2009

Exploring utilization of visualization for computer and network security

Andy Luse
Iowa State University, andyluse@iastate.edu

Recommended Citation

Luse, Andy, "Exploring utilization of visualization for computer and network security" (2009). *Graduate Theses and Dissertations.* Paper 12042.

Exploring utilization of visualization for computer and network security

by

Andrew William Luse

A dissertation submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Co-Majors: Human Computer Interaction; Computer Engineering

Program of Study Committee:
Anthony Townsend, Co-major Professor
Doug Jacobson, Co-major Professor
Brian Mennecke
Kevin Scheibe
Thomas Daniels
Dimitris Margaritis

Iowa State University

Ames, Iowa

2009

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

The role of the network security administrator is continually morphing to keep pace with the ever-changing area of computer and network security. These changes are due in part to both the continual development of new security exploits by attackers as well as improvements in network security products available for use. One area which has garnered much research in the past decade is the use of visualization to ease the strain on network security administrators. Visualization mechanisms utilize the parallel processing power of the human visual system to allow for the identification of possible nefarious network activity. This research details the development and use of a visualization system for network security. The manuscript is composed of four papers which provide a progression of research pertaining to the system. The first paper utilizes research in the area of information visualization to develop a new framework for designing visualization systems for network security. Next, a visualization system is developed in the second paper which has been utilized during multiple cyber defense competitions to aid in competition performance. The last two papers deal with evaluating the developed system. First, an exploratory analysis provides an initial assessment using participant interviews during one cyber defense competition. Second, a quasi field experiment explores the intention of subjects to use the system based on the type of visualization being viewed.

CHAPTER 1: INTRODUCTION

1.1 ORGANIZATION

This document is composed of four separate manuscripts which comprise the research in, development, and evaluation of a visualization product for Cyber Defense Competitions (CDCs). Each manuscript is copied almost exactly from the original submission (except for some minor formatting changes). The figures, tables, and references for each manuscript are included in the same chapter as the respective manuscript as it did for the original submission. A general introduction is provided here as well as a general conclusion at the end of this document. Also, references utilized in the introduction and/or conclusion are included in a reference section at the end of the entire document.

The manuscripts included in this document follow a logical progression from initial topic research, through product development, and finally product evaluation. The first manuscript proposes a new component-based framework for development of visualization systems for network security. This manuscript utilizes information visualization theory primarily by Shneiderman (Shneiderman & Plaisant, 2005) and Few (Few, 2006) as background for the proposed methodology. A review of 23 network visualization products are then utilized as a first-pass mechanism for verifying that the pieces of the proposed framework are currently being utilized.

The second manuscript details the development of a system, Cyber Defense Competition Visualization (CDCVis), for use by participants in a CDC. The manuscript utilizes a design science approach outlined by Hevner (Hevner, March, Park, & Ram, 2004) for designing products as solutions to novel problems. The manuscript thoroughly describes the process behind the development of the module-based CDCVis system. Parallels are then made between the use of CDCVis during competitions and visualization for network security.

The third manuscript provides an exploratory analysis of the CDCVis system. The study utilizes interviews with users of the system during actual deployment. The users include CDC participants during a CDC competition. Textual analysis is utilized as a first pass at understanding the usage of the CDCVis system.

Finally, the fourth and final manuscript describes a quasi field experiment utilized to further analyze the use of CDCVis. Specifically, the research utilizes technology acceptance, through the use of the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh, Morris, Davis, & Davis, 2003), to measure the likelihood that users of CDCVis would be likely to use the system for network administration in the future.

1.2 Literature Review

This section provides a brief literature review of some of the more pertinent topics concerning the research in this document. Each of these topics is discussed in greater depth in at least one of the included manuscripts. This section is only intended to give the reader a brief introduction into the topics.

1.2.1 Security Administration

Network security administration is a daunting task that is ever-increasing in both workload and complexity. The problem still remains that corporations are not willing to set aside the necessary funds to adequately support network administration (Whitman, 2003). In fact, 53% of those corporations interviewed in the CSI Computer Crime and Security Survey said that they allocated 5% or less of their overall IT budget to security while the average estimated losses due to cybercrime increased (Richardson, 2008). This implies that while cybercrime is increasing, the amount of money allocated to network security is still very minimal. Therefore, network administrators must either do more with less, or neglect an area, which can have severe repercussions for the organization.

Network security involves intrusion detection (ID) analysis of network activity. Two types of ID exist. Signature-based detection utilizes pre-existing signatures of attacks which are compared with current network traffic to detect intrusions (McHugh, Christie, & Allen, 2000; Mukherjee, Heberlein, & Levitt, 1994). Anomaly-based detection begins by establishing a baseline of "normal" network activity and then detecting traffic which strays from this established norm (Denning, 1986; Kemmerer & Vigna, 2002). Traditionally, signature-based systems have been predominantly implemented utilizing text-based logs which must be serially processed. Typically, human involvement with the actual analysis process is low as the shear amount of logs is impossible to analyze (Takada & Koike, 2002).

1.2.2 VISUALIZATION FOR COMPUTER AND NETWORK SECURITY

During the past decade, visualization for network security has become a hot research topic. The infoVis community provides links to various research projects in the area of network visualization (Aigner, 2009). Also, the VizSec community has promoted the issue both through its online community as well as through its sponsored VizSec Conference (Inc., 2009).

Several products have been developed to promote research in the area of visualization for network security. NVisionIP has been the subject of many different articles. The system utilizes multiple views to allow the user to view various network segments with varying levels of granularity (Lakkaraju, Bearavolu, & Yurcik, 2003; Lakkaraju, Yurcik, Bearavolu, & Lee, 2004;

Lakkaraju, Yurcik, & Lee, 2004). TNV provides a timeline approach to allow the user to view network traffic over time (Goodall, Lutters, Rheingans, & Komlodi, 2005), while VisFlowConnect partitions the visualization screen into two parts to allow the user to view traffic between the internal and external networks (Yin, Yurcik, Treaster, Li, & Lakkaraju, 2004). These are just a few examples of many different research projects on network security visualization (see Chapter 2 for more examples).

Three predominant frameworks have been proposed to help researchers more adequately develop visualization systems for network security. The systems are based on three main areas of the systems involved with network security: users, inputs (security alarms), and the visualization components which make up the system. The user-based perspective looks at the system from the user's perspective and tries to design the system around their needs (Goodall, 2005; Goodall, Lutters, & Komlodi, 2004; Goodall, Ozok, Lutters, Rheingans, & Komlodi, 2005; Komlodi, Goodall, & Lutters, 2004; Komlodi, Rheingans, Ayachit, Goodall, & Joshi, 2005). The input-based perspective, or *w^3 premise*, designs the system around the security alerts which are sent to the visualization system (Foresti, Agutter, Livnat, Moon, & Erbacher, 2006; Livnat, Agutter, Moon, Erbacher, & Foresti, 2005). Finally, the component-based framework looks at the system from the standpoint of the visual components with which it is composed (Luse, Scheibe, & Townsend, 2008).

1.2.3 Cyber Defense Competitions

Cyber defense competitions (CDCs) are utilized as a method for teaching network security concepts using live exercises. These competitions have been shown to be effective for teaching network security concepts (Conklin, 2006) and also for raising awareness of security exploits, tools, and countermeasures (Jacobson & Evans, 2006). Two primary types of CDCs have been utilized to date. The first involves teams of students that both defend their pseudo-corporate network while also trying to attack and exploit the networks of other student teams (Cowan, Arnold, Beattie, Wright, & Viega, 2003; Hoffman, Rosenberg, Dodge, & Ragsdale, 2005). The second type requires students to act only as defenders of their corporate network against attacks perpetrated by an external attacking team (Jacobson & Evans, 2006).

CDCs provide a rich test-bed for research in the area of network security administration. While not a true field experiment setup, these competitions provide real-time attack scenarios between actual defenders and attackers. Furthermore, most of these competitions require that the student teams maintain certain corporate services (web, email, file transfer, etc.) which is directly in-line with corporate network security administration.

1.3 PURPOSE OF RESEARCH AND METHODOLOGY

The purpose of this research is to investigate current theories and research in the area of visualization for computer and network security. This background will help to show the current trends in the area and state-of-the-art theories. This understanding will allow for greater understanding of visualization theory as it applies to computer and network security and therefore allow the user to both critically examine research in the area and also better develop visualization mechanisms of their own for network security.

Secondly, this research provides the development of a functioning prototype for visualization of network security events. This prototype utilizes some of the extant research to develop a system which can aid in network administration. Specifically, the system is developed for CDCs, to allow participants at these competitions to better understand network security concepts and better perform network security functions. The design science research methodology is utilized as a mechanism for the development of the system.

Third, this research provides an evaluation of the prototype utilizing both qualitative and quantitative measures. These evaluations provide a first step at understanding how to evaluate network security visualization systems. The exploratory research methodology provides a first pass at understanding these types of systems, while the quasi field experiment provides a more structured methodology for evaluation.

1.4 PLAN OF PRESENTATION

The following chapters are reprints of papers which have been written pertaining to the research plan above. Chapter 2 proposes a novel component-based framework for the development of network security visualization systems. Chapter 3 details the development of a network visualization system for use during CDCs. Chapter 4 provides a qualitative analysis of the system detailed in the previous chapter utilizing participant interviews during a CDC. Chapter 5 details a quasi field experiment which tests the intention of users to utilize the system developed in Chapter 3. Finally, Chapter 6 will offer some concluding remarks in regard to the papers and also some limitations with the current implementation as well as future research plans.

CHAPTER 2: A COMPONENT-BASED FRAMEWORK FOR VISUALIZATION OF INTRUSION DETECTION EVENTS

Modified from a paper published in *Information Security Journal*

Andy Luse[1], Kevin P. Scheibe, and Anthony M. Townsend

KEYWORDS

Intrusion Detection, Information Visualization, Framework, Security

ABSTRACT

Visualization systems for intrusion detection are becoming more prevalent with time, but the lack of an organizing framework for proper development of these systems is problematic. This paper introduces a component-based structure which can be used to adequately design and implement intrusion detection information visualization systems. This component-based structure implements a combination of common information visualization components with operational components which are specific to the critical, real-time nature of intrusion detection. The manuscript also performs an analysis of intrusion detection visualization research projects by verifying their use of the components described by this framework.

[1] I performed the primary portion of the manuscript preparation as well as the literature review and analysis for the descriptive study.

INTRODUCTION

The traditional method for network security examination has been the analysis of logs, a tedious and difficult task with which many administrators contended. This analysis involved sifting through text-based log files in a search for activity which could be interpreted as system misuse. While many intrusions and security breaches have been detected by log examination, the system is not without its flaws: First, the logs are encoded as simple text and uncovering a security breach requires a highly serial examination of all of the log data; second, many logs only record application specific behavior, which only provide information, often not security related, relevant to specific applications on the system; finally, the sheer magnitude of the logs which must be inspected is so immense that even well-intentioned examinations may be cursory and ineffective (Takada & Koike, 2002b).

Intrusion Detection (ID) is a network security mechanism which has increased in popularity during the last two decades and is seen as a viable method for dealing with nefarious code, as well as network intrusions. The goal of ID is simple: detect intrusive behavior (Kemmerer & Vigna, 2002) through an automated analysis of both network logs and real time network traffic to prevent successful attacks on the network. ID relieves network specialists of the tedium of log examination and offers a much quicker turnaround time than mere human analysis, expediting intrusion detection and prevention.

Unfortunately, high false detection rates have eroded confidence in many ID implementations. Two types of false detection, false positives and false negatives, can be problematic. False positives interpret normal behavior as intrusive while false negatives fail to recognize truly intrusive behavior (Koike, Ohno, & Koizumi, 2005). Current ID systems often have a high concentration of both of these false detections.

Information visualization (IV) has been explored extensively in recent years as a mechanism for improving ID analysis of network traffic. This mechanism attempts to improve the quality of the human contribution to the overall ID system, with the goal of reducing system detection error. While IV-enabled systems continue to employ machine filtering for intrusive behavior detection, the network specialist is given a more active role in the overall detection strategy than in traditional ID systems. IV exploits the extraordinary capacity of the human visual system for analyzing and understanding complex concepts via visual stimuli to augment the automated processes of traditional ID.

IV-enabled ID systems are currently developed within one of two frameworks: A user-based framework, where operator tasks receive the majority of visualization augmentation, or an input-based framework, where the visual presentation of alerts is the impetus for visualization development. While research and system design are well-documented within both of these frameworks, research focusing on a comprehensive visualization scheme for ID systems has yet to be explored. Accordingly, our research develops a comprehensive methodology for IV-enabled ID systems that is consistent with extant research and practice, and which embraces broader information visualization theory.

We first review background research in ID itself, in existing IV-enabled ID research, and in IV theory. Following this review, we describe how IV theory suggests an additional visualization framework that can be combined with existing IV-enabling systems to construct a comprehensive visualization scheme. To demonstrate the viability of this comprehensive approach we perform a review and analysis of 23 ID visualization systems that have been described in ID research and identify their visualization elements.

BACKGROUND

Intrusion Detection (ID) was formally coined in the 1980's (Denning, 1986). Proctor describes ID as "the art of detecting and responding to computer misuse" (Proctor, 2001). ID involves a machine or human detecting behavior on a computer or network which could be intrusive and then taking actions to verify the behavior as truly intrusive before stopping or mitigating the effects of the intrusive behavior.

Ideally, ID would be in real-time. If an attacker is performing an intrusive action, system administrators would like to stop this action as soon as possible. Temporally speaking, the closer the detection is to an attack the more proactive the system administrator can be to prevent damage, and this is the goal for most ID systems. Towards this goal, several frameworks have been developed for different types of ID systems. The remaining portion of this section provides an overview of categorizations of the various types of ID systems.

Detection Type Categorization

Two primary methods can be used to decipher the intent of activities on a network – signature-based and anomaly-based. Both methods have their inherent advantages and disadvantages.

Signature-based systems employ descriptions or "signatures" of known attacks to identify a matching attack (McHugh, Christie, & Allen, 2000). The system compares the traffic or user activity to a rule-base of techniques used by attackers to compromise systems (Mukherjee, Heberlein, & Levitt, 1994). These signatures are typically made up of data which an attack packet or stream would contain. The ID system collects raw packet data from network traffic and compares these data to the signature. This type of detection mechanism is also known as *misuse detection* as the system is attempting to discover misuse according to known system misuse mechanisms (Kemmerer et al., 2002). These signatures are analogous to the virus definitions a virus scanner updates and uses to detect viruses in files.

Anomaly-based systems use models of intended or “normal” behavior on the network as a baseline to detect deviations from this norm (Kemmerer et al., 2002). This approach assumes that exploitation of system vulnerabilities will involve some abnormal use of the system (Denning, 1986). Detecting intrusive behavior based on deviations from an established norm allows the system to detect novel attacks (McHugh et al., 2000). Whereas signature-based systems rely on encoding of previously known attacks, anomaly-based systems do not rely on such signatures.

While both detection type methods are currently in use, anomaly-based mechanisms are more widely deployed for IV. Signature-based visual analysis is generally useful only after an operator has worked with a system for some time and begins to recognize certain visual patterns as specific attacks. Conversely, anomaly-based methods can be employed successfully by all technicians, even those new to the network. Operators will begin to notice visual outliers that deviate from the normal visual pattern of network data and, consequently, explore this abnormal data further for possible intrusive activity.

Topology-based Categorization

Topology-based ID categorizations provide delineations according to the ID system’s position within the network topology. This position in the network allows multiple, differently located detection mechanisms to more efficiently analyze certain types of intrusive activity across the system. Within each of these topology-based categorizations, the respective system can consist of signature-based or anomaly-based detection. Table 1, following this section, gives an overview of these combinations.

Network-based ID systems typically consist of independent machines on the network which are used to monitor the network traffic flow for intrusions (Mukherjee et al., 1994). Network ID systems analyze packets as they traverse the network from host to host. A variety of filters can be set to analyze fields within the packet header as well as the data portion of the packet. Network-based ID systems offer an overview of all activity on the network and are usually placed at a critical position in the network (e.g. where the internal corporate network connects to the external Internet). For this reason, network-based ID systems see all traffic going into and out of a network and, therefore, are capable of showing a high-level overview of network traffic.

Host-based systems operate on a single host within the network, analyzing audit and/or log data as well as traffic to and from the host. Various application and operating system (OS) logs can be used to discover a broader range of intrusive behavior as opposed to solely analyzing network traffic data (which is performed by network-based ID). Also, the behaviors and system calls of various applications on the host can be monitored for anomalous behavior (McHugh et al., 2000). Host-based ID systems are superior for analyzing host-specific data. Host-based systems can monitor various applications in a way that would be impossible for a network ID system because it involves intrusive acts on the computer which does not send data across the network (McHugh et al., 2000). Host ID systems have a greater understanding about what payloads of packets will do to a specific host (Xin, Dickerson, & Dickerson, 2003).

Distributed ID systems combine information from distributed nodes into a central repository for further analysis (Snapp, Brentano, Dias, Goan, Heberlein, Ho, Levitt, Mukherjee, Smaha, Grance, Teal, & Mansur, 1996). Each host in the network is equipped with a monitoring device that, in turn, sends all locally monitored data to a centralized management machine. This machine can then correlate this host data with data it has collected using network-based ID mechanisms (Mukherjee et al., 1994). Distributed ID systems attempt to combine the advantages of both network-based and host-based ID systems. With distributed, host-based sensors at each machine, intrusive activity that occurs at a single host is monitored even if it is not visible to a network monitor. The data from these individual monitors are then used to augment the data which has been collected using network-based ID systems. In this way both ID types are leveraged together to better understand the activity on the network as a whole.

While all three of the above topology-based ID types have been used for data collection for ID visualization systems, network-based systems are currently the most often employed. There are several reasons for this. First, many companies are primarily interested in attacks which originate from the Internet and are not as concerned with activities on any single host. Second, the burden of collecting data from multiple machines greatly decreases the likelihood of real-time data analysis, which is a primary expectation for the system. Third, the cost involved with deploying many host-based or distributed ID endpoints is much greater than deploying one network-based ID system.

Table 1: Combinations of intrusion detection categorization types

Topology-based Categorizations	**Detection Type Categorizations**	
	Signature-based	**Anomaly-based**
Network	compares network traffic to rules ofalready known intrusive behavior	analyzes network traffic for deviations from "normal" traffic patterns (current work)
Host	compares host activity with rules ofalready known intrusive behavior	analyzes host activity for deviations from "normal" system usage
Distributed	gathers information from distributed endpoints and combines this with network data comparing this data to rules of already known intrusive behavior	gathers information from distributed endpoints and combines this with network data analyzing this data for deviations from "normal" systemusage

Information Visualization Theory

In its broadest sense, information visualization utilizes computer graphics to help understand abstract data. Many scientific disciplines (geology, meteorology, animal science, etc.) use conventional visualizations to help analyze data which are based on underlying spatial data (Chi, 2002). Conversely, IV is designed to take advantage of visualizations that represent abstract data (Card, Mackinlay, & Shneiderman, 1999). Industries such as banking, manufacturing and consumer products are using IV for analysis (Wright, 1997). Other applications of IV exist in data mining and knowledge discovery (Fayyad, Grinstein, & Wierse, 2001), concept maps (Cañas, Carff, Hill, Carvalho, Arguedas, Eskridge, Lott, & Carvajal, 2005) and medicine (Chittaro, 2001), to name a few.

Information Visualization Components

IV theory posits that common components become necessary for the user when interacting with IV systems. Shneiderman (Shneiderman & Plaisant, 2005) delineates a common framework of certain components which should be available to the user of any IV system. These components provide the user with a usability structure that enables effective interaction with the data that is being visually presented, and are necessary regardless of the type of data being visualized.

Overview – An overview provides an overall picture of the entire underlying dataset of an IV system. This type of view commonly includes zoomed-out pictures of the data with an adjoining detail view.

Zoom – Zooming allows the user to zoom in and focus on a specific portion of the IV. Quality systems allow the user to control this feature fluidly and provide smooth zooming to preserve the user's sense of position and context.

Filter – The filter task allows the user to filter out uninteresting data values and focus on those items of interest. This can follow either a subtractive model (where the user removes those values he or she deems unneeded or uninteresting) or a additive model (where the user highlights items which he or she believes are of greater interest, thereby drawing attention away from uninteresting data values).

Details-on-demand – The user is allowed to select certain aspects of the visualization to gain more detailed information about the underlying information pertaining to that piece or subsection of the data. Details-on-demand typically coincide with the overview task and the zoom task above.

Relate – Relation allows the users to specify relations among data present in the visualization system. These relationships can be revealed using lines, colors, textures, as well as many other visual components.

History – History allows users to review the visualization during past states. This allows the user to replay the data for further review, undo actions taken, and also refine actions.

Extract – The user is allowed to extract data and or visualizations for later viewing or displaying to others. This often involves statistical summaries using common statistical visualization methods (histograms, pie charts, etc.) or captures of the visualization state at specific moments.

The Real-Time Imperative

Requirements for IV systems differ based on the requirements for the system. The book *Information Dashboard Design* (Few, 2006) describes visual dashboards which are used to aid in various business activities. The book describes some interesting taxonomies of task orientations (e.g., role-based classification, orientating the visuals toward strategic, operational, and analytical functions) but most importantly, notes the imperative for real-time display of information when visualizing time-dependent activities. While this may seem to be a self-evident characteristic for security visualizations, it is not a characteristic common to all IV and must be added to the general component structure described above. All of the components of an IV-enabled ID system must present both historical system data, as well as real-time information as it is happening.

Current Intrusion Detection Visualization

Little research has been done in designing a comprehensive structure for intrusion detection visualization systems. Currently, IV-enabled ID systems are built around two different operational frameworks, which are based on the two primary actors in an ID visualization system: the user and the alert.

The user-based framework (Goodall, 2005; Goodall, Lutters, & Komlodi, 2004; Goodall, Ozok, Lutters, Rheingans, & Komlodi, 2005b; Komlodi, Goodall, & Lutters, 2004; Komlodi, Rheingans, Ayachit, Goodall, & Joshi, 2005) describes an approach which looks at ID visualization systems from the user's perspective. Research in this aspect of system design involved interviews and prototype evaluations using security analysts with ID expertise. This work led to a user-based process model for ID visualization. The model laid out a framework based on three phases of user interaction with the system: monitoring, analysis, and response. Each of these three areas involves certain user tasks included in the following delineation.

1. Monitoring: monitoring attack alerts and identifying potential attacks

2. Analysis: analyzing alerts and other data to diagnose an attack

3. Response: responding to the attack, documenting and then reporting

In (Komlodi et al., 2004), the authors broadly describe high-level visualization mechanisms which analysts need access to during the above three phases, but do not offer detail and instead focus on the user process. The research offers a very good framework for user policy when delineating necessary tasks for the successful use of an ID visualization system.

The alert-oriented framework (Foresti, Agutter, Livnat, Moon, & Erbacher, 2006; Livnat, Agutter, Moon, Erbacher, & Foresti, 2005) is designed around the presentation of system alerts. The authors' framework, which they refer to as the w^3 premise, focuses on three attributes of a possible attack on the network. This includes *when* in time the alert happened, *where* the alert took place on the network, and *what* type of alert it is. This framework focuses on alerts as the primary item of interest, and designs the system around what is necessary to assess these alerts effectively. The framework allows for effective ID visualization by designing the system entirely around the data inputs to the system.

Taken together, these two frameworks codify the operational underpinnings of effective ID visualization; however, while they describe what the system needs to accomplish, they do not offer a clear methodology of presentation, in particular, one which is consistent with broader IV theory. By taking these operational dicta and reforming them within Shneiderman's component structure (Shneiderman et al., 2005), they offer a unified and comprehensive approach to effective visualization of network security.

A COMPREHENSIVE SYSTEM

Development of any visualization system necessarily involves various pieces which interact. A comprehensive system for development provides a clear sense of the operational needs for the system and an effective method to structure these operations for the most effective user visualization and interaction. In Figure 1, we present a diagram of this system that shows the operational criteria presented within the user-based and input-based frameworks, along with the organizing structure imposed by IV theory (the component structure).

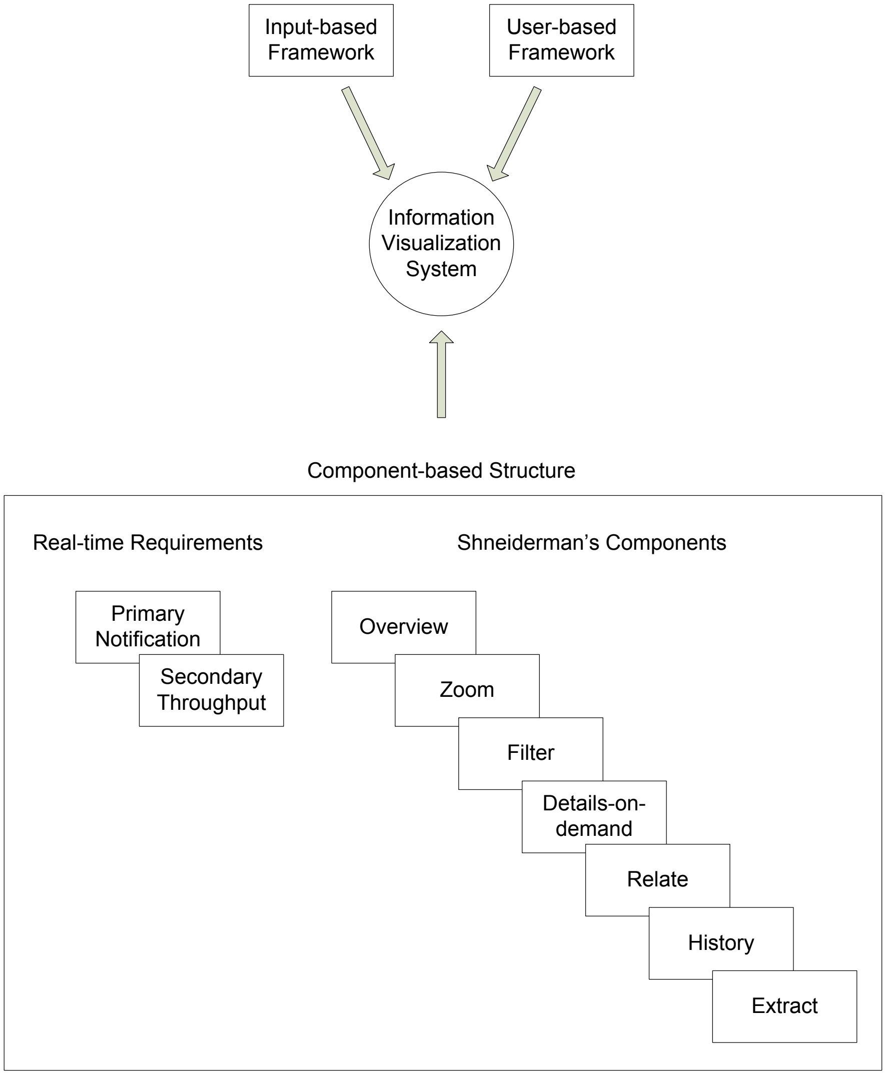


Figure 1: Overall information visualization framework showing operational frameworks and organizing structure.

In more detail, the comprehensive framework shows:

1. User-based framework, which looks at the system from a user's perspective. This framework describes the processes the user executes when interacting with the system.
2. Input-based framework, which focuses on the presentation of data gleaned from the various network security analyses.
3. Component-based structure, describes the actual method of presenting the above operations for maximum user facility. Whether user-based or input-based information is

visually presented, it would be presented in a system where each activity would have overview, zoom, filter, etc. capacity to allow for maximally efficient interaction between the user and the IV-enabled system.

An effective framework for ID visualization thus incorporates the operational imperatives of both the user-based framework (Goodall, 2005; Goodall et al., 2004; Goodall et al., 2005b; Komlodi et al., 2004; Komlodi et al., 2005) and the input-based framework (Foresti et al., 2006; Livnat et al., 2005) organized within a component-based structure.

At this point, we can present our ID visualization framework in full detail; with the component-based structure for ID visualization systems built around the data, activities, and analyses unique to the underlying nature of ID data. The common visualization components are taken from Shneiderman (Shneiderman et al., 2005) (as described above).

