WI-FI TISCOM:
Wireless Access and Security

Final
Project Report

Cadet 1st Class Mark Bruno

Project Advisor: LT Todd Moyer

Projects in Electrical & Computer Engineering
United States Coast Guard Academy
26 April 2006

WI-FI TISCOM

Cadet 1st Class Mark Bruno

Project Advisor: LT Todd Moyer

Projects in Electrical & Computer Engineering
United States Coast Guard Academy
26 April 2006

ABSTRACT

Currently, the Coast Guard does not have a wireless computer networking solution for service-wide implementation. The Coast Guard Telecommunication and Information Systems Command (TISCOM) has begun development of a model design, which can be scaled and modified for implementation at any Coast Guard unit with a justifiable mission requirement for wireless connectivity. The Coast Guard Academy Electrical and Computer Engineering Section is assisting TISCOM in the development of this system by setting up a test network, and conducting testing of the concept. Designing this solution requires use of the latest secure networking and monitoring technology. After spending a semester researching and evaluating network component specifications, ordering required equipment, and planning to implement the network and commence testing, the project produced a wireless network local area network design. During testing the solution met or surpassed the promulgated security standards, and the design was submitted for final approval. Once approved, the design will be the Coast Guard Standard for wireless networking.

INTRODUCTION

The use of wireless technology to access computer networks and transfer information is becoming more widespread in both the private and public sectors [1]. For the 2006 fiscal year, estimated revenues for Wireless Local Area Networking (WLAN) will surpass $5.2 billion worldwide [2]. This figure is almost $2 billion more then estimates made in 2002 [3].

Benefits

Wireless systems improve access to information. A study conducted in 2003 by Cisco Systems and NOP World-Technology estimated employees are 22% more productive; utilizing 1.75 hours more *per day* for work across a WLAN connection [4]. WLAN solutions can also reduce costs and latent time in network deployment and upgrades. A single access point can support upward of 100 connections, be wired to a highly accessible area, and be modified to support changing network needs [5]. Wireless network also allows several types of data to coexist and for users to roam throughout the covered area while retaining connectivity to the network resources.

Risks

Unfortunately, the use of wireless systems also result in an increased security risk tied to unauthorized access to Coast Guard systems [5]. Wireless devices are equipped with radio transmitters, broadcasting information to the network. WLAN transmissions are broadcast in the 2.4 Gigahertz or 5 Gigahertz license-free broadcast frequencies [6]. These bands may be monitored by anyone with a reciever for those frequencies, and are used for several types of short range wireless devices, including portable home phones. If specific precautions are not taken, an unsecured wireless network is extremely vulnerable to access from users outside the authorized group. The potential for loss of information and network services is also great. Malicious, or rogue, devices or users can prevent access for authorized users, highjack connections, and steal information passed over the airwaves. Limitations in radio broadcast and wireless technology restrict the available bandwidth, making the network subject to denial of service overloading, effectively consuming all the bandwidth available and halting network traffic.

Project

I will be working with the Coast Guard Telecommunication and Information Systems Command (TISCOM) to implement a "best-practice" wireless solution for the Coast Guard. The "best-practice" design process uses the latest applicable technology, combined with extensive planning and testing, to produce a standard. Once perfected, the Coast Guard could use this base model on a case-by-case basis at units which demonstrate a need for a wireless solution. Such stations include temporary offices on a larger base, small boats and short range cutters. Using planned wireless implementations the Coast Guard can provide secure network connectivity in emergency situations on shore, as part of the Incident Command System. These units can all benefit from having users free to move throughout their workspaces without the need for an network plug.

In the secure military network system, the .mil environment, extra considerations must be given to enhance security and network access. Current Coast Guard policy utilizes Microsoft Active Directory user management and hardwired encryption. A user must be authenticated, or accepted by the network controller, to access network resources, but additionally, wireless authentication must be possible. To ensure a computer and its user are both eligible to access the network wirelessly, several additional layers of security are involved in user logon. Protecting information once a user is authenticated also presents problems, as radio transmissions are more difficult to manage.

Paper

Proper planning and testing before the deployment of a wireless system is also part of the best practice development process. This paper addresses the research and design process used to create the best practice system that meets the Coast Guard standards and can provide the benefits of wireless. The first step involves understanding the current standards for Coast Guard computing, and then looking at how wireless solutions can be integrated into the existing infrastructure. Lastly, it covers the design and testing of a system that meets the information assurance requirements, and briefly explores some potential for future research for wireless implementations in the Coast Guard.

OBJECTIVE

Proof of Concept

The project was driven by several general goals, which are outlined in the Project Plan, included in Appendix 1. The increased productivity, mobility, and ease of use make the use of wireless technology attractive. This project establishes a proof of concept, presenting a wireless solution which meets the Department of Homeland Security and Coast Guard CG-6 requirements. There are minimally manned, remote units which could benefit from the use of secure wireless. One example is temporary site installation. "Last mile" wiring is a term which describes the extensive wiring runs that connect users from their workstation to the network. This segment of wire tends to be the most expensive and the most difficult to install, as it requires one branch of every user device. Small boats and shorter range cutters could also be included in wireless networks.

Coast Guard Wireless Standard

The goal of this project is to provide TISCOM with a base model from which to work. We are also testing the security requirements drafted by CG-6. The solution will be guided mainly by Draft Command, Control, Communications, Computes, and Information Technology (C4&IT) instructions. These standards outline management and technical considerations in order to successfully implement wireless network in the Coast Guard, including configuration instructions and administrative controls which must be used [7]. This solution will be a small scale test network, accessible from TISCOM for remote access management efforts, and by a small user base at the Academy. However, once the C4&IT standards are completely tested and authorized, the validated network configuration will be part of the TISCOM inventory for deployment where they deem necessary.

The wireless solution developed will be a model for networking remote sites or special cases. To date, ESU Baltimore and Headquarters have implemented wireless networking solutions; however, these solutions are not acceptable at the enterprise level. The cost and maintenance required for these systems preclude them from use by most units. The solution developed at CGA is being designed to be scalable, so the size can be adjusted at the site as the need dictates. If a site is eliminated, or receives more users, these changes can be managed within the existing infrastructure. The solution will also be repeatable. It will be implemented for sites with

justifiable needs or barriers to wired networking and the implementation and administration will be the same for all sites.

