Wireless LAN Consortium
Wireless WPA AP MAC Test Suite v2.4 Report

UNH InterOperability Laboratory — 121 Technology Drive, Suite 2 — Durham, NH 03824 — +1-603-862-0090

January 3, 2013
Report Rev. 1.0

Joe Vendor
Magic Wireless Company
52 OFDM Drive
Mimo, NH 010111

Mr. Vendor,

Enclosed are the results from the Wireless WPA STA MAC Test Suite testing performed on the:

Magic Device Name MD-360 802.11 a/b/g Station

This testing pertains to a set of standard requirements, put forth in the IEEE Std. 802.11-2007 Edition, as well as WPA for 802.11 v2.0. The tests performed are part of the WPA STA MAC Test Suite v2.4, which is available on the UNH-IOL's website:

ftp://ftp.iol.unh.edu/pub/wireless/TestSuites/mac/802.11_WPA_STA_MAC_Test_Suite_v2.4.pdf

Issues Observed While Testing
1.1.2. TKIP Replay Protection: The DUT was observed to transmit a TKIP-PSK encrypted ICMP Echo response upon the reception of a TKIP-PSK encrypted ICMP Echo request that had an improperly incremented TSC value.

As always, we welcome any comments regarding this Test Suite. If you have any questions about the test procedures or results, please contact me via e-mail at ext1@iol.unh.edu or by phone at +1-603-862-2263.

Regards,

Eric X. Tester

UNH-IOL
2013.01.03 16:05:01 -05'00'

DIGITAL SIGNATURE INFORMATION

This document was created using an Adobe digital signature. A digital signature helps to ensure the authenticity of the document, but only in this digital format. For information on how to verify this document's integrity proceed to the following site:

http://www.iol.unh.edu/certifyDoc/

If the document status still indicates "Validity of author NOT confirmed", then please contact the UNH-IOL to confirm the document's authenticity. To further validate the certificate integrity, Adobe 6.0 should report the following fingerprint information:

MD5 Fingerprint: **EEE1 7A82 7806 EB21 AF94 F189 E4BE 361B**
SHA-1 Fingerprint: **ECFB 7FAF AB4A 0832 2408 E965 9F5C E3F2 D784 AAAB**

Table 1 - Result Key - The following table contains possible results and their meanings

Result	Interpretation
PASS	The DUT was observed to exhibit conformant behavior.
FAIL	The DUT was observed to exhibit non-compliant behavior.
PASS with Comments	The DUT was observed to exhibit conformant behavior, however, additional explanation of the situation is included.
Warning	The DUT was observed to exhibit behavior that is not recommended.
Informative	Results are for informative purposes only and are not judged on a pass or fail basis.
Refer to Comments	From the observations, a valid pass or fail could not be determined. An additional explanation of the situation is included.
Not Applicable	The DUT does not support the technology required to perform these tests.
Not Available	Due to testing station or time limitations, the tests could not be performed, or were performed in a limited capacity.
Not Tested	Not tested due to time constraint of the test period.
Borderline	The observed values of the specified parameter are valid at one extreme, and invalid at the other.

Table 2 - Setup and Configuration Information

Product	
Manufacturer	Magic Device Machine
Model	MD-360
MAC Address	00:02:bc:24:36:1f
Hardware Version	X4
Firmware Version	2.34.3
IOL Label	WIRELESS-MDM-0000008632
PSK	wireless
Test System Hardware	
RF Isolated Environment	USC-26 RF/EMI Isolation Chamber 16'x 8' x 8' @ 100dB
Sniffer	Atheros DK4 Sniffer Station
Test Station	Atheros DK4 Testing Station

In many traces, identification frames were used to simplify result collecting. These frames are identified by their source MAC address (00:00:01:ba:bb:1e). Below is an example of an identification frame found in a trace:

No.	Info	Protocol	Source	Destination
1	Beacon frame, BI=100, SSID=MAC""	IEEE 802.11	Xerox_00:00:11	Broadcast
2	Part a: Non-Acknowledged Frames	Babble Frame	0.0.0.0	255.255.255.255
3	MSDU1 => ICMP Echo Request with Protocol Version > 0	Babble Frame	0.0.0.0	255.255.255.255
4	Echo (ping) request	ICMP	192.168.0.102	Vendor (abcd)
5	Acknowledgement	IEEE 802.11		Xerox_00:00:11
6	Clear-to-send	IEEE 802.11		Vendor (abcd)
7	Data	IEEE 802.11	Xerox_00:00:11	Vendor (abcd)

Rows highlighted in green are Management Frames.
Rows highlighted in blue are Control Frames.
Rows highlighted in white are Data Frames.
Rows highlighted in violet are ICMP Echo Requests/Responses

Fields or Frame excerpts highlighted in this reports are important and directly related to the issue being shown in the trace excerpt.

GROUP 1: FIELD CHECKING

Test # and Label	Part(s)	Result(s)
1.1.1: TKIP Countermeasures	**a**	**PASS**
	b	**PASS**
	c	**PASS**
	d	**PASS**
	e	**PASS**
	f	**PASS**

Comments on Test Procedure

Purpose: To verify that:

- the DUT can properly create and transmit TKIP-PSK encrypted frames.
- the DUT disassociates if two frames with invalid MIC values are received within 60 seconds of each other.
- the DUT does not transmit or receive frames during the 60-second blackout period.
- the DUT checks the FCS, ICV, and IV fields before checking the MIC.
- the DUT keeps track of MIC failures independent of which key was used.

