecting both locations' services, which is the web hosting services. Based on our initial correlation networks C_n^A and C_n^B for Location A and Location B, we show the correlation of the vulnerabilities between the two areas. At this point, we look at C_1^A and C_1^B which is the correlation network of vulnerabilities in each locations correlation network set. Based on the correlation of vulnerabilities that we have occurring, if the correlated pair exists in both C_2^A and C_2^B, we create the connection line between the locations based on the total number of existing pairs (i.e. the more existing pair the larger the line). This visually shows the degree for which they are connected.

Next, we match the current storm(s) with known storms by comparing them using the correlation network comparison mentioned in Random Matrix Theory section to known storms in the security storm database.

First, we compare the current storm S_c to a known storm S_k by comparing correlation networks C_1 from the matrix set representation of each storm C_n. We calculate the similarity m based on the following measurement:

$$m = \omega_{SI} \cdot \sum_{e \in E_{SI}} (1 - |\rho(e^c) - \rho(e^k)|)$$

$$+ \omega_{BR} \cdot \left(\frac{|E_{BR}^c|}{|E^c|} \sum_{e \in E_{BR}^c} \rho(e) + \frac{|E_{BR}^k|}{|E^k|} \sum_{e \in E_{BR}^k} \rho(e) \right)$$
$$- \omega_{NI} \cdot \left(\frac{|E_{NI}^c|}{|E^c|} \sum_{e \in E_{NI}^c} \rho(e) + \frac{|E_{NI}^k|}{|E^k|} \sum_{e \in E_{NI}^k} \rho(e) \right),$$

Equation 1: Correlation Network Similarity

where ω_{SI} , ω_{BR} , and ω_{NI} are weighted coefficients for three subsets of edges and $|E|$ represents the number of edges in E [27], [28], [29].

The similarity between the current storm S_c to a known storm S_k is defined by Equation 1: Correlation Network Similarity. The first term defines the similarity between the overlapping subgraphs of the storm correlation networks. The second term defines the relationship between the shared and non-shared nodes. If there is a high correlation between nodes, it is considered positive because it shows significance in shared nodes. The third term defines the relationship between the nodes that are only contained in one network, which is considered a negative factor because the nodes do not exists in both networks. Finally, we do not consider the external edge subsets because they do not contain any shared nodes and should not have any significance on the similarity. The purposed for this comparison is to present the user with a list of potential known security storms. Therefore, the user can be presented with a number of security storm characteristics and saved information in relation to risk mitigation.

Now, we will select a location and see the affected services. This is where we use the correlation between vulnerabilities and time to show the relationship of the vulnerabilities between the services. So, if there is a relationship between V_1 and V_2 and V_1 exists in Service A and V_2 exists in Service B, then, there should be a correlation line between the two. The line will be larger depending on the number of correlations that exists between the two services as show in Figure 7: Security Storm Map Drill-down to Service. Finally, we did a drill-down from the service as shown in Figure 8: Security Storm Map - Drill Down to Devices. We continue to use the correlation information here by showing connections between devices. So, if there is a relationship between vulnerability V_1 and V_2 and V_1 exists on a Device A and V_2 exists on Device B there would be a line between the two. The line size would increase based on the number of correlated events that exist between the two as shown in Figure 8: Security Storm Map - Drill Down to Devices. In addition, there is a vulnerability detail bar where the user can scroll through details in reference to the selected device.

There are visualization, correlation, modeling and analysis research that focus solely on the technical as shown Figure 6: Geo-spatial Attack Graph User Interface. As stated in the Related Work section, determining the impact of a security vulnerability or breach requires input from more than IT and security professionals. There are typically financial, legal, procedural factors that are associated thus, requiring information to be consumable across different organizations. It is difficult to explain to someone there is a ssh vulnerability that needs to be fix. Business organizations want to know what it means to them and being able to sale a product or service.

المنـــارة للاستشارات
www.manaraa.com

They do understand the concept of not being able to provide a business service and the loss (i.e. financial, etc.) associated. Therefore, the purpose for abstracting vulnerabilities up to the business service level via a geospatial reference allows the other organizations to assess how it will influence their organizations (i.e. sales, finance, legal, etc.).