Security

The security provided by this solution must meet Coast Guard Information Assurance (IA) standards [7]. To meet the standards, the wireless solution must support wired security measures for user authentication, including "strong passwords," and data encryption. These precautions include the use of high end encryption algorithms, based on the Advanced Encryption Standard, and utilizing the most secure cryptography standards available [8]. The 802.11 standard from the Institute of Electrical and Electronics Engineers addresses all wireless technology. The 802.11i standard, completed in 2004, is the highest security protocol, designed to concentrate on enterprise security concerns [9]. The 802.11i standard is a required compatibility standard for this project.

802.11i meets several basic security needs. The security protocol preceding it was Wired Equivalent Privacy (WEP). WEP was found to have several severe security flaws and was deemed unusable for enterprise security. While the 802.11i standard was being completed, the Wi-Fi Alliance developed Wi-Fi Protected Access. This is a scaled version of the 802.11i standard and implemented several of the key features [10] [11]. The final standard implements 802.1x authentication, including use of the Extensible Authentication Protocol, discussed in detail later, and includes the Counter Mode with Cipher Block Chain Message Authentication Code Protocol, or CCMP. The CCMP is built around the Advanced Encryption Standard required from the Federal Information Processing Standards 140-2 [12].

The proper operation and administration of the wireless solution is a vital part of secure operation. My project will also concentrates on various network monitoring tools and security controls to address the new vulnerabilities that a wireless network segment creates. Evaluating the new security hazards created by adding wireless, and finding any existing issues will bolster the entire network. This portion of the project is still fairly vague, as the security evaluation is still under development. Several protocols and specific products have been recommended, however, an appropriate choice can not be made at this time.

Wireless networks can be used to augment or supplant wired user systems. Complete replacement of wired systems is not feasible at this time. It is a gross waste of money to remove entire wired networks, and even the wireless solutions are connected to Ethernet or fiber as a link in the system. Additionally, the large bandwidth required to provide file sharing and some streaming media services have been attained by wireless transmission. The 802.11i standard builds on the existing 802.11 standards, providing connection speeds from 11 Mega Bytes per second (Mbps) to 54 Mbps., depending on the network implementation.

Wired network traffic is sent out across an Ethernet wire plugged into the machine to a switch. The switch uses the hardware, or Media Access Control, address from the packet of information and routes the packet to the corresponding receiving device. The basic operation of a wireless network follows the same rules; however there are several notable differences.

General Wireless Networking

In lieu of a CAT5 network cable running from the computer into the wall, each machine intended for use on the wireless network must be equipped with its own wireless transceiver. This device can be a Universal Serial Bus device or an installed card. This card is a radio transmitter, broadcasting the signal from the workstation to the wireless access point.

Access Points

The Access Point (AP) is a second wireless transceiver, connected via CAT5 or fiber optic connection to a network switch. The access point is the contact node for the network users. Most home application access points are wireless routers, allowing both Ethernet and wireless connections. An access point broadcasts and receives packets over a specific area, creating a "hotspot" or wireless enabled location. The access point then connects to the switch, providing a connection for many users at a time.

Project Execution

I spent the majority of my time finishing the details of the design and testing. TISCOM provided significant direction concerning the way the solution must work, but allowed sufficient latitude to select components to fulfill the requirements, detailed in Requirements Document in Appendix 2. Once the design was completed, LTjg Lars McCarter, my TISCOM point of contact, and I worked out a formal test methodology, attached in Appendix 3. This test methodology addresses security concerns of the wireless system, including physical security and signal availability and security. We also spent time

ensuring that the wireless system could be administered by TISCOM remotely. By considering and testing several variations of the system, we assured the solution reached, fulfilled all the requirements from TISCOM and provided the best possible solution. I spent the first semester of this year researching the available products and concepts behind the operation of a secure wireless network. Early this semester parts arrived and configuration testing took place. Once the network was stable, we were able to execute the test plans. The final design has documented and submitted to TISCOM for approval. Once the design has been vetted, further research can be done, and initial sites for deployment can be considered. Initial discussions have indicated that areas affected by Hurricane Katrina might be prime field test locations.

SYSTEM DESIGN

To effectively design a solution for the Coast Guard, the issues surrounding user authentication, data encryption, and remote management must be addressed. Implementing the appropriate physical layer is the first step towards creating a network which meets all the requirements.

Secure Wireless

Access Points

The Cisco 1130 Access Point (APs) provided the most robust and cost effective answer to the security and encryption requirements from TISCOM. These APs can be used in enterprise implementations and broadcast both 2.4 GHz and 5 GHz signals. This model is capable of handing between 30 and 100 users per AP. This provides flexibility needed for scaling the specific network instance. These units are capable of utilizing power over Ethernet, using the dormant conductors in a CAT5 cable to provide the AP with power [13].

The AP can be operated autonomously or in a lightweight mode. Autonomous operation uses native Cisco programming to manage each access point. The lightweight mode seeks a management unit for configuration and security policies. This removes the configuration from the single AP level. The management functions for a Cisco Lightweight AP reside on a Wireless Local Area Network (WLAN) controller.

Alternatively, the Cisco 1000 series lightweight access point can be used. This access point does not support all of the same functionality the 1130 does, but it can still provide the services required and integrates well with the other wireless components.

WLAN Controller

The 2006 controller is part of the Aerospace product line available from Cisco. This device is responsible for system wide wireless LAN functions, such as security policies, intrusion prevention, RF management, quality of service, and connection establishment. They work in conjunction with Cisco 1130 Series Access Points and the Cisco Wireless Control Server (WCS) to support business-critical wireless applications. The WCS application further centralizes the wireless configuration management. These units connect to the switch to interface with the APs. The controller firmware supports a web interface for easy management [14].

