6-2011

A Design Methodology and Implementation for Corporate Network Security Visualization: A Modular-Based Approach

Andy Luse
Iowa State University, andyluse@iastate.edu

Brian E. Mennecke
Iowa State University, mennecke@iastate.edu

Janea L. Triplett
Iowa State University, rdtrip@iastate.edu

Nate Karstens
Garmin International, Inc.

Doug Jacobson
Iowa State University, dougj@iastate.edu

A Design Methodology and Implementation for Corporate Network Security Visualization: A Modular-Based Approach

Abstract

Research surrounding visualization for computer and network security has produced differing accepted methods for adequately developing security visualization products. The current work proposes a design methodology that melds the research of the three competing frameworks for security visualization development. In addition, a product that incorporates the proposed design methodology is developed, used, and evaluated. Findings show that users of the system believe the system has increased their effectiveness at performing network security tasks and are likely to use such a system in the future.

Disciplines

Management Information Systems

Comments

This article is from *AIS Transactions on Human Computer Interaction* 3, no. 2 (2011): 104–132. Use for profit is not permitted.

AIS Transactions on Human-Computer Interaction

Transactions on
Human-Computer Interaction

THCI

Original Research

A Design Methodology and Implementation for Corporate Network Security Visualization: A Modular-Based Approach

Andy Luse
Iowa State University
andyluse@iastate.edu

Brian E. Mennecke
Iowa State University
mennecke@iastate.edu

Janea L. Triplett
Iowa State University
rdtrip@iastate.edu

Nate Karstens
Garmin International Inc.
nate@karstens.us

Doug Jacobson
Iowa State University
dougj@iastate.edu

Abstract

Research surrounding visualization for computer and network security has produced differing accepted methods for adequately developing security visualization products. The current work proposes a design methodology that melds the research of the three competing frameworks for security visualization development. In addition, a product that incorporates the proposed design methodology is developed, used, and evaluated. Findings show that users of the system believe the system has increased their effectiveness at performing network security tasks and are likely to use such a system in the future.

.

Keywords: Security, visualization, design science, modular, cyber defense competition, multi-method

Alan Hevner was the accepting Senior Editor. This article was submitted on 6/30/2010 and accepted on 4/26/2011. It was with the authors 164 days for 2 revisions.

Luse, A., B. E. Mennecke, J. L. Triplett, N. Karstens, and D. Jacobson (2011) "A Design Methodology and Implementation for Corporate Network Security Visualization: A Modular-Based Approach," *AIS Transactions on Human-Computer Interaction* (3)2, pp. 104-132.

INTRODUCTION

The purpose of viz is insight, not pictures.
-Ben Shneiderman (Visualization Security Conference – VizSec 2008).

The importance of corporate network security in today's network-centric computing environment has become a critical issue for most corporate network technicians. Organizations are being forced to devote significant additional resources to network security as reported incidents – including external attacks, internal breaches, malicious code, etc. – continue to increase and affect a greater number of mission-critical systems (Dhillon and Torkzadeh, 2006, Richardson, 2009). Recently, visualization has been proposed as an effective mechanism for assisting security professionals with corporate network security management, and with the increase in the power and flexibility of mobile and desktop computing platforms, visualization tools are likely to increasingly be integrated into commercial security products (see Luse et al., 2008 for an overview of security visualization research).

Various design methodologies for developing effective security visualization products have been proposed. Three design mechanisms have emerged as the primary methods for effective network security visualization: the *user-based framework* (Goodall et al., 2005), the *alert-oriented framework* (Foresti et al., 2006), and the *component-based framework* (Luse et al., 2008). While a variety of security systems have been developed that use both the user-based and alert-oriented frameworks separately, no research has explored the development of a comprehensive network security visualization system that incorporates all three frameworks. Second, and maybe more importantly for security professionals and IT researchers no one system has been developed that implements all the components described in the component-based framework, which itself builds on information visualization theory proposed by Shneiderman (2005). Therefore, research is needed to develop a methodology for effectively designing network security visualization systems that can provide for successful implementation of all aspects of the three network security visualization frameworks.

Three purposes drove our research: 1) to propose a design methodology for developing network security visualization systems which would provide the potential for implementing all aspects contained within the three dominant frameworks for network security visualization, 2) to develop an IT artifact which would provide an exemplar and instantiation of the proposed design methodology, and 3) to deploy this artifact in a live test-bed environment in which it would be used by the potential members of the target audience of corporate network administrators.

The rest of this manuscript is formatted as follows: First, the background section furnishes necessary contextual information pertaining to the three dominant frameworks for network security visualization. Next, we propose a design methodology for developing network security visualization systems. The Cyber Defense Competition Visualization section offers an IT artifact exemplar of the proposed design methodology. A requirements review and qualitative and quantitative assessments provide an evaluation of the developed system. Finally, we present a discussion and concluding remarks regarding the framework, the system, and our research.

BACKGROUND

Security Visualization Frameworks

Research examining visualization for network security has increased during the past decade. High false alarm rates of traditional intrusion detection systems have provided impetus for giving the corporate security administrator a more active role in securing the corporate network (Luse et al., 2008). With security visualization tools, corporate network administrators have a more complete arsenal for detecting and mitigating security threats to the network. Visualization systems allow for "visual" data mining of network traffic (Yurcik et al., 2003) by using the parallel processing power of the human visual system (Breitmeyer, 1992). Also, traditional intrusion detection systems utilize signature-based mechanisms for detecting possible nefarious network activity, but since an attack must be known beforehand to create these signatures, signature-based systems are not able to recognize novel attack sequences (Luse et al., 2008). Conversely, security visualization systems provide the ability for anomaly-based intrusion detection, which allows for the detection of nefarious network activity based on deviations from established traffic norms. This enables the detection of novel attacks that do not yet have a signature script in place (McHugh et al., 2000). While visualization systems for security can also use signature-based mechanisms, the sheer volume of network data and limits on human memory make an anomaly-based approach more realistic. When viewing a visualization system, humans are typically better at seeing surges or spikes that are "outside the norm" (anomaly-based) than remembering how a particular attack looked visually from one time to the next (signature-based).

To build effective security visualization systems, a framework must be in place that provides the processes and components necessary for designing the system. Three different security visualization frameworks have been proposed, including a user-based framework, an alert-oriented framework, and a component-based framework (Luse et al., 2008). These frameworks provide three separate views of the necessary requirements for effectively designing a security visualization system. While each framework overlaps somewhat with the others, these three frameworks offer very distinct views of development.

The user-based framework proposes design metrics for security visualization based on the system user's perspective (Goodall, 2005, Goodall et al., 2004, Goodall et al., 2005, Komlodi et al., 2004, Komlodi et al., 2005). The researchers who proposed this framework relied on prototype evaluations and interviews of security analysts with expertise in network security as the source of their data. Based on these observations, they developed a model consisting of a framework composed of three phases of user interaction with the system: monitoring, analysis, and response (Luse et al., 2008). Each phase involves specific user tasks with the system including:

- Monitoring: monitoring and identifying potential attacks
- Analysis: analyzing alerts and supporting data to diagnose network attacks, and
- Response: responding to identified nefarious activity, documenting, and reporting information

The alert-oriented framework proposes design metrics patterned after security alerts that occur on the corporate network (Foresti et al., 2006, Livnat et al., 2005). The alert-oriented framework asks the developer to focus on the inputs to the security visualization system (i.e., the alerts) and to base the system design around these alerts (Luse et al., 2008). This framework, or w^3 premise, focuses on three attributes of an alert that occurs on the network, specifically:

- When: At what time did the alert happen?
- Where: At what location on the network did the alert take place?
- What: What type of alert was triggered?

The component-based framework proposes design metrics through the use of specific visualization components that maximize user facility (Luse et al., 2008). These components are derived from research in information visualization (Shneiderman and Plaisant, 2005) and operational information dashboard designs (Few, 2006). The proposed components provide the necessary building blocks for designing effective security visualization systems. Specifically, these components include (Luse et al., 2008):

- Overview: provide an overview of activity on the network,
- Zoom: provide the ability to zoom displays to areas of interest,
- Filter: filter out unneeded information items,
- Details-on-demand (Secondary Throughput): provide specific information about a particular network activity,
- Relate: provide views of relationships between items on the network,
- History: provide views of the history of activity on the network,
- Extraction: provide current state indicators of network activity at a specific moment, and
- Primary Notification: provide notification that a security alert has occurred.

The *complete security visualization framework* proposes that a comprehensive design framework for security visualization would include all three of the aforementioned frameworks; that is, the user-based framework, the alert-oriented framework, and the component-based framework (see Figure 1 for a diagrammatic representation) (Luse et al., 2008). In considering these three elements together, we conclude that activity theory represents an appropriate theoretical model for tying these three frameworks together. Activity theory (Engeström, 1987) suggests that the analysis of certain phenomena involving human actors resides within a particular context (O'Leary, 2010) and that activities represent a form of doing or acting by an actor with a focus on and a goal of engaging with an object. As a result, activity theory posits that people engage in collective activities that are outcome-driven and socially determined and that these outcomes are mediated through a combination of context, tools, and symbols. This indicates that in any given activity system, the subject, object, and tool are all present during human action and need to be considered and applied when the user responds with the objective of generating an outcome from the object of the activity (e.g., a user responds to a security alert as an object within an activity system).

Activity theory has been applied in a number of problem areas to define where, when, and how social actors can, in a collective context, use tools to solve problems; it has therefore been applied both as a theory to inform educational and learning system design as well as the design of software and hardware systems (Bedny and Karwowski, 2003, Nardi, 1996). When users interact with tools and objects they do so in a historical context in which learning and understanding take place. Thus, activity theory presents a useful perspective for framing the design and development of new tools and processes, such as our proposed visualization system (Kaptelinin and Nardi, 2006). Within the context of security visualization, the network administrator (i.e., the subject or user) utilizes a system composed of visualization components (i.e., tools) to analyze various objects (i.e., alerts) on the network (i.e., part of the context). In other words, if we consider the three frameworks jointly, while overlap exists between these frameworks, each "centers" on one of the three dimensions suggested by activity theory. The user-based perspective corresponds to the "subject" and defines what is needed by the user to "learn" and "understand" the context in which alerts occur. The component-based framework corresponds to the "tools" and defines what is available to be used to respond. Finally, the alert-oriented framework addresses the focus of security tasks and activities and defines what the focus of an alert and response activity will entail. In the context of an activity theory perspective, we see how these three frameworks complement one another. Further, by considering this problem in the context of activity theory, we also see that all three of these elements (i.e., tools, users, and objects) must be considered when designing a network security visualization system; by doing so a more robust framework for security visualization system design will be achieved.

The problem is that no current security visualization system includes all necessary framework components. Within the component-based framework alone, a review of the literature demonstrated that no one system includes all eight visualization components deemed necessary for effective security visualization. Specifically, no research has explored the inclusion of all components of the component-based framework in one visualization system. Furthermore, from an overarching perspective, no research has attempted to integrate all items from all three frameworks into one system. Research needs to first explore a design methodology that holds potential to include all items from all three security visualization frameworks. Second, research should develop a system that incorporates this design methodology.

