

Senior Design Project in Electrical Engineering



Wireless Security and Ethical Hacking

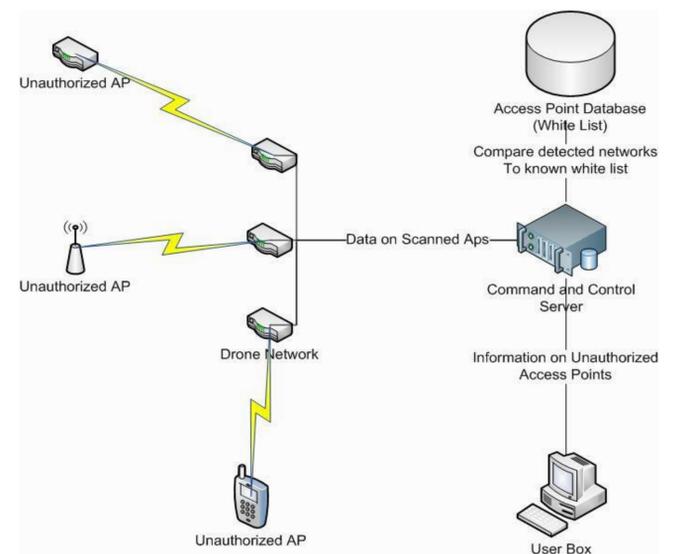
1/c Matthew Monahan, 1/c Laura Carts Advisor: Dr. Brett Sovereign, CDR Joseph Staier
Sponsor: TISCOM (POCs: CDR William Randall, Mr. Tom Clark)

Project Background

The Coast Guard has many different information networks. CG One, commonly known as “.mil” is a secure network over which sensitive information can be transferred. CG One has only two authorized wireless nodes, and any unauthorized wireless nodes present a potential weakness. Unauthorized wireless access points could be actively malicious or they could simply be misconfigured, but both types expose the CG One network to attack and data loss. 1/c Monahan and 1/c Carts (collectively called Team Fresh) have continued the work of last year’s group and have developed a system whereby unauthorized networks are detected and monitored. Furthermore, the system developed by Team Fresh includes the capability to mitigate the potential threat vectors by preventing connections to select unauthorized access points.

Access
Detection
Monitoring
Interruption
Network

Network Design



Project Parameters

The project parameters are as follows:

- Detect all wireless networks
- Capture data on all unauthorized networks
- Be able to restrict access to networks selected by the system administrator

Project Components

- Drone Devices:** Raspberry Pi ARM (with Wireless Adapter)
- Wireless Adapter:** Tenda Mini 11n Wireless USB Adapter
- Mobile Server:** Ubuntu 12.04.3 virtualized server
- Client Machine:** Windows 7 running on MacBook Pro



Capturing Wireless Traffic

```
CH 5 [( Elapsed: 12 s [( 2014-02-17 19:48 [( paused output
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
28:C6:8E:23:00:94 -39 2 0 0 6 54a, OPN Dynamic Shaf
00:17:DF:AB:87:62 -43 6 0 0 1 54a, WPA2 CCMP PSK <length: 1>
00:17:DF:AB:87:63 -43 6 0 0 1 54a, WPA2 CCMP MGT cac_wifi
00:17:DF:AB:87:60 -44 6 21 0 1 54a, WPA2 CCMP PSK eenet
00:17:DF:AB:87:61 -44 6 0 0 1 54a, WPA2 CCMP PSK <length: 1>
00:1D:46:25:30:A5 -78 2 0 0 11 54a, WPA2 CCMP MGT cac_wifi
00:1D:46:25:30:A3 -78 2 0 0 11 54a, WPA2 CCMP PSK eenet_tv
00:1D:46:25:30:A0 -78 2 0 0 11 54a, WPA2 CCMP PSK eenet
00:1D:46:25:30:A2 -78 4 0 0 11 54a, WPA2 CCMP PSK <length: 1>

BSSID STATION PWR Rate Lost Frames Probe
(not associated) CB:3A:35:CD:81:39 0 0 0 0 0 11
00:17:DF:AB:87:60 28:AA:4B:8E:9A:94 11 54 0 0 1
00:17:DF:AB:87:60 58:8B:3E:AB:24 -42 0 -54 0 1
00:17:DF:AB:87:60 24:FD:52:EC:D6:79 -56 54 -54 0 19
```