Switching

After reviewing several types of switch, I chose the Cisco 3750 for the Academy network. It provides different features from the switches used at TISCOM and allows us to compare another piece of the infrastructure. The 3750 provides a scalable design and smart switching. The fixed configuration switch utilizes the Cisco IOS programming. The switch can be purchased with the IP Base or IP Services licensing. We will be using the IP Services license due to its routing capacity, web interface, and several enterprise-class management features

These switches also support Cisco Stack-Wise, a scaling feature which allows multiple switches to be combined and managed as a single oversized switch. A master switch is selected and any additional switches are slaved to that switch. This meets the requirement for scalability, by allowing network administrators to build any size implementation for any size unit.

The Cisco 3750 switch is also capable of providing Power over Ethernet (PoE). While this in not a project requirement, the investment in PoE technology can serve to further reduce the cost of a wireless implementation. Current Ethernet data transmission uses only two of the four pairs of conductors in the CAT5 cable. The other two pairs can have a DC voltage inserted by the switch or a power injector, a device which connects to the cable for the sole purpose of providing power. A device which can accept Power over Ethernet or a separator allows for one Ethernet cable run to a given device, carrying both power and data [15].

Network Services

In a full implementation of a wireless solution the entire .mil network would be available to a wireless

user. Wireless networking has no effect on operation of e-mail, internet use, file and print services once it has been successfully integrated into a wired LAN.

The testing network will not provide all of these services, but important sever processes; including user database management and authentication will be installed. Secure authentication requires that a new user be authenticated into both the network resources and the wireless infrastructure. Cisco Access Control Server (ACS) will be providing interface for this authentication. Using Active Directory, the Coast Guard standard user management database, ACS receives the user's identification and password from the WLAN controller, and then authenticates the user as if they were working over a wired connection. If the user is authenticated to access the network, ACS will also authenticate the user for wireless connection, and the encrypted connection will be initiated.

A detailed picture of the authentication process is available in Appendix 4, as it is beyond the scope of the discussion here. The most effective protocol is the Protected Extensible Authentication Protocol, PEAP. It uses several authentication methods to assert pre-loaded credentials for the server, at the client machine, which allows the two machines to pass the encryption key to the authenticated user. This is a highly attractive option for enterprise solution [16]. For the proof of concept we implemented PEAP encryption.

The last piece of the secure networking solution is access to the other military networks and Internet resources. This access will be over the Coast Guard Data Network Plus (CGDN+). This is a data network maintained solely for the Coast Guard to pass data and voice traffic. The connection to this Wide Area Network is vital to the WLAN, so as to share network applications and services.

RESULTS

The configuration and design testing dominated the majority of the work I did this semester. Using the network topology I designed last semester, I was able to work with TISCOM to implement a network which surpassed the required standards and test it before trying to attach it to the .mil network.

There were several considerations to make while designing the network. Ensuring the wireless design was secure and available to the users was of utmost importance. Ensuring the administrative workload was acceptable developed into a secondary goal as the project progressed.

Authentication and Encryption

The Coast Guard Active Directory user database is the Information Technologies standard for large organization user management. This constrains the solution to compatible components. The Cisco ACS software provides seamless integration between Active Directory and the wireless clients. This software has, however, proven to be difficult to register users. It requires that a user name be entered to search the Active Directory entries. The only concern with this entry method is considering the number of users at a unit where the solution might be deployed. If larger sites were to adopt wireless, it would generate a larger, more demanding administrative load. A better integration system between Cisco ACS and Active Directory may address this issue, allowing users to be entered centrally and user accounts to be globally available.

In addition to the ACS software, the Coast Guard is currently evaluating the most effective way to implement two-factor authentication, where two separate factors are used to authenticate a user in the .mil domain. In this case, the Coast Guard uses a two-factor method requires that the user know something, their private password, and have something, their personal military identification card. The final implementation of this project will be robust in its ability to incorporate the two-factor authentication technology. As new technology is developed, authentication continues to improve.

The authentication process directly supports the encryption process. Protected Extensible Authentication Protocol encryption uses server certificates to allow the client to ensure the server is trusted and to create an encrypted tunnel which allows for secure transfer of logon information. Once the user is authenticated, another shared, secure key is traded through the already encrypted tunnel, and creates another tunnel for the user session. Using this method of encryption invalidates many type of attacks used to disable or penetrate wireless networks.

Remote Management

The Active Directory structure also facilitates the remote management goal for the wireless network. Once the configuration is accepted and deployed; TISCOM will be able to manage access and troubleshoot user issues remotely. The WLAN controllers and the Wireless Control Software will allow TISCOM technicians to troubleshoot the hardware systems.

Also under consideration is the Simple Network Monitoring Protocol (SNMP). The SNMP allows a network administrator to see vital statistics about network use, manage network segments, and consolidate all the information about the data transmission into one interface. Use of a monitoring and statistic tracking suite could enhance the remote management capabilities. It also supports the TISCOM change management policies. This protocol could be used to augment both the wired and wireless segments of the network. Accurate monitoring and reporting of network statistics and operation is vital to information systems decision making, and to evaluating the performance of the wireless solution.

Wireless Design

Using the components discussed in the system design section of this paper, I was able to complete the design of the network segment required to operate wireless at any Coast Guard unit. This scaled, proof of concept design is shown in Figure 1, adjacent. The final design utilized a converted workstation to support the Access Control Server, which would not be a regular practice, and the switch and access points originally selected

Several other options were weighed as I learned more about the Cisco products available for wireless networking. The wireless LAN controller was used, but other models were also available and could be substituted. The controller can manage a maximum of 6 APs. There are Cisco Wireless Solution Engines capable of supporting wireless solutions for the entire Coast Guard. Several other options were also being investigated by TISCOM engineers, including AirFortress custom solutions. Once the entire design was completed in itself, the environmental factors and several other external factors were taken into consideration, shown in Appendix 5.

CONCLUSIONS

Potential

This solution will save the Coast Guard time and money. This network segment could be added to the inventory at TISCOM and be deployed to select units and locations. The proof of concept project was successful, creating a network solution that meets the requirements. However, the completion of my project has uncovered other ideas which may create a better solution for the Coast Guard, but do not meet all of the requested requirements. Further research and testing of alternative solutions is recommended. The technologies currently available will be improved and using the best available technology provides the most effective defense and security.

