2006

ISECUBE: a portable ISEAGE

Ryan Roger Rathje
Iowa State University

ISECUBE – A Portable ISEAGE

by

Ryan Roger Rathje

A thesis submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Co-Majors: Computer Engineering; Information Assurance

Program of Study Committee:
Douglas Jacobson (Major Professor)
Thomas Daniels
Yu-Che Chen

Iowa State University

Ames, Iowa

2006

UMI Number: 1444566

ProQuest Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

Table of Contents

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

As the Internets' potential continues to grow in functionality and services, malicious activity becomes more prevalent. Professionals and researchers are working hard to create and implement secure systems, but this can require extensive tools and training to arising situations.

ISECUBE has been developed to be used in conjunction with Iowa State University's Internet Scale Event and Attack Generation Environment (ISEAGE) to act as a self sustaining portable environment as well as an extension of its functionality and services. ISECUBE is a transportable device that provides different realistic environments. These environments were designed with the classroom, research collaboration, and corporate use in mind. Overall statistics of usage is collected and can be viewed in different formats for later analysis. By developing such a device, the education and security fields can benefit from ISECUBE's capability.

CHAPTER 1. INTRODUCTION

The risks associated with using the Internet remain high. Risks such as security flaws, credit card fraud, data privacy and confidentiality, and more importantly, identity theft are serious threats. Controls have to be developed to counter these risks. ISECUBE is a multi-purpose tool that provides a number of useful features for various scenarios in order to combat these risks through teaching, training, analyzing, testing and implementation. By combining these five areas, risks can be greatly reduced. The main focus in the development of ISECUBE is to have a fully portable device that can act as a highly configurable Internet environment suited for multiple scenarios. By implementing such a device, ISECUBE will show how awareness in security can be increased and the collaboration of research can be made easier.

ISECUBE will consist of a partially enclosed rolling rack mount case that can be transported to classrooms for educators, labs for researchers, and companies for testing and development. It provides all the services that the Internet exhibits as well as three distinct networks for different types of activity; Active/Virtual network, Spanning network, and Mapper network.

ISECUBE has the ability to be configured for various scenarios such as teaching/outreach and research. Exercises can be developed within ISECUBE to show inherent weakness in different systems as well as proper implementation of security mechanisms. Deploying Cyber Defense Competitions are also available within ISECUBE's configuration set that can be used to further education or research efforts. Techniques can be utilized to analyze data or the testing of new hardware or software tools for research purposes.

When people use the Internet, they expect certain things such as confidentiality and data integrity, but it is important to remember that uninformed people mainly cause security problems [1]. People need to understand what the specific risks are that their company or home network faces from being connected to the Internet. Having an elaborate security scheme does little good if employees are not using proper methods when accessing sensitive information. A recent report about the Internet security threats stated that home users are less likely to have established security measures in place. Attackers are using new techniques aimed at client-side applications including Web browsers, e-mail clients, and other desktop applications. Vulnerabilities affecting Web applications accounted for 69 percent of all vulnerabilities in the first half of 2006 [2].

ISECUBE is primarily a self sustaining system that is able to react based on a given configuration. The overall functionality of ISECUBE shares some similarities to that of a virtual network that utilize programs such as VMWARE [3] or Virtual PC [4]. The functionality of ISECUBE differs greatly from both of these as it is not aimed at emulating the Internet through virtual links, but rather by transmitting traffic through physical network architecture to obtain real world results. The uses for ISECUBE can range from testing exercises in an isolated environment to traditional network operations when attached to a live network. This introduces the desire for different configurations.

First, ISECUBE can be configured to be a complete isolated Internet environment. While traditional networks are wide spread and consist of many nodes, ISECUBE must be able to obtain the same type of "look and feel" that the Internet exhibits from a client's perspective; this includes everything from routing, breadth and depth of content, to the services that are normally available.

Secondly, ISECUBE must have the ability to switch configuration with ease. The transition from an isolated Internet environment to the live attachment of an existing network

should not take an extended period of time or effort. Typically this will be governed by a graphical menu in which an administrator can set various options.

Thirdly, act as an extension of services that the Internet Scale Event and Attack Generation Environment (ISEAGE) offers. The ISEAGE facility was created with the primary goals of researching, designing, and testing cyber defense mechanisms as well as the analysis of cyber attacks in a controlled environment [5]. There are numerous applications that ISECUBE isn't capable of performing. These applications may include situations that require a large amount of processing power, capable of performing advanced routing routines, or to study the communication between multiple nodes. ISEAGE is designed to handle larger and more advanced types of scenarios whereas ISECUBE compliments ISEAGE by being portable and more versatile on a smaller scale.

ISECUBE's design was inspired to meet the specific needs of the ISEAGE lab. ISECUBE was designed to be deployed out in the field as an extension of ISEAGE. ISECUBE assists ISEAGE on different levels, these include offering services remotely but primarily focusing on the training and teaching aspects.

The structure of this thesis is such that Chapter 2, titled Background will discuss many relevant technologies and the rational for designing ISECUBE. Chapter 3 will depict various scenarios in which ISECUBE can be used. Chapter 4 will discuss the ethical issues revolving around the release of such an environment. Chapter 5 will detail design and implementation aspects. Chapter 6 presents future work and Chapter 7 is the conclusion.

CHAPTER 2. BACKGROUND

There are various ways of creating a virtual environment. VMWare [3] and Bochs [6] allow one physical machine to run multiple operating systems at once, each within their own environment. Using these tools, a virtual network can be setup to perform a given task. Another similar method is to use physical hardware for each operating system and use the private addresses as defined by the Requests for Comments (RFC) 1918. The development of ISECUBE is based on a number of existing applications and techniques. This section will serve as the introduction of these methods as well as discuss the parent project of ISECUBE.

Virtual Networks

Virtual networks are a common practice whether it's used in the lab environment for research/education, or the corporate world for testing and development of different applications. Honey potting is just one example that makes use of VMWare which proves to be a valuable tool when examining data in memory. In the event that a disposable network is needed (emulated or physical), virtual networks often use a private IP range as defined by RFC 1918 as a safeguard against the information being leaked out into the Internet.

When creating a virtual network, its configuration is dependent on the physical hardware, such as the type and number of network adapters of the host operating system. The configuration and physical hardware of the host operating system are usually different across computers.

Virtualization

Virtual networks are often implemented where physical hardware resources are low. Running virtual machines on a host saves on physical maintenance, physical space, ease of use, and saves time. As strong as these advantages may be, there exist equally weighted disadvantages especially when hardware complications arise. When creating a virtual network, its configuration is dependent on the physical hardware, such as the type and number of network adapters of the host operating system. The configuration and physical hardware of the host operating system are usually different across computers. Hardware-specific device drivers and applications are not supported in virtualized servers. VMWare contains hardware limitations that prohibit certain functionality which hinder its usability:

- VMware virtual machines do not support FireWire
- VMware virtual machines provide no direct USB 2.0 support, but make USB 2.0 devices in the host operating-system visible to the guest operating-system as USB 1.1 devices
- VMware virtual machines provide only experimental support for 3D hardware acceleration
- The bugs of the host become the bugs of the guest OSes

In addition, the performance of virtual machines (vm) are only as efficient as the number of emulated operating systems divided by the hosts installed memory and raw physical processing power. Ultimately, as the number of installed vms increases, the lower the individual performance becomes.

Virtualization may introduce new security weaknesses. Machine-level virtualization might allow systems to be hijacked without users' knowledge. A proof-of-concept attack has

been demonstrated using the "Pacifica" virtualization support in AMD's processors, and is undetectable to security tools running in the target system.

Physical

Using physical hardware to create a virtual network allow researchers to test out security configurations prior to deployment and witness how real attacks might play out against real hardware and software systems. In terms of realism, using physical hardware incorporates actual latency on the wire, whereas with virtual machines, the communication is handled internally. When measuring performance, it is important to keep in mind that the best predictions can be made by using real-world activity.

Portable Educational Network

The Portable Educational Network (PEN) was developed at The George Washington University. PEN is a transportable device that was designed for classroom use. PEN is divided into three domains; Attack, Target, and Administrative. External workstations (laptops) are used in the attack network, while vulnerable machines make up the target network. The Administration network is used to manage the logging of information as well as well storing ghosted states of each workstation [7].

While ISECUBE and PEN share similar goals, implementation and use vary. The design and implementation of ISECUBE incorporates all aspects of the Internet. This includes the look and feel of brows able random web pages that contain linkable content and the redirection of communication. Additionally, ISECUBE has the ability to change functionality to host/join Cyber Defense Competitions without modifying or losing any locally stored information. The desire to keep these networks unique and separate is attained.

ISEAGE

The ISEAGE project was developed by Dr. Doug Jacobson at Iowa State University. The intent of ISEAGE is to provide "a world-class research and education facility to enhance the current state of the art in information assurance"" by creating a virtual Internet environment that realistically portrays all aspects of the authentic Internet. With this type of an environment, "researching, designing, and testing cyber defense mechanisms can all be brought together for a common goal of making computing safer [8]. The ISEAGE project can be used in many different applications. Figure 1 shows the different uses for such an environment.