Analyzing Wireless Traffic

```
mon0 [Wireshark 1.8.5]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
No. Time Source Destination Protocol Length Info
361 59.944282000 Apple_f1:b1:57 Cisco_6f:40:00 802.11 118 Data,
362 59.944287000 Apple_f1:b1:57 (RA) 802.11 28 Ackno
363 59.945980000 Cisco_6f:40:00 Apple_f1:b1:57 802.11 118 Data,
364 59.945997000 Cisco_ab:87:60 (RA) 802.11 28 Ackno
365 59.946007000 Cisco_6f:40:00 Apple_f1:b1:57 802.11 118 Data,
366 59.946015000 Cisco_ab:87:60 (RA) 802.11 28 Ackno
367 59.946528000 Apple_f1:b1:57 Cisco_6f:40:00 802.11 118 Data,
368 59.946533000 Apple_f1:b1:57 (RA) 802.11 28 Ackno
369 59.946563000 Apple_f1:b1:57 Cisco_6f:40:00 802.11 118 Data,
370 59.946569000 Apple_f1:b1:57 (RA) 802.11 28 Ackno
371 59.947548000 Cisco_6f:40:00 Apple_f1:b1:57 802.11 118 Data,
372 59.947565000 Cisco_ab:87:60 (RA) 802.11 28 Ackno
373 59.948234000 Apple_f1:b1:57 Cisco_6f:40:00 802.11 118 Data,

> Frame 324: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
> Radiotap Header v0, Length 13
> IEEE 802.11 Probe Request, Flags: .....
> IEEE 802.11 wireless LAN management frame
```

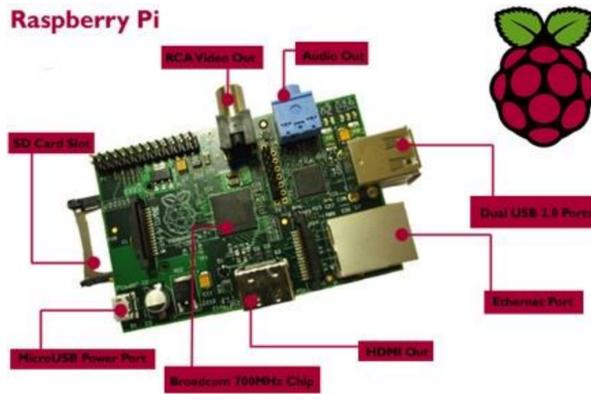
Interruption of Access

```
root@kali:~# sudo aireplay-ng -0 0 -a 00:17:DF:AB:87:60 mon0
19:51:04 Waiting for beacon frame (BSSID: 00:17:DF:AB:87:60) on channel 1
NB: this attack is more effective when targeting
a connected wireless client. (-c <client's mac>)
19:51:04 Sending DeAuth to broadcast -- BSSID: [00:17:DF:AB:87:60]
19:51:04 Sending DeAuth to broadcast -- BSSID: [00:17:DF:AB:87:60]
19:51:05 Sending DeAuth to broadcast -- BSSID: [00:17:DF:AB:87:60]
19:51:06 Sending DeAuth to broadcast -- BSSID: [00:17:DF:AB:87:60]
19:51:06 Sending DeAuth to broadcast -- BSSID: [00:17:DF:AB:87:60]
19:51:07 Sending DeAuth to broadcast -- BSSID: [00:17:DF:AB:87:60]
19:51:07 Sending DeAuth to broadcast -- BSSID: [00:17:DF:AB:87:60]
19:51:08 Sending DeAuth to broadcast -- BSSID: [00:17:DF:AB:87:60]
19:51:08 Sending DeAuth to broadcast -- BSSID: [00:17:DF:AB:87:60]
19:51:09 Sending DeAuth to broadcast -- BSSID: [00:17:DF:AB:87:60]
19:51:09 Sending DeAuth to broadcast -- BSSID: [00:17:DF:AB:87:60]
19:51:10 Sending DeAuth to broadcast -- BSSID: [00:17:DF:AB:87:60]
19:51:10 Sending DeAuth to broadcast -- BSSID: [00:17:DF:AB:87:60]
19:51:11 Sending DeAuth to broadcast -- BSSID: [00:17:DF:AB:87:60]
```

Drone Device

By using commercial off-the-shelf (COTS) components such as the Raspberry Pi we avoided customization problems. The Raspberry Pi is portable, consumes little power, and provides all necessary functionality. The Raspberry Pi is easily flashed with a number of customized GNU/Linux images available for download at no cost.

Raspberry Pi



Results

ADMIN currently operates as a mobile unit capable of performing all of its tasks given a preexisting network communication background. ADMIN is a simple to use yet effective tool that discovers and analyzes exactly what kinds of Wifi devices exist in a certain controlled network environment. ADMIN even offers the capability to mitigate the security threat of a rouge or poorly configured access point through a deauthentication protocol which renders all hosts in the area unable to communicate with the targeted access point.

Field Test at USCG Base Boston

On Thursday, 25 April 2014 we traveled up to USCG Base Boston to conduct a field test of our new equipment. Once ADMIN was set up, it allowed us to determine what and how many devices were broadcasting in the Wifi Band, what their level of encryption was, and how frequently they were being used. While our visit to Base Boston lasted only a day, ADMIN can be set up to automatically monitor the wireless environment for longer durations. This type of survey could provide valuable decision making information to Base Boston personnel.