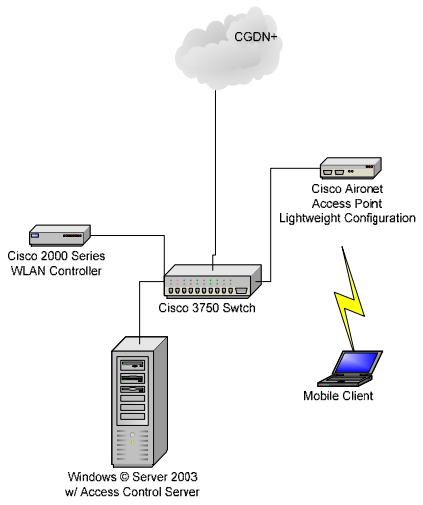


Figure 1-Academy Based Test Network

I would recommend using a Wireless Solution Engine to support access points at every Coast Guard unit. As I studied the art and science of wireless networking, I came to realize that wireless is available everywhere, including many times in places where it doesn't belong. Using a USB wireless adapter and some surreptitious programming, any computer in any place, can become a wireless access point. Using an access point at every unit would allow wireless transmissions in any area to be monitored. It is fairly easy to configure an access point which will allow monitoring with out providing wireless services. In addition to monitoring wireless transmissions at every unit in the Coast Guard, there are many units which would benefit from wireless installations.

This solution would not be the next iteration of .mil networking, rather a tool to overcome problems with installing a wired network. Temporary or emergency relief sites, set up on short notice and removed after the mission is complete, would be more effectively implemented with wireless. No longer would the site need to be pre-wired, any building could be provided with connectivity for any length of time. Office trailers or satellite offices on a larger Coast Guard installation would no longer need their own infrastructure, only a wireless connection to another

building. Providing remote sites with "last mile" access by implementing a wireless connection could vastly reduce the costs associated with cable trenches and lessen environmental impact. The research into these concepts is not complete but the potential for wireless to improve Coast Guard mission readiness is tangible.

Ongoing Efforts

Now that the proof of concept had been completed, the finalized solution will be submitted and reviewed. If accepted, it will be available to implement soon afterwards. Sites like ESU New Orleans, the Academy, and several major headquarters units have expressed interest in wireless capabilities.

Installation and testing of these systems is priority one. This proof of concept project provided a baseline, and further testing and field deployment will refine the design. Also planned for the near term is a deployment of wireless capabilities at the Coast Guard Technical Expo in Tampa, Fl over the summer. This unveiling of the system will be used to test security and user interest.

Also, the examination of related technologies, like SNMP and wireless collaboration tools, is advisable. Once a secure technology to support them is in place, their use can only serve to improve Coast Guard mission readiness. As the Coast Guard moves towards a more network-centric operations plan, the state of the .mil network will become even more important.

There are several other ideas which have developed throughout this project, and mentioned in passing in this paper. Providing a wireless solution lends a new adaptability to the networks we currently use, and create opportunities that did not exist before.

Using antenna specifically designed for long range lobe broadcasts, it would be possible to build shore side stations which could beam highly directional signals to cutters nearby, using GPS or VHF direction finding positioning techniques.

Incident Command Centers could be implemented with wireless connections to assist responders and command establishment more timely and efficient. This same premise applies to establishing temporary offices, either in the field or on a Coast Guard base.

The economic benefits of implementing new networks with wireless are also a consideration. As the service expands and fills needs in new areas doing new missions, we are extending our infrastructure too. Last mile access, being the most expensive part of new installations could be lower using wireless.

Wireless is becoming an industry standard, but currently the Coast Guard is not poised to take advantage of it. Using this baseline design Coast Guard Information Technology staffs can improve productivity and mission effectiveness. Setting the baseline standard is an integral first step to proper development of wireless technology in the Coast Guard.

REFERENCES

Works Cited

[1] Cox, John. "Wireless Growth." Network World. July 2005. Available: http://www.networkworld.com/weblogs/wireless/009948.html. Accessed Oct 05.

[2] Cox, John. "Wireless apps growing in popularity." Network World. November 2004. Available: <http://www.networkworld.com/weblogs/wireless/006866.html>. Accessed Nov 05.

[3] Lawson, Stephen. "WLAN use growing fast, researchers say" Network World. August 2002. Available: http://www.networkworld.com/news/2002/0801wlan.html. Accessed Nov 05.

[4] Rowley, Patrick. "Wireless LAN's: When and Where." INS Whitepapers. September 2003.

[5] Cicso. "Wireless Support Resources." Cisco Product Support. <http://www.cisco.com /en/US/products/hw/wireless/tsd_products_support_category_home.html>. Accessed Dec 05

[6] Grier, Jim. "Making the Choice: 802.11a or 802.11g." Tutorials. April 2002. Available: <http://www.wi-fiplanet.com/tutorials/article.php/> Accessed Oct 05.

[7] United States Coast Guard Office of Command, Control, Communications, Computers, and Information Technology. Wireless C4&IT Systems Practices. Washington: CG-6, 2005.

[8] Information Technology Laboratory. Federal Information Processing Standards 140-2. Washington: National Institute of Standards, 2001. Pg iv.

[9] Chen, Jyh-Cheng, Ming-Chia Jiang and Yi-wen Liu. "Wireless LAN and IEEE 802.11i." Wireless Communications, 12.1 (2005) 27-29.

[10] Chen, Jyh-Cheng, Ming-Chia Jiang and Yi-wen Liu. "Wireless LAN and IEEE 802.11i." Wireless Communications, 12.1 (2005) 30.

[11] IEE 802.11i. Wikipedia. 27 Nov 05. <http://en.wikipedia.org/wiki/802.11i> Accessed Jan 06.

[12] Information Technology Laboratory. Federal Information Processing Standards 140-2. Washington: National Institute of Standards, 2001. Pg 12.

[13] Cisco Systems Inc. CISCO AIRONET 1130AG SERIES IEEE 802.11A/B/G ACCESS POINT. <http://www.cisco.com/en/US/products/ps6087/products_data_sheet0900aecd801b9058.html> Accessed Nov 05.

[14] Cisco Systems Inc. CISCO AIRONET 1130AG SERIES IEEE 802.11A/B/G ACCESS POINT. <http://www.cisco.com/en/US/products/ps6087/products_data_sheet0900aecd801b9058.html> Accessed Nov 05.