Since its initial debut in 2003, ISEAGE has already hosted a variety of events such as computer security camps for IT professionals, training sessions for the Information Assurance Student Group (IASG) and various Cyber Defense Competitions (CDC) ranging from the high school level up to the regional event. Other tools have been developed as well. The traffic generator was developed to generate background traffic or noise. Racks that hold eight computers (called Glaciers) are fully accessible from anywhere on the Internet that provides alternative methods of accessibility and configuration.

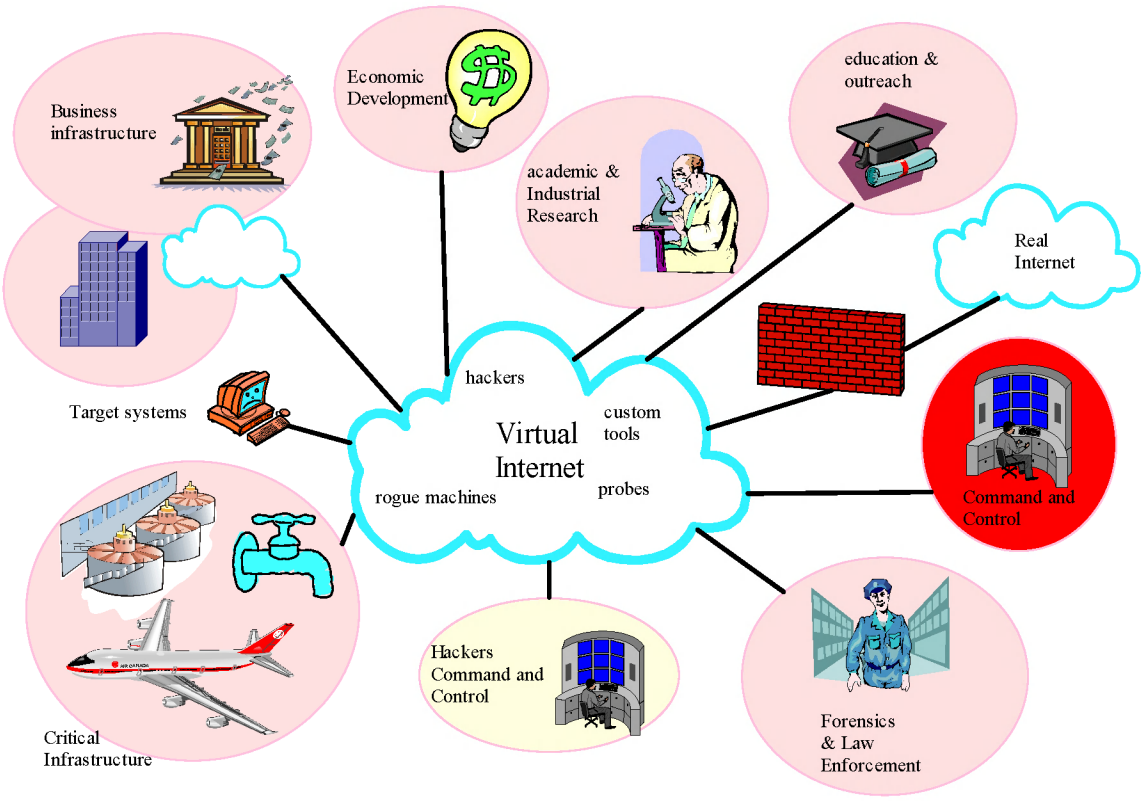

Figure 1. ISEAGE Applications

ISEAGE Functionality

At the heart of ISEAGE lies a gigabit switching core that is interconnected by 64 nodes. Each node controls a virtual subnet in which any number of routers can be emulated thereby managing any IP range. By combining all these routers together, it allows the recreation of large portions of the Internet by representing hundreds of subnets.

Having the core of the Internet in place is not enough to merit its authenticity. Applications have been developed to aid this process. Advanced Packet Obfuscation and Control Program (APOC) [9], and Simple Network Imitator Program (SNIP) [10] are tools that have been developed at Iowa State for ISEAGE to assist in creating a realistic environment. This includes creating background traffic between virtual hosts to generate

both malicious and non-malicious communication. Additionally, early stages of the Intrusion Collector and Emulator (ICE) project have surfaced which will collect and replay attacks.

CHAPTER 3. SCENARIOS

The goal of ISECUBE is to have a portable system that will provide any number of possible uses all while requiring little or no configuration change. Currently, there are a number of possible scenarios that ISECUBE can be applied to. These scenarios can be broken down into three environments: 1) a fully functional isolated Internet environment, 2) an active extension of an existing live network, and 3) an extension of services provided by ISEAGE. The design and development of ISECUBE was inspired for the use outside of the ISEAGE lab, primarily for onsite teaching and research.

Outreach/Teaching Scenarios

These scenarios encompass exercises that are used to educate others about certain aspects of information or network security. The traffic that is generated from these exercises should not be transmitted outside of the intended environment due to potential damage to other networks and violation of usage policies. The goals of these scenarios are to expose the students to vulnerabilities and weakness in systems.

ISEAGE

ISEAGE will serve as a central core where deployed ISECUBEs will be able to connect or "call home". It will also be utilized for advanced teaching or training topics. Deploying ISECUBE into the field will act as an outreach effort that will promote the available resources that are housed within ISEAGE. This connectivity incorporates a test bed environment in which advanced exercises, testing and evaluation, and the continuation of computer and network security education will be delivered.

Plaintext

In cryptography, plaintext is usually the input that is accepted by an encryption algorithm, whereas the generated output from this algorithm is called cipher text. Plaintext could be any piece of information ranging from a simple message, bank records, to a social security number that someone would like to keep from preying eyes. Plaintext is a form where it is readable by anyone because it is not protected by any means of encryption.

In the realm of security, weakness can be introduced through insecure handling of plaintext whether it's processed or stored. ISECUBE has injected this weakness into its application module by allowing username and passwords to be sent in plaintext. By using a sniffer program, such as Wireshark [11], students can collect this traffic, analyze it, and see firsthand the potential dangers of poorly implemented solutions such as unencrypted html and email messages. This type of exercise can be extended to other protocols such as FTP and telnet.

Secure Channels

Web browsers send and receive information without encryption to communicate with web servers. For sensitive information, such as bank records, credit card information, or social security numbers, the browser and web server use encryption (HTTPS) for protection from eavesdroppers. HTTPS is not a separate protocol, but refers to the combination of normal HTTP traffic in conjunction with encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS).

SSL runs above the TCP/IP protocol and beneath application protocol layers such as HTTP, FTP, SMTP and NNTP and can be applied to almost any sort of connection-oriented communication. While adding security to any protocol that uses reliable connections is preferred, it is commonly used with HTTP to form HTTPS.

Even though a number of client and server applications support SSL natively, there are many others that lack this functionality Alternatively, users may implement other standalone products like Stunnel that rely on being able to obtain an SSL connection immediately by a separate port. The rational for a separate port reverts back to 1997 where the Internet Engineering Task Force (IETF) recommended that application protocols always start unsecured and instead offer a way to upgrade to TLS - which a pure wrapper like Stunnel cannot cope with [12].

Wired Equivalent Privacy (WEP)

WEP was designed to offer the same level of security of that of Local Area Networks (LAN). LANs can be defined as more secure because of the physicality of a network being located in a building that in itself can be protected from unauthorized access. Wireless Local Area Networks (WLAN) use radio frequencies which can't be bound by the same structure as LANs therefore are susceptible to tampering. To help aid in making it secure, WEP provides end-to-end encryption. However, WEP has been proven not to be as secure as initially thought. Wi-Fi Protected Access (WPA), WPA2, Lightweight Extensible Authentication Protocol (LEAP) are more robust encryption algorithms that have been developed and can be used in WLANs.

Implementing a wireless access point is only as strong as the configuration that the administrator chooses. Placing an access point within the Active/Virtual network (see figure 2), allows clients to have a transmitting wireless network, and enables them to learn about the different security levels. Configuring an access point to use WEP (64 or 128 bit key) and place it within ISECUBE allows the client to use another method of access. Furthermore, having an access point connected to an isolated network that is transmitting large amount of data, clients can use wireless attack tools to exploit the underlying weakness of the WEP

algorithm as well as other wireless attack methods. These exercises emphasize how critical it is to use good security practices.

Email (Spam, Phishing)

Phishing has been a major problem on the Internet. Phishing is the sending of false email messages attempting to scam the end user of private information that could be used for financial gain on behalf of the attacker. Phishers attempt to bypass filtering technologies by creating multiple randomized messages and distributing those messages in a broad uncontrolled fashion. During the first six months of 2006, 157,477 unique phishing messages were detected, marking an increase of 81 percent over the previous period. At the same time, spam made up 54 percent of all monitored e-mail traffic, a slight increase from 50 percent the previous period. Most spammers are opting to exclude malicious code with their spam to decrease the chances of being blocked [13].

The dangers of participating in phishing and spam messages can weigh in heavily on people as well as corporations. Using ISECUBE, phishing and spam messages can be sent to the mail module through an internal open relay. By allowing such activity, users can be educated how to spot phishing/spam message, how to track their origins, and how to further protect themselves against becoming a victim. Sometimes email messages contain links to other websites. These links can lead to websites that host malicious code that can turn the connecting machine into an attacker's playground.

