WiFi Security Scenario Generation Suite (WiFi: SSGS)

1. Motivation behind the Project:

Wireless networks (WiFi networks) use air as transmission medium which is inherently broadcast. This allows anyone in proximity to sniff the traffic and launch the various attacks over WLAN. As wireless networks are used as an extension to wired network, they provide an easy gateway to the wired network. Enterprises spend millions of dollars securing their wired networks. But, unmanaged and unsecured WLAN can jeopardize entire enterprise networks, data and operations. The implications from a security breach can impact the enterprise’s reputation, intellectual property and regulated information. Therefore there exist security products to monitor, manage and secure WLANs.

But there is no method to determine whether the product meets all of the specifications, advertised features, and promises that have been made about it. There should be some mechanism to seek out and identify any potential problems, so there are no unexpected results after deploying the security product. This gives rise to need for a tool which can assist in performing what-if analysis and scenario generation to judge the reliability of security product.

In order to tackle this problem, we come up with a comprehensive solution—a Security Scenario Generation Suite (SSGS) for IEEE 802.11 (a/b/g) – WiFi standard. Scenario generation includes various types of traffic generation, attacks generation, emulation of APs/clients etc on single wireless NIC. Emulating the APs/clients on a single NIC provides the most cost-effective and scalable solution to the enterprises. SSGS also provides most comprehensive and generic meta language to assist in generating any custom scenarios. It consists of a plaintext format like an English sentence which provides great flexibility to the user. Using the meta language of the SSGS several most generic attack (like man in the middle, DoS etc), templates are provided. Besides scenario generation, this tool also puts emphasis on the performance analysis of a WLAN. It considers the effects of change in the environment through noise detection and noise generation over different channels.

Thus user can rely on this tool to penetrate the WiFi deployment for security testing and for finding vulnerabilities in the network.
2. Design of Project:

1. Architecture:

WiFi SSGS provides most extensive Wi-Fi library in ‘C’ abstracting different type of packet generation. It generates different types of traffic like IEEE 802.11 management, control and data frames, different patterns viz. office traffic and garbage traffic, airborne threats, emulation of APs/clients etc on single wireless NIC. It also supports data payload of TCP/IP like ARP, IP, ICMP, TCP, UDP etc. On the top of our Wi-Fi library, we have built up the meta language and web based UI. The Wi-Fi SSGS meta language is constructed using Lex and Yacc which provides the mechanism to the user for generating various scenarios through user mindset. Web based UI is developed using CGI scripting which serves the purpose of being platform independent. It also provides certain predefined template for scenario generations which are of most importance and common use.
User Interface

Meta Language

Wi-Fi C Library

Madwifi Driver

Lexical Analyzer

Parser

Diag.2: Architecture View
The following diagram depicts the plan for the Meta language.

Diag. 3: Plan for Meta language

3. Algorithms/Methods Used:
   i. AP:
      1. Send beacon frame periodically with beacon interval (100msec).
      2. If frame received is probe request having ssid either null or same as its own ssid, send ACK followed by probe response frame with appropriate information.
      3. If frame received is for AP, then send ACK frame and received frame is of following type, then:
         i. Authentication Request: Check all appropriate fields in the frame. If everything is fine, send authentication response frame and wait for ACK. If ACK is not received, retransmit the frame until retransmission counter exhaust.
         ii. Association Request: Check whether station is initially authenticated from AP-Station Info Table. If not, then send deauthentication frame. If station is
authenticated, send Association Response frame and wait for ACK. If ACK is not received, retransmit the frame until retransmission counter exhaust.

iii. Disassociation: If station leaves BSS and sends disassociation frame, then change the state of station to authenticated and unassociated in AP-Station info table.

iv. Data frame: Check FromDS, ToDS, address fields in the frame and AP-Station Info Table and accordingly send a frame.

ii. Client:

1. State1 (Unauthenticated and unassociated): Only class1 frames are allowed to be transmitted in this state. Client initially discovers for AP by broadcasting probe request frame and wait for probe response. After getting probe response, it will send ACK frame followed by authentication frame to authenticate with discovered AP. After successful authentication, it goes to state2.