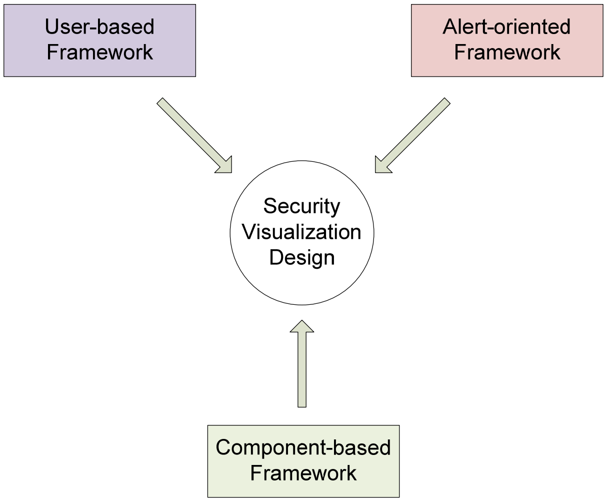


Figure 1: Complete Security Visualization Design Framework (Luse et al., 2008)

Modular Programming

Modular programming is a relatively old concept within software engineering that involves decomposing systems into various constituent modules and using these modules to compose a system (Griswold et al., 2006). Other concepts that are related to modular programming have also been used, including object-oriented programming, component-based programming, and aspect-oriented programming (Kozaczynski and Booch, 1998). Modular programming allows for different tasks within a software system to be divided into separate, distinct modules that are independent from other modules in the system (Parnas, 1972). Modules are then combined into groups that each have their own interface. These interfaces allow for communication among the modules and also common information dissemination to all modules in a group (Bauer et al., 2003).

One problem associated with the lack of research and/or software products that can accommodate each of the security visualization frameworks is the lack of multiple views. While some research has begun to look at multiple views for network security visualization (Ball et al., 2004, Lakkaraju et al., 2003, Lakkaraju et al., 2004a, Lakkaraju et al., 2004b), no research has explored modular-based mechanisms for developing visualization objects that can support all of the components present in the three frameworks. By developing a modular visualization design methodology, the user could implement any of the desired components and mix and match these components into one comprehensive visualization system.

DESIGN METHODOLOGY

Our proposed design methodology for network security visualization incorporates a modular design approach to design a system with the components listed in all three existing frameworks. As described above, this method offers many advantages, but our primary objective is providing the ability to incorporate all features of the three existing network security visualization frameworks. By using a modular approach, separate visualization modules can be utilized to implement all desired components of the frameworks as well as offer extensibility for future revisions to these or other frameworks.

Figure 2 provides a graphical representation of the design methodology for developing a modular network security visualization system. The methodology includes three primary mechanisms that can be applied to designing a security visualization system. First, each visualization system will be composed of one or more paradigm frames. A paradigm is described as a pattern, archetype (Merriam and Webster, 2004), or a way of viewing reality (Kuhn, 1996). Therefore, a paradigm describes different mechanisms by which subject matter is viewed, or how reality is framed by the user. The paradigm frame allows for the visualization to be viewed from different contextual loci. For example, one frame of the visualization may provide a view of information that is more user-specific, while another frame may provide a view of information in the context of security alerts on the network as a whole. Figure 2 demonstrates three features of the paradigm frame: first, it shows how frame1 can be composed of two modules; second, it shows how modules can be subsets of other modules depending on the level of analysis; and, third, it demonstrates how both modules receive data from the data1 and data2 information sources.

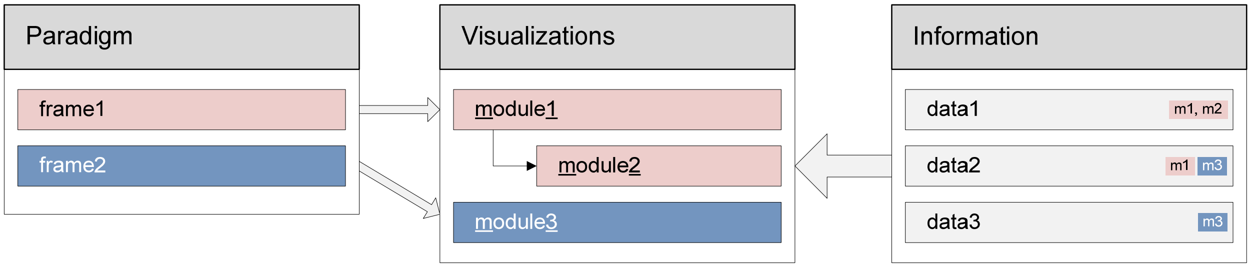


Figure 2: Network Security Visualization Design Methodology

The second set of mechanisms derived from our security visualization design methodology consists of the actual *visualization modules*. As described above, each module is designed around a distinct task or context. For our design methodology, each module is composed of a distinct visualization mechanism that is designed with particular attributes pertaining to security visualization. These attributes can be composed of anything of interest to the user, and specifically provide a mechanism for accommodating each aspect in the three visualization frameworks. Each module can be further used to drill down into the data within a specific focus area. For example, a pie chart visualization could show all traffic on the network or be further defined to only show traffic for a specific organizational unit (this is a form of inheritance, on which we elaborate below). Each paradigm frame is composed of one-to-many modules. These modules can be mixed and matched to provide the most appropriate visualization system for the specific corporate network environment.

Finally, the third mechanism associated with the security visualization design methodology consists of *informational sources*. While the visualization modules provide for critical user interaction with the system, data is needed for running these modules. Separate datasets provide information to one or more modules based on the informational requirements of the module. As illustrated in Figure 2, the frame1 paradigm is composed of two modules (a module and a child module). Furthermore, in this example module1 requires information from data1 and data2 while module2 only requires information from data2.

Object-oriented programming techniques are used to implement the modules for this design methodology. Figure 3 represents a high-level UML diagram depicting the three mechanisms described above. Each separate area is developed as a super-class that its constituent subclasses can implement. The subclass inherits operations and internal structure that allow it to perform the same actions as the super-class and extend these operations to its own needs (Johnson and Foote, 1988). For the proposed design methodology, a super-class called *Paradigm* is designed as a class. While no *Paradigm* object is ever instantiated explicitly, paradigm frames for the system are created that implement the *Paradigm* class by extending its operations and structure. Each *Paradigm* frame in turn instantiates one or more *Visualization* modules and includes them in the visualization's *Paradigm*. Also, specific data *Information* sources are instantiated that are then allowed to pass this information to the *Visualization* module(s) that need the particular *Information*. The *Paradigm* frame acts as an interface object in the modular visualization system (Bauer et al., 2003).

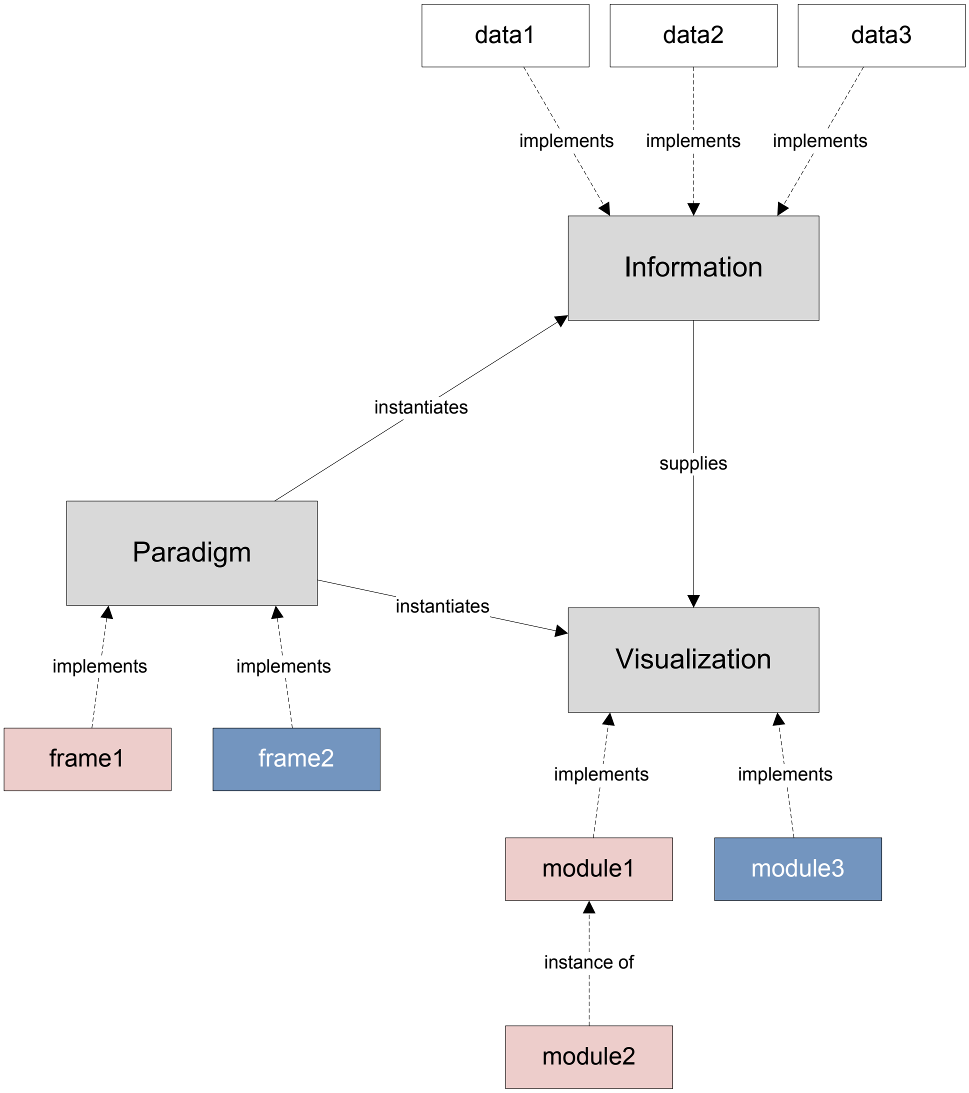


Figure 3: UML Depicting Development of the Design Methodology

An XML definition schema was also designed specifically for the security visualization system. XML has been utilized as a viable technology for data exchange using a standard language (Aalst and Kumar, 2003). XML can be employed to allow visualization designers to define tags that detail the structure of a document (Miller et al., 1998, St. Laurent, 1997) and to delineate an interface. The visualization designer can then use an XML file as a configuration file that the visualization program will use to create the interface. The XML elements defined for this security visualization design methodology are quite simplistic, but they will allow the visualization designer to mix and match modules to craft a security visualization system that fits their individual needs.

The first component in the XML schema is the *frame element*. There can be just one frame or many frames depending on the types of paradigm perspectives the user wishes to accommodate. Also, multiple frames accommodate multiple physical displays by the system. The frame object requires a name as well as the numerical delineation of the physical display the frame will use.

```
<frame name="frame1" display="1">

      ...

</frame>
```

Second, *informational sources*, or data, must be defined so the visualization modules of the system can use them. There can be one or many data objects depending on the informational needs of the modules employed by the system. Each data object requires both a name and a type, where the type is the kind of data that will be provided.

```
<data name="data1" type="datatype1" />
```

The third element that is defined in the XML file consists of modules. As noted earlier, there can be one or many modules within the system. Each module requires a name as well as screen coordinates identifying where the module will appear on the screen. This includes the left and top coordinates of the upper left corner of the module as well as the width and height of the module. Each module also contains from one to many child *datasource* objects that indicate which data object the module will use from the data specifications. Unlike the other two object types, modules are themselves children of a specific frame object. A frame can contain from one to many modules depending on the screen area provided by the physical screen space used by the specific frame.

```
<frame name="frame1" display="1">

             <module name="module1" left="0" top="0" width="1024" height="384">

                    <datasource name="data1" />

             </module>

             <module    name="module2"    left="0"    top="384"    width="1024"

height="384">

                    <datasource name="data1" />

                    <datasource name="data2" />

             </module>

             <module    name="module3"    left="512"    top="384"    width="1024"

height="384">

                    <datasource name="data3" />

             </module>

      </frame>
```

CYBER DEFENSE COMPETITION VISUALIZATION

This section describes the implementation of our design methodology. This implementation provides a useful mechanism for verifying that the proposed system is a practical solution to network security visualization by launching a viable instantiation of an IT artifact (Orlikowski and Lacono, 2001).