When a BSS is using WPA TKIP, any station receiving an encrypted frame should check the FCS, ICV, and IV before checking the MIC. If all of these fields are valid, then the frame is to be decrypted and processed. In the case that any of these checks fail before checking the MIC, the frame is to be discarded. In the event that the MIC check fails, a MIC failure is to be recorded. If two MIC failures occur within a minute of each other, the STA is disassociated with a reason code of MIC Failure or unspecified failure, and enters into a 1-minute blackout period in which it is not allowed to receive or transmit frames.

Comments on Test Results

a. There were no issues uncovered during the testing process.

Test # and Label	Part(s)	Result(s)
1.1.2: TKIP Replay Protection	**a**	**PASS**
	b	**PASS**
	c	**PASS**
	d	**PASS**
	e	**FAIL**
	f	**Informative**

Comments on Test Procedure

Purpose: To verify that:

- the DUT initializes its TSC values properly.
- the DUT keeps separate TSC values for pairwise and group keys.
- the DUT increments its TSC by 1.
- the DUT detects replayed frames.

TKIP encryption uses a TSC to keep track of frame order. There is one TSC per encryption key, and it should be monotonically incrementing. As such, any frame that is received with a TSC less than the last received TSC is to be dropped. This counter should be initialized to 1 (TGi mandates 0), and is to be initialized whenever the associated key is initialized or refreshed. The TSC is a multi-byte quantity, and the rollover of the bytes needs to be properly handled.

Comments on Test Results

a-d. There were no issues uncovered during the testing process.

e. The DUT was observed to transmit a TKIP-PSK encrypted ICMP Echo response upon the reception of a TKIP-PSK encrypted ICMP Echo request that has an improperly incremented TSC value. The DUT should not transmit a TKIP-PSK encrypted ICMP Echo response upon the reception of a TKIP-PSK encrypted ICMP Echo request that has an improperly incremented TSC value. See IEEE 802.11-2007 Edition, subclause 8.3.2.6. Refer to Table 3 for more information regarding this test case.

f. The DUT was observed to NOT send a Deauthentication or Disassociation frame upon the reception of the second transmission of a TKIP-PSK encrypted ICMP Echo request containing an improperly incremented TSC value.

TRACE EVALUA TION:

Table 3
Test # 1.1.2: TKIP Replay Protection
From: 1.1.2.dk2 (802.11 a/b DK Sniffer)

No.	Info	Protocol	Source	Destination
508	Echo (ping) request	ICMP	IOL-TS	MD-360
509	Acknowledgement	IEEE 802.11	MD-360	IOL-TS
510	Echo (ping) reply	ICMP	MD-360	IOL-TS
511	Acknowledgement	IEEE 802.11	IOL-TS	MD-360
512-522	Beacon Frames were removed for convenience			
523	Echo (ping) request	ICMP	IOL-TS	MD-360
524	Acknowledgement	IEEE 802.11	MD-360	IOL-TS
525	Echo (ping) reply	ICMP	MD-360	IOL-TS
526	Acknowledgement	IEEE 802.11	IOL-TS	MD-360

|-Frame #508 (Data)
|-Frame Dump
|-0000 - 000F : 08 41 2C 00 00 23 4E C6 F0 3C 00 00 01 00 00 01
|-0010 - 001F : 00 23 4E C6 F0 3C 00 02 11 31 11 20 11 11 00 00
|-0020 - 002F : 4C 8D 9C 7C E7 F7 3D 49 DB 8A AA 68 B8 9A FB 72
|-0030 - 003F : 60 22 8D D1 83 B7 EB 11 F7 08 91 4F DC 46 31 03
|-0040 - 004F : C8 05 A4 67 11 72 D2 8B 47 52 4F BD EF 7E 6F 90
|-0050 - 005F : F8 3F 21 FA 51 CE 27 34 A0 E8 14 86 C6 FD 7D 1C
|-0060 - 006F : 57 20 1E D9 19 1D 17 1B 68 E6 C8 89 87 5D C1 4B
|-0070 - 0073 : 98 CE F9 91
|-TKIP
|-IV16: 0x1111
|-IV32: 0x00001111
|-MAC Header
|-Frame Control: 0x4108
|-Computed FCS: 0x91f9ce98
|-Frame FCS: 0x91f9ce98

|-Frame #523 (Data)
|-Frame Dump
|-0000 - 000F : 08 41 2C 00 00 23 4E C6 F0 3C 00 00 01 00 00 01
|-0010 - 001F : 00 23 4E C6 F0 3C 10 02 00 20 00 20 00 00 00 00
|-0020 - 002F : 74 4A 00 5E 14 2A 8C D6 5D 02 D5 ED E6 85 07 9D
|-0030 - 003F : CD 3C 1F 65 C3 38 75 0C 33 D2 41 87 CD 08 72 3D
|-0040 - 004F : 76 4C 95 45 2C 5E AB 6F FD 07 E1 C7 07 00 83 85
|-0050 - 005F : 72 9D E9 22 F0 B0 E5 BC EA A4 CF 28 86 BE 78 43
|-0060 - 006F : F5 7E E8 0D C9 82 0A 30 63 1E 5B 47 9B 60 D9 87
|-0070 - 0073 : B7 EE 1D 80
|-TKIP
|-IV16: 0x0000
|-IV32: 0x00000000
|-MAC Header
|-Frame Control: 0x4108
|-Computed FCS: 0x801deeb7
|-Frame FCS: 0x801deeb7