The operational role also dictates two additional real-time requirements which are critical in ID visualization: primary notification and secondary throughput (Few, 2006). Primary notification describes the necessary requirement that the user is made aware of an alert. If the user is not notified that an alert has arisen, the user will not be able to respond to the alert in a timely fashion. Second, the data necessary to evaluate and respond to an alert must be made available to the user. This entails the throughput of the information related to the identified alert.

Using the combination of the above elements, a component-based structure can be described. These common visual components will be described in relation to their use in ID visualization systems. The following description is abbreviated in Table 2.

Overview – Provides an overall picture of the network. This may be a literal mapping of the data to physical locations or a logical mapping with no tie to physical space. An overview allows the analyst to get an idea of what is occurring on the entire network.

Zoom – Allows the analyst to zoom in on a specific area of the network. This may correspond to increased network activity in a specific area or greater detail of an area where an alert has been spotted.

Filter – Filter allows the analyst to focus on specific characteristics of interest on the network. The subtractive model would allow the user to remove those items on the network which he or she is not currently interested in. The additive model allows the user to highlight (possibly using colors, contrast, etc.) those items of interest.

Details-on-demand – The analyst can select certain aspects of the visualization to receive detailed information about the network, traffic, and/or alerts in a specific section. Many times this involves two separate views where the user clicks on one view and receives information pertaining to the selection in the first view displayed in the second view.

Relate – Analysts can setup relationships between similar items. Typically this involves using various visual mechanisms (lines, colors, textures) to delineate this relationship (see Figure 2).

History – The analyst is allowed to review past network traffic and alert data. This will allow for reconnaissance as well as evidentiary corroboration for legal trials which may result from certain illegal acts perpetrated on the network (see Figure 3).

Extract – Extraction allows the analyst to capture the state of the network at specific moments of interest. Many times statistical charts (histograms, pie charts, etc.) as well as screen captures are employed to organize information that is to be captured (see Figure 4).

Primary Notification – The user is notified that an alert has occurred. This involves real-time notification and may even occur before all the data pertaining to the alert is available to the user. This is different from traditional IV systems which typically have all the pertinent information available when it is made available to the user. This type of visual notification is usually accomplished with visual cues such as color change, flashing, etc.

Secondary Throughput – The data pertaining to a specific alert is made available to the user for greater detail once the data has been completely received. This component typically utilizes the details-on-demand component above and will therefore be categorized with it.

Table 2: Components for intrusion detection information visualization

Tasks	***Description***
Overview	Gain an overview of all activity on the network.
Zoom	Zoom in on areas of interest in the network.
Filter	Filter out those items which are not needed.
Details-on-demand (Secondary Throughput)	Select an item to receive detailed information about that specific network activity.
Relate	View relationships among items on the network.
History	History of activity on the network to support reconnaissance and future legal activities.
Extract	Extract state indicators of the network at a specific moment.
Primary Notification	Notification to the user that an alert has occurred.

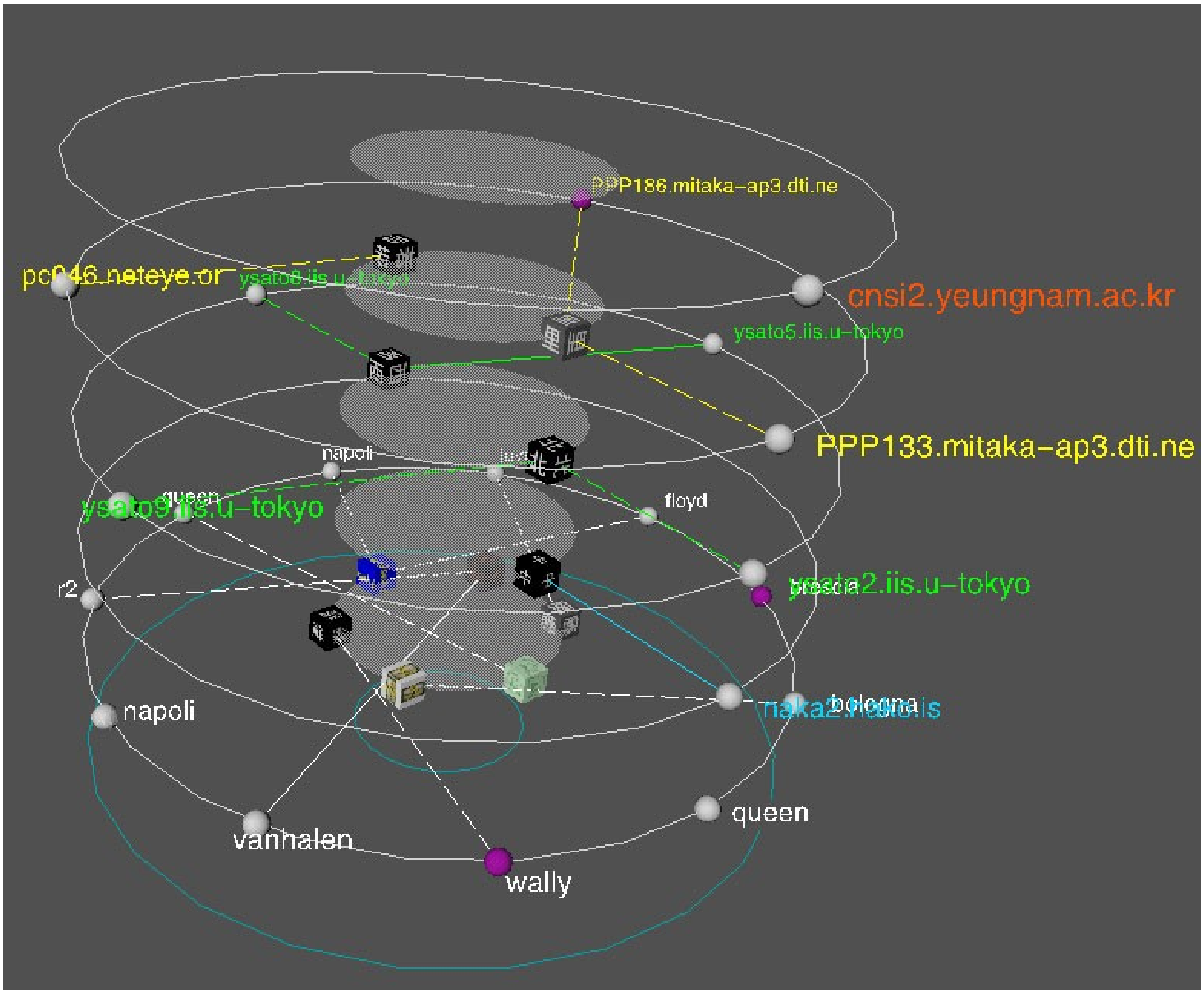
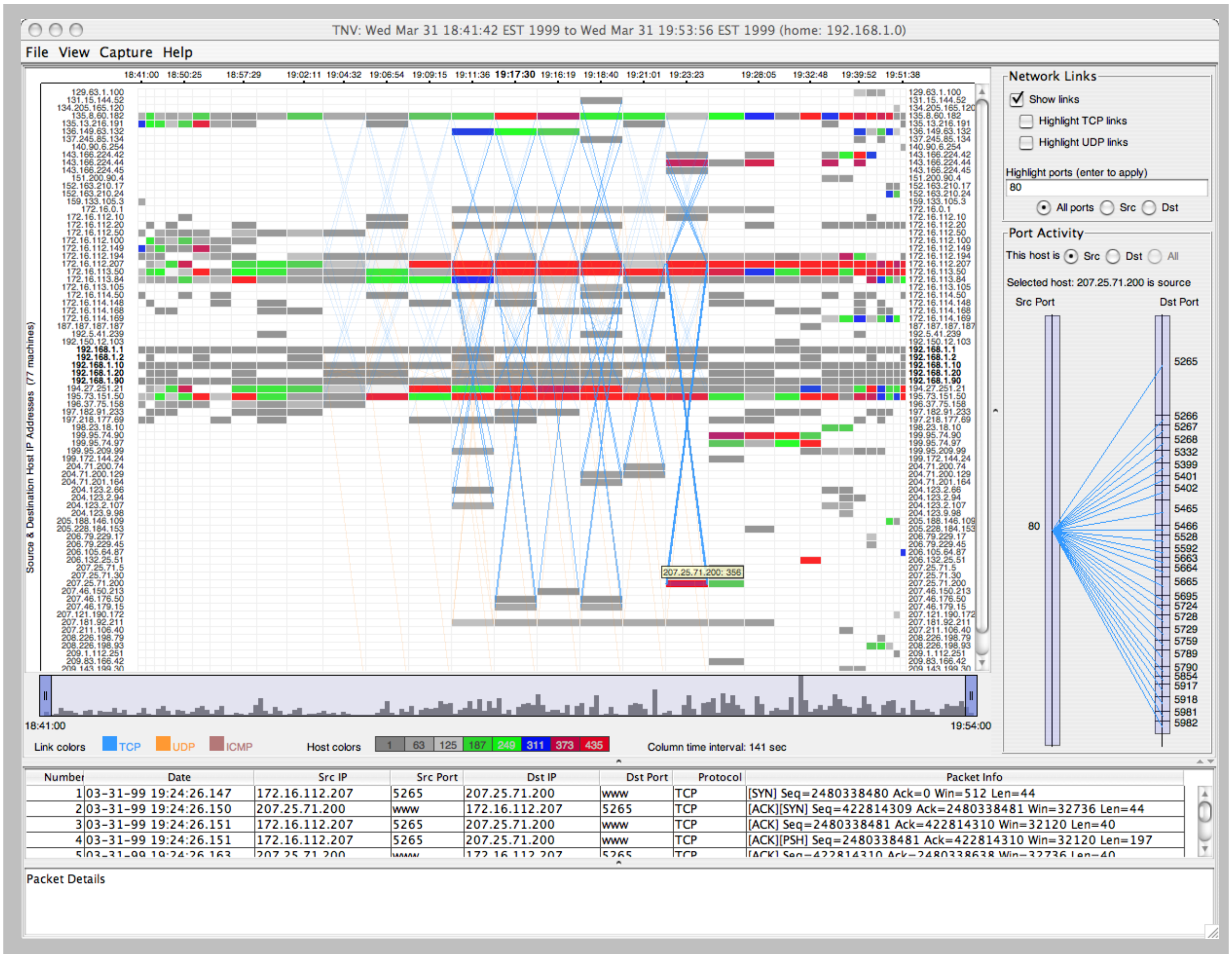


Figure 2: Tudumi (Takada et al., 2002b) showing *relation* (available at http://www.vogue.is.uec.ac.jp/~koike/tudumi/tudumi1024.jpg).



TNV: Wed Mar 31 18:41:42 EST 1999 to Wed Mar 31 19:53:56 EST 1999 (home: 192.168.1.0)

Network Links

☑ Show links

□ Highlight TCP links

□ Highlight UDP links

Highlight ports (enter to apply)

80

● All ports ○ Src ○ Dst

Port Activity

This host is ● Src ○ Dst ○ All

Selected host: 207.25.71.200 is source

Link colors 🟦 TCP 🟧 UDP 🟥 ICMP

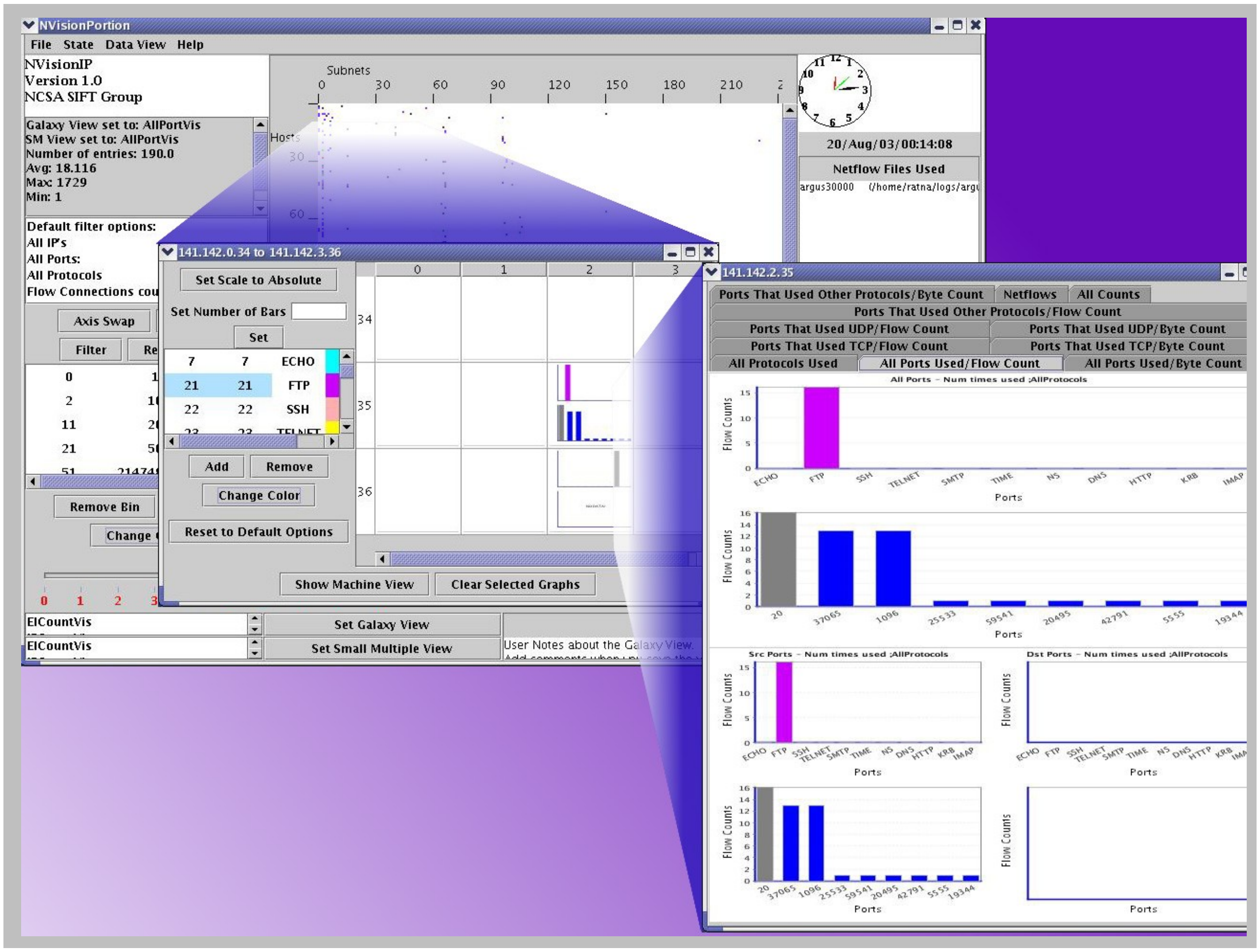
Host colors 1 63 125 187 249 311 373 435

Column time interval: 141 sec

Number	Date	Src IP	Src Port	Dst IP	Dst Port	Protocol	Packet Info
1	03-31-99 19:24:26.147	172.16.112.207	5265	207.25.71.200	www	TCP	[SYN] Seq=2480338480 Ack=0 Win=512 Len=44
2	03-31-99 19:24:26.150	207.25.71.200	www	172.16.112.207	5265	TCP	[ACK][SYN] Seq=422814309 Ack=2480338481 Win=32736 Len=44
3	03-31-99 19:24:26.151	172.16.112.207	5265	207.25.71.200	www	TCP	[ACK] Seq=2480338481 Ack=422814310 Win=32120 Len=40
4	03-31-99 19:24:26.151	172.16.112.207	5265	207.25.71.200	www	TCP	[ACK][PSH] Seq=2480338481 Ack=422814310 Win=32120 Len=197
5	03-31-99 19:24:26.163	207.25.71.200	www	172.16.112.207	5265	TCP	[ACK] Seq=422814310 Ack=2480338638 Win=32736 Len=40

Packet Details

Figure 3: TNV (Goodall, Lutters, Rheingans, & Komlodi, 2005a) showing *historical* timeline (available at http://userpages.umbc.edu/~jgood/research/tnv/screenshots/tnv_web.png).



NVisionIP
Version 1.0
NCSA SIFT Group

Galaxy View set to: AllPortVis
SM View set to: AllPortVis
Number of entries: 190.0
Avg: 18.116
Max: 1729
Min: 1

Default filter options:
All IP's
All Ports:
All Protocols

20/Aug/03/00:14:08

Netflow Files Used
argus30000 (/home/ratna/logs/argu

User Notes about the Galaxy View

Figure 4: NVisionIP (Lakkaraju, Bearavolu, & Yurcik, 2003; Lakkaraju, Yurcik, Bearavolu, & Lee, 2004a; Lakkaraju, Yurcik, & Lee, 2004b) showing statistical *extraction* (available at http://security.ncsa.uiuc.edu/distribution/NVisionDownLoad/pix/AllViewBig.JPG).

ANALYSIS

To examine the viability of our framework with regard to contemporary systems, we analyzed 23 ID visualization systems described by research in this area. We attempted to be as complete as possible in the compilation of the list of ID visualization system research. Table 3 provides a listing of the features of the component-based structure which are evident in these projects. Most products have been listed and referenced using their given name, but those which were not given names just have their reference given.

Table 3: Component-based structure research analysis

	Component-based Sub-Framework Elements							
Product	**Overview**	**Zoom**	**Filter**	**Details-on-Demand (Secondary Throughput)**	**Relate**	**History**	**Extract**	**Primary Notification**
IDS-V(Hiraishi & Mizoguchi, 2001)	x		x	x	x	x		x
(Erbacher, 2003)	x			x		x	x	
Tudumi(Takada et al., 2002b)			x		x			x
NIVA(Nyarko, Capers, Scott, & Ladeji-Osias, 2002)	x			x	x			x
SnortView(Koike & Ohno, 2004)	x			x	x			x
CyberSeer(Papadopoulos, Kyriakakis, Sawchuk, & He, 2004)	x						x	x
TNV(Goodall et al., 2005a)	x	x		x	x			x
(Colombe & Stephens, 2004)	x	x		x				x
VisFlowConnect(Yin, Yurcik, Treaster, Li, & Lakkaraju, 2004)	x	x	x	x	x	x		x
PortVis(McPherson, Ma, Krystosk, Bartoletti, & Christensen, 2004)	x	x	x					
VISUAL(Ball, Fink, & North, 2004)	x		x	x		x		
NVisionIP(Lakkaraju et al., 2003; Lakkaraju et al., 2004a; Lakkaraju et al., 2004b)	x	x	x	x	x		x	x
SCPD(Lau, 2004)	x							x
(Krasser, Conti, Grizzard, Gribschaw, & Owen, 2005)	x	x	x	x		x		
Flatland(Fisk, Smith, Weber, Kothapally, & Caudell, 2003)	x	x		x		x		
Nam(Estrin, Handley, Heidemann, McCanne, Xu, & Yu, 2000)		x		x	x	x	x	
(Abdullah, Lee, Conti, & Copeland, 2005)	x			x		x	x	
IDS RainStorm(Abdullah, Lee, Conti, Copeland, & Stasko, 2005)	x	x	x	x				x
IDGraphs(Ren, Gao, Li, Chen, & Watson, 2005)	x		x	x	x			
IP Matrix(Koike et al., 2005)	x			x		x		x
Visual Firewall(Lee, Trost, Gibbs, Beyah, & Copeland, 2005)	x				x		x	x
MieLog(Takada & Koike, 2002a)	x		x	x	x	x		
Island(Oline & Reiners, 2005)	x							

An examination of the table confirms that all of the components that we identify as critical exist in ID visualization systems. It is also clear that no one system utilizes all of these components (See Sidebar for further discussion). While “overview,” “primary notification,” and “secondary throughput” components are well represented in most of these systems (91%, 56%, and 73% respectively) none of the other components are represented in more than 50% of these systems, which we believe indicates an opportunity for more optimal system design.

DISCUSSION

Our component-based structure provides a useful taxonomy of visualization components for ID visualization systems and provides the visual mechanisms for the organization and presentation of the analytics and operations recommended in the user-based and input-based frameworks. The components which make up the component-based structure are a combination of traditional IV components combined with urgency-based components which are unique to the operational environment surrounding ID visualization systems.

Our analysis of IV-enabled ID systems suggest both positive and negative interpretations of the current state of IV-enable ID systems. Many of the systems are aligned with traditional IV theory, in that they provide the user with an overview of the data and subsequent details-on-demand when needed. Unfortunately, most of the systems fail to effectively reflect IV theory in most other respects. About half the systems do not provide proper zoom mechanisms for greater data analysis, filtering capabilities, the ability to relate visual mechanisms on the screen, and the capability for historical forensic analysis. Two-thirds of the systems do not allow extraction of state data and the ones who did have this capability typically provided it only in some sort of statistical analysis. Finally, and probably most disturbing, is that almost half the systems did not provide primary notification of alerts to users. This is very discouraging as effective ID depends on real-time alerts of potential attacks.

CONCLUSION

In this paper we have presented an organizing structure for designing ID visualization systems, incorporating the operational imperatives of contemporary user-based and input-based visualization schemes, and then aligning these operational imperatives with a modified component-based structure taken from IV theory. The component-based structure was specifically developed using a combination of Shneiderman's (Shneiderman et al., 2005) IV component delineation and Few's (Few, 2006) Information Dashboard role-based categorizations (specifically, the operational category). The resulting structure combined common IV components with urgency-based components, to best meet the requirements of ID systems. Finally, a survey of 23 different ID visualization research projects was conducted to evaluate the applicability of the above structuring system.

FUTURE WORK

This article provides several avenues for future research. First, the above delineation of a component-based structural framework setup for IV has only been discussed here with regards to ID visualization systems. The author's believe this same organizing approach can potentially be applied to IV systems in other fields, but greater testing is needed. Additionally, our literature review provides corroboration that past research in ID visualization systems have employed some or all of the components described in the sub-framework, albeit not in a comprehensive system. Greater research needs to be undertaken to actually develop a system that fully embraces the advantages of the component-based system that we describe, and examine the utility and practicality of such a system in production.

ACKNOWLEDGEMENTS

We would like to thank Dr. A.B. Schwarzkopf of the University of Oklahoma for his constructive comments regarding the development of the component-based sub-framework. We would also like to thank Dr. Kenneth Kozar and Dr. Gerald R. Wagner for their help with background material. Also, thanks to Dr. Derrick Parkhurst who helped to initiate interest in this research.

REFERENCES

Abdullah, K., Lee, C., Conti, G., & Copeland, J. A. (2005). Visualizing network data for intrusion detection. In Proceedings from the Sixth Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005., pp. 100 - 108, Georgia Inst. of Technol., WA, 15-17 June 2005.

Abdullah, K., Lee, C., Conti, G., Copeland, J. A., & Stasko, J. (2005). IDS rainStorm: visualizing IDS alarms. In IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05), pp. 1-10, Minneapolis, MN, Oct. 26, 2005.

Ball, R., Fink, G. A., & North, C. (2004). Home-centric visualization of network traffic for security administration. In Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, pp. 55 - 64, Washington DC. ACM Press.

Cañas, A. J., Carff, R., Hill, G., Carvalho, M., Arguedas, M., Eskridge, T. C., et al. (2005). Concept Maps: Integrating Knowledge and Information Visualization. In *Lecture Notes in Computer Science* (Vol. 3426, pp. 205-219): Springer Berlin / Heidelberg.

Card, S. K., Mackinlay, J., & Shneiderman, B. (1999). *Readings in Information Visualization: Using Vision to Think*: Morgan Kaufmann.

Chi, E. H. (2002). *A Framework for Visualizing Information* (Vol. 1). Dordrecht, Netherlands: Kluwer Academic Publishers.

Chittaro, L. (2001). Information visualization and its application to medicine. *Artificial Intelligence in Medicine,* 22(2).

Colombe, J. B., & Stephens, G. (2004). Statistical profiling and visualization for detection of malicious insider attacks on computer networks. In Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, pp. 138 - 142, 2004. ACM PressWashington DC.

Denning, D. E. (1986). An intrusion-detection model. *IEEE Transactions on Software Engineering,* 13, 222-232.

Erbacher, R. F. (2003). Intrusion behavior detection through visualization. In IEEE International Conference on Systems, Man and Cybernetics, 2003., pp. 2507-2513, Albany Univ., NY, 5-8 Oct. 2003.

Estrin, D., Handley, M., Heidemann, J., McCanne, S., Xu, Y., & Yu, H. (2000). Network visualization with Nam, the VINT network animator. *Computer,* 33(11), 63 - 68.

Fayyad, U., Grinstein, G. G., & Wierse, A. (2001). *Information visualization in data mining and knowledge discovery*. San Francisco, CA: Morgan Kaufmann Publishers Inc.

Few, S. (2006). *Information Dashboard Design: The Effective Visual Communication of Data*. Sebastopol, CA: O'Reilly Media, Inc.

Fisk, M., Smith, S. A., Weber, P. M., Kothapally, S., & Caudell, T. P. (2003). Immersive Network Monitoring. In Passive and Active Measurement Workshop Proceedings, pp. 249-258, Apr. 2003.

Foresti, S., Agutter, J., Livnat, Y., Moon, S., & Erbacher, R. (2006). Visual Correlation of Network Alerts. *IEEE Computer Graphics and Applications,* 26(2), 48-59.

Goodall, J. R. (2005). User Requirements and Design of a Visualization for Intrusion Detection Analysis. In Proceedings of the 2005 IEEE Workshop on INformation Assurance and Security, pp. 394-401, United States Military Academy, West Point, NY. IEEE.

Goodall, J. R., Lutters, W. G., & Komlodi, A. (2004). The Work of Intrusion Detection: Rethinking the Role of Security Analysts. In Proceedings of the Tenth Americas Conference on Information Systems, pp. 1421-1427, New York, NY.

Goodall, J. R., Lutters, W. G., Rheingans, P., & Komlodi, A. (2005a). Preserving the big picture: visual network traffic analysis with TNV. In IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05), pp. 47-54, Minneapolis, MN, Oct. 26, 2005.

Goodall, J. R., Ozok, A. A., Lutters, W. G., Rheingans, P., & Komlodi, A. (2005b). A user-centered approach to visualizing network traffic for intrusion detection. In Conference on Human Factors in Computing Systems, pp. 1403 - 1406, Portland, OR, 2005. ACM Press.

Hiraishi, H., & Mizoguchi, F. (2001). Design of a visual browser for network intrusion detection. In Tenth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2001. WET ICE 2001. Proceedings., pp. 132-137, Chiba, Japan, 20-22 June 2001.

Kemmerer, R., & Vigna, G. (2002). Intrusion detection: a brief history and overview. *Computer,* 35(4), 27-30.

Koike, H., & Ohno, K. (2004). SnortView: visualization system of snort logs. In Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, pp. 143-147, Washington DC, 2004. ACM Press.

Koike, H., Ohno, K., & Koizumi, K. (2005). Visualizing cyber attacks using IP matrix. In IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05), pp. 91-98, Minneapolis, MN, Oct. 26, 2005.

Komlodi, A., Goodall, J. R., & Lutters, W. G. (2004). An Information Visualization Framework for Intrusion Detection. In Conference on Human Factors in Computing Systems, pp. 1743-1746, Vienna, Austria, 2004. ACM Press.

Komlodi, A., Rheingans, P., Ayachit, U., Goodall, J. R., & Joshi, A. (2005). A user-centered look at glyph-based security visualization. In IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05), pp. 21 - 28, Minneapolis, MN, Oct. 26, 2005.

Krasser, S., Conti, G., Grizzard, J., Gribschaw, J., & Owen, H. (2005). Real-time and forensic network data analysis using animated and coordinated visualization. In Proceedings from the Sixth Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005, pp. 42 - 49, Atlanta, GA, 15-17 June 2005.

Lakkaraju, K., Bearavolu, R., & Yurcik, W. (2003). Nvisionip – a traffic visualization tool for security analysis of large and complex networks. In International Multiconference on Measurement, Modelling, and Evaluation of Computer-Communications Systems (Performance TOOLS), 2003.

Lakkaraju, K., Yurcik, W., Bearavolu, R., & Lee, A. J. (2004a). NVisionIP: an interactive network flow visualization tool for security. In 2004 IEEE International Conference on Systems, Man, and Cybernetics, pp. 2675 - 2680, Urbana, IL, 10-13 Oct. 2004.

Lakkaraju, K., Yurcik, W., & Lee, A. J. (2004b). NVisionIP: netflow visualizations of system state for security situational awareness. In Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, pp. 65 - 72, Washington DC, 2004. ACM Press.