Safe Internet Practice

As networks grow and technology expands into new areas, network security becomes critical. As more and more people come to use the Internet and its services, the same people need to understand the basics of security in a networked world. When a network is penetrated by an attacker, it's immediately assumed that the attacker broke something to gain access. On the contrary, it's common (especially in home networks) to find that the security

measures that were in place didn't fail at all, but rather were not enabled from the start. Often, such security does not even exist, allowing one user to easily access another user's machine using well-known exploits, trust relationships and default settings. Most of these attacks require little or no skill, putting the integrity of a network at stake.

Internal network security is often underestimated. In most networks, employees do not need access to each other's machines, administrative functions, or network devices. However, because of the flexibility that's required for day to day operations, it would be a nightmare to enforce maximum security. On the other hand, with poor or no security at all, internal users can be a major threat to many corporate internal networks seeing how 80% of network attacks originate from inside the firewall [14].

The overall design of ISECUBE is to offer an Internet environment in which any scenario can be played out. When dealing with new technology, administrators are in no rush to incorporate it into their networks until a good understanding of its capabilities is in place. Without that knowledge, they place their entire network in jeopardy. Attaching new devices to ISECUBE allows administrators to accomplish this, giving them a live isolated version of the Internet; implementing new or existing technology is made easier and safer. Additionally, changes in network topology and communication can hurt productivity. Whether it's testing a new firewall rule set or adding another subnet and diverting traffic through a router, certain things cannot be experimented without previous testing in a live environment. By accomplishing this, right versus wrong implementation, good versus bad techniques can be learned.

Research Scenarios

The following scenarios are designed to attach active networks to ISECUBE to help diagnose network problems, predict traffic patterns, search for network vulnerabilities, as

well as plan for product roll out. This has the potential danger of damaging the active network if executed poorly. The intended goals of these scenarios are to interact with active networks, sending communication to and from ISECUBE, therefore increasing the effort for network hardening.

ISEAGE

Since ISECUBE is an extension of ISEAGE, this allows for distributed research projects to exist. ISECUBE can be deployed in multiple locations to serve as a collaborative research effort which can attach back into ISEAGE. ISEAGE encompasses a variety of tools that are not suitable for ISECUBE as a standalone device. Access to these tools are made available through ISECUBE only when connected to ISEAGE to perform remotely.

Black Hat Activities

Computer and network specialists (white hat) have fought against computer criminals (black hats) in attempts to stay ahead. As computers become more powerful, as does the skills of criminals, traditional security measures become less effective therefore experts have to battle to stay on top. This is known as the security arms-race. Computer and network forensics are new fields of study whose goal is to diminish discovery time and respond more rapidly after an attack.

After the discovery of a breach, surveys are conducted to reveal the extent of the damage on other systems. Methods used by attackers to hide their malicious actions after a successful break-in have become more complex over recent years whether it's root kits, network backdoors or covert channels. This kind of activity can be difficult to detect, or worse, knowing when/if it has ever happened on other systems. Developing and testing new offensive techniques from within is no longer looked at as a waste of resources, but rather a good investment. Using ISECUBE to develop and test these new offensives can give

personnel a new way of attacking their own design and testing the robustness of their systems.

Network Heuristics/Statistics

Knowing what is happening in a network is critical. The collection of communication can be useful but often turns into a tedious analytical task when seeking lesser details. When the collection of specific information can pose certain security risks, heuristics can prove to be more insightful specifically when interested in traffic patterns and anomalies. In the case of ISECUBE, traffic is needed to recreate the legitimacy of the impersonating network. Replaying the original information from certain networks could pose as a security breach due to the sensitive nature of its contents. Choosing to use the heuristics instead of actual data keeps the legitimacy of the environment as well as not compromising any identifiable information. By using a third party analyzer, such heuristics can be derived from the attached network. These heuristics can be replayed; in the form of a packet generator; within ISECUBE to achieve realistic background traffic or "noise".

Internal Pen Testing

When the perimeter of a network is secured and hardened, it is equally important to complete an internal audit. The goal of internal penetration testing (pen test) is to test the security policies on the inside of a network and to find any violations that could affect the integrity of the overall system. It's a process whereby a company contracts with a security firm; and/or uses its own security personnel; to attempt to break into a network and its resident systems by using a variety of exploits and methods.

Testing New Hardware/Software/Methods

Many organizations build an ad hoc lab each time they need test facilities for a new project. These labs serve as the testing and evaluation grounds of hardware and software to

determine efficiency, reliability, and compatibility with existing systems. Additionally, they help aid the development procedures for installation, use, and problem solving of hardware and software issues.

The testing of large network-based applications can be difficult, especially in early development. Experimenting with an early or beta version of software on an active network can lead to vulnerabilities and leave it susceptible to future attacks if not maintained. The same can be said about implementing new network modules when not configured properly.

ISECUBE combines the demands of ad hoc labs into a single environment to facilitate testing. The benefits range from setup/tare down time to collecting and reviewing the results. An example is best shown by the testing of an IDS or IPS. An IDS can be attached to the spanning network; in which a copy of all traffic is passed through; to better understand and evaluate its performance and capabilities. At the same time, network statistics are collected by the monitoring module making the overall procedure easier to execute and analyze.

Cyber Defense Competition (CDC)

The CDC is an event between students and industry professionals centered on network security and information assurance. It is designed to test student abilities against a realistic scenario and to provide an educational test-bed to encourage growth and collaborative teamwork. These competitions give students the opportunity to expand on their knowledge base from an individual standpoint to a collaborative movement. Challenges such as the installation of an operating system to the implementation of various security techniques are met and overcome. "Participating students learn in a true active learning environment. Instructors are able to evaluate the thoroughness of their curriculum in its intended setting. Other students learn as teams prepare for the competition. In the end, everyone feels they had learned important lessons." [15]

CHAPTER 4. ETHICS

One of the most discussed topics in the field of computers is computer security. Today we find ourselves in a race condition in keeping our data/network secure from preying eyes. In the past, algorithms were developed in hopes that raw processing power would not catch up to the computation time required to break it, such as hashing, and brute force methods.

Despite the challenges that computer security has over come in its history, nothing has been more of a heated topic because of the advancements made in technology and its aggressiveness. Having processors powerful enough to break password hashes in a matter of minutes (given the right data set), or computers portable enough to scan the wireless traffic in the air while on a holiday trip can be unsettling or disturbing to some.

As Tavani states, computer security has its tradeoffs that can be viewed in cost, convenience and flexibility [16]. Based on Tavani's statements, it is suggested that the cost factor can be viewed as negligible (except for the extreme conditions). The cost of implementing an effective infrastructure that could be initially expensive for a company is far less than what it would cost due to the loss of information, ramifications of a security breach plus the loss of consumer confidence. The flexibility of such infrastructure usually comes in the form of high cost. Finally, convenience can never be absolute without affecting the other two.

In the event of a security breach, computer forensics has to be able to extract bits of information to help investigators. Furthermore, it remains important not to develop next

generation security tools to limit/hinder that aspect. Releasing a security technology that is considered revolutionary can act as a double edged sword; one side for corporations to protect their data and the other side for criminals to hide theirs [17].

This section of the paper will discuss various aspects; both positive and negative; due to the design and development of ISECUBE. These aspects include Internet Service Provider (ISP) policies and appropriate Internet conduct, hacking techniques, available exercises, privacy, and advantages/disadvantages of ISECUBE and how it ties into Internet security.

Internet Conduct

No global usage policies exist, only those enforced at the service provider level. Even when a violation has occurred, usually no action is taken unless a third party notifies them of that user's activity. Additionally, if all service providers enforced their policies, there could potentially be a great deal of difference between them. At best, there does exist a "10 Commandment of Computer Ethics"

1. Thou Shalt Not Use A Computer To Harm Other People.
2. Thou Shalt Not Interfere With Other People's Computer Work.
3. Thou Shalt Not Snoop Around In Other People's Computer Files.
4. Thou Shalt Not Use A Computer To Steal.
5. Thou Shalt Not Use A Computer To Bear False Witness.
6. Thou Shalt Not Copy Or Use Proprietary Software For Which You have Not Paid.
7. Thou Shalt Not Use Other People's Computer Resources Without Authorization Or Proper Compensation.
8. Thou Shalt Not Appropriate Other People's Intellectual Output.

9. Thou Shalt Think About The Social Consequences Of The Program You Are Writing Or The System You Are Designing.
10. Thou Shalt Always Use A Computer In Ways That Insure Consideration And Respect For Your Fellow Humans. [18]

Even though this list depicts good Internet practice for common users, there are a few that need to be emphasized when using ISECUBE. First, due to the nature of ISECUBE as a teaching tool, commandments 2 and 3 should be highly respected and upheld. Disrupting and meddling with a systems or files are examples of common scenarios that encompass ISECUBE. Secondly, the research aspect of ISECUBE allows for the analysis of attack methods and data sets. Attacks methods are often discussed to show others the importance of proper implementation as well as the techniques that were used. Once these attacks have been understood, it's common to educate others about the impact that these attacks can have on systems. By educating others about proper implementation and possible attack types, this creates an ethical dilemma; it increases the level of overall knowledge that one can use to protect a system, but in retrospect, it also potentially increases the number of those who have malicious intentions for its use, which goes directly against the 4th commandment. Lastly, the 7th commandment states that one should not use computer/resources in which they are not authorized. This can be summarized by the previous two points; upon the successful understanding of an attack (research aspect), and the sharing of that knowledge (teaching aspect) it should never be assumed that outcome should be taken as acceptable Internet conduct and widely dispersed.

