WiFi Security Scenario Generation Suite

Pune Institute of Computer Technology, Pune

Guided By:
  Mr. Aniruddha Patwardhan

Sponsored By:
  Dreamz Group, Pune

Team Members:
  Umesh S. Chandak
  Vivek G. Relan
  Rishikesh S. Naik
  Bhushan E. Sonawane
What is a Wireless LAN/ WiFi?

- First international standard for Wireless Local Area Network (WLAN) – IEEE standard 802.11
- Data communication system implemented as an extension to, or as an alternative for, a wired LAN within a building or campus
- Uses air as transmission medium
Wireless LAN components

- **Client** –
  A client is a mobile network node that is equipped with a wireless network device.

- **Access Point (APs)** –
  An AP is a wireless network device that acts as an Ethernet bridge and forwards the communications to and from the wired and wireless.

- **Types of 802.11 frame**
  a. Management Frames
  b. Control Frames
  c. Data Frames
Modes of operation

Ad-hoc mode
Used to connect wireless clients when a wireless AP is not present.

Infrastructure mode
The wireless client uses the wireless AP to access the resources of a wired network.
Position of WiFi SSGS
Project Goals

- To develop the tool for WiFi to judge the reliability of WiFi deployment
- Exploration of wireless vulnerabilities
- To monitor the WiFi deployment
- To generate different type of scenario
- To determine all the specifications, advertised features and promises made about WiFi security products
Features of WiFi SSGS

- Scanning
- Security
- Meta Language
- Traffic
- Favorites
- Test Report Generation
Scanning

- To collect the information about the current wireless environment
- To get feel of the wireless network
- Use to generate specific traffic or to launch attacks or performance analysis etc
Security

- To launch different type of attacks over WLAN
- To penetrate the WiFi deployment for
  - Security testing
  - Finding Vulnerabilities in the networks
Deauthentication Flood

- Type of Denial of Service (DoS) attack
- Authenticated stations will drop their network connections
- Here, spoofed MAC addresses are as:
  - Client’s MAC address – 00:06:25:48:29:19
  - AP’s MAC address – 00:06:25:4B:4A:9B
Meta Language

- Most generic and extensible Meta language
- Assists in generating any custom scenarios
- Provides predefined templates for scenario generation
- Plain text format like an English sentence
- Supports hierarchical structure
- Supports looping
- Supports control statement
Script for Authentication Flood

Do
{
    Generate auth req from MAC 00:0C:41:16:16:16 to MAC 00:06:25:4B:4A:9B channel 11 standard b
}

Repeat 100 times
Traffic

- Emulation of APs and clients on single wireless Network Interface Card (NIC)

- Various types of frame generation

- Predefined templates like office traffic, garbage packets, valid end to end client-AP session etc.
Favorites

- To store the most frequently used patterns like
  - attack patterns
  - traffic patterns
  - performance patterns
Test Report Generation

- Test the security product against the various wireless threats
- Generate report for the promises made and actual obtained test result
Architecture

Madwifi Driver (Wireless Driver) ioctl
Architecture

WiFi ‘C’ Library

ioctl

Madwifi Driver
(Wireless Driver)
WiFi ‘C’ Library

- Abstract library for IEEE 802.11 frame generation
- Emulation of APs/clients
- Supports data payload of TCP/IP
- Handy to develop new wireless network tool
Architecture

Meta Language

WiFi ‘C’ Library

Madwifi Driver (Wireless Driver)

ioctl

Lexical Analyzer

Parser
Meta Language Design

- **Lexical Analysis** – To separate tokens of language

- **Token** – Basic entity of the language
e.g. generate, receive, beacon, probe req, TCP, if, do, repeat etc

- **Parser** – To determine the syntactic meaning and take the appropriate action
# Test Results

<table>
<thead>
<tr>
<th>Attacks</th>
<th>Snort wireless IDS</th>
<th>SpectraGuard SAFE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deauth flood</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Auth flood</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>RTS flood</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>NAV/Duration</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Null Probe</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Rogue AP</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Traffic Replay</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Out of order frag</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Monkey Jack</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
Conclusion

User can rely on WiFi SSGS to penetrate the WiFi deployment for security testing, finding vulnerabilities in the network and for performing custom what-if analysis.
Future Work

- Performance of the Network
- Variable handling in Meta Language
- Auto generation of Meta Language script
Questions ???
Thank You !!!