WLAN

The Wireless Local Area Network Consortium

WPA
Access Point MAC Layer Test Suite
Version 2.5

Technical Document

Last Updated: February 18, 2013

Wireless LAN Consortium
InterOperability Laboratory
University of New Hampshire

121 Technology Drive, Suit 2
Durham, NH 03824
Phone: +1-603- 862-2263
Fax: +1-603- 862-4181
http://www.iol.unh.edu/consortiums/wireless/

MODIFICATION RECORD

- February 2013 -Version 2.5
  Jackson Corson: updated the 802.11 references to the 2012 standard
- November 2008 - Version 2.4 Released
  Daniel Reynolds: Removed RCC reference. Removed "Invalid TSC" test case from test 1.1.1. Moved INFORMATIVE case from 1.1.1 to 1.1.2. Changed observable results in 1.1.2 parts a. and c. to include that 1 or 0 can be used.
- June 2007 - Version 2.3 Released
  Jon Zink: IEEE Std. 802.11i-2004 references changed to IEEE Std. 802.11-2007.
- June 2006 - Version 2.2 Released
  Anthony Murabito: corrected procedures and observable results. 802.11i reference now for 2004 instead of draft
- May 2005 - Version 2.1 Released
  MAC Team: Minor editorial changes.
- February 2005 - Version 2.0 Released
  Matt Newcomb: Renumbered Tests, updated procedures, and observable results.
- February 2004 - Version 1.0 Released

ACKNOWLEDGMENTS

The University of New Hampshire would like to acknowledge the efforts of the following individuals in the development of this test suite.

Chris Kane	University of New Hampshire
Kevin Karcz	University of New Hampshire
Matt Newcomb	University of New Hampshire
Chris Polanec	University of New Hampshire
Anthony Murabito	University of New Hampshire
Jonathan Zink	University of New Hampshire
Daniel Reynolds	University of New Hampshire

INTRODUCTION

Overview

The University of New Hampshire's InterOperability Laboratory (UNH-IOL) is an institution designed to improve the interoperability of standards based products by providing an environment where a product can be tested against other implementations of a standard. This particular suite of tests has been developed to help implementers evaluate the functionality of WPA TKIP-PSK encryption in their APs.

These tests are designed to determine if a product conforms to specifications defined in IEEE Std. 802.11-2012 and WPA for 802.11 version 2.0. Successful completion of all tests contained in this suite does not guarantee that the tested device will operate with other devices. However, combined with satisfactory operation in the IOL's interoperability test bed, these tests provide a reasonable level of confidence that the device under test (DUT) will function properly with the MAC layer of other devices when WPA TKIP-PSK is used.

Organization of Tests

The tests contained in this document are organized to simplify the identification of information related to a test and to facilitate in the actual testing process. Each test contains an identification section that describes the test and provides cross-reference information. The discussion section covers background information and specifies why the test is to be performed. Tests are grouped in order to reduce setup time in the lab environment. Each test contains the following information:

Test Number

The Test Number associated with each test follows a simple grouping structure. Listed first is the Test Group Number followed by the test's number within the group. This allows for the addition of future tests to the appropriate groups of the test suite without requiring the renumbering of the subsequent tests.

Purpose

The purpose is a brief statement outlining what the test attempts to achieve. The test is written at the functional level.

References

The references section lists cross-references to the IEEE 802.11 standards and other documentation that might be helpful in understanding and evaluating the test results.

Resource Requirements

The requirements section specifies the test hardware and/or software needed to perform the test. This is generally expressed in terms of minimum requirements, however in some cases specific equipment manufacturer/model information may be provided.

Last Modification

This specifies the date of the last modification to this test.

Discussion

The discussion covers the assumptions made in the design or implementation of the test, as well as known limitations. Other items specific to the test are covered here.

Test Setup

The setup section describes the initial configuration of the test environment. Small changes in the configuration should be included in the test procedure.

Procedure

The procedure section of the test description contains the systematic instructions for carrying out the test. It provides a cookbook approach to testing, and may be interspersed with observable results.

