Key Reinstallation Vulnerability Detection Test Plan

Version 2.5

10900-B Stonelake Boulevard, Suite 126
Austin, TX 78759

Phone: 512.498.9434 • Fax: 512.498.9435 • Email: support@wi-fi.org
www.wi-fi.org

Latest version available at: https://www.wi-fi.org/members/certification-programs

THIS DOCUMENT IS PROVIDED "AS IS" AND WITHOUT WARRANTY OF ANY KIND. TO THE GREATEST EXTENT PERMITTED BY LAW, WI-FI ALLIANCE DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF TITLE, NONINFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. WI-FI ALLIANCE DOES NOT WARRANT THAT THIS DOCUMENT IS COMPLETE OR WITHOUT ERROR AND DISCLAIMS ANY WARRANTIES TO THE CONTRARY. NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE SUITABILITY OR NON-SUITABILITY OF A PRODUCT OR A SERVICE FOR CERTIFICATION UNDER ANY CERTIFICATION PROGRAM OF WI-FI ALLIANCE OR ANY THIRD PARTY.

Table of contents

List of tables

List of figures

1 Overview

1.1 Scope and purpose

This document is the test plan for validating if a device operating in the 2.4 GHz, 5 GHz or 60 GHz band is vulnerable to key reinstallation vulnerabilities.

The identified security vulnerabilities [1] exploit the security protocol implementation, including 4-way handshake and group key handshake, to reinstall a key that is already in use, and thereby reset nonces and/or replay counters associated to this key. Depending on the data confidentiality protocol being used, packets may be decrypted, replayed, and/or forged in one or both directions (AP → STA / STA → AP).

The primary goal of this test plan is to identify if a DUT implementation is vulnerable to the security vulnerabilities by utilizing a Security Vulnerability Detection (SVD) tool that has been developed to detect and report the identified security vulnerabilities on AP and STA devices.

1.2 Definition of devices under test

The device under test (DUT) may be an Access Point (APUT) or Station (STAUT). The general characteristics of the DUT are entered in the Wi-Fi Alliance website registration system and are summarized in Table 1.

Prior to submission to the authorized test labs, the implementer shall complete the following capabilities declaration table for use in performing this certification testing.

Table 1. DUT general capabilities declaration

Item	Question	Test case	Vendor response
1	Does the APUT support the 802.11r Fast BSS Transition feature using WPA2-Personal?	4.2.1	Yes/No
2	Does the APUT support 802.11r Fast BSS Transition using WPA2-Enterprise?	4.2.1	Yes/No
3	Does the APUT support FILS Shared Key authentication?	4.3.1	Yes/No
4	Does the STAUT support accepting plaintext EAPOL Message 3 after installation of the session key?	[4]	Yes/No
5	Does the STAUT perform encryption and decryption functions in the Wireless NIC?	[4]	Yes/No
6	Does the STAUT support generation of Temporal PTK (TPTK) construction?	[4]	Yes/No
7	Is the DUT an 802.11a/b/g/n/ac device?	For APUT: 4.2.1, 4.3.1 For STAUT: [4]	Yes/No
8	Is the DUT an 802.11ad (60 GHz) device?	5.2.3, 5.3.1	Yes/No

1.3 References

The documents listed in this section are included in requirements made in the body of this test plan. Knowledge of their contents is required for the understanding and implementation of this test plan. If a listing includes a date or a version identifier, only that specific version of the document is required. If the listing includes neither a date nor a version identifier, the latest version of the document is required.

[1] Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2, https://papers.mathyvanhoef.com/ccs2017.pdf

[2] IEEE Standard for Information technology-Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Std 802.11-2016, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6178212&isnumber=6178210

[3] IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 1: Fast Initial Link Setup", IEEE Std 802.11ai-2016, https://standards.ieee.org/findstds/standard/802.11ai-2016.html

[4] QuickTrack test plans, https://wi-fi-login.force.com/membersupportportal/s/topic/0TO4y000000U27DGAS/test-plans

1.4 Acronyms and definitions

1.4.1 Acronyms and abbreviations

Table 2 defines the acronyms and abbreviations used throughout this document. Some acronyms and abbreviations are commonly used in publications and standards defining the operation of wireless local area networks, while others have been generated by Wi-Fi Alliance. Refer to the Wi-Fi Alliance Acronyms Terms Definitions document for a complete list of approved acronyms and abbreviations.

