Chellam – a Wi-Fi IDS/Firewall for Windows
Vivek Ramachandran

B.Tech, ECE
IIT Guwahati

802.1x, Cat65k
Cisco Systems

WEP Cloaking
Defcon 19

Caffe Latte Attack
Toorcon 9

Media Coverage
CBS5, BBC

Microsoft
Security Shootout

Trainer, 2011

Wi-Fi Malware, 2011
SecurityTube and Pentester Academy
Motivation

• Attack! Attack! Attack!

• Defense?

• Important problem?

• Solution viable?
Enterprise Premise Focused

Automatic protection against any unauthorized Wi-Fi activities.

- Hacker
- Authorized AP
- Rogue AP
- Mis-configured AP
- Client Mis-association
- External AP
- Corporate Firewall
- Internet
Roaming Clients?

- **State of current solutions**
  - Lockdown Wi-Fi, Bluetooth etc.
  - Policy based on SSID
  - Not BYOD ready
  - No Attack detection

- **Heterogeneous Devices**
  - Varied Operating Systems
  - Non standard Wi-Fi API
  - No low level support e.g. iOS
What about the rest of us?

- World beyond Enterprise
- Millions of Personal Devices
- Every Internet capable device
- Internet Of Things (IoT)
Wi-Fi Client Attack Surface

- Honeypots
  - AP-less WEP/WPA/WPA2 Cracking
- Evil Twins
- Mis-Associations
- Hosted Network Backdoors
- ...

©SecurityTube.net
Typical Attack
AP-less Cracking

- No Encryption
- WEP
- WPA/WPA2 PSK
- WPA/WPA2 PEAP, EAP-TTLS
- Cloud Cracking
  - Caffe Latte
  - Hirte

AP-less Cracking

Handshake, MS-CHAPv2 CR
Where are you SAFE? Nowhere!!!
Hijack Wi-Fi == Hijack Layer 2

- Traffic Monitoring
- DNS Hijacking
- SSL MITM
- Application Attacks
Defining the Scope

- Windows Endpoints
  - No custom hardware or drivers
- Detect Honeypot creation Tools
- Firewall like Rule Creation
  - “Allow”, “Deny”
- Monitoring Wi-Fi state machine
- Detect Wi-Fi backdoors
Wi-Fi Native API

- **State Machine**: 802.11 state machine per Wi-Fi card
- **Scan Data**: Periodic Scan Results with BSS data
- **Network Profiles**: XML network profile data
- **Card Control**: Scan, Connect, Disconnect, Lock etc.
typedef struct _WLAN_BSS_ENTRY {
    DOT11_SSID          dot11Ssid;
    ULONG              uPhyId;
    DOT11_MAC_ADDRESS   dot11Bssid;
    DOT11_BSS_TYPE     dot11BssType;
    DOT11_PHY_TYPE     dot11Bss PhyType;
    LONG               lRssi;
    ULONG              uLinkQuality;
    BOOLEAN            bInRegDomain;
    USHORT             usBeaconPeriod;
    ULONGLONG          ullTimestamp;
    ULONGLONG          ullHostTimestamp;
    USHORT             usCapabilityInformation;
    ULONG              ulChCenterFrequency;
    WLAN_RATE_SET      wlanRateSet;
    ULONG              ulIeOffset;
    ULONG              ulIeSize;
} WLAN_BSS_ENTRY, *PWLAN_BSS_ENTRY;

typedef struct _WLAN_NOTIFICATION_DATA {
    DWORD NotificationSource;
    DWORD NotificationCode;
    GUID InterfaceGuid;
    DWORD dwDataSize;
    PVOID pData;
} WLAN_NOTIFICATION_DATA, *PWLAN_NOTIFICATION_DATA;

