Proceedings of the 13th Colloquium for Information Systems Security Education
University of Alaska, Fairbanks
Seattle, WA June 1 - 3, 2009

# A Framework for Modeling Security Measures

Keith Harrison, Gregory White, *The University of Texas at San Antonio*
{kharriso@cs.utsa.edu, greg.white@utsa.edu}

***Abstract – In this paper we introduce a framework that provides a model for describing security measures and their relative effectiveness as well as importance. This model enhances computer security training and educational curriculum by providing experimental data and analysis to educators and students. Business environments will benefit from this model by enabling more cost effective allocation of scarce IT and security resources. Additional benefits include but are not limited to better development of operating systems, applications, and user interfaces.***

**Index terms – Security, education, cyber defense competition, best practices, effectiveness**

## I. Introduction

In this paper we introduce a framework that provides a model of security measures and their effectiveness. The model provides both an overall effectiveness comparison and a priority level that should be considered in time critical situations. Our framework allows existing security best practices to be experimentally validated. Additionally, the model produced by the framework makes important contributions to security research. Educational environments will be able to use our model in order to focus their limited resources on the most effective security measures. Similarly, small businesses will be able to more efficiently allocate scarce resources to provide more cost effective security. Operating system and application designers will have the data needed to justify more secure default configurations, and be able to more effectively focus their efforts on the most critical security features. User interface designers will more accurately be able to determine what security settings are most critical and make these configuration options easier to understand and modify.

## II. Related Work

A survey of small business security tools and practices was performed at George Washington University (GWU) [1]. The purpose of this survey was to provide "insight into what works and what appears unused or ineffective." The survey gathered information on access privilege management, management tool usage, technology tool usage, and security incidents. Relationships were identified between security incidents and access privilege policies, management tool usage, and technology tool usage.

While the overall goals of this work are similar to our goals, our work is significantly different. The work from GWU focuses on identifying broad general relationships such as businesses with higher rates of past data loss are more likely to currently use backup software. The focus of our work is on the relative effectiveness of many more specific defenses against remote threats only.

In the research performed at GWU, conclusions and causal relationships prove difficult to make due to the lack of a controlled environment and a reliance on businesses to report known security incidents. The Author points out that "respondents indicating the use of a technology tool were more likely to also indicate having experienced a given problem." However, the author goes on to describe that the cause for this is difficult to determine and it may just be that those who are more likely to use the tools are more aware of potential problems [1]. Our methodology differs significantly to avoid these issues. We do not rely on surveys or individuals to determine security incidents or the current status of a machine. Our framework utilizes more controlled environments which start out exactly the same before different security measures are applied. Our analysis not only tells us if certain security measures are effective, we are also able to determine which security methods are most effective and which security methods are most important in time critical situations.

The CyberDefense Laboratory [2] was created in order to provide information security education. Students engage in attack-defend scenarios and thereby gain experience and insights into information security. The CyberDefense Laboratory and similar education environments [3, 4, 5] share some similarities with the National Collegiate Cyber Defense Competition (NCCDC), which is the basis for our framework. However, our frame work is specifically designed to work with the NCCDC and similar cyber defense competitions. However, it may be possible to modify our framework to gather useful data from educational and laboratory environments as well.

## III. Motivation

Industry best practices and checklists are commonly used by administrators as a first step towards enhancing security. These best practices are usually chosen with good justifications, however few are experimentally verified. Furthermore, there exists no experimental comparison on the effectiveness and the relative priority that should be given to a set of security measures. We believe educators, small businesses, and researchers will all benefit from such a comparison.

Educators have limited time to provide instruction throughout their course. Educators would benefit from having a model, based on experimental data, which is able to describe the relative effectiveness and importance of recommended security measures. Educators could focus their efforts with greater confidence. Students would benefit from analyzing such a model as well.

Similarly, small businesses have limited resources such as time, money, and manpower. A model comparing the effectiveness of security measures would be critical in helping small businesses determine the most cost effective ways to improve security. Additionally IT personnel would have experimental data to use as evidence of the benefits of increased spending on security.

An accurate, experimental comparison of security measures would leave the door open to further research. For example, it would be very useful to know why certain practices are more important than others. Learning why certain security measures in a given application are more effective than others would be the first step in improving less effective security measures.

What is needed is an environment that is controlled enough to gather specific data on the effects of differing approaches to security. These differing approaches to security should be thoroughly and equally tested in order to gain insights into which security measures were most effective. In order to provide insights into time sensitive situations an environment that simulates a "first day on the job" situation is needed. The National Collegiate Cyber Defense Competition [6] can provide this environment.