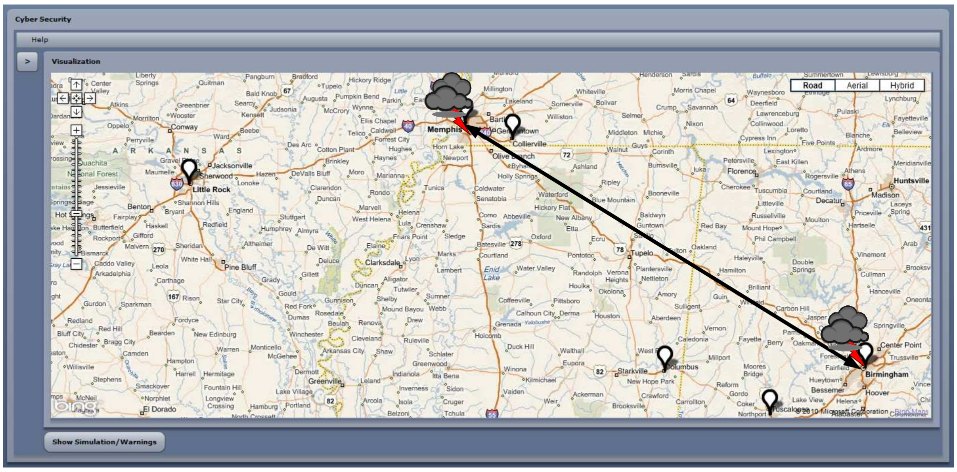


Figure 5: Security Storm Map for Example Scenario

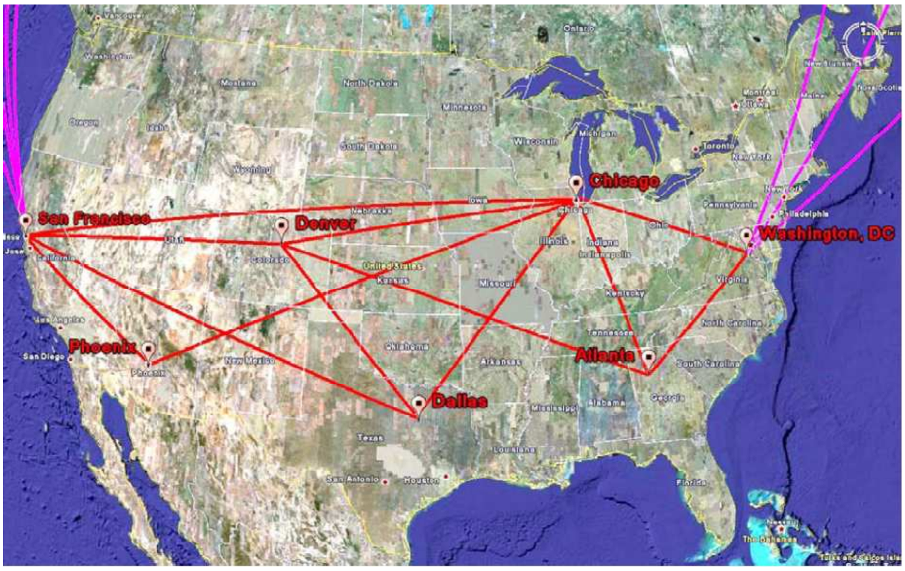


Figure 6: Geo-spatial Attack Graph User Interface **[30]**

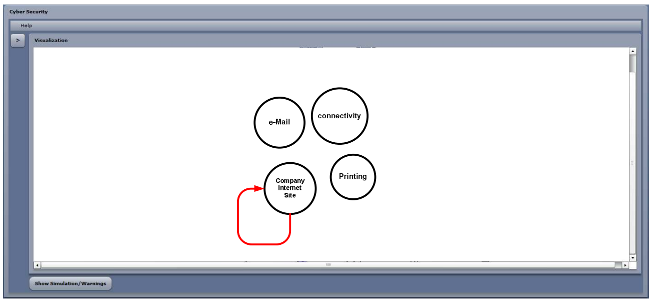


Figure 7: Security Storm Map Drill-down to Service

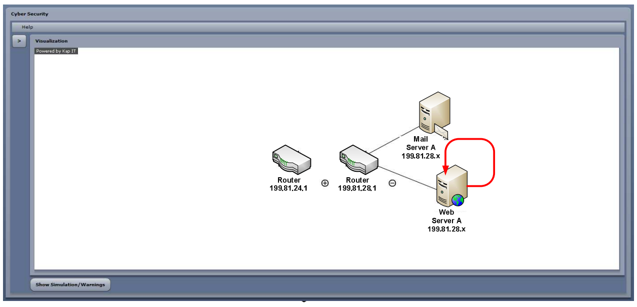


Figure 8: Security Storm Map - Drill Down to Devices

المنارة للاستشارات
www.manaraa.com

REFERENCES

[1] Apple. [Online]. http://www.apple.com

[2] M. Bishop, *Introduction to Computer Security*. Boston, MA: Addison-Wesley, 2004.

