EVALUATION OF THE UNITED STATES COAST GUARD'S REMOTE NETWORK ACCESS PROCEDURES

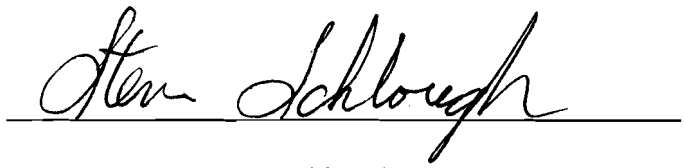
by

Craig Olesnevich

A Research Paper
Submitted in Partial Fulfillment of the
Requirements for the
Master of Science Degree
In

Management Technology

Approved: 2 Semester Credits



Steve Schlough
Research Advisor

The Graduate School

University of Wisconsin-Stout

December, 2005

The Graduate School
University of Wisconsin Stout
Menomonie, WI 54751

Author: Olesnevich, Craig T.

Title: *Evaluation of the United States Cost Guards Remote Access Procedures*

Graduate Degree/ Major: MS Management Technology

Research Adviser: Steve Schlough

Month/ Year: December, 2005

Number of Pages: 42

Style Manual Used: American Psychological Association, 5th edition

ABSTRACT

Advances in high performance technologies and improvements to information security have increased the popularity of telecommuting and remote access programs. The Commandant of the United States Coast Guard (USCG) supports the use of remote access solutions, as a way to harness new technologies and provide the workforce with the flexibility needed to meet the service requirements while also obtaining national goals (COMMANDANT INSTRUCTION 12630.1). The Coast Guard's effort to capture the benefits of new technology amplified the pressure to ensure a safe and secure way to obtain remote access to their data network. The remote user ranges from the day extenders who only need access to e-mail, to the travelers and full time telecommuters who need access to the systems core applications. The Coast Guard Telecommuting Program provides a flexible work environment to the end user, solving transportation problems, improving employee productivity and efficiency, resulting in an overall improvement to the quality of work life. However, risks are inherent with any technology

that provides outside access to an otherwise secure network. Some of the risks are the same when accessing a Local Area Network (LAN), some risks are increased by the use of remote access technology, and some risks are new. The most significant risk in allowing remote access to a network is that unauthorized users may gain access to an agencies systems and information. The biggest challenge for the Coast Guard is to protect against malicious attacks without making it difficult for the remote users to access the Coast Guard Data Network (CGDN).

The purpose of this study is to identify an acceptable process to ensure secure remote access to the CGDN. The objectives are to collect data on new user strong authentication technologies and evaluate them against the Coast Guard's established procedures.

TABLE OF CONTENTS

Chapter I

Research Problem and Objectives

Introduction

The United States Coast Guard is a military, multimission, maritime service. Its mission is to protect the public, the environment, and US economic interest. The Coast Guard has developed a modern digital communications network and integrated computer technology into its daily routine to provide its members with the tools necessary to better complete this mission. The CGDN provides all members access to vital information necessary to affectively complete their assignments as well as improving efficiencies and increasing productivity.

The Coast Guard has over 500 locations with approximately 30,000 to 40,000 users. According to the Telecommunication Systems Director for the United States Coast Guard in fiscal year 2005 8000 of those users were able to remotely connect to the CGDN. The Remote Access Solution provides these remote users with access to the menu items that would be available to them if they were directly connected to the network. There are significant risks involved with running a remote access system of this size and every effort must be made to prevent unauthorized access and to avoid malicious attacks.

Problem Statement

The purpose of this study is to evaluate the Coast Guard's remote network access procedures and identify if any new strong authentication technologies can feasibly be implemented to increase security.

Research Objectives

This study is meant to identify an acceptable process to ensure secure remote access to the CGDN.

The objectives are to:

1. Evaluate the Coast Guard's current remote access procedures.
2. Collect data on new user strong authentication technologies
3. Compare the current remote access procedures to the new strong authentication technologies.
4. Determine if any changes should be made to the remote access procedures.
5. Determine if any changes can be justified by the increase in security added to the remote access procedure.

Significance of the Study

The Coast Guard is determined to keep pace with technology, capturing the benefits and efficiencies, providing its workforce with the tools necessary to meet the changing demands of the work environment. Remote access technologies allow members to work from home or to connect into the data network from anywhere while on the road, reducing stress of commuting, increasing productivity by allowing employees to work any time day or night without interruptions, and cutting cost by reducing office space requirements (Kasacavage, 2002). Employees remain productive and are able to react to the ever changing environment on a moments notice. The use of computers has not only improved the quality of work but allows the user to complete more tasks in less time. By allowing users remote access to the data network, the Coast Guard has extended the workday for some and for others utilized productivity hours that were lost due to required travel. Providing members with remote access has become essential to mission success.

Network security has become a positive infrastructure element and is essential to the safe operation of any information system. The benefits obtained from remote access could be negated by one malicious attack. On July 8th, 1997 the Coast Guard sustained a malicious attack on a personnel data base which cost $40,000 to recover from and 1800 hours to restore the lost data (Didio, 1998). The hacker was able to gain access to the network by using the password of an unsuspecting end user. Traditional fixed passwords represent a serious, growing vulnerability for many organizations because they can be stolen and used repeatedly. Three-factor authentication is far more secure than traditional passwords because it requires the use of a personal identification number (PIN), a hardware device, and in some cases a form of biometric, to generate a unique one-time-only pass code. Strong authentication will be imperative to the success of this research and to protecting the classified information stored on the CGDN.

Limitations

The limitations of this study are:

1. The results of this study are limited to the United States Coast Guard.
2. The new strong authentication technologies were evaluated only to United States Coast Guard's data network and more specifically to the configurations of that network and how that network handles remote user access.
3. The existing USCG network was not audited and no network traffic or applications were analyzed.
4. No Prototype Networks or Pilot Networks were designed or tested regarding new technologies; all recommendations were limited by cost of implementation and ownership, ease of use, and security.

5. No actual hands on testing was completed, the results of the paper rely exclusively on the information published by industry professionals.

Assumptions

The assumptions of this study are:

1. The United States Coast Guard remote access procedures currently work as per their published specifications.

Definitions

Analog Dial-up connection – Computers, which handle data in digital form, require modems to turn signals from digital to analog before transmitting those signals over communication lines such as telephone lines that carry only analog signals. The signals are turned back into digital form (demodulated) at the receiving end so that the computer can process the data in its digital format (Webopedia.com, 2005).

Authentication – The process of identifying an individual usually based on a username and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual (Webopedia.com, 2005).

Bandwidth – The amount of data that can be transmitted in a fixed amount of time. For digital devices, the bandwidth is usually expressed in bits per second (bps) or bytes per second. For analog devices, the bandwidth is expressed in cycles per second, or Hertz (Hz) (Webopedia.com, 2005).

Callback Control Protocol (CBCP) – Allows the server to negotiate with the client to call the client back to establish the connection (Windows 2000 Remote Access Website, 2005).

Challenge Handshake Authentication Protocol (CHAP) – a type of authentication in which the authentication agent (typically a network server) sends the client program a random value that is used only once and an ID value. Both the sender and peer share a predefined secret. The peer concatenates the random value (or nonce), the ID and the secret and calculates a one-way hash using MD5. The hash value is sent to the authenticator, which in turn builds that same string on its side, calculates the MD5 sum itself and compares the result with the value received from the peer. If the values match, the peer is authenticated (Webopedia.com, 2005).

Circuit-Switched Connections – A WAN-switching method, in which a dedicated physical circuit through a carrier network is established, maintained, and terminated for each communication session (Paquet, 1999)

Dedicated Connections – Also know as leased line, the established path is permanent and fixed for each remote network that is reached through the carrier facilities (Paquet, 1999).

Digital Subscriber Line (DSL) – DSL technologies use sophisticated modulation schemes to pack data onto copper wires. They are sometimes referred to as last-mile technologies because they are used only for connections from a telephone switching station to a home or office, not between switching stations (webopedia.com, 2005).

Frame Relay – A packet-switching protocol for connecting devices on a Wide Area Network (WAN). Frame Relay networks in the U.S. support data transfer rates at T-

1 (1.544 Mbps) and T-3 (45 Mbps) speeds. In fact, you can think of Frame Relay as a way of utilizing existing T-1 and T-3 lines owned by a service provider (Webopedia.com, 2005).

Integrated Service Digital Network (ISDN) Connections – Are circuit-switched connection that provides WAN access when needed, rather than requiring a dedicated link and offers increased bandwidth over a typical dial-up connection (Paquet, 1999).