## IV. Framework Design

The National Collegiate Cyber Defense Competition (NCCDC) serves as the base for the framework. During the competition data is gathered on the system configurations and security measures implemented by each team. Our framework allows us to correlate these security measures with scoring data that is an accurate measure of the overall effectiveness of security measures implemented by each team.

### *A. Testing Environment*

The NCCDC is an event in which several teams work simultaneously to defend their network from a special team of attackers known as the "red team." The red team consists of industry experts in cyber security and penetration testing. The red team is not competing in the competition, it is their job to attack the other teams, try to disrupt critical business services, and steal critical information. Procedures are in place to ensure that the red team targets each team in a fair and equal manner with exactly the same scans and attacks. Red team members are allowed to perform denial of service attacks only if it is necessary as a stepping stone for another type of attack.

The teams that compete in the NCCDC are purely defensive in nature. Any and all security measures employed by the competing teams are for their defense only. Network traffic is monitored and the competing teams are warned against attempting to interfere with other teams' networks or scoring operations that are running against other teams' networks. The "white team" acts as observers, referees, and also a simulated management.

At the start of the competition each team is given an identical network of computers that simulates a working small business environment. The teams all have identical hardware, software, and software configurations except for only the most necessary changes such as IP addresses. Each team gets several computers that run different operating systems and software that may or may not be important to the operation of the simulated small business that they are working for.

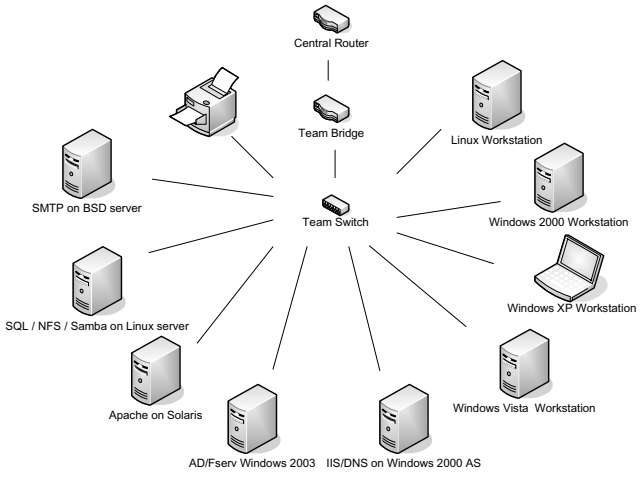


**Figure 1: An example diagram of a single team's network [7]**

The equipment each team gets is usually already connected through both a working but not configured

firewall and a router. Each teams' router, including the red team, leads to a central router that also allows each team to access the Internet in order to perform searches and download tools and patches for example. The teams are kept relatively isolated from real life internet worms and attackers though a carefully configured and monitored router, firewall, and intrusion detection system.

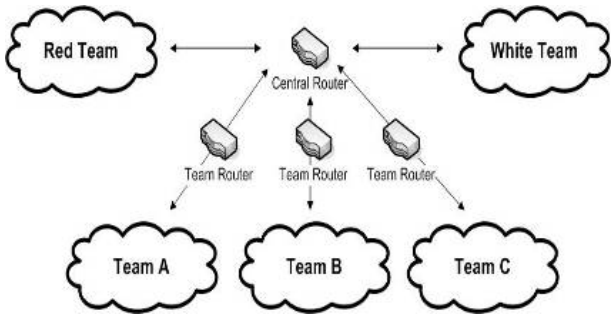


**Figure 2: An illustration of the overall layout [7]**

The teams experience a "first day on the job" situation when they are introduced to an already working business environment that may have been neglected by previous administrators. In addition, previous employees may have intentionally placed malicious software on the machines. Viruses, worms, or other malware may have previously infected any or all of the systems. As soon as the competition begins the teams should expect to be under immediate attack from the red team.

The competition lasts three days. The competition is temporarily suspended during the night in order for other activities to take place, and for the team members to get some sleep. During this three day long competition, the teams compete to keep their business critical services running while at the same time protecting vital intellectual property and customer data. The winner is chosen based on a final score that is calculated from three main sources:

1. Service status scores

Service status scores are calculated by a scoring engine that determines if the business critical services are up and running correctly. These business critical services may for example include web, email, dns, ftp, and ssh services. If the team's services are down for an extended period of time they may violate service level agreements which incur an additional penalty. The NCCDC scoring engine is responsible for evaluating the status of services on the teams' computers. The IP address of the scoring engine changes randomly with each check. Choosing random IP addresses reduces the ability of the teams to cheat by separating the address of the scoring engine from the addresses used by the red team. Delays between checks are distributed uniformly across a range that is easily configurable. This random delay also reduces the ability of the teams to cheat by knowing when checks are going to occur. The scoring engine checks each team and each service simultaneously in order to be as fair as possible.