We chose Cyber Defense Competitions (CDCs) as the target context for the implementation of the network security visualization system. Cyber Defense Competitions 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 simulated corporate IS infrastructures (Conklin, 2006, White and Williams, 2005). Competitions also increase awareness and understanding of security exploits, tools, and countermeasures in the rapidly changing network security environment (Jacobson and Evans, 2006). Competitions allow participants to use skills and theories learned in the classroom in a live setting (Hoffman and Ragsdale, 2004). This setting offers a valid testing environment for the network security visualization system because it involves professionals and students engaged in a realistic, live network security scenario. Several competitions have been run including seven involving student groups from the sponsoring university, three involving student groups from state community colleges, four involving student groups from several different colleges and universities, and four involving high school student groups.

The CDCs utilized as a test environment for this research were conducted at a large Midwestern public university in the US (Jacobson and Evans, 2006). The competitions consisted of four primary teams which were designated using color associations. These included the blue, green, red, and white teams as described below (see Figure 4).

- Blue Teams: Each Blue Team consisted of between four and eight students. These teams were tasked with running their own pseudo-corporate network. This involved providing services to users – including email, file storage, shell access, and maintaining a corporate web presence – all while defending their network from attack. The visualization system was targeted specifically at these individuals, although all teams and external participants used the visualization system.

- Green Team: This team of local professionals and graduate students acted as users of the services provided by the Blue Teams. Each Blue Team provided the Green Team with the credentials necessary to access the services available on their respective networks (email, file storage, etc.). The Green Team members acted as users of the Blue Teams' systems, and therefore measured system usability. Blue Teams were given points for each required service that the Green Team was able to access at periodic periods throughout the competition.

- Red Team: The Red Team consisted of local professionals, professors, and advanced graduate students tasked with attacking the Blue Teams' networks. These individuals were able to use almost any means necessary to compromise the Blue Teams' systems. The Red Team used hacking techniques to attack Blue Team networks throughout the entire competition. The Red Team divided their members and assigned specific groups to attack each Blue Team's network. Each successful attack by the Red Team resulted in a loss of points from the Blue Team that was successfully hacked. The number of points subtracted was decided upon based on the severity of the attack, the ease of performing the attack, etc. An important point to note is that the Red Team members were located in a separate physical location and had no interaction with members of the Green Team or the Blue Teams.

- White Team: The White Team acted as administrators for the competition as a whole. They provided assistance to all teams and also functioned as intermediaries between the Red Team and other teams if necessary. Each Blue Team could also submit reports to the White Team detailing any type of nefarious activity that had occurred on their network (i.e., attacks by the Red Team) and the actions they had performed to mitigate or correct this activity. This allowed the Blue Teams to redeem points that they may have lost due to actions taken by the Red Team and it also provided a chance for the Blue Teams to learn from prior attacks. The White Team was also in charge of tallying the scores of all teams (Green, Red, and White) at the conclusion of the competition.

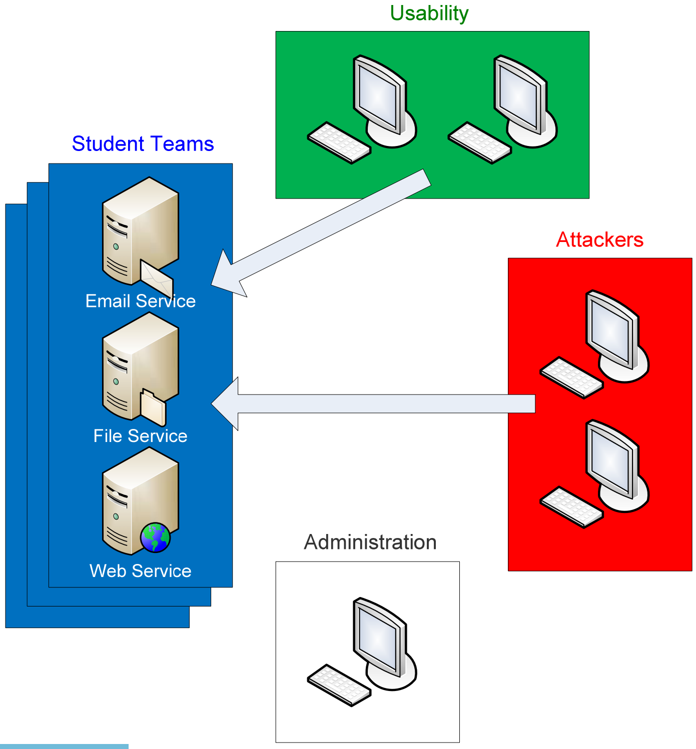


Figure 4: Team Layout for Cyber Defense Competition Target Testing Environment

These competitions typically lasted for eight to 16 hours. The Blue Teams were allotted approximately one month to setup their machines using remote services, and they were allowed to perform last minute configurations beginning one day prior to the competition date. The competition has been run as either an all-day event or as an overnight event to create a stressful, realistic scenario.

Development

CDCVis (Cyber Defense Competition Visualization) was designed as an IT artifact to incorporate the proposed design methodology, specifically for cyber defense competitions. The system uses elements designed for visualization of network traffic and visual analysis of current network activity. These elements were designed using all three security visualization frameworks outlined in a previous section (Luse et al., 2008). We now provide details pertaining to the methods used in the construction of the artifact (Hevner et al., 2004). Additionally, we also present a use case diagram (Figure 5) to further describe the interaction of a user with the system that was developed through this process.

The development of CDCVis followed the classic Systems Development LifeCycle (SDLC) waterfall methodology (Royce, 1970) and was performed by 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 CDC coordinators offered their requirements for the system both to the competitors as well as the coordinators and workers. Coordinators also discussed ideas about the features and capabilities of the visualization mechanisms the system should contain. Then, 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 consisted of a single machine containing three high-end graphics cards capable of supporting six separate physical 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 regarding the programming language, the programming environment (IDE), the graphical library, and the backup and dissemination mechanism. Java was selected as the development programming language because it supports object oriented and class-based programming, which are compatible with our proposed modular design methodology. 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.

Analysis: The team met with the event coordinators a second time to develop a better understanding of the requirements. Specifically, they engaged in discussions regarding each stakeholder for the system including each type of team (i.e., blue, green, white, red) as well as outside supporters of the competition. They also discussed more detailed visualization requirements.

Program Design: The program design phase involved a highly iterative approach. During this process, members of the design team first sketched representations for visualization mechanisms they envisioned for the system. Using these initial sketches, they decided upon a specific subset of visualization parameters and capabilities, and made more detailed electronic drafts for each module. After the individual modules had been finalized, the design team developed more elaborate electronic screen mockups showing possible aggregations of the individual modules within overarching paradigms.

Coding: The coding process was a highly object-oriented approach that included 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 development team member was then responsible for building a subset of classes.

Testing: Testing consisted of “plugging” the visualization modules into the container paradigms designed for the overall CDCVis system. We used various combinations of modules as well as various aggregations of information within paradigms. Also, we ran traffic simulations to verify that the system was adequately capturing and displaying the proper information.

Operations: Finally, the system was used at a number of CDCs. Valuable information was gathered at each CDC, and various changes were made as use continued by revisiting relevant stages of the development process.

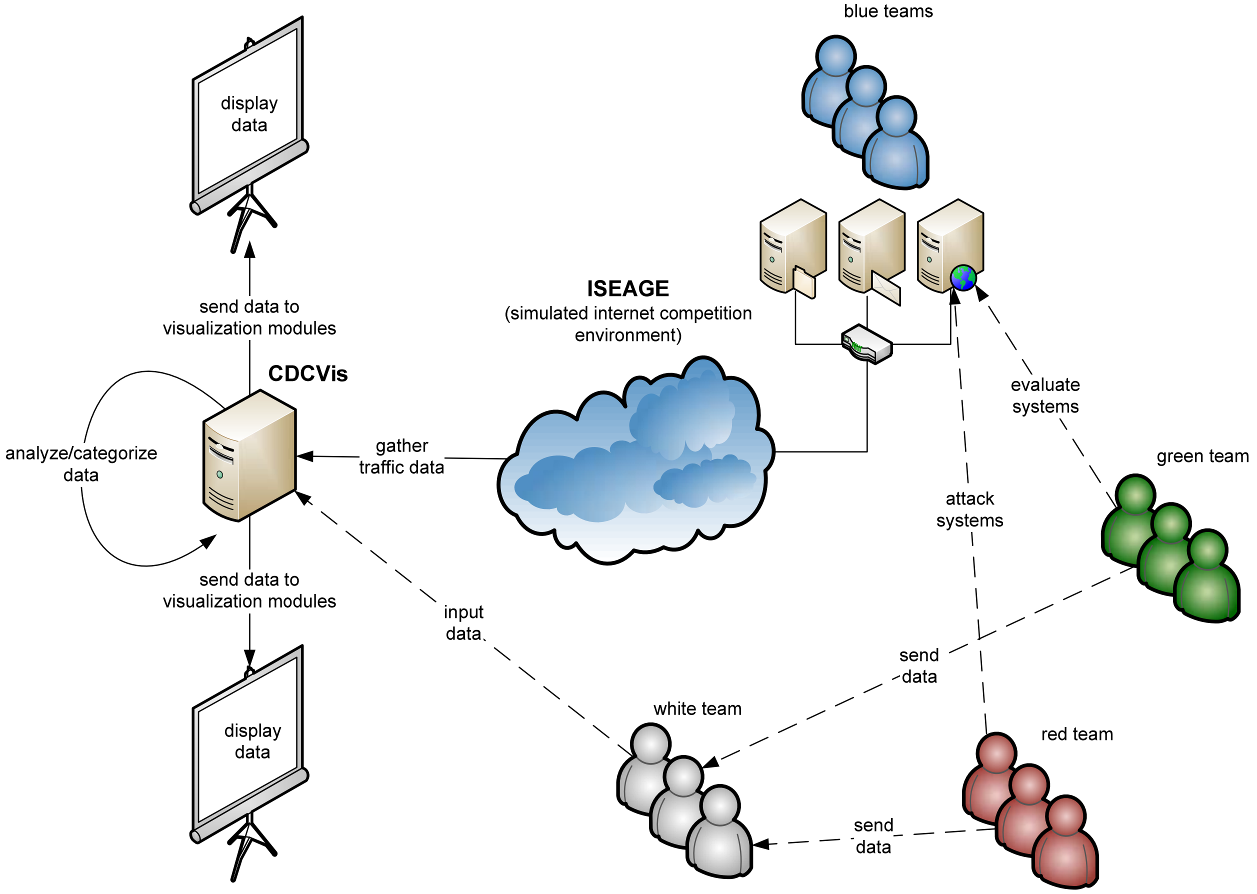


Figure 5: CDCVis Use Case Diagram

System Explanation

The visualization system for the CDC is delineated by three paradigm views that encompass three primary aggregations of information within the competition. The following explanations are categorized by these three overarching paradigm frames, with each component within each frame represented as a separate modularized visualization. Table 1 provides a delineation of the types of data that are used as input to the system, the sources of this data, and the modules that use the data including the paradigm frame that contains the module.

