Secure Outlook Web Access

A Project Report
Submitted to the Faculty
of the
UNITED STATES COAST GUARD ACADEMY
in partial fulfillment of the requirements for the
Degree of Bachelor of Science
in
Electrical Engineering
by

1/c Kevin Connell

1/c Hermie Mendoza

Projects in Electrical and Computer Engineering
02 May 2007

Reviewed By:

LT Todd W. Moyer, Project Advisor

LCDR David J. Godfrey, Class Coordinator

Professor Keith C. Gross, Chief, Electrical & Computer Engineering Section

Abstract

The Coast Guard Telecommunications and Information Systems Command (TISCOM) has requested a design to determine whether the Common Access Card (CAC) provides enough security to access Outlook Web Access (OWA) from an internet-enabled computer. Coast Guard personnel are currently limited to accessing email via one of two methods: being directly logged on to the Coast Guard Data Network (CGDN+), or using remote access server (RAS) tokens to remotely access the network. By providing an alternative method for service personnel to securely access email remotely, the benefits of such a system could easily increase productivity.

This paper will discuss the configuration of our prototype network. The testbed network utilizes an Active Directory architecture with Exchange Server 2003, similar to the CGDN+ and implements a hardware-based Cisco Secure Socket Layer Virtual Private Network device (SSL VPN) to establish secure remote connections into the prototype network. Several difficulties were encountered in implementing the prototype network including having inadequate hardware licenses. At the conclusion of the fall semester, a simple prototype network was established.

Throughout the spring semester, additions were made to the network to increase the security and interoperability with CAC-enabled logons. The inclusion of a Microsoft Internet Security and Acceleration server has enabled a software-based approach to authenticating users with their Common Access Cards. This has provided TISCOM a second method to deploy a wide-scale CAC authentication-based system. By utilizing the methods included in this project, it is possible to create a network solution to authenticate remote users over the Internet to securely access a web-based email portal known as Outlook Web Access.

Table of Contents

Introduction	page 1
Background	page 3
Objective	page 10
System Design	page 13
Results	page 22
Conclusions	page 26
References	page 28
Bibliography	page 30
Appendices	page 32
Appendix A: Project Plan	page A-1
Appendix B: Requirements Document	page A-2
Appendix C: Support Plan	page A-3
Appendix D: Test Plan	page A-4
Appendix E: System Design Specifications	page A-5

Introduction

Electronic mail, or email, has developed into one of the most important means of communication for many organizations [11,12]. In the proprietary private military computer network called the .MIL network, email is example of a readily available network resource. The current methods in accessing .MIL email are to (1) be logged onto the wide area network (WAN), the Coast Guard Data Network Plus (CGDN+), or (2) to use remote access server (RAS) tokens to remotely access the CGDN+. At the workplace, Coast Guard personnel log onto the CGDN+ on his or her Standard Workstation III (SWIII) computer and access email by using Microsoft Outlook software. However, RAS tokens are used when Coast Guard personnel would like to access network resource from a home computer.

RAS tokens are pocket-size devices that have a time-sensitive number, which is verified by a server. Although logging onto the CGDN+ is the primary and safest method to access email, there are several problems resulting from the usage of RAS tokens. These derive from their limited usability and the cumbersome feature of a server key changing every minute. Thus, TISCOM has identified the need for an alternative method to access email on the CGDN+.

Currently, the Department of Defense (DoD) uses the Common Access Card (CAC), or the military identification card, to provide its personnel access to vital network resources such as email. Unlike RAS tokens, the CAC can be used for data encryption, email signatures, user authentication, and user non-repudiation (proving that the identities of the sender and receiver of

a message). This project evaluates and recommends whether the CAC can help provide alternative method of authenticating to access email for the Coast Guard. The project also considers the usage of the newest secure socket layer virtual private networks (SSL VPN) technologies available, to be utilized in a simulated CGDN+.

Last year's project with the CAC by Simon Barr and Grant Wyman focused on using it to remotely access all network resources [1]. Unlike the previous project, this project's main objective is to provide secure email with an SSL VPN connection by using a CAC. The CACs provide a potential solution to the Coast Guard's limited email access, while creating new opportunities to access network resources. If this project is successful, then the next step could be to provide remote access to other network resources via the CAC.

By providing an alternate and secure means to access the .MIL email, all Coast Guard personnel will have the capability of accessing their email regardless of their location. The only prerequisite to this benefit is the need for Internet access and a USB connection.

The paper will first introduce the SSL VPN technologies that form the foundation of the prototype network. Then a discussion of the project requirements and objectives as prescribed by TISCOM follows. Included in the paper are a detailed explanation of the project design and the complications encountered this semester. Lastly, the paper will summarize major accomplishments this semester and establish the next semester's project goals.

Background

Network administrators must "…provide confidentiality, integrity, and authenticity" as information is sent across a local area network (LAN) and the Internet [2]. In order to accomplish secure communications between the LAN and the Internet, organizations are relying on third party vendors to secure their networks by implementing new security software or hardware devices instead of reconfiguring the core network topology. A notable method used by network administrators to secure data between LANs and the Internet is the implementation of a public key infrastructure (PKI). Unlike other network security methods, it has four distinct security benefits: authentication, data integrity, non-repudiation, and confidentiality [3].. An SSL VPN and its related technology used for the prototype network relies on the development and usage of PKI. The following sections will briefly describe SSL VPN and its related technologies.

Public Key Infrastructure (PKI)

A public key infrastructure (PKI) is defined as "the framework and services that provide…the generation, distribution, control, tracking, and destruction of public key certificates" [4]. These infrastructures, or software depositories, are based on the concept of mutual trust. To establish trust, each user's identify must be independently verified. This verification process results from asymmetric cryptography. In asymmetric cryptography, a user has a private key and a freely distributed public key, which are generated simultaneously by a cryptographic algorithm. The public key enables any party, who could be another user or a server, to encrypt a message and have it only be decrypted with the user's private key.