2. Business injects

Business injects are IT related tasks given to each team by a simulated management. These tasks are important not only because they have security related aspects, they also serve to simulate a real life working environment where employees are pressed for time and resources. Teams that have been able to use their time more efficiently securing their systems will have an increased chance of receiving a higher score on business injects.

3. Red team incidents

Red team incidents are deductions that occur when the red team is able to compromise systems and retrieve vital data, such as intellectual property or customer information. Red team members submit incident reports that include details on exactly what was done and the severity of the compromise. The more severe the compromise, the higher the deduction that is applied against that team. If teams are effectively using tools such as intrusion detection systems they may notice the intrusion and can reduce the deduction applied against them by submitting an incident report of their own to a white team member.

### *B. Environment Limitations*

Due to the nature of cyber defense competitions we are not able to test security measures which defend against social engineering attacks. Prolonged denial of service attacks are for the most part not allowed as part of the competition, therefore the opportunity to test defenses against them is not significant. Additionally physical security measures such as physical locks or automatic session locking when away cannot be tested. We do not see this as a hindrance, but as an opportunity to focus on remotely executed network based threats.

### *C. Relevant Data*

Literature sources[8,9,10] were surveyed to provide a list of relevant security measures that we wish to investigate. Using these sources we have identified 6 main categories of data that are relevant to determining what security measures were implemented by each team:

1. User and administrator passwords

Ideally, we would like to have knowledge of all user and administrator passwords, and to know exactly when each password is changed.

2. Network firewall configuration

Specifically, we want to know exactly what types of incoming and outgoing connections are allowed in order to determine the effectiveness of specific firewall configurations.

3. Installed services and applications

We need to have a complete picture of exactly what software is currently installed and the version of that software. The presence of installed applications such as virus scanners, port scanners, host based firewalls should add to the overall security of a system. Removing unneeded applications and services from the system should increase the security of a system as well.

4. Running services and applications

It is important to know what applications such as virus scanners and intrusion detection systems are currently running. In the ideal case it would be useful to know exactly what processes are running at any given point in time.

5. Operating system, service, and application configurations

A multitude of important security settings exist for applications such as host based firewalls, services such as apache, and operating system components such as file sharing. Ideally we would like to gather all possible configuration settings for important applications, services, and operating system components.

6. Operating system and service patches

Downloading and installing the latest operating system, and network service patches is very important to the security of a system. It is important to have an accurate record of exactly which patches and software updates were installed and when.

*D. Data Collection*

Multiple complementing methods for gathering relevant data are utilized:

1. Business injects

Twice a day, team members are instructed to run an application that is provided to them as part of a business inject. Every Team will run this program on each of their computers. This application will gather as much information as possible such as installed programs, currently running processes, configuration files, system logs, application logs, installation logs, important file modification times, update histories, and password hashes. A file will be created containing all of this information for each computer of every team. The teams will be able to submit these files manually via removable media or by uploading the files to an FTP site.

2. Password submissions

The teams are currently required to turn in any user password changes to the white team in order to be utilized by the scoring engine. The scoring engine must be aware of user passwords in order to accurately check services that require a password in order to check for proper functionality. Examples of these types of services include ssh, pop3, and ftp. Password changes for accounts not associated one of these services, such as administrator accounts, are not required to be submitted.

3. Active scanning

Computers with specialized software are placed outside and inside of the team networks. These computers can coordinate to determine network based firewall settings. Additionally, these research computers actively perform port scanning operations on the target computers. Banners of running services are captured and saved. More specific enumeration operations for each running service will be performed. Actively scanning machines in this manner reveals important security measures that have been applied to the current configuration of the operating system, services, and firewalls. Additionally, with frequent scans it is possible to determine at approximately what time each security measure was applied.

4. Passive monitoring

The teams are not allowed to bring any physical media into the competition. All network traffic will be recorded and saved, thus it is possible to determine exactly what tools and patches the teams are downloading and intend on running.

5. Surveys

At the beginning of days 2 and 3, team members are given a brief survey based on activities that were observed on the previous day. The teams are asked to rank order their actions from the first to last by time, and rank order their actions by importance to the team. At the end of the competition teams are surveyed again on which security measures were used by the teams and their priority to the teams.

