RP2 - Availability analysis of SURFwireless

Kasper van Brakel
July 4th, 2019
Introduction

- SURFwireless: Wi-Fi-as-a-Service since 2016
- Aerohive, Hivemanager
- Investigate potential attacks that threaten the availability for clients of SURFwireless
Research questions

- How can SURFnet detect that the availability of the SURFwireless service is under threat and determine its impact?

Sub-questions:
  - Which common attacks on 802.11 networks can be used to threaten the availability of SURFwireless?
  - What impact can these attack cause on the wireless clients of SURFwireless?
  - What measures can SURFnet take to defend SURFwireless against attacks on availability?
Scope

- Potential attacks must be applicable on 802.11 with WPA2-Enterprise
- The general security of eduroam is out of scope, only investigating attacks on availability
- Only detection and prevention methods of the attacks that can be configured from the Hivemanager were investigated
Related work

- **Type of DoS attacks (Bicakci et al.)**:
  - Radio Frequency (RF) jamming
  - MAC layer attacks
  - Above MAC layer attacks (protocol based i.e. ARP, ICMP, TCP)

- **MAC layer Denial-of-Service (DoS) attacks**:
  - Deauthentication attack (Bellardo et al.)
  - Channel Switch attack (Könings et al.)
  - Quiet attack (Könings et al.)
Experiments

Parameters:
- iPerf3 and ping
- Experiments performed 30 times for 60 seconds
- Scapy

Experiments:
- Basetest
- Deauthentication attack
- Channel Switch attack
- Quiet attack

Figure 4: Testbed setup
Deauthentication attack

- Abuses deauth frames

![Figure 1: Generic Deauthentication frame. Source: 802.11 Wireless Networks: The Definitive Guide, Oreilly](image-url)
Channel Switch attack

- Abuses 802.11h amendment
- Transmitted in Beacon, Probe response or action frame

![Diagram of generic Channel Switch element](source: 802.11 Wireless Networks: The Definitive Guide, Oreilly)
# Quiet attack

- 802.11h amendment
- Transmitted in Beacons, Probe response
- Depending on driver implementation clients can be silenced for up to 65535 Time Units

<table>
<thead>
<tr>
<th>bytes</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>2</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Element ID</td>
<td>Length</td>
<td>Quiet count</td>
<td>Quiet period</td>
<td>Quiet duration</td>
<td>Quiet offset</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Figure 3: Quiet element. Source: 802.11 Wireless Networks: The Definitive Guide, Oreilly*
Deauthentication attack.

Ping experiment: packet loss rate in 60 seconds.

Packet loss rate in %

Delay in seconds between attack frames:
Deauthentication attack

iPerf3 experiment: total transmitted data in 60 seconds.

Deauthentication attack

iPerf3 experiment: #retransmitted packets in 60 seconds.

Delay in seconds between attack frames.
Channel switch attack.

Ping experiment: packet loss rate in 60 seconds.
Quiet attack.

Ping experiment: packet loss rate in 60 seconds.

Packet loss rate in %

Delay in seconds between attack frames.
Quiet attack

IPerf3 experiment: total transmitted data in 60 seconds.

Quiet attack

IPerf3 experiment: #retransmitted packets in 60 seconds.
Vulnerable devices

- Vulnerable against Deauthentication and Channel Switch attack

<table>
<thead>
<tr>
<th>Device</th>
<th>802.11 chip</th>
<th>OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell XPS 13</td>
<td>Intel 6235-N</td>
<td>Linux mint 2019.1</td>
</tr>
<tr>
<td>Samsung S10</td>
<td>Broadcom</td>
<td>Android 9</td>
</tr>
<tr>
<td>One Plus 6T</td>
<td>Qualcomm</td>
<td>Android 9</td>
</tr>
</tbody>
</table>
Detection