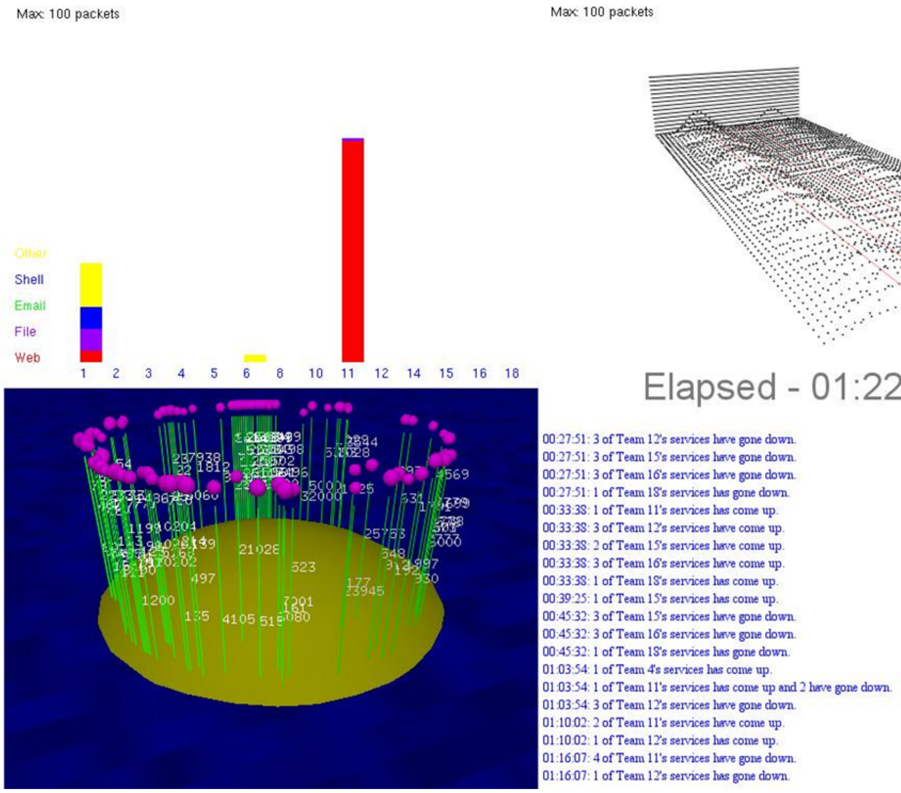
Global Network Paradigm Frame

The global network paradigm frame provides a composite view of the network, which includes information and traffic pertaining to all team subnets involved in the competition. The screen capture shown in Figure 6 provides an example of the global network paradigm frame. The frame is composed of the following visualization modules from left to right, top to bottom: Composite Bar Graph, NetSquall, Island, and Announcements (See Figure 6).

Composite Bar Graph: The composite bar graph is a commonly used 2D statistical visualization that 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:

- Web – HTTP, HTTPS
- File Transfer – FTP, SMB, NetBIOS
- Email – SMTP, POP2, POP3, POP3+SSL, IMAP4, IMA4+SSL
- Shell (Terminal) – Telnet, Telnet+SSL, SSH
- Other

