802.11b Firmware-Level Attacks

Mike Kershaw <dragorn@kismetwireless.net>

Joshua Wright <jwright@hasborg.com>

September 29, 2006

1 Abstract

Denial of Service (DoS) attacks are a common threat to 802.11 wireless networks. Using widely available software and an inexpensive wireless LAN card, an attacker can halt the service of a wireless LAN at their whim. While very effective, these tools lack persistence in their operation – when the attacker stops the attack or leaves the range of the victim network, client workstations automatically resume their connectivity to the network.

This paper describes a new style of DoS attack against 802.11 networks that abuses flaws in the firmware of popular 802.11 wireless cards. The impact of this attack is more damaging than other 802.11 DoS attacks, requiring as few as two packets from an attacker to deny service to all target users, often requiring a system restart to recover from the attack. It is the author's hope that the public disclosure of this flaw will motivate 802.11 product manufacturers to resolve firmware flaws in their products, and to make those updates freely available to customers.

2 Summary

When an 802.11b wireless card from a variety of manufacturers is in a state where it expects a probe response packet, a bug exists in the firmware by which a maliciously injected probe response with the SSID tag length set to 0 can cause a lockup of the card itself, and depending on the platform and drivers, of the host operating system.

Once the 802.11b card has locked, it nearly always requires a reset of the adapter (via eject/insert for PCMCIA and USB adapters or a full reboot for PCI or other adapters). Some operating systems and drivers require a full reboot to reinitialize the driver.

3 Details

The 802.11 specification makes extensive use of management frames for a variety of functions including controlling access to the medium, advertising wireless service availability, station authentication and association, and power management. All 802.11 frames use the same standard header to identify packet source, destination, network identification information and frame type (data, management or control). Management frames utilize fixed or variable length fields in the packet payload to identify the various functions they perform.

When a wireless client or station (STA) wishes to communicate on the network, they first complete the active scanning procedure defined by the IEEE 802.11 specification. When seeking wireless network access, the STA will initially send frames requesting access to any available network in the form of probe request management frames. Available access points (AP's) will respond with probe response management frames, giving the station the necessary information to begin the authentication and association process.

Tables 1 and 2 identify the layout of a standard 802.11 frame header, with an expanded view of the frame payload. The expanded frame payload is typical of a probe response frame from an access point - three fixed length parameters (basic service set timestamp, beacon interval and capability information) followed by one or more variable length options.

Description	frame ctrl.	duration	addr 1	addr 2	addr 3	seq. ctrl	payload
Size (bytes)	2	2	6	6	6	2	variable

Table 1: Standard 802.11 Header

Description	Header (above)	timestamp	beacon interval	capability	*tagged parameters*
Size (bytes)	24	8	2	2	*n*

Table 2: Probe Response Management Frame

Variable length options are expressed with an element ID or tag type, followed by a length in bytes, followed by the actual management information. This is illustrated in table 3.

Description	Element ID	Element Length	Element Data
Size (bytes)	1	1	*n*

Table 3: 802.11 Tagged Parameter

The 802.11 specification provides several optional pieces of information in the form of variable length management fields. A partial list of variable length management fields is listed in table 4 (length is expressed in bytes).

Element ID	Description	Min Length	Max Length
0	Service Set Identifier (SSID)	0	32
1	Supported data rates	1	8
2	Frequency Hopping Set	5	5
3	Distribution System Set	1	1
4	Contention Free Set	6	6
5	Traffic Indication Message	5	254
6	Independent Basic Service Set	2	2
16	Privacy Challenge Text	1	253

Table 4: Variable-length management fields

Element ID 0 is used to identify the service set identifier (SSID) of the network, or the “network name”. In the case of a probe request from a STA, the SSID element ID is set in the management frame with a length of 0. This is a special case for variable length management frames to indicate a “broadcast” SSID, and is the only element ID that can be of a length less than 1.

When an AP receives a probe request with a broadcast SSID, the AP can be optionally configured to respond with the network SSID. This is largely considered to be a security risk on wireless networks, so many organizations have opted to disable this feature in the AP and preconfiguring their wireless STA’s with the name of the configured SSID. This is commonly referred to as a “cloaked” SSID.