Information Security and Privacy

The youth of today's culture appear to have misunderstood the importance of privacy and security. Using public websites to post personal habits, phone numbers, and addresses as a form of self expression seem to convey that this type of activity is acceptable when in fact it is not by any measure. By freely dispersing sensitive information, this shows that others are not being properly educated about how important one's privacy is, nor the understanding about the subjection of vulnerability that one imposes due to this type of risky behavior.

ISECUBE is designed to show the initial lack of security that the Internet exhibits that can ultimately lead to the breach of one's privacy. The building and maintaining of a security system that respects the individual's (or user's) right to privacy as well as fulfill the duties and obligations to one's employer and client is the intended goal of any network [19]. The question arises: Is there a point when the benefit of security outweighs the value of the user's privacy? In terms of privacy and how it relates to ISECUBE, ISECUBE can be used to show that by being able to identify its users, a union occurs between security and privacy. This, in itself, increases the overall security of the system because then an attacker or intruder can be more easily detected therefore better protecting the systems' assets. Furthermore, by properly implementing a secure system within ISECUBE, protecting its internal user's privacy through secure channels become self evident.

There are different scenarios in which ISECUBE can be configured to emphasis the importance of information security. The contribution that ISECUBE makes to the information security field can be seen from many different aspects. These include societal values that effect individuals, groups, and companies; security aspects that can range from a single person to an entire corporation and even an awareness aspect that Iowa State University can use to disperse valuable information to partners.

Society benefits from the development of ISECUBE on many different levels. First, the end user benefits from more secure products that become available due to the research

that's made possible. Secure products protect the average consumer from becoming a victim of credit card fraud, or phishing scams. Additionally, secure methods permit users to view sensitive information by means of encryption, allowing only those that are authorized. Secondly, companies and corporations can try out new network and security applications without putting their networks in jeopardy. By taking this approach, this leads to better implemented services as well as higher availability and security which then turn enhances the business to consumer experience and trust relationship. Lastly, researchers have the flexibility they need to be able to test for a variety of cases. Again, this leads to better developed products and services.

Email Scenario

This section discusses the specific issue of privacy and the use of ISECUBE as well as risk and prevention revolving around electronic email (e-mail). Email has become such a common tool used for communication; it is convenient, fast, and free. When sending a letter through the traditional mail system, it's usually protected in a sealed envelope. Unfortunately, sending an email message does not carry this same type of protection, in fact email messages are sent in the clear, by default. E-mail privacy, without some security precautions, can be compromised because of the following:

- e-mail messages are generally not protected by encryption;
- e-mail messages traverse through intermediary nodes (or computers) before reaching its destination. Making it relatively easy for others to intercept and read messages;
- many Internet Service Providers (ISP) store these messages on their mail servers before delivering. Backups are usually stored for an extended amount of time even after the recipient retrieves it.

- identifiable information is stored in email headers, preventing anonymous communication.

There are applications that encrypt messages to serve as a solution to one or more of the above risks. Applications such as Tor (anonymity network) or using Virtual Private Networks (VPN) can encrypt traffic from node to node. Others include PGP or S/MIME can be used for end-to-end message encryption, and SMTP STARTTLS or SMTP over Transport Layer Security/Secure Sockets Layer. A common risk is that e-mail servers may not implement secure methods of initial authentication; therefore passwords might be intercepted during the sign-in procedure. SASL is an encrypted authentication scheme that could be used to help prevent this type of activity. [20]

Computer Break-in

Is there a time when breaking into a computer system is ethical? Hackers and crackers are defined as those who break into systems to steal or destroy information. This type of activity is not deemed as ethical from the white hat perspective because this modifies/alters the information in a way that could potentially hurt people. The only type of ethical hacking that exists today is in the form of education, and even this can be risky. By educating students about methods that violate system policies by real world examples, the real importance about proper implementation and security practices becomes self apparent immediately. After understanding these techniques, countermeasures can be derived and put in place to aid against such offensives.

Penetration Testing

What is the value of finding and patching a hole before it can be exploited when a multi-billion dollar company completes all of its business over the Internet? The act of

finding and patching a hole that would have cost the company a few million dollars is well worth the associated cost of testing. If these things are never even looked for, it's only a matter of time before the company is hurt financially and its reputation is tarnished. When thinking about how a pen test of a network should be carried out, two different approaches are available. A common approach is to contract a third party. This approach can take weeks and can be costly to the company. Independent teams and third-party contractors have no such allegiances and are more likely to be ruthless in their critique of the network. No matter how bad the news, hearing it from them is preferred rather than having it splashed across the news in front of their clients. The second approach is to have an IT group who is internal to the company complete the pen test. The primary weakness with this approach is the lack of creative outside knowledge and secondly they may be predisposed to avoid situations that expose shortcomings; essentially, they may be simply too close to remain objective. Ultimately the best type of pen test is the combination of a third party company as well as an internal group of the company. This yields the most effective results and can be costly, but it still outweighs the damage associated with financial lost and customer confidence.

Exposure

Understanding how quickly a virus can spread and its effects on a network can mean the difference between little interruptions or massive denial of service when proper counter measures are not in place. The monitoring module can give an overview on how rapid a virus can spread based on how many IP addresses it targets. If a trojan or malicious code is allowed to traverse through ISECUBE, then any device that is connected could be affected. It is important that the environment is clean before attaching ISECUBE to a live network.

In the case that actual traffic is replayed through ISECUBE, it must be understood that attached clients could be ultimately affected by covert methods that aren't initially

evident. This can lead to data loss as well as potential hardware damage depending on the severity of the situation. Using ISECUBE as a research tool is a primary function, but with this functionality comes great risks as well as greater benefits.

Risks v Benefits

Since the initial development of ISECUBE, it has been assessed heavily in terms of risk. This is because there are particular ethical issues that arise surrounding the purpose and use of ISECUBE, particularly the issue of misuse. This section will discuss one of the major goals of ISECUBE, which is to maximize the associated benefits and to minimize the related risks.

Understanding the different scenarios in which ISECUBE can be configured; one might conclude that this could be furthering the advancements for malicious activity. While this view point carries weight, it can be mitigated from the security aspect. By allowing such activity to play an important role within ISECUBE, security methods can be quickly developed and shared to decrease the initial threat. To further discredit this risk, ISECUBE is far too expensive to "fall" into the wrong hands, and furthermore attackers typically don't buy hardware to support their cause. Since ISECUBE was developed using all open source applications, the risk of distributing ill developed (or buggy) software has potential. By utilizing open source, more people have the opportunity to enhance and improve the software through contribution.

The associated benefits of using ISECUBE outweigh the above risks in many areas. Since ISECUBE is destined for production, this means that ISECUBE could be used for other applications that have not been described here. Secondly, increasing ISECUBE's base means more research and development in the security field resulting in better products and methods of information assurance. Additionally, because of the strong focus that ISECUBE

has on the education sector, students and alike will be better equipped to make smarter decisions pertaining to their personal security as well as proper implementation of tools. Thirdly, the mobility of ISECUBE is a key driving aspect behind the availability and collaboration of information. This is crucial as corporations grow and as classroom diversify. From a time and cost perspective, it's difficult to organize large identities to move to a certain location for training and isn't always cost effective. Lastly, the Iowa State University Information Assurance program can benefit greatly from ISECUBE in terms of outreach. The outreach effort can include training seminars that are distributed to remote sites, network analysis to help diagnose and remedy bottlenecks and other potential problems, and even execute remote CDC events that tie back into ISEAGE to increase overall involvement.

In summary, from an ethics perspective there are questionable aspects which exist, none of which cannot be controlled with proper care. Greater yet are the benefits that can be seen from the standpoints of society, consumers, companies, education and government. These benefits ultimately lead to the advancement of security tools, applications, techniques, education of privacy, security and information assurance.

CHAPTER 5. DESIGN AND IMPLEMENTATION

This section will provide an in-depth look into how ISECUBE works and problems that were overcome in its development. It will start by explaining a general module from a hardware aspect, and then it will continue to explain the function of each module in relationship to the entire environment giving examples of real world application.

Structure

The design of ISECUBE is to replicate all communication channels in an environment that can be isolated, readily accessible, and easily configurable for different scenarios. ISECUBE is broken down into five modules; core, application, protocol, monitor, and mapper. Each module has an associated function or operational process. These modules are needed in order to bring together all aspects of the Internet to a common platform. Typically there will be little to no communication between modules in order to keep the primary focus on client and module interaction.