The composite bar graph allows each of the five types of traffic to be represented using unique colors all within a single bar. Each bar then represents the relative volume of the five types of traffic originating from or destined for a particular Blue Team (numbered along the bottom of the graph).



```
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 1: Global Network Paradigm Frame

NetSquall: Like the composite bar graph, NetSquall (see Figure 7) provides a statistical graph with heights representing the number of packets for each of the five traffic types 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 functioning 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.

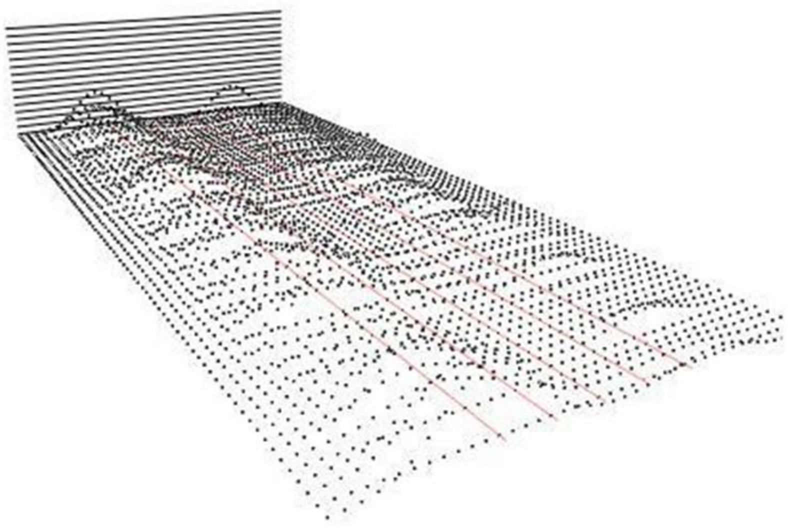


Figure 7: NetSquall Visualization Module

Island: The Island visualization provides a unique 3D view of current traffic on the network. The system was developed by Oline and Reiners (2005) as a 3D method for analyzing traffic on a network. The system resembles an island containing trees sprouting from the base. The positions of the trees correspond to the ports that have traffic. The ports start at the outside of the island with one and increase, spiraling towards the center. The smaller and more frequently used ports are represented using a larger coverage area compared to the less frequently used ports. Each tree also contains a fruit at the apex that, based on its relative size, indicates the amount of traffic occurring on that port (see Figure 8). With permission from its creators, the Island was adapted as a module to be used within the CDCVis system and helps to show the power and reusability of a modular-based visualization system.

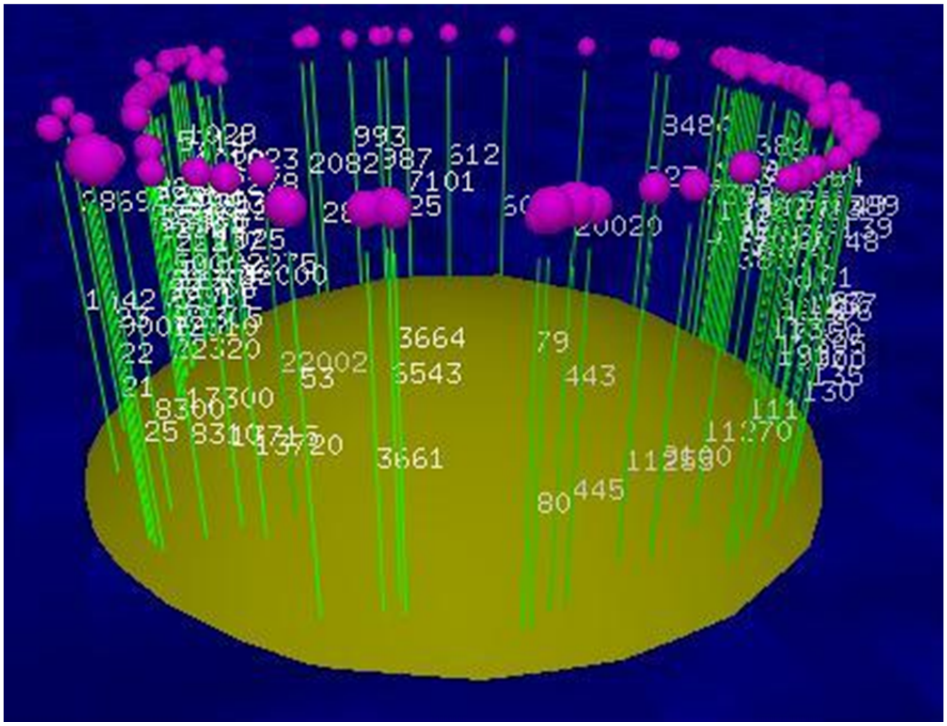


Figure 2: Island Visualization Module (Oline and Reiners, 2005)

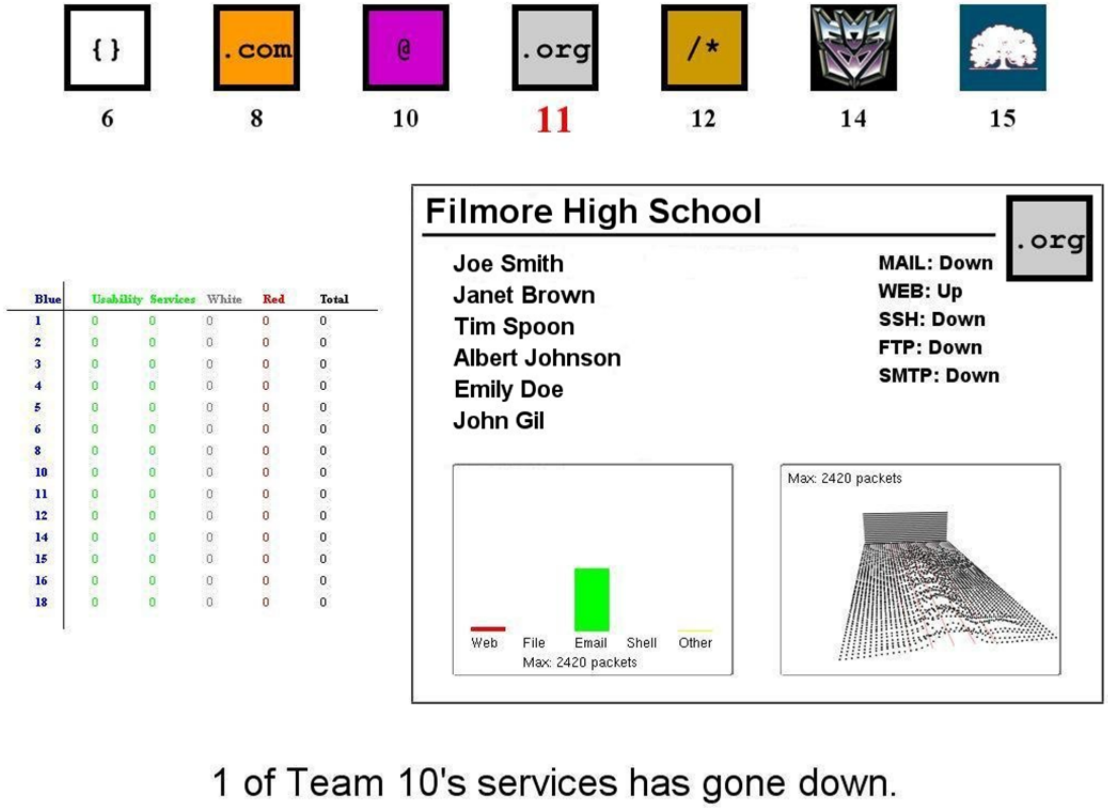
Announcements: The announcements component provides users with various pieces of information that they may find useful throughout the competition. Given that a variety of expected as well as unexpected events occur during the course of a CDC, the announcements are useful for disseminating pertinent information to participants. Examples of the types of announcements include team-specific service interruptions or system-wide network events.

Team Subnet Paradigm Frame

The team subnet paradigm frame provides information and current traffic patterns pertaining to each Blue Team's network subnet. The visualization operates on a timer to switch between teams at predefined time intervals; teams can also request their specific team data to be shown in the frame. Figure 9 represents a typical team subnet paradigm frame composed of the following visualization modules: represented left to right, top to bottom, the Team Logo Strip, the Scoreboard, the Team Information Panel (composed of unique team information including Service States, Bar Graph and NetSquall modules), and the Announcement Strip.

Team Logo Strip: The Team Logo Strip along the top provides a pictorial representation of each Blue Team that is included in the specific Team Subnet Paradigm Frame (multiple Team Subnet Paradigm Frames are used for large competitions). These pictures consist of a logo that designates the team with a corresponding team number included below each logo. As the Team Information Panel (below) is cycled to view each team subnet, the number of the team currently being displayed is enlarged and the color changed in the Team Logo Strip (e.g., Team 11 in Figure 9).

Scoreboard: The scoreboard offers each of the Blue Teams a synopsis of their current point assessments from the various judging teams in the competition. This module features a grid-like scoreboard alignment with the number of the participating Blue Team on the left side and the judging teams along the top. The current scores of each of the three judging teams are provided as well as the combined total score for each team[1].



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 3: Team Subnet Paradigm Frame

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.

- Team Name: Used to describe the team
- Team Members: Used to list each team member
- Service States: Provides feedback to the Blue Team about which of the services that they are expected to be providing are available to the Green Team.
- Bar Graph: Represents each of the five traffic types, with each type given its own bar. The height of the bar represents the amount of the specific type of traffic either coming from or going to the specified subnet. This module is a slight modification of the Composite Bar Graph in the Global Network Paradigm Frame.
- NetSquall: Shows the five types of traffic levels with a representation of history as with the global view.
- However, at this level only the traffic pertaining to the specified Blue Team is displayed[2]. The NetSquall is a modification of the NetSquall used in the Global Network Paradigm Frame.

Announcement Strip: The Announcement Strip is used to display the most recent content of the Announcements module in the Global Network Paradigm Frame to highlight current notifications.

Location-Based Paradigm Frame

The location-based paradigm frame provides information pertaining to the subnet location of traffic origination and destination. This frame offers geographical information pertaining to network traffic to supplement subnet-based information. Figure 10 shows an example of the location-based paradigm frame consisting of one module, the map.

Map: The map module offers a visual representation of network traffic by drawing lines to and from the participating teams to the network hub. This is, of course, a simulated representation of distance because team subnets within the CDC are all located in the same geographical area during the competition. Nevertheless, the module allows for an alternate view of traffic patterns over the network that could be used in a multi-location corporation.

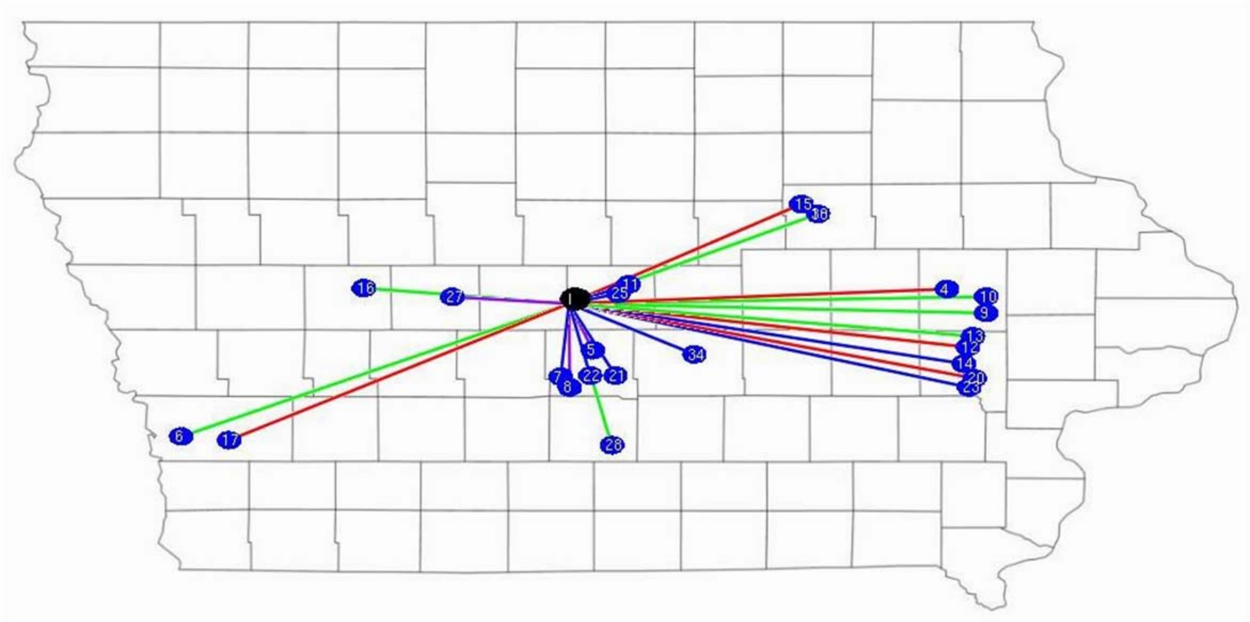


Figure 4: Location-Based Paradigm Frame

Table 1: CDCVis Input Data Including Origination, Destination, and Paradigm Frame

Data	Origination	Destination Module(s)	Paradigm Frame
Network Traffic	ISEAGE network (including blue teams)	Composite Bar Graph	Global
		NetSquall	Global
		Island	Global
		Bargraph	Team
		NetQuall	Team
		Map	Location
Service Availability	White team	Service States	Team
Announcement	White team	Announcements	Global
Team Information	White team	Team Logo Strip	Team
		Team Information	Team
Score	White team	Scoreboard	Team
	Green team		
	Red team		

EVALUATION

This research has proposed and implemented a design framework for network security visualization systems to provide a product for network security administration that accommodates all components of the three security visualization frameworks, and is also a usable product for network administrators. We then conducted an evaluation to assess both the proposed design framework and the implemented CDCVis artifact with these initial design goals in mind. WE used multiple types of evaluation and included a requirements review as well as qualitative and quantitative evaluations of the developed CDCVis system.

Requirements Review

The first evaluative mechanism reviewed both the design framework and the implemented artifact for accommodation of the components within the three security visualization frameworks used. Table 2 provides an overview of the modules in the CDCVis system and the corresponding components each incorporated.

Table 2: Security Visualization Framework Components Supported by CDCVis Visualization Modules

Security Visualization Framework Components	CDCVis Visualization Modules										
	Global Network Paradigm Frame				Team Subnet Paradigm Frame						Location-Based Paradigm Frame
	Composite Bar Graph	NetSquall	Island	Announcements	Team Logo Strip	Scoreboard	Team Information	Service States	Bargraph	NetQuall	Map
User-based Framework											
Monitoring	x	x	x	x		Modules designed for the competition and not for security visualization		x	x	x	x
Analysis				x				x			
Response				x				x			
Alert-oriented Framework											
When		x		x						x	
Where	x	x		x							x
What	x	x	x	x				x	x	x	x
Component-based Framework											
Overview	x	x	x								x
Zoom									x	x	
Filter									x	x	
Details-on-demand (Secondary Throughput)				x							
Relate											x
History		x	x	x						x	
Extract	x								x		
Primary Notification	x	x	x	x				x	x	x	x

Table 2 shows that all components within the three security visualization frameworks were accommodated by at least one module within the CDCVis implementation. While no prior research has investigated the ability of a security visualization system to accommodate the components of all three security visualization frameworks, Luse and colleagues did specifically investigate the ability of security visualization systems to include all components within the component-based framework alone (2008). Of the 23 systems they investigated, no single system provided support for all components within the component-based framework. Furthermore, they also showed that with the exception of three of the components (i.e., overview, primary notification, and secondary throughput), all the remaining components were represented in less than 50 percent of the systems. Our proposed design framework provides the capability to accommodate all components in all three security visualization frameworks using multiple visualization modules within one omnibus visualization system. The implication is that this allows the construction of systems that are flexible and adaptable to a specific situational context. For example, while some settings may call for the use of only specific modules, this design framework is sufficiently flexible to accommodate all of the components. Research has shown that particular corporate environments call for a subset of visualization mechanisms (Foresti et al., 2006, Goodall, 2005, Goodall et al., 2004, Goodall et al., 2005, Komlodi et al., 2004, Komlodi et al., 2005, Livnat et al., 2005, Luse et al., 2008); therefore, the ability to mix and match modules is beneficial when a context calls for a subset of capabilities and functions.

Qualitative Evaluation

The second evaluative mechanism consisted of a two-part qualitative study involving users and administrators of the CDCVis system. The primary purpose of this study was to gain an initial overview of general user attitudes towards the system as a first-pass assessment. The participants for the first phase of the study were students who participated in one CDC at a large Midwestern university. The student participants were individuals pursuing college majors in network and security administration. Participants for the second phase were professionals who had a combined level of experience of two years as Blue Team participants, five years as Red Team participants, and 16 years as White Team administrators (see Appendix A for a copy of the open-ended questions used).

Students involved in the first phase of the study came from eight different colleges/universities across one state with school size ranging from community colleges to research-intensive universities. Each team consisted of four to seven members. Participants were provided with the competition scenario one month prior to the competition detailing a fictitious corporate environment they were expected to setup and administer. The teams were allowed to utilize four computers provided by the host university as well as any legally obtained software. The competition began at 5:00 p.m. on a Friday and concluded at 11:00 a.m. the next day.

Data Collection

The first phase of study of the CDCVis system was conducted about seven hours into the competition so that the student participants had sufficient time to become acquainted with both the competition and the CDCVis system. One of the developers of the CDCVis system was on-hand assisting with the administration of the competition and responding to questions pertaining to the operation of the CDCVis system. Six different teams were interviewed with seventeen individuals contributing to the discussion. The purpose of the interviews was to:

- Explore general attitudes about the visualization,
- Assess how the CDCVis visualization system was used during the competition, and
- Identify any problems that might lead to improvement of the system.

User attitudes were defined as the tendency to respond positively or negatively to a given person, situation, or object (Aiken, 2002). Usage was operationalized according to how the visualization system helped participants accomplish tasks. Additionally, problems were represented and measured by documenting and classifying user reports of frustration. Two hours of interviews and discussions were recorded, resulting in 145 statements from participants about the visualization system. Coding of the data followed the suggested procedures recommended by usability practitioners (Beyer and Holtzblatt, 1998, Kuniavsky, 2003) and an affinity diagram was also created to reveal common issues and themes (Beyer and Holtzblatt, 1998).

The second phase of the qualitative study involved in-depth interviews with two professionals who had been involved in the CDC for at least five years. These informants had served in various roles (i.e. attackers and administrators) before and after the introduction of the CDCVis visualization system. The professionals were asked to compare and contrast the competition prior to and after the visualization system was implemented. Questions also addressed such topics as how the visualization system impacted student decision-making, data contextualization, team comparisons, as well as student fun and learning. The recorded interviews resulted in 112 statements describing the competitions before and after the introduction of the visualization system.

Results

Phase One: Five of the six teams interviewed had participated in previous CDCs, but none of the teams had previously used a visualization system to support their activities in these competitions. Several themes emerged that suggested how the visualization was being used and the problems and benefits that the users experienced with the system.