Observable Results

This section lists the specific observables that can be examined by the tester in order to verify that the DUT is operating properly. When multiple values for an observable are possible, this section provides a short discussion on how to interpret them. The determination of a pass or fail outcome for a particular test is often based on the successful (or unsuccessful) detection of a certain observable.

Possible Problems

This section contains a description of known issues with the test procedure, which may affect test results in certain situations. It may also refer the reader to test suite appendices and/or whitepapers that may provide more detail regarding these issues.

TABLE OF CONTENTS

GROUP 1: Field Checking

Scope: The following tests cover MAC operations specific to the reception and processing of TKIP-PSK encrypted frames.

Overview: These tests are designed to verify that the device under test properly handles WPA TKIP-PSK encrypted frames, and that station is not retransmitting a frame previously transmitted from another station. The MAC functions explored are defined in IEEE Std. 802.11-2012 and WPA for 802.11 version 2.0.

Test #1.1.1: TKIP Countermeasures

Purpose: To verify that:

- the DUT can properly create and transmit TKIP encrypted frames.
- the DUT disassociates only if two frames with invalid MICs 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 before checking the MIC.
- the DUT keeps track of MIC failures independent of which key was used.

References:

[1] IEEE Std. 802.11-2007, Clause 11.4.2.4, 11.4.2.3
[2] WPA for 802.11 version 2.0, Appendix H, Figure 8

Resource Requirements:

- A testing station (TS) that is capable of transmitting user defined MAC frames and does not participate in the MAC protocol
- A monitor configured for capturing and analyzing MAC frames
- An Ethernet STA (STA-E) on the DS that is capable of receiving and responding to ICMP echo requests

Last Updated: November 20, 2008

Discussion: 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.

Test Setup: Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Place STA-E on the same DS as the DUT. Enable WPA TKIP encryption and PSK on the DUT. Set the PSK to “wireless” (without quotes).

Table 1 - Test Frame(s)

Frame Label	Description
MSDU1	ICMP Echo Request containing a length of 32 bytes
MSDU2	ICMP Echo Request containing a length of 32 bytes, with a MIC of all zeros
MSDU3	ICMP Echo Request containing a length of 32 bytes, with a MIC one less than the computed MIC
MSDU4	ICMP Echo Request containing a length of 32 bytes, with an invalid FCS and an invalid MIC
MSDU5	ICMP Echo Request containing a length of 32 bytes, with an invalid ICV and an invalid MIC
MSDU6	ARP Request containing an invalid MIC

Procedure:

Part a: Proper Encryption

1. Instruct the TS to associate and successfully complete the 4-way handshake with the DUT.
2. Instruct the TS to send MSDU1 and wait for a response
3. Repeat steps 1 and 2, two more times within a minute.
4. Observe transmissions from the DUT.

Part b: All Zero MIC

1. Instruct the TS to associate and successfully complete the 4-way handshake with the DUT.
2. Instruct the TS to send MSDU2.
3. Instruct the TS to send MSDU2.
4. Instruct the TS to send MSDU1.
5. Wait 1 minute.
6. Instruct the TS to deauthenticate the DUT.
7. Observe transmissions from the DUT.

Part c: MIC One Less Than the Proper Value

1. Instruct the TS to associate and successfully complete the 4-way handshake with the DUT.
2. Instruct the TS to send MSDU3.
3. Instruct the TS to send MSDU3.
4. Instruct the TS to send MSDU1.
5. Wait 1 minute.
6. Instruct the TS to deauthenticate the DUT.
7. Observe transmissions from the DUT.

Part d: Invalid FCS and MIC

1. Instruct the TS to associate and successfully complete the 4-way handshake with the DUT.
2. Instruct the TS to send MSDU4.

3. Instruct the TS to send MSDU4.
4. Instruct the TS to send MSDU1.
5. Wait 1 minute.
6. Instruct the TS to deauthenticate the DUT.
7. Observe transmissions from the DUT.