[15] Cisco Systems Inc. Cisco Catalyst Switch Guide. <http://www.cisco.com/en/US/products/hw/switches/ps5023/prod_brochure0900aecd80357ff4.html> Accessed Nov 05.

[16] Phifer, Lisa. "Deploying 802.1X for WLANs: EAP Types." Sept. 2003 <http://www.wifiplanet.com/tutorials/article.php/3075481> Accessed Nov 05.

References Reviewed

Cruz, David, LTjg USCG. Project Charter. Project Charter from TISCOM. 01Aug05.

APPENDICES

Appendix 1- Requirements Document

Appendix 2- Test Plan

Appendix 3- 802.1X Protected EAP Architecture

Appendix 4- Project Plan

Appendix 5- Support Plan

Appendix 1
Wi-Fi TISCOM-Wireless Access and Security
Project Plan
26Apr06

Purpose:

The purpose of my project is to work with the TISCOM engineers to implement and evaluate wireless solutions for the Coast Guard. Currently, the Coast Guard lacks a feasible way to deploy, support, and manage a secure, wireless enterprise solution.

The use of wireless networking technology is exploding in both the public and private sectors. Wireless networking facilitates increased productivity, lowers costs of connecting to networked resources and provides seamless communications. However, the increased risk of unauthorized access and loss/theft of information stored and transmitted over the network is of significant concern in the secure .mil environment. Extensive evaluation and assessment of authentication and protection technologies available is a vital initial step in the wireless rollout.

Organization

Project Sponsor: *Telecommunications and Information Systems Command, USCG*

Project Contact(s): *Mr. William Randall, TISCOM Project Manager*
LTJG David Cruz, TISCOM Project Engineer
LTJG Lars McCarter, TISCOM Project Engineer

Project Advisor: *LT Todd Moyer, USCGA Electrical Engineering Instructor*

Cadet: *Cadet First Class Mark Bruno*

Goal

My goal for this semester is to provide the TISCOM wireless team with a remote wireless test-bed and work with the TISCOM engineers to evaluate potential wireless solutions for use across the Coast Guard. Constructing a wireless access solution on the .mil network at CGA is the foremost deliverable.

This design is going to be submitted to TISCOM for approval as the Coast Guard wireless standard. The design will be documented, both hardware and software configurations, in a design submission made to TISCOM upon the completion of the TISCOM test plan. The plan is for the design to be presented at TISCOM and The Coast Guard Technical Expo over the summer.

Technical Challenges

Challenge 1:

- The first challenge is to combine the concepts used here at the Academy with the TISCOM design. Matching these networks and testing the resulting system is vital to designing the best possible wireless solution for the Coast Guard.

Challenge 2:

- The actual development of the network security test is going to be fairly time intensive. There are commercially available network security tests; however, the secure .mil environment requires a testing plan that more thoroughly addresses all security concerns.

Action Items/Responsibilities

1. Test Wireless Deployment at CGA-1/c Bruno

2. Generate and execute security test procedure-1/c Bruno and Project Advisor coordinated with TISCOM

3. Generate and submit all project documentation-1/c Bruno

Timeline

- Jan 30: CGA Testbed Design complete
- Jan 30: Security Test Plan Finalized
- Feb 10 TISCOM Security Survey at CGA
- Feb 20: Interim Authority To Connect requested
- Mar 01: Test-bed constructed on .mil network
- Mar 10: Security Test Plan Executed
- Mar 20: Draft Wireless Design Prepared
- May 14: Spring Project Presentation, Final Design Delivered
- May 14 Spring Paper/Project Notebooks due

Project Members:

_____ Date: _____

Project Advisor:

_____ Date: _____

Appendix 2
WI-FI TISCOM-Wireless Access and Security
Requirements Specification
26Apr06

Background: The purpose of my project is to implement and evaluate wireless solutions for the Coast Guard. Currently, the Coast Guard lacks a feasible way to deploy, support, and manage a secure, wireless enterprise solution. Working in conjunction with TISCOM, I am seeing to provide a model system which can be quickly deployed and activated in a variety of situations

The use of wireless networking technology is exploding in both the public and private sectors. Wireless networking facilitates increased productivity, lowers costs of connecting to networked resources and provides seamless communications. However, the increased risk of unauthorized access and loss/theft of information stored and transmitted over the network is of significant concern in the secure .mil environment. Extensive evaluation and assessment of authentication and protection technologies available is a vital initial step in the wireless rollout.

Problem Statement: Designing an enterprise level wireless solution is not as easy as developing a home wireless network. The infrastructure needed must be carefully planned, tested, optimized, and re-tested. Deployment of a system with even tiny faults can cause catastrophic damage to any network. Hijacked access points, denial of service attacks, and compromised network services all impact productivity and information security. If a military network were compromised, sensitive information would be at risk.

In an effort to properly test the wireless standards promulgated by the Coast Guard and Department of Homeland Security, several isolated test sites are being organized. TISCOM has established a central management site on their campus, CGA has been asked to provide one network segment, and ESU New Orleans may be used as another segment. Using these separate sites will allow complete testing for management and access features. It also allow for each site to make local adjustments. Implementing a wireless test bed system is the first step. Finding the system configuration which provides the best connectivity with the most security is next. Lastly, security, both internal and external, needs to be evaluated and appropriate an appropriate implementation made.