- DoS protection by Aerohive
- Only deauthentication attack was detected

<table>
<thead>
<tr>
<th>DoS Detection Type</th>
<th>Alarm Threshold Client (frames per minute)</th>
<th>Alarm Threshold SSID (frames per minute)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probe Request</td>
<td>1200</td>
<td>12000</td>
</tr>
<tr>
<td>Probe Response</td>
<td>2400</td>
<td>24000</td>
</tr>
<tr>
<td>(Re) Association Request</td>
<td>600</td>
<td>6000</td>
</tr>
<tr>
<td>Association</td>
<td>240</td>
<td>2400</td>
</tr>
<tr>
<td>Disassociation</td>
<td>120</td>
<td>1200</td>
</tr>
<tr>
<td>Authentication</td>
<td>600</td>
<td>6000</td>
</tr>
<tr>
<td>Deauthentication</td>
<td>120</td>
<td>1200</td>
</tr>
<tr>
<td>EAP Over LAN (EAPol)</td>
<td>600</td>
<td>6000</td>
</tr>
</tbody>
</table>

Table 1: Overview of default threshold values Hivemanager.
Detection

- Formula: 
  \[ \text{time/attackFrameRate} \times \text{connectedClients} \]

<table>
<thead>
<tr>
<th>Clients</th>
<th>0.1</th>
<th>0.5</th>
<th>1</th>
<th>1.5</th>
<th>2</th>
<th>2.5</th>
<th>3</th>
<th>3.5</th>
<th>4</th>
<th>4.5</th>
<th>5</th>
<th>5.5</th>
<th>6</th>
<th>6.5</th>
<th>7</th>
<th>7.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>600</td>
<td>120</td>
<td>60</td>
<td>40</td>
<td>30</td>
<td>24</td>
<td>20</td>
<td>17.1</td>
<td>15</td>
<td>13.3</td>
<td>12</td>
<td>10.9</td>
<td>10</td>
<td>9.2</td>
<td>8.6</td>
<td>8</td>
</tr>
<tr>
<td>10</td>
<td>6000</td>
<td>1200</td>
<td>600</td>
<td>400</td>
<td>300</td>
<td>240</td>
<td>200</td>
<td>171</td>
<td>150</td>
<td>133</td>
<td>120</td>
<td>109</td>
<td>100</td>
<td>92</td>
<td>86</td>
<td>80</td>
</tr>
</tbody>
</table>

Table 2: Overview of threshold values for Hivemanager per investigated attack frame rate.
Prevention

- 802.11w protects:
  - Robust action frames
  - Deauthentication frames
  - Dissasociation frames

- Channel switch and Quiet attack can both abuse beacon and probe response frames ← not protected

<table>
<thead>
<tr>
<th>Code</th>
<th>Action type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Spectrum management</td>
</tr>
<tr>
<td>1</td>
<td>QoS</td>
</tr>
<tr>
<td>2</td>
<td>DLS</td>
</tr>
<tr>
<td>3</td>
<td>Block Ack</td>
</tr>
<tr>
<td>5</td>
<td>Radio</td>
</tr>
<tr>
<td>6</td>
<td>Fast BSS Transition</td>
</tr>
<tr>
<td>8</td>
<td>SA Query</td>
</tr>
<tr>
<td>9</td>
<td>Protected Dual of Public Action</td>
</tr>
<tr>
<td>126</td>
<td>Vendor-specific Protected</td>
</tr>
</tbody>
</table>

Table 3: Overview of robust action frames from 802.11 specification Source
Discussion

- SSID threshold not variable based on client count
- Quiet attack may potentially work on other devices
- More sophisticated detection methods to determine MAC address spoofing based attacks i.e. by sequence number exists (Guo et al). [Source](#)
- For 802.11w protection both client and AP must support it
- Attacks were conducted on a single access point environment
Conclusion

- Deauthentication attack and Channel Switch attack both succeeded
- Impact on the wireless clients depend on used attack frame rate
- Only the deauthentication attack was detected by Aerohive WiPs
- 802.11w protects against deauthentication attack, channel switch and quiet attack remain unaddressed
Future work

- Locate attacker, combining 802.11-based positioning and frame thresholds per AP

- Investigate other relevant attacks that potentially threaten the availability of SURFwireless and determine the threshold value for Aerohive WiPs.

- Investigate the possibility to extend the current 802.11w amendment to support all frames if client is authenticated.
Questions?