Table 2. Acronyms and abbreviations

Acronyms	Definition
AKM	Authentication Key Management
ANonce	Authenticator nonce
AP	Access Point
CCMP PN	Counter Mode CBC-MAC Protocol packet number
CVE	Common Vulnerability and Exposure
DHCP	Dynamic Host Configuration Protocol
DUT	Device Under Test
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN

Acronyms	Definition
FT	Fast Transition
FILS	Fast Initial Link Setup
GTK	Group Temporal Key
HLP	Higher layer protocol
IGTK	Integrity Group Temporal Key
OOB	Out of the box
PFS	Perfect Forward Secrecy
PMF	Protected Management Frames
PMK	Pairwise Master Key
PTK	Pairwise Transient Key
SK	Shared Key
SSID	Service Set Identifier
STA	Station
SVD	Security Vulnerability Detection
TPTK	Temporary Pairwise Transient Key
WNM	Wireless Network Management

1.4.2 Definitions

This test plan contains no special definitions.

2 Test tools, methodology and approach

This section defines the tools, methodology, and approach for testing and certifying devices for Key Reinstallation Vulnerability Detection certification.

2.1 Sniffer

A sniffer test tool is required to be used for test cases throughout this test plan. The sniffer test tool requirements are:

- Dual band operation (2.4 GHz and 5 GHz) - applicable to test cases in Section 4
- Capable of dissecting 802.11 Management, Control and Data frames
- 60 GHz operation (only applies to 60 GHz testing) - applicable to test cases 5.2.3, 5.3.1

2.2 Wi-Fi Test Suite software

The Wi-Fi Alliance's Wi-Fi Test Suite provides configuration, test control, traffic generation, and results analysis services. Unless otherwise noted, the entire test plan may be executed in a fully automated manner using Wi-Fi Alliance-distributed Wi-Fi Test Suite Command Scripts and the Wi-Fi Test Suite Unified CAPI Console. Additional information is available through the member website https://www.wi-fi.org/members/certification-testing/wi-fi-test-suite.

2.3 Basic system test configuration

Figure 1 depicts the basic system test configuration for Key Reinstallation Vulnerability Detection APUT testing in manual mode.

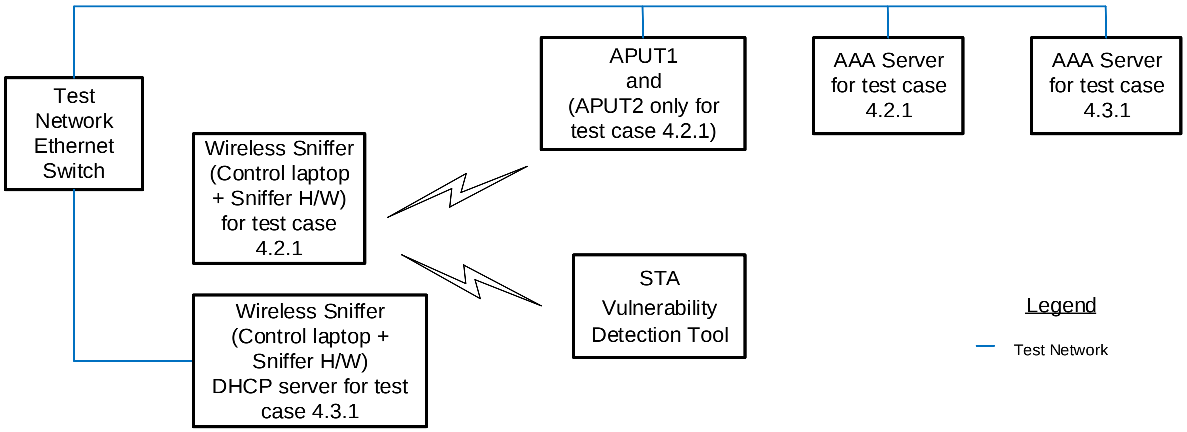
Test Network Ethernet Switch
Wireless Sniffer (Control laptop + Sniffer H/W) for test case 4.2.1
Wireless Sniffer (Control laptop + Sniffer H/W) DHCP server for test case 4.3.1
APUT1 and (APUT2 only for test case 4.2.1)
AAA Server for test case 4.2.1
AAA Server for test case 4.3.1
STA Vulnerability Detection Tool
Legend
Test Network

Figure 1. Key Reinstallation Vulnerability Detection test configuration for APUT - manual mode

2.4 Test bed capability requirements

2.4.1 Test bed STA requirements

Table 3 defines the general test configuration for test cases for the Security Vulnerability Detection tool acting as a STA. If required, the following parameter values are modified for specific test cases.