*E. Modeling*

Several methods are in place for deriving useful information and models from the collected data:

1. Effectiveness Modeling

The coefficient of correlation between overall team scores and the implementation of a predefined security measure is calculated. If the implementation of a given security measure is highly correlated with the overall team score then that security measure is very effective. A security measure that is ineffective will not be significantly correlated with the teams overall score. This provides a model that describes the effectiveness of implementing each security measure.

Additionally, or in the case that some security measures were applied by every team, normalized scores before and after implementing a security measure are compared to describe how important each security measure was for each team. By doing this we will be able to say, for example, that every team on average scored *x* more points per minute after implementing security measure *y*. A higher value of *x* implies a higher effectiveness of *y*.

2. Priority Modeling

Scores for teams that gave priority to implementing a certain security measure are compared against scores for teams that did not give priority to the given security measure but implemented it later in the competition. In this case the coefficient of correlation can be calculated between the overall score of the team and the time that a given security measure was implemented. If teams that implemented a given security measure early in the competition had a significantly higher score, then this implies that this security measure is very time sensitive and should be given priority. A higher correlation implies that a higher priority should be given to that security measure. This provides a model useful for describing the importance of giving priority to each security measure in time critical situations.

## V. Analysis

Our framework provides the ability to produce models of security measures ranked by both overall effectiveness and priority in time critical situations. As of the writing of this paper the National Collegiate Cyber Defense Competition has not yet taken place. However by the time this paper is published we will have ample time to perform an in depth analysis of all relevant security measures. The NCCDC is scheduled this year for April 17 – 19. Our analysis will provide experimental validation of current security best practices. The most important contribution of our analysis will pinpoint both the most effective security measures and the security measures that need to be given the highest priority in time critical situations. In addition, a descriptive statistical analysis will be performed.

## VI. Conclusion

In this paper we outlined a framework that enables us to model security measures which are utilized for defending against remote attacks in a simulated small business environment. Our model describes both the overall effectiveness of security measures and which security measures need to be given priority in critical time sensitive situations.

This model can be used to improve security education and experimentally validate currently taught best practices. Small businesses will have a useful model that tells them how to more cost effectively allocate IT resources. Operating system and application designers can use this information in order to create more secure software and more secure default configurations. User interface designers will know where to focus their efforts making key security settings more easily accessible and easy to understand.

## VII. Future Work

Currently we are preparing to gather data and perform a detailed analysis at the 2009 NCCDC. During the 2010 NCCDC we plan on verifying and updating the results gathered by the 2009 NCCDC. We also plan on following up the results of the 2009 NCCDC with studies to determine why certain security measures were more effective. Depending on the exact results there may be many more opportunities for research as new questions are raised.

It may be possible to modify this framework for use in other environments. For example a similar framework designed for a more controlled environment such as a laboratory could provide data for evaluating the effectiveness of proposed user interface changes. A similar laboratory environment could be used to study the security implications of initial system configurations vs. ongoing user behaviors.

## VIII. REFERENCES

[1] J. Ryan. "Information security tools and practices: what works?" Computers, IEEE Transactions on, 53(8):1060-1063, Aug. 2004.

[2] M. Aboutabl. "The cyberdefense laboratory: A framework for information security education." Information Assurance Workshop, 2006 IEEE, pages 55-60, June 2006.

[3] J. Hu and C. Meinel. "Tele-lab it security: a means to build security laboratories on the web. Advanced Information Networking and Applications." 2004. AINA 2004. 18th International Conference on , pages 285-288 Vol.2, March 2004.

[4] K. Krishna, W. Sun, P. Rana, T. Li, and R. Sekar. "V-netlab: a costeffective platform to support course projects in computer security." 9th Colloquium for Information Security Education , pages 44-50, June 2005.

[5] V. Padman and N. Memon. "Design of a virtual laboratory for information assurance education and research." 9th Colloquium for Information Security Education , pages 51-58, June 2005.

[6] Official Collegiate Defense Competition™ Website, UTSA Center for Infrastructure Assurance and Security, http://www.nationalccdc.org/

[7] 2007 National Collegiate Cyber Defense Competition, UTSA Center for Infrastructure Assurance and Security, http://www.nationalccdc.org/packets/teampacket.doc

[8] H. Setty, "System Administrator - Security Best Practices." SANS Institute, 2001

[9] S. McClure, J. Scambray, and J. Kurtz, "Hacking Exposed 6: Network Security Secrets & Solutions." McGraw-Hill, 2009

[10] Defense Information Systems Agency "Best Practices Security Checklist V2R1." January 29, 2007