Modem – Coverts digital signals to analog, and vice versa (Paquet, 1999)

Plain Old Telephone Service (POTS) – Regular phone lines (Paquet, 1999).

Password Authentication Protocol (PAP) – the most basic form of authentication, in which a user's name and password are transmitted over a network and compared to a table of name-password pairs (Webopedia.com, 2005).

Packet-Switched Connection – A WAN-switching method, in which network devises share a single point-to-point link to transport packets from a source to a destination across a carrier network (Paquet, 1999).

Point-to-Point Link (PPP) – Encapsulation used for asynchronous serial, ISDN, and synchronous serial types of connections. PPP supports vendor interoperability (Paquet, 1999)

Remote Access Service - A feature built into Windows NT that enables users to log into an NT-based LAN using a modem, X.25 connection or WAN link. RAS works with several major network protocols, including TCP/IP, IPX, and Netbeui (Webopedia.com, 2005).

Topology - The shape of a local-area network (LAN) or other communications system. Topologies are either physical or logical (Webopedia.com, 2005).

Virtual Private Networks (VPN) – a network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted (Webopedia.com, 2005).

Wide Area Network (WAN) – A data communication network covering a relatively broad geographic area, used to connect various sites at different geographic regions.

X.25 – Encapsulation typically seen in a packet-switched environment and has built in reliability (Paquet, 1999).

Chapter II

Review of Literature

Introduction

The Evaluation of the United States Coast Guard's existing remote access procedures will be a benchmark to compare against new strong authentication technologies and alternate telecommunication procedures. This study is intended to identify if there is any value added by changing the United States Coast Guard's existing remote access procedures to incorporate new technologies. The driving factors for this study will be security, usability, and cost, resulting in a system that balances between the protection of data and ease of use, while also minimizing operating and ownership costs.

Remote Access Technology

Today communication technology offers more options for sending and receiving data than ever before. Using a computer workstation an employee can access an internet provider, enter a network using one topology and utilize a public or private system on a second topology to remotely access their home network running on an entirely different topology (ksaa, 1997). The added flexibility of interconnecting multiple different topologies has opened the door to a range of network access possibilities, and provides a company the ability to better utilize their workforce, i.e. implementing telecommuting solutions.

There are several remote access technologies available today. The most popular are terminal servers, remote control, remote node, internet-base access, and a combination of these methods (Kasacavage, 2002). Each of these methods is a little different and has characteristics that are more conducive to certain functions. Terminal

servers are used when the remote clients need to access multi-user systems. The remote control process allows a user to take control of a host computer on a corporate network via a slow-speed analog modem connection (ksaa, 1997). Remote node technology allows the remote workstation access the corporate network and allows the remote user to act as real node on the network through a varity of connection options. Internet-base remote access provides the remote user access to the corporate network via the internet by using an outside internet service provider (ISP) connection. Each of these technologies will be reviewed in more detail in the following sections.

A terminal server is a device that is connected to the Local Area Network (LAN) and has multiple serial ports, used to provide remote user's access to the LAN (Kasacavage, 2002). The terminal server uses a process called modem pool to allow many users to access the LAN at the same time; typically with a user to port ratio is 10:1 (Nedeltchev, 2003). Security is a big concern when using this technology because the server is connected to the data network as well as to the outside world, strong authentication is required (Kasacavage, 2002).

Remote control users dial up the host using remote control application software, then take over the screen and keyboard of a host computer on the network (ksaa, 1997). One host computer must be made available for each remote user wishing to connect to the corporate network. All applications launched by the remote user run on the host computer, not on the remote one. The disadvantages to this technology are that it is very slow; difficult to manage, not suited for graphic-intensive applications making it extremely difficult to copy and manage files (Kasacavage, 2002). Remote control offers little in way of security, relying on simple password schemes for protection. Because of

these limitations and extra hardware requirements, today remote access is only used for troubleshooting or as a training tool.

Faster connection speeds and advances in software have championed remote node technology to the favored method on connecting remote users. The remote user can run their network protocol stack on their workstation allowing the user the ability to complete most tasks as if they were at their office computer (ksaa, 1997). Due to the fact that remote node does not require a dedicated host computer resource, it increases the number of possible simultaneous connections, limited only by the number of modems installed. Users may dial into the network using a number of different technologies offering much faster data transfer options and more secure connections through the use of existing network password schemes coupled with third-party security tools. Remote node supports many platforms, extending the existing network, providing access to all network resources, and is more widely used by industry today (Kasacavage, 2002).

The internet provides the remote user with the ability to log in from anywhere and gain access to the corporate network (Kasacavage, 2002). The remote user can connect using an analog dial up connection, digital subscriber line, cable modem, or a wireless connection, providing greater flexibility and faster connection speeds (Sudhir, 1999). The demand for high-speed data access keeps growing and network designers continue to utilize emerging technologies to create greater flexibility and performance. Internet-based access is vulnerable and requires increase security to reduce the risk of compromised data.

The integrated solution combines aspects of all three methods terminal servers, remote control, remote node, and internet-based access. By using multiple technologies

you can run some of your applications locally and others on the client's computer (Kasacavage, 2002). This process combines multiple technologies into one interface which provides access to the entire network and is well suited for companies that have multiple servers. An Integrated system is not easy to set up and comes with the same security issues as using the terminal server, but is much easier to manage once it is up and running.

Connectivity Options

Last Mile

The last mile of a connection describes how the remote user connects to the companies services (Robichaux, 1999). There are four major connection types, which are analog modems, integrated services digital network (ISDN), asymmetric digital subscriber line (ADSL) virtual private networks (VPN), and cable. A company may decide to use one or more of these connection types depending on where the user intends to connect from and what type of transfer speeds will be required.

Dial-Up Remote Access Connections (using an analog modem)

Of all the remote access connection types, dial-up remote access is the easiest to set up, but is more difficult to remotely manage. Almost every computer has an installed modem which is compatible with any standard phone line, providing the remote user a wide range of flexibility in locating a connection source. Two notable facts about the V.90 modem (the universal modem) are that the up-stream data rate is slower than the down-stream data rate and a digital trunk line to the telephone companies central office is required to provide dial up service (Robichaux, 1999).

Integrated Services Digital Network (ISDN)

ISDN is designed to use the existing telephone lines to offer voice and data services to a home or office (Robichaux, 1999). The basic rate interface offers three digital channels for transferring data. ISDN services have been expanded to all metropolitan areas as well as most small communities.

Asymmetric Digital Subscriber Line (ADSL)

ADSL provides digital service over analog phone lines (Robichaux, 1999). Like dial-up (analog modem) technology ADSL has two different transfer rates, but with the ADSL it is at a much faster speed, designed to transfer compressed video. ADSL is a point-to-point switched technology, operating at the physical layer used to support higher level protocol stacks (Dixit, 1999). The use of ADSL is a cost effective way to set up a company's network backbone.

Virtual Private Networks

Virtual Private Networks (VPN) transfer private data over public networks (Nedeltchev, 2003). Service provider VPN's provide the remote user the same policies that are deployed on private networks over a shared infrastructure. The use of VPN's to supplement existing networks has become increasing popular due to the substantial increase in cost savings (Kasacavage, 2003). The remote user can connect to a private network by using a service called Remote Access to Multiprotocol Label Switching Virtual Private Network (RA to MPLS VPN). This service enables users to connect through a dial up connection, ISDN, DSL, cable, or wireless technologies (Nedeltchev, 2003). The additional access methods provided by RA to MPLS VPN enables the service provider to offer extended end to end services to its customers. The remote user can access the VPN via a high speed internet connection gaining access to the corporate

network maintaining the high data transfer speeds. This technology not only offers better efficiencies, but is also a low cost remote access solution. VPN's offer both cost savings and security, low cost access for users and protection of the link between two points (Kasacavage, 2003).

Cable

The delivery of data services over a cable network is completed by using a modulator/demodulator (cable modem) to convert data form digital to analog and then transferring it over the existing coax cable lines (Nedeltchev, 2003). These lines offer a wide bandwidth capable of performing full-duplex communications, and analog voice services as well. Cable technology is a shared medium, the transfer speeds are directly related at the demand on the line at the time and is considered its biggest disadvantage.

Local Loop

The local loop is the connection between the telephone companies central office to the lines in the scribers office (webopedia.com, 2005). The term local loop not only carries telephone services, but now carries ISDN and DSL technologies as well. There are three types of WAN connection types that function on the local loop, which are dedicated connectivity (leased lines), circuit-switched networks, and packet-switched networks (Paquet, 1999).