Lau, S. (2004). The Spinning Cube of Potential Doom. *Communications of the ACM,* 47(6), 25 - 26.

Lee, C. P., Trost, J., Gibbs, N., Beyah, R., & Copeland, J. A. (2005). Visual firewall: real-time network security monitor. In IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05), pp. 129-136, Minneaplis, MN, Oct. 26, 2005.

Livnat, Y., Agutter, J., Moon, S., Erbacher, R. F., & Foresti, S. (2005). A Visualization Paradigm for Network Intrusion Detection. In Proceedings of the 2005 IEEE Workshop on Information Assurance and Security, pp. 30-37, United States Military Academy, West Point, NY, 17-19 June 2005. IEEE.

McHugh, J., Christie, A., & Allen, J. (2000). Defending yourself: the role of intrusion detection systems. *IEEE Software,* 17(5), 42-51.

McPherson, J., Ma, K.-L., Krystosk, P., Bartoletti, T., & Christensen, M. (2004). PortVis: a tool for port-based detection of security events. In Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, pp. 73 - 81, Washington DC, 2004. ACM Press.

Mukherjee, B., Heberlein, L. T., & Levitt, K. N. (1994). Network intrusion detection. *IEEE Network,* 8(3), 26-41.

Nyarko, K., Capers, T., Scott, C., & Ladeji-Osias, K. (2002). Network intrusion visualization with NIVA, an intrusion detection visual analyzer with haptic integration. In 10th Symposium on Haptic Interfaces for Virtual Environment and Teleoperator Systems, 2002. HAPTICS 2002. Proceedings., pp. 277-284, Baltimore, MD, 24-25 March 2002.

Oline, A., & Reiners, D. (2005). Exploring three-dimensional visualization for intrusion detection. In IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05), pp. 113 - 120, Minneapolis, MN, Oct. 26, 2005.

Papadopoulos, C., Kyriakakis, C., Sawchuk, A., & He, X. (2004). CyberSeer: 3D audio-visual immersion for network security and management. In Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, pp. 90 - 98, Washington DC, 2004. ACM Press.

Proctor, P. E. (2001). *The practical intrusion detection handbook*. Upper Saddle River, NJ: Prentice-Hall.

Ren, P., Gao, Y., Li, Z., Chen, Y., & Watson, B. (2005). IDGraphs: intrusion detection and analysis using histographs. In IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05), pp. 39-46, Minneapolis, MN, Oct. 26, 2005.

Shneiderman, B., & Plaisant, C. (2005). *Designing the User Interface* (4th ed.): Pearson Education, Inc.

Snapp, S. R., Brentano, J., Dias, G. V., Goan, T. L., Heberlein, L. T., Ho, C.-L., et al. (1996). DIDS (distributed intrusion detection system) - motivation, architecture, and an early prototype. In Proceedings of the 19th National Information Systems Security Conference, pp. 361-370, October 1996.

Takada, T., & Koike, H. (2002a). MieLog: A Highly Interactive Visual Log Browser Using Information Visualization and Statistical Analysis. In Proceedings of LISA '02: Sixteenth Systems Administration Conference, pp. 133-144, Berkeley, CA, Nov. 3-8, 2002.

Takada, T., & Koike, H. (2002b). Tudumi: information visualization system for monitoring and auditing computer logs. In Sixth International Conference on Information Visualisation, 2002. Proceedings., pp. 570-576, Japan, 10-12 July 2002.

Wright, W. (1997). Business visualization applications. *IEEE Computer Graphics and Applications,* 17(4), 66-70.

Xin, J., Dickerson, J. E., & Dickerson, J. A. (2003). Fuzzy feature extraction and visualization for intrusion detection. In The 12th IEEE International Conference on Fuzzy Systems, 2003. FUZZ '03., pp. 1249-1254, Ames, IA, 25-28 May 2003.

Yin, X., Yurcik, W., Treaster, M., Li, Y., & Lakkaraju, K. (2004). VisFlowConnect: netflow visualizations of link relationships for security situational awareness. In Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, pp. 26 - 34, Washington DC, 2004. ACM Press.

SIDEBAR

The component-based model contains eight categories that delineate specific visual components and interaction mechanisms exemplified in the literature. These components are further corroborated by their inclusion in at least one of all the reviewed products (with the least included still existing in roughly one-third of the products). Sidebar Figure 1 shows a count of products per category. It is tempting to interpret prioritization of categories is Sidebar Figure 1, but is misleading. For example, while most products have an overview feature, it may not be because that category is considered more important than the others but because it may be the simplest to provide. Then again, it may be the most important feature. A very interesting study would be to determine the relative importance of each category to those using these types of systems.

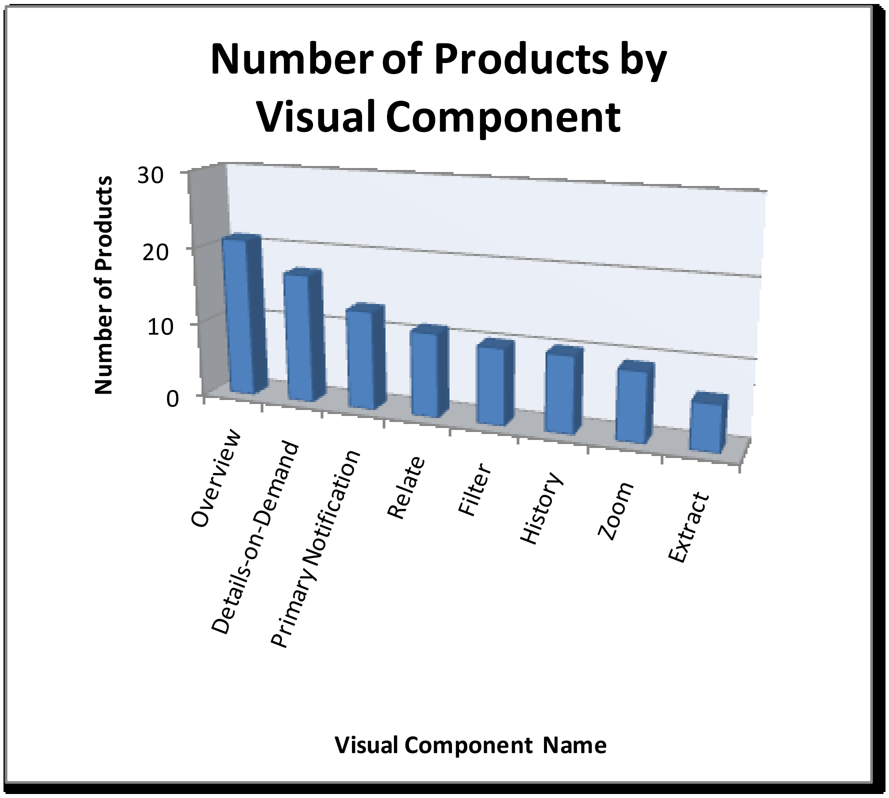


Figure 5: Sidebar 1

Sidebar Figure 2 provides a ranking of the products according to the number of components each possesses. As is with the first graph, this is only an initial assessment of the “best” product, and future work should investigate better delineations of the ranking of the components in the model and thereby the products which contain these components.

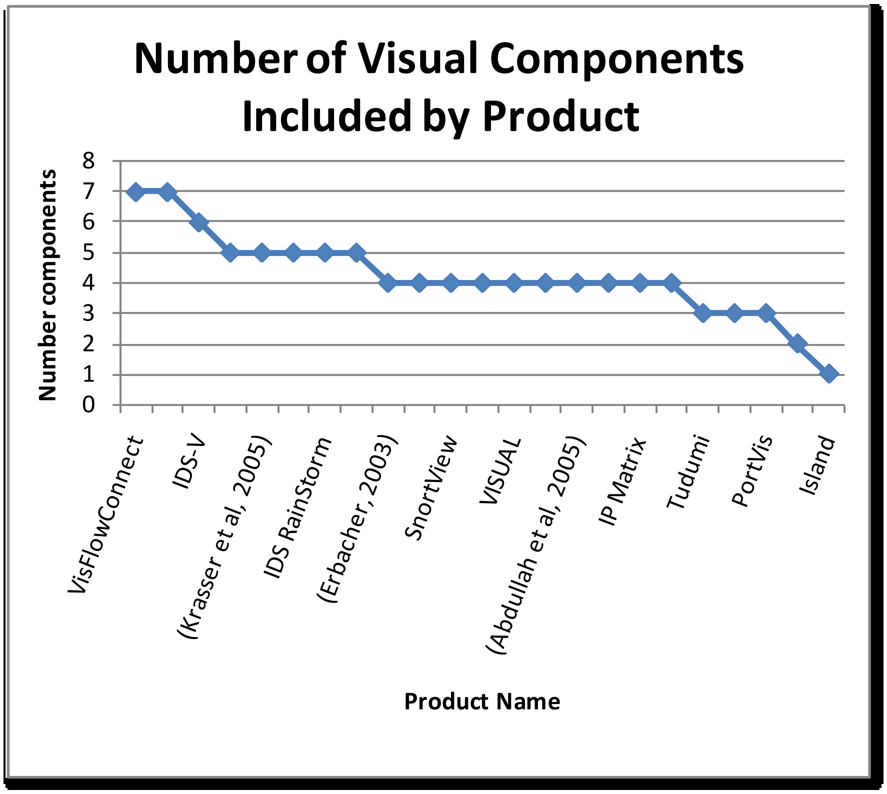


Figure 6: Sidebar 2

CHAPTER 3: CDCVIS: A CONFIGURABLE VISUALIZATION MECHANISM FOR CORPORATE NETWORK SECURITY ADMINISTRATION

Modified from a paper currently being revised for submission.

Andy Luse[2], Brian Mennecke, Nate Karstens, Doug Jacobson

ABSTRACT

Corporate network security administration is a never-ending balancing act for network administrators straddling the line between information protection and availability. The constant increase in informational needs, speed, and sharing coupled with the proliferation of more advanced attacks, provides a daunting workload for most network security administrators. The objective of this paper is to alleviate the task of network security administration through the development of a novel, modular, plug-and-play, information visualization system for network security. A design science research paradigm is utilized whereby the visualization product is planned, designed, developed, deployed, and evaluated. A pseudo-corporate environment and analogous target population are provided using cyber defense competitions as a production test bed. These competitions provide fodder for system enhancements as well as a user population for more formal tests of usefulness and usability of the developed system.

[2] I performed the primary portion of the manuscript preparation and also completed a good portion of the development of the product utilized for the research.

KEYWORDS

network administration, computer and network security, information visualization, cyber defense competition, design science

INTRODUCTION

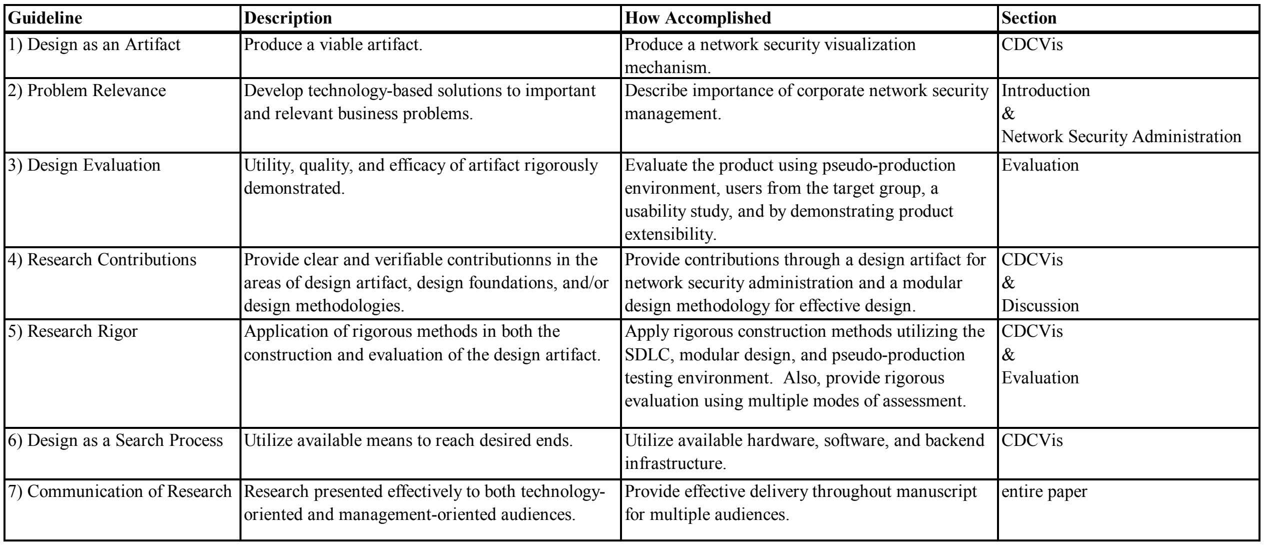
Informational needs of organizations as well as their social nature require that organizations process information (Mackenzie 1984). Also, due to information needs both within the corporate structure as well as between partners, customers, and other external entities, information must be shared (Daft et al. 1986) and this sharing forms the basis of all organizational activity (Barrett et al. 1982). The above two requirements of information need and information sharing along with shrinking time requirements require the use of modern digital networks for exchanging this information.

Information Assurance involves all aspects of information, particularly focused on insuring that information is where you want it, when you want it, in the condition you need it, and readily available to those who should have access to it (Blyth et al. 2001). This has typically been thought of with regards to the CIA model, specifically *Confidentiality*, *Integrity*, and *Availability* (Denning 1999). Various types of information, both good and bad, are flowing in, out, and through the corporate network. The challenge is to protect corporate information from attackers, both internal and external, who wish to compromise this data.

Network security has increased in importance within the past decade as the need for effective network security administration has become a critical factor in the overall health of a business. Network security administration aims to deter, prevent, detect, and correct security violations to transmitted data (Stallings 2005). Many forms of corporate security administration are necessary; for example, firms need to manage everything from host-based security to securing the corporate Internet gateway (Kaeo 2003). Of great importance is the detection of computer misuse to allow for responsive action, or intrusion detection (Denning 1987; Proctor 2001). Traditionally, researchers have looked for more effective methods for intrusion detection (Lippmann et al. 2000; Northcutt 1999; Zhu et al. 2001) as even a 1% false alarm rate can inundate administrators with unmanageable amounts of data (Durst et al. 1999).

Information Visualization has recently been explored as a means for reducing false alarms with regards to intrusion detection and more broadly, network security (Luse et al. 2008). Information visualization research for intrusion detection attempts to utilize the parallel processing power of the human vision system (Breitmeyer 1992) for analysis of network events. Network administrators are able to utilize these information visualization dashboards to allow for better decision-making with regards to potentially nefarious activity on their network. While many different programs have been developed, very few multi-module visualization systems for network security have been created where multiple visualization components can be utilized for evaluation of network activity. Furthermore, very little research has been conducted to test these systems, especially in production scenarios by individuals planning a career in network security and administration.

Design science allows researchers to develop new artifacts to solve existing problems (Hevner et al. 2004). Design science research has received a great deal of notice as a viable research method (Hevner et al. 2004; March et al. 1995; Walls et al. 1992), but researchers in the IS field have only recently begun to utilize this technique. Hevner posits that effective design science research will incorporate seven guidelines which are listed in Table 1 (Hevner et al. 2004). These guidelines provide a basis for development of the artifact as well as methods for rigor with regard to the problem and research. The research here utilizes all seven guidelines and this manuscript is designed to address each point. Table 1 provides the name of each guideline, a short description of the guideline, a small explanation as to how the guideline is addressed for this research, and the respective section(s) of the manuscript which address(es) each guideline.



Guideline	Description	How Accomplished	Section
1) Design as an Artifact	Produce a viable artifact.	Produce a network security visualization mechanism.	CDCVis
2) Problem Relevance	Develop technology-based solutions to important and relevant business problems.	Describe importance of corporate network security management.	Introduction & Network Security Administration
3) Design Evaluation	Utility, quality, and efficacy of artifact rigorously demonstrated.	Evaluate the product using pseudo-production environment, users from the target group, a usability study, and by demonstrating product extensibility.	Evaluation
4) Research Contributions	Provide clear and verifiable contributionns in the areas of design artifact, design foundations, and/or design methodologies.	Provide contributions through a design artifact for network security administration and a modular design methodology for effective design.	CDCVis & Discussion
5) Research Rigor	Application of rigorous methods in both the construction and evaluation of the design artifact.	Apply rigorous construction methods utilizing the SDLC, modular design, and pseudo-production testing environment. Also, provide rigorous evaluation using multiple modes of assessment.	CDCVis & Evaluation
6) Design as a Search Process	Utilize available means to reach desired ends.	Utilize available hardware, software, and backend infrastructure.	CDCVis
7) Communication of Research	Research presented effectively to both technology-oriented and management-oriented audiences.	Provide effective delivery throughout manuscript for multiple audiences.	entire paper

Table 4. Design Science guidelines and how each is addressed in this manuscript.

The intention of this work is to provide a new technical approach to cyber security and information assurance by alleviating the strain of network security administration for administrators of corporate networks through information visualization. This will be accomplished using design science methodologies through the development, deployment, and evaluation of an information visualization mechanism for more effective network security administration. We conclude with a discussion of the implications of the research and future research in the area.

NETWORK SECURITY ADMINISTRATION

Network security administration refers to any personnel responsible for the design, implementation, and/or maintenance of security services for a network infrastructure (Kaeo 2003). This management is a daunting task as attacks are becoming more sophisticated and technically complex (Verma 2002). Also, the threat of monetary loss from security incidents continues to increase. In 2007 alone, the average annual losses reported per corporate entity from computer and network security related events increased to over $350,000 (Richardson 2007). Furthermore, the number of connections between disparate groups within the organization, remote users, business partners, and customers, puts a large burden on those in charge of security management (Dhillon et al. 2000).

The need for trained network security administrators by corporations and government entities is increasing at an exponential rate. This is evident by the various security certifications which have become well-known including the CISSP (Certified Information Systems Security Professional) certification and the CompTIA Security+ certification. Also, the NSA began designating Centers of Academic Excellence in Information Assurance Education in 1999 in response to Presidential Decision Directive 63 calling for the training of individuals to protect the US critical network infrastructure (DOJ 1998). Seven schools initially received the designation in 1999, but this number has risen to 87 schools in 2007, due to market needs (NSA 2008).

As the area has matured, various methods and products have been introduced to help alleviate the strain on network security administrators and better enforce network security (Stallings 2006). Intrusion Detection systems are one such mechanism for automating the task of detecting possible network attacks (Denning 1987). These systems, while somewhat effective, produce high rates of false alarms thereby bogging down an already overworked network administrator (Koike et al. 2005). Also, these systems provide only one view of the overall network security health. Finally, as the systems are primarily automated in nature, the administrator does not receive a personal "view" of the overall status of network activity, and very little decision-making capacity with regard to traffic is given to him or her.

Recently, information visualization techniques have been looked upon as a valid mechanism for enabling more effective network security (Luse et al. 2008). Information visualization theory (Shneiderman et al. 2005) has enabled the effective design of such systems. The problem with this research is that it does not offer an overall network administration tool for effective network security. Also, very little research has been conducted to evaluate the usefulness and usability of such systems in actual production environments. For effective network administration, an operational visualization dashboard is needed. These dashboards are currently used in government facilities and manufacturing production (Few 2006), but no exploration has been conducted on their use by network administrators for network security administration activities.

DESIGN SCIENCE

Design science is one side of a two-sided coin for acquiring knowledge in IS research, the other being behavioral science (Hevner et al. 2004; March et al. 1995). Design science comes from the engineering or applied reference disciplines within IS (Baskerville et al. 2002; Culnan 1987; Simon 1996). These reference disciplines, in addition to research in MIS, have provided the necessary groundwork and knowledgebase from which products can be designed, built, and implemented. The design science paradigm seeks to solve problems through the creation of innovations and technically capable products which accomplish a specific information system task (Denning 1997; Tsichritzis 1998).

Design science has been called upon extensively as a viable and needed research method in IS. Design science seeks to develop systems, or IT artifacts, which have been called the core subject matter of the IS field and which have not been adequately utilized (Orlikowski et al. 2001). Design science research involves both theories and instantiations, where the theories explain how artifacts are created and adapted to their environment (Weber 2003). The instantiations are the actual artifacts which are used to solve a specified problem existing in the field.

Two primary processes and four artifact types are identified by March and Smith (March et al. 1995). The processes include both building the artifact and evaluating the artifact once built. The types of artifacts can include constructs, models, methods, and instantiations. The first three artifacts are primarily less concrete in nature as compared to instantiations. These instantiations typically involve some type of system building and subsequent analysis of the system. One problem with instantiations is deciding whether they fall into a category of system building as opposed to design science. System building involves applying existing knowledge to an organizational problem whereas design science research deals with unsolved problems in unique or inventive ways or solved problems more efficiently (Hevner et al. 2004).

The following research approaches the problem of network security administration using an innovative visualization mechanism. This mechanism involves an instantiation of a novel security visualization system built on information visualization theory which has been tested multiple times by individuals in pseudo-corporate, production environments. The research follows the outline set forth by Hevner and his colleagues for effective design science research (2004).

CYBER DEFENSE COMPETITIONS

Cyber Defense Competitions (CDCs) offer real-world environments for instruction and evaluation of students and practitioners in computer and network security. These competitions offer the opportunity for individuals to test their network security skills in a simulated corporate IS infrastructure (Conklin 2006; White et al. 2005). Competitions also increase awareness and understanding of security exploits, tools, and countermeasures in the rapidly changing network security environment (Jacobson et al. 2006). Competitions allow participants to utilize skills and theories learned in the classroom in a live setting (Hoffman et al. 2004).

CDCs offer a form of active learning where participants are allowed to experiment with network security concepts in a trial and error manner (Riding et al. 1998). This type of exercise has been shown to be an effective method for learning information security concepts centered around management of security in a business setting (Conklin 2006). The exercise offers a form of enactive mastery (Bandura 1986) where the participants are able to personally implement network security concepts they have learned in class.

Competence-based education has been a topic of debate for many years and regards performance as the assessment of education focusing on outcomes as opposed to learning processes (Burke 1989). While debates have arisen around competence-base education, some areas require competence more than others. For example surgeons, while definitely requiring learning processes, need to possess competence at outcomes with regard to their patients. Network security professionals also need to have competencies as they are required to effectively defend and protect a corporate network. CDCs provide an effective method for developing these needed competencies while also utilizing learning processes participants have acquired from more traditional studying methods.

CDCs are growing in popularity as a viable method for effectively teaching network security administration concepts. Various types of CDCs have been developed across the US. These competitions have ranged from small internal competitions (Chamalese et al. 2004; Jacobson et al. 2006) and those involving a select subset of institutions (Dodge et al. 2004; Schepens et al. 2002; Schepens et al. 2003) to competitions spanning many universities covering a large geographical area (Vigna 2003a; Vigna 2003b). These competitions vary in their methods, but typically involve a group of individuals trying to protect their respective network from another group of individuals attempting to attack this network. These competitions allow individuals to test their security skills in a controlled yet "real-world" environment.

The CDC utilized as a test environment for this research has been implemented at a large Midwestern public university in the US (Jacobson et al. 2006). The competition consists of 4 primary teams designated using color associations (see Fig. 1). These include the blue, green, red, and white teams described below.

- Blue Team: Each blue team consists of between 4 and 8 students. These are the participant teams and are tasked with running their own pseudo-company network. This involves providing services to users – including email, file storage, shell access, and maintaining a corporate web presence – all while defending their network from attack.
- Green Team: This team consists of users of the services provided by the Blue Teams. Each Blue Team provides the Green Team with the credentials necessary to access the services available on their respective network. The Green Team members act as users of the Blue Team systems and therefore measure system usability.
- Red Team: The Red Team consists of personnel tasked with attacking the Blue Team networks. These individuals can use almost any means necessary to compromise the Blue Team systems. An important note is that the Red Team is located in a separate physical area and has no interaction with either the Green Team or any of the Blue Teams.
- White Team: The White Team acts as administrators for the competition as a whole. They provide assistance to all the teams as well as a middle-man if any interaction is needed between the Red Team and any other participating team. Each Blue Team can also submit reports to the White Team detailing any type of nefarious activity which has occurred on their network (aka, the Red Team) and the actions they performed to mitigate or correct this activity. This allows the Blue Teams to earn points back which they may have lost due to actions taken by the Red Team and also provides a chance for the Blue Teams to learn from attacks which have taken place against their network.

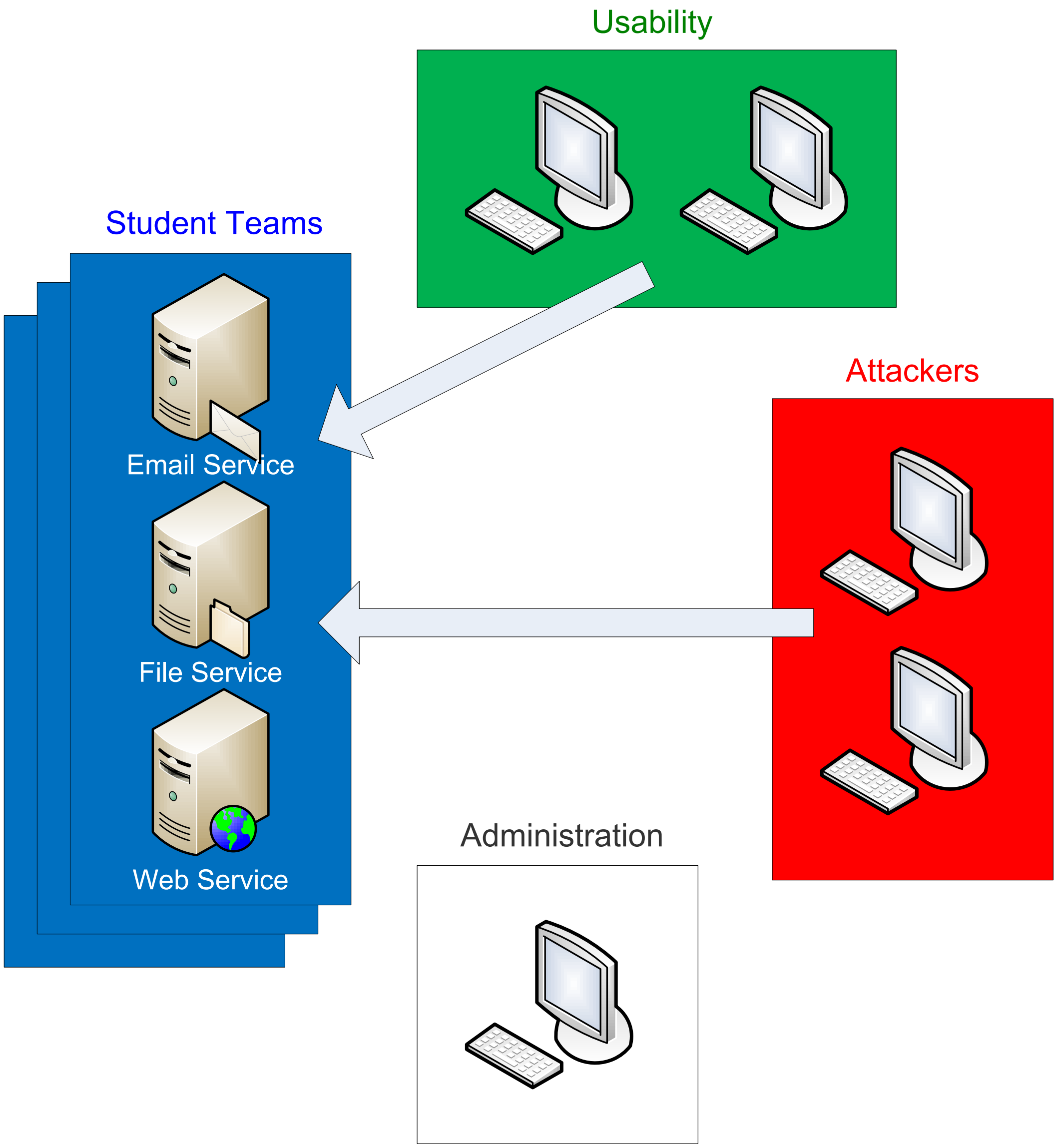


Figure 7. Team layout for Cyber Defense Competition evaluation mechanism (CDC).

