



Senior Design Project in Electrical & Computer Engineering



Wireless Security

1/c Robert Litts, 1/c Michael Rauch, and 1/c Kathryn Weber

Advisors: LT Matthew Kempe and Dr. Brett Sovereign

Sponsor: TISCOM (Liaison: CDR Keist and Mr. Bill Randall)

Results

As shown on the map below, our system of "Wireless Monitoring Devices" are placed throughout the Academy and connected to the .EDU network. We were able to create an automatic scanning and report system that alerts a central authority anytime a rogue network is detected at USCGA. This system scans the area, sends information back to a central server, and compares the list of detected networks to a pre-established list of authorized networks. Any discrepancies or rogue networks are immediately reported via email to the central monitoring authority.

Key Terms:

- Wireless Monitoring Device – Repurposed router designed to automatically scan for wireless traffic operating in an area
- White List – List of authorized networks operating at an installation
- Flagged Networks – Rogue networks that do not appear on the White List
- Flagged Access Points – Physical access points corresponding to each Flagged Network

What We Can Detect:

- Mobile Hotspots



- Personal Wireless Networks



Information Obtained from Scan

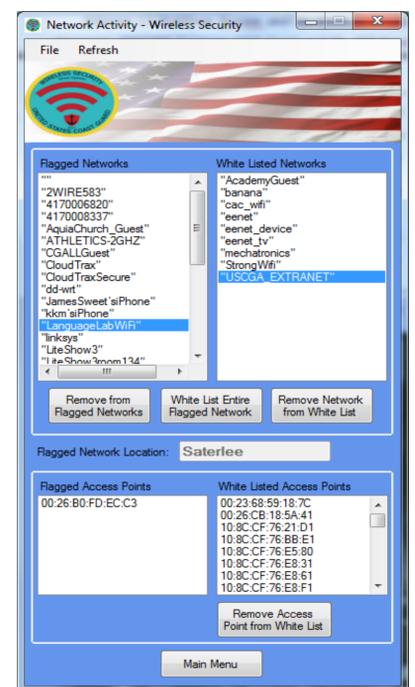
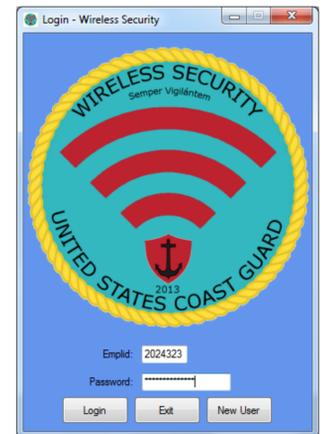
- ESSID (Network Name)
- MAC Address
- Signal Strength
- Encryption Type
- Frequency
- Network Mode

Project Background

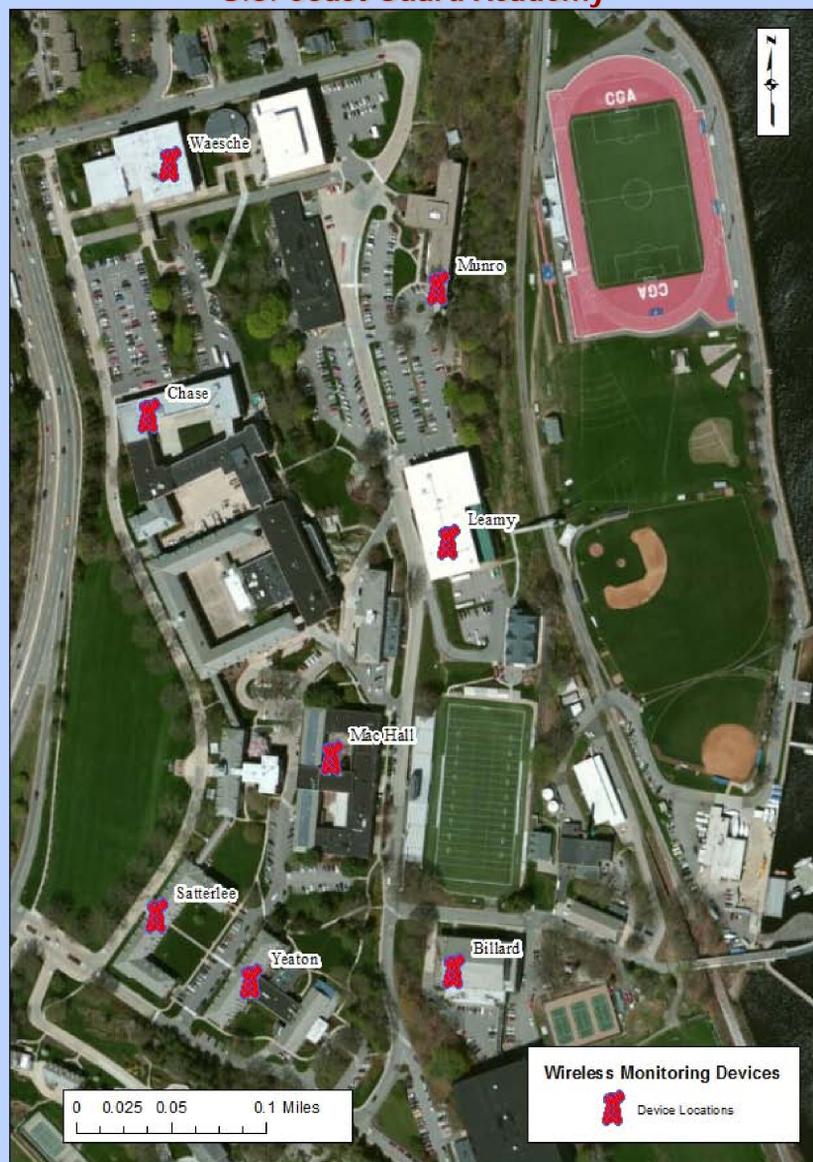
Unauthorized and misconfigured 802.11 wireless access points (WAPs) provide a ripe target for attacks and information disclosure. The Coast Guard is currently uncertain about the security of WAPs at units throughout the country. Unsecured wireless networks operating at a Coast Guard installation could mean that sensitive information is at risk. These "rogue networks" create an operational security risk and provide the potential for unauthorized individuals to gain access to sensitive information. Although there is currently only one authorized wireless .MIL network in the Coast Guard at Surface Forces Logistics Center (SFLC) Baltimore, this could potentially be the gate through which an attacker gains access to the United States' .MIL framework. The fact that .MIL is being transmitted as a wireless network means that the Coast Guard harbors a responsibility to ensure that unauthorized access cannot be obtained. A system is needed to discover and document operating wireless networks at a Coast Guard installation to increase awareness of potential threats to the security and integrity of Coast Guard personnel and operations.

Project Deliverables

- Graphical User Interface (GUI) to easily manage White List, flagged networks, and other pertinent information



Map of Wireless Monitoring Device Locations at U.S. Coast Guard Academy



Project Functionality

- Automatically displays all rogue networks, their corresponding access points, and their locations
- Immediately alerts system administrator via email whenever a new network is flagged as a rogue network
- Easily add approved networks to the White List

Impact on the Coast Guard

- Increased awareness of potential security threats
- Preparing for the increased usage of .MIL wireless networks within the Coast Guard
- Provide the Coast Guard with the ability to monitor all wireless traffic from a central location

Future Project Goals

- Restrict connectivity to unauthorized networks
- Check network connectivity to .MIL
- Transfer project platform from .EDU to the .MIL domain
- Create a robust system resistant to spoofing
- Check configuration of authorized networks
- Triangulate rogue network location