Each module contains three network interface cards to access the three networks, which include Virtual/Active Network, Spanning Network, and the Mapper Network. Figure 3 shows the complete ISECUBE topology. These networks allow for various devices to be directly attached. The Virtual/Active Network allow devices such as single/multiple user systems to be connected. These devices include computers, servers, wireless access points, basic networking devices, and similar technology. The Spanning Network is designed to be a virtual "tap" that all communication can be viewed or analyzed from. Appropriate devices that would attach at this point would be intrusion detection systems (IDS), intrusion prevention systems (IPS), or other network analysis tools. The Mapper Network is a special network that can only be accessed via the special boot sequence Preboot Execution

Environment (PXE). This environment is intended to tie into the backplane of ISEAGE utilizing the Internet as the communication medium.

By combining the uniqueness of these three networks into one environment, ISECUBE is capable of being configured for virtually any type of framework.

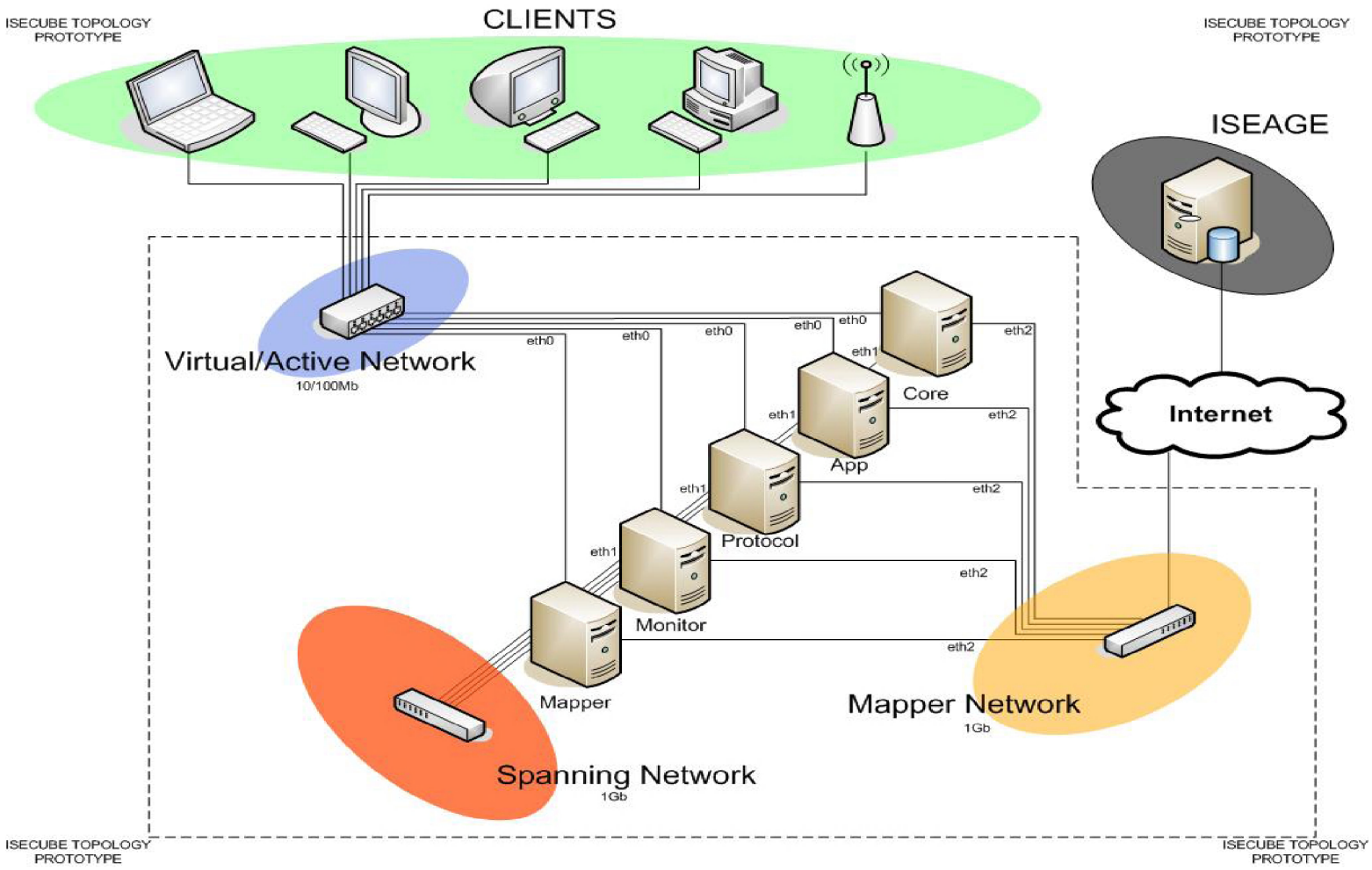

Figure 2. ISECUBE Topology

Core

The core is the primary module that communication is sent through. It handles the assignment of unique Internet Protocol (IP) addresses for connected devices, randomly generating destination IPs for web pages upon request, and creating dynamic web page content. The main objective for this module is to provide as much of the look and feel of the authentic Internet as possible while remaining completely transparent to the clients.

Dynamic Host Configuration Protocol (DHCP)

In a traditional network, clients obtain unique IP addresses and other parameters such as default router, subnet mask, and IP addresses for DNS servers from a DHCP server. This takes place immediately after booting and before the client initiates any IP based communication with other hosts. This information is necessary for the client as it indicates its presence on the network as well as providing routing information. Without this information, the client is left blind; not knowing anything about the network in which it's connected to.

The core module contains a standard DHCP server that handles the assignment of a class C range. The DHCP class range can be changed or can be completely disabled to meet the demands of a custom environment via the administration access control. Since the DHCP regulates the distribution of unique IP addresses, this ensures that two client cannot be assigned the same address. This also keeps the statistics collected by the monitor module separated. Table 1 depicts the number of unique IP addresses associated by each class as well as other relevant information.

Class	Purpose	Start	End	Subnet mask	CIDR	# of networks	# of IPs per network
A	Few large organization	1.0..0.0	127.255.255.255	255.0.0.0	/8	126	16,777,214
B	Medium-size organization	128.0.0.0	191.255.255.255	255.255.0.0	/16	16,384	65,534
C	Relatively small organization	192.0.0.0	223.255.255.255	255.255.255.0	/24	2,097,152	254
D	Multicast groups	224.0.0.0	239.255.255.255		N/A	N/A	N/A
E	Experimental	240.0.0.0	255.255.255.255		N/A	N/A	N/A

Table 1. Internet Protocol Address Classes

Domain Name Service (DNS)

Originally, computers utilized a file called "HOSTS.TXT" which contained a one-to-one mapping of a name to an IP address. A problem would occur when a name was entered and there was no associated IP. As technology changed dramatically and networks grew, a more scalable system was needed. The place of the hosts file was no longer kept on each computer but rather in a globally accessible domain name space [21]. This tree structure is shown in figure 3. There are different levels which are responsible for answering certain requests; such as .edu domain or the .com domain, these are referred to as root name servers. In order to translate a fully-qualify-domain-name (FQDN) into an IP address, these root name servers would have to be contacted every time a request is made. In order to help reduce the overhead that this can create, DNS provides a mechanism called caching which retains the answer that it receives for a period of time.

When the DNS server (or name server) receives a request from a client, it's checked against the server's cache. If it exists, the associated IP is returned to the originating client. In the event that it does not exist, the DNS takes over and handles the remaining queries to other name servers until either an IP is returned or an error stating that it doesn't exist.

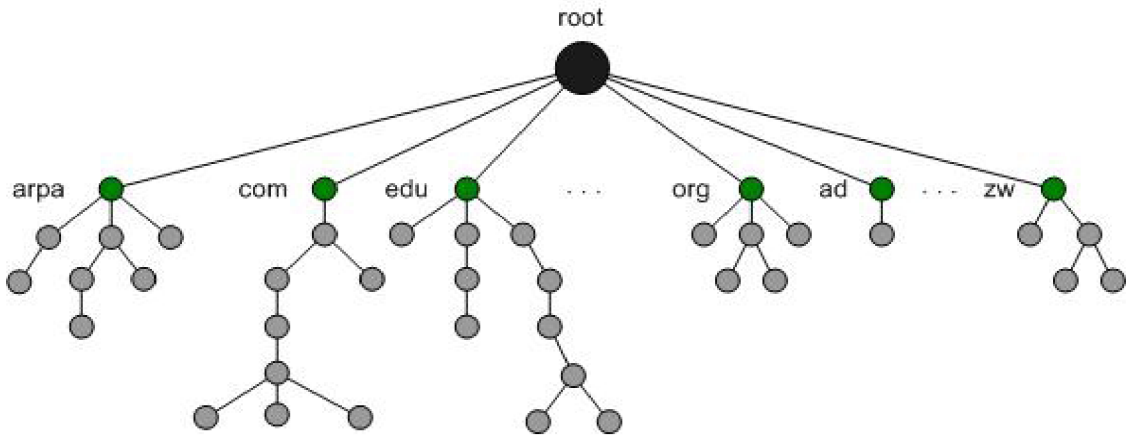

Figure 3. Domain Name Space Structure

Finally it takes this information, caches it, and passes it back to the originating client. The overall operation of a DNS server consists of four routines:

1) answer the request because it's already cached that address.
2) query another name server for the information
3) pass off the request to another name server
4) reply back with an error message due to an invalid name or nonexistence.