The competition itself typically lasts for 8 to 16 hours. The Blue Teams are given a set amount of time to setup their machines using remote services (typically around a month) and are allowed to come in one day early to perform more setup before the competition begins. The competition has been run as either an all-day event or an overnight event to simulate prime attacking hours. Several competitions have been run including 5 involving student groups from the sponsoring university, 2 involving student groups from state community colleges, 3 involving student groups from several different colleges and universities, and 3 involving high school student groups.

CDCVIS

CDCVis (Cyber Defense Competition Visualization) is a visualization system designed for cyber defense competitions. The system utilizes elements designed for visualization of network traffic and visual analysis of current network activity. These elements are designed using both traditional information visualization theory and visualization mechanisms suited to the specific requirements of network security (Luse et al. 2008; Shneiderman et al. 2005).

Development

The development of CDCVis has followed the classic Systems Development LifeCycle (SDLC) waterfall methodology (Royce 1970) involving a team of individuals. Each stage of the SDLC is listed below along with the actions taken.

- **System Requirements**: The design team first met with the coordinators of the CDCs where the system would be used. The coordinators gave their requirements for what the system should provide both to the competitors as well as the coordinators and workers. Rough ideas were also given as to the types of visualization mechanisms the system should contain. After this, the design team met to discuss what type of hardware would be needed to support this proposed system. The initial prototype consisted of two machines, each running separate visualization elements. The final system consists of a single machine which contains 3 high-end graphics cards capable of supporting 6 separate screens.

- **Software Requirements**: After meeting with the event coordinators, the design team set about deciding on the software to be used for the system. Team members gathered information with regards to the programming language, the programming environment (IDE), the graphical library, and the backup and dissemination mechanism. Java was decided upon as the programming language due to the ease of object oriented and class-based programming for a multi-programmer team project. Eclipse was then chosen as the IDE for its easy integration with Java and also its built-in CVS (content version system) capabilities. OpenGL was selected as the graphical library due to its high market use and standardization. More specifically JOGL, the java library for OpenGL was employed. Finally, CVS was chosen as the backup, versioning, and content dissemination system for use by the design team during development.
- **Analysis**: The team again met with the event coordinators to get a better understanding of the requirements. Specifically, discussions with regard to each stakeholder for the system took place including each type of team (blue, green, white, red) as well as outside supporters of the competition and other random observers. More detailed visualization requirements were also discussed.
- **Program Design**: The program design phase involved a highly iterative approach. Members of the design team first sketched representations for visualization mechanisms they envisioned for the system. From these initial sketch-ups, a specific

subset was decided upon and more detailed electronic drafts for each component were made. After the individual components had been finalized, more elaborate electronic screen mockups were developed showing possible aggregations of the individual components.

- **Coding**: Coding for the project took a highly object-oriented approach with many levels of inheritance for the visualization components and other pieces of the system. First, the various visualization components and other proposed pieces were broken up into classes. Each member was then given a certain subset of classes for which he/she was responsible for delivering.
- **Testing**: Testing consisted of "plugging" the visual components into the container class designed for the overall CDCVis system. Various combinations were used as well as various aggregations of information within each. Also, traffic simulations were run to verify that the system was adequately capturing and displaying the information which it was supposed to.
- **Operations**: Finally, the system was utilized at a number of CDCs. Valuable information has been gathered at each CDC and various changes have been made along the way by reusing the above process. These changes have included both a new traffic capture mechanism as well as new visualization modules.

Project Components

CDCVis consists of various components which were developed using the above methodology. These components include both visualization mechanisms and other needed components for the operation of the system. These components can be aggregated into two overarching categories described below: information capture/categorization and information dissemination.

Information Capture/Categorization

The purpose of the system is to allow individuals to make better decisions about their network security configurations based on the visualization of traffic. To make these decisions, traffic must be captured and categorized accordingly. The network is setup so that all traffic runs through a primary hub where traffic capture can be implemented. The first implementation of CDCVis used a third party capture program to gather and categorize network traffic information. This information was then sent to the visualization machine for display purposes. It was decided that this configuration was not optimal due to the low configurability of the proprietary program and network and program latency issues. The second iteration provided a module directly built into the program. This module uses jpcap, the java implementation of the popular WinPcap network data capture library (WinPcap 2008) for capturing all data on the utilized network.

Once the traffic has been captured, it must be evaluated as to its use in the system. This involves a number of steps based on the individual visualization mechanism utilizing the information. First, the information is divided into traffic which is destined to or coming from each participating blue team. Second, the traffic is categorized based on the type of traffic it represents. This is dependent on the visualization mechanism, as some do not categorize by traffic type, but the primary categorizations consist of five traffic types (described in more detail below): Web, File Transfer, Email, Shell (Terminal), and Other.

Information Dissemination

After the relevant network traffic information has been gathered and categorized, this information must be made available to the user to help in decision-making. All the visualization components are derived from a top-level abstract *Visualization* class. This class allows all the visualization modules to easily inherit specific attributes and pass information between all these visualization mechanisms.

A modular approach was taken with regards to the overall visualization method. Each visualization mechanism was coded as a separate module in its own class. These modules could then be placed anywhere on the screen of the overall visualization system. This provided a very unique and adaptable system whereby the programmer can setup the environment specific for each CDC by mixing, matching, and arranging the various visualization components as desired.

The design of each network traffic visualization module was also based on Information Visualization (IV) theory. Specifically, Shneiderman and Plaisant's delineations were used as components necessary for effective IV. Also, components from the real-time imperative of intrusion detection visualization were utilized (Few 2006; Luse et al. 2008). Table 2 provides a listing of these components as well as each of the CDCVis visualization modules which utilize each respective component. As this visualization system is utilized and tested in a competition-based, multiuser environment, no interaction with the system is permitted by the Blue Team members and therefore none of the components allow for zoom or details-on-demand.[3]

[3] While the Blue Team members are not allowed to control zoom or details-on-demand, the administrators are allowed such access, just as a network security administrator would be allowed such access. Greater explanation on this is given below.

Components	CDCVis Visualization Module					
	Composite Bar Graph	NetSquall	Island	Bargraph (Team)	NetQuall (Team)	Map
Overview	x	x	x			x
Zoom						
Filter				x	x	
Details-on-demand (Secondary Throughput)						
Relate						x
History		x	x		x	
Extract	x			x		
Primary Notification	x	x	x	x	x	x

Table 5. CDCVis modules and the respective ID information visualization components they address.

System Explanation

The current system was developed for use during CDCs (Jacobson et al. 2006). This includes students from both high school and college, including community college through graduate students. The system is designed to disseminate two primary types of information: information pertaining to network traffic and competition-specific data. Within these 2 categories, two aggregations of information are used; team-based information is relevant for a specific team while global information is a combination of information for all teams in the competition (see Table 3).

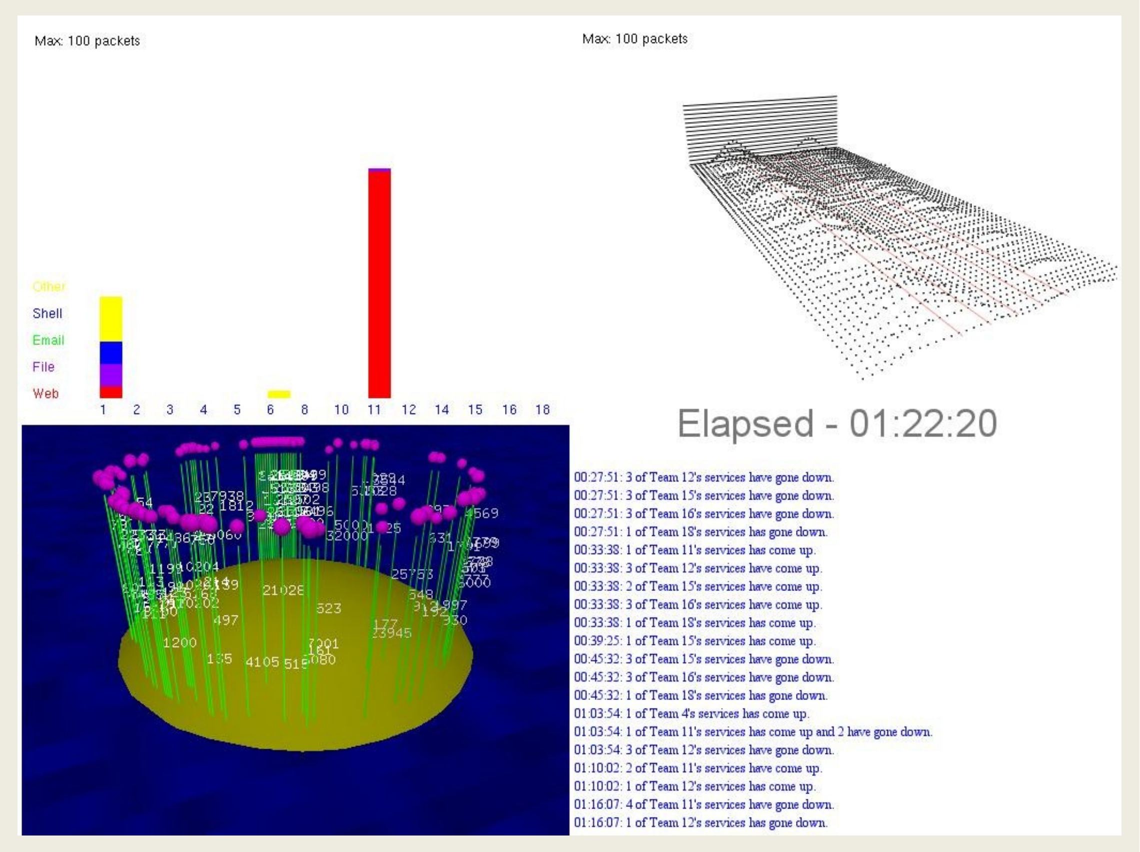
		Information Types	
		network traffic	competition-specific
Aggregation	team-based	traffic visualization components for an individual team	competition information for an individual team
	global	traffic visualization components for all teams in the competition	competition information for all teams in the competition

Table 6. Explanation of CDCVis information types by aggregation method.

The overall visualization system for the CDC is delineated by two views which encompass the two main aggregations within the competition. The following explanations are categorized by these two overarching views, while each component within each view is a separate modularized element.

Global View

The global view provides a composite view of the network which includes information and traffic pertaining to all Blue Teams involved. The following screen capture provides an example of the global view (Figure 2). The view is composed of the following visualization components from left to right, top to bottom: Composite Bar Graph, NetSquall, Island, and Announcements.



```
00:27:51: 3 of Team 12's services have gone down.
00:27:51: 3 of Team 15's services have gone down.
00:27:51: 3 of Team 16's services have gone down.
00:27:51: 1 of Team 18's services has gone down.
00:33:38: 1 of Team 11's services has come up.
00:33:38: 3 of Team 12's services have come up.
00:33:38: 2 of Team 15's services have come up.
00:33:38: 3 of Team 16's services have come up.
00:33:38: 1 of Team 18's services has come up.
00:39:25: 1 of Team 15's services has come up.
00:45:32: 3 of Team 15's services have gone down.
00:45:32: 3 of Team 16's services have gone down.
00:45:32: 1 of Team 18's services has gone down.
01:03:54: 1 of Team 4's services has come up.
01:03:54: 1 of Team 11's services has come up and 2 have gone down.
01:03:54: 3 of Team 12's services have gone down.
01:10:02: 2 of Team 11's services have come up.
01:10:02: 1 of Team 12's services has come up.
01:16:07: 4 of Team 11's services have gone down.
01:16:07: 1 of Team 12's services has gone down.
```

Figure 8. Global View of CDCVis configured for a CDC.

Composite Bar Graph: The composite bar graph is a common 2D statistical visualization which conveys the rate of occurrence of a particular element by the height of its associated bar. Our visualization system uses the composite bar graph to display the number of packets that have been sent or received by a particular category of services, which is determined by port number and header information. The current categories of traffic used are:

1. Web – HTTP, HTTPS
2. File Transfer – FTP, SMB, NetBIOS
3. Email – SMTP, POP2, POP3, POP3+SSL, IMAP4, IMA4+SSL
4. Shell (Terminal) – Telnet, Telnet+SSL, SSH
5. Other

The composite bar graph allows all the above 5 types of traffic to be viewed using various colors all within a single bar. Each bar then represents the amount of the 5 types of traffic originating from or destined for a particular Blue Team (numbered along the bottom of the graph).

NetSquall: Like the composite bar graph, NetSquall (see Figure 3) provides a statistical graph with heights representing the number of packets for each of the 5 traffic types above, while adding a history component to indicate trends in network usage. The values for the five traffic types are plotted in space and connected with a B-spline curve, with three points on either end of the curve to act as anchors for the resulting curve. The display is updated with a new wave every 50 milliseconds, with a total of 82 curves (4.1 seconds) displayed at once. Old curves are pushed towards the horizon.

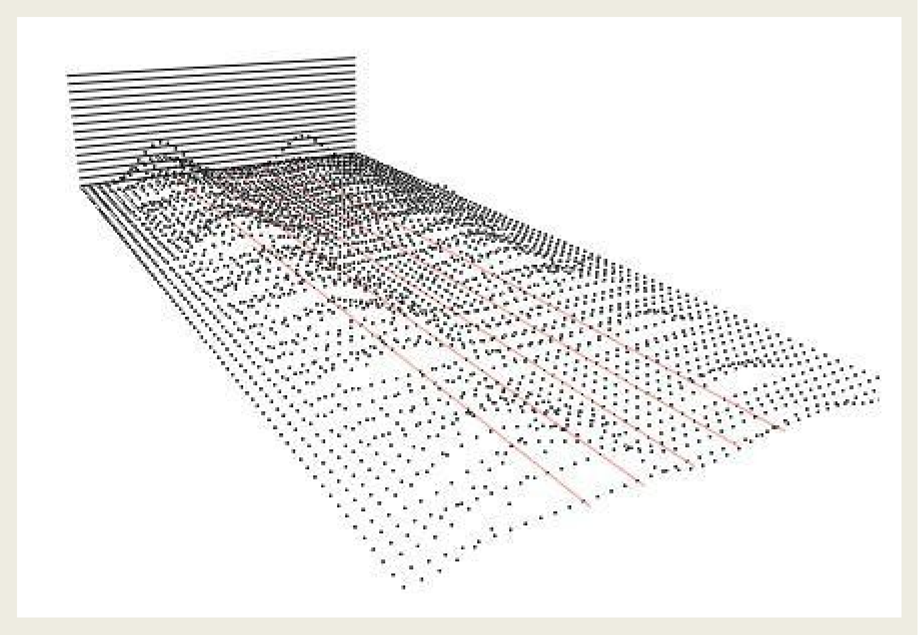


Figure 9. NetSquall visualization module.

Island: The Island visualization provides a unique 3D view of current traffic on the network. The system was developed by Oline and Reiners as a 3D method for analyzing traffic on a network (Oline et al. 2005). The system resembles an island with trees growing up from it. The positions of the trees correspond to the ports which have traffic on them. The ports start at the outside of the island with 1 and increase, spiraling towards the center. The smaller, and typically more used, ports are given a greater area of coverage as opposed to the less used upper ports. Each tree also contains a fruit on top whose respective size indicates the amount of traffic on the respective port (see Figure 4).

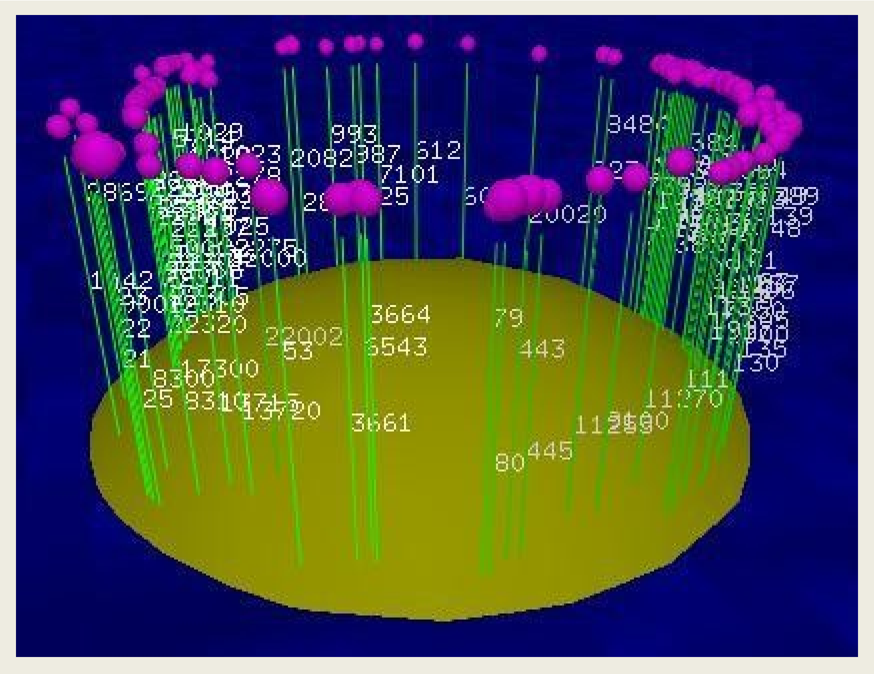


Figure 10. Island visualization module (Oline et al. 2005).

Announcements: The announcements portion provides users with various pieces of information which they may find useful throughout the competition. Also, a time clock is included showing the time elapsed in the competition. With the various expected as well as unexpected events that occur during the course of a CDC, providing a means for announcements allows this information to be disseminated to all parties involved.

Map: Another component which was added after initial user evaluation of the system (described below) is the map. This item is contained in a separate view and contains a visual representation of network traffic by drawing lines to and from the participating teams to the network hub. This is, of course, an unreal representation of distance as teams are all located in the same geographical area during the competition, but allows for an alternate view of traffic patterns over the network (see Figure 5).

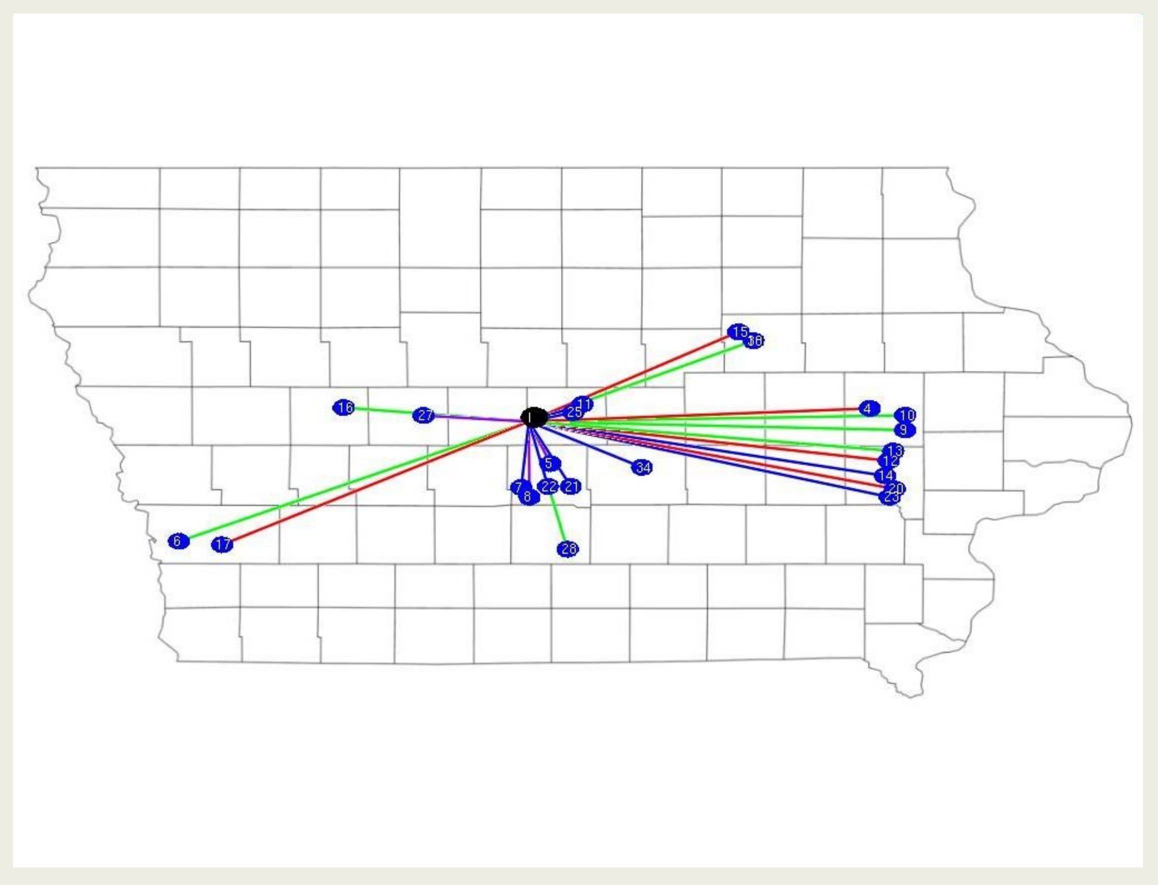
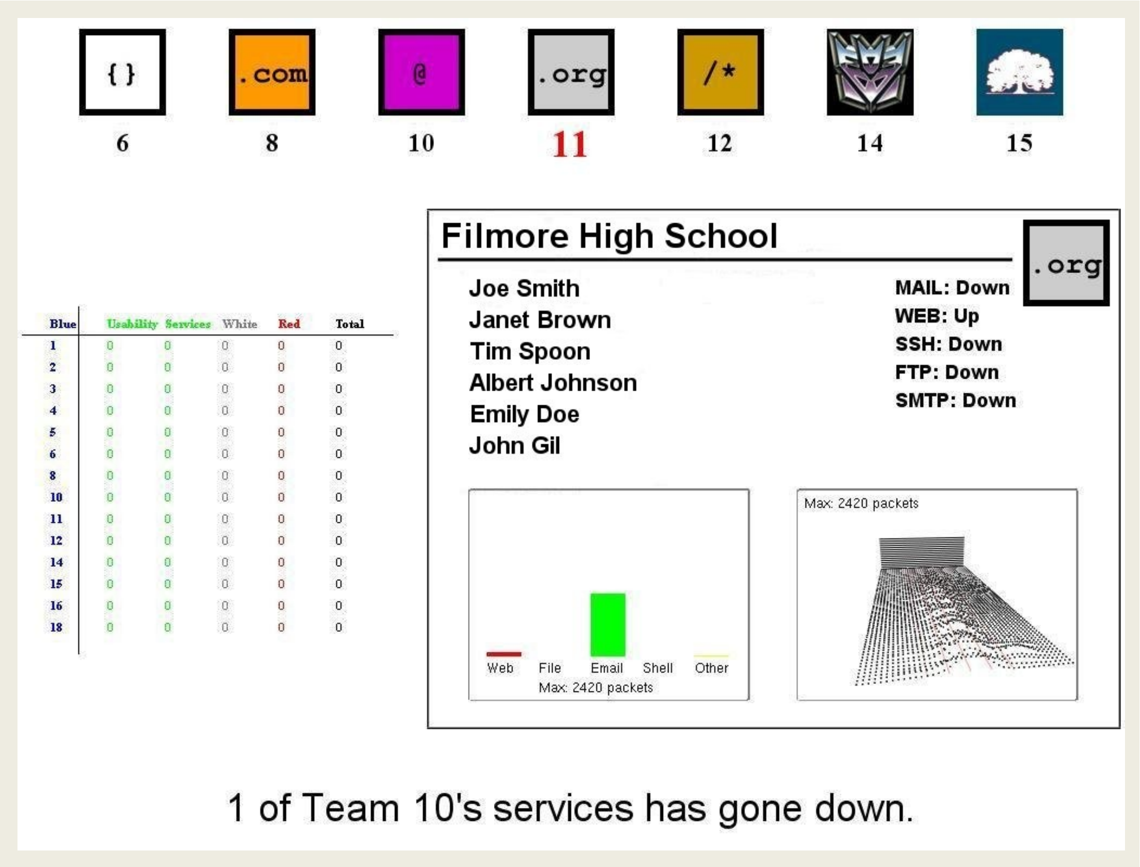


Figure 11. Map-based CDCVis visualization module.

Team View

The team view primarily provides information and current traffic patterns pertaining to a specific Blue Team. The visualization is setup on a timer to switch between teams every predefined time interval. The scoreboard is the exception to this view, as it shows the scores for all teams involved in the competition. The following screen capture provides an example of the team view (Figure 6). The view is composed of the following visualization components from left to right, top to bottom: Team Logo Strip, Scoreboard, Team Information Panel, and the Announcement Strip.



Blue	Usability	Services	White	Red	Total
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0
5	0	0	0	0	0
6	0	0	0	0	0
8	0	0	0	0	0
10	0	0	0	0	0
11	0	0	0	0	0
12	0	0	0	0	0
14	0	0	0	0	0
15	0	0	0	0	0
16	0	0	0	0	0
18	0	0	0	0	0

Filmore High School

Joe Smith
Janet Brown
Tim Spoon
Albert Johnson
Emily Doe
John Gil

MAIL: Down
WEB: Up
SSH: Down
FTP: Down
SMTP: Down

1 of Team 10's services has gone down.

Figure 12. Team View of CDCVis configured for a CDC.

Team Logo Strip: The team logo strip along the top provides a pictorial representation of each Blue Team which is included in the specific Team View (multiple Team Views are used for large competitions). These pictures allow the teams to choose a logo which they would like to use to designate their team. The respective team number is also included below each picture. As the Team Information Panel is cycled to view each team, the team currently being displayed has their number in the Team Logo Strip enlarged and the color changed.

Scoreboard: The scoreboard offers the Blue Teams a synopsis of their current point assessments from the various judging teams in the competition, as described above. This module features a grid-like scoreboard alignment with the number of the participating Blue Team down the left side and the judging teams along the top. The current scores from each of the 3 judging teams are provided as well as the combined total score for each team.

Team Information Panel: Each team's information is provided in the Team Information Panel on a rotating basis. The Team Information Panel is composed of various modules pertaining to the specific team currently selected.

1. Team Name: This name is used to describe the team. During the college competition, competitors are allowed to choose a name for their team. During the high school competition, the name of the specific high school is used.
2. Team Members: Each team member as well as the team sponsors (in the case of the high school competition) is listed here. For privacy concerns, the team name and member names have been removed and replaced with fake names for this paper in Figure 6.

3. Service States: Each team is expected to maintain specific services running as described above. This section provides an indication to the team as to what services are currently available to the Green Team.
4. Bar Graph: This component is a slight modification of the Composite Bar Graph in the Global View. Instead, each of the 5 traffic types described above is given its own bar with the height representing the amount of the specific type of traffic either coming from or going to the specified Blue Team.
5. NetSquall: The NetSquall is again a modification of the NetSquall used in the Global View. The traffic levels of the 5 types are still shown with a history component, but instead only the traffic pertaining to the specified Blue Team is displayed.

Announcement Strip: The announcement strip is used to display the most recent announcement from the Announcements section in the Global View so participants can see what the most current notification is.

CDCVis and Network Security Administration

While maybe not initially apparent, the correlation between CDCVis and network security administration is quite noticeable after some thought and explanation. First, the two different aggregated views correspond quite well to those needed by network security administrators. The overall view provides three different views of network traffic aggregated according to specific criteria as well as an announcement area for pressing alerts from other automated security systems. The team-based aggregations can easily be replaced by another aggregation method, such as network segment, offering overall information regarding all segments on the network. The team view, excluding the scoreboard, corresponds to a specific view of a certain segment on the network. An administrator, upon viewing suspicious activity in the overall view, can be allowed to select a specific network segment to view specific information in the team view. This functionality is currently available to the administrators of the CDC to allow them to select a specific team if this is needed. Therefore, while details-on-demand and zoom capabilities are not available to the participants of the CDC (see Table 2), this functionality is currently available in the system and can easily be implemented.

EVALUATION

The evaluation mechanisms for CDCVis have utilized various methods to assess the product development, correlation of the competition system with network security administration, as well as the usability of the system. These mechanisms have provided valuable feedback and have led to the addition and improvements of components along the way.