Utilization was high for several of the modules and the visualization system as a whole. The most highly cited module used was the scoreboard module. Teams also extensively utilized the service state module to verify which services were currently available to users on their network subnet. Statements by participants also indicated that the visualization system helped them improve their response time, discover service vulnerabilities, and allowed them to focus on important security tasks.

Problems were also found with some aspects of the visualization system. Many participants were confused by the scoring metrics and whether positive or negative numbers were indicators of good performance. Several individuals reported problems understanding the island module while many participants requested a user guide explaining each of the visualization modules in the system.

While users experienced some problems, more positive attitudes toward the visualization system were found as compared to negative attitudes. Specifically, 70 percent of the statements pertaining to the visualization system were positive. Four of the six teams wanted to know if the system was available for personal use at their schools. Also, the participants indicated that the visualization system helped them to focus on the problem at hand and notified them about whether possible nefarious activity was occurring on their subnet.

Phase Two: Line-by-line coding of the interviews with professionals revealed themes about the drawbacks and benefits of using the CDCVis system. One drawback was that the usage of the system added more setup time for the administrators. However, the interviewees agreed that setup time involved could be improved by more familiarity with and streamlining of the process. The interviewees agreed that the benefits to students out-weighed any burden to the administrators.

A content analysis of the interviews indicated that of the 112 statements, 10 statements addressed the drawbacks of using the system while 102 statements addressed the benefits. Three overarching benefits emerged from using the CDCVis system; specifically administrators had seen increases in 1) student engagement, 2) team performance, and 3) opportunities for learning. Specifically noted was that using the visualization system facilitated understanding and engagement: "I think the biggest thing is that it [CDCVis] gives the competitors something tangible to see. Otherwise the competition is so abstract. Without it, it's hard to get them excited about what was going on."

Qualitative Discussion

The study was intended as a first pass at understanding user attitudes towards the CDCVis system utilizing the proposed design framework. The analysis of the data was general in nature so as to gain a very high-level preliminary analysis. Responses show that the system functioned in a way that was consistent with network security visualization. Both positive and negative attitudes as well as drawbacks and benefits pertaining to the system were identified, including areas for improvement.

Several modifications to both the system and other materials were implemented as a follow up to our discussions with users and administrators. First, the scoring metrics were changed (e.g., the "lower is better" scoring system was replaced by a "higher is better" metric and negative scores were no longer allowed) and the scoreboard module was modified to visually depict these changes. Second, because many participants had difficulty interpreting the Island visualization module, the module was modified to only display port and traffic information rather than source and destination information ("flags" and "branches" had represented source and destination IPs in the original Island visualization module). The modular nature of the system allowed for both the Scoreboard and Island modules to be easily updated without modifying substantial components of code. Finally, a user guide was developed to describe the information being depicted by each of the visualization modules. While not a technical update, the guide helped users to better understand each module and more fully utilize the module for network security visualization activities during the competition.

The second phase of the study was designed to allow us to evaluate a "baseline" condition by which we could contrast the competition prior to and after the implementation of the visualization system. Because the visualization system has become an integral part of the competitions and is used as an important learning tool at all CDCs, it is infeasible and unethical to run competitions without it. As a result, we relied on this qualitative approach to gain insights about the impact that the visualization system has had on administrators and users. While some drawbacks of using the system were identified, the overarching message is that the visualization system has substantially improved the competition environment.

Quantitative Evaluation

The final evaluative mechanism consisted of a quantitative field study. The purpose of this study was to gain a more nuanced measure of user attitudes towards the CDCVis system. Field studies offer high external validity by studying participants in a real-life setting (Heppner et al., 2008). Given the nature of the competitions that utilized the CDCVis system, a field study offered an appropriate study environment for the system. Also, given that CDCVis was designed to help with network security administration, the CDCs offered a prime test setting.

The participants for the study were individuals who participated in three different CDCs at three separate times spanning a period of one year. While field studies offer high external validity, internal validity can be problematic as it is difficult to enforce experimental control. Given these limitations, care was taken to ensure that each of the three CDCs were as similar as possible (e.g., competitions were hosted at the same venue, task and competition parameters were identical, and timeframes and operational parameters were comparable). To increase generalizability, participants were drawn from a variety of educational settings (e.g., high school, community college, and university students). All three cohorts used the same or similar scenarios and the CDCVis system was configured comparably for each competition.

To further test for similarity across the three competitions, separate ANOVAs were run for each of the study variables in question. No significant difference was found between participants in the three competitions on performance expectancy ($F = 1.347$, $p = 0.266$), effort expectancy ($F = 0.383$, $p = 0.683$), social influence ($F = 2.265$, $p = 0.110$), or behavioral intent ($F = 2.193$, $p = 0.118$). Also, self-efficacy regarding use of the system was shown to be not significantly different between groups ($F = 1.664$, $p = 0.196$). As a result, while we drew our sample from a diverse set of sources, these groups were comparable on the measures evaluated in the study.

Data Collection

The data were collected at approximately the mid-point of each competition to allow the participants to become accustomed to both the competition and the CDCVis system. One of the system developers administered the surveys. Measures consisted of items adapted from the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al., 2003) and were selected because these items could be used to gauge user acceptance of the technology. Specifically, Performance Expectancy (PE), Effort Expectancy (EE), and Social Influence (SI) were measured as well as their effect on Behavioral Intent (BI) to use the system in the future. Our a priori expectations were that performance expectancy, effort expectancy, and social influence would have a significant positive impact on intended future use of CDCVis.

As a second component of this study, we explore differences in preexisting subject expertise in network security, operationalized as differences between high school and college-aged students. Prior research has suggested that existing expertise in a domain may significantly influence attitudes about technology acceptance (Bhattacherjee, 2000, Bhattacherjee and Sanford, 2006, Mathieson et al., 2001). Based on this research, we hypothesized that prior expertise would have a significant effect on the relationship between PE, EE, and SI on BI. Findings from this portion of the research will be useful in quantifying the differences between experienced users and novice or less mature users. Such a contrast increases the generalizability of our research to domains where greater expertise is more common (e.g., a corporate or professional security setting).

Given this, we hypothesize:

- H1: A user's performance expectancy with regard to CDCVis will significantly affect behavioral intent to use CDCVis in the future.
- H1a: The greater the expertise of the individual with network security, the more significantly performance expectancy will influence behavioral intent to use CDCVis in the future.
- H2: A user's effort expectancy with regard to CDCVis will significantly affect behavioral intent to use CDCVis in the future.
- H2a: The greater the expertise of the individual with network security, the more significantly effort expectancy will influence behavioral intent to use CDCVis in the future.
- H3: The level of social influence a user feels toward using CDCVis will significantly affect behavioral intent to use CDCVis in the future.
- H3a: The greater the expertise of the individual with network security, the more significantly social influence will influence behavioral intent to use CDCVis in the future.

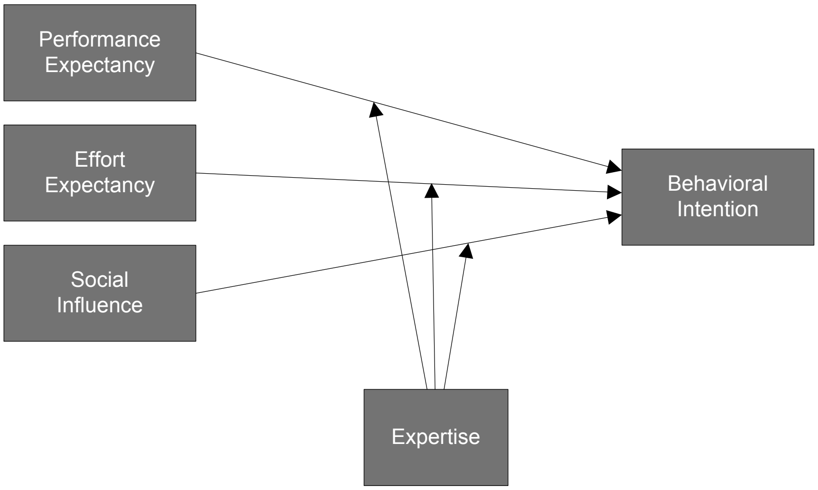


Figure 11: Research Model for Quantitative Evaluation Derived from UTAUT

Results

In total, 87 students filled out the questionnaires handed out during the competitions. The study examined one dependent variable and four independent variables. The dependent measure, BI, consists of three items and has a high reliability (Cronbach's α = 0.958, CI = [0.939, 0.971]). Three of the independent measures – PE, EE, and SI – also had relatively high reliability with Cronbach's α equal to 0.889 (CI = [0.845, 0.923]), 0.911 (CI = [0.875, 0.938]), and 0.831 (CI = [0.758, 0.885]) respectively. This indicates that the participants responded consistently to the items in the measures. The other independent variable indicated whether or not the participant was in college (proxy for expertise).

Table 3 presents each of the tested variables with their respective mean, standard deviations, and Cronbach's alpha values (including confidence intervals). One finding worth mentioning is the nature of the values of the mean scores reported by the participants. As can be seen, all mean values were found to be in the ~2.7 to ~3.0 range. These measures used a six item scale from strongly agree (1) to strongly disagree (6); therefore, a smaller than average score indicates desirable outcomes with regard to this study (see Appendix B for a copy of the questionnaire used). A one-sample t-test was used to evaluate whether the mean values were significantly better (i.e. lower) than a neutral score of 3.5 on this 1 to 6 scale. Participants, on average, agreed that CDCVis would increase their performance for network security administration (t = -5.4, p < 0.001, CI = [-0.46, -0.99]), would be easy to learn to use (t = -5.8, p < 0.001, CI = [-0.49, -1.01]), and would be something they would receive encouragement from others to use (t = -3.4, p = 0.001, CI = [-0.20, -0.78]). Furthermore, on average, participants agree that they would be likely to use CDCVis in the future (t = -5.0, p < 0.001, CI = [-0.49, -1.13]).

Table 3: Mean, Standard Deviation, and T-test Values for Study Variables

	PE (Performance Expectancy)	**EE** (Effort Expectancy)	**SI** (Social Influence)	**BI** (Behavioral Intention)
Utilizing CDCVis n=87	2.78 (1.25) (*t*= -5.4, *p*< 0.001, CI=[-0.46, -0.99])	2.75 (1.22) (*t*= -5.8, *p*< 0.001, CI=[-0.49, -1.01])	3.01 (1.35) (*t*= -3.4, *p*= 0.001, CI=[-0.20, -0.78])	2.69 (1.51) (*t*= -5.0, *p*< 0.001, CI=[-0.49, -1.13])

(minimum preferred)	4-items
	Min = 1, Max = 6
	α = 0.889
	(CI=[0.845, 0.923])
		4-items
		Min = 1, Max = 6
		α = 0.911
		(CI=[0.875, 0.938])
			3-items
			Min = 1, Max = 6
			α = 0.831
			(CI=[0.758, 0.885])
				3-items
				Min = 1, Max = 6
				α = 0.958
				(CI=[0.939, 0.971])

We used OLS (ordinary least squares) regression analysis (see Table 4) to examine the relationship between these independent variables and intention to use the system; therefore, multiple regression is an appropriate statistical technique. The results for model 1 (M1) indicate that the model was highly significant (F(4,82) = 41.74, p < 0.001) and also explained a substantial amount of variance in the dependent variable (R2 = 0.671). Of the three independent variables used in M1, only PE and SI were significant (t = 3.546, p = 0.001 and t = 6.572, p < 0.001 respectively) while EE was not significant (t = 1.224, p = 0.225) (see Table 5 for a complete list). This offers support for H1 and H3, but does not support H2. Prior expertise (indicated by whether the student was in college) was also examined to check for a significant difference between the high school and college-aged groups. The results showed no significant difference between the two groups (t = 0.598, p = 0.551). These results indicate that there was no significant difference in BI based on expertise.

Table 2: Regression Model Tested, Including *F*, *p*, and *R*^{2} Values

Model	Equation	F-value	p-value	R^2-value
M1	$BI = \beta_0 + \beta_1 PE + \beta_2 EE + \beta_3 SI + \beta_4 College$	*F(4,82)* = 41.74	0.000	0.671

Table 3: ANOVA Table for Model

	M1		
	b	**t-ratio**	**p**
PE	0.368 (0.104)	3.546	0.001
EE	0.134 (0.109)	1.224	0.225
SI	0.594 (0.090)	6.572	0.000
College	0.119 (0.199)	0.598	0.551
Intercept	-0.575 (0.295)	-1.947	0.055
SSR (w/df)	131.564(4)		
MSE (w/df)	0.788(82)		
R-squared	0.671		