Table 3. Test bed STA default parameters

Parameter	Description	Security Vulnerability Detection tool acting as a STA
SSID	Service Set Identifier	N/A
Security	802.11 Security method	WPA2-Personal
Cipher Suite	Cipher Suite	CCMP (00-0F-AC:4)
Passphrase	Key used for encryption	12345678
DHCP	DHCP client	Enabled
PMF	Protected management frame	OOB

2.4.2 Test bed AP requirements (60 GHz)

Table 4 defines the general test configuration for test cases for the Security Vulnerability Detection tool acting as an AP. If required, the following parameter values are modified for specific test cases.

Table 4. Test bed AP default parameters

Parameter	**Description**	**Security Vulnerability Detection tool acting as a AP**
SSID	Service Set Identifier	krack
Security	802.11 Security method	WPA2-Personal
Cipher Suite	Cipher Suite	GCMP (00-0F-AC:8)
Passphrase	Key used for encryption	12345678
Operating channel	Operating channel	2

3 Requirements for Wi-Fi Alliance certification

The following items describe the necessary features that are required for a DUT to pass Key Reinstallation Vulnerability Detection test plan.

3.1 General requirements

3.1.1 Prerequisite certification requirements

There are no prerequisite certification requirements for the APUT and STAUT to pass Key Reinstallation Vulnerability Detection test plan.

3.1.2 Testing requirements

This section lists the DUT requirements that are necessary to execute the test cases in this test plan.

- If the APUT supports 802.11r Fast BSS Transition (FT), then the APUT shall be able to be configured to enable FT feature as per Table 10
- If the APUT supports FILS-SK authentication, then the APUT shall be able to be configured to enabled FILS-SK feature as per Table 12

3.2 Applicability of tests

The applicable tests for certification are the tests of mandatory features and tests of optional features that a vendor chooses to declare or that are indicated by the DUT as described in the underlying technical specifications. Table 5, Table 6, and Table 7 list the applicable tests for the APUT and STAUT.

“Applicability” indicates whether a feature and its associated tests are either mandatory or optional to implement. Mandatory (M) tests are required for certification.

Optional (O) tests are performed if the vendor declares the feature, or the DUT indicates the feature as described in the underlying technical specifications via transmitted frames or transmitted messages or user interfaces. If the optional feature is declared and if that test fails, the DUT shall fail the Key Reinstallation Vulnerability Detection certification. Conditional (C) tests are mandatory if certain specified conditions pertain to the DUT (again, as declared by the vendor during the submission or indicated by the DUT), and are optional otherwise.

If the feature requires information, in particular if the vendor implements or supports an optional feature, the fourth column contains a “Y” and the vendor shall provide information in the DUT Information spreadsheet. (A copy of the spreadsheet is accessible through the online Wi-Fi Alliance Certification System.)

If a vendor declares an optional feature, that feature shall be indicated by the DUT as described in the underlying technical specifications. Declaration of an optional feature by a vendor comprises inclusion of the feature in the appropriate Wi-Fi Alliance registration and DUT Information spreadsheet at the time of submission. An optional feature that was not declared, but is indicated within an associated capabilities field(s), IE’s, or any transmitted frames comprises inclusion of the feature.

Each vendor shall fill out the DUT Information spreadsheet completely. Test labs will verify that the list of optional features declared by the vendor matches the list indicated by the DUT; each optional feature for which any test exists in this test plan and that appears in one list shall also appear in the other. The information determines which tests and which test parameters apply to the certification.

3.2.1 APUT tests (2.4 and/or 5 GHz)

Table 5 summarizes the Key Reinstallation Vulnerability Detection APUT tests.

Table 5. APUT test applicability

Test case description	Test plan section / Test case reference	Applicability: Mandatory (M) / Optional (O) / Conditional (C)	FlexTrack certification path	QuickTrack certification path	Security Vulnerability Detection tool supported? (Y/N)
Key reinstallation vulnerability test on 802.11r AP test	4.2.1	C	Yes	No	Yes Note: Manual execution only (No Wi-Fi Test Suite support)
Key reinstallation vulnerability test for FILS SK authentication test	4.3.1	C	Yes	No	Yes Note: Manual execution only (No Wi-Fi Test Suite support)

3.2.2 STAUT tests (2.4 GHz)

Table 6 summarizes the Key Reinstallation Vulnerability Detection STAUT tests.