Dedicated connectivity (leased lines)

Leased lines offer a single, pre-established point-to-point WAN connection and should be considered when more than 15-30 users at same time (ksaa, 1997). This option provides a dedicated path from the customer, through the carrier to the remote network (Paquet, 1999). The dedicated lines are reserved for the company for the entire time of

the agreement. The company has a high level of control over the leased lines and is afforded very high speeds. These lines are used when a company needs long connection times over a short distance.

Circuit-switched networks

The circuit-switched networks use the same lines as the dedicated line method, only a dedicated physical circuit through the network is set up and terminated for each communication session (Paquet, 1999). These types of connections are asynchronous serial and ISDN. Asynchronous is the least expensive and uses the existing phone lines. The ISDN technology can increase bandwidth over a dial-up connection, but usually is configured to work over a T1 connection.

Packet-switched networks

A packet-switched network is a WAN-switching method that shares a single point-to-point connection of a carrier network (Paquet, 1999). The end to end connectivity is completed through the use of virtual circuits. This type of technology offers less control over the connection and the bandwidth is shared.

Security

Security is the number one concern when allowing remote access to a corporate network (Kara, 2001). The challenge is to protect your system without overcomplicating the user connection process (ksaa, 1997). Kasacavage (2003) stated that a secure remote access system will include the following:

- Reliable authentication of users and systems
- Easy-to-manage, granular control of access to particular computer system, files, and other network resources

- Protection of confidential data
- Logging and auditing of system utilization
- Transparent reproduction of the workplace environment
- Connectivity to a maximum number of remote users and locations
- Minimal costs for equipment, network connectivity, and support.

Kasacavage's list provides the fundamentals for designing a secure remote network access network. There is no one perfect solution for all networks and a designer must thoroughly review their company's network situation before implanting any remote access technology.

The use of simple passwords is no longer an acceptable solution for securing remote access to a corporate network. The use of strong authentication, encryption, and access control can greatly enhance the security levels of a remote access network. Strong authentication provides remote access networks an option to verify the identity of the connecting user prior to granting access to the network (Robichaux, 1999). Robichaux (1999) defined three major categories of authentication, something you know, something you have, or something you are. Based on one or more of these three categories the remote user can prove that they are who the say they are and gain access to the network. Access is not the only problem; the data is also vulnerable while transiting the connection from the remote user to the corporate network. The data should be encrypted before it is sent and decrypted when it is received on the other end. A unique key is used the sending and receiving units to correctly code and decode the information. By limiting who has access to the network can greatly reduce the probably of sustaining an attack.

Authentication

The simplest means of limiting access to a network is by using a Password Authentication Protocol (PAP) (Robichaux, 1999). This process requires the user to submit a password that is then authenticated by a remote access server in order to be permitted access. The passwords are sent to the server in clear text with no encryption, making it easy for hackers to learn the passwords. This type of authentication should only be used as a last resort, when no other protocols are available.

The Challenge-Handshake Authentication Protocol (CHAP) requires password authentication prior to gaining access (ksaa, 1997). Unlike PAP, CHAP uses a challenge response mechanism which authenticates the user to the network. The server sends a challenge value to the client; the client encrypts the challenge value with their password and sends it back to the server. The server has both the encryption key and client's password so it will check the response to see if it is correct (Robichaux, 1999). The encryption key is only good for a short amount of time and then a new key must be generated, minimizing exposure to attacks.

Remote Authentication Dial-In User Service (RADIUS) is a protocol designed to perform user authentication for a number of systems or servers (Robichaux, 1999). Remote access servers use RADIUS servers to perform the authentication for request for service by remote users. The exchange between the remote user and RADIUS server is encrypted and when the user is verified the remote access server is notified weather to accept or deny access.

A client can use a token to gain remote access to a network. The token is a small physical device that generates a unique password which is synchronized with an

authentication server and is usually accompanied by a personal identification Number (PIN) (ksaa, 1997). The password is changed on a periodic basis and remains in sync with the authentication server; this process is called Time-Synchronous Authentication Scheme. Token access is a challenge and response exchange requiring the client to respond to the challenge, enter a password or pin in addition to the token generated password. The responses are verified by an authentication server prior to gaining access to the network.

United States Coast Guard Remote Access Solution

The United States Coast Guard employs a diversified workforce of remote access users, ranging from telecommuting, business traveler, remote office connections, to the after hour access. There are four different connection options for the USCG remote access clients. The first option is for the client to dial into the RAS system directly using a one eight hundred number (see Appendix A for more details). The second option is for the client to use a dial up modem to connect to their ISP and then use the ExtraNet Client to gain access to the CGDN. The third option is for the client to use a cable modem and their ISP to connect to the internet and then use the ExtraNet Client to gain access to the CGDN. The final options for remote access client connection is to use DSL services to access an ISP and then use the ExtraNet Client to connect the CGDN. This wide range of connection options affords the client the ability to access the CGDN from almost anywhere in the United States or world.

The United States Coast Guard Remote Access Solution contains 10 PRI T1 lines which can handle 230 concurrent connections with the availability of expanding 46 more connections (2 additional PRI T1 connections) in the Alameda office. The remote

connections are split into two separate offices one in Alameda CA and the other in Martinsburg WV. If the client is attempting access from the West and has a West Coast area code the call will be routed to Alameda office, but if the call has an East coast area code and originates from the East, the call is routed to the OSC Martinsburg office (see Appendix A for more details). This system evenly distributes the load between the two offices.

The USCG RAS supports the use of Windows 95, 98, WIN NT, and XP and uses TCP/IP protocol suite to connect their computers to the internet in the form of dial up networking. The IP address to the USCG DNS server, which maps host alphanumeric names into IP addresses, is statically entered on the client's computer during the initial setup. Windows Internet Naming Service (WINS) is used on the CG Windows NT Sever 4.0 to eliminate Broadcasts and maintain a dynamic database of name to IP address mappings. The location and management of this server gives the USCG better control over authentication and access process.

The United Sates Coast Guard utilizes Virtual Private Network (VPN) technology to provide its members with remote access to their Data Network. The VPN prevents unauthorized users from accessing data by using encryption to create a private tunnel through the Internet for the secure delivery of data. The tunneling protocol used is a Client-Initiated VPN, which requires the client to establish a PPP session, by using an Internet Service Provider to create a VPN connection with the VPN Server. The client starts this process by either dialing directly into the server via the one eight hundred number or by connecting to their ISP. After establishing a connection the client will use the ExtraNet client to dial up the ISP's local POP to establish a PPP session. The client

uses this connection to establish a VPN connection with the VPN server, enabling a connection the CGDN.

An ExtraNet switch is used at OSC Martinsburg to better manage the Remote Access traffic. The ExtraNet switch combines remote access protocols, security, authentication, authorization, and encryption technologies into one unit. The switch supports many secure protocols including IPSec, PPTP, and layer 2 Tunneling Protocol (Nortell Networks, 2001). A Quality of Service feature includes call administration and packet forwarding priorities and the switch can be configured to perform authentication against an external RADIUS server. . IPSec requires authentication through User Name and Password which is checked using a secure ID token authenticated to the switch and is protected by the Internet Security Association and Key Management Protocol. Additionally the user is authenticated through the RADIUS server with a Group Name and Password. The transmitted information is protected using the IPSec Protocol Suite, encapsulating all of the information using an Encapsulated Security Pay load with triple Data Encryption standard (64 bit DES) and an Authentication Header with Message Authentication Code Secure Hash Algorithm. The switch can be configured to conduct secure key management and perform the challenge handshake authentication protocol. This is the first line of security protecting against unauthorized access for the CG Remote Access Solution.

The USCG is using a Windows NT4.0 server in combination with VacMan Security Suite to provide Token Authentication and RADIUS accounting for their Remote Access Solution. The Windows NT4.0 server is a multipurpose operating system that combines a wide range of network services (Microsoft, 2001). The server has a built

in Internet Authentication Service that authenticates dial-In users by using the RADIUS protocol. The VacMan Security suit adds an additional level of security by conducting Token Authentication. The security suite includes features such as dynamic user registration, auto token assign, and token grace period to automatically manage the 8000 remote users (VASCO, 2002). VacMan RADIUS middleware offers managers a single interface so that they have more control of the entire suite. They can issue tokens and handle strong authentication challenges. The VacMan Suite combined with the RADIUS Accounting provides a strong two factor authentication system.

Token authentication when used in conjunction with RADIUS Accounting can provide protection against unauthorized users gaining access to sensitive data files. Token based systems are more secure than passwords alone, but also become more complicated and harder to manage. The USCG remote access solution, the Vasco Data Security's VacMan/Server 3.0 was tested by Tere Parnell in 1999 and was found to be the best overall system tested that year, providing the most flexible security server, top management capabilities, and superb accounting functions (Parnell, 1999).