Initially routines 2 and 3 present a problem due to ISECUBE's design; a self sustaining environment in which no inbound or outbound traffic is allowed. Figure 4 shows the resolution for the address girigiri.gbrmpa.gov.au of a host in a domain. In order to give

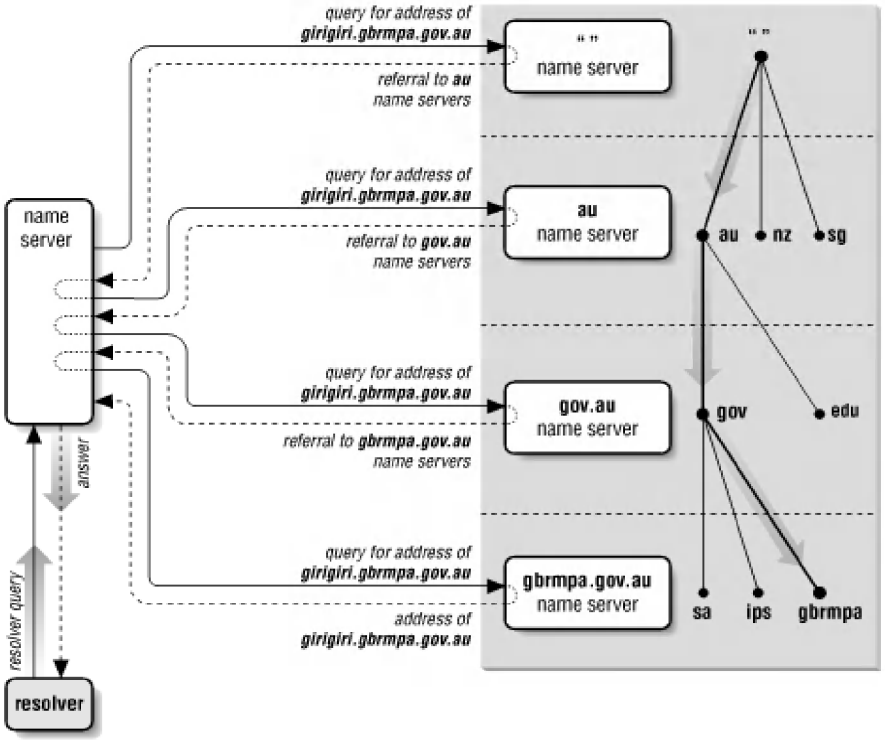

Figure 4. Traditional DNS diagram

the illusion of this functionality; while in an isolated or disconnected environment, a custom DNS server had to be written in order to compensate for these features. The result included stripping out the functionality of routines 2 and 3 from a traditional DNS server and replacing them with a random IP generator function. The name resolution component is now capable of answering any request as well as caching the results for later queries by other clients. By using a random IP generator function, this creates the uniqueness of each DNS query, much like that of the Internet. Furthermore, the queries initiated on behalf of the DNS server are not usually seen by the client, therefore by adding the random IP function internally, the overall communication model (from the clients standpoint) is unchanged.

After implementation, when a DNS request is sent on the wire initiated by a client, the DNS server receives this request, checks its cache, if nonexistent, then generates an IP, caches the record, and replies to the client's request.

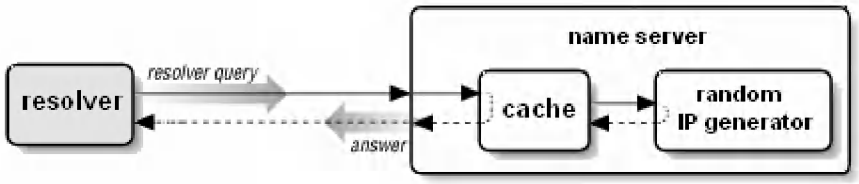

Figure 5. ISECUBE custom DNS diagram

Web Server

Web servers are computers on the Internet that host websites. The term "web server" also refers to the piece of software that runs on those computers, accepting HTTP connections from web browsers and delivering web pages and other files to them. There are many web server applications available, including public domain software from National Center for Supercomputing Applications (NCSA) and Apache, and commercial packages

from Microsoft, Netscape and others. Every web server has a unique address so that other computers connected to the Internet know where to find it on the vast network.

When a client clicks on a link to visit a website, like www.iastate.edu, the web browser sends out a request to iastate's IP address. This request includes return information and is transferred across the network. This request passes through several computers (or routers) on the way to www.iastate.edu, each routing it closer to its ultimate destination.

When the request reaches its destination, the web server that hosts iastate's website sends the page in HTML code back to the client's address. This travels back through the network to the client who receives the code and the browser interprets the HTML code then displays the page in graphic form.

ISECUBE utilizes the Apache web server with Pre Hypertext Processor (PHP) extensions as the method to serve web content. The Apache HTTP Server Project is a collaborative software development effort aimed at creating a robust, commercial-grade, featureful, and freely-available source code implementation of an HTTP Web server. Even though Apache is the application that handles web traffic, it does not receive its requests directly from clients but rather a transparent proxy.

Transparent Proxy - Squid

A proxy server is a computer that offers a computer network service to allow clients to make indirect network connections to other network services. A client connects to the proxy server, and then requests a connection, file, or other resources available on a different server. The proxy provides the resource either by connecting to the specified server or by serving it from its cache. In some cases, the proxy may alter the client's request or the server's response for various reasons [22].

Transparent proxies are often deployed in businesses to enforce acceptable use policies, and to ease administrative burden, since no configuration is required by the client's

browser. These proxies are also commonly used by ISPs in many countries in order to lower the upstream bandwidth by providing a shared cache to their customers. Additional rational for implementation may include security, load balancing, and censorship or filtering. Filtering proxies isolate objectionable elements of web pages such as cookies, ad banners, dynamic content like JavaScript, Java Applets and ActiveX controls. Some anonymous proxies use encryption, to protect against routine monitoring or even dedicated surveillance.

Proxy servers can vary in functionality that includes caching, SSL, or intercepting (transparent) proxies. ISECUBE's configuration requires a transparent proxy for the purpose of obscurity. There exist a number of proxy applications that can be configured to be transparent such as ComTun [23], WinProxy [24], and Squid-cache [25]. The incorporation of Squid into ISECUBE was based on its configuration set and transparent proxy support.

Since a proxy server acts on behalf of the client and the server, all requests from the clients to the Internet are transparently picked up through the proxy server. Then the proxy analyses the request, and if valid, re-establishes the requests on the outbound side to the Internet. Additionally, outside responses or initial requests coming from the Internet pass through the proxy, analyzed, and then passed to the client if valid. From the client and server standpoint, they appear to be communicating with one another, but are only dealing with the proxy.

In order for a successful transparent proxy to work, a firewall is needed that plays a crucial role. The firewall needs to be in place to "hijack" all port 80 traffic and redirect it to the proxy for further analyzing. This is accomplished by using the IPFW rule:

add fwd 127.0.0.1,3128 tcp from any to any 80 in via <interface name>

At this point, ISECUBE has a method of "hijacking" all web traffic transparently and has a web server to display content. Now the problem lies in getting the requests from the

transparent proxy to be sent to the web server and then back to the client. To bridge these two components, Squid has a redirect directive, when supplied in the configuration file, will pass certain traffic to a specific web server. The ideal case is to redirect all traffic from the proxy to the web server so that any request for web content will be answered.

Redirector

Since Squid has the ability to rewrite requested URLs, it can be configured to pass every incoming URL through a redirector process that returns either a new URL, or a blank line to indicate no change. Redirectors can have different degrees of functionality which can range from a simple and basic design based on a comparative rule set to those that are designed with educational establishments in mind to help block against certain content or banners/ads. The redirector becomes the link that ties communication between squid and the web server. The Squid package does not contain a redirector application, but it does contain a path for a redirector plug-in. Third party plug-ins include squirm [26], jesred [27], squidGuard [28] and others.

Application

The application module is intended as a secondary/ternary component in conjunction with the protocol module. The main goal for this module is to act as another element of the Internet, electronic mail (email) and similar protocols. The secondary goal is to show different access methods to the same dataset. Lastly, by focusing on just the email element of the Internet, various exercises be developed to emphasis policies, security, and common attacks.

Electronic Mail (E-Mail)

E-mail was one of the tools responsible for creating the Internet. In the beginning, messages where stored on machines that users would access using time-sharing procedures. Then the system expanded rapidly due to the ARPANET computer network. Today, email is one of the most important services that the Internet provides. According to the February-April 2006 survey by Pew [29], of the reported 147 million users, 91% of Internet users send or read email. Many people sign up for an email account and use some type of application such as Eudora or Microsoft Outlook to access it. For some people email use is just now becoming main stream, while hackers have been using it for 20 years or more.