Requirements:

Level	Sponsor Need	Engineering Requirement	Justification
1	***Performance***		
1A1	Uninterrupted Connectivity	Self Aware Wireless Network	Self Healing compensates for system errors
1A2		Monitoring Capability	Simple Network Monitoring Protocol allows for remote management

			access to network devices
2	***Security***		
2A	Ensuring Authorized network users	"Strong" Authentication User Designations	Required by Ref. 1-WLAN.tech.21 & WLAN.tech.24 & WLAN.mgmt.11
2B1	Safeguarding Data	FIPS 140-2 Advanced Encryption Standard	Required by Ref. 1-WLAN.tech.7, .8, .9
2B2		IEEE 802.11i standards for all Wireless Devices	Required by Ref. 1-WLAN.tech.7, .8, .9
2C1	Signal Limitations	Physical Site Security	Required by Ref. 1-WLAN.mgmt.10 & WLAN.tech.1
2C2		Power Limited Signal	Required by Ref.1-WLAN.tech.1 , .25
3	***Functionality***		
3A1	Flexible Networking	Upgradeable Hardware	Required by Ref. 1-WLAN.mgmt.5
3A2		Flash Updates for firmware	Required by Ref. 1-WLAN.mgmt.5
3A3		Commercial off the shelf (COTS) software products	
3B1	Unimpeded Network Access	Live Update Anti-Virus Software	Required by Ref. 1-WLAN.tech.14
3B2		Standard Workstation III computer mages	Required by Ref. 1-WLAN.mgmt.8
3B3		Maximum Available Bandwidth in the Service Area	Required by Ref. 1-WLAN.tech.1
4	***Power***		
4A	Power to Access Points		
4A1		90-240 VAC Power	Product Requirement due to TISCOM product selection

References:

1) Wireless C4&IT Systems Practice Appendix A: Wireless Systems Configuration Requirements. Dated 27JUNE05.
2) Project Charter- WI-FI TISCOM.

Appendix 3
Wi-Fi TISCOM- Wireless Access and Security
Test Plan
26Apr06

Synopsis: Testing for the Wi-Fi project is proof of concept and standards acceptance testing. I will be testing to ensure the promulgated wireless standards can be met with a standard wireless networking solution. Testing physical site security, broadcast security and data security will be the three main phases.

Personnel: Using the remote access capabilities embedded in Windows and the domain management features in Active Directory, testing will be limited to 3 people or less. I will be onsite here and at least one TISCOM engineer will be at the TISCOM site. Phone contact and network connectivity between the two sites will be important. Each testing phase will begin on the phone- Both network segments must be connected and activated for testing to commence. TISCOM testing varies from local testing, and I will be running my local tests concurrently with TISCOM's efforts.

Procedure: The Academy test network is fully operation in the 10.10.1.XXX IP Address Space, using the test.bruno domain. It is connected to a DSL circuit to the outside internet, which will be replaced with a connection to CGDN+. The necessary .mil patch connection is provided in the lab, and once an Interim Authority to Connect has been approved, the switch which connects the wireless segment together can be connected to .mil network. CGA IS technicians will need to establish a server to run the necessary services and adjust the address space for the Academy test network. TISCOM will be utilizing the test bed at the Academy to complete their project, in addition to my tests here. My testing should take less then two days to complete. The TISCOM testing could take several weeks to find the optimal configuration. Once the remote management considerations and system configuration detail are finalized, the complete network solution will be recorded and submitted as the result, including the results of this test procedure.

Equipment Required:

1. *See Attached Inventory for Academy and TISCOM Equipment Lists*

Initial Set-up: Currently the Academy test network has a single Dell Optiplex Desktop machine running Windows© Server 2003, which provides Active Directory User Management, Dynamic Host Control Protocol, Domain Name Service forward lookup, and Cisco Access Control Server. This machine will be phased out of the network design, and replaced with a Dell server in the Academy Information Systems server closet. There is a second Dell Optiplex Desktop computer running as a wired LAN workstation. This work station will be replaced with a wired Workstation III laptop. Additionally, a wireless laptop workstation III will be used to test the wireless connection. The wired network segment contains the Cisco Wireless LAN controller, the access points, the wired laptop, and the server. All of the test network equipment is in Room 214, MAC hall, the Projects in Electrical and Computer Engineering Lab. The testing we will be doing will use the Coast Guards Active Directory domain and be controlled using the Cisco Access Control Server. The WLAN controller has already been configured to require EAP-LEAP authentication for users desiring a connection. Ensuring this works properly is part of the test.

Test # 1 – *Physical Site Security*

Objective: This test is intended to evaluate the security of the workstations, servers, and workspaces which are equipped with wireless networks.

Requirements:

Requirement ID	**Engineering Requirement**
2C1	*Physical Site Security*

Test Overview: This test does not require any use of the network or the wireless capabilities. This test will merely test the security of the system in its surroundings.

Test Procedure:

1. Enter Hamilton Hall. Check security (AKA-Shake Door Handles and Look around at IS Spaces)

Doors Secure?	
IS Spaces Access Limited (Locks/Personnel)	
Proper Security Warnings Posted?	

2. Enter Macallister Hall. Check Lab Security

Doors Secure? Cipher Lock Working?	
Lab Bench Properly Marked?	
Proper Security Warnings Posted?	

3. Check Switching Closet Security

Doors Secure? Lock working?	
Switch Cabinet Configured Properly	
Proper Security Warnings Posted?	

Results:

Test # 2 – *Signal Availability and Security*

Objective: This test is intended to evaluate the security and broadcast controls of the wireless networking equipment.

Requirements:

Requirement ID	Engineering Requirement
1A1	Self Aware Wireless Network
2C2	Power Limited Signal
3A3	COTS Solutions
3B3	Maximum Available Bandwidth in the Service Area

Test Overview: This test will move methodically through the intended service area, measuring available signal, for the Access Point to the limits of service. Once a reading at high power is taken, the configuration of the WLAN Controller will be adjusted to provide the best service pattern for the lab. These requirements also substantiate the use of Commercial off the Shelf products.

Test Procedure:

1. Using NetStumbler, ensure that the Wireless Network "MAC_LAB" is available. This may require the SSID broadcast to be enabled. To Enable the SSID broadcast, login to the WLAN Controller and toggle the "Broadcast SSID option" on.

2. Once the network is determined available, open Ethereal and set up a capture session on the wireless network card. Use a third party laptop with wireless capabilities to complete this step.

3. With Ethereal running a capture session; use a verified laptop to logon to the network. Did Ethereal capture packets from the Access Point to the Supplicant and Back??

4. Now that we have verified the network is broadcasting packets, we will begin testing the limits of the signal area. Using the third party laptop, we can verify signal strength with NetStumbler.

a. First create a block diagram of the lab area, and the surrounding rooms.

b. Walk around with the NetSumbler laptop and evaluate signal strength at a variety of spots throughout the area.

c. Label the block diagram with the signal strengths

d. Continue this process until the signal diminishes to nothing.