The first, and primary, mechanism for evaluation of the system were the actual competitions themselves. These competitions allow for a more realistic testing environment as compared to testing performed on previous information visualization network security programs. While providing actual attack data for visualization, the competitions also utilized ISEAGE (Internet-Scale Event and Attack Generation Environment) which provides an Internet-like test bed for research, complete with all the background traffic expected on the actual Internet (Jacobson 2008). This allowed the filtering mechanisms of the system to be tested with both relevant attack data and non-relevant background data. Also, the competitions allowed the system to be utilized by individuals who were planning a career in network security administration, thereby providing the target audience for the research.

While many small changes occurred due to the feedback, three will be discussed here as validation to the usefulness of the CDCs as a testing environment. During the first competition, competitors displayed an interest in knowing when their services were up or down. This typically became apparent to them after some time, but they wanted to see if users (the Green Team) were able to access their services (email, web, etc.) in a real-time manner. After discussions, the design team decided this would be a valid addition as network administrators would highly benefit from a graphical notification that a specific service was no longer accessible on the network. Therefore, service availability notifications were added to each of the individual team views (see Figure 6).

The second modification based on user feedback was the development of our own traffic capture and categorization system (described above). Many users in the first competition complained about the lag in visualization time of network traffic. Also, the built-in aggregations of the proprietary network capture system were not designed for the needs of the CDCVis system. This led to the development of our own network capture and categorization utility which offered the necessary real-time traffic capture and tailored traffic categorization for system and user needs.

The final modification was a later addition to the system. Users started to hint at a better graphical representation as opposed to the traditional statistic-based charts primarily utilized by the system. Investigations by the design team found that map-based visualization mechanisms have been shown to increase decision effectiveness and timeliness (Mennecke et al. 2000) which are both of extreme importance for network administrators for overall corporate network security. Therefore, a map-based mechanism was developed. While teams were physically present in the same area during the competition, the map placed each team on their respective school location with the location of the competition offering a visual hub for traffic flow. This modification provided a much needed component and also provided corroboration that the system could be extended with new visualization mechanisms based on user needs.

The second evaluation mechanism was to check the expandable nature of the system. The above map addition was one such evaluation mechanism, but the Island mechanism provided greater corroboration by implementing a visualization mechanism not originally developed for CDCVis. A user of the visualization system during the first deployment of CDCVis mentioned research done in the same university as the competition by another student and commented on how it would be nice to have this visualization mechanism implemented in the CDCVis system. The design team found that Oline and Reiners had published a paper on their work and we contacted them (Oline et al. 2005). Oline gave us permission to use his work and provided us with the source code. While his product had been developed using OpenGL within Python, the code was converted to Java and JOGL and successfully integrated at the second CDC where CDCVis was utilized. This, in addition to the map module, provided corroboration as to the extensible nature of the module capabilities of the CDCVis system, and assurance that future needs of network administrators could be met.

The third evaluation mechanism involved a small usability assessment utilizing current research in the area (Venkatesh et al. 2003). The purpose of the study was to measure whether the participants in the competition would be likely to use CDCVis in the future. 32 Participants from a single CDC consisting of 6 teams from 5 different universities were given a questionnaire similar to that provided by Venkatesh et al. The questionnaire was given after 7 hours of competition, which was about the halfway point. No training was given on how to use CDCVis, but participants were free to ask questions as needed. Since intention to use was the dependent variable and not actual usage, only four constructs from the original UTAUT model were utilized; specifically, *Performance Expectancy* (PE), *Effort Expectancy* (EE), *Social Influence* (SI), and *Behavioral Intention* (BI). A simultaneous multiple regression analysis was performed using BI as the dependent variable.

The results show that both PE and SI are significant at the 0.05 and 0.000 p value levels respectively, while EE is marginally significant at the 0.1 p value level. Our primary interest was with PE and EE. The significance of PE shows that these users would find CDCVis to increase their performance during a competition. This implies that as these participants are performing network security administration tasks on their pseudo-corporate networks, they find the system increases their performance for the job at hand. The extension might therefore be plausible that these same individuals would find the system increases performance when they become network security administrators in the future. While EE is only marginally significant, these findings were positively received as the participants found the effort needed to learn and operate the system minimal, even with no training on how to use the product.

	PE	**EE**	**SI**	**BI**
	(Performance Expectancy)	(Effort Expectancy)	(Social Influence)	(Behavioral Intention)
utilizing CDCVis				
n=32	9.83	10.41	8.58	7.19
	(4.35)	(4.58)	(4.37)	(4.44)
	4-items	4-items	3-items	3-items
(minimum preferred)	Min = 4, Max = 24	Min = 4, Max = 24	Min = 3, Max = 18	Min = 3, Max = 18
	α = 0.893	α = 0.931	α = 0.899	α = 0.965

Table 7. Sample size, mean, and standard deviations for study variables.

	Regression Parameters			
Outcome	***ß***	***SE***	***t***	***p***
Performance Expectancy	0.254	0.118	2.158	0.040
Effort Expectancy	0.207	0.107	1.935	0.064
Social Influence	0.566	0.120	4.733	0.000

Table 8. Summary of regression results.

DISCUSSION

Current corporate network security needs place a heavy burden on network security administrators which involves a balancing act between protection of and access to information. This can include both external attacks and insider abuse which threaten the CIA cornerstones of information assurance (Denning 1999). Digital networks and the increasing need for information sharing and rapid information transfer place even greater job loads on overextended network administrators.

Intrusion detection is being utilized with ever-increasing frequency as a means to detect possible nefarious network activity and allow for prevention or mitigation measures to be taken against the activity. Typically automated in nature, these systems suffer from high false alarm rates which lays more work on the network administrator for deciphering legitimate attacks amongst the overflow of alarms. These systems can be fine-tuned, to a degree, but the problem remains that the machine decides for which events to sound alarms and gives little initial decision-making power to the network administrator.

Information visualization has been recently researched as a means for presenting network traffic information to administrators to allow for greater decision-making effectiveness with regards to possible network attacks (Luse et al. 2008). This takes some of the decision-making authority away from the machine and brings it back to the human operator. By utilizing information visualization theory, many different visualization programs have been designed. These programs offer a visualization mechanism by which network administrators can view network traffic activity and make decisions about possible security threats. While these programs have provided much needed advancements in the area of visualization for network security, the research suffers from three primary flaws: (1) multiple visualization components are not offered to accommodate needed information according to information visualization theory, (2) the products are not utilized and tested in production-type settings, and (3) the users of the systems are not individuals within the target demographic of the product, specifically network security administrators.

This research employs a design science approach to solving the problem of network security administration in corporate environments utilizing information visualization. Also, the research aims to solve the flaws inherent with previous research in the area. First, a new system, CDCVis, has been developed to allow visualization of network traffic and events. System development followed a traditional SDLC model in a team-based environment. Various visualization modules were developed in compliance with information visualization theory to accommodate different views of information. CDCVis allows for tailoring the environment to a specific scenario and also provides extensibility for adding new modules in the future. This extensibility was tested by incorporating both a new map-based visualization mechanism as well as integrating a visualization component not originally designed for the system.

Various evaluation mechanisms were employed to test CDCVis. First, CDCVis was tested in a pseudo-production environment emulating a corporate network setting. CDCs have been shown to be an effective learning tool for network and security related concepts (Conklin 2006). This research utilized a CDC to test CDCVis by providing the system to participants in the competition. The competition provided a much more realistic test bed for CDCVis as compared to testing of previous products developed for network security visualization. The CDC included a pseudo-corporate environment on an Internet-type test bed.

Most of the previous research in the area of visualization for network security has utilized non-security individuals in non-production environments. Conversely, CDCVis has been utilized by individuals studying in the areas of network security and who plan to pursue a career in this area. The system is also utilized by actual network security administrators participating on the green, white, and red teams. The combination of the real-time testing environment with the subject pool provides greater verification as to the applicability of the system as a network security administration tool.

Feedback from the users of the system during the CDCs provided another form of evaluation. This feedback provided areas of improvement with regards to CDCVis including improved network capture and categorization, service state reminders, as well as new modules to the system. These modules provided an added form of evaluation by testing the expandable nature of the system. This included adding both a new map-based module for the system as well as a previously designed island visualization mechanism. A more standardized usability survey was also used to evaluate the usability of the system. Results showed that participants thought CDCVis would both increase their performance at performing network security administration tasks and that the system would be easy to learn.

CONCLUSIONS AND FUTURE WORK

Corporate network security administration is a highly complex job which can easily overload network administrators. Various mechanisms and research have attempted to alleviate this load. This research utilizes design science to provide a novel information visualization mechanism for network security administration. Testing of the system improves on previous research by utilizing the system in a pseudo-corporate setting within a CDC. System improvements are made utilizing user feedback.

While this research provides a much needed piece to the area of corporate network security, greater research is needed. First, testing of the system in actual production scenarios is needed. Second, greater testing is required both of a qualitative and quantitative nature. Tests are also necessary to assess actual improvements in decision-making effectiveness and timeliness with regards to network security administration when utilizing the system.

REFERENCES

Bandura, A. *Social foundations of thought and action: A social cognitive theory* Prentice-Hall, Englewood Cliffs, NJ, 1986.

Barrett, S., and Konsynski, B. "Inter-Organization Information Sharing Systems," *MIS Quarterly* (6) 1982, pp 93-105.

Baskerville, R.L., and Myers, M.D. "Information Systems as a Reference Discipline," *MIS Quarterly* (26:1) 2002, pp 1-14.

Blyth, A., and Kovacich, G.L. *Information Assurance: Surviving the Information Environment* Springer, London, 2001.

Breitmeyer, B.G. "Parallel processing in human vision: History, review, and critique," in: *Applications of Parallel Processing in Vision,* J.R. Brannan (ed.), North-Holland, Amsterdam, 1992.

Burke, J.W. *Competency Based Education and Training* Routledge, 1989.

Chamalese, G., and Pridgen, A. "The Success of the UT IEEE Communications Society," 8th Colloquium for Information Systems Security Education, 2004, pp. 9-12.

Conklin, A. "Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course," Proceedings of the 39th Annual Hawaii International Conference on System Sciences, 2006. HICSS '06, IEEE, 2006, pp. 220b-220b.

Culnan, M.J. "Mapping the Intellectual Structure of MIS, 1980-1985: A Co-Citation Analysis," *MIS Quarterly* (11:3) 1987, pp 341-353.

Daft, R.L., and Lengel, R.H. "Organizational Information Requirements, Media Richness and Structural Design," *Management Science* (32:5) 1986, pp 554-571.

Denning, D.E. "An intrusion-detection model," *IEEE Transactions on Software Engineering* (13:2) 1987, pp 222-232.

Denning, D.E. *Information Warfare and Security* Addison-Wesley, Reading, MA, 1999.

Denning, P.J. "A new social contract for research," *Communications of the ACM* (40:2) 1997, pp 132-134.

Dhillon, G., and Backhouse, J. "Information system security management in the new millennium," *Communications of the ACM* (43:7) 2000, pp 125-128.

Dodge, R.C., and Ragsdale, D.J. "Organized Cyber Defense Competitions," Proceedings of the IEEE International Conference on Advanced Learning Technologies, IEEE Computer Society 2004, pp. 768-770.

DOJ "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63," Retrieved June 29, 2008 from http://www.usdoj.gov/criminal/cybercrime/white_pr.htm.

Durst, R., Champion, T., Witten, B., Miller, E., and Spagnuolo, L. "Testing and evaluating computer intrusion detection systems," *Communications of the ACM* (42:7) 1999, pp 53-61.

Few, S. *Information Dashboard Design: The Effective Visual Communication of Data* O'Reilly Media, Inc., Sebastopol, CA, 2006, p. 211.

Hevner, A.R., March, S.T., Park, J., and Ram, S. "Design Science in Information Systems Research," *MIS Quarterly* (28:1) 2004, pp 75-105.

Hoffman, L.J., and Ragsdale, D. "Exploring a National Cyber Security Exercise for Colleges and Universities," CSPRI-2004-08 & ITOC-TR-04001.

Jacobson, D. "ISEAGE: Internet-Scale Event and Attack Generation Environment," Retrieved June 30, 2008 from http://www.iac.iastate.edu/iseage/.

Jacobson, D., and Evans, N. "Cyber Defense Competition," 2006 ASEE Annual Conference & Exposition: Excellence in Education, 2006.

Kaeo, M. *Designing Network Security*, (2nd ed.) Cisco Press, Indianapolis, 2003.

Koike, H., Ohno, K., and Koizumi, K. "Visualizing cyber attacks using IP matrix," IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05), Minneapolis, MN, 2005, pp. 91-98.

Lippmann, R., and Cunningham, R. "Improving intrusion detection performance using keyword selection and neural networks," *Computer networks* (34:4) 2000, pp 597-603.

Luse, A., Scheibe, K.P., and Townsend, A.M. "A Component-Based Framework for Visualization of Intrusion Detection Events," *Information Security Journal* (17:2) 2008, pp 95-107.

Mackenzie, K.D. "Organization Structures as the Primal Information System," in: *Management of Office Information Systems,* S.K. Chang (ed.), Plenum Publishing Corporation, New York, 1984, pp. 27-46.

March, S.T., and Smith, G.F. "Design and natural science research on information technology," *Decision Support Systems* (15:4) 1995, pp 251-266.

Mennecke, B.E., Crossland, M.D., and Killingsworth, B.L. "Is a Map More than a Picture? The Role of SDSS Technology, Subject Characteristics, and Problem Complexity on Map Reading and Problem Solving," *MIS Quarterly* (24:4) 2000, pp 601-629.

Northcutt, S. *Network Intrusion Detection: An Analysis Handbook* New Riders Publishing, Indianapolis, 1999.

NSA "Centers of Academic Excellence," Retrieved March 31, 2008 from http://www.nsa.gov/ia/academia/caeiae.cfm.

Oline, A., and Reiners, D. "Exploring three-dimensional visualization for intrusion detection," IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05), Minneapolis, MN, 2005, pp. 113 - 120.

Orlikowski, W.J., and Lacono, C.S. "Research Commentary: Desperately Seeking the 'IT' in IT Research--A Call to Theorizing the IT Artifact," *Information Systems Research* (12:2) 2001, pp 121-134.

Proctor, P.E. *The practical intrusion detection handbook* Prentice-Hall, Upper Saddle River, NJ, 2001.

Richardson, R. "2007 CSI Computer Crime and Security Survey," Computer Security Institute, 2007, pp. 1-28.

Riding, R., and Rayner, S. *Cognitive styles and learning strategies* David Fulton Publishers, London, 1998.

Royce, W.W. "Managing the Development of Large Software Systems," Proceedings of IEEE WESCON, IEEE, 1970, pp. 1-9.

Schepens, W., Ragsdale, D., and Surdu, J.R. "The Cyber Defense Exercise: An Evaluation of the Effectiveness of Information Assurance Education," *The Journal of Information Security* (1:2) 2002.

Schepens, W.J., and James, J.R. "Architecture of a Cyber Defense Compeition," IEEE International Conference on Systems, Man and Cybernetics, IEEE, 2003, pp. 4300-4305.

Shneiderman, B., and Plaisant, C. *Designing the User Interface*, (4th ed.) Pearson Education, Inc., 2005, p. 652.

Simon, H.A. *The Sciences of the Artificial*, (3rd ed.) MIT Press, Cambridge, MA, 1996.

Stallings, W. *Cryptography and Network Security*, (4th ed.) Prentice Hall, 2005, p. 592.

Stallings, W. *Network Security Essentials: Applications and Standards*, (3rd ed.) Prentice Hall, 2006.

Tsichritzis, D. "The Dynamics of Innovation," in: *Beyond Calculation: The Next Fifty Years of Computing,* P.J. Denning and R.M. Metcalfe (eds.), Copernicus Books, New York, 1998, pp. 259-265.

Venkatesh, V., Morris, M.G., Davis, G.B., and Davis, F.D. "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* (27:3) 2003, pp 425-478.

Verma, D.C. "Simplifying network administration using policy-based management," *IEEE Network* (16:2) 2002, pp 20-26.

Vigna, G. "Teaching Hands-On Network Security: Testbeds and Live Exercises," *Journal of Information Warfare* (3:2) 2003a, pp 8-24.

Vigna, G. "Teaching Network Security Through Live Exercises," 3rd Ann. World Conf. Information Security Education (WISE 3), Kluwer Academic Publishers, 2003b, pp. 3-18.

Walls, J.G., Widmeyer, G.R., and Sawy, O.A.E. "Building an Infomiarion System Design Theory for Vigilant EIS," *Information Systems Research* (3:1) 1992, pp 36-59.

Weber, R. "Editor's Comments: Still Desperately Seeking the IT Artifact," *MIS Quarterly* (27:2) 2003, pp iii-xi.

White, G.B., and Williams, D. "The Collegiate Cyber Defense Competition," Proceedings of the 9th Colloquium for Information Systems Security Education (CISSE 05), Georgia Institute of Technology, 2005, pp. 26-31.

WinPcap "WinPcap: The Windows Packet Capture Library," Retrieved June 25, 2008 from http://www.winpcap.org/default.htm.

Zhu, D., Premkumar, G., Zhang, X., and Chu, C.-H. "Data Mining for Network Intrusion Detection: A Comparison of Alternative Methods," *Decision Sciences* (32:4) 2001, pp 635-660.

CHAPTER 4: UTILIZING VISUALIZATION MECHANISMS TO IMPROVE USER PERFORMANCE DURING CYBER DEFENSE COMPETITIONS

Modified from a paper in the proceedings of the *MidWest Association for Information Systems conference (MWAIS 2009)*

Andy Luse,[4] Janea Triplett

ABSTRACT

This paper describes the development of a visualization system used by students participating in a collegiate cyber defense competition. Feedback was gathered from first-time users of the system through open-ended field interviews. This initial contextual analysis examined user attitudes about appropriating a new technology in their overall competition strategy. While challenges in the data display and user interface were reported, the interviewees reported that the team and network views offered by the new visualization system enabled them to improve their performance during the competition activities.

Keywords

Visualization, usability, performance, cyber defense competition, network security

INTRODUCTION

Computer and network security has gained national recognition in recent years due to its importance to both the corporate and governmental communities. The 2008 CSI

[4] I performed all the literature review and description of CDCVis for this paper. Janea performed the user interview analysis and reported the results.

(Computer Security Institute) Computer Crime and Security Survey, arguably one of the most cited surveys in the area, reports that "broad changes in the habits of the criminal world—are making significant, hard-hitting attacks easier and more lucrative for their perpetrators" (Richardson, 2008). Specifically, the survey reported that 43 percent of respondents experienced security incidents with another 13 percent who were unsure. Also reported was that average financial loss due to each security incident was $289,000. This dollar figure was attributed to loss from external attacks even though internal attacks occurred in greater frequency (Richardson, 2008). These types of statistics confirm that organizations are in need of individuals trained in the area of computer and network security. Many different educational programs are now offering studies in computer and network security, or Information Assurance (IA) education. The National Security Agency (NSA) and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in IA Education for those schools that have such programs and meet certain criteria. Originally, in 1999, seven schools met this criteria and this number has grown to 94 with the increased demand for students educated in this area. Even with all these new programs and educational opportunities, educators are always searching for innovative ways of teaching computer and network security concepts.

Cyber defense competitions (CDCs) are simulation activities which allow student teams to learn computer and network security concepts by requiring them to defend a "corporate" network from attack. These competitions have been shown to be effective in learning network security concepts (Conklin, 2006). Many different types of these competitions have been utilized in varying degrees all over the United States. Now that these competitions are becoming more commonplace, educators are looking for ways to improve the educational quality of these exercises. Security visualization for network security has become a very large area for research within the past decade. Research has found that visualization allows users to take advantage of the parallel processing nature of the human visual system to more effectively discover possible network attacks (Luse, Scheibe, & Townsend, 2008). While these systems are being researched for computer and network security, very little research has looked at how these systems can be utilized for cyber defense competitions in educational settings. This research describes the development of CDCVis (Cyber Defense Competition Visualization), a system for use during such an exercise. The structure of the developed system is discussed as well as a first-pass exploratory view of user response to the system.

The manuscript is organized as follows. The Background section describes the expansion of security visualization and cyber defense competitions. The CDCVis section provides a brief overview of the developed visualization system utilized for one such competition. Data Collection and Results gives information surrounding the deployment of the user study to help evaluate the system. The Discussion section offers some proposed explanations about the results found in the study. Finally, the Conclusion and Limitations and Future Work sections provide final comments, future avenues of research, and shortcomings of the current study.

BACKGROUND

Security Visualization

Many different streams of research on computer and network security visualization have become popular over the past decade. This research has dealt both with products designed for network security visualization as well as development methodologies for such systems. Products such as NVisionIP create multiple views of a network to illustrate an overall galaxy view, small views of multiple machines, as well as a machine view for screening network activity on a single machine (Lakkaraju, Bearavolu, & Yurcik, 2003; Lakkaraju, Yurcik, Bearavolu, & Lee, 2004; Lakkaraju, Yurcik, & Lee, 2004). TNV was also developed to allow network administrators to view traffic over a specific period of time for the network (Goodall, Lutters, Rheingans, & Komlodi, 2005). Also, VizFlowConnect allowed the user to view traffic based on whether that traffic originated from the internal corporate network or the external Internet (Yin, Yurcik, Treaster, Li, & Lakkaraju, 2004).

Research has also looked at various methodologies for effectively developing network security visualization products. Three primary methodologies have been researched as mechanisms for developing security visualization systems. First, the user-based framework looked at security visualization systems from the user's perspective (Goodall, 2005; Goodall, Lutters, & Komlodi, 2004; Goodall et al., 2005; Komlodi, Goodall, & Lutters, 2004; Komlodi, Rheingans, Ayachit, Goodall, & Joshi, 2005). The researchers utilized interviews with experts in the area to develop a framework based on the three phases of user interaction with the system: 1) monitoring – monitoring and identifying potential attacks, 2) analysis – analyzing alerts and data for attack diagnosis, and 3) response – responding to the attack. Second, the alert-oriented framework, or w^3 premise, was designed around the alerts which occurred during possible system threats (Foresti, Agutter, Livnat, Moon, & Erbacher, 2006; Livnat, Agutter, Moon, Erbacher, & Foresti, 2005). The framework looked at **w**hen the alert occurred, **w**here on the network it took place, and **w**hat type of alert was triggered. Therefore, the alert was the primary focus of interest for systems developed using this methodology. The final network security visualization development framework looked at the components which made up the system (Luse et al., 2008). This framework added a third component to the above two and offered a comprehensive visualization development framework. Visualization components were taken from Shneiderman's information visualization theory (Shneiderman & Plaisant, 2005) and Few's research on the real-time imperative (Few, 2006).

Cyber Defense Competitions

Cyber Defense Competitions (CDCs) are competitions where students can apply computer and network security concepts in a live exercise. These competitions utilize active learning which enables students to apply and practice computer and network security concepts (Riding & Rayner, 1998). These competitions have been shown to be effective both in education of network security concepts as well as raising awareness for security methods in a rapidly changing field (Jacobson & Evans, 2006).

Many different types of CDCs have been utilized to educate students in network security concepts. These have ranged from small intra-university competitions (Chamalese & Pridgen, 2004; Jacobson & Evans, 2006) and competitions with a few universities (Dodge & Ragsdale, 2004; W. Schepens, Ragsdale, & Surdu, 2002; W. J. Schepens & James, 2003) all the way to large competitions involving remotely connected university teams (Vigna, 2003a, 2003b). The competitions typically involve one of two competition types. One type requires students to be both defenders of their own network as well as attackers of other student networks which allows students to get inside an attacker's head (Cowan, Arnold, Beattie, Wright, & Viega, 2003; Hoffman, Rosenberg, Dodge, & Ragsdale, 2005). The other type allows students to only act as network administrators defending their own networks against an outside team which is charged with attacking the student networks (Jacobson & Evans, 2006).

The competition utilized for this research involved student teams which were only allowed to defend their networks. The competition was composed of four primary team types. The Blue Teams consisted of the student teams which were charged with setting up and defending their small corporate network (more details given in data collection section). The Green Team was comprised of individuals who acted as users of the services provided by each Blue Team. The Red Team acted as the hackers of the Blue Team networks and could use most any means necessary to remotely attack the systems. Finally, the White Team acted as administrators of the competition by providing assistance to all teams and interaction between the Red Team and any Blue Teams if the need arose. The White Team was also in charge of scoring and allowed each Blue Team to submit reports if they were able to correct a problem found by either the Green or Red teams to gain back points.

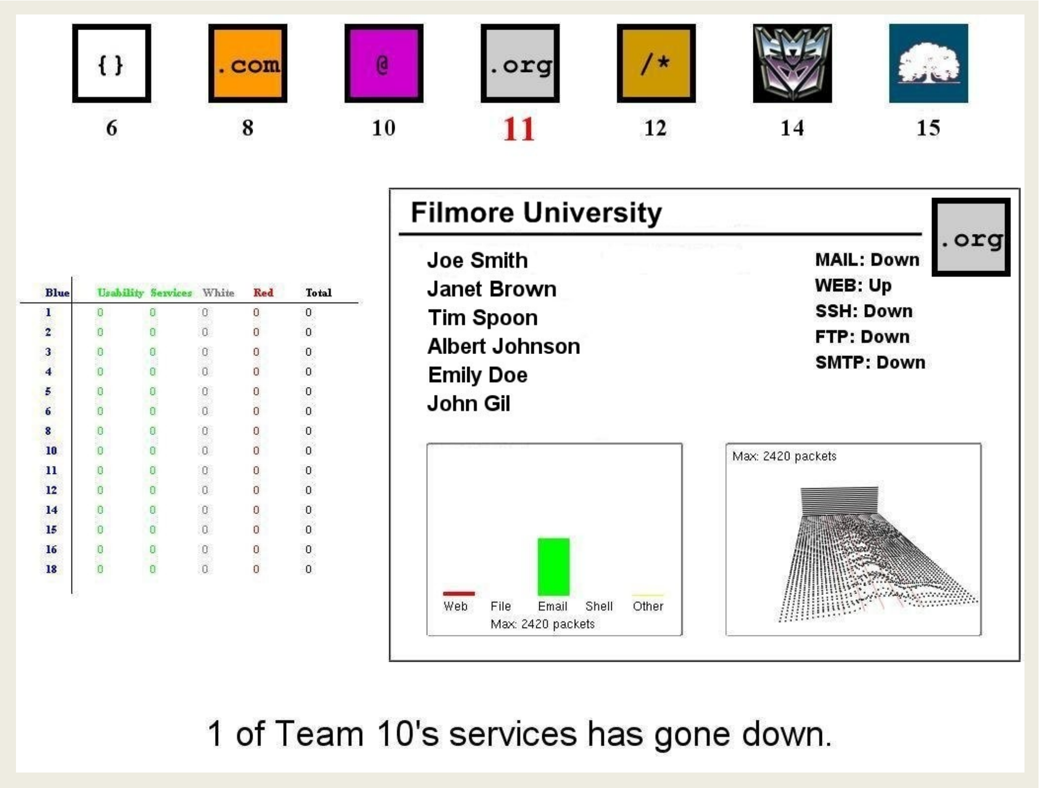
CDCVIS

CDCs, as described above, are very hectic and stress-filled environments. The competitions themselves last anywhere from eight to 16 hours and can consume either an entire day or span overnight. Each team does its best in the allotted time and scenario to protect their network from attack while supplying the necessary services to the users of their network. In order to make effective decisions regarding their network, team members need as much information as possible about both the competition itself and the state of both their respective team network as well as the overall competition network as a whole. Effective dissemination of information to the teams is tantamount to their success and the overall learning outcomes of the competition.

While many different CDCs have been organized and held in recent years, very little research has been performed regarding the visualization systems for CDCs. The only research found was for a visualization system utilized during Defcon's Capture the Flag competition (Cowan et al., 2003). This visualization system was designed after a Nasdaq-like display system. The system was very simple in that it only showed updates to team performance and did not disclose overall team scores. The motivation to withhold information which revealed the overall team scores was done to prevent lagging teams from getting discouraged and thus keep those teams participating in the competition. Very little information was given about this system, but the purpose was only for updates of performance and to act as a mechanism to keep the audience entertained.

The purpose of a CDC is to help educate students in computer network security. A visualization system for CDCs can be utilized for a number of functions to help further this educational objective. CDCVis, or Cyber Defense Competition Visualization, was designed to provide features above and beyond just updating team performance. CDCVis was designed around two different informational views: a team-based view and an overall network view. The two informational views were deemed necessary to allow students to both visualize their own progress as well as view activities which would enable them to envision potential threats on the competition network at large. The system was also designed around a modular, plug-and-play interface. This allowed for visualization modules to be aggregated and arranged in different configurations on the display depending on the needs of the competition. This also allowed for many of the modules to be utilized both at the team and overall network levels of visualization.