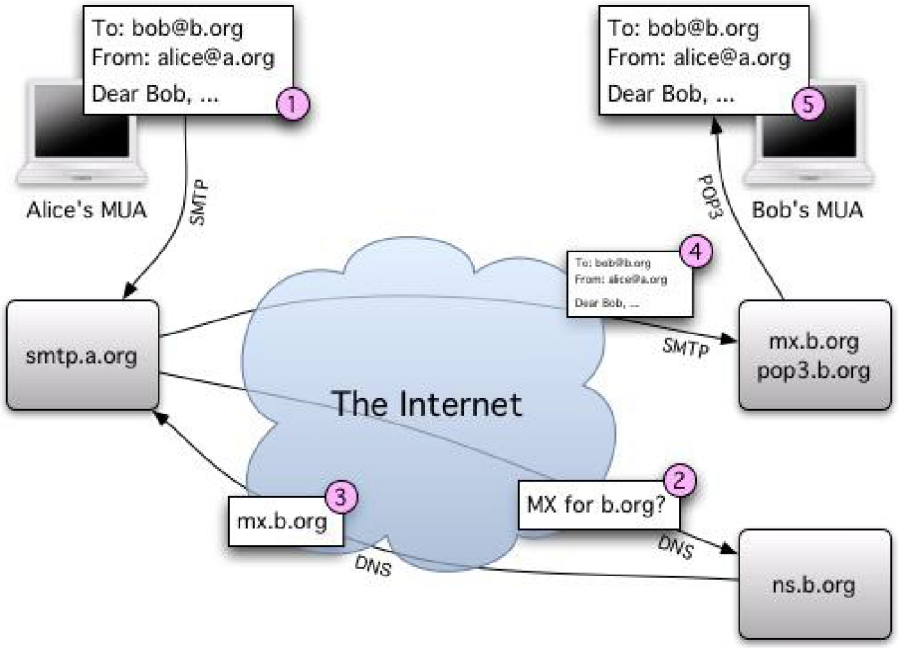

Figure 6. How Email Works

The diagram above displays the overall operation of the composition and delivery of an email message.

There are a number of methods of accessing email, all of which are used for different purposes. Once an email message is received by a mail server, a client is then authorized to start the retrieval processes. A web mail server can be used to interface between the client and the mail server. This is typically accessed via the client's web browser. All information is kept at the server level. This allows the client to be anywhere on the Internet and still have access. The drawback of web mail is that it can't be stored for offline usage. Other protocols such as Internet Message Access Protocol (IMAP) and Post Office Protocol (POP) were designed for this purpose. When using IMAP or POP3 (depending on the ISP configuration), a remote user can connect to the mail server and send and receive (or download) all messages locally. This enables the remote user to review and create messages while not connected to the Internet.

Even though all of these methods are implemented widely in industry, they may not be secured properly. Web mail, POP and IMAP protocols are available for clients to connect via browser or email application. Incorporating these protocols within the application module enables clients to interact with another system of the Internet in secure and non-secure channels. When email servers aren't properly secured, other threats such as spamming, phishing and email worms limit its usefulness. The other useful aspect of the application module is the open relay. Open relays allow anyone on the Internet to relay (or send) email through it. Opening the application module up for potential abuse shows the potential damage that can result from such a configuration.

As depicted in figure 6, a DNS query is sent across the Internet to look up the MX (or mail) record for b.org. This presents a problem much like that of the web request mentioned earlier. The solution is to further modify the same custom DNS server to handle MX records. With this modification, a query is sent to the DNS server and then it responds with the IP address of the application module diverting steps 2 and 3 to be handled internally.

Room For Expansion

The application module can also be used to implement other software modules to offer their respective services as well as their vulnerabilities. Such software modules may include a Structured Query Language (SQL) database to play Injection attacks, backup applications to compromised transferred information, or Internet Information Server (IIS) to take advantage of an existing vulnerability.

Protocol

When dealing with the Internet, a protocol is an established way to transfer information between computers. Many protocols are used over the Internet to provide different services via applications. Samba (SMB) and File Transfer Protocol (FTP) are common application protocols that allow for the transfer of files from one computer to another, TCP/IP (Transmission Control Protocol/Internet Protocol) is the basis for many other standard Internet protocols.

Application protocols that the core module utilizes are Hypertext Transport Protocol (HTTP) for web, DNS for name to IP resolution, and DHCP for IP address assignment. Additionally, the application module uses IMAP, POP3 and telnet for sending and receiving email messages, as well as HTTP/S for the web interface. The monitor module handles the display mechanism by HTTP.

Other protocols that don't fit into the other modules are implemented here. These protocols include Secure Shell (SSH), FTP, Gnutella, and others. The main goals for this module are to inherit the remainder of the Internet communication, and provide actual sub systems that clients can interact with. These protocols will point to a common repository of documents, images, and large data sets.

Monitor

The Internet is quickly developing into a common-ground of information gathering, communication, and entertainment. Access to the Internet grows critical for engineering, research, and all sorts of collaborative activities. One problem persists; the visualization of communication and information. This module helps clients understand, from a visual aspect, what is happening within ISECUBE.

The monitor module consists of a listener (tcpdump), parser, storage (MySQL), and a display component (web). By combining these four components, all communication is collected, sorted, stored, and then displayed in a graphical user interface (see figure 7). The purpose is to show protocol, user, and overall Internet statistics that can be referenced and understood with ease.

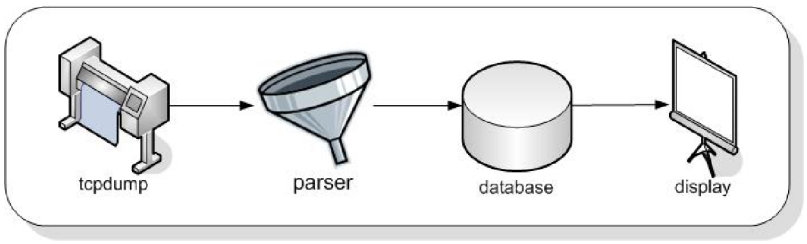

Figure 7. Component Interactions

TCPDump

The listener component consists of tcpdump which listens to all traffic in promiscuous mode. Tcpdump is a powerful tool that enables the running host to intercept and display packets being transmitting over the network to which it's connected. Tcpdump enables the host to precisely see all the traffic. As information is collected, it's then passed on to the parser component.

Parser

Parsing is the process of analyzing an input in order to determine its structure. Once established, statistics can be taken from the structure and stored for later retrieval. A custom parser was written to analyze every packet, extract statistical data such as source IP, destination IP, packet type, etc and finally send it to the storage component.

Database

MySQL is used as the storage component that acts as a library of Internet statistics and is addressable by the display component. Clients can view different datasets using the display component. Statistic interfaces that are available include: per client and overall system levels. The following are a few of the statistics that can be collected at the client level and is represented via a graph/chart:

Throughput (line)	Lookups (bar)	Utilization (line)
Overall packet count (bar)	Per protocol (pie)	Protocol packet count (table)
Packet size distribution (pie)		

Table 2. Client Statistics Chart Types

The following are a few of the statistics that can be collected at the system level and is represented against all clients via a graph/chart:

Protocol usage (pie)	Protocol count (table)	Utilization (line)
Packet count (bar)	Packet size distribution (pie)	

Table 3. Network Statistics Chart Type

Mapper

The mapper is a unique module that doesn't communicate with any other module when ISECUBE is configured to act as a virtual/physical Internet. By configuring ISECUBE to connect to ISEAGE, the mapper module becomes the primary link between ISECUBE and ISEAGE. The mapper network is where boards receive their boot directives to boot into a separate operating system and run an instance of the mapper software. Once the boards have loaded their operating system via PXE (eth2), the spanning network becomes the inter-board communication backbone. Additionally, each board has an Ethernet interface to transfer data to other boards via the communication backbone (eth1) as well as interface to the virtual/physical network (eth0). Figure 8 shows ISECUBE in ISEAGE configuration.

The mapper software is capable of recreating up to 50 routers. Each router on a board has a unique ID with ID 0 given to the router that connects to the eth0 interface. The mapper software is configured by a binary configuration file that can be created from a text file or as an output from other programs [30].