To establish a user's credentials, digital certificates are formed from the user's public and private keys [3]. Each digital certificates carries the following standard information: user name, a serial number, expiration dates, the user's public key, and the digital signature of a certificate-issuing authority, which will be discussed in further detail. The primary purpose of digital certificates is to grant third parties access to the user's public key in order to verify the user's identification. User verification, however, is not the only benefit of PKI. Certificates can also be used to confirm data integrity, by ensuring that the message was not altered during transmission between users. If the message's data had been changed during transmission, then the message will have a different hash, or data digest, from the original message. Thus, two different hashes will indicate a compromise of data integrity [3].

To effectively monitor digital certificates, organizations employ certificate authorities (CA), whose sole purpose is to act like notaries for their networks. The CAs are responsible for:

- Verifying a certificate's rightful owner,
- Posting a certificate revocation list (CRL) to keep track of expired certificates, and
- Assisting in settling session disputes caused from old certificates by providing an archive of expired certificates that were previously marked as trusted by the CA [3].

By developing a simulated CA on the prototype network, users are afforded the opportunity to view and send encrypted emails.

The Department of Defense (DoD) has established its own implementation of PKI based on X.509 Version 3 as established in DoD Instruction 8520-2 [5]. This certificate policy outlines

how a DoD operated CA functions. Due to its large organizational structure, the DoD utilizes two CAs: the National Security Agency (NSA) and the Defense Information Systems Agency (DISA) [3]. These CAs utilize Registration Authorities (RA) and Local Registration Authorities (LRA), who are in charge of issuing certificates upon the confirming the user's military status. The certificate, in order to be issued, requires the user to be enrolled with the Defense Enrollment Eligibility Reporting System (DEERS), which is TRICARE's enrollment for military medical insurance, and be at the local military identification issue office for Real-time Automated Personnel Identification System (RAPIDS) verification. To retrieve a user's digital certificates available in the DoD PKI, a user must access the public key on the Microsoft Exchange Global Access List (GAL). Each user has only one public key on the GAL.

The technical standards for a federal agency's PKI was primarily developed by the National Institute of Standards and Technology (NIST) [3]. Among some of the items thoroughly discussed and addressed by NIST are encryption algorithms, security standards and risks, and the organization's PKI architecture [3]. Although the NIST's documentation did not describe specific methodology to implement a federal PKI, it did explain how federal PKI services could be deployed effectively by presenting a PKI overview and analysis of its primary components. The PKI cost-benefit breakdown must still be considered prior to an agency's implementation [3].

DoD Common Access Card (CAC)

The purpose of the Common Access Card, as outlined in DoD Directive 8190.3, is threefold [7]. First, the CAC is "the standard identification card for active duty Uniformed Services personnel (to include the Selected Reserve), DoD civilian employees, eligible contractor personnel, and eligible foreign nationals" [8]. The second purpose is for the CAC to become the "Department's primary platform for the public key infrastructure authentication token used to access DoD computer networks and systems in the unclassified environment" [8]. The final objective is to have the CAC act as the "principal card enabling physical access to buildings, facilities, installations, and controlled spaces" [8].

A two-dimensional barcode and a magnetic stripe are two of the security and storage technologies located on the CAC. Pertinent personal information such as the member's name, rank, service, Social Security Number (SSN), and date of birth, are stored in the two-dimensional barcode and printed on the card [8]. The other security and storage technology is the one-dimensional barcode featured on the back of the CAC. However, the CAC's gold chip holds the user's sensitive personal information and more.

The CAC's integrated circuit chip (ICC) provides a high security solution for every cardholder's personal information. The data held on the chip is encrypted and cannot be accessed without either the user's Personal Identification Number (PIN) or a master number only given to card issuing authorities [9]. The ICC allows the capability to store information from the card's other

three security technologies while incorporating several pieces of innovative information not found anywhere else. The ICC also contains the cardholder's public and private key certificates, which can be used over a broad range of purposes, such as training accountability, entrance control at installations, and access to both the Non-classified Internet Protocol Router Network (NIPRNet) and the Secret Internet Protocol Router Network (SIPRNet) classified network. The NIPRNet and the SIPRNet are the two sub-networks of both the DoD and Coast Guard's .MIL network.

Secure Socket Layer

To combat insecure Internet connections, Netscape® created a secure Internet protocol (IP) for the World Wide Web. In 1996, the company developed the specifications for Secure Socket Layer (SSL) 3.0 and became the industry standard for securing information on the Internet [CITE]. This section will also discuss how the transport layer security (TLS) has superceded SSL in become the industry standard and the differences between the protocols. For the prototype network, SSL will be the primary protocol used to establish secure communications when users access Outlook Web Access (OWA).

SSL acts as an independent security layer. It is designed to be run beneath the application layer and the above transport protocols in the five-layer Transmission Control Protocol (TCP)/IP model [10]. Though it is most often viewed as operating over TCP, it is designed to function across any protocol. Typically, SSL is used to secure information being passed across the

Internet. It is widely used for commercial transactions when credit card numbers are being passed across the Internet on business transaction forms within web pages. For example, banking institutions utilize SSL to encrypt a customer's web page so that sensitive information, such as bank account numbers and routing strings, are not published across an open connection.

In January 1999, SSL was reconfigured to comply with the upgrade to HTTP Version 1.1 and received a new name, the TLS, Version 1 [2]. The differences between TLS and SSL Version 3.0 are minimal. However, when the client and server agree to utilize a certain encryption protocol, SSL and TLS must pick the same protocol, as are not interoperable. As of April 2006, TLS was upgraded to Version 1.1 and the differences between it and SSL are still minimal.