The team-based view was primarily concerned with team information as it pertained to the competition. A sample screen capture of a team-based view during a CDC is illustrated in Figure 1. The upper strip of the view contained team logos along with respective team numbers which were provided for the teams in the competition. The currently active team in the visualization had a number which was larger and colored in red. Below this strip, in the left middle of the screen was the scoreboard for the competition. This gave scoring updates for each of the blue teams by each of the teams which were judging the competition as well as an aggregated total score. Next to this was the primary team panel. This panel displayed the relevant information for a single team. First, the name of the university and the members of the team were displayed as well as the team logo. Next to the logo, services were displayed along with their respective state. For example, in Figure 1, this team was expected to support user email connections (IMAP, POP3), a website, SSH, file transfer, and email transfer (SMTP). This allowed each team to see what services were currently up according to the White team and therefore which services were usable by the Green team. By showing this information, each team could work to reconfigure their network to allow these services to be reached. In the lower portion of the Team Panel were two real-time graphs. Each contained visual references to the traffic of a certain type and the current activity of that traffic type on the network. The traffic types included *web* (HTTP, HTTPS), *file transfer* (FTP, SMB, NetBIOS), *email* (SMTP, POP2, POP3, POP3+SSL, IMAP4, IMA4+SSL), *shell* (Telnet, Telnet+SSL, SSH), and other. The bargraph depicted the relative amount of each traffic type (delineated by a bar of a single color) at a specific moment while the NetSqual used a NURBS surface where the five traffic types were located at equal intervals along the width of the surface. The ripples indicated the amount of traffic of a specific type and displayed the traffic trends over time (running from front to back along the length of the graph). Finally, along the bottom was the most current announcement (announcements described in greater detail below).



Blue	Usability	Services	White	Red	Total
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0
5	0	0	0	0	0
6	0	0	0	0	0
8	0	0	0	0	0
10	0	0	0	0	0
11	0	0	0	0	0
12	0	0	0	0	0
14	0	0	0	0	0
15	0	0	0	0	0
16	0	0	0	0	0
18	0	0	0	0	0

Filmore University

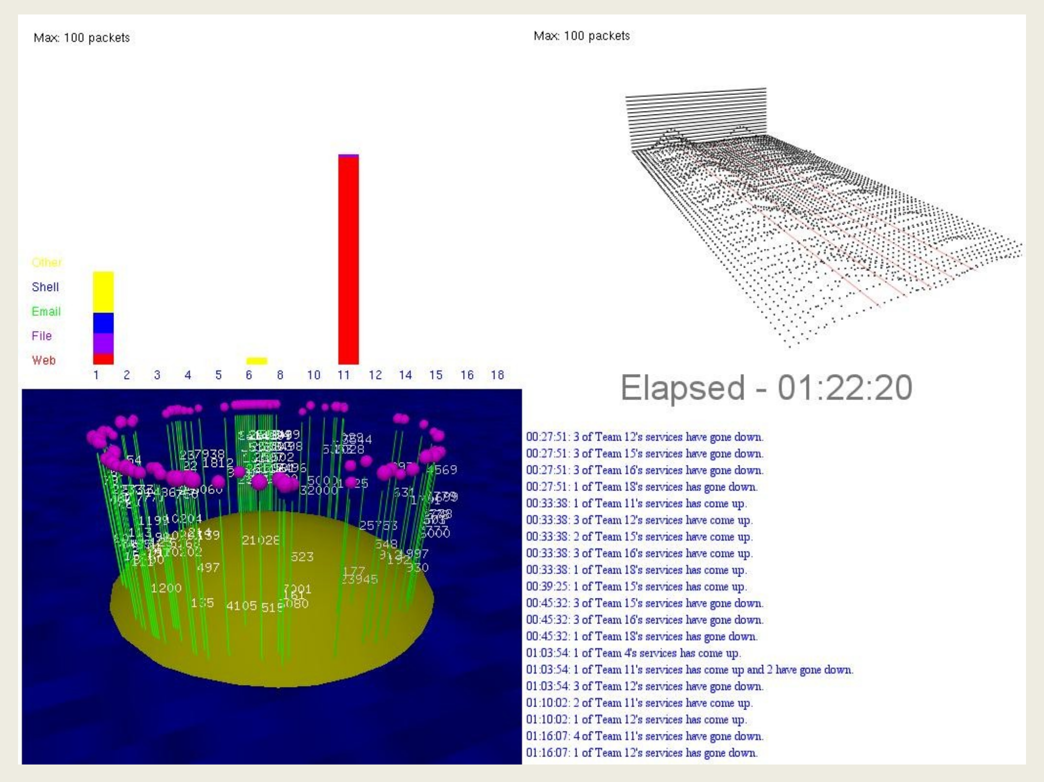
Joe Smith
Janet Brown
Tim Spoon
Albert Johnson
Emily Doe
John Gil

MAIL: Down
WEB: Up
SSH: Down
FTP: Down
SMTP: Down

1 of Team 10's services has gone down.

Figure 13. CDCVis Team-based View

The overall network view provided visualizations pertaining to overall network events on the competition network. The sample visualization shown in Figure 2, displayed various information relevant to all Blue teams in the competition. First, in the upper left was a stacked bargraph. This bargraph was slightly modified from the team-based graph in that along the bottom, each Blue team number was listed. The bars for each team consisted of a stacked bargraph of colors pertaining to the five types of traffic either coming into or leaving the team's network at a particular moment. The NetSquall in the upper right again displayed the five traffic types over time, but instead aggregated these five types across all teams. In the lower left, the Island display presented traffic on specific ports as "trees" with the "fruit" on the tree representing the amount of traffic. The ports started at the outside with the lowest ports and increased in a circular pattern. This visualization module was adapted from work done by Oline and Reiners (Oline & Reiners, 2005) and helped to demonstrate the adaptability of the system by bringing in outside visualization modules to plug in. Finally, the lower right portion of the panel contained a time clock with the amount of time which had elapsed in the competition as well as announcements posted by the system and the White Team for participant informational needs.



```
00:27:51: 3 of Team 12's services have gone down.
00:27:51: 3 of Team 15's services have gone down.
00:27:51: 3 of Team 16's services have gone down.
00:27:51: 1 of Team 18's services has gone down.
00:33:38: 1 of Team 11's services has come up.
00:33:38: 3 of Team 12's services have come up.
00:33:38: 2 of Team 15's services have come up.
00:33:38: 3 of Team 16's services have come up.
00:33:38: 1 of Team 18's services has come up.
00:39:25: 1 of Team 15's services has come up.
00:45:32: 3 of Team 15's services have gone down.
00:45:32: 3 of Team 16's services have gone down.
00:45:32: 1 of Team 18's services has gone down.
01:03:54: 1 of Team 4's services has come up.
01:03:54: 1 of Team 11's services has come up and 2 have gone down.
01:03:54: 3 of Team 12's services have gone down.
01:10:02: 2 of Team 11's services have come up.
01:10:02: 1 of Team 12's services has come up.
01:16:07: 4 of Team 11's services have gone down.
01:16:07: 1 of Team 12's services has gone down.
```

Figure 14. CDCVis Overall Network View

DATA COLLECTION

Subjects for the usability portion of this research consisted of teams of individuals who participated in a CDC at a large Midwestern university. The teams consisted of college students pursuing a major involved with network and security administration. Teams came from eight different colleges/universities across the state. School size varied from community colleges to a Research University with very high research activity.[5] Teams were comprised of four to seven members. This group was solicited due to the live nature of the field study and the range of different participants. Participants were provided with a scenario one month before the competition which detailed a fictitious corporation they must setup and

[5] This is according to the Carnegie Classification of colleges and universities which can be found at http://www.carnegiefoundation.org/classifications/index.asp?key=783.

administer. Each team was allowed to use four machines with any legally obtained software they deemed fit, which was provided by the host university. The teams were given one month prior to the competition to remotely setup their networks utilizing a network-based KVM, and were also allowed to come in one day prior for any final setup needed. The competition lasted from Friday at 5:00 p.m. until Saturday at 11:00 a.m. during the spring semester.

The study of CDCVis was undertaken about seven hours into the competition around 12 midnight so the participants had become accustomed to the competition but were not yet drained from the all-night contest. One of the developers of CDCVis was on-hand and answered any questions about the system both before and after the study. Two interviewers questioned the students utilizing only a PDA recorder and a pad of paper.

During the 18-hour Collegiate Cyber Defense Competition, six teams were interviewed. Seventeen individuals contributed to the discussion of the newly introduced visualization system. The purpose of the unstructured interview was to

1. explore the general attitudes of the group about the visualization system
2. assess how the visualization system was used during the competition
3. discover what problems existed which might suggest further development iterations

Attitudes were defined as the tendency to respond positively or negatively to a given person, situation, or object (Aiken, 2002). Usage was simply measured by how the system helped participants accomplish the task at hand. Problems were measured by the expressions and reports of frustration.

Nearly two hours of discussion was recorded which resulted in 145 statements from the participants about the visualization system. The interview data was coded following recommendations offered by usability researchers (Beyer & Holtzblatt, 1998; Kuniavsky, 2003). An affinity diagram approach (Beyer & Holtzblatt, 1998) was used to reveal common issues and themes.

RESULTS

Five of the six teams had prior experience participating in previous Collegiate Cyber Defense Competitions. However, none of the teams had used a visualization system to support their defense activities. Common themes emerged suggesting how the visualization system was being used and what problems were experienced.

Each of the six teams said that they used the visualization system to check on their scores. Three teams said that they used the system to check on their services. Another team stated that they used the visualization system to help them improve their response time, to discover their service vulnerabilities, and to focus on the task at hand.

- Now I look up there whenever to see your scores. [Team2]
- It helps seeing all the services. [Team 5]
- It definitely helps with the response time. What exactly we were vulnerable to. What we really needed to be looking at. And what's not important to be looking at. And it helps us cut down on what we don't need to worry about either. [Team 3]

Three teams expressed problems with interpreting the scoring. They were confused by the graph of negative and positive numbers. The problems were resolved by asking other teams for clarification. The confused teams were then assured that the negative numbers were good scores and the positive numbers were demerits.

- I went over and looked and then said, ‘are high numbers good or bad?’ [Team1]
- But once I figured out that the negatives were better, then it was pretty simple. [Team2]
- At the beginning we asked around a little bit because some of the things weren’t clear. [Team 6]

Two teams expressed problems with the program’s interface.

- Yeah, when you try to click on ‘status’ there’s no way to go back that I’ve found. When you try to click the ‘back’ button you have to log back in. That’s really annoying. [Team 4]
- It’s just a pain in the ass when I’m sitting here going, ‘refresh!’ [Team 4]

Two teams requested a user guide to assist them with interpreting the visualization graphics.

- Some kind of user guide, I guess, would have been nice. [Team1]
- Are there any documents saying what each zone is about and how to use them? [Team 3]

Despite the problems experienced, the teams expressed more positive attitudes toward the visualization system than negative. Of the 79 statements that directly referred to the visualization system, 55 of those statements were positive and 24 were negative.

- Would it be possible to get this kind of thing running at our school? We would definitely be interested. [Team 1]
- It's all pretty cool. [Team 2]
- The visualization helped us focus more on what exactly the problem was at the time. [Team 3]
- It's definitely not something I would want to get rid of. There are just tweaks and of course, that just comes with time. [Team 4]
- I think it would be real cool if we could use it at name of school. [Team 5]
- This is my second year coming to competitions and I feel like it's really neat to just see, 'oh shoot' we're going to get hit with this sort of traffic or whatever. [Team 6]

DISCUSSION

The investigative study of the usability of the newly introduced visualization program provided valuable information as to how the participants appropriated this technology into their overall team strategy. Training materials had not been decimated before the competition pertaining specifically to the visualization system. The feedback received from the user interviews lead to the development of a 'how-to' CDCVis document for future competitions. Even though the field interviews and user observation revealed that the visualization system could be improved by further iterations, the user feedback was more positive (71 percent) than negative.

There were challenges noted with the display of information. The scoring schema reproduced in the graphs was not intuitive to the users. Teams were initially confused because the graph displayed positive team scores with negative numbers and team demerits with positive numbers. However, once participants understood the scoring schema they were no longer confused and were able to interpret the display. There were also suggestions offered from the interviewees about the general usability of the program's interface. Users requested quicker "refresh" times and a more visible "back" button to allow them to return to the main views.

These new users learned to interpret the team and network views in the first hour of exposure to the information visualization program. The teams then used the visualization to check their scores and to discover higher-level threats and vulnerabilities. The team and network views were used to assist competition participants with decision making and performance. Several teams noted that their performance improved because their response times decreased. In addition to improving team performance, several interviewees also noted that the visualization system reduced the stress of the competition because the display allowed them to focus on the immediate problems and ignore the periphery, non-threatening activities.

The user interviews concluded by half of the teams inquiring if the visualization system would be used in future cyber defense competitions. The qualitative interviews and field observations indicated that the visualization system added value to the competition.

New users were able to quickly interpret the team and network views and were able to appropriate that information in their overall strategy.

CONCLUSION

This purpose of this study was to look at the utilization of visualization systems for computer and network security. Specifically, this research explored the types of visualization systems used during a cyber defense competition. The study has two main contributions. First, it details a visualization system which has been implemented for a current cyber defense competition. This information can be used by others who are also interested in developing such a system for use during similar competitions. Second, the research provides a first-pass look at the usefulness of the system by the users. This provides initial insights into the educational impacts of the system and how the system can be better leveraged to accomplish these objectives.

While not direct, this study in this type of environment provides a corollary to actual corporate network security administrators utilizing visualization systems for computer and network security. As with many corporate situations, it is difficult to adequately conduct research in actual production environments. CDCs provide a valid testing ground for field experiments in the area of corporate network security. This study capitalizes on this environment to provide an initial look at the use of visualization systems in corporate environments for network security.

LIMITATIONS AND FUTURE WORK

The exploratory nature of the open-ended interviews and the small sample size are limitations of this study. In order to develop a richer understanding of the usability and value of the information visualization system to participants of cyber defense competitions, more field interviews need to be gathered. In addition to interviews, formal usability testing of the visualization system should also be conducted. Many participants noted that their performance in the competition improved by utilizing CDCVis, however, those individual reports should be corroborated by quantitative measures.

Various changes to the system have been instituted since this work has been completed. First, a 'how-to' document was written and has been provided to users at the start of subsequent competitions to allow for better understanding of the system. Similarly, the scoring metrics of the competition have been changed in response to user feedback so that higher scores are now better and demerits are applied negatively. A written explanation of the scoring has also been provided to participants in subsequent competitions.

REFERENCES

Aiken, L. (2002). Attitudes and Related Psychosocial Constructs: Theories, Assessment, and Research. Thousand Oaks, CA: Sage Publications.

Beyer, H., & Holtzblatt, K. (1998). Contextual Design: Defining Customer-Centered Systems. San Francisco, CA: Morgan Kaufmann Publishers, Inc.

Chamalese, G., & Pridgen, A. (2004). The Success of the UT IEEE Communications Society. Paper presented at the 8th Colloquium for Information Systems Security Education.

Conklin, A. (2006). Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course. Paper presented at the Proceedings of the 39th Annual Hawaii International Conference on System Sciences, 2006. HICSS '06.

Cowan, C., Arnold, S., Beattie, S., Wright, C., & Viega, J. (2003). Defcon Capture the Flag: Defending Vulnerable Code from Intense Attack. Paper presented at the 2003 DARPA Information Survivability Conference and Exposition.

Dodge, R. C., & Ragsdale, D. J. (2004). Organized Cyber Defense Competitions. Paper presented at the Proceedings of the IEEE International Conference on Advanced Learning Technologies.

Few, S. (2006). Information Dashboard Design: The Effective Visual Communication of Data. Sebastopol, CA: O'Reilly Media, Inc.

Foresti, S., Agutter, J., Livnat, Y., Moon, S., & Erbacher, R. (2006). Visual Correlation of Network Alerts. IEEE Computer Graphics and Applications, 26(2), 48-59.

Goodall, J. R. (2005). User Requirements and Design of a Visualization for Intrusion Detection Analysis. Paper presented at the Proceedings of the 2005 IEEE Workshop on INformation Assurance and Security, United States Military Academy, West Point, NY.

Goodall, J. R., Lutters, W. G., & Komlodi, A. (2004). The Work of Intrusion Detection: Rethinking the Role of Security Analysts. Paper presented at the Proceedings of the Tenth Americas Conference on Information Systems, New York, NY.

Goodall, J. R., Lutters, W. G., Rheingans, P., & Komlodi, A. (2005, Oct. 26, 2005). Preserving the big picture: visual network traffic analysis with TNV. Paper presented at the IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05), Minneapolis, MN.

Hoffman, L. J., Rosenberg, T., Dodge, R., & Ragsdale, D. (2005). Exploring a national cybersecurity exercise for universities. IEEE Security & Privacy, 3(5), 27-33.

Jacobson, D., & Evans, N. (2006). Cyber Defense Competition. Paper presented at the 2006 ASEE Annual Conference & Exposition: Excellence in Education.

Komlodi, A., Goodall, J. R., & Lutters, W. G. (2004, 2004). An Information Visualization Framework for Intrusion Detection. Paper presented at the Conference on Human Factors in Computing Systems, Vienna, Austria.

Komlodi, A., Rheingans, P., Ayachit, U., Goodall, J. R., & Joshi, A. (2005, Oct. 26, 2005). A user-centered look at glyph-based security visualization. Paper presented at the IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05), Minneapolis, MN.

Kuniavsky, M. (2003). Observing the User Experience: A Practitioner's Guide to User Research. San Francisco, CA: Morgan Kaufmann Publishers, Inc.

Lakkaraju, K., Bearavolu, R., & Yurcik, W. (2003, 2003). Nvisionip – a traffic visualization tool for security analysis of large and complex networks. Paper presented at the International Multiconference on Measurement, Modelling, and Evaluation of Computer-Communications Systems (Performance TOOLS).

Lakkaraju, K., Yurcik, W., Bearavolu, R., & Lee, A. J. (2004, 10-13 Oct. 2004). NVisionIP: an interactive network flow visualization tool for security. Paper presented at the 2004 IEEE International Conference on Systems, Man, and Cybernetics, Urbana, IL.

Lakkaraju, K., Yurcik, W., & Lee, A. J. (2004, 2004). NVisionIP: netflow visualizations of system state for security situational awareness. Paper presented at the Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, Washington DC.

Livnat, Y., Agutter, J., Moon, S., Erbacher, R. F., & Foresti, S. (2005, 17-19 June 2005). A Visualization Paradigm for Network Intrusion Detection. Paper presented at the Proceedings of the 2005 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY.

Luse, A., Scheibe, K. P., & Townsend, A. M. (2008). A Component-Based Framework for Visualization of Intrusion Detection Events. Information Security Journal, 17(2), 95-107.

Oline, A., & Reiners, D. (2005, Oct. 26, 2005). Exploring three-dimensional visualization for intrusion detection. Paper presented at the IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05), Minneapolis, MN.

Richardson, R. (2008). 2008 CSI Computer Crime & Security Survey. Computer Security Institute, 1-30.

Riding, R., & Rayner, S. (1998). Cognitive styles and learning strategies. London: David Fulton Publishers.

Schepens, W., Ragsdale, D., & Surdu, J. R. (2002). The Cyber Defense Exercise: An Evaluation of the Effectiveness of Information Assurance Education. The Journal of Information Security, 1(2).

Schepens, W. J., & James, J. R. (2003). Architecture of a Cyber Defense Compeition. Paper presented at the IEEE International Conference on Systems, Man and Cybernetics.

Shneiderman, B., & Plaisant, C. (2005). Designing the User Interface (4th ed.): Pearson Education, Inc.

Vigna, G. (2003a). Teaching Hands-On Network Security: Testbeds and Live Exercises. Journal of Information Warfare, 3(2), 8-24.

Vigna, G. (2003b). Teaching Network Security Through Live Exercises. Paper presented at the 3rd Ann. World Conf. Information Security Education (WISE 3).

Yin, X., Yurcik, W., Treaster, M., Li, Y., & Lakkaraju, K. (2004, 2004). VisFlowConnect: netflow visualizations of link relationships for security situational awareness. Paper presented at the Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, Washington DC.

CHAPTER 5: EMPLOYING INTERACTIVE MAPS TO INCREASE USER UTILIZATION OF VISUALIZATION MECHANISMS FOR NETWORK SECURITY

Modified from a paper being prepared for submission.

Andy Luse[6], Brian Mennecke

ABSTRACT

Visualization technologies offer a powerful tool to aid in corporate network security administration. The purpose of this article is to examine the use of interactive maps to increase the use of such visualization mechanisms. The study utilizes two cyber defense competitions as a live test-bed for the developed visualization system. A quasi field experiment is run to analyze user differences in intention to use the system based on whether or not a map-based visualization mechanism is used. Results show that there is a significant difference in subject intention to use a map-based system depending on the level of prior knowledge that the subject has in computer and network security.

INTRODUCTION

The physical world is made up of places and objects separated by distance, which is an easy method for most to organize when thinking of these items. GIS systems provide a way to manage, analyze, and display information using a computer-based system (Mennecke,

[6] I performed most of the literature review (excluding the portion on GIS) and all the data gathering and analysis for this paper.

Crossland, & Killingsworth, 2000). Spatial decision support systems (SDSS) provide a decision-making environment which allows users to analyze geographic information (Densham, 1991). These tools allow for users to analyze information in a spatially-based context corresponding to real-world places.

Corporate network security has become very important in recent years due to increased malware, threats from hackers, insider abuse, and cyberterrorism (Richardson, 2008). Traditionally, many tools have utilized commandline approaches to network security analysis of vast amounts of text logs (Takada & Koike, 2002). Recently, network security visualization mechanisms have been explored as a means for more effective analysis of network security events (Luse, Scheibe, & Townsend, 2008). These mechanisms have utilized information visualization as a means for visualization abstract data. One question which has received little attention is whether a map-based mechanism is an effective tool for making decisions regarding security events. Specifically, what are user attitudes toward the use of a map-based visualization mechanism for visualizing network security events, which leads to the intended use of such a system.

This research explores the use of a map-based interactive visualization module for use in discovering and reacting to network security events. User attitudes toward such a system are gathered during the use of such a system in the field. These attitudes are used to gauge whether or not the user perceives such a system useful to the task at hand and whether they would be inclined to use such a system. Prior experience of the subject is also utilized as a moderating factor.

The rest of this manuscript is organized in the following manner. The Literature Review section reviews relevant research in the areas of security visualization, map-based decision making, and technology acceptance. The Map-Based Module for CDCVis describes cyber defense competitions (CDCs), and its utilization for field experiments in network security administration as well as CDCVis (cyber defense competition visualization), a visualization mechanism designed for CDCs. The Data Collection section describes the operalization of the field experiment while the Results section follows with a summary of the results from this experiment. Finally, a Discussion of the implications of this research as well as Limitations and Future Research are discussed.

LITERATURE REVIEW

Security Visualization

A large amount of research on visualization mechanisms for computer and network security has surfaced within the last decade. Many different products have been developed as a means to adequately view this information. These projects utilize information visualization as a means of displaying abstract data in a way which allows for greater overall decision-making (Shneiderman & Plaisant, 2005). NVisionIP was developed as a network security visualization tool to allow for multiple views of the same network data (Lakkaraju, Bearavolu, & Yurcik, 2003; Lakkaraju, Yurcik, Bearavolu, & Lee, 2004; Lakkaraju, Yurcik, & Lee, 2004). This is accomplished utilizing a galaxy view of an entire network, small multiple views of a large number of machines at once, and a machine view of traffic on a particular machine. TNV provides a timeline-view approach to allow for analysis of network traffic over a specific period of time to better understand possible security threats (Goodall, Lutters, Rheingans, & Komlodi, 2005). VisFlowConnect allows for investigation of anomalous activity by partitioning the visualization into two parts: the home network and the external network (Yin, Yurcik, Treaster, Li, & Lakkaraju, 2004). This type of delineation provides an "us and them" approach to corporate network security visualization.

Many different initiatives to promote research in visualization projects have also been initiated during the past few years. The VizSec community promotes research in visualization for cyber security.[7] This is accomplished through events, software development, SDK tutorials, as well as publications, particularly from the VizSec annual conference. The infovis community also provides an array of resources, specifically a section devoted entirely to Mapping, Maps, Graphs, and Network Visualization Links.[8] These are just some of the resources now available to those interested in network security visualization.

Various visualization methodologies for the development of network security visualization mechanisms have been proposed. Three primary methodologies have been researched as mechanisms for developing security visualization systems. The user-based framework looks at ID visualization systems from the user perspective (Goodall, 2005; Goodall, Lutters, & Komlodi, 2004; Goodall, Ozok, Lutters, Rheingans, & Komlodi, 2005; Komlodi, Goodall, & Lutters, 2004; Komlodi, Rheingans, Ayachit, Goodall, & Joshi, 2005). Interviews with experts in the area led to a framework based on the three phases of user interaction with the system: monitoring – monitoring and identifying potential attacks, analysis – analyzing alerts and data for attack diagnosis, and response – responding to the attack. The alert-oriented framework, or *w^3 premise*, is designed around the alerts which occur during possible system threats (Foresti, Agutter, Livnat, Moon, & Erbacher, 2006;

[7] http://www.vizsec.org/
[8] http://www.infovis-wiki.net/index.php?title=Mapping%2C_Map%2C_Graph%2C_and_Network_Visualization_Links

Livnat, Agutter, Moon, Erbacher, & Foresti, 2005). The framework looks at *when* the alert occurred, *where* on the network it took place, and *what* the type of alert was. In this way, the alert is the primary focus of interest of the visualization system. The final network security visualization development framework looks at the components which make up the system (Luse et al., 2008). This framework adds a third component to the above two, for a comprehensive visualization development framework. Visualization components are taken from Shneiderman's information visualization theory (Shneiderman & Plaisant, 2005) and Few's research on the real-time imperative (Few, 2006).

Even with all the above research, little research to date has looked at map-based mechanisms as solutions to the problem of network security. Maps offer a spatially-based mechanism for network data which utilizes real world maps for greater association with the actual physical world. Second, not research can be found which has studied user attitudes towards these map-based security visualization mechanisms, which is essential to developing products and systems which users will both utilize and utilize effectively. Finally, very little research has been performed to empirically test these user attitudes towards a security visualization system in an actual real-life environment. This provides much more realistic results as users are actually utilizing the system during production scenarios.

Map-based Decision-making

One of the most commonly used types of display tools for managing, portraying, and analyzing spatial data is a geographic information system (GIS). Much research has focused on the role that maps, GIS, and other spatial decision support systems (SDSS) play in decision making. For example, Smelcer and Carmel (1997) compared maps and tables and found that maps are more efficient because the map image reduces the number of knowledge states that the user needs to process and thus the task is perceived to be less complex. Dennis and Carte (1998) examined cognitive fit theory (Vessey, 1991, 1994; Vessey & Galletta, 1991) for geographic tasks and found that map presentations improve performance and efficiency for certain types of tasks (i.e., those involving adjacency relationships) but not for others (i.e., those where there were no geographic adjacency relationships). Swink and Speier (1999) studied data aggregation and data dispersion of spatially-referenced data and found that performance was lower on larger sized problems, data dispersion was inversely related to performance, and that user spatial skill influenced performance. Mennecke and colleagues (2000) studied task complexity, GIS use, and user characteristics (i.e., novices vs. domain expert) and found that GIS improved decision making when users worked on complex tasks and significantly improved the performance of novice decision makers. These and numerous other studies suggest that GIS support allows decision makers to be more efficient (i.e., time savings) and effective (i.e., improved decision quality).

GIS and other display technologies that allow the user to visualize spatial data offer several affordances that support improved performance for decision makers. First, GIS layer data to display multiple data types on one visual display. For example, a GIS can be used to simultaneously display building or terrain features, activity that has or is currently taking place within a locale, and attributes or characteristics associated with that geographic location (e.g., the asset value of or risk assessment for an object at a location). Secondly, GIS allow the user to organize the data using a schema that is often relevant to problem solving; that is, the spatial arrangement of the elements involved in the problem solving activity. While not all problems are best solved by considering the spatial arrangement of the components of the problem, it is often the case that these components are not arranged in space in a random way and, therefore, a spatial display often provides a way to organize, categorize, and discover relationships that are not otherwise obvious. Third, by collapsing data about problem components (i.e., multiple data layers) into one visual display, problems are simplified by creating a more efficient display environment; that is, an *image*.