Parnell's test consisted of reproducing a typical enterprise network with eight Windows NT workstations, two Windows NT servers, two Sun Solaris workstations, and a Windows NT Workstation Access Server (Parnell, 1999). The vendor's security systems were installed and users were able to access the workstations two different ways, one by dialing in to the RAS and the other by gaining access using the internet. Two different type of routers were tested, firewall and virtual private Networks with all security software installed on one of the Windows NT server. The network was set up and then Parnell tried to break into each of the networks. Parnell (1999) rated system

from 1-10 in six categories manageability, OS integration, scalability, security, and time to authenticate (see Appendix B for more details). These scores were weighted and added to provide a total score. The VacMan suite received the highest score of 7.7, with the next closest score being a 7.45. These results prove that the VacMan suite is easy to manage, flexible, secure, as well as being the least expensive of all the tested security suites.

The USCG RAS is a combination of performance, accessibility, and security which provides the remote user with flexible, reliable user options. Emerging technologies and fiscal constraints demand that institutions continually strive to improve their business practices. In an effort to identify a more economical, but equally secure way of accessing the CGDN without inconveniencing the user, the remainder of this study will attempt to identify any new remote access technologies that meet this high standard established by the existing system.

Biometric Technology

Strong authentication or two factors of identification are become the standard in the computing industry (Chirillo, 2003). Biometrics is the process of automatically identifying an individual based on some characteristic that they possess (Bolle, 2004). Where passwords can be stolen or guessed, biometrics links authentication directly to the user (Hitchcock, 2003). A security system must be accurate and cost-effective in verifying or identifying a person's identity. People must physically posses something, a key or a passport, or know something, like a secret password, or use biometrics, appearances or characteristics that differentiate them from others to gain access to a secure system (Bolle, 2004). Biometrics separates two different modes of authenticating a user, verification and identification. Verification is an identifier that singles out a person

combined with that person's biometrics. Identification relies only on biometric measurements and checks those measurements to a pre-established data base (Bolle, 2004). The most commonly used physical biometrics identifies consist of fingerprint, facial recognition, hand geometry, iris scan, retinal scan, and vascular patterns.

The biometric recognition system is essentially a pattern recognition system that compares templates created during the enrollment process. Bolle (2004) identified the four basic design factors of a biometric system, which are system accuracy, computational speed, exception handling, and system cost. He also identified security and privacy as being very important when designing a biometric system. The end result when using the identification system is positive identification or negative identification and when using the verification system is either a positive enrollment or negative enrollment. Many forms of biometric authentication exist for the identification and verification of users, spanning a wide range of prices and error rates, requiring extensive review prior to selecting and implementing a biometric authentication process.

Biometric authentication systems suffer from two kinds of errors, false acceptance of imposters (False Accept Rate FAR), and false rejection of authorized users (False Reject Rate FRR) (Hitchcock, 2003). These false rates directly influence the cost of the project and must be addressed by balancing convenience versus security. The more convenient the system seems to the user the higher the FAR reducing the security level. When the system is less convenient to the user, returning a higher FRR it is more secure, but also more expensive to manage.

Hitchcock (2003) conducted testing on Biometric Authentication systems, dynamic signature verification system, thumbprint system, iris scan system, and voice

scan system. The Iris scan system had a high FRR of 16.1%, the thumbprint system suffered from an FAR of 12.9% when the impostor used a silicone copy of the user's thumbprint, the signature scan system's FAR was 50% for tracing, and poor results with the voice scan system scoring a FAR of 60% giving imposters a higher rate of success than did authorized users (Hitchcock, 2003). Hitchcock's study indicated that all four systems could identify authorized users, but none of them on their own possessed an acceptable FAR and FRR score, so Hitchcock was forced to develop a cascading system which incorporated multiple biometric systems in an effort to obtain an acceptable error rate (Hitchcock, 2003).

The cost for as biometric system would include the initial price for obtaining the hardware, setup and maintenance cost, the fees associated with managing the authentication, and user's time spent accessing the system. Hitchcock (2003) also identifies the need to maintain a separate authentication system for users who can not be enrolled in the biometric system. There is a cost associated with dealing with the authorized users who are falsely rejected when a system has a high FRR or if a person damages a finger print working with rocks over the weekend and then is falsely rejected access to the system Monday at work. The more secure the system must be, low FAR, combined with convenient to user, low FRR, the higher the accrued costs.

Summary

Remote access networking spans a wide range of networking technologies and protocols to provide the remote user access to the corporate network. The United States Coast Guard is currently using VPN technology with VacMan token security suite to allow remote users access to their data network. The VacMan security package rated the

highest among all tested suites in 1999, while also being the most affordable. Biometric authentication eliminates need for hard passwords, by using person's individual characteristics to verify and identify their identity. A biometric system can be configured to be very strict, only allowing exact matches access to the network, or very lenient, allowing an acceptable error rate. The more lenient the system the less secure it is and the more it costs to run due to the fact that the administrator must manually conduct the authentication process. Employing multiple biometric systems will reduce the error rates to an acceptable level, but at the cost of user convince. Although Standalone Biometric Solutions offer many benefits, strict security evaluations must be completed prior to implementing them in publicly accessible or physical-access arenas. The biometric remote access solution will be compared and evaluated against the current USCG RAS to determine if there is a more secure, user friendly, cost effective way of accessing the CGDN.

Chapter III

Research Methods

Introduction

The United States Coast Guard's Remote Access Solutions provides approved users access to the CGDN from their home or while on the road. At the time of this study the United States Coast Guard managed 8000 remote access tokens with over 4000 of them being used on a regular basis. The purpose of this study is to evaluate the United States Coast Guard's remote access procedures and create a benchmark to be compared against emerging technologies.

Research Design

The methodology of this study is historically based and designed to compare Biometric Remote Access Solutions against the United States Coast Guard's existing procedures. The information was collected using extensive research in numerous areas; network evaluation, published training material, and high level testing recorded in published thesis. The research provided ample information to successfully conduct a comparative analysis. A decision support software application Expert Choice 11 was used to structure the decision making approach. Expert Choice 11 is based on analytic hierarchy process; more specifically it is a mathematical model that controls decision-making methodologies. This software package assisted in structuring the decision into objectives and alternatives, allowed for measuring the objectives and alternatives using pairwise comparisons, provided documentation, and conducted final sensitivity analysis. The use of Expert Choice 11 provided a seamless transition of research data into specific decision making criteria resulting in an organized more justifiable decision.

Population

The population for this study consists of the United States Coast Guard's existing Remote Access System using VPN technology coupled with VacMan Token Security suite. The United States Coast Guard's Remote Access procedures were carefully documented by reviewing existing information provided by the Telecommunication Systems Director for the United States Coast Guard. The Biometric Solutions chosen for this study were of the industry leaders, and also as a result of David Hitchcock's extensive biometric testing conducted at the University of Florida in 2003. Biometric Remote Access Solutions consist of Fingerprint System, Iris Scan System, Voice Scan System, and Dynamic Signature Verification System. Hitchcock's (2003) test results for the selected biometric systems provided a standard comparison criterion which can then be further evaluated against the USCG existing access procedures. The remote access procedures will be compared on four major categories with their respective subcategories:

Goal: Select The Best Remote Network Access Procedures For The United States Coast Guard

1. Security: Protection of information assets through the use of technology (L: .483)
1.1. Flexibility (L: .143)
1.2. Management (L: .286)
1.3. Identification and Authentication (L: .571)

2. Reliability: Remote Access Solution that is efficient and dependable (L: .088)
2.1. Connection Speed (L: .333)
2.2. Error Rate (L: .667)

3. Usability: Remote Access Solution that is not over complicated (L: .157)
3.1. Equipment (L: .667)
3.2. Procedures (L: .333)