Part e: Invalid ICV and MIC

1. Instruct the TS to associate and successfully complete the 4-way handshake with the DUT.
2. Instruct the TS to send MSDU5.
3. Instruct the TS to send MSDU5.
4. Instruct the TS to send MSDU1.
5. Wait 1 minute.
6. Instruct the TS to deauthenticate the DUT.
7. Observe transmissions from the DUT.

Part f: Invalid ICV and MIC

1. Instruct the TS to associate and successfully complete the 4-way handshake with the DUT.
2. Instruct the TS to send MSDU6.
3. Instruct the TS to send MSDU3.
4. Instruct the TS to send MSDU1.
5. Wait 1 minute.
6. Instruct the TS to deauthenticate the DUT.
7. Observe transmissions from the DUT.

Observable Results:

The DUT should:

a. respond to every transmission of MSDU1 with an ACK followed by an ICMP Echo response. (parts a-g).
b. transmit an ACK for and discard both transmissions MSDU2. The DUT should transmit a disassociation or deauthentication frame with a reason code indicating MIC failure, in response to the second transmission of MSDU2.
c. transmit an ACK for and discard both transmissions MSDU3. The DUT should transmit a disassociation or deauthentication frame with a reason code indicating MIC failure, in response to the second transmission of MSDU3.
d. not respond to MSDU4 with an ACK nor process the frame.
e. transmit an ACK for and discard both transmissions MSDU5.The DUT should not send a disassociation or deauthentication in response to any transmission of MSDU5.
f. transmit an ACK for and discard both MSDU6 and MSDU3. The DUT should transmit a deauthentication or disassociation frame with a reason code indicating MIC failure in response to MSDU3.

Possible Problems: None.

Test #1.1.2: TKIP Replay Protection

Purpose: To verify that:

- the DUT initializes its TSCs when the corresponding key is initialized or refreshed.
- the DUT initializes the TSC for pairwise and group keys to 1.
- the DUT keeps separate TSC values for pairwise and group keys.
- the DUT increments its TSC by 1.
- the DUT properly forms the TSC in TKIP encrypted frames.
- the DUT detects replayed frames.
- the DUT can properly handle the TSC spanning bytes and rollover.

References:

[1] IEEE Std. 802.11-2007, Clause 11.4.2.4, 11.4.2.3
[2] WPA for 802.11 version 2.0, Appendix H, Figure 8

Resource Requirements:

- A testing station (TS) that is capable of transmitting user defined MAC frames and does not participate in the MAC protocol
- A monitor configured for capturing and analyzing MAC frames
- An Ethernet STA (STA-E) on the DS that is capable of receiving and responding to ICMP echo requests

Last Updated: November 20, 2008

Discussion: 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, also acceptable), and is to be initialized whenever the associated key is initialized or refreshed. The TSC is a multibyte quantity, and the rollover of the bytes needs to be properly handled.

Test Setup: Place the DUT, TS, and sniffer in a RF isolated environment and in range of each other. Place STA-E on the same DS as the DUT. Enable WPA TKIP encryption and PSK on the DUT. Set the PSK to “wireless” (without quotes).

Table 2 - Test Frame(s)

Frame Label	Description
MSDU1	ARP Request from the TS to STA-E
MSDU2	ICMP Echo Request from the TS to STA-E
MSDU3	Deauthentication frame from the TS to the DUT containing a status code of 1
MSDU4	ICMP Echo Request from the TS to STA-E containing a previously used TSC
MSDU5	ICMP Echo Request from the TS to STA-E containing a TSC of 0xff
MSDU6	ICMP Echo Request from the TS to STA-E containing a TSC of 0x100
MSDU7	ICMP Echo Request from the TS to STA-E containing a TSC of 0xffff
MSDU8	ICMP Echo Request from the TS to STA-E containing a TSC of 0x10000
MSDU9	ICMP Echo Request from the TS to STA-E containing a TSC of 0xffffff
MSDU10	ICMP Echo Request from the TS to STA-E containing a TSC of 0x1000000
MSDU11	ICMP Echo Request from the TS to STA-E containing a TSC with all bits set
MSDU12	ICMP Echo Request from the TS to STA-E containing a TSC with no bits set

Procedure:

Part a: TSC Initialization

1. Instruct the TS to associate and successfully complete the 4-way handshake with the DUT.
2. Instruct the TS to send MSDU1 and wait for a response.
3. Instruct the TS to send MSDU2 and wait for a response.
4. Observe transmissions from the DUT.