When a station queries the AP for the network SSID in a probe request frame with the active scanning procedure, the AP will respond with a probe response that uses a specially formatted SSID element ID, as shown in table 5.

	Element ID	Size	Data
Value	0	1	0x20

Table 5: Cloaked SSID Tagged Parameter Response

Where the ASCII representation for the value 0x20 is the standard space character.

In this fashion, the AP can still comply with the 802.11 specification and answer probe request frames, but avoids disclosing the actual SSID used by the network.

A flaw in the firmware of 802.11 wireless cards was first discovered by Seng Ooh Toh, a student at the Georgia Institute of Technology in a group research paper titled "Wireless Intrusion Detection and Response, Final Report". Toh discovered that a probe response frame from an access point that had the SSID element ID set with a length of 0 would cause some wireless network cards to stop responding. This is not an illegal use of the SSID element ID tag according to the IEEE 802.11 MAC specification, but is improbable since a probe response would never use the reserved "broadcast" value that is interpreted with a tag length of 0.

With additional research, we discovered that this flaw is widespread among popular 802.11 wireless cards. Furthermore, the implementation of an attack tool to exploit this weakness was simple, and very effective.

When a card running a vulnerable firmware version receives a probe-response packet containing the SSID tagged parameter with the length set to 0, it often experiences a complete lockup (resulting in timeouts or lockups in the driver and physical symptoms such as freezing of the status LEDs at the current display values).

Recovery from this attack often required a full system reboot, or the removal and reinsertion of the affected card. We were unable to recover a victim machine in all cases without a full power-cycle and reinitialization of the 802.11 card firmware.

4 Attack Methods

Mounting an attack against this vulnerability is trivial. An attacker can force a STA into a position where they will automatically start sending probe request frames by abusing other weaknesses in the 802.11 protocol. This is typically performed by sending spoofed "disassociate" requests with the source MAC and BSSID of the legitimate access point, an attack which is available in numerous publicly available tools. Once an attacker coerces a STA to disassociate from their legitimate network, they simply wait for a probe request frame from the victim, as it starts looking for an alternate access point for access. The attacker then submits a malformed probe response frame, which causes the STA to stop functioning.

A successful attack can be completed in less than a second, but may take as much as a minute or longer of repeated attack. It is crucial that the malicious probe response from the attacker reach the client before a legitimate probe response from the AP. Timing in reception of probe-request packets, transmission of the malicious response and radio propagation time all affect the chances of a successful attack. The effectiveness of this attack can be be assessed remotely by monitoring the number of probe-requests which are received after each disassociation.

It is important to note that this attack may be launched from close physical proximity to the target network, or from a significant distance if an attacker uses a hi-gain antenna or wireless amplifier. With a parabolic antenna that utilizes a wide beam width, it is conceivable for an attacker to launch an attack against a significanly larger target, such as several city blocks.

5 Attack Code

Proof of concept code was written by modifying the hunter_killer tool included in the Airjack utilities to detect probe request packets, and to transmit a malicious response packet. For every non-probe request packet seen the code transmits a series of deauthentication and disassociation packets, and for every probe request a poisoned response is sent. This produced a very effective attack tool, capable of causing large networks of wireless clients to cease operation in a very short time.

This code is easily modified to run on any driver system which supports raw packet transmission (currently Linux and BSD systems).

6 Detection

Detection of a current attack is trivial – simply identify packets that are probe responses containing an element ID of 0 with a length of 0. Client 802.11b cards in monitor mode are not vulnerable to this attack, as they would not attempt to process a probe-response packet, and may be used to capture malicious traffic for the purposes of identifying an attack.