4. Cost: Total spent on goods and services (L: .272)
4.1. Equipment Procurement (L: .667)
4.2. Ownership (L: .333)

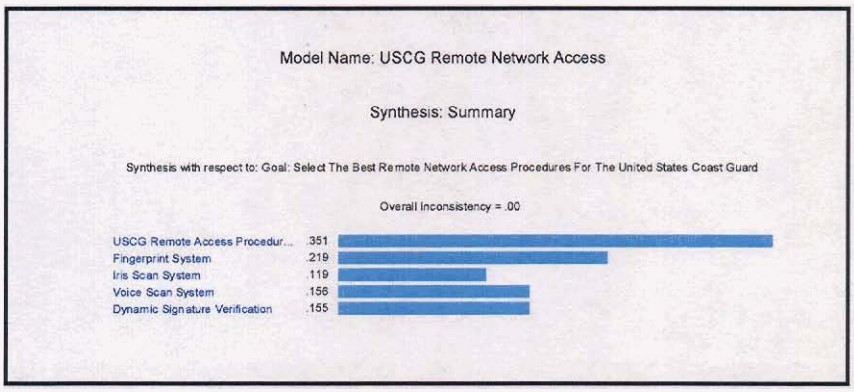
Chapter IV

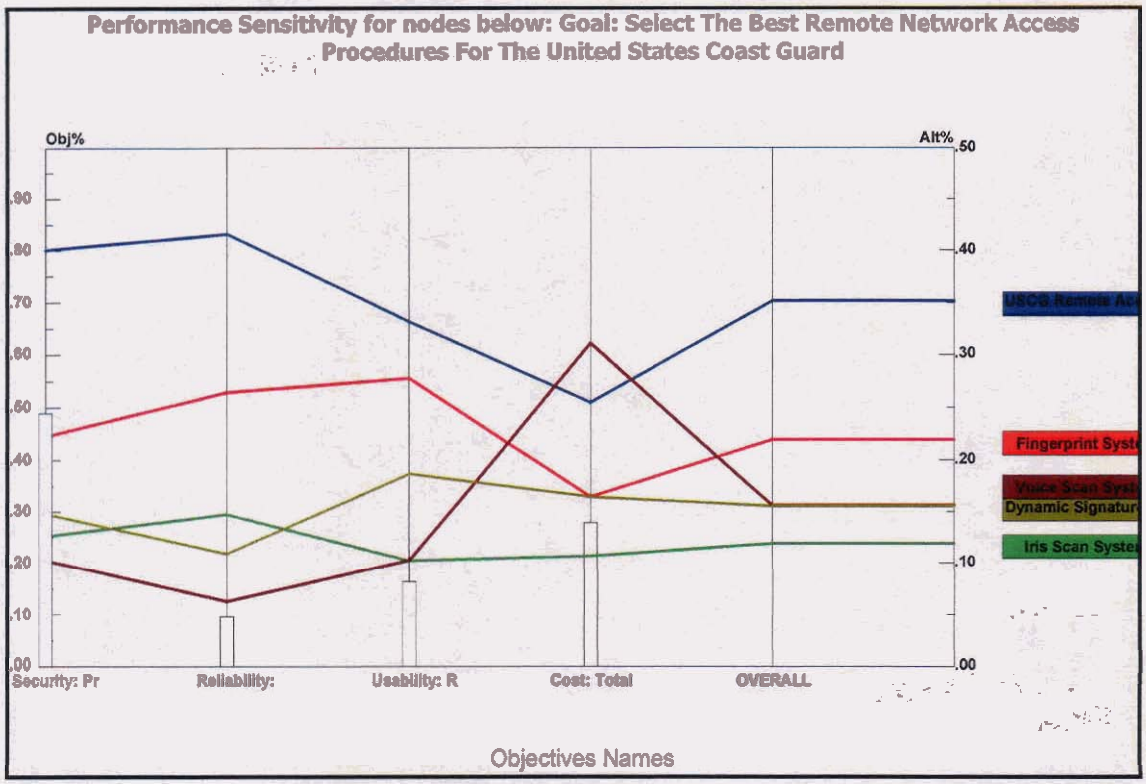
Results

Introduction

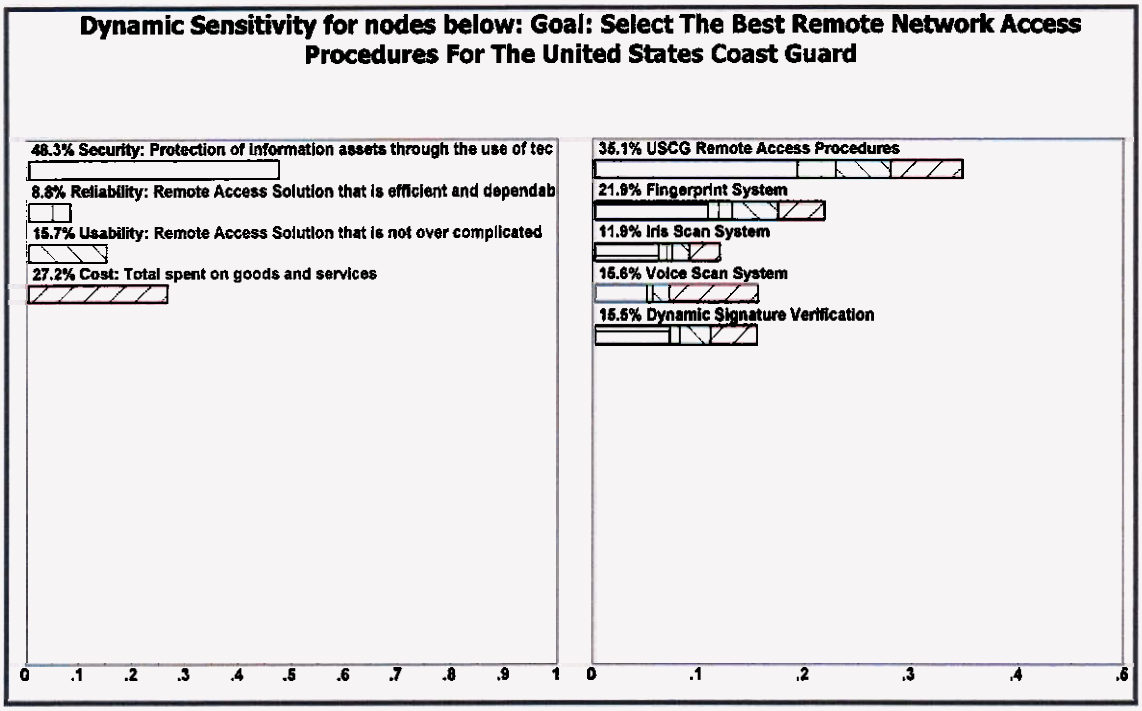
The purpose of this study is to evaluate the United States Coast Guard's remote access procedures and create a benchmark to be compared against emerging technologies. Research has shown that many new biometric technologies are being implanted for use in remote access systems. These emerging technologies were found to possess both good and bad user qualities. The use of biometric technology requires a constant balance between security and usability. Some biometric technologies provided high levels of security, but also produced high error rates. Other technologies such as Dynamic Signature Verification allowed too many false acceptances to use on its own, so two or more biometric technologies were combined, providing safe and secure access, but resulted in unacceptable increases in user costs.

This chapter will present the results provided by Expert Choice 11. The Synthesis summary clearly indicates that the United States Coast Guard's existing Remote Access Procedures are by far the overall best choice. The USCG existing procedures rated a .351 with the closets alternative, Fingerprint System receiving a .219. The Iris Scan System received an overall score of .119 indicating that it should not be considered as a viable replacement for the existing system.