<?xml version="1.0" encoding="US-ASCII"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
    <name>SampleWPA2PSK</name>
    <SSIDConfig>
        <SSID>
            <name>SampleWPA2PSK</name>
        </SSID>
    </SSIDConfig>
    <connectionType>ESS</connectionType>
    <connectionMode>auto</connectionMode>
    <autoSwitch>false</autoSwitch>
    <MSM>
        <security>
            <authEncryption>
                <authentication>WPA2PSK</authentication>
                <encryption>AES</encryption>
                <useOneX>false</useOneX>
            </authEncryption>
        </security>
    </MSM>
</WLANProfile>

Demo – Data Sources
Data Collection and Storage

- Stored in SQLITE databases
- Makes it easy to write plugins
- 3rd party tools can use the database
Demo – SQLITE DB Data

<table>
<thead>
<tr>
<th>row_id</th>
<th>sniffed_row_id</th>
<th>ssid</th>
<th>phy_id</th>
<th>bssid</th>
<th>bss_type_id</th>
<th>rssi</th>
<th>net_center_freq</th>
<th>rates_string</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>MOVISTAR_1BD9</td>
<td>2</td>
<td>788085BD9...</td>
<td>1</td>
<td>-92</td>
<td>2437000</td>
<td>1; 2; 5.5; 11; ...</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>ONO9297</td>
<td>1</td>
<td>600138F2...</td>
<td>1</td>
<td>-106</td>
<td>2412000</td>
<td>1; 2; 5.5; 11; ...</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>ONO0702</td>
<td>1</td>
<td>600138F2...</td>
<td>1</td>
<td>-104</td>
<td>2412000</td>
<td>1; 2; 5.5; 11; ...</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>JAZZTEL_C561</td>
<td>1</td>
<td>6480C6B1...</td>
<td>1</td>
<td>-107</td>
<td>2462000</td>
<td>1; 2; 5.5; 11; ...</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>MOVISTAR_455C</td>
<td>2</td>
<td>810C6A37...</td>
<td>1</td>
<td>-112</td>
<td>2462000</td>
<td>1; 2; 5.5; 11; ...</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>wifi_10</td>
<td>1</td>
<td>7268C6B1...</td>
<td>1</td>
<td>-108</td>
<td>2462000</td>
<td>1; 2; 5.5; 11; ...</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>WLAN_7432</td>
<td>2</td>
<td>001A2B0A...</td>
<td>1</td>
<td>-109</td>
<td>2442000</td>
<td>1; 2; 5.5; 11; ...</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>WLAN_C7A1</td>
<td>2</td>
<td>001A2B0A...</td>
<td>1</td>
<td>-106</td>
<td>2442000</td>
<td>1; 2; 5.5; 11; ...</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>h1Rozuelo</td>
<td>1</td>
<td>001D4596...</td>
<td>1</td>
<td>-93</td>
<td>2472000</td>
<td>1; 2; 5.5; 11; ...</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>SAENBRUS</td>
<td>2</td>
<td>18172533...</td>
<td>1</td>
<td>-101</td>
<td>2472000</td>
<td>1; 2; 5.5; 11; ...</td>
</tr>
</tbody>
</table>
Rule Matching and Analysis

- Rules can be written to include:
  - BSSID
  - Neighboring Networks
  - Channel use patterns and frequencies
  - Information Elements in the Beacon / Probe Response
  - Access pattern based on time of day
### Demo – Monitoring and Event Detection