Secure Socket Layer Virtual Private Network

Business employees in the 21st century are telecommuting now more than ever before [11]. Advances in technology have allowed workers to utilize intranet resources previously not available for use outside the company's walls. For example, Coast Guard personnel use RAS tokens to telecommute in order to remotely access email. Sensitive information from an intranet that is sent over the Internet must be transmitted in a secure mode [12]. A common method of extending the intranet for secure remote access is establishing a Virtual Private Network (VPN).

A traditional VPN uses IP security (IPSec) and is “an overlay network built with tunnels in which the tunnel payloads are encrypted and authenticated” [12]. In a broad sense, a VPN is viewed as an encrypted tunnel which runs through a larger network to an authenticated client. Traditional VPNs rely on IPSec to secure connections between two endpoints and requires users to have a remote desktop program (RDP) such as Citrix as seen in Figure. In comparison, the technology of a Secure Socket Layer Virtual Private Network (SSL VPN) utilizes the Secure Socket Layer protocol for establishing and maintaining secure connections. Since most major internet browsers and operating systems inherently support SSL, this type of VPN is extremely flexible and versatile and, under certain configurations, may not require the user to install an RDP to establish the connection. TISCOM has a Juniper Networks hardware-based SSL VPN, but it has not been added to the CGDN+ for personnel usage. Table 1 features a summary of the differences between IPSec and SSL VPNs.

Table 1: Comparison of IPSec VPNs and SSL VPNs

	IPSec	**SSL**
Installation of Client Software	Yes	No
Interoperability Problems	Yes	No
Usage	Site-to-site communications	Remote access for Web-based applications

Outlook Web Access

The prototype network must include a method of affording users the opportunity to remotely access email. This will be completed by enabling Outlook Web Access (OWA). In Microsoft's Exchange Server 2003, users can access email from Exchange folders via the Internet by using OWA) This application is a webmail service that acts and looks very similar to the Microsoft Outlook desktop client. The only downside of using OWA is its need for an Internet connection.

Summary of Main Points

For the testbed network to have secure communications, a concept of mutual trust must form between users and servers, which is established by developing a PKI. Digital certificates are a component of a PKI and verify a user's credentials. The DoD has developed its own PKI, which utilizes the CAC to store the user's public and private key certificates. The CAC will be also used in the prototype network for user verification and network security. In order to extend network resources, organizations such as the Coast Guard use VPNs. A specialized type of VPN

is an SSL VPN, which utilizes the technology of SSL to establish and maintain secure connections. Email is an example of a network resource commonly extended in a VPN. An organization's users in a Microsoft-based network can access his or her email via the Internet by using OWA. With an SSL VPN, the prototype network can extend email outside of the network for users by enabling OWA on Exchange Server 2003.

Objective

Project Requirements

The sponsor, TISCOM, has requested that Coast Guard members access their email from the .MIL network over the Internet by using an Internet-capable computer and authenticating each individual using their assigned username, password, and the CAC. The project's requirements are divided into two levels: functionality and authentication. Both levels will be discussed in depth.

The goal of the functionality level is to enable users of the .MIL network to easily access their email from any computer connected to the Internet. In order to accomplish this goal, a secure network bridge from the .MIL network to a user's computer must be established, or the user will not be able to access the network. The secure network bridge between the .MIL network and a user's computer will utilize VPN technology given VPN technology's standard network protocol that has a wide user support base and is known for providing stable networks. For easy, low monetary cost, and quick implementation, a commercial-off-the-shelf (COTS) VPN-based product should be used. Also know for a wide user support base and known for providing security, the network bridge will be secured with SSL technology. Furthermore, a hardware-

based SSL VPN bridge will be implemented to allow for multiple connections into the network simultaneously, minimizing network lag. A firewall must be incorporated to deny unwanted traffic to access the .MIL network.

The second level of the project requirements is authentication. Its goal is to enable two-factor authentication using a CAC. Two-factor authentication is verifying a user who has the CAC itself in possession and knows the CAC's pin. Hence, it will force users to login to the network using their username and password combination and their CAC as an increased network security measure. For more information on project specifications, refer to Appendix A.

Project Objectives

Rather than evaluating the merits of using smart cards versus RAS tokens, this project will assess the feasibility of installing and configuring a network device to establish secure connections to users from the .MIL network for remote email access. The project's primary objective is to provide a proof-of-concept design that determines whether the CAC is an effective method to authenticate to OWA as specified in the project specifications in Appendix A.

The proof-of-concept design involves designing and implementing a prototype network according to TISCOM's specifications for the CGDN+, creating an SSL VPN connection for secure access, and enabling secure logins with a user's CAC. Furthermore, the project is divided into three stages, as described in Appendix B: (1) prototype network development, (2) design of an SSL VPN connection, and (3) remote email access.

The second objective is for the prototype network to conform to government policies concerning secure network access, as mentioned in the project support plan in Appendix B. Any piece of electronic equipment added to the CGDN+ undergoes testing for compliance with government network security policies. A third objective is to evaluate the procurement costs and support to determine if the developed system can be applied operationally [Appendix B]. To achieve the project's three objectives, the user must access OWA by logging into the network with a CAC over the Internet. A system design using an SSL VPN based hardware device that conforms to Coast Guard specifications will be delivered to TISCOM at the conclusion of the project.

System Design

Project Scope

The prototype network design is divided into two general parts for administration, hardware and software (Figure 1). The system hardware focuses on the systematic setup of the SSL VPN. The software components involve configuring the necessary enterprise network administration. These components and their configuration in the model network will be discussed in detail in this section. This information can also be found in both the Test Plan and System Design, in Appendices D and E, respectively.