5. Next adjust the power settings to "Low" and repeat step 4.

6. Attach both signal maps to the test packet.

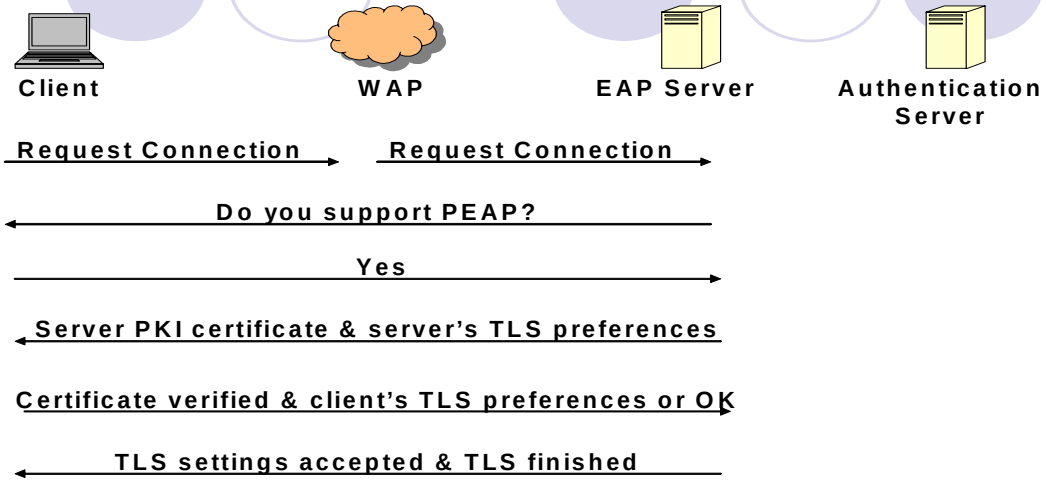
7. Programs such a AirMagnet and the Cisco Wireless Control Server can use these maps to create idea signal broadcast.

Results: See Attached Signal Map

Appendix 4
Wi-Fi TISCOM- Wireless Access and Security
Protected Extensible Authentication Protocol
26Apr06

How does PEAP work?

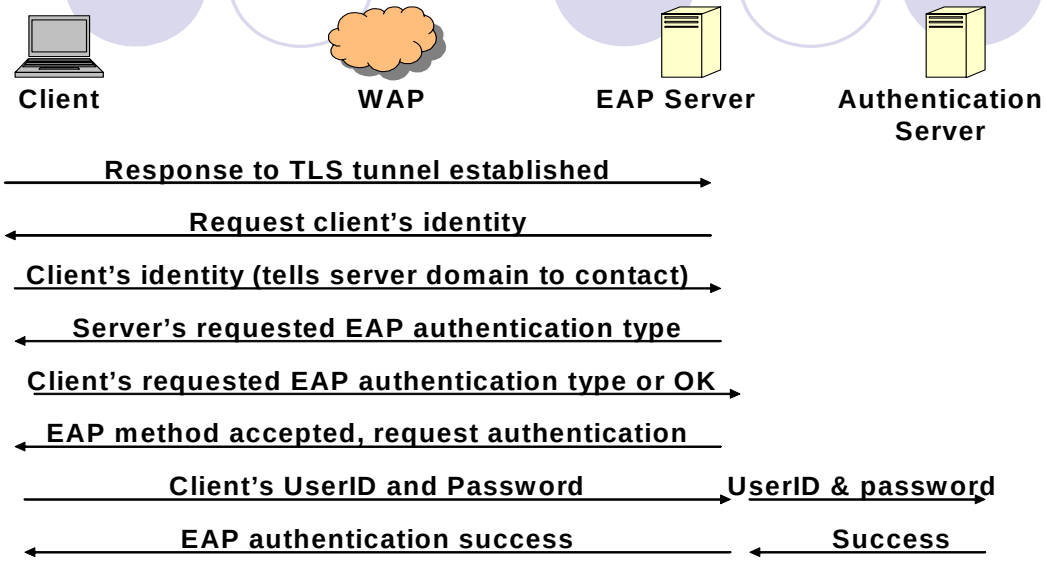
- Part 1 – Establish TLS tunnel



- TLS tunnel established

How does PEAP work?

- Part 2 – EAP authentication within the TLS tunnel



- TLS tunnel torn down

Appendix 5
WIFI TISCOM-Wireless Security and Access
Support Plan
26APR06

Purpose: The project is a proof of concept and "best-practice" design and testing effort. The wide spread popularity of wireless networking in both the public and private sectors has convinced the Coast Guard to evaluate the addition of wireless solutions to its network infrastructure. The benefits of wireless are undeniable; increased productivity, decreased network implementation and maintenance costs, and improved communications. However, this suite of enhancements is not without pitfalls. Wireless transmission opens the door for unauthorized users to access to the network. Proper management and initial configuration are important.

Design Solution: The design solution under consideration for this project revolves around the use of Cisco Aironet wireless enterprise components. The Cisco Aironet family includes "Smart" Access Points, Wireless Local Area Network (WLAN) controllers, Access Control utilities, and can be used with several versions of Cisco switches. This solution can be seamlessly integrated into the current .mil infrastructure and is implemented entirely with commercial off-the-shelf products. This product line satisfies the internal security requirements, provides support and design continuity, and falls in line with industry standard wireless solutions.

Support Considerations:

Economic:

This project is receiving funding from several sources. The trip that I will be taking to TISCOM is funded by the EE department, and will cost approximately $1000. The equipment gained by this trip to TISCOM will account for about $3,000 worth of project inventory. The remaining $2,000-$4,000 dollars of equipment will be purchased through the EE department and IS. This price range is so large based on the fact that Power over Ethernet switches are being considered, but may not be used. Cisco products were selected by TISCOM and must be used as part of my final solution to meet their requests. This project is a proof of concept, so it will most likely be deactivated and the equipment will be returned once the project terminates.