To gain a better understanding of the difference between the two experience groups for the internal workings of the model, blocking was used to test the model for each group separately. By blocking, we looked at how prior expertise manifested itself for each of the groups. Table 6 provides the statistical results for each group. PE was found to be a significant predictor of BI for participants with greater expertise (the college group), with PE becoming nonsignificant with less expertise (the high school group). This suggests that experience was an important factor influencing behavioral intent, supporting H1a. EE was also found to be a significant predictor of BI for participants with more prior expertise, supporting H2a. The significance of SI predicting BI did not change between groups, which fails to support H3a. Nevertheless, SI was found to be a highly significant predictor of BI in both groups.

Table 6: Blocked Results for College and High-School Groups

	Regression Parameters							
	College (n = 54)				**High School (n = 33)**			
Outcome	*β*	*SE*	*t*	*p*	*β*	*SE*	*t*	*p*
Performance Expectancy	0.389	0.125	3.103	0.003	0.398	0.199	1.997	0.055
Effort Expectancy	0.267	0.133	2.008	0.050	0.012	0.201	0.059	0.953
Social Influence	0.511	0.105	4.853	0.000	0.657	0.177	3.703	0.001

Quantitative Discussion

The quantitative analysis was used to provide a more nuanced understanding of user attitudes towards CDCVis. Specifically, the analysis involved three CDCs to analyze the acceptance of CDCVis and the intended use of the system by participants in the future. We hypothesized that PE, EE, and SI would have a significant impact on intention to use CDCVis in the future. Both PE and SI showed a significant impact on BI while EE did not. Also, we hypothesized that greater prior network security expertise (operationalized as high school vs. college) would have a significant impact on the relationship between PE, EE, and SI on BI. The results show this to be true for PE and EE, but not for SI.

This evaluation provides several important contributions. First, through the use of means analysis, we demonstrated that participants agree that CDCVis would improve their job performance, that the effort needed to learn to operate the visualization would be low, that those who influence their work were believed to be likely to encourage using the CDCVis, and that the users would be likely to use CDCVis again in the future. Second, we showed that these participant beliefs about performance expectancy and social influence significantly increase overall behavioral intent to use CDCVis in the future. Finally, evidence suggests that greater prior expertise has a significant impact on the relationship between performance expectancy, effort expectancy, and behavioral intent. Future research should analyze how to better convey the performance benefits of using CDCVis to those with less experience, which will hopefully increase their future use of the system. Also, greater prior expertise is shown to create less effort expectancy, which significantly affects behavioral intention to use the product. This provides an area of potential future research given that those with less experience need to be shown that the system does not take much effort to learn, which would hopefully significantly affect their intention to use the system. Overall, each model offers an informative picture for corporate network administrators who would most likely have greater expertise in network security, which is the potential target market for this type of product.

DISCUSSION

This special issue was motivated, in part, by the desire to foster and publish innovative research examining the IT artifact in the context of human use. Our research offers several theoretically relevant contributions to the design science literature as well as practical and theoretically important contributions for security researchers and practitioners.

In our network-centric society it is increasingly important to consider how users and administrators can defend information systems from intruders and identify and evaluate sources of threats. Visualization tools have been used extensively by researchers and practitioners to identify patterns, evaluate alternatives, and facilitate decision making about a variety of complex and apparently chaotic phenomena; yet, visualization aids have not been applied to address security and intrusion detection problems as often as one would expect. This research (our framework and the testing of a system built upon these principles) has relevance in this broad domain because it marries the need for visualization aids with the solid design principles and evaluations that facilitate robust system design. In this context, this research represents an important contribution as a demonstration not only of the suitability of the proposed framework and system but also of the process by which this system was built and tested.

The proposed design framework offers a critical step towards effective development of network security visualization systems. Previous research in security visualization (Luse et al., 2008) and activity theory (Engeström, 1987) suggest that the ability to accommodate all three security visualization frameworks – including the user-based, alert-oriented, and component-based frameworks – is necessary for effective development of security visualization systems. Our proposed framework offers the necessary capability to combine all three frameworks. Through a modular-based visualization approach, separate visualization modules can be built, mixed, and matched to accommodate any or all aspects of the three security visualization frameworks, and remains flexible for future enhancements.

Of course, an important part of this examination is the evaluation of the system built using design science guidelines. In this context, we demonstrated that users reacted positively to the affordances offered in the visualization system and that their intentions were to not only seek to use a system with these features but to also identify how they could continue to use the system in their future educational and career-related activities. This positive feedback is instrumental in demonstrating the value of this system but it also demonstrates why it is important to evaluate a system using multiple modes of inquiry. Our evaluative techniques involved a three-prong approach including a requirements review of the prototype system and both a qualitative and quantitative assessments of system use. We used not only a survey technique but also included qualitative, open-ended questions about the user experiences and intentions for future use. While open-ended questions are often touted in systems analysis textbooks as important tools for systems analysis and design activities, research examining systems use and adoption intentions often focus primarily on quantitative approaches for evaluation. Our methodology for collecting results and feeding these findings back into the system also conforms to the iterative design approaches suggested by the design science literature.

These results are also important not only because of the practical, theoretical, and methodological relevance, but also because of the contribution this research offers in terms of rigor in the context of relevance. Hevner and colleagues (2004) pointed out the following: “Success is predicated on the researchers skilled selection of appropriate techniques to develop or construct a theory or artifact and the selection of appropriate means to justify the theory or evaluate the artifact” (p. 88). We have applied several relevant theories such as Schneiderman’s guidelines for visualization aids and activity theory and we examined these during the development and evaluation of the artifact investigated in this research. The theoretical contribution of this research is evident and suggests that practitioners, developers, and researchers should whole-heartedly embrace these and similar visualization aids in their products and security services.

CONCLUDING REMARKS

Our research offers several important insights about the attitudes that prospective users of visualization aids develop after their use of these systems in a cyber-defense competition. While our results were collected in the context of a robust empirical study, the study does have limitations that should be considered in evaluating these results. Chief among these limitations is the context of the study itself; a hectic cyber-defense competition where our participants were engaged in a variety of exercises and activities related to engagement in a simulation of a cyber attack. Of note is the fact that the participants were students; thus, they represent a particular sample of a broader population of security experts. Students have been recruited extensively as participants in research, and while their responses to psychological and other experimental stimuli generally offer reliable and valid results, care must be taken in generalizing findings to other contexts or populations (Hughes and Gibson, 1991). For example, professionals with significant work expertise might respond differently to exposure to these tools. Nevertheless, these participants were not students drawn from a random sampling of the general student population; rather, they are students who are pursuing or are considering careers in the security field. As such, they possess not only educational training in the topic, but they also have an intense interest in the topic, and are motivated to learn and apply their skills to the security challenges they faced. Thus, we could consider these participants to be knowledgeable and motivated respondents. In this regard, their responses to our queries were not from an entirely uninformed sample and the results should therefore be comparable to those offered by other “informed” security and IT experts.

A second consideration is the exercise as the context for our testing. While cyber defense competitions are intense and challenging, they are not cyber attacks on “real” organizational or personal systems. The students were engaged in the competition and, as with most competitions, the motivation to “win” was high in most or all participants. Nevertheless, unlike settings in organizations or other professional contexts, the participants would not be severely penalized for failure or for inattentiveness. It is possible, in this light, that results might be influenced by this context because, for example, participants might have not fully evaluated their use of these aids. In spite of this, however, we consider this concern to be of minimal importance because, as noted, the participants generally are highly engaged in these events and the attacks offered by the professionals and others are realistic and intense. The common theme we saw in our results was that participants had responses to these visualization aids that suggested that their positive affect was a reaction generated from consideration not only of the practical benefits of these features but also a positive visceral reaction to their interactions with these aids.

A third limitation involves the contribution of the evaluative mechanisms used in this study. We claim, and do believe, that a complete security visualization system should include all of the components of the three frameworks used previously (i.e. the user-based framework, the alert-oriented framework, and the component-based framework). Given the nature of the testing environment, it was not feasible to perform a baseline test with no visualization system used as this would have subtracted from the learning experience of the students involved. We have attempted to gauge how the competition would be different without the visualization system through expert assessment, but these assessments are subjective and subject to potential recollection biases.

Future research should examine these limitations and seek to generalize these results to other contexts. For example, it would be useful to conduct a similar evaluation by security professionals with significant professional experience. Similarly, an evaluation of the use of these tools in real organizations during “real” attacks would bolster our confidence in these results. Both of these situations would involve implementing the system on a corporate network and allowing network administrators to use the system. The number of events detected by using the system and the response times could then be compared to statistics for previous attacks on the same network.

A second related area for future research is more numerous evaluations of the proposed combined framework in both lab and field settings. We have provided an initial analysis of a system which incorporates all three visualization sub-frameworks here, but more research is needed to verify the use of each of the sub-frameworks and their constituent parts. For example, what is the advantage of incorporating modules that provide for the user-based framework above and beyond the other two frameworks? Also, what is the advantage of incorporating all 8 pieces of the component-based framework as opposed to say six or seven? There are many different layers of complexity and thoroughness which can be evaluated in future research.

Another area of potential future research is the use of the various visualization modules. Specifically, research should be done to identify good mixes of modules that can be effectively utilized in particular contexts. The proposed design framework provides the necessary contextual elements to allow for various modules to both be created and implemented in a variety of ways. Future research should extend this modularity by identifying best practices for the use of different types of modules and combinations of modules.

Finally, while a thorough discussion of activity theory lies beyond the scope of this paper, we suggest that additional research should examine the role of activity theory, a theoretical perspective that has been found to be useful in system design and evaluation, as a basis for the design and evaluation of a variety of IS systems, as well as its potential usefulness in design science. For example, a marriage between concepts and techniques used by activity theorists and researchers with researchers applying design science would, we believe, be fruitful. As noted by Hevner and colleagues (2004), the utility of an artifact and evidence demonstrating that utility are critical design science questions. Activity theory offers a theoretical model that can be used to identify and frame artifact utilities within an activity-based contextual system. In the context of activity-centered design, Norman (2005) suggests that well designed devices work well because they were “…developed with a deep understanding of the activities that were to be performed” (p. 14). In considering user and activity centered design and the science of evaluating these designs, it seems logical that activity theory would be useful as a framework for informing the design science community by providing a framework for evaluating artifacts in the context of use.