Hardware – SSL VPN Configuration

Commercial-off-the-shelf (COTS) products were utilized to create and maintain our testbed network. Among the hardware that was selected was an SSL VPN engine for establishing secure tunnels between clients across the Internet and servers located on our network. Although

TISCOM has in its possession a Juniper SSL VPN, the Academy's Cisco grant enabled us to use a Cisco PIX firewall. With upgraded firmware, the PIX gains VPN capabilities.

The hardware used for the project can be categorized as either relating to security or connectivity, which presented two options in deciding how to set up the network. Although software can be loaded onto a computer to act as a firewall or VPN device, hardware-based implementations often provide much higher bandwidth throughput, thereby increasing the total amount of users who can simultaneously access the device. This decision to use hardware implementations meets the expectations set forth in project requirements in Appendix A. This piece of hardware serves a dual purpose: it enables a large amount of users to VPN into the network, and, acts as a firewall that denies unwanted traffic. In this sense, hardware implementations of an SSL VPN protocol increase the number of users who are able to access the network while adding a firewall to increase the overall security. This decision in using COTS hardware devices fulfills one of the project requirements.

After integrating the PIX into our prototype network, a network topology was drawn representing the physical connections between the computers, servers, and firewall. This network typology is further described in Figure (1).

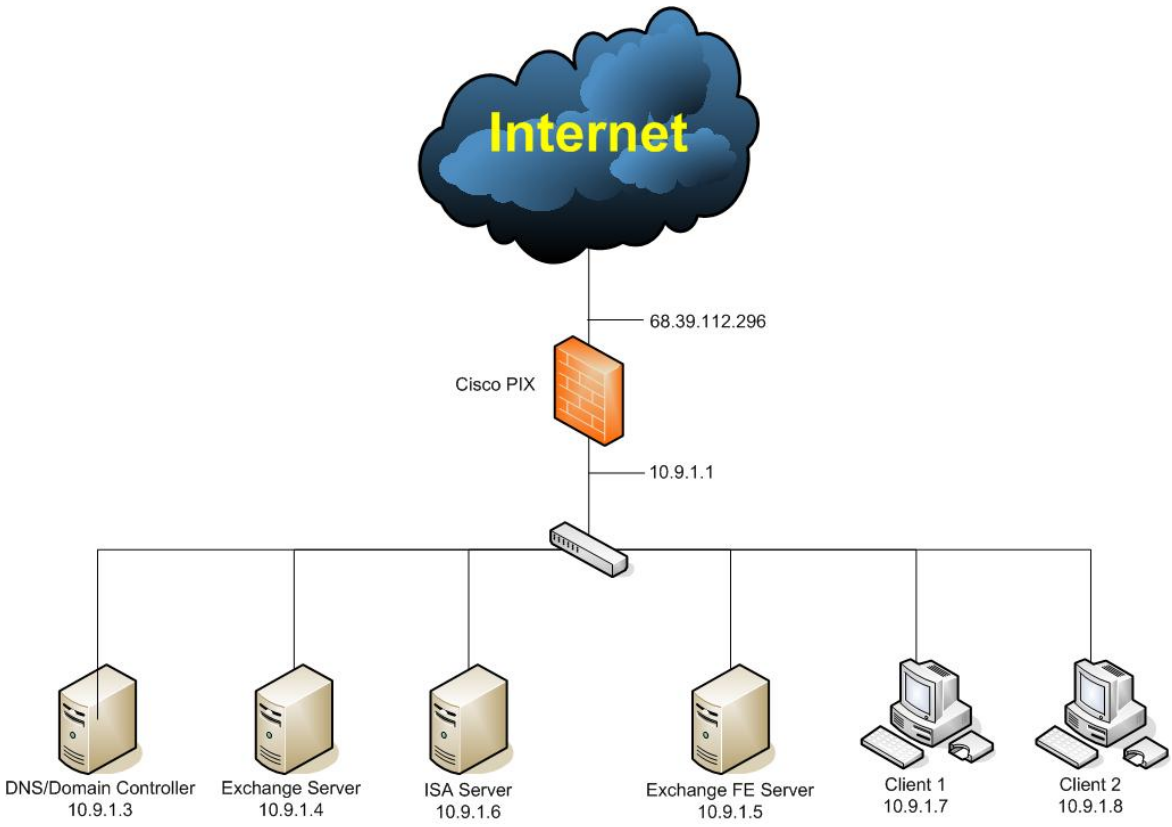

Figure 1: Prototype Network Topology

Equipment choices are limited due to the small budget afforded and existing hardware. With the partnership of Cisco Networks, several pieces of equipment are available for the project, including the Cisco PIX firewall. The Cisco hardware is chosen rather than the Juniper Networks SSL VPN for convenience and monetary reasons.

Though the Cisco PIX is primarily a firewall, another problem has arisen: to determine whether one piece of hardware is going to be used, or two distinct devices to handle the VPN connections and firewall services independently. To fulfill the project requirements, only one piece of hardware is used.

Software – Network Administration

The model network is dependent on Microsoft's Active Directory® and Exchange Server 2003. Microsoft's Windows Server 2003 and XP Professional are the operating systems running on the servers and client computers. Each client computer and test computer will need to be installed with smart card drivers and software in order to access the CAC's certificates. The smart card drivers and software will be COTS products currently used by TISCOM.

The prototype network uses Microsoft's Active Directory® service to create an accessible central repository to store, organize, and secure all enterprise network information and configurations. In addition, Active Directory® helps network administrators to enforce enterprise network policies, deploy programs across the network, and disseminate critical security updates.