Chellam - a Wi-Fi Firewall for Windows

<table>
<thead>
<tr>
<th>SSID</th>
<th>BSSID</th>
<th>BSS Type</th>
<th>Signal Strength (dB)</th>
<th>Frequency (kHz)</th>
<th>Last Seen</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jazztel_C561</td>
<td>64:68:0C81:1C5:62</td>
<td>Infrastructure</td>
<td>-105</td>
<td>246200</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>Jazztel_75</td>
<td>4C:ED:DEF2:AA:11</td>
<td>Infrastructure</td>
<td>-115</td>
<td>243700</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>MHVYO</td>
<td>00:1A:2B:92:7A:12</td>
<td>Infrastructure</td>
<td>-104</td>
<td>245700</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>MOVISTAR_18D9</td>
<td>F8:8E:85:D9:18:DA</td>
<td>Infrastructure</td>
<td>-90</td>
<td>243700</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>MOVISTAR_455C</td>
<td>8C:0CA:37:45:5C</td>
<td>Infrastructure</td>
<td>-98</td>
<td>246200</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>MOVISTAR_A842</td>
<td>F8:8E:85:CA:A8:43</td>
<td>Infrastructure</td>
<td>-96</td>
<td>241200</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>ON00702</td>
<td>00:01:38:F2:CD:3C</td>
<td>Infrastructure</td>
<td>-112</td>
<td>241200</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>ON09297</td>
<td>00:01:38:F2:CD:38</td>
<td>Infrastructure</td>
<td>-110</td>
<td>241200</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>Orange-32A3</td>
<td>88:03:55:16:32:A5</td>
<td>Infrastructure</td>
<td>-111</td>
<td>246200</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>Orange-7214</td>
<td>50:7E:8D:60:72:16</td>
<td>Infrastructure</td>
<td>-111</td>
<td>241200</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>Orange-F48F</td>
<td>88:03:55:75:F4:91</td>
<td>Infrastructure</td>
<td>-104</td>
<td>245200</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>Orange-d20e</td>
<td>00:19:70:3D:A4:B4</td>
<td>Infrastructure</td>
<td>-108</td>
<td>243700</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>SAENBRUS</td>
<td>18:13:27:33:A4:7C</td>
<td>Infrastructure</td>
<td>-106</td>
<td>247200</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>VodafoneECC4</td>
<td>84:9CA:6D7:EC:C4</td>
<td>Infrastructure</td>
<td>-111</td>
<td>241200</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>WLAN_1F03</td>
<td>00:1A:2B:BB:FA:5F</td>
<td>Infrastructure</td>
<td>-108</td>
<td>241700</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>WLAN_6987</td>
<td>00:1A:2B:AA:47:5E</td>
<td>Infrastructure</td>
<td>-106</td>
<td>243200</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>WLAN_7432</td>
<td>00:1A:2B:AD:37:24</td>
<td>Infrastructure</td>
<td>-106</td>
<td>244200</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>WLAN_783F</td>
<td>00:1A:2B:82:6FCD</td>
<td>Infrastructure</td>
<td>-107</td>
<td>244200</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>WLAN_C7A1</td>
<td>00:1A:2B:AE:56:6D</td>
<td>Infrastructure</td>
<td>-107</td>
<td>244200</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
</tbody>
</table>

©SecurityTube.net
Understanding Attack Detection
Fingerprinting the Network

- BSSID(s)
- BSS type
- PHY type
- Beacon Interval
- Channel(s) & Hopping
- Rates – basic and extended
- Capability Information
- Information Element(s)

- Neighboring Access Points
  - AP details as above

- IP, Gateway
- DNS, ARP cache

- Subnet scan
- OS and service scan

802.11 (pre connect)

IP & Above (post connect)
### Typical Attack Mitigation

- **BSSID(s)**
- **Channel(s) & Hopping**
- **Rates – basic and extended**
- **Capability Information**
- **Information Element(s)**
- **Neighboring Access Points**
- **AP details as above**
### Demo – Attack Tool Detection (Airbase)