2. State2 (Authenticated and unassociated): Only class1 and class2 frame are allowed to be transmitted in this state. Client sends association request to an AP and wait for association response. After receiving association response frame, it will send ACK frame and goes to state3.

3. State3 (Authenticated and associated): Class1, class2 as well as class3 frame are allowed to be transmitted in this state. After successful authentication and association, data communication between AP and client starts.

   If any frame other than allowed frame in that state is transmitted, then AP sends deauthentication frame to client and it goes to state 1.

4. Contribution towards the solution:

   We have contributed towards the solution through the following:

   • Abstract ‘C’ library for WiFi
   • Meta Language with the help of Lex and Yacc
   • Platform independent web based UI using HTML, CGI and Java scripting consisting of scanning, favorites, traffic, security and performance modules
   • Modifications in the Madwifi driver module for performance improvement
5. Commercial value, utility and expected market size:

As per the experts, the market size of wireless security products is around 1.5 billion dollars. Thus, overall market size of security scenario generation suite could be estimated around 500 million dollars.

6. Software and hardware requirement:

**Hardware:**
2 PCs with wireless NIC (Linksys with Atheros Chipset), 1 Access Point.

**Software:**
Linux Kernel -2.6.10, Madwifi Driver cvs current 1.34, Apache Server, Libnet Library, Lex, Yacc.

7. Other uses of Tool:

Apart from using this tool as security scenario generation suite, it can also be used by researchers to emulate wireless scenarios and conduct various experiments, thus performing analysis.
Script written for emulation of client using WiFi: SSGS meta language

This script is for IEEE 802.11b standard. It emulates a client having MAC address 00:0C:41:16:16:16 on channel 1 which is trying to associate with an AP having MAC address 00:11:95:71:0B:2E and ssid “DreamzGroup”.

label1:
generate probe req from mac 00:0c:41:16:16:16 ssid DreamzGroup channel 1 standard b
receive probe resp from mac 00:11:95:71:0b:2e to mac 00:0c:41:16:16:16 ssid DreamzGroup channel 1 standard b timeout 100000
if not goto label1
generate ack to mac 00:11:95:71:0b:2e channel 1 standard b
label2:
generate auth req from mac 00:0c:41:16:16:16 to mac 00:11:95:71:0b:2e channel 1 standard b
receive auth resp from mac 00:11:95:71:0b:2e to mac 00:0c:41:16:16:16 channel 1 standard b timeout 100000
if not goto label2
generate ack to mac 00:11:95:71:0b:2e channel 1 standard b
label3:
generate assoc req from mac 00:0c:41:16:16:16 to mac 00:11:95:71:0b:2e channel 1 standard b
receive assoc resp from mac 00:11:95:71:0b:2e to mac 00:0c:41:16:16:16 channel 1 standard b timeout 100000
if not goto label3
generate ack to mac 00:11:95:71:0b:2e channel 1 standard b
CTS Frame

Mac Address of Receiver: 00 06 25 4b 4a 9b

Frame Control

- Protocol: 0
- Wep Encryption
- Ordered
- Power Management
- Retry

Duration Field: 13A

Protocol: 802.11a

Channel: 36

Start

Diag. 4: Screenshot of CTS frame generation
## Man In The Middle (MITM)

<table>
<thead>
<tr>
<th>Mac Address of AP</th>
<th>00 06 25 4b 4a 9b</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac Address of Client</td>
<td>00 06 25 25 25 25</td>
</tr>
<tr>
<td>Wireless Standard</td>
<td>802.11b</td>
</tr>
<tr>
<td>Client's Channel</td>
<td>1</td>
</tr>
<tr>
<td>Rogue AP Channel</td>
<td>11</td>
</tr>
</tbody>
</table>

Start

Diag. 5 : Screenshot of Man In The Middle attack