As shown in Figure 2, the domain name of the prototype network is PECE.USCGA.EDU. The domain is configured to have six objects: four servers and their related services and two client computers. These six objects form a single Active Directory® forest. To facilitate network administration, the Active Directory® forest is subdivided into four organizational units (OUs): domain controllers, network computers, Exchange servers, and ISA Servers. For example, the domain controllers OU groups all those objects that are domain controllers in the network, and the network computers OU organizes all client computers into a single group. Each OU is configured with a unique group policy and monitored by delegated network administrators. The group policies for each OU are network policies describing those software and hardware components users are able to access, modify, and/or delete on the respective computer.

The Active Directory® domain of the model network is not affiliated with the USCGA.EDU domain, but rather it is a sub-domain of the Coast Guard Academy's network. Moreover, the prototype domain is not a trusted domain, which signifies that the users of the PECE.USCGA.EDU domain cannot access the USCGA.EDU domain.

The DNS/DC server in Figure 2 is the network's primary domain controller (DC), which houses the network's foremost Active Directory®. The Exchange and Exchange FE servers also have Active Directory® software loaded. Information in the DC and/or secondary Active Directory® stores are replicated amongst each other at a minimum of 30 second intervals. This ensures that each server with the Active Directory® software have the latest enterprise network configurations.

Microsoft Exchange Server 2003, or simply referred to as Exchange, is another software suite currently used on the prototype network. Exchange is responsible for providing the network's message and email capabilities including Outlook Web Access (OWA).

As featured in Figure 1, the prototype network has two Exchange servers because the Exchange front-end (FE) and back-end (BE) architecture. An Exchange FE provides OWA while the BE server provides mailbox storage. Thus, the FE is a proxy for Internet email client access protocols such as HTTP, POP3, and SMTP. The reasons why a FE and BE architecture are used include SSL offloading from the BE server, a reduction of attack surface by having a decreased number of ingress points into the network, and simply load balancing enhancements.

For the prototype network, all users are given access to his or her mailbox account. In addition, each individual is given permission and rights to access OWA. The email client access protocol used is only SMTP; all other protocols are disabled and not in use.

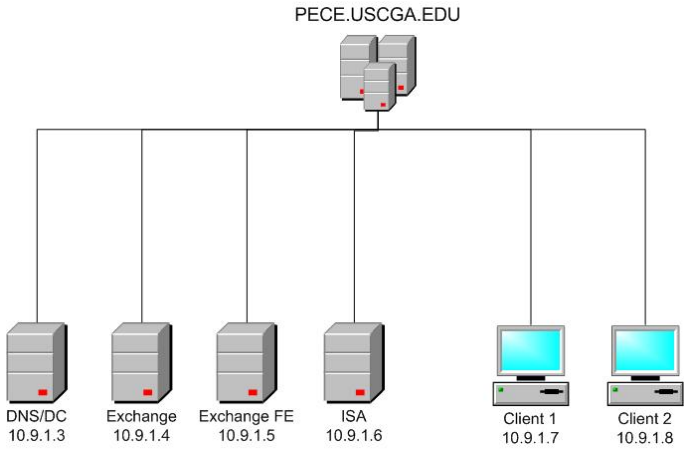

Figure 2: Active Directory architecture of the PECE.USCGA.EDU Domain

The OWA's configuration requires a multi-layer authentication for email access. As specified by the Coast Guard, two-factor authentication is the minimum authentication for remote access as dictated in Appendix A. However, it has been determined that a four-factor authentication will be implemented, which includes the CAC, the CAC's PIN, network username, and network password. This is accomplished by using Microsoft's Internet and Security Accelerator (ISA) server.

The ISA server currently deployed in the prototype network is Microsoft's integrated edge security gateway, which is a software proxy firewall. It is another layer of security for network and provides secure remote access to network applications and data. This type of proxy firewall

works by blocking ports and analyzing incoming and outgoing traffic as seen in Figure 3. It also resides outside the local area network (LAN) but before the hardware based Cisco PIX firewall. Combined with the CISCO PIX firewall, the ISA server can mitigate network attacks through HTTP and signature filtering, defends the network from flooding attacks from unauthenticated and authenticated users, force clients to present identification credentials on existing SSL connects, filter and restrict logon certificates, packet inspection, and a reduce the total attack surface by exposing fewer services for access. For this project, the ISA server is used to securely publish the Outlook Web Access for remote access and verify users with the DoD public key infrastructure's (PKI) certificate revocation list (CRL).

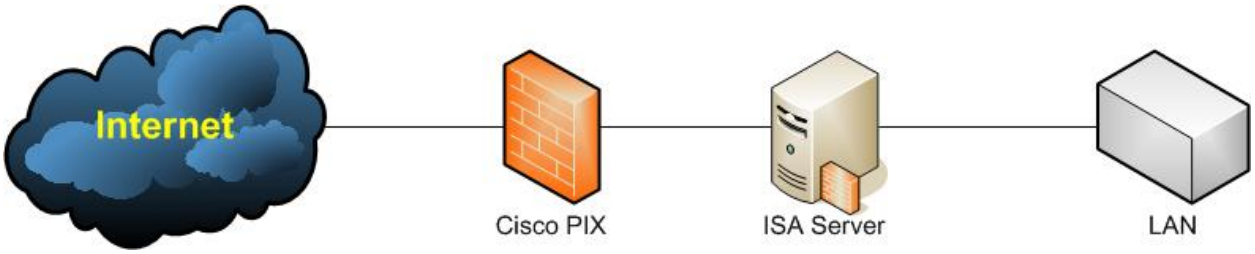

Figure 3: Simplified Network Topology with ISA Server

Within the internal prototype network, Figure 4 shows the login page for Outlook Web Access. This particular type of user interface requires the user to know his or her network's domain name in addition to their username and password combination. Also featured is the ability to choose what type of client the user is and where the user is logging in from for security measures. To have this type of login, forms-based authentication must be enabled, and it requires an secure socket layer (SSL) connection between the user and network. When accessing OWA from an external network or computer, the user must have a smart card reader by ActivIdentity and his or

her respective CAC prior to accessing the page. Upon authentication, the user's inbox will resemble and have most of the features in Microsoft Outlook.