Image Theory (Bertin, 1967, 1983) offers a theoretical basis for understanding the importance of images. The theory proffers that some types of data representations are more efficient than other types of representations. For example, Bertin observed that a representation is more efficient "if, in order to obtain a correct and complete answer to a given question, all other things being equal, one construction requires a shorter observation time than another construction" (Bertin, 1983, p. 139). Bertin suggested that displays could be classified as either images or figurations (1983). An image is a visual form such as a graph or single map that has meaning and is perceptible in a minimum instant of visualization. As such, images support the development of a Gestalt understanding of the relationships that exist in a problem domain. Figurations, on the other hand, are multifaceted illustrations that are complex and cannot be represented by a single image (i.e., they are composed of multiple images). When multiple images are needed to convey a concept or data, decision makers will take more time and the cognitive load will be greater and, therefore, decision making performance will likely be reduced.

Technology Acceptance

Technology acceptance has long been used as a measure of usability for an information system. Various models have been developed which consistently explain over

40% of the variance associated with an individual's intention to use a technology. The Technology Acceptance Model, or TAM, is one of the most widely recognized measures in this area (F. D. Davis, 1989). TAM was developed using both the Theory of Reasoned Action (TRA) (Ajzen & Fishbein, 1980; Fishbein & Ajzen, 1975) and the Theory of Planned Behavior (TPB) (Ajzen, 1985) as a model for explaining motivation for performing a task. Specifically, TAM was tailored to the context of information systems, explaining how users come to accept and use a technology. TAM argues that Perceived Usefulness and Perceived Ease of Use of a technology explain why people accept technology within an organization. Later, TAM2 (Venkatesh & Davis, 2000) added subjective norm as another predictor in the model.

Recently the Unified Theory of Acceptance and Use of Technology (UTAUT) has become popular as the most encompassing theory of technology acceptance (Venkatesh, Morris, Davis, & Davis, 2003). This model combines models and theories of individual acceptance including TRA, TAM TPB, the Motivational Model (F.D. Davis, 1992), the Model of PC Utilization (MPCU) (Thompson, Higgins, & Howell, 1991), Innovation and Diffusion Theory (IDT) (Rogers, 1995), and Social Cognitive Theory (Bandura, 1986; Compeau & Higgins, 1995). The model proposes that Performance Expectancy, Effort Expectancy and Social Influence together predict Behavioral Intention and Behavioral Intention along with Facilitating Conditions predict Use Behavior.

Along with the above four major constructs, the four moderators of gender, age, experience, and voluntariness of use also influence both Behavioral Intention and Use Behavior (see Figure 1). Several previous studies also found experience to be a significantly contributing factor. It was found that attitude was more important with increasing experience while subject norm became less important with increasing experience under TRA (Karahanna, 1999). Studies have also shown that ease-of-use becomes nonsignificant with increased experience under TAM (Davis, 1989; Szajna, 1996). The Model of PC Utilization found that complexity, affect toward use, social factors, and facilitating conditions all became more significant with less experience. Differences in adoption vs. usage behavior were also found based on the amount of experience (Karahanna, 1999). Developmental studies for UTAUT utilized a longitudinal approach with three levels of experience based on the time used (Venkatesh et al., 2003). TRA, TAM, TPB, MPCU, and IDT all found that the significance of the effect of some constructs decreases or sometimes disappears with increasing experience.

The technology acceptance research area, including the current UTAUT implementation, typically utilizes a path model to measure whether or not an individual uses a system and the constructs which help to predict that use. In the case of UTAUT, this is due to the three level nature of the model. In order to effectively measure technology acceptance under UTAUT, a path model must be utilized to measure the relationship between the four exogenous variables and the two endogenous variables which are themselves at differing levels in the model. This research aims to predict technology acceptance in a probable future scenario. Specifically, the research wants to see whether users of a visualization system during a cyber defense competition would be likely to utilize a similar visualization in the future if they were a network security administrator. Therefore, we do not wish to measure actual use, but only the intention to use. With this in mind, the research here will only look at the endogenous variable of *Behavioral Intention* and its three predictor variables of *Performance Expectancy*, *Effort Expectancy*, and *Social Influence*. Also, *Experience* will be explored as a moderating variable and will be operationalized as an interaction. With only two levels within the research model, regression analysis is acceptable and will be utilized here. Figure 1 shows the complete UTAUT model with the elements utilized for this study darkened.

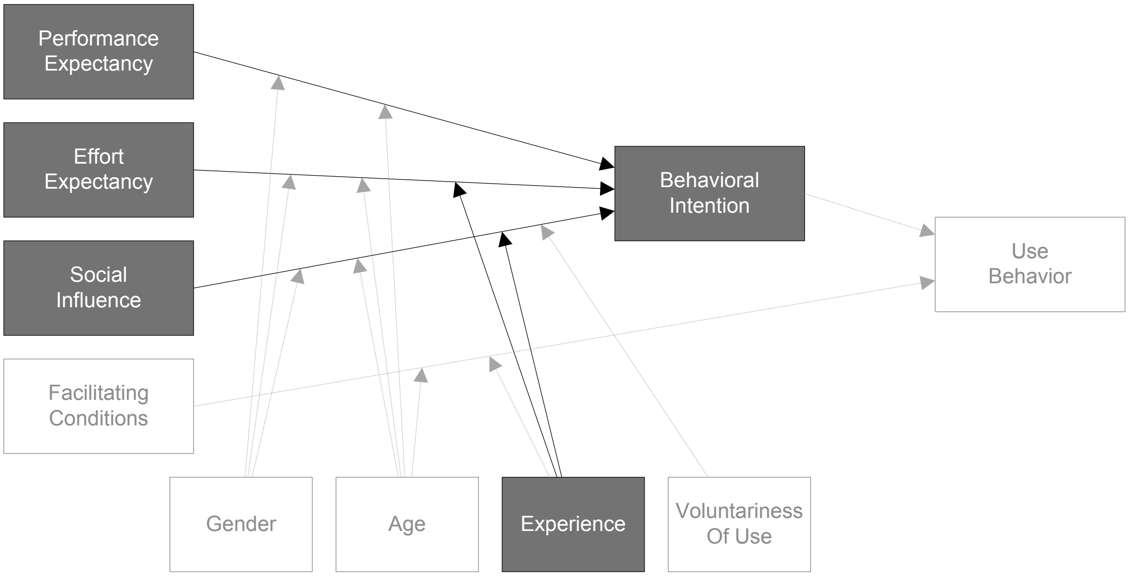


Figure 15: UTAUT model highlighting measures utilized in the current study.

MAP-BASED MODULE FOR CDCVIS

Cyber Defense Competitions

Cyber Defense Competitions (CDCs) are competitions which allow for students to practice network security administration in a live, controlled environment. These competitions have become popular in recent years as an active learning methodology for effectively teaching network security concepts (Riding & Rayner, 1998) and their effectiveness or learning these concepts has also been shown (Conklin, 2006). These competitions also increase awareness and understanding of security exploits, tools, and countermeasures in the rapidly changing network security environment (Jacobson & Evans, 2006).

Various types of CDCs have been utilized to date. The competitions range from small-scale internal competitions between students in the same university (Chamalese & Pridgen, 2004; Jacobson & Evans, 2006) or from a small number of universities (Dodge & Ragsdale, 2004; W. Schepens, Ragsdale, & Surdu, 2002; W. J. Schepens & James, 2003) all the way to competitions which involve many universities covering a large geographical area (Vigna, 2003a, 2003b). The competitions vary widely in their team compositions and metrics for measuring success, but typically involve teams of individuals trying to protect their specific network from other individuals who are trying to attack their network.

The types of network attack/defend scenarios fall into a matrix of four possible options. Some competitions require students to be both defenders as well as attackers under the assumptions that you cannot truly understand your adversary without putting yourself in his shoes (Cowan, Arnold, Beattie, Wright, & Viega, 2003; Hoffman, Rosenberg, Dodge, & Ragsdale, 2005). The other popular type of competition for students involves student teams only defending their networks against a team of non-student external attackers. These two types of scenarios can be seen in the top row of Table 1[9].

[9] The remaining student scenario involves students attacking non-student machines. This type of competition is not currently discussed in the literature. The fourth and final scenario is not student-centered, but involves non-student members both attacking and defending. This type of scenario is present during actual security scenarios in a real-world situation.

		Attackers	
		Students	Others
Defenders	Students	Teams of students defend own network while attacking other student networks	Teams of students defend own networks from non-student team of attackers
	Others	Non-student teams defend their networks against student teams of attackers	Non-student teams defend their networks against non-student teams of attackers (real world)

Table 9: Types of CDCs based on the roles of the students and other participants.

The CDCs utilized for this research employed a defense learning environment coinciding with usability maintenance. The two CDCs for this study were both run at a large Midwestern university in the US. The student teams consisted of 4 to 8 individuals. Each team was given a scenario which involved their own fictitious organization. The teams were in charge of setting up their own "corporate network" utilizing up to four separate machines. The machines could utilize a combination of any operating system(s) including Windows, Linux, and/or Mac OS. All the member machines were present at the competition home on the university. The members of each team were given one month of remote setup for the machines utilizing IP-based KVMs. Also, the teams were allowed to come in for a final setup one day prior to the start of the competition. Both competitions lasted from 9:00 AM til 5:00 PM on a Saturday during the spring semester.

The student teams had two primary objectives. The first objective involved securing the network against external attackers. The students were not allowed to attack back or to attack other student teams, coinciding with the highlighted competition type in the above table. The attacking group consisted of both advanced graduate students and local security professionals from the surrounding community. The second objective of the student teams was to support users by offering a set of services which should be available. This task was added to better emulate a corporate environment where security must be maintained concurrently with user-based services. The services the teams had to provide included email, file sharing (through FTP), shell access (including the ability to remote launch test code), and a corporate web site. These services were deemed appropriate for a small technical firm.

The competition was broken up into four separate teams. First, the Blue Teams were the student based teams in charge of setting up, defending, and providing services on the networks. Second, the Green Team consisted of student helpers not otherwise involved in the competition. These students acted as the users of the Blue Team networks and were given access rights and credentials by each of the Blue Teams to test for the usability of the student networks. The Red Team included the hacking graduate students and professionals who were in charge of attacking the Blue Team networks using any means necessary. Finally, the White Team acted as administrators of the competition, providing assistance to all the teams as well as a middle-man if any interaction is needed between the Red Team and any other participating team. The White Team was also in charge of scoring and allowed each Blue Team to submit reports if they were able to correct a problem found by either the Green or Red teams to gain back points. Figure 2 shows a simple overview of those involved in the competition.

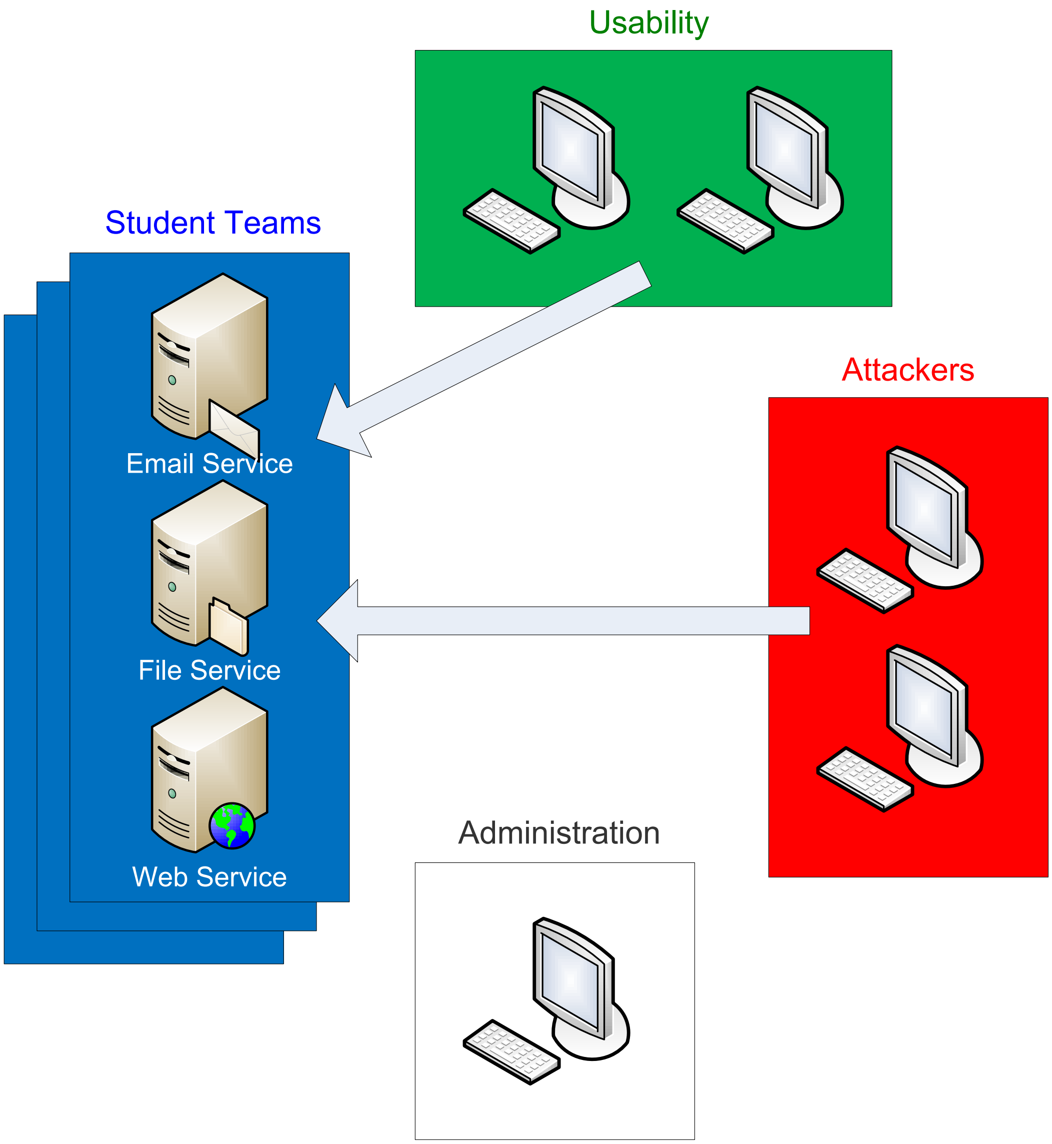
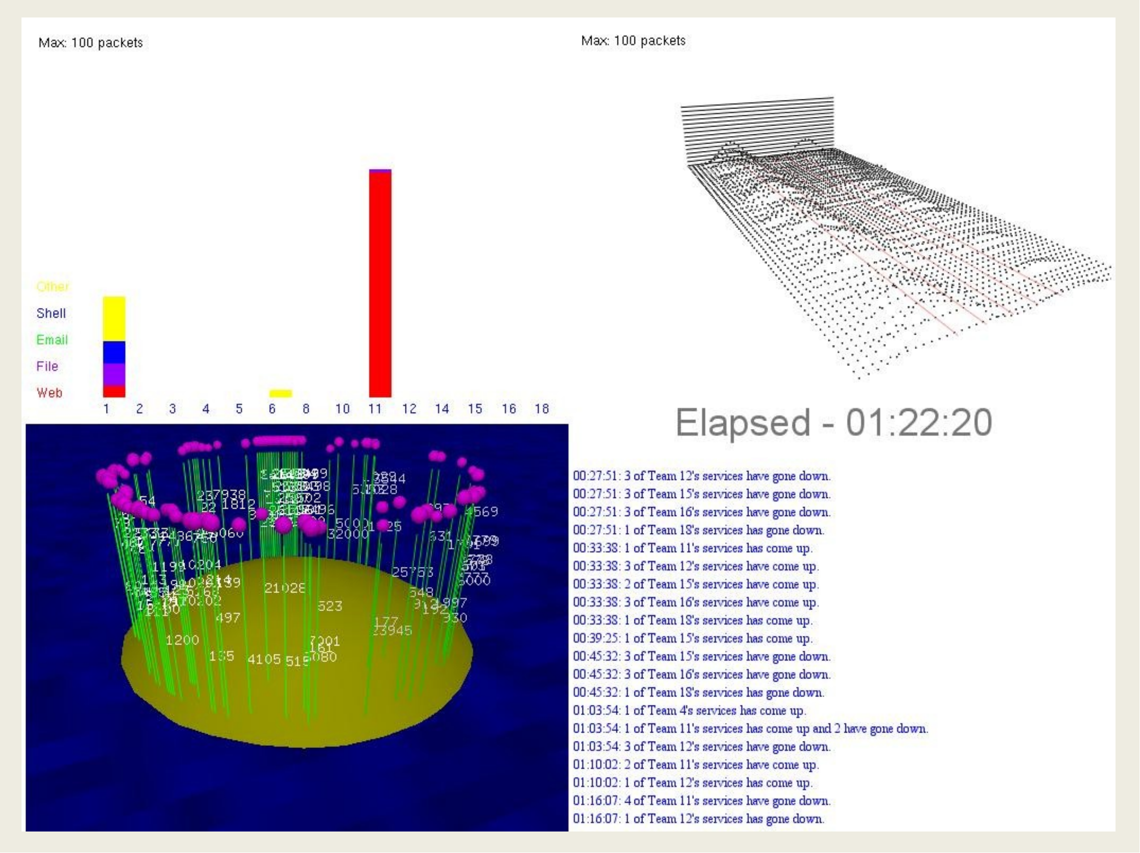


Figure 16: Teams involved in the CDC utilized for the study.

CDCVis

CDCVis (Cyber Defense Competition Visualization) is a visualization system developed specifically for use during CDCs. The system utilizes elements designed for visualization of network traffic and visual analysis of current network activity. These elements were designed using both traditional information visualization theory and visualization mechanisms suited to the specific requirements of network security (Luse et al., 2008; Shneiderman & Plaisant, 2005).

The system employs a modular-based, plug-and-play approach to allow for multiple visualization objects. These visualization objects provide live, animated mechanisms for displaying network traffic and events to users. The system consists of traditional 2D objects as well as 3D visualization mechanisms for displaying information to the user. The system divides the data into five categories based on the types of services the student teams must provide including web, file transfer, email, shell (terminal), and other traffic types. Figure 3 shows an example output from CDCVis where the upper left quadrant contains a stacked bargraph for each team with five colors representing the types of traffic being received by each team at any moment. The upper right quadrant contains a nurbs surface showing the five types of traffic present on the network aggregated for all teams over time. The lower left quadrant shows a 3D island visualization, adapted from another research project, displaying traffic present on respective ports (Oline & Reiners, 2005). The lower right quadrant shows the time elapsed in the competition as well as announcements.



```
00:27:51: 3 of Team 12's services have gone down.
00:27:51: 3 of Team 15's services have gone down.
00:27:51: 3 of Team 16's services have gone down.
00:27:51: 1 of Team 18's services has gone down.
00:33:38: 1 of Team 11's services has come up.
00:33:38: 3 of Team 12's services have come up.
00:33:38: 2 of Team 15's services have come up.
00:33:38: 3 of Team 16's services have come up.
00:33:38: 1 of Team 18's services has come up.
00:39:25: 1 of Team 15's services has come up.
00:45:32: 3 of Team 15's services have gone down.
00:45:32: 3 of Team 16's services have gone down.
00:45:32: 1 of Team 18's services has gone down.
01:03:54: 1 of Team 4's services has come up.
01:03:54: 1 of Team 11's services has come up and 2 have gone down.
01:03:54: 3 of Team 12's services have gone down.
01:10:02: 2 of Team 11's services have come up.
01:10:02: 1 of Team 12's services has come up.
01:16:07: 4 of Team 11's services have gone down.
01:16:07: 1 of Team 12's services has gone down.
```

Figure 17: Example output from CDCVis viewed by both groups.

The map-based module provides a visual representation of network traffic during the competition in a spatially-oriented context. One of the two competitions tested consisted of student groups from across the state of Iowa. To simulate the idea of traffic over distance, the map placed a circle with each team's number inside the circle. The map then drew lines interactively when traffic was either destined to the team or sent from the team. The line colors coincided with the same colors used above for the five different traffic types and was routed through a central circle symbolizing the place of the competition. Figure 4 shows a screen capture of this visualization mechanism.

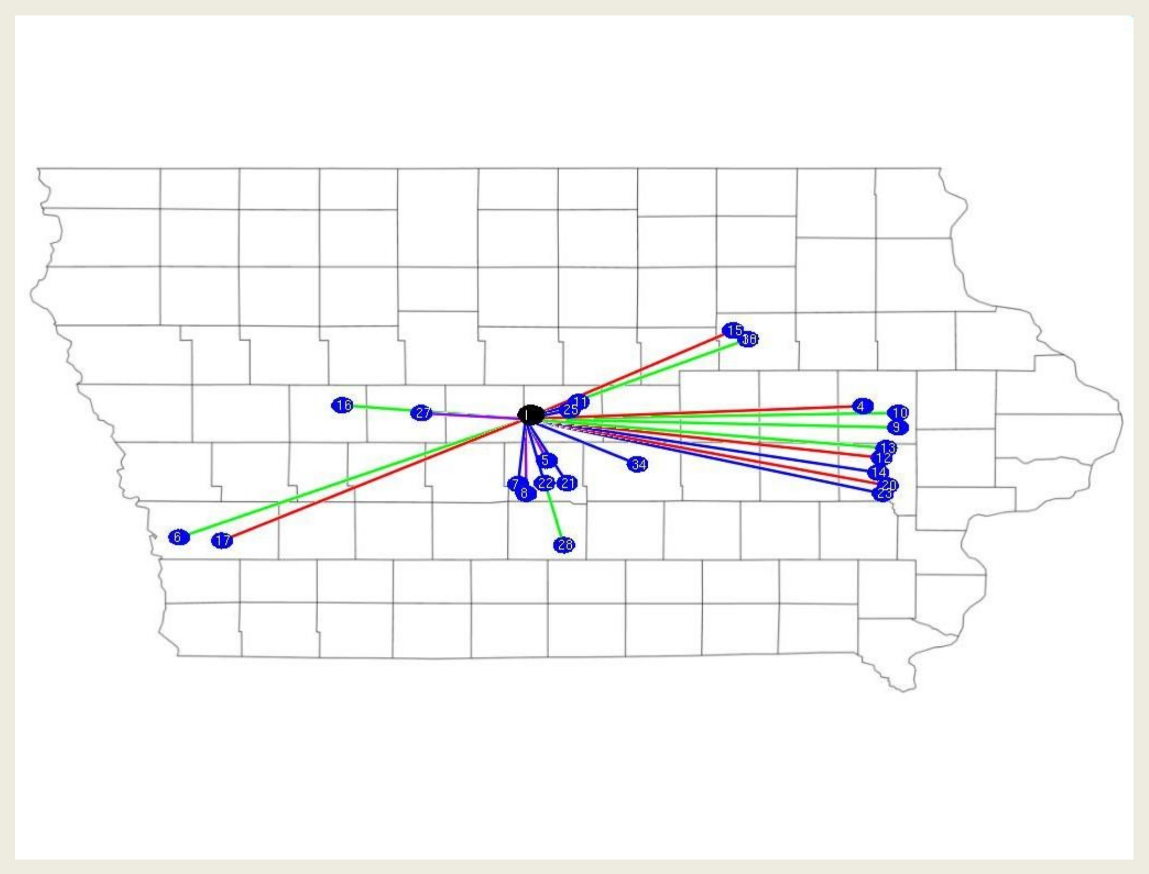


Figure 18: Map-based visualization mechanism of CDCVis.

Given the research on decision-making using GIS-based visualization above as well as technology acceptance in the face of the moderating effect of experience, we believe that a map-based mechanism for network traffic visualization will influence the likelihood an individual would be inclined to use the system in the future. More formally…

H_1: A map-based module for displaying network traffic will influence a user's behavioral intention to use the system compared to a visualization system which does not contain such a module depending on the number of prior security courses the subject has taken.

H_{1a}: The greater the experience of the subject with network security administration, the more likely the intention that he or she will use the map-based system in the future.

H_{1b}: The less the experience of the subject with network security administration, the less likely the intention that he or she will use the map-based system in the future.

DATA COLLECTION

This research utilized a quasi-field experiment involving two different groups during two different CDCs. The field experiment was the most logical choice as a first step towards a more structured experimental evaluation of the system. Also, since the system is utilized by teams at these competitions, a valid testing metric was in the deployment of the product to the actual users of the product. Field studies offer the best combination of causal assumptions and generalizability that's attainable within a single study (Heppner, Wampold, & Kivlighan, 2008). While the treatment of map-based vs. non map-based visualization mechanism utilization was randomized between the two groups, the subjects were already members of teams which had chosen to come to each competition. For this reason, the experiment is quasi in nature.

Each CDC group was composed of approximately 30 individuals with 32 viewing the non-map implementation and 34 viewing the map-based implementation. The two competitions lasted for approximately 8 hours and were conducted from 9 to 5 on a Saturday. Each section viewed the exact same combination and arrangement of visualization modules except for the treatment group which also viewed an extra screen with the map-based visualization module. Both competitions utilized the same scoring method and rules and were given very similar corporate scenarios. The same person running the visualization system was present at both competitions and answered any questions posed about the system. A limited how-to sheet was given to the teams at the start of the competition, but this consisted of only one sheet as the researchers were interested in the use of the system by novices.

The procedures used for both competitions were very similar in nature. The teams were introduced to CDCVis at the start of the competition. The members were given a chance to view the system before the small informational sheet was given to them. The students were then allowed to ask any questions about the system as the individual running the system walked around the area. After the system had been utilized for a period of time, questionnaires were distributed to all the members of each team. Both questionnaires were given right after lunch and the students were given around a half hour to complete the questionnaires. The questionnaires consisted of all seven areas of the original UTAUT questionnaire, including the two areas later removed from the model by the researchers. Also, demographic and personal experience questions were given at the end of the questionnaire. The actual questionnaire used can be viewed in Appendix A.

RESULTS

In total, 66 students filled out the questionnaires handed out during the competition. The study examined one dependent variable and five independent variables (not including the interaction). The dependent measure, BI (Behavioral Intention), consists of three items and has a high reliability (Cronbach's $\alpha = 0.955$). Three of the dependent measures – PE (Performance Expectancy), EE (Effort Expectancy), and SI (Social Influence) – also had relatively high reliability with Cronbach's α equal to 0.912, 0.916, 0.840 respectively. This indicates that the subjects responded consistently to the items in the measures. The other two independent variables consisted of the number of security courses taken by the subject and the treatment variable of whether or not the map-based visualization mechanism was used during the subject's CDC. Each of the three independent measures of PE, EE, and SI were examined in separate one-way ANOVA tests to check for any significant differences between the subjects in each group, but no significance was found. A fourth one-way ANOVA was run to look for significant differences between the two groups in the number of security courses taken by the subjects. This result was found to be significant and therefore the data displayed below is only given for the range of values for each group (see Figure 6). For instance, if you look at the regression lines in Figure 6, you will see that the positive sloping line has values ranging from 0 to 11 while the negative sloping line has values ranging from 0 to 7. Therefore, the lines are restricted to the actual range of values represented by the group and no type of prediction is postulated by extending the line beyond the values represented in the group.

	PE	**EE**	**SI**	**BI**	**NumSec**
	(Performance Expectancy)	(Effort Expectancy)	(Social Influence)	(Behavioral Intention)	(Number Security Courses)
with map-based mechanism					
n=32	11.65	11.15	8.5	7.82	0.77
	(6.27)	(5.82)	(4.09)	(5.13)	(1.57)
without map-based mechanism					
n=34	9.83	10.41	8.58	7.19	4.25
	(4.43)	(4.74)	(4.37)	(4.37)	(3.81)
	4-items	4-items	3-items	3-items	
(minimum preferred)	Min = 4, Max = 24	Min = 4, Max = 24	Min = 3, Max = 18	Min = 3, Max = 18	
	α = 0.912	α = 0.916	α = 0.840	α = 0.955	

Table 10: Sample size, mean, and standard deviations for study variables.