Part b: TSC Increasing

1. Instruct the TS to associate and successfully complete the 4-way handshake with the DUT.
2. Instruct the TS to send MSDU2.
3. Repeat step 1 two more times.
4. Observe transmissions from the DUT.

Part c: Key Initialization/Refresh

1. Instruct the TS to associate and successfully complete the 4-way handshake with the DUT.
2. Instruct the TS to send MSDU3.
3. Instruct the TS to associate and successfully complete the 4-way handshake with the DUT.
4. Instruct the TS to send MSDU1 and wait for a response.
5. Instruct the TS to send MSDU2 and wait for a response.
6. Observe transmissions from the DUT.

Part d: Replay Detection

1. Instruct the TS to associate and successfully complete the 4-way handshake with the DUT.
2. Instruct the TS to send MSDU2.
3. Instruct the TS to send MSDU2.
4. Instruct the TS to send MSDU4 with the TSC from the first transmission of MSDU2 in this part.
5. Repeat step 4.
6. Instruct the TS to send MSDU1.
7. Observe transmissions from the DUT.

Part e: TSC Rollover

1. Instruct the TS to associate and successfully complete the 4-way handshake with the DUT.
2. Instruct the TS to send MSDU5 and wait a response.
3. Instruct the TS to send MSDU6 and wait a response.
4. Instruct the TS to send MSDU7 and wait a response.
5. Instruct the TS to send MSDU8 and wait a response.
6. Instruct the TS to send MSDU9 and wait a response.
7. Instruct the TS to send MSDU10 and wait a response.
8. Instruct the TS to send MSDU11 and wait a response.
9. Instruct the TS to send MSDU12 and wait a response.
10. Observe transmissions from the DUT.

Observable Results:

The DUT should:

a. transmit the first group key with a TSC of 1 or 0. The DUT should also use a separate monotonically incrementing TSC for each TK and each GTK.
b. use monotonically incrementing TSCs for each ICMP Echo Response transmitted.
c. transmit the first group key with a TSC of 1 or 0. The DUT should also use a separate monotonically incrementing TSC for each TK and each GTK.
d. discard both transmissions of MSDU4 after transmitting an ACK for each one. The DUT should also reply to MSDU1 with an ARP Response.
e. forward the ICMP Echo Response to MSDUs5-11. The DUT should also discard MSDU12 after transmitting an ACK for it.

INFORMATIVE:

f. The DUT may send a deauthentication or disassociation in response to the second transmission of MSDU4. [2] does not specify if an invalid TSC qualifies as a MIC failure event, but the current version of 802.11i specifies that it does not constitute a MIC failure event. (part d).

Possible Problems: None.

Appendix A: Abbreviations

Abbreviation	Description
AP	Access Point
ARP	Address Resolution Protocol
BSS	Basic Service Set
DS	Distribution System
DUT	Device Under Test
FCS	Frame Check Sequence
GTK	Group Transient Key
ICMP	Internet Control Message Protocol
ICV	Integrity Check Value
IV	Initialization Vector
MAC	Media Access Control
MIC	Message Integrity Code
MSDU	MAC Protocol Data Unit
MSDU	MAC Service Data Unit
PSK	Pre-Shared Key
PTK	Pairwise Transient Key
STA	Station
TK	Transient Key
TKIP	Temporal Key Integrity Protocol
TS	Testing Station
TSC	TKIP Sequence Counter
WPA	WiFi Protected Access