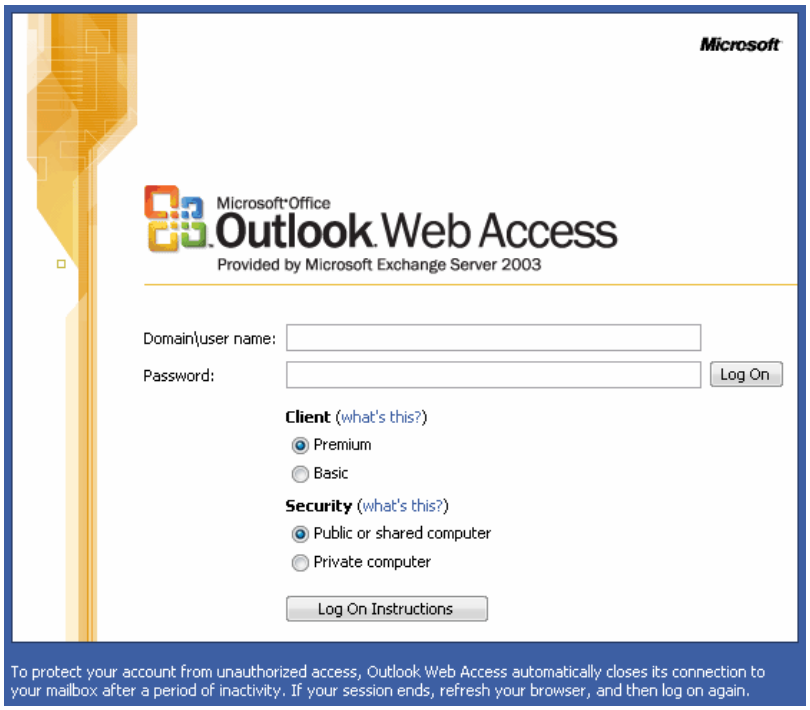

Figure 4: Sample Outlook Web Access login

On the prototype network, there are several ways for a user to access his or her email. One method is to be locally logged onto the network and utilize Microsoft Outlook to access his or her mailbox from the Exchange BE server. The second way is to access the OWA page internally from the network, which requires only a username and password combination. The last method is to access the OWA page from a computer external from the network.

In order for a user to access his or her email from an external computer, he or she needs a smart card reader and his or her respective CAC as seen in Figure 5. The user will first need to type

the OWA URL into an Internet web browser. Then the ISA server will then request the client's certificate, which is supplied by entering the CAC's PIN. The ISA will validate the SSL client certificate with the DC and check if the certificate is not on the DoD's CRL. Simultaneously, it will request for a Kerberos ticket under the client's name to use the Exchange FE. Once confirmed, the ISA is trusted to access the Exchange FE and gives a ticket. The ISA will send a request to the Exchange FE using integrated authentication with the ticket given by the DC. The Exchange FE will check the ticket provided b the ISA, look up the user's mailbox, and request a ticket to use the Exchange BE. The DC will also confirm if the Exchange FE can be trusted to access the Exchange BE and give it a ticket. Using the ticket given by the DC, the Exchange FE sends a request to the Exchange BE with the client's mailbox using integrated authentication. The Exchange BE then validates this ticket and sends the client's mail to the Exchange FE mailbox. The Exchange FE will render the OWA HTML page containing the client's mail and sends it to ISA. Lastly, the ISA sends the rendered OWA HTML page with the client's email to the client.

The reasoning behind using Microsoft products is to adhere as closely as possible to the technical specifications for the CGDN+ as set forth by TISCOM. In addition, Microsoft products fulfill the project's requirement of using COTS products. With similar configurations, problems experienced during installation can be identified and resolved prior to a service-wide implementation.

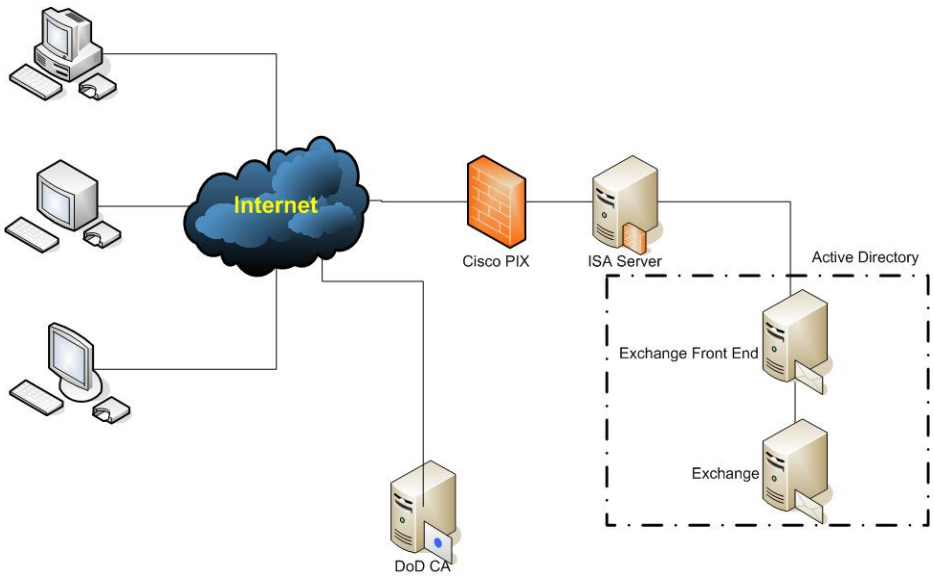

Figure 5: Mail Flow Diagram

Synopsis

The developed prototype network uses COTS products to fulfill the project requirements. The COTS products can be subdivided into two components, hardware and software. The hardware utilized is a Cisco PIX firewall with SSL VPN capabilities. Microsoft Windows Server 2003 and Windows XP are the software loaded onto the servers and client computers respectively. The CAC authentication and OWA will be implemented in the upcoming semester.