While future work is needed, these results are useful as a first step toward examining not only these visualization aids in supporting cyber security, but also as a demonstration of the use of design science principles in activities related to system design and evaluation. We hope that this paper inspires additional research in this domain that can be used to both advance theory and also apply these concepts in practice.

REFERENCES

Aalst, W. M. P. v. d. and A. Kumar (2003) "XML-Based Schema Definition for Support of Interorganizational Workflow," *Information Systems Research* (14) 1, pp. 23-46.

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

Ball, R., G. A. Fink, and C. North. (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, October 25-29, 2004.

Bauer, L., A. W. Appel, and E. W. Felten (2003) "Mechanisms for Secure Modular Programming in Java," *Software Practice & Experience* (33) 5, pp. 461-480.

Bedny, G. Z. and W. Karwowski (2003) "A Systemic-Structural Activity Approach to the Design of Human-Computer Interaction Tasks," *International Journal of Human-Computer Interaction* (16) 2, pp. 235-260.

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

Bhattacherjee, A. (2000) "Acceptance of E-Commerce Services: the Case of Electronic Brokerages," *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on* (30) 4, pp. 411-420.

Bhattacherjee, A. and C. Sanford (2006) "Influence Processes for Information Technology Acceptance: An Elaboration Likelihood Model," *MIS Quarterly* (30) 4, pp. 805-825.

Breitmeyer, B. G. (1992) “Parallel Processing in Human Vision: History, Review, and Critique,” in J. R. Brannan (Ed.) *Applications of Parallel Processing in Vision*, Amsterdam: North-Holland.

Conklin, A. (2006) “Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course,” in *Proceedings of the 39th Annual Hawaii International Conference on System Sciences* (9), pp. 220b-220b. Kauai, HA, January 4-7, 2006.

Dhillon, G. and G. Torkzadeh (2006) "Value-focused Assessment of Information System Security in Organizations," *Information Systems Journal* (16), pp. 293-314.

Engeström, Y. (1987) *Learning by Expanding: An Activity-Theoretical Approach to Developmental Research*. Helsinki: Orienta-Konsultit Oy.

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

Foresti, S., J. Agutter, Y. Livnat, S. Moon, and R. Erbacher (2006) "Visual Correlation of Network Alerts," *IEEE Computer Graphics and Applications* (26) 2, pp. 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, United States Military Academy, West Point, NY, 2005*, pp. 394-401.

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

Goodall, J. R., A. A. Ozok, W. G. Lutters, P. Rheingans, and A. Komlodi (2005) “A User-Centered Approach to Visualizing Network Traffic for Intrusion Detection.” in *Proceedings of Conference on Human Factors in Computing Systems,* pp. 1403 - 1406. Portland, OR, April 2-7, 2005.

Griswold, W. G., M. Shonle, K. Sullivan, Y. Song, and H. Rajan (2006) "Modular Software Design with Crosscutting Interfaces," *IEEE Software* (23) 1, pp. 51-60.

Heppner, P. P., B. E. Wampold, and D. M. Kivlighan (2008) *Research Design in Counseling*, 3rd edition. Belmont, CA: Thomson.

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

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

Hughes, C. T. and M. L. Gibson (1991) "Students as Surrogates for Managers in a Decision-making Environment: An Experimental Study," *Journal of Management Information Systems* (8) 2, pp. 153-166.

Jacobson, D. and N. Evans (2006) “Cyber Defense Competition,” Paper presented at *2006 ASEE Annual Conference & Exposition: Excellence in Education*. Chicago, IL, June 18-21, 2006.

Johnson, R. E. and B. Foote (1988) "Designing Reusable Classes," *Journal of Object-Oriented Programming* (1) 2, pp. 22-35.

Kaptelinin, V. and B. Nardi (2006) *Acting with Technology: Activity Theory and Interaction Design*. Cambridge, MA: MIT Press.

Komlodi, A., J. R. Goodall, and W. G. Lutters. (2004) “An Information Visualization Framework for Intrusion Detection.” in *Proceedings of Conference on Human Factors in Computing Systems,* pp. 1743-1746. Vienna, Austria, April 24-30, 2004.

Komlodi, A., P. Rheingans, U. Ayachit, J. R. Goodall, and A. Joshi (2005) “A User-Centered Look at Glyph-Based Security Visualization.” In *Proceedings of IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05)*, pp. 21 - 28. Minneapolis, MN, October 26, 2005.

Kozaczynski, W. and G. Booch (1998) "Guest Editors' Introduction: Component-Based Software Engineering," *IEEE Software* (15) 5, pp. 34-36.

Kuhn, T. S. (1996) “The Structure of Scientific Revolutions,” in 3rd edition, Chicago and London: University of Chicago Press.

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

Lakkaraju, K., R. Bearavolu, and W. Yurcik. (2003) “Nvisionip - A Traffic Visualization Tool for Security Analysis Of Large and Complex Networks.” Paper presented at *International Multiconference on Measurement, Modelling, and Evaluation of Computer-Communications Systems (Performance TOOLS),* September 2-7, 2003.

Lakkaraju, K., W. Yurcik, R. Bearavolu, and A. J. Lee. (2004a) “NVisionIP: An Interactive Network Flow Visualization Tool for Security.” in *Proceedings of 2004 IEEE International Conference on Systems, Man, and Cybernetics,* pp. 2675-2680. The Hague, The Netherlands, October 10-13, 2004.

Lakkaraju, K., W. Yurcik, and A. J. Lee. (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, October 25-29, 2004.

Livnat, Y., J. Agutter, S. Moon, R. F. Erbacher, and S. Foresti (2005) “A Visualization Paradigm for Network Intrusion Detection.” in *Proceedings of the 2005 IEEE Workshop on Information Assurance and Security United States Military Academy,* pp. 30-37. West Point, NY, June 15-17, 2005,

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

Mathieson, K., E. Peacock, and W. W. Chin (2001) "Extending the Technology Acceptance Model: The Influence of Perceived User Resources," *SIGMIS Database* (32) 3, pp. 86-112.

McHugh, J., A. Christie, and J. Allen (2000) "Defending Yourself: The Role of Intrusion Detection Systems," *IEEE Software* (17) 5, pp. 42-51.

Merriam and Webster (2004) *Merriam-Webster's Collegiate Dictionary*, 11th edition: Merriam-Webster, Inc.

Miller, J. A., D. Palaniswami, A. P. Sheth, K. Kochut, and H. Singh (1998) "WebWork: METE0R2's Web-based Workflow Management System," *Journal of Intelligent Information Systems* (10) 2, pp. 185-215.

Nardi, B. A. (1996) *Context and Consciousness: Activity Theory and Human-computer Interaction*. Cambridge, MA: MIT Press.

Norman, D. A. (2005) "Human-centered design considered harmful," *Interactions* (12) 4, pp. 14-19.

O'Leary, D. E. (2010) "Enterprise Ontologies: Review and An Activity Theory Approach," *International Journal of Accounting Information Systems* (11) 4, pp. 336-352.

Oline, A. and D. Reiners (2005) “Exploring Three-Dimensional Visualization for Intrusion Detection,” in *Proceedings of IEEE Workshop on Visualization for Computer Security(VizSEC 05)*, pp. 113 - 120. Minneapolis, MN, October 26, 2005.

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

Parnas, D. L. (1972) "On the Criteria to Be Used in Decomposing Systems into Modules," *Communications of the ACM* (15) 12, pp. 1053-1058.

Richardson, R. (2009) "14th CSI Computer Crime and Security Survey." Retrieved June 27, 2011, from www.pathmaker.biz/whitepapers/CSISurvey2009.pdf

Royce, W. W. (1970) “Managing the Development of Large Software Systems,” in *Proceedings of IEEE WESCON*, pp. 1-9. August, 1970.

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

St. Laurent, S. (1997) *XML: A Primer*. New York: MIS Press.

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

White, G. B. and D. Williams (2005) “The Collegiate Cyber Defense Competition,” in *Proceedings of the 9th Colloquium for Information Systems Security Education (CISSE 05)*, pp. 26-31. Atlanta, GA, June 6-10, 2005.

Yurcik, W., K. Lakkaraju, J. Barlow, and J. Rosendale (2003) “A Prototype Tool for Visual Data Mining of Network Traffic for Intrusion Detection,” Paper presented at *the ICDM Workshop on Data Mining for Computer Security (DMSEC’03)*. Melbourne, FL, November 19, 2003.

[1] The Scoreboard module is unique to the CDC environment and is the only module that would not appear in a typical corporate network security administration environment.

[2] Both the Bar Graph and the NetSquall demonstrate the power of inheritance within the modular framework by demonstrating that inheritance allows the team-based versions to be inherited from the global-based versions.

APPENDIX A

CDCVis Visualization System Interview Questions – Administrators

1. Can you envision how the competition would operate if the visualization system wasn't being used?
2. Would there be any benefits of removing the visualization system?
3. If the visualization system were, as not available would it impact the number of questions the students asked?
4. If the visualization system were not available, would it impact the quality of decisions that the students are making?
5. If the visualization system were not available, would it impact the quantity of decisions that the students are making?
6. If the visualization system were not available, would it impact the speed of the student's ability to contextualize the data?
7. If the visualization system were not available, would it impact the student's ability to make team comparisons?
8. If the visualization system were not available, would it impact team effectiveness?
9. If the visualization system were not available, would it impact team efficiency?
10. If the visualization system were not available, would it impact student fun?
11. If the visualization system were not available, would it impact student learning?
12. When considering the visualization system, does it affect their understanding of attacks, frequency and number?
13. Do you have any other comments?

APPENDIX B

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 school you are representing? ________________________

Circle your gender. M F

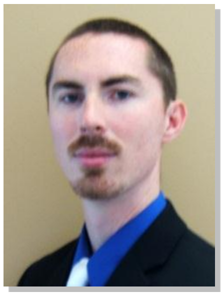
Enter your age. _________

ABOUT THE AUTHORS

Andy Luse is a Ph.D. student in Business and Technology at Iowa State University. Andy has a Ph.D. in Human Computer Interaction and Computer Engineering from Iowa State University and has conducted research in computer and network security and visualization mechanisms for such systems. He is currently involved in research into user technology acceptance and methodological issues surrounding interest in Information Technology as a major.

Brian E. Mennecke is an Associate Professor of Management Information Systems at Iowa State University. His research interests include collaboration and collaborative systems, social media and virtual worlds, embodiment and perceptions of space, security systems and biometrics, mobile and electronic commerce, and spatial technologies. He has previously published a book on mobile commerce and articles in academic and practitioner journals such as Management Information Systems Quarterly, the Decision Sciences Journal, the International Journal of Human-Computer Studies, the Journal of Management Information Systems, Organizational Behavior and Human Decision Processing, the International Journal of Human Computer Studies, the Journal of Information Privacy and Security, and the Journal of Digital Forensics, Security & Law.

Janea Triplett is a Ph.D. student in human-computer interaction at Iowa State University. She has published in peer-reviewed journals, refereed conferences and has a patent pending for an algorithm that discovers online social networks. Her research interests include virtuality, social media, and technology and social change. Janea also holds master’s in international development and an M.B.A. in information systems. She has done IT consulting for local clients as well as NGOs in SE Asia and Africa.



Nate Karstens works as a Software Engineer for Garmin International, Inc., where he has been involved in instrumentation, networking, and localization projects for the marine product segment. Nate graduated Summa Cum Laude from Kansas State University in 2005, where he earned a B.S. in Computer Engineering with a specialization in Embedded Systems. In 2007 he earned a M.S. in Information Assurance from Iowa State University, where he worked as a Research Assistant on the ISEAGE project. Nate currently resides in Olathe, Kansas, and is an active member of the community – he volunteers his time as a soccer coach and as a mentor to high school students studying digital electronics.

Doug Jacobson is a University Professor in the Department of Electrical and Computer Engineering at Iowa State University. He is the director the ISU Information Assurance Center, which has been recognized by the National Security Agency as a charter Center of Academic Excellence for Information Assurance Education. Dr. Jacobson teaches network security and information warfare and has written a textbook on network security. He is director of the IT-Adventures program and oversees the cyber defense competitions hosted at ISU. His research is targeted at developing large scale attack simulation environments and is the director of the Internet-Scale Event and Attack Generation Environment (ISEAGE) test bed project. Dr. Jacobson has received two R&D 100 awards and two patents for his security technology. He has given over 75 presentations in computer security and has testified in front of the U.S. Senate committee of the Judiciary on security issues associated with peer-to-peer networking.

ISSN: 1944-3900

Transactions on Human-ComputerInteraction