Detection of this attack has been added to Kismet (http://www.kismetwireless.net), which will generate a NULL-PROBERESP event when this activity is observed. Wireshark (http://www.wireshark.org) can be configured to report this malicious activity with the following filter rule:

```
wlan.fc.type_subtype eq 5 and wlan_mgt.tag.number eq 0 and wlan_mgt.tag.length eq 0
```

7 Mitigation Techniques

Unfortunately, little can be done to mitigate the effectiveness of this attack. Selecting 802.11 wireless cards that are confirmed as not vulnerable to this attack is recommended, but is little consolation to those organizations who have already deployed vulnerable equipment. Organizations should express their concern regarding this attack to their wireless LAN equipment vendors, encouraging them to provide patched firmware for vulnerable products. Organizations should apply patched firmware when it becomes available to AP's and end-user workstations.

8 Vulnerable Hardware

The following list of firmware has been tested by the authors, and confirmed to be vulnerable to the attack method we describe in this paper.

- Agere
  - Firmware 6.04, vulnerable, card becomes inoperative.
  - Firmware 6.06, vulnerable, card becomes inoperative.
  - Firmware 6.08, vulnerable, card becomes inoperative.
- Intersil Prism 2
  - Firmware 0.8.3, vulnerable, card becomes inoperative.
- Intersil Prism 2.5
  - Firmware 1.3.6, 1.4.9, vulnerable, card becomes inoperative.
- Intersil Prism 3.0

  - *Not* vulnerable.

- Apple Airport (Agere based)
  - Vulnerable, card becomes inoperative and OS X requires a reboot to reinitialize the card.
- Cisco
  - Potentially vulnerable, testing not conclusive.
- Atmel
  - Firmware 0.100.2.16, *not* vulnerable.

Other hardware and firmware versions may be vulnerable, but were not available for testing. 802.11a and 802.11g firmware may also be vulnerable to this attack, but drivers capable of raw packet transmission (802.11a) and lack of available hardware (802.11g) prevented testing.

9 Vendor Notification

Before releasing public information about this flaw in 802.11 WLAN card firmware, the authors went to extensive lengths to contact WLAN card manufacturers and the Wireless Fidelity (WiFi) group in an attempt to give them the opportunity to resolve this issue, making patched firmware available to customers. Unfortunately, most vendors chose simply not to respond to our pleas for assistance in resolving this flaw. We present a time line of contact information starting on 2003/1/9 in our attempt to notify vendors of this flaw.

- 2002/12/28
  PoC code completed. Flaw confirmed in multiple cards used by the authors.
- 2003/1/9
  Sent e-mail to Mark Shapiro of Davis-Morrin Communications, public relations representative for ORiNOCO, notifying him of the discovered flaw, and asking for assistance to get in contact with the appropriate representatives at Agere/ORiNOCO to address this issue. Joshua Wright spoke with Mr. Shapiro briefly, and it was agreed that Mr. Shapiro would respond to Wright's e-mail message with additional information once he located the correct contacts at Agere.
  Sent e-mail to Greg Ennis, WiFi Alliance technical director, asking for his assistance in contacting Intersil and Agere/Proxim to report this vulnerability.
- 2003/1/29
  Received no response from Shapiro or Ennis to date.
- 2003/1/30
  Sent a follow-up e-mail to Mr. Shapiro and Mr. Ennis, asking for their assistance in contacting the appropriate people at Agere/Proxim and Intersil.
  Received a response from Mr. Shapiro indicating that Agere was aware of the flaw in their firmware and suggested I contact Richard Edgar at Agere for further communication regarding this issue.
- 2003/1/31
  Sent e-mail to Richard Edgar, Agere ORiNOCO Product Manager, notifying him of the discovered flaw and asking for his assistance in working with the appropriate group at Agere on resolving this issue.
- 2003/5/15
  No contact from either Mr. Edgar or Mr. Ennis to date.

10 Change Log

- 2006/09/26
  - Initial Release.

References

[1] Y. Lim, V. Kanotra, N. Namjoshi, S.Toh: *Wireless Intrusion Detection and Response, Final Report*, Georgia Institute of Technology, School of Electrical and Computer Engineering

[2] M. Lynn, R. Baird: *Advanced 802.11 Attack*, Blackhat 2002 presentation, http://802.11ninja.net

[3] ANSI/IEEE: *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 1999, http://getieee.ieee.org/