[3] Baecker, Card, Carey, Gasen, Mantei, Perlman, Strong and Verplank Hewett. (1996) ACM SIGCHI Curricula for Human-Computer Interaction. [Online]. http://old.sigchi.org/cdg/cdg2.html#2_1

[4] J. Bayne. (2002) SANS Institute InfoSec Reading Room. [Online]. http://www.sans.org

[5] R. Marty, *Applied Security Visualization*.: Addison-Wesley Professional, 2008.

[6] ArcGIS. [Online]. http://www.esri.com/software/arcgis/index.html

[7] R. Witty, C. Baum, S. Mingay, and K. Noakes-Fry. (2006, June) Gartner. [Online]. http://www.gartner.com

[8] (2010, August) Best Management Practice. [Online]. http://www.best-management-practice.com/knowledge-centre/news/itil-news/?di=594707

[9] V. Arraj. (2010, August) Best Management Practice. [Online]. http://www.best-management-practice.com/Knowledge-Centre/White-Papers/?CLICKID=002094

[10] J. Dugmore and S. Taylor. (2008, March) Best Management Practice. [Online]. http://www.best-management-practice.com/Knowledge-Centre/White-Papers/?CLICKID=002094

[11] (2010, August) ITIL. [Online]. http://www.itil-officialsite.com/home/home.asp

[12] T. Scholtz. (2009, November) Gartner. [Online]. http://www.gartner.com

[13] (2009, July) PCI Security Standards Council. [Online]. https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html

[14] (2010) PCI Security Standards Council. [Online]. https://www.pcisecuritystandards.org/index.shtml

[15] (2010) ISO/IEC/ITU-T SAG on Security (SAG-S). [Online]. http://www.iso.org/iso/iss_iso-iec-itu-t_sag-on-security.htm

[16] (2010) International Organization for Standardization. [Online]. http://www.iso.org/iso/about.htm

[17] (2010) International Standardization on Security. [Online]. http://www.iso.org/iso/iss_home.htm

[18] J. Witty and L. Boyle. (2010) Gartner. [Online]. http://www.gartner.com

[19] T. Scholtz and F. Byrnes. (2010, February) Gartner. [Online]. http://www.gartner.com

[20] L. Lyons IV. (2006) SANS. [Online]. http://www.sans.org

[21] C. Ware, *Information Visualization: Perception for Design*. San Francisco, CA: Morgan Kaufmann Publishers Inc., 2004.

[22] K. Nesbitt, "Using Guidelines to Assist in the Visualization Design Process," in *Asia Pacific Symposium on Information Visualization (APVIS 2005)*, Sydney Australia, 2005, pp. 115-123.

[23] F. Mansmann, F. Fischer, D. A. Keim, and S.C. North, "Visual Support for Analyzing Network Traffic and Intrusion Detection Events Using TreeMap and Graph Representations," in *Proceedings of the Symposium on Computer Human interaction For the Management of information Technology (Baltimore, Maryland, November 07 - 08, 2009). CHiMiT '09*, New York, NY, 2009, pp. 19-28.

[24] S. Foresti, J. Agutter, Y. Livnat, S. Moon, and R Erbacher, "Visual Correlation of Network Alerts," *IEEE Computer Graphics and Applications*, pp. 48-49, 2006.

[25] (2009) Forum of Insident Response and Security Teams. [Online]. http://www.first.org/cvss/cvss-guide.html

[26] (2010, May) Common Vulnerability Scoring System. [Online]. http://nvd.nist.gov/cvss.cfm

[27] Q. Wu, D. Ferebee, Y. Lin, and D. Dasgupta, "Visualization of Security Events Using an Efficient Correlation Technique," in *In the proceedings of the Symposium on Computational Intelligence in Cyber Security (CICS) at the IEEE Symposium Series on Computational Intelligence (SSCI 2009)*, Nashville, TN, 2009.

[28] Q. Wu, D. Ferebee, Y. Lin, and D. Dasgupta, "Monitoring Security Events Using Integrated Correlation-Based Techniques," in *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies*, Oak Ridge, Tennessee, 2009.

[29] Q. Wu, D. Ferebee, Y. Lin, and D. Dasgupta, "An Integrated Cyber Security Monitoring System Using Correlation-based Techniques," in *Fourth International Conference on System of Systems Engineering*, Albequerque, New Mexico, 2009.

[30] (2010, November) Common Vulnerabilities and Exposures. [Online]. http://cve.mitre.org/

[31] (2007, October) Best Management Practice. [Online]. http://www.best-management-practice.com/Knowledge-Centre/White-Papers/?CLICKID=002094

[32] A. Litan, C. Casper, and P. Proctor. (2009, November) Gartner. [Online]. http://www.gartner.com

المنارة للاستشارات

www.manaraa.com