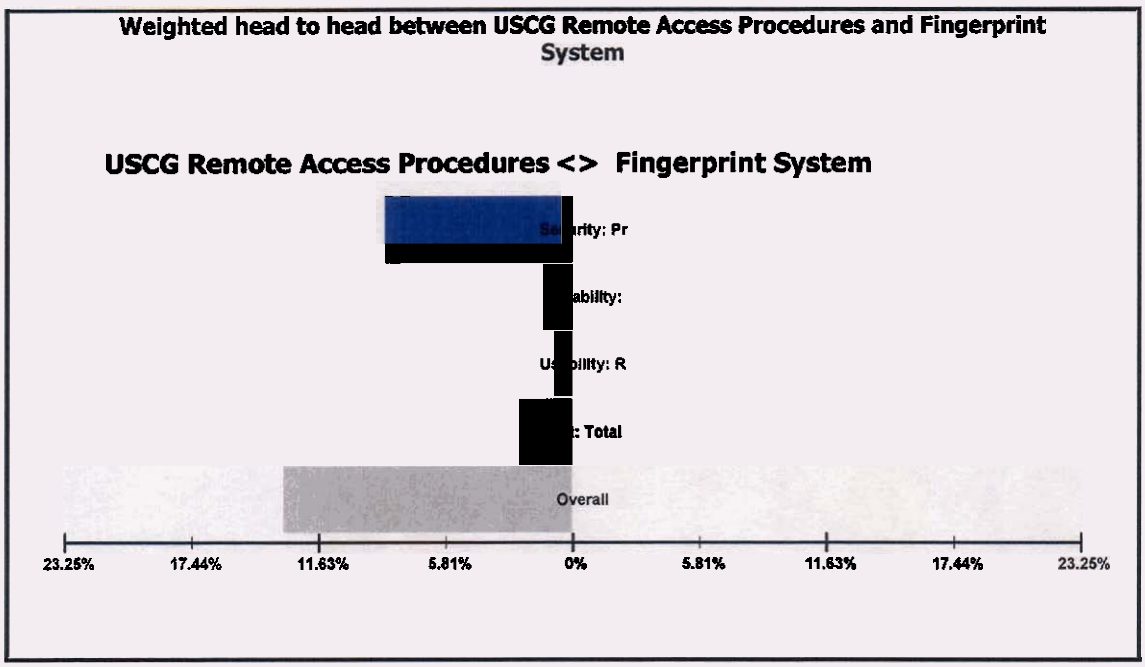




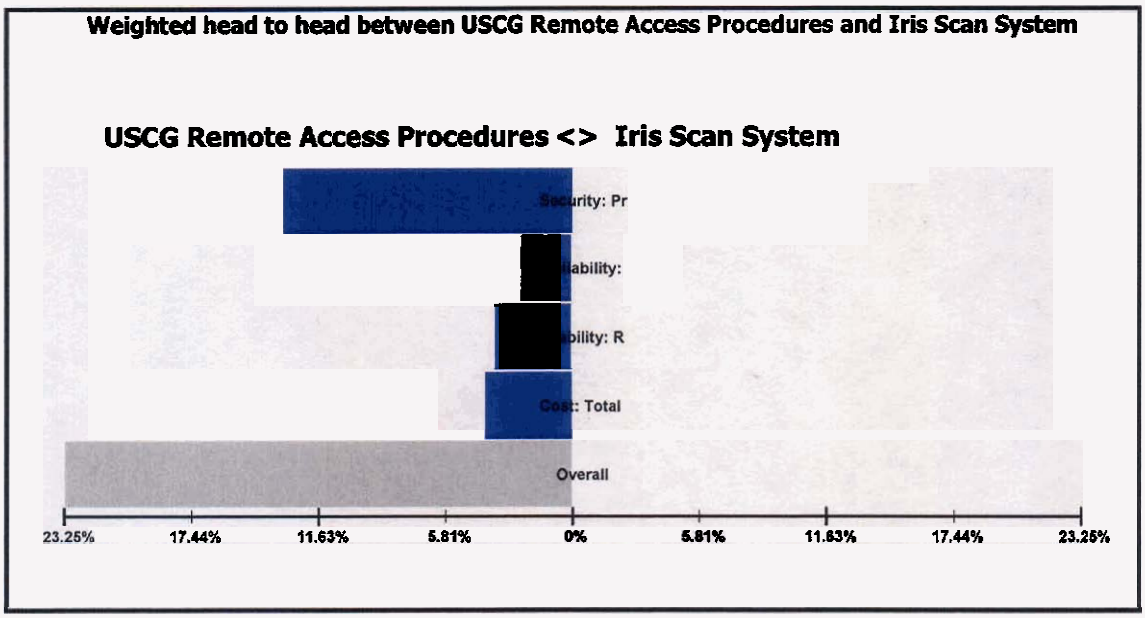
The Performance Sensitivity report shows how the alternatives were prioritized relative to other alternatives with respect to each objective as well as overall. The right Y axis indicates the overall comparison of alternatives with the sum of the alternatives totaling to one. The USCG existing Remote Access Procedures overall scored the highest of all the alternatives. In each individual category USCG existing Remote Access procedures clearly scored better than the entire group, except in the Cost category, where Voice Scan System proved to be a more cost effective solution. Security was a strong factor in the decision process, as per the chart above the USCG Remote Access System far exceeds any of the alternatives. The existing system provides safe and secure access without False Acceptance or False Rejection. This factor also affected the Reliability and usability scores as well. According to the graph above the overall score identifying that the USCG should not change the way the USCG connects remote users to the CGDN.



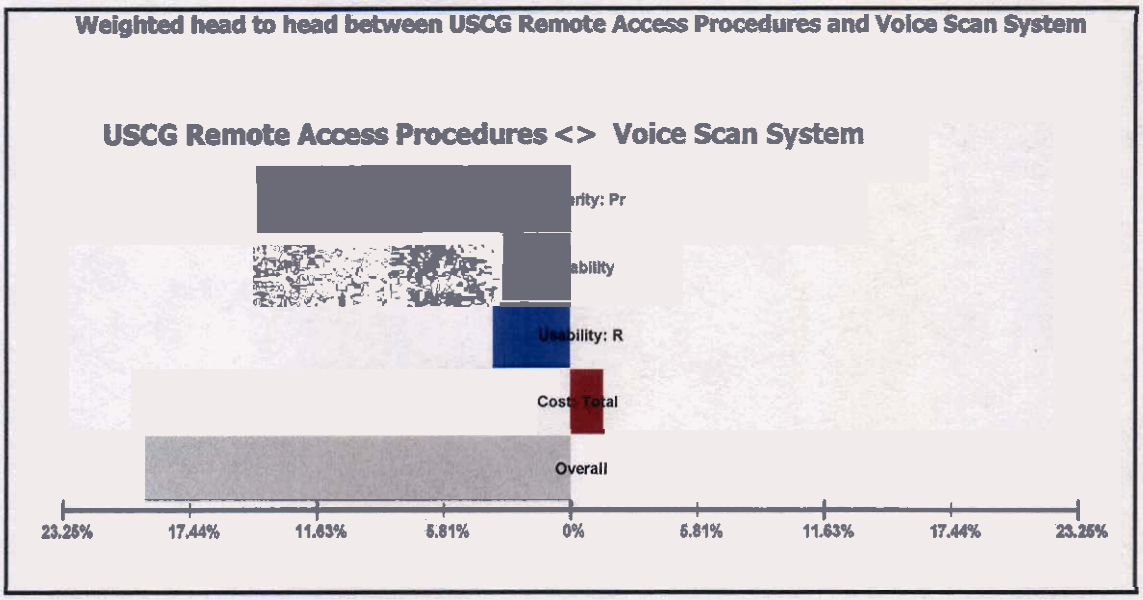
The Dynamic Sensitivity model indicates the priority of the objectives and how they affect the outcome of the alternatives. The graph also displays how the categories are distributed in each alternative. Security was the overall driving force in this decision at 48.3%. Cost was also considered to be very important, realizing 27.2% influence over the decision. Usability and Reliability were influencing factors, but had less of impact on the overall decision. The USCG existing Remote Access Procedures received a score of 35.1% because it has the best security to cost balance. The closest alternative, Fingerprint System, was 9.6% difference from the USCG existing procedures. In order for the alternatives to achieve the same level of security, combining two or more biometric solutions, they must increases their cost to an unacceptable level.



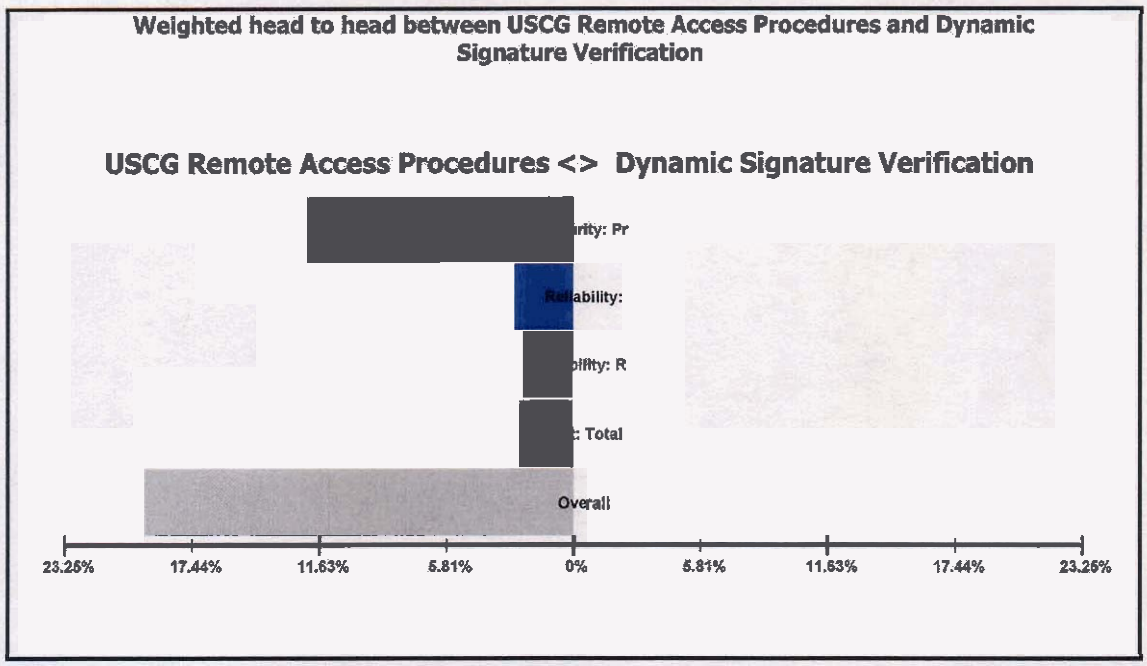
This chart presents a weighted head to head comparison of USCG Remote Access Procedures and Finger Print System. The USCG Remote Access Procedures outperformed the Fingerprint System in all four categories. This graph indicates that the Fingerprint System alternative was the best of all the biometric alternatives, but was outperformed by the USCG Remote Access Procedures by more than 11%. Hitchcock (2003) described some disadvantages of Fingerprint Systems as an inability to acquire a good sample. Finger Print readers sometimes draw a blank on some users due to the fact that they have hard skin or work with chemicals. These systems are also prone to spoofing, gaining access by using a latent print or wax forgery. This vulnerability to spoofing reducing the systems security and increases the cost of ownership, eliminated the Finger Print System as a viable option.