Results

The project's primary objective to provide a proof-of-concept design had been achieved with the development and configuration of the prototype network. However, the project did not verify and determine whether the CAC is an effective method to authenticate to OWA due to two major shortcomings. The second objective to conform to government policies concerning secure network access had been also achieved this semester. For example, all internal and remote

access user logon procedures had a minimum of two-factor authentication, which conforms to the Coast Guard technical security specifications. An in-depth explanation of the project's accomplishments, difficulties, and recommendations of possible project deployment for the Coast Guard will be described in the following section.

The first major accomplishment is the development of a basic prototype network. This accomplishment alone fulfilled the functionality level of the project requirements in Appendix . One example of the functionality level goals met is the implementation of the hardware-based Cisco PIX firewall with SSL VPN capabilities.

The second major accomplishment is that all network users have the capability of composing and receiving emails internally. This also includes the ability for users to utilize the internal OWA web portal. To be able to access OWA form a computer external of the network, a domain name is required. With the assistance of the U.S. Coast Guard Academy's Information System Division, the pece.uscga.edu domain was obtained, which is the project's third major accomplishment.

The testbed network's configuration presented two major shortcomings: a lack of both inbound Internet traffic and the establishment of a Public Key Infrastructure (PKI). These problems are the main reason why the authentication goals were not met this semester. Access Control Lists (ACLs) allow or block information from being passed to and from a network's servers and an external network. The PIX was configured to pass all information requests on port 80 (standard port for HTTP traffic) from the Internet to the Microsoft ISA server. The ISA server, in turn,

would attempt to authenticate the user with the public certificate offloaded from the user's CAC and continue to either block entry to the network or allow the user to access the OWA web portal.

The problem in the firewall lies in the network configuration. NAT, or Network Address Translation, reconfigures the return IP address of packets sent out through multiple networks. Since the IP address of a computer on an internal network may not be visible to a router outside of the network. Under NAT, a router assigns its external IP address (that is seen by other routers outside the network) to packets coming from computers within its network. Therefore, computers that are not directly connected to the user's network will be able to send back packets of information that will follow the daisy chain of IP addresses assigned to the original packet. Under our determination, the PIX firewall was incorrectly set up to handle NAT. This led to the misrouting of packets from the Internet back into the internal network. Packets sent from client computers on the Internet arrive at the outside interface of the PIX, but are internally misrouted and never reach the intended recipient.

Consequently, users are not able to resolve the address pece.uscga.edu and cannot login to the network. The user, instead, will receive an error on their Internet browser indicating that the website is temporary unavailable and/or the connection has timed out. By not having the capability to login to the network, users could not be verified with their CACs and could not access their email. These problems are the main reason why the authentication level goals were not met this semester.

Although the project did not fulfill the authentication level requirements, the lack of a proof-of-concept design should not hinder the Coast Guard from pursuing OWA and using SSL VPN technologies. The reasons why the Coast Guard should pursue OWA is to increase mobility in effective communication and to offer another solution for Coast Guard members and civilians to "work-on-the-go". The OWA web portal affords users the ability to check and send email instead of using a remote desktop program to obtain all programs and files attached to their user profile on the network. Moreover, it would be quicker in terms of logging onto the network and simpler than using a RAS token.

The foreseeable need for an alternate method for easy, remote access to email can be resolved by deploying OWA on the CGDN+. Currently available are two options for deploying OWA in a network infrastructure: (1) to use a smartcard, or CAC, logon and (2) to solely utilize the username and password combination. As previously described, the other military services have already implemented the CAC for authentication onto their respective networks. Thus, the first option has been proven successful by DoD. The United States Army is the most recent military service to have implemented CAC authentication on their network. In a whitepaper dated August 2006, Cisco Systems engineers created "a solution for implementing DoD PKI on [Cisco hardware] with the CAC and Active Directory smart card logon" [[14]]. Enabling the CAC logon of OWA will also complement the Coast Guard's transition to CAC workstation logons. The second option for OWA deployment is at present being used by academic institutions such as the United States Coast Guard Academy and corporate organizations. Regardless of the what option

is pursued, the benefits of convenient, simple email outweigh the imposed network threats and vulnerabilities.

Conclusions

The project sponsor, TISCOM, has identified the need for an alternative method to access email on the CGDN+. Thus, the project's main goal is to provide a proof-of-concept design to determine whether the CAC is an effective method for authentication in accessing OWA. The primary technology used to accomplish this goal is to establish a connection between the client computer and the Exchange server is a SSL VPN. The project culminated with the development of a testbed network, which simulates the CGDN+ on a simple, basic level, enabling network users the ability to send and receive email internally, and acquired the pece.uscga.edu domain. The testbed network uses a Cisco PIX firewall with SSL VPN to provide the project's "bridge" between the server application and the user and implements Microsoft's ISA server to upload the DoD's CRL daily.

Future project work could focus on implementing the prototype network to re-configure it for ROSCOE, a Real-time Offline Simulator of the Common Operating Environment. It is a virtual lab environment representing the current configuration currently deployed in the CGDN+. By using ROSCOE, OWA can be activated, and an evaluation can determine whether an SSL VPN can connect to it with a SSL VPN.