The next iteration of wireless networking in the Coast Guard will be a roll out of wireless infrastructure to units. This potential installation does not fall under my project, but would use the findings from my work as a baseline for site configurations. This enterprise level implementation would have a more carefully managed budget. To implement wireless for any given site in the coast guard, a site survey will need to occur first. This survey will vary in cost, depending on the construction and desired system design. The release of wireless technology for a unit would require the initial purchase of equipment. Funds for replacement of parts will also need to be available.

Manufacturability:

This project is implemented entirely with commercially available equipment. This equipment is built on demand. To support this on-demand system, Cisco advertises a 20 day lead time for orders made. For any parts that might need to be available sooner then 20 days, a 5% sparing inventory should be maintain at ELC.

Configuration and installation requirements are easily met with Coast Guard resources. Enlisted and contract IT personnel can install and configure these access points with a fairly limited amount of training and guidance. This system, once configured correctly, does not have any other major work associated with the installation.

Sustainability and Reliability:

The implementation of a wireless network segment requires a site survey for each site. For the wireless network at the Academy, this survey was done in a cursory mode. The test network is being installed in an area where it will work and it has a limited user base. No users will be accessing this system for daily use. This is a test environment and will be manipulated as such. Reliability is dictated by the configuration we choose. Once we find a stable configuration, the wireless segment should provide connectivity on schedule. Scheduled management of access is an additional security measure. By controlling the times that the wireless signal is available, I can both provide security and schedule time for any maintenance. The wireless domain controller can be configured to limit the times of day and days of the week during which a wireless signal is available.

The use of wireless networks at Coast Guard land units will be determined by the results of the site survey and if the system is desired. If a site is not conducive to wireless transmission, or does not support a large network node it is most likely not a strong candidate for wireless connectivity. Once a site has been approved for wireless, the system will be implemented and the load of network connection will shift onto the wireless system. Administrators need to be cognizant of problems, but the system design will be sufficient to provide the appropriate connectivity for the system.

Life-Cycle Costs:

This project should be terminated by May of 2006. This is the end of trial determined by TISCOM. This project is an effort to find and recommend the best possible wireless solution for the Coast Guard.

Once this system has been developed and approved, it can be implemented anywhere. Actual site implementations should be administered on a 5 year life cycle. The pace of information technology development and the development of more complex malicious computing techniques ma dictate the need for upgrade or removal of the wireless infrastructure at an earlier time. At the end of the 5 year period, the technology needs to be evaluated and a new system implemented if the current configuration is inadequate. The parts are commercial and as such can be reset to factory configurations and be resold or disposed of using regular IT end-of-life disposition procedures.

Recurring costs for a wireless network are low. Wireless systems are inherently low maintenance, as all the working parts are easy accessed by authorized personnel, eliminating costly and time intensive repair procedures. This access is controlled by key sets or code locked doors, into areas where the components are stored. As mentioned previously, spare parts will have to be maintained either on site, or at the nearest

electronics support type unit, as there is a lag associated with ordering parts from the manufacturer. It is recommended that about 5% sparing be maintained, proportional to the amount of units deployed.

Upgrades and expansion costs will remain fairly low, provided current technology is maintained. Should a new standard be developed or unit requirements change from the initial system, a new solution may be necessary. The use of "Smart" access points and simple upgrade of all components through flashable firmware provides easy, automatic upgrades for the system. The training for IT support members can be minimal. Installations will be performed by onsite personnel with guidance from TISCOM. For larger installations, or units with out IT personnel, installation teams can be deployed to configure wireless services. The project design, at this stage, calls for remote management of all pieces of the system. Centralized management of the user base and system hardware significantly lowers the administrative load at the units, and provides better configuration management for the system overall.

For this project, a majority of the funding has been provided by TISCOM. For actual installation at Coast Guard sites, the IT budget for the site or from TISCOM will fund the procurement, installation, and maintenance of the individual system.

External Considerations:

Environmental:

Due to the COTS nature of all products used in this project, it complies with the FCC regulations that govern radio transmissions and wireless technology. This solution will also comply with Institute of Electrical and Electronics Engineers 802.11 standards for wireless networking.

The final system must also comply with Coast Guard, Department of Defense, Department of Homeland Security, and C4&IT directives concerning Information Assurance and Secure Networking. These Commandant and Department instructions are being used during the consideration of the components and configurations during development. Some sites may discover interference during their site surveys, making wireless obsolete. Once the final system is authorized to be used at the enterprise level and the unit is certified for a wireless solution, there will be no concerns about environmental impact.

Health and Safety:

There is little need for concern about health and to personnel in the vicinity of the test wireless network. It is in an area designed for computer testing and it will meet all commercial and governmental standards for emissions and wiring safety, based on the commercial off the shelf components. The same standards it meets in the lab will be met in the field.

Ethical, Social & Political:

The ethical standards in question for this project relate mainly to information assurance. Protecting user data, government network resources, and securing wireless transmissions are all governed by Coast Guard Information Assurance and Federal Privacy law. These documents provide the minimum standard for protections that must be applied to the Coast Guard networks. These standards are guiding parts of the system design.

The social considerations include the push towards wireless work places and improved communications at work. This social shift towards ireless is also a guiding principle of the project. Remaining contemporary with the private sector is vital to information and network defense.

Political pressures on this project are few. Some agencies have begun making the transition to wireless, including the NSA for internal traffic and SiperNet traffic at specified units.

Software Considerations:

Privacy:

User data is stored on the Cast Guards system and is not at any greater risk for dissemination over wireless then a wired network. The privacy concerns arise from the potential for units which deploy a wireless solution

and the potential for “packet sniffing,” or external monitoring of data moving over the network. Security features of the network will address these issues.

Security

Security of the transmission system is the largest concern. The network will not store any new or more sensitive information due to the wireless network. However, privileged information that was passed over wired networks is more vulnerable. Physical security, like proper placement of access points and server security are important. Power and signal management also play a major role in controlling wireless transmissions.

Physical security is already tightly controlled. All server spaces maintain access control lists via TISCOM. Active Directory and domain structuring allow system administrators to keep positive control over the access right of users. This system is nearly completely secure and is being improved whenever possible. The implementation of a wireless network at any given site would be governed by standing C4&IT protocol. These protocols require that signal management techniques, like power limitation, directional broadcasting, and