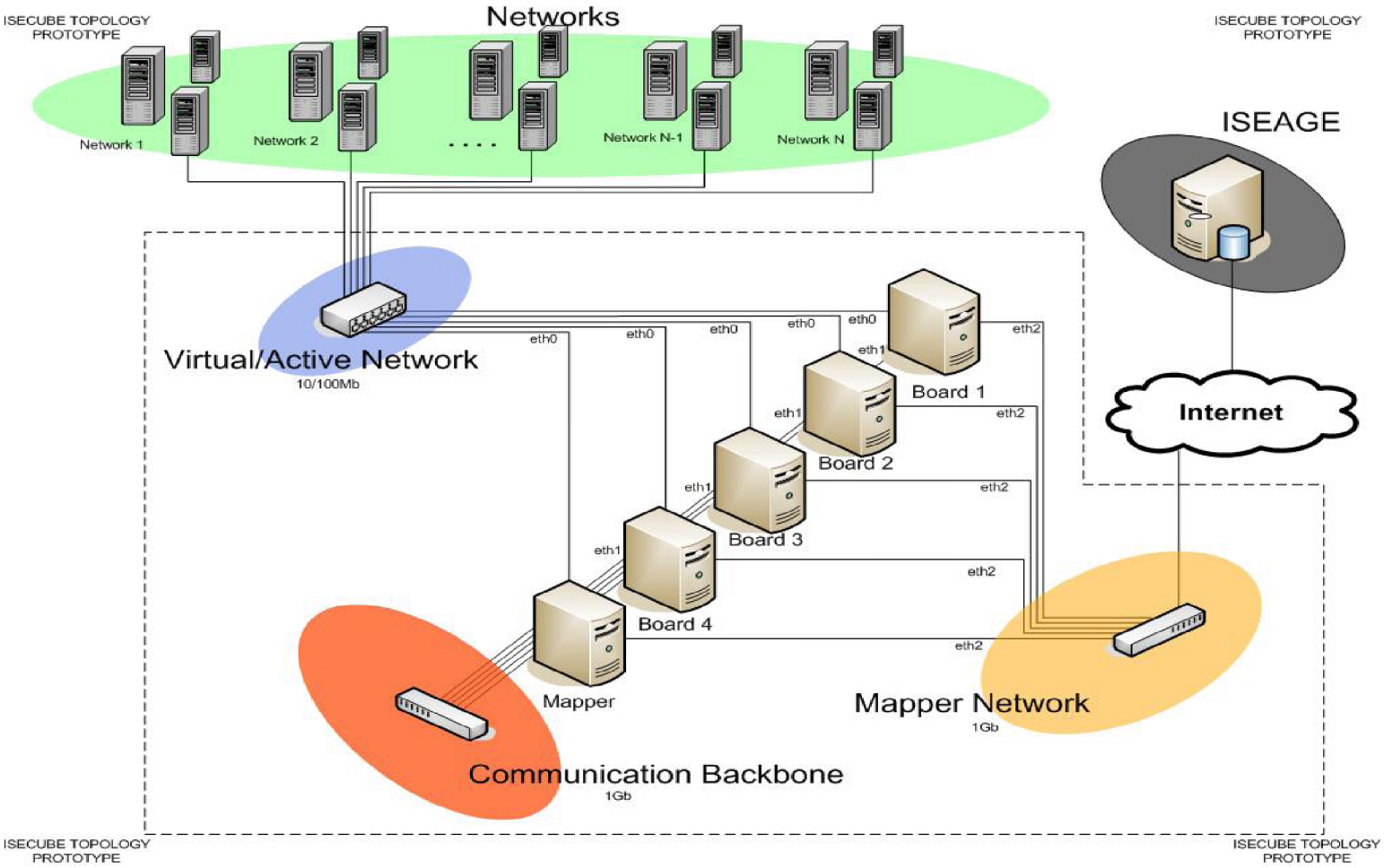

Figure 8. ISECUBE Configuration

CHAPTER 6. FUTURE WORK

Even though the underlining structure of ISECUBE is in place and functional, there are areas to improve upon to order to achieve better functionality, realism, and effectiveness. The following is a description of existing limitations identified as possible areas for future work.

DHCP

While ISECUBE has been developed to assign class C IP addresses to attached devices, a custom application needs to be written to assign completely random IP addresses to clients instead of using a traditional DHCP server. This improvement will give each client a sense of being truly unique. This will make exercises more challenging, for discovery purposes, instead of all clients being within the same subnet.

Web Server

Currently, when ISECUBE is configured to be an isolated environment and a client visits a website, general packet level and client identifiable information is displayed along with name of the visited website. To enhance this experience, a random webpage layout generator needs to be in place to give a sense of webpage uniqueness. This information also needs to be cached in a way that if accessed again, the same layout/information is presented again. In addition, hyperlinks to other web address also need to present in the randomly generated pages.

Redirector

The current state of the redirector only redirects HTTP (or web) traffic. Other protocols need to be incorporated such as FTP, SAMBA, SSH, etc. Upon execution, these requests will be directed to the protocol module which already offers these services. This will continue the illusion that the traffic was sent from the originating website (i.e.: yahoo.com, msn.com) instead of the same IP address for every request. The only limitation that will exist is that the contents that are housed within a service (FTP, SAMBA, SSH) will be the same.

Mapper

Even though the mapper as a module that is complete, the current interface to access the configuration consists of a text editor and needs to be improved upon. The proposed enhancement for the module is to create a web interface and integrate it into the administration access control.

CHAPTER 7. CONCLUSION

The goal of ISECUBE is to provide a highly configurable and portable environment that meets the challenges of traditional research, training, and teaching methods. Currently ISECUBE provides many environments; these primarily consist of a fully isolated authentic Internet environment, an active network, and an ISEAGE extension network. ISECUBE's functionality extends well beyond the local features, additionally providing remote access to advanced tools housed within ISEAGE.

In the past, extensive teaching and training was made possible by sending personnel to costly training sessions to receive such information. This thesis has described a portable device and methods to help decrease this associated while increasing the efficiency and availability such information.

There are a number of scenarios that can benefit from the usage of ISECUBE, which in turn will ultimately enhance the overall level of security through these three key areas.

BIBLIOGRAPHY

[1] Behrouz Forouzan. (2003). TCP/IP Protocol Suite, Second Edition. New York: McGraw-Hill Higher Education. Page 749.

[2] Internet Security Threat Report. (2006). On-line. Available: http://www.symantec.com/about/news/release/article.jsp?prid=20060925_02 (Date Accessed: 28 September 2006).

[3] "VMware: Virtualization, Virtual Machine & Server." 28 September 2006. <http://www.vmware.com/>.

[4] "Microsoft Virtual PC 2004." 28 September 2006. <http://www.microsoft.com/windows/virtualpc/default.mspx>.

[5] Jacobson, Doug. (2005). ISEAGE: Implementation Plan. 9. http://www.iac.iastate.edu/iseage/implementation_plan.pdf

[6] Butler, Timothy R. "Bochs: The Open Source IA-32 Emulation Project." sourceforge.net. 28 September 2006. <http://bochs.sourceforge.net/>.

[7] Hoffman, L.J., Rosenberg, T., Willmore, S., Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society 18-20 June 2003 Page(s): 217 – 220.

[8] Jacobson, Doug. "ISEAGE: Internet Scale Event and Attack Generation Environment." (2005): 12.

[9] Hahn, Adam (2006) Advanced Packet Obfuscation and Control program (Apoc). Masters thesis, Iowa State University.

[10] Myers, Brett (2004) The design and development of SNIP: Simple Network Imitator Program. Masters thesis, Iowa State University.

[11] "Wireshark: Network Protocol Analyzer." 28 September 2006. <http://www.wireshark.org/>.

[12] "Transport Layer Security - Wikipedia." 28 September 2006. <http://en.wikipedia.org/wiki/Secure_Sockets_Layer>.

[13] "Cyber Attacks Increasingly Target Home Users." 25 September 2006. 28 September 2006. http://www.symantec.com/about/news/release/article.jsp?prid=20060925_02>.

[14] "Security: IT Locks Down." 1 January 2002. 28 September 2006. <http://www.symantec.com/about/news/release/article.jsp?prid=20060925_02>.

[15] Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course Conklin, A.; System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on Volume 9, 04-07 Jan. 2006 Page(s):220b - 220b.

[16] Tavani, H (2004), "Ethics & Technology" P.169.

[17] Pilson, C, Presentation on Computer Security and Forensics, February 2005.

[18] "The Ten Commandments of Computer Ethics". Computer Ethics Institute, 1992. http://www.brook.edu/its/cei/overview/Ten_Commanments_of_Computer_Ethics.htm (Date Accessed: 28 September 2006).

[19] Schultz, Robert A. _Contemporary Issues in Ethics and Information Technology_. Hershey, PA: IRM Press, 2006.

[20] "Email - Wikipedia." 28 September 2006. <http://en.wikipedia.org/wiki/Email>.

[21] "Domain Name System - Wikipedia." 28 September 2006. <http://en.wikipedia.org/wiki/Domain_name_system>.

[22] "Proxy Server - Wikipedia." 28 September 2006.

<http://en.wikipedia.org/wiki/Domain_name_system>.

[23] "Linkbyte: Internet Sharing/Proxy Server Solution." 28 September 2006. <http://www.linkbyte.com/>.

[24] "WinProxy Security." 28 September 2006. <http://www.winproxy.com/>.

[25] "Squid Web Proxy Cache." 28 September 2006. <http://www.squid-cache.org/>.

[26] "Squirm - A redirector for Squid." 28 September 2006. <http://squirm.foote.com.au/>.

[27] "Jesred - A redirector for Squid." 28 September 2006. <http://www.linofee.org/~jel/webtools/jesred/>.

[28] "Ultra fast free filter/redirector/access for Squid." 28 September 2006. <http://www.squidguard.org/>.

[29] "Internet Activities." 19 July 2006. www.pewinternet.org. 28 September 2006. <http://www.pewinternet.org/trends/Internet_Activities_7.19.06.htm>.

[30] Jacobson, Doug. Internal ISEAGE Technical Report. 2004

ACKNOWLEDGEMENTS

I would like to take this opportunity to express my thanks to those who helped me with various aspects of conducting research and the writing of this thesis. First and foremost, Dr. Doug Jacobson for his guidance, patience, funding and support throughout the research, the writing of this thesis and the trails and errors during implementation. Secondly, I'd like to thank my fellow colleagues for listening and for their suggestions. Lastly, I'd like to thank my family for their support and words of encouragement over the last couple of years.