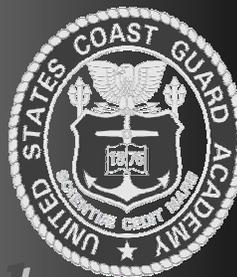


New for 2006!



# Senior Design Project in Electrical & Computer Engineering



## Secure CG Networks Access

Cadets: 1/c Grant Wyman 1/c Simon Barr

Advisors: LCDR Joseph Staier LT Joseph Benin

Sponsor: TISCOM

### Project Background

Access to the Coast Guard .MIL network has historically been the source of frustration for members who are operating away from their home units. This is because there was no standardization of usernames or email throughout the Coast Guard enterprise. This has recently been solved by migration to Microsoft Exchange Server 2003 and standardization of member access to the network. The Coast Guard is now looking for a way to allow network access for all members from any location. This must be done in accordance with very high measures of security to comply with both Department of Homeland Security and Department of Defense standards.



The DoD already has infrastructure in place to use CACs to secure data. CACs can be used for many tasks, from logging in securely to sending secure e-mails.

One way to obtain this level of security is through the use of digital certificates for public key cryptography. Since the late 1990's the Department of Defense has been developing Public Key Infrastructure (PKI) which provides and manages certificates for public key cryptography. The certificates are used to identify the individual named in the certificate, and bind that person to a particular public/private key pair. This has the effect of allowing anyone using a secure network or network resource to unequivocally prove that they are in fact who they say they are which in turn guarantees complete network security assurance. PKI provides the data integrity, user identification and authentication, user non-repudiation, data confidentiality, encryption and digital signature services for programs and application, which use the network.

PKI certificates are already issued in the Coast Guard thanks to the Department of Defense Common Access Card (CAC) which is the standard military identification issued to every member of the Coast Guard. The CAC contains an integrated circuit chip which has PKI certificates stored on it.

### Project Plan

This project will compare and contrast legacy Coast Guard implementation of remote network access to the standard DoD CAC authorization method. Each method has differing levels of security, compatibility, usability, and financial implications that need to be addressed before permanently adopting one system. A major part of the project will involve setting up a test-bed system to issue, manage, and accept certificates; enabling such functions as web-based e-mail access and remote logon capabilities. Since the commercial sector has also started producing similar products, several competing commercial systems will also be included in the examination.



PKI can be used to secure data transmission within the Coast Guard network and without.

### Project Deliverables

The project will deliver the design for a working system combining network access hardware and software. The hardware will be required to house and read the security certificates and read the certificates. The software will be required to process the security information and enable secure data exchange. This system will be implemented on the CG Academy .EDU network and a plan for migration to CG .MIL network will be provided. The system will conform to CG, Department of Homeland Security, and Department of Defense security policies.

### Project Work

- This project requires the study of government security policies, cryptographic functions, and security infrastructure.

- We will construct a small scale server-client network using Windows Server 2003® with security functions being provided by the CAC and PKI certificates. Initially the system will provide secure remote email access. Eventually it will allow for remote access to all SWIII functions. The lessons learned from the first implementation will be used to migrate the system onto the Academy .EDU network for further testing on a much larger system.



The process of public key cryptography is fairly straight forward. A sender encrypts the transmission with the receiving party's public key and sends it. The receiving party is the only one who has the private key able to decrypt the message.