This chart presents a weighted head to head comparison of USCG Remote Access Procedures and Iris Scan System. The USCG Remote Access Procedures out performed this alternative in every category, especially Security and Cost. Iris Scan System was by far the worst biometric alternative and is not a viable option. According to Hitchcock (2003) Iris Scan hardware is more expensive than the alternatives. He also concluded that it is the most difficult to use, requiring the user to undergo training and be very attentive when using the system to avoid false rejection. This system is very difficult to spoof, but with the amount of errors, it still received a low score in Security. These errors also added to the already expensive hardware to push the overall cost to the highest of all the alternatives. This alternative does not provide a substantial increase to the USCG existing system without increasing the costs and should not be selected.



This chart presents a weighted head to head comparison of USCG Remote Access Procedures and Voice Scan System. The USCG Remote Access Procedures out performed the Voice Scan System every category except one Total Cost. These cost savings resulted in the use of the computers existing microphone and sound card, no additional hardware is needed to use this alternative. Hitchcock (2003) stated Voice Scan Systems are susceptible to replay attacks and high error rates due to low-fidelity microphones and further degraded by ambient background noise. The user is also required to speak the same way as they did during enrollment or they will receive a false rejection. These factors lowered the Security and Usability scores eliminating it as an option to replace the existing USCG Remote Access Procedures.



This chart presents a weighted head to head comparison of USCG Remote Access Procedures and Dynamic Signature Verification. Hitchcock (2003) discussed spoofing techniques by where an unauthorized person traces a user's signature in order to gain unauthorized access to the system. The Security score for this system was reduced due to this problem. Also inconsistent signatures lead to increased error rates and the authorized user does not have the ability to change their signature if it is stolen. These factors directly reduced the Usability and Cost scores. This alternative does not demonstrate the Security and Cost savings necessary to replace the existing USCG Remote Access Procedures.

The four graphs illustrate exactly how the USCG existing Remote Access Procedures compare to each alternative. The graphs compare each alternative in all four categories, Security, Reliability, Usability, and Cost, while also listing an overall score. The graphs show that the USCG existing Remote Access Procedures strongest category was Security, consistently outscoring all biometric alternatives. The most significant disparity between the alternatives was the USCG existing Remote Access Procedures and Iris Scan System. The USCG Remote Access Procedures score was in 23 percentile,

clearly indicating superior performance and usability. The graphs above indicate that biometric solutions solve some of the problems associated with lost or stolen passwords and tokens, but also indicate that biometric information can be stolen or spoofed as well. Hitchcock (2003) makes the point that biometric data can be stolen during transmission from the device to the computer, or when it is stored on a computer. This is more a problem for biometric technology because if a password is stolen it can be change, but if biometric data is stolen it cannot. The overall scores above without a doubt indicate that the USCG Remote Access Procedures out perform the alternatives in all of these categories.

Chapter V

Summary, Conclusions and Recommendations

Introduction

This study was meant to identify an acceptable process to ensure secure remote access to the CGDN and to determine if any changes should be made to the existing remote access procedures. Any recommended changes would have to increase security without overcomplicating usability and not significantly increasing overall cost. Providing user's remote access to the CGDN is imperative to mission success. This chapter will draw the conclusions from the results outlined in Chapter Four.

Statement of the Problem

This study was designed to determine through research if the USCG Remote Access Procedures can be improved upon using new technologies, specifically biometric authentication systems. The United States Coast Guard is well aware of the importance of keeping up with technology and return on investment for implementing these technologies. But the USCG is also concerned with the vulnerabilities that are associated with new underdeveloped procedures. This paper is dedicated to identifying which remote access procedures are right for the United States Coast Guard in respect to security, reliability, usability and cost.

Summary of Study Procedures

The USCG Remote Access Procedures were documented and then evaluated to identify the current level of security, usability and cost of running such a system. These procedures were also tested by Parnell in 1999 resulting in the VacMan RADIUS server with token authentication receiving the highest rating for all token authentication systems tested that year. The four alternatives selected, Finger Print System, Iris Scan System,

Voice Scan System, and Dynamic Signature Verification were of the industry leaders and were meticulously tested and documented in a paper titled Evaluation and Combination of Biometric Authentication Systems written by David C. Hitchcock. In this paper Hitchcock explained the strengths and weaknesses of the four alternative biometric technologies selected and conducted testing to further evaluate their vulnerabilities. All the research cited in this paper was used to evaluate the identified technologies in the USCG Remote Access implementation scenario.

Expert Choice 11, a software program designed as a multi-objective decision support tool based on the Analytic Hierarchy Process and was used to facilitate the decision making process. This process consisted of brainstorming, structuring a decision hierarchical model and prirwise comparison of alternatives to the objectives. Expert Choice 11 assessed the results and then performed a sensitivity analysis and produced the graphical results found in Chapter Four.

Conclusions and Implications

Upon conclusion of the research for this paper and further review of the results produced by the Expert Choice 11 it is this researcher's opinion that the United States Coast Guard should continue to use the existing Remote Access Procedures. The results of this study clearly identified multiple problems associated with the use of biometric technologies in the remote access environment. Biometric technologies are vulnerable to spoofing, causing a high rate of false positives, and when corrected cause unacceptable levels of false rejections. The excessive error rates associated with biometric technologies reduces system security, reliability and increases overall costs of ownership. To obtain an acceptable level of security when using biometrics the user would be forced to combine one or more of the evaluated technologies, resulting in a higher cost and reducing

usability. Another factor that increases costs is when a biometric system is compromised. Unlike passwords or tokens which can be changed or reset a biometric access is permanent, forcing the administrator to run two authentication systems to accommodate the user who can no longer gain access via biometrics. The USCG current Remote Access Procedures are a secure, user friendly, affordable solution and should not be replaced at this time.

Recommendations

Upon conclusion of this study it is recommended that the United States Coast Guard continue to use the Remote Access Procedures that are currently in place. The results have shown that it is not cost affective nor will it improve remote access security by implementing any of the biometric alternatives. The United States Coast Guard's Remote Access Procedures provide a safe, secure, and user friendly process for connecting remote users.

Recommendations for Further Studies

The United States Coast Guard should continue to monitor the progress of Biometric Technologies and evaluate them against the current procedures on an annual basis. A more detailed study should be conducted on the USCG current system including diagnostic testing, throughput, packet loss, and user connection range. A user survey should be conducted to determine the exact level of usability and token error rate. The study should also be expanded to include wireless connections with the new security standards IEEE 802.11i.

References

Bolle, R., Connell, J., Pankanti, S., Ratha, N. & Senior, A. (2004). *Guide to biometrics*. New York: Springer-Verlag.

Chirillo, J., & Blaul, S. (2003). *Implementing biometric security*. Indianapolis, IN: Wiley Publishing, Inc.

Commandant Instruction 12630.1 (July 15, 1997) Coast Guard Telecommuting Program, Washington, DC: United States Coast Guard.

DiDio, L. (1998, July 22). U.S. coast guard beefs up security after hack. *Computerworld*, Retrieved July 13, 2005, from http://www.cnn.com/TECH/computing/9807/22/coastguard.idg/.

Dixit, S. (1999). Data rides high on high-speed remote access. *IEEE Communications Magazine*, *37*(1), 130-141.

Hitchcock, D. (2003). Evaluation and Combination of Biometric Authentication Systems. In. (Eds.), (pp. 1-159). Gainesville, FL: University of Florida.