#### Chellam - a Wi-Fi Firewall for Windows

<table>
<thead>
<tr>
<th>SSID</th>
<th>BSSID</th>
<th>BSS Type</th>
<th>Signal Strength (dB)</th>
<th>Frequency (kHz)</th>
<th>Last Seen</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airbase-AP</td>
<td>E8:DE:27:2060:11</td>
<td>Infrastructure</td>
<td>-10</td>
<td>2412000</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>JAZZTEL_C561</td>
<td>64:68:00:C8:1C3:62</td>
<td>Infrastructure</td>
<td>-106</td>
<td>2462000</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>Jazztel_75</td>
<td>4C:ED:DE:F2:AA:11</td>
<td>Infrastructure</td>
<td>-110</td>
<td>2437000</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>MHYYO</td>
<td>00:1A:28:92:7A:12</td>
<td>Infrastructure</td>
<td>-105</td>
<td>2457000</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>MOVISTAR_18D9</td>
<td>F8:BE85:E9:18:DA</td>
<td>Infrastructure</td>
<td>-92</td>
<td>2437000</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>MOVISTAR_455C</td>
<td>8C:OC:A3:37:45:5C</td>
<td>Infrastructure</td>
<td>-102</td>
<td>2462000</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>MOVISTAR_5E33</td>
<td>F8:BE85:40:5E:34</td>
<td>Infrastructure</td>
<td>-116</td>
<td>2421000</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>MOVISTAR_A842</td>
<td>F8:BE85:C5:A8:43</td>
<td>Infrastructure</td>
<td>-94</td>
<td>2421000</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>ONO0702</td>
<td>00:01:38:F2:CD:3C</td>
<td>Infrastructure</td>
<td>-110</td>
<td>2421000</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>ONO9297</td>
<td>00:01:38:F2:CD:3B</td>
<td>Infrastructure</td>
<td>-110</td>
<td>2421000</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>Orange-32A3</td>
<td>88:03:55:1F:32:A5</td>
<td>Infrastructure</td>
<td>-109</td>
<td>2421000</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>Orange-7214</td>
<td>50:7E:50:80:72:16</td>
<td>Infrastructure</td>
<td>-111</td>
<td>2421000</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>Orange-F48F</td>
<td>88:03:55:75:F4:91</td>
<td>Infrastructure</td>
<td>-99</td>
<td>2437000</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>Orange-d20e</td>
<td>00:19:70:3D:A4:84</td>
<td>Infrastructure</td>
<td>-109</td>
<td>2421000</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>Qlik</td>
<td>08:86:39:D8:F8:22</td>
<td>Infrastructure</td>
<td>-111</td>
<td>2421000</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>SAIENBRUS</td>
<td>18:17:25:33:AA:7C</td>
<td>Infrastructure</td>
<td>-104</td>
<td>2421000</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>VodafoneECC4</td>
<td>84:9C:A6:D7:EC:C4</td>
<td>Infrastructure</td>
<td>-109</td>
<td>2421000</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>WLAN_086F</td>
<td>00:1A:28:8B:F9:D5</td>
<td>Infrastructure</td>
<td>-112</td>
<td>2421000</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>WLAN_1R03</td>
<td>00:1A:28:8B:F9:F5</td>
<td>Infrastructure</td>
<td>-106</td>
<td>2421000</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
<tr>
<td>WLAN_0128</td>
<td>8C:4D:68:14:95:22</td>
<td>Infrastructure</td>
<td>-107</td>
<td>2421000</td>
<td>0 min ago</td>
<td>Details</td>
</tr>
</tbody>
</table>

**Attack Tool Detected!**

**Network:** Airbase-AP

**Message:** This network seems to have been created by an Attack Tool which creates Fake Access Points. Do not connect to this network.

[Dismiss Alert]
Why is this important?

• Attack tools will have to significantly improve

• Make it difficult to fingerprint
  – No hardcoded values, random BSSID etc.

• More features to mimic authorized networks
  – Ability to “clone” network beacons / probe responses
  – Ability to closely follow Clocks (timestamp)
  – Have to be on the right channel and band

• Very difficult to beat Whitelist approach
Roadmap - Enhancements

• Whitelist vs Blacklist

• Plugin Architecture
  – SQL with Python

• Intrusion Prevention / Firewall with custom Driver

• Assisted and automatic learning of whitelists

• Downloadable blacklists for attack tools
Questions?