For the analysis of the data, OLS (ordinary least squares) regression analysis was conducted utilizing five hierarchically related models (see Figure 5). Regression was utilized as this study aimed to find whether subjects "intended" to use the software in the future if they were a network administrator. Since only the intention was under investigation this left a set of two-level hierarchically related models; therefore, a simple regression is an appropriate statistical technique for analyzing these relationships. The results for model 1 (M1) indicate that the section of the UTAUT mechanism used to measure Behavioral Intention (BI) is highly significant ($F(3,51) = 44.627$, $p = 0.000$) and also explains a large amount of variance in the dependent variable ($R^2 = 0.724$). Of the three independent variables used in M1, only PE and SI are significant ($t = 2.692$, $p = 0.010$ and $t = 5.967$, $p = 0.000$ respectively) while EE is not significant ($t = 0.633$, $p = 0.529$). Model M2 was examined to check for a significant difference between the groups that used the map-based visualization mechanism and those that did not use this tool. The results show that there is no significant difference between M1 and M2 with the addition of the variable MU (map used) in M2 (partial $F = 0.055$, $p = 0.816$). These results provide no support for Hypothesis H_1 and indicate that the use of the map-based visualization system does not significantly increase a user's behavioral intention to use the system. Next, in Model M3 we checked to see if there is a difference in the model due to the number of security courses taken by the user (NumSec). The results indicate that there is no significant increase in the F-value between M1 and M3 (partial $F = 0.326$, $p = 0.570$). Finally, Model M5 was run to evaluate whether there is a significant change in the overall model F-value when an interaction term of map used crossed with the number of security courses taken is entered into the model. This proved to be significant (partial $F = 4.442$, $p = 0.040$) which indicates that there is a significant effect due to whether or not a map-based visualization mechanism is used only when analyzed in the context of the number of security courses the subject has taken (see Figure 6). While not supporting our hypothesis, this indicates that the relationship predicted by the hypothesis exists when the number of security courses taken by the subject is considered.

$$M1: BI = \beta_0 + \beta_1 PE + \beta_2 EE + \beta_3 SI$$

$$M2: BI = \beta_0 + \beta_1 PE + \beta_2 EE + \beta_3 SI + \beta_4 MU$$

$$M3: BI = \beta_0 + \beta_1 PE + \beta_2 EE + \beta_3 SI + \beta_5 NumSec$$

$$M4: BI = \beta_0 + \beta_1 PE + \beta_2 EE + \beta_3 SI + \beta_4 MU + \beta_5 NumSec$$

$$M5: BI = \beta_0 + \beta_1 PE + \beta_2 EE + \beta_3 SI + \beta_4 MU + \beta_5 NumSec + \beta_6 MUNumSec$$

Figure 19: Hierarchical models used for the study utilizing the independent variables PE (Performance Expectancy), EE (Effort Expectancy), SI (Social Influence), MU (Map Used), and NumSec (Number of Security courses) and the dependent variable BI (Behavioral Intent).

	M1			M2			M3			M4			M5		
	b	t-ratio	p	b	t-ratio	p	b	t-ratio	p	b	t-ratio	p	b	t-ratio	p
PE	0.266	2.692	0.010	0.262	2.565	0.013	0.272	2.716	0.009	0.260	2.540	0.014	0.324	3.131	0.003
	(0.099)			(0.102)			(0.100)			(0.102)			(0.104)		
EE	0.063	0.633	0.529	0.064	0.637	0.527	0.057	0.565	0.575	0.056	0.552	0.584	0.024	0.238	0.813
	(0.100)			(0.101)			(0.101)			(0.102			(0.099)		
SI	0.648	5.967	0.000	0.651	5.893	0.000	0.648	5.926	0.000	0.658	5.921	0.000	0.674	6.255	0.000
	(0.109)			(0.110)			(0.109)			(0.111)			(0.108)		
MU				-0.168	-0.234	0.816				-0.550	-0.642	0.524	-1.503	-1.593	0.118
				(0.718)						(0.857)			(0.943)		
NumSec							0.063	0.571	0.570	0.108	0.825	0.413	-0.485	-1.570	0.123
							(0.110)			(0.131)			(0.309)		
MU x NumSec													0.736	2.107	0.040
													(0.349)		
Intercept	-1.577	-1.793	0.079	-1.483	-1.522	0.134	-1.708	-1.867	0.068	-1.495	-1.530	0.133	-1.474	-1.560	0.125
	(0.880)			(0.974)			(0.915)			(0.978)			(0.945)		
SSR (w/df)	882.237(3)			882.603(4)			884.417(4)			887.205(5)			915.248(6)		
MSE (w/df)	6.590(51)			6.714(50)			6.678(50)			6.757(49)			6.314(48)		
R-squared	0.724			0.724			0.726			0.728			0.751		

Table 11: ANOVA Table for hierarchical models.

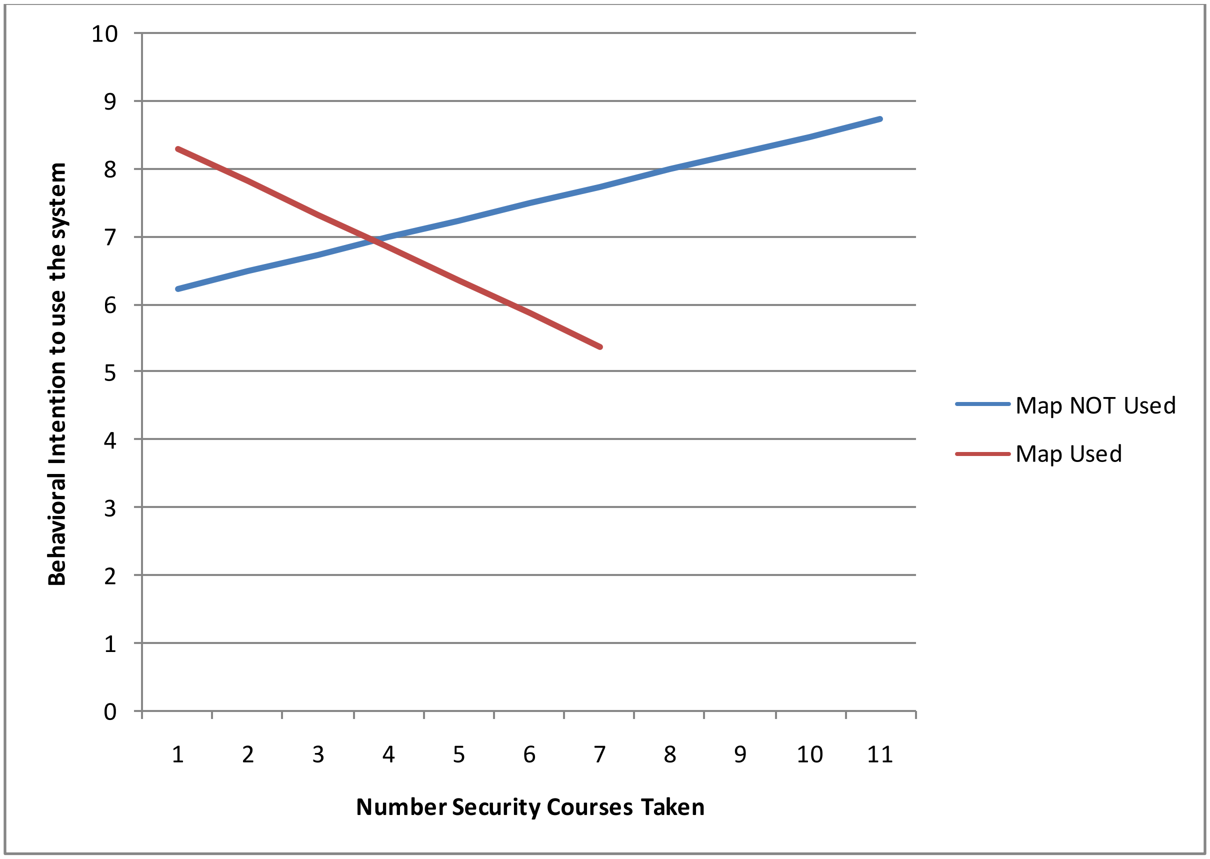


Figure 20: Interaction between the number of security courses taken and whether or not the map-based visualization mechanism was utilized.

DISCUSSION

This study was designed to examine the differences in subjects' behavioral intention to use a visualization product for network security administration in the future. The study also examined the combined effects of utilizing a map-based visualization mechanism along with the security background of the subject measured by the number of courses taken on the subject. The study utilized a quasi field experiment with two similar groups of individuals competing in two different cyber defense competitions. We hypothesized that a map-based visualization mechanism for network security would influence a user's behavioral intention to use the system. Specifically, those individuals with greater exposure to network security would be more inclined to use the product in the future if it included a map-based visualization mechanism, but the less knowledge of network security, the less likely an individual would use a security visualization product with a map-based visualization mechanism. The results of the study show support for the hypotheses.

This study has two important contributions. First, it utilizes a live field environment for the testing of a network security product. Many behavioral researchers utilize traditional experiments to isolate the effects of a new treatment. While these laboratory experiments provide a more controlled environment for studying these effects, they also separate the user from the actual experience and circumstances where the treatment will be used. This is even more pronounced in network security visualization as the high stress and real-time nature of the situation are critical to the use of the products being researched. Decisions must be made on the fly which could make the difference between a secure network and the loss of corporate secrets which could be fatal for the organization and its customers.

Second, the study demonstrates a first pass at formal evaluation of network security visualization mechanisms. While many different visualization products have been developed and some product design metrics have been researched, very little has been done to test these products and theories. This research provides a first pass at evaluating security visualization products, specifically in the context of cyber defense competitions.

Of primary interest here are the implications for corporations hiring for network security positions. When providing network security visualization mechanisms for network security employees, the exposure of the individual to network security is of key importance.

For those which are more experienced with network security, corporations should provide access to visualization mechanisms which include a map-based, or geospatially based visualization mechanism. This could include a floor schematic for smaller corporations in single buildings to state, country, or world maps for multinational organizations. For less experienced individuals, the use of such map-based visualization mechanisms should be an option, but not a requirement as the use of such mechanisms may actually cause the network security administrator to be less likely to use the system, thereby missing potential security threats which could wreak havoc on the corporate network.

LIMITATIONS AND FUTURE RESEARCH

This research provides a first step in measuring the usefulness of map-based visualization mechanisms for network security administration, but there are many limitations and areas for future work. First, the study utilizes a quasi field experimental design for testing. While this provides a real-world context for the subjects, a more controlled environment will need to be utilized in future research to verify the findings of this research. Second, greater granularity of map-based visualization mechanisms is needed. The use of different types of maps as well as maps at different levels is needed to see how these properties affect the intention to use the system.

REFERENCES

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckmann (Eds.), *Action control: From cognition to behavior*. New York: Springer-Verlag.

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Englewood Cliffs, NJ: Prentice-Hall.

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Englewood Cliffs, NJ: Prentice-Hall.

Bertin, J. (1967). *Semiologie Graphique*. Paris: Mouton-Gautier.

Bertin, J. (1983). *Semiology of graphics: Diagrams, networks, maps* (W. J. Berg, Trans.). Madison, WI: University of Wisconsin Press.

Chamalese, G., & Pridgen, A. (2004). *The Success of the UT IEEE Communications Society.* Paper presented at the 8th Colloquium for Information Systems Security Education.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly, 19*(2), 189-211.

Conklin, A. (2006). *Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course.* Paper presented at the Proceedings of the 39th Annual Hawaii International Conference on System Sciences, 2006. HICSS '06.

Cowan, C., Arnold, S., Beattie, S., Wright, C., & Viega, J. (2003). *Defcon Capture the Flag: Defending Vulnerable Code from Intense Attack.* Paper presented at the 2003 DARPA Information Survivability Conference and Exposition.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340.

Davis, F. D. (1992). Extrinsic and intrinsic motivation to use computers in the workplace. *Journal of Applied Social Psychology, 22*(14), 1111-1132.

Dennis, A. R., & Carte, T. (1998). Using Geographical Information Systems for Decision Making: Extending Cognitive Fit Theory to Map-based Presentations. *Information Systems Research, 9*(2), 194-203.

Densham, P. J. (1991). *Spatial Decision Support Systems* (Vol. 2). London: Longman Scientific & Technical.

Dodge, R. C., & Ragsdale, D. J. (2004). *Organized Cyber Defense Competitions.* Paper presented at the Proceedings of the IEEE International Conference on Advanced Learning Technologies.

Few, S. (2006). *Information Dashboard Design: The Effective Visual Communication of Data*. Sebastopol, CA: O'Reilly Media, Inc.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.

Foresti, S., Agutter, J., Livnat, Y., Moon, S., & Erbacher, R. (2006). Visual Correlation of Network Alerts. *IEEE Computer Graphics and Applications, 26*(2), 48-59.

Goodall, J. R. (2005). *User Requirements and Design of a Visualization for Intrusion Detection Analysis.* Paper presented at the Proceedings of the 2005 IEEE Workshop on INformation Assurance and Security, United States Military Academy, West Point, NY.

Goodall, J. R., Lutters, W. G., & Komlodi, A. (2004). *The Work of Intrusion Detection: Rethinking the Role of Security Analysts.* Paper presented at the Proceedings of the Tenth Americas Conference on Information Systems, New York, NY.

Goodall, J. R., Lutters, W. G., Rheingans, P., & Komlodi, A. (2005, Oct. 26, 2005). *Preserving the big picture: visual network traffic analysis with TNV.* Paper presented at the IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05), Minneapolis, MN.

Goodall, J. R., Ozok, A. A., Lutters, W. G., Rheingans, P., & Komlodi, A. (2005, 2005). *A user-centered approach to visualizing network traffic for intrusion detection.* Paper presented at the Conference on Human Factors in Computing Systems, Portland, OR.

Heppner, P. P., Wampold, B. E., & Kivlighan, D. M. (2008). *Research Design in Counseling* (3rd ed.). Belmont, CA: Thomson Brooks/Cole.

Hoffman, L. J., Rosenberg, T., Dodge, R., & Ragsdale, D. (2005). Exploring a national cybersecurity exercise for universities. *IEEE Security & Privacy, 3*(5), 27-33.

Jacobson, D., & Evans, N. (2006). *Cyber Defense Competition.* Paper presented at the 2006 ASEE Annual Conference & Exposition: Excellence in Education.

Komlodi, A., Goodall, J. R., & Lutters, W. G. (2004, 2004). *An Information Visualization Framework for Intrusion Detection.* Paper presented at the Conference on Human Factors in Computing Systems, Vienna, Austria.

Komlodi, A., Rheingans, P., Ayachit, U., Goodall, J. R., & Joshi, A. (2005, Oct. 26, 2005). *A user-centered look at glyph-based security visualization.* Paper presented at the IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05), Minneapolis, MN.

Lakkaraju, K., Bearavolu, R., & Yurcik, W. (2003, 2003). *Nvisionip – a traffic visualization tool for security analysis of large and complex networks.* Paper presented at the International Multiconference on Measurement, Modelling, and Evaluation of Computer-Communications Systems (Performance TOOLS).

Lakkaraju, K., Yurcik, W., Bearavolu, R., & Lee, A. J. (2004, 10-13 Oct. 2004). *NVisionIP: an interactive network flow visualization tool for security.* Paper presented at the 2004 IEEE International Conference on Systems, Man, and Cybernetics, Urbana, IL.

Lakkaraju, K., Yurcik, W., & Lee, A. J. (2004, 2004). *NVisionIP: netflow visualizations of system state for security situational awareness.* Paper presented at the Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, Washington DC.

Livnat, Y., Agutter, J., Moon, S., Erbacher, R. F., & Foresti, S. (2005, 17-19 June 2005). *A Visualization Paradigm for Network Intrusion Detection.* Paper presented at the Proceedings of the 2005 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY.

Luse, A., Scheibe, K. P., & Townsend, A. M. (2008). A Component-Based Framework for Visualization of Intrusion Detection Events. *Information Security Journal, 17*(2), 95-107.

Mennecke, B. E., Crossland, M. D., & Killingsworth, B. L. (2000). Is a Map More than a Picture? An Examination of the Role of Subject Characteristics, Task Complexity, and Technology on Map Reading and Decision Making. *MIS Quarterly, 24*(4), 601-630.

Oline, A., & Reiners, D. (2005, Oct. 26, 2005). *Exploring three-dimensional visualization for intrusion detection.* Paper presented at the IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05), Minneapolis, MN.

Richardson, R. (2008). 2008 CSI Computer Crime & Security Survey. *Computer Security Institute*, 1-30.

Riding, R., & Rayner, S. (1998). *Cognitive styles and learning strategies*. London: David Fulton Publishers.

Rogers, E. (1995). *Diffusion of Innovations*. New York: The Free Press.

Schepens, W., Ragsdale, D., & Surdu, J. R. (2002). The Cyber Defense Exercise: An Evaluation of the Effectiveness of Information Assurance Education. *The Journal of Information Security, 1*(2).

Schepens, W. J., & James, J. R. (2003). *Architecture of a Cyber Defense Compeition.* Paper presented at the IEEE International Conference on Systems, Man and Cybernetics.

Shneiderman, B., & Plaisant, C. (2005). *Designing the User Interface* (4th ed.): Pearson Education, Inc.

Smelcer, J. B., & Carmel, E. (1997). The Effectiveness of Difference Representations for Managerial Problem Solving: Comparing Tables and Maps. *Decision Sciences, 28*(2), 391-420.

Swink, M., & Speier, C. (1999). Presenting Geographic Information: Effects of Data Aggregation, Dispersion, and Users' Spatial Orientation. *Decision Sciences, 30*(1), 169-195.

Takada, T., & Koike, H. (2002, 10-12 July 2002). *Tudumi: information visualization system for monitoring and auditing computer logs.* Paper presented at the Sixth International Conference on Information Visualisation, 2002. Proceedings., Japan.

Thompson, R. L., Higgins, C. A., & Howell, J. M. (1991). Personal computing: toward aconceptual model of utilization. *MIS Quarterly, 15*(1), 124-143.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science, 46*(2), 186-204.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425-478.

Vessey, I. (1991). Cognitive Fit: Theory-based Analyses of the Graphs Versus Tables Literature. *Decision Sciences, 22*(1), 219-241.

Vessey, I. (1994). The Effects of Information Presentation on Decision Making. *Information & Management, 27*(2), 103-117.

Vessey, I., & Galletta, D. (1991). Cognitive Fit: An Empirical Study of Information Acquisition. *Information Systems Research, 2*(1), 63-84.

Vigna, G. (2003a). Teaching Hands-On Network Security: Testbeds and Live Exercises. *Journal of Information Warfare, 3*(2), 8-24.

Vigna, G. (2003b). *Teaching Network Security Through Live Exercises.* Paper presented at the 3rd Ann. World Conf. Information Security Education (WISE 3).

Yin, X., Yurcik, W., Treaster, M., Li, Y., & Lakkaraju, K. (2004, 2004). *VisFlowConnect: netflow visualizations of link relationships for security situational awareness.* Paper presented at the Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, Washington DC.

APPENDIX A

CDCVis Visualization System Questionnaire

Please answer each of the following questions pertaining to the visualization system used for the competition (CDCVis). This information will aid in the modification and improvement of the visualization system. Thank you for your input.

	Strongly Agree					Strongly Disagree
1. I find CDCVis useful.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○
2. Using CDCVis enables me to accomplish some tasks in the competition more quickly.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○
3. Using CDCVis increases my productivity during the competition.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○
4. If I use CDCVis, I will increase my chances of doing well in the competition.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○

If used in the future…	Strongly Agree					Strongly Disagree
5. my interaction with CDCVis would be clear and understandable.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○
6. it would be easy for me to become skillful at employing CDCVis during a competition.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○
7. I would find CDDVis easy to use.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○
8. learning to operate CDCVis would be easy for me.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○

	Strongly Agree					Strongly Disagree
9. Using CDCVis at competitions is a good idea.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○
10. CDCVis makes the competition more interesting.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○
11. Using CDCVis is fun.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○
12. I like working with CDCVis.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○

	Strongly Agree					Strongly Disagree
13. People who influence my behavior think that I should use CDCVis.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○
14. People who are important to me think that I should use CDCVis.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○
15. In general, the support staff has been helpful in the use of CDCVis.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○

	Strongly Agree					Strongly Disagree
16. I have the resources necessary to use CDCVis.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○
17. I have the knowledge necessary to use CDCVis.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○
18. CDCVis is comparable with other systems I have used.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○
19. A person (or group) is available for assistance with difficulties I have with CDCVis.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○

I could employ CDCVis for my use…	Strongly Agree					Strongly Disagree
20. if there was no one around to tell me what to do as I go.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○
21. if I could ask someone for help if I got stuck.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○
22. if I had a large amount of time to work with CDCVis.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○
23. if I just had documentation about CDCVis for assistance.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○

Throughout the competition…	Strongly Agree					Strongly Disagree
24. I intend to use CDCVis.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○
25. I predict I will use CDCVis.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○
26. I plan to use CDCVis.	1 ○	2 ○	3 ○	4 ○	5 ○	6 ○

How many programming courses have you taken? ____________

How many computer/network security courses have you taken? ____________

How many programming languages can you program fluently in? ____________

What is the name of the high school you are representing? ____________________________

Circle your gender. M F

Enter your age. ____________

CHAPTER 6: CONCLUSION

6.1 SUMMARY

The objective of this research is to provide insight into the use of visualization mechanisms for network security. This was carried out through the use of four papers which provided a progression of the research of a network security visualization project.

The first paper provided a new component-based framework for developing network security visualization systems. This framework provided the third and final piece, including both a user-based framework and an input-based framework, for more effective development of network security visualization systems. The paper also provided a review of current network security visualization systems and their respective utilization of the proposed components in the framework.

The second paper provided the development of a network security visualization system, CDCVis. The research utilized a design science methodology for development of the system. The system was developed specifically for use during cyber defense competitions, which is argued, provides a corollary to network security administration.

Third, a paper is provided which details an exploratory evaluation of CDCVis. This provides a first-round evaluation metric for assessing the usefulness and usability of such a system. The research utilizes participant interviews during a live cyber defense competition.

Finally, the fourth paper provides a quasi field experiment to further assess the CDCVis system. The research again utilized participants during two live cyber defense competitions. Specifically, this research looks at the perceived usefulness of the system and its impact on a user's intention to use the system for network security administration tasks in the future. Experience in network security is also found to provide a significant interaction effect.

6.2 FUTURE WORK

While this research provides a first pass at a complete network security visualization research project, further research is needed in the area to further assess the viability of the research.

First, greater research is needed to verify the utilization of the component-based framework for development of network security visualization systems. Specifically, stricter operalization of each specific component is needed in a developed system.

Second, the research test-bed for the developed system, CDCVis, are cyber defense competitions. While it is argued that such environments provide a valid testing ground for such research, it is still not exactly the same as a live corporate environment. More studies pertaining to the use of systems such as CDCVis need to be undertaken by actual network security administrators in live corporate environments.

REFERENCES

Aigner, W. (2009). Mapping, Map, Graph, and Network Visualization Links. Retrieved February 26, 2009, from http://www.infovis-wiki.net/index.php?title=Mapping%2C_Map%2C_Graph%2C_and_Network_Visualization_Links

Conklin, A. (2006). *Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course.* Paper presented at the Proceedings of the 39th Annual Hawaii International Conference on System Sciences, 2006. HICSS '06.

Cowan, C., Arnold, S., Beattie, S., Wright, C., & Viega, J. (2003). *Defcon Capture the Flag: Defending Vulnerable Code from Intense Attack.* Paper presented at the 2003 DARPA Information Survivability Conference and Exposition.

Denning, D. E. (1986). An intrusion-detection model. *IEEE Transactions on Software Engineering, 13*, 222-232.

Few, S. (2006). *Information Dashboard Design: The Effective Visual Communication of Data*. Sebastopol, CA: O'Reilly Media, Inc.

Foresti, S., Agutter, J., Livnat, Y., Moon, S., & Erbacher, R. (2006). Visual Correlation of Network Alerts. *IEEE Computer Graphics and Applications, 26*(2), 48-59.

Goodall, J. R. (2005). *User Requirements and Design of a Visualization for Intrusion Detection Analysis.* Paper presented at the Proceedings of the 2005 IEEE Workshop on INformation Assurance and Security, United States Military Academy, West Point, NY.

Goodall, J. R., Lutters, W. G., & Komlodi, A. (2004). *The Work of Intrusion Detection: Rethinking the Role of Security Analysts.* Paper presented at the Proceedings of the Tenth Americas Conference on Information Systems, New York, NY.

Goodall, J. R., Lutters, W. G., Rheingans, P., & Komlodi, A. (2005, Oct. 26). *Preserving the big picture: visual network traffic analysis with TNV.* Paper presented at the IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05), Minneapolis, MN.

Goodall, J. R., Ozok, A. A., Lutters, W. G., Rheingans, P., & Komlodi, A. (2005). *A user-centered approach to visualizing network traffic for intrusion detection.* Paper presented at the Conference on Human Factors in Computing Systems, Portland, OR.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly, 28*(1), 75-105.

Hoffman, L. J., Rosenberg, T., Dodge, R., & Ragsdale, D. (2005). Exploring a national cybersecurity exercise for universities. *IEEE Security & Privacy, 3*(5), 27-33.

Inc., A. V. (2009). vizSEC. Retrieved February 26, 2009, from http://www.vizsec.org/

Jacobson, D., & Evans, N. (2006). *Cyber Defense Competition.* Paper presented at the 2006 ASEE Annual Conference & Exposition: Excellence in Education.

Kemmerer, R., & Vigna, G. (2002). Intrusion detection: a brief history and overview. *Computer, 35*(4), 27-30.

Komlodi, A., Goodall, J. R., & Lutters, W. G. (2004). *An Information Visualization Framework for Intrusion Detection.* Paper presented at the Conference on Human Factors in Computing Systems, Vienna, Austria.

Komlodi, A., Rheingans, P., Ayachit, U., Goodall, J. R., & Joshi, A. (2005, Oct. 26, 2005). *A user-centered look at glyph-based security visualization.* Paper presented at the IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05), Minneapolis, MN.

Lakkaraju, K., Bearavolu, R., & Yurcik, W. (2003, 2003). *Nvisionip – a traffic visualization tool for security analysis of large and complex networks.* Paper presented at the International Multiconference on Measurement, Modelling, and Evaluation of Computer-Communications Systems (Performance TOOLS).

Lakkaraju, K., Yurcik, W., Bearavolu, R., & Lee, A. J. (2004, 10-13 Oct. 2004). *NVisionIP: an interactive network flow visualization tool for security.* Paper presented at the 2004 IEEE International Conference on Systems, Man, and Cybernetics, Urbana, IL.

Lakkaraju, K., Yurcik, W., & Lee, A. J. (2004, 2004). *NVisionIP: netflow visualizations of system state for security situational awareness.* Paper presented at the Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, Washington DC.

Livnat, Y., Agutter, J., Moon, S., Erbacher, R. F., & Foresti, S. (2005, 17-19 June 2005). *A Visualization Paradigm for Network Intrusion Detection.* Paper presented at the Proceedings of the 2005 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY.

Luse, A., Scheibe, K. P., & Townsend, A. M. (2008). A Component-Based Framework for Visualization of Intrusion Detection Events. *Information Security Journal, 17*(2), 95-107.

McHugh, J., Christie, A., & Allen, J. (2000). Defending yourself: the role of intrusion detection systems. *IEEE Software, 17*(5), 42-51.

Mukherjee, B., Heberlein, L. T., & Levitt, K. N. (1994). Network intrusion detection. *IEEE Network, 8*(3), 26-41.

Richardson, R. (2008). *CSI Computer Crime & Security Survey* Computer Security Institute.

Shneiderman, B., & Plaisant, C. (2005). *Designing the User Interface* (4th ed.): Pearson Education, Inc.

Takada, T., & Koike, H. (2002, 10-12 July 2002). *Tudumi: information visualization system for monitoring and auditing computer logs.* Paper presented at the Sixth International Conference on Information Visualisation, 2002. Proceedings., Japan.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly, 27*(3), 425-478.

Whitman, M. E. (2003). Enemy at the gate: Threats to information security. *Communications of the ACM, 46*(8), 91-95.

Yin, X., Yurcik, W., Treaster, M., Li, Y., & Lakkaraju, K. (2004). *VisFlowConnect: netflow visualizations of link relationships for security situational awareness.* Paper presented at the Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, Washington DC.