Ibe, O. (1999). *Remote access networks and services*. New York: John Wiley & Sons, Inc.

Kara, A. (2001). Secure remote access from office to home. *IEEE Communications Magazine*, *39*(10), 68-72.

Kasacavage, V. (2002). *Complete book of remote access; connectivity and security*. Boca Raton, Fla: Auerbach Publications.

Korean Studies Association of Australasia, (n.d.). Upgrading and repairing networks. Retrieved July 08, 2005, from Chapter 27 Adding Remote Network Access (Telecommuting) Web site: http://www.ksaa.edu.ru:8101/book/net/ch27.htm.

Microsoft, (2001). Microsoft Windows NT Server. Retrieved Oct. 11, 2005, from Microsoft Windows NT 4.0 Server Details Web site: http://www.microsoft.com/ntserver/ProductInfo/features/Features.asp.

Nedeltchev, P. (2003). *Troubleshooting remote access networks*. Indianapolis, IN: Cisco Press.

Nortell Networks (2001): FIPS 140-1, Cryptographic Module Security Policy. Retrieved Oct. 11, 2005, from National Institute of Standards and Technology Website. http://csrc.nist.gov/cryptval/140-1/140sp/140sp185.pdf

Paquet, C. (1999). *Building Cisco remote access networks*. Indianapolis, IN: Cisco Press.

Parnell, T. (1999). Id, please. *Network World*, Retrieved Oct 21, 2005, from http://www.networkworld.com/reviews/0301rev.html.

Robichaux, P. (1999). *Remote access 24seven*. San Francisco: SYBEX, Network Press.

Sudhir, D. (1999). Data rides high on high-speed remote access. *IEEE Communications Magazine, 37*(1), 130-141.

The Computer Technology Documentation Project, (n.d.). Retrieved Jul. 08, 2005, from Windows 2000 Remote Access Web site: http://www.comptechdoc.org/os/windows/win2k/win2kras.html.

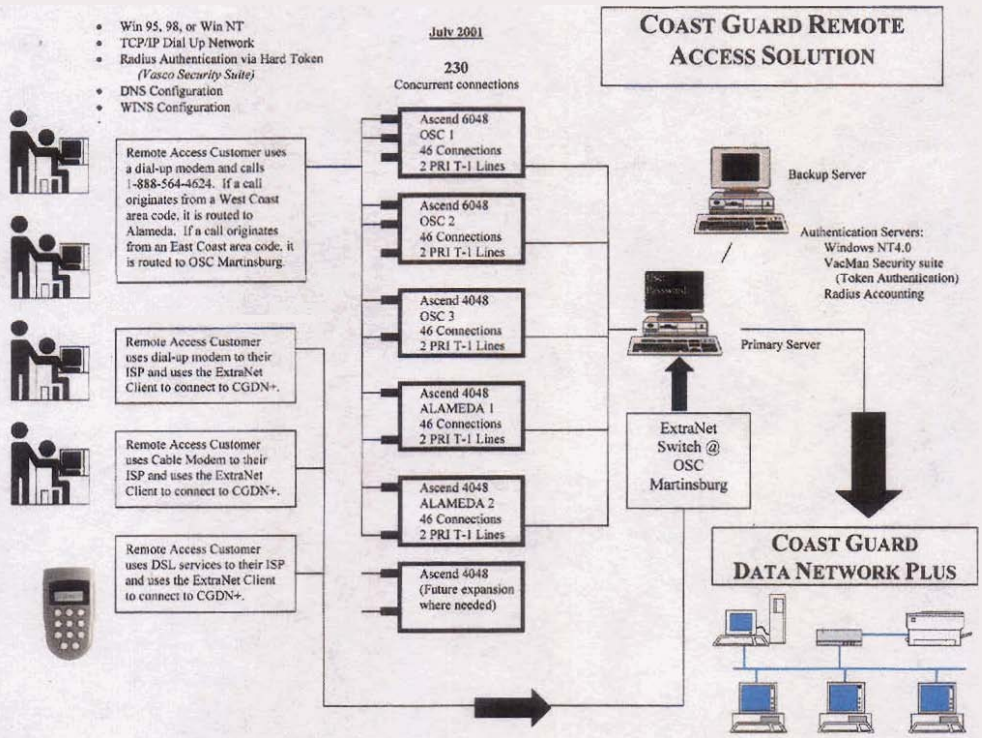
VASCO, (2002). Vacman radius middleware. Retrieved Oct. 11, 2005, from Auto Management Web site: http://www.idepro.fr/upload%5CFournisseur%5CVasco%5CVasco_VACMAN.pdf.

Webopedia: Online Computer Dictionary for Computer and Internet Terms and Definitions, (n.d.). Retrieved July 08, 2005, from Webopedia Web site: Webopedia.com.

Appendix A

Diagram 1

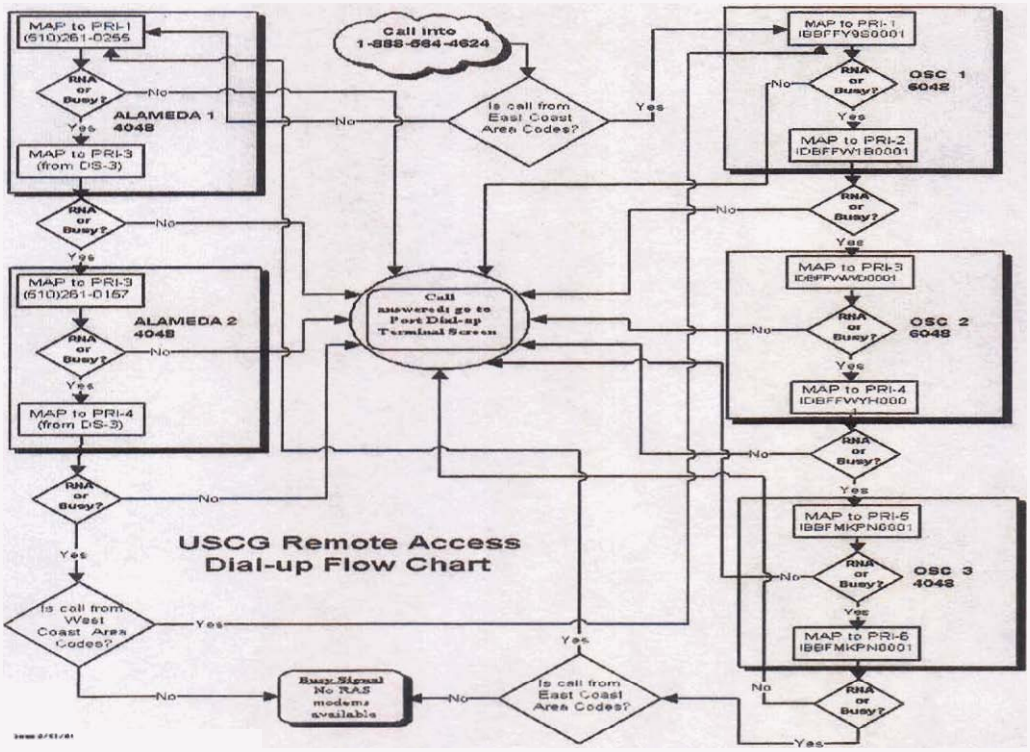
United States Coast Guard Remote Access Solution



Appendix A

Diagram 2

United States Coast Guard Remote Access Dial-Up Flow Chart



Appendix B

Diagram 3: Remote Access Scorecard

Tere Parnell (1999)

	Manage-ability 20%	OS inte-gration 20%	Scala-bility 20%	Secur-ity 20%	Time to auth-enti-cate 10%	Docu-menta-tion 5%	Install. 5%	TOTAL
VacMan/ Server	8x.2 =1.6	8.2 =1.6	8x.2 =1.6	8x.2 =1.6	7x.1 =0.7	5x.05 =0.25	7x.05 =0.35	7.7
ActivPack	8x.2 =1.6	8x.2 =1.6	6x.2 =1.2	8x.2 =1.6	7x.1 =0.7	7x.05 =0.35	8x.05 =0.4	7.45
SafeWord	6x.2 =1.2	7x.2 =1.4	7x.2 =1.4	8x.2 =1.6	7x.1 =0.7	6x.05 =0.3	5x.05 =0.25	6.75
Defender Security Server	6x.2 =1.2	5x.2 =1	5x.2 =1	8x.2 =1.6	7x.1 =0.7	6x.05 =0.3	7x.05 =0.35	6.15

Note: Products are ranked on a 1-10 scale in each category, and then multiplied by the weight in each category. These are added to give a total score.