The project's benefits to the Coast Guard are incredible. With the project merging into the .MIL environment, the potential exists for Coast Guard personnel to not only access email from any Internet-enabled computer, but also implement SSL VPN technologies to access other high-priority applications. The other military services have utilized the CAC's capabilities combined with VPN technology to create secure, seamless web interfaces, but the Coast Guard has not reaped these benefits. By providing an alternate and secure means to access the .MIL email, all Coast Guard personnel can have the capability of accessing their email regardless of their location. Not only will the project open doors of opportunity, CAC and SSL VPN may change the perception that the Coast Guard can keep abreast with the current computer technologies.

References

[1] Barr, Simon and Grant Wyman, “Secure Coast Guard Network Access.” (United States Coast Guard Academy, 2006), 1-3.

[2] Alshamsi, A. and T.Saito, "A technical comparison of IPSec and SSL," Advanced Information Networking and Applications, 2005. AINA 2005. 19th International Conference on, vol.2, no.pp. 395- 398 vol.2, 28-30 March 2005

[3] Kuhn, D. Richard, Vincent C. Hu, W. Timothy Polk, and Shu-Jeng Chang. 2001. Introduction to Public Key Infrastructure and the Federal PKI Infrastructure. NIST.

[4] United States of America. SPAWAR. DoD PKI Regional Conference. “PKI 101 – Introduction to PKI”, Microsoft PowerPoint.

[5] United States of America. Department of Defense. DoD Instruction 8520.2: Public Key Infrastructure (PKI) and Public Key Enabling (PE). Washington, D.C: 2004.

[6] United States of America. Assistant Secretary of Defense. Department of Defense. Public Key Enabling (PKE) of Applications, Web Servers, and Networks for the Department of Defense (DoD). Washington, D.C.: 2001.

[7] United States of America. Department of Defense. DoD Directive 8190.3: Smart Card Technology. Washington, D.C.: 2002. [online]: available from http://www.dtic.mil/whs/directives/corres/pdf/d81903_083102/d81903p.pdf; (accessed on 10 Oct. 2004).

[8] United States of America. Department of Defense. Common Access Card. Washington, D.C.: 2002.

[9] Nokia. June 2003. An Introduction to SSL/TLS.

[10] Weaver, A.C. "Secure Sockets Layer," Computer , vol.39, no.4 pp. 88- 90, April 2006.

[online] available from:

http://ieeexplore.ieee.org/iel5/2/33950/01621007.pdf?isnumber=33950&prod=JNL&arnumber=1621007&arnumber=1621007&arSt=+88&ared=+90&arAuthor=Weaver%2C+A.C; (accessed on 12 Oct. 2006).

[11] Pitt-Catsouphes, Marcie, Judi Casey and Sandee Shulkin. Sloan Work and Family Research Network. Boston College. "Opportunities for Policy Leadership on Telework and Telecommuting." Policy Leadership Series – Work-Family Information for State Legislators, no. 3 (2005). [online] available from: http://wfnetwork.bc.edu/pdfs/policy_makers3.pdf; (accessed 15 Oct. 2006).

[12] Snader, Jon C. 2005. VPNs Illustrated: Tunnels, VPNs, and IPsec. New York: Addison Wesley Professional.

[13] Overview of Designing the Active Directory Logical Structure." Microsoft Corporation. [online]: available from http://technet2.microsoft.com/WindowsServer/en/library/2bd36720-ed2e-47ed-a80d-fa43a403b4361033.mspx?mfr=true; (accessed 11 Nov. 2006).

[14] Cisco Systems, Inc. "Department of Defense: Adaptive Security Appliance Common Access Card" (2006), 1-2.

Bibliography

Bhatt , Deep Vardhan, Stefan Schulze, and Gerhard P. Hancke. "Secure Internet Access to Gateway Using Secure Socket Layer," IEEE Transactions on Instrucmentation AND Measurement 55, no. 3 (2006).

Burr, William E., W. Timothy Polk, and Donna F. Dodson. "Draft Recommendation for Electronic Authentication." NIST Special Publication 800-63, Jan. 2004.

Cooke, J.C. and R. L. Brewster. "The Use of Smart Cards for Communication Systems Security." (Aston University, U.K.).

E-Government Act of 2002. 24 Oct. 2006. Hr 2458. Sec. 2. 2-3.

Komar, Brian. Microsoft Windows Server 2003 PKI and Certificate Security. Redmond: Microsoft, 2004.

McBee, Jim and Barry Gerber. Microsoft Exchange Server 2003. San Francisco: SYBEX Inc., 2004.

"Public Key Infrastructure." Defense Information Systems Agency. 24 Oct. 2006. Department of Defense. 22 Jan. 2006. <http://iase.disa.mil/pki>.

Russell, Charlie, Sharon Crawford, and Jason Gerend. Microsoft Windows Server 2003 Administrator's Companion. Redmond: Microsoft, 2003.

United States of America. Assistant Secretary of Defense. Department of Defense. Public Key Infrastructure Roadmap for the Department of Defense. 2000.

United States of America. DoD Public Key Infrastructure Program Management Office. Department of Defense. X.509 Certificate Policy. U.S. Government Printing Office, 2005.

United States of America. Deputy Secretary of Defense. Department of Defense. Smart Card Adoption and Implementation. 1999.

United States of America. Government Services Administration. Smart Card Policy and Administrative Guidelines. 2000.

United States of America. National Institute of Standards and Technology. Department of Commerce. FIPS-201. Personal Identity Verification (PIV) of Government Employees and Contractors. Technology Administration, 2005.

Appendices

Appendix [A] Project Plan

Appendix [B] Requirements Document

Appendix [C] Support Plan

Appendix [D] Test Plan

Appendix [E] System Design Specifications