NOTE: Current QuickTrack tool listed in appendix A.1 only supports 2.4 GHz.

Table 6. STAUT test applicability

Test case description	Test plan section / Test case reference	Applicability: Mandatory (M) / Optional (O) / Conditional (C)	FlexTrack certification path	QuickTrack certification path
Immediate retransmission of plaintext EAPOL M3 during initial 4-way handshake test	CT_Security_WPA2Personal_STA_4wayHandshakeVulnerability-ImmediateM3Retransmission_10003_1 [4]	M	Yes	Yes
Retransmission of encrypted EAPOL M3 during pairwise rekey handshake test	CT_Security_WPA2Personal_STA_4wayHandshakeVulnerability-EncryptedM3Retransmission_10002_1 [4]	M	Yes	Yes
PTK reinstallation in 4-way handshake using a random ANonce when STA uses Temporal PTK construction test	CT_Security_WPA2Personal_STA_4wayHandshakeVulnerability-RandomANonce_10005_1 [4]	M	Yes	Yes
PTK reinstallation in 4-way handshake using the same Anonce when STA uses Temporal PTK construction test	CT_Security_WPA2Personal_STA_4wayHandshakeVulnerability-SameANonce_10006_1 [4]	M	Yes	Yes
Group key handshake vulnerability test	CT_Security_WPA2Personal_STA_GroupKeyHandshakeVulnerability_10138_1 [4]	M	Yes	Yes

Test case description	Test plan section / Test case reference	Applicability: Mandatory (M) / Optional (O) / Conditional (C)	FlexTrack certification path	QuickTrack certification path
STAUT replay protection test	CT_Security_WPA2Personal_STA_ReplayProtection_10249_1 [4]	M	Yes	Yes

3.2.3 STAUT tests (60 GHz)

Table 7 summarizes the Key Reinstallation Vulnerability Detection STAUT tests.

Table 7. STAUT test applicability

Test case description	Test plan section / Test case reference	Applicability: Mandatory (M) / Optional (O) / Conditional (C)	FlexTrack certification path	QuickTrack certification path	Security Vulnerability Detection tool supported? (Y/N)
Immediate retransmission of encrypted EAPOL M3 during pairwise rekey handshake test	5.2.3	M	Yes	No	Yes
Group key handshake vulnerability test	5.3.1	M	Yes	No	Yes

3.3 Configuration requirements

The DUT parameters that require manual configuration are listed below.

1. SSID
2. Wireless operational mode (a/n/ac/ad)
3. Channel
4. Local IP address and subnet mask

If any of the above items cannot be configured through the user interface, then the DUT test fails.

3.3.1 APUT configuration requirements

Table 8 lists the default APUT configuration values that a technician shall set within a test procedure. Specific test cases may impose additional configuration requirements.

Table 8. APUT default configuration requirements

Parameter	Description	APUT
SSID	Service Set Identifier	krack

Parameter	Description	APUT
Security	802.11 Security method	WPA2-Personal
Cipher Suite	Cipher Suite	CCMP (00-0F-AC:4)
Passphrase	Key used for encryption	12345678
Operating channel	Operating channel	6 in 2.4 GHz 36 in 5 GHz
PMF	Protected management frame	OOB
DHCP	DHCP server	Enabled (if built-in DHCP server)

3.3.2 STAUT configuration requirements (60 GHz)

Table 9 lists the default STAUT configuration values that a technician shall set within a test procedure. Specific test cases may impose additional configuration requirements.

Table 9. STAUT default configuration requirements

Parameter	Description	STAUT
SSID	Service Set Identifier	N/A
Security	802.11 Security method	WPA2-Personal
Cipher Suite	Cipher Suite	GCMP (00-0F-AC:8)
Passphrase	Key used for encryption	12345678
DHCP	DHCP client	Enabled

3.4 Testing rules

1. If the DUT fails any tests, no further testing will be performed until the vendor addresses the problems and has updated the device.
2. The default DUT parameters shall be configured on devices at the start of each test case unless otherwise noted.
3. All tests shall be run inside an RF shielded room to prevent the Security Vulnerability Detection tool from reporting false test results.
4. Each test case in this test plan is repeated five times to validate the consistency of the reported result. Any test repetition failure results in a test case failure.
5. When executing STAUT tests, if the following message is displayed on the Security Vulnerability Detection tool's console, fix/upgrade the supplicant to resolve this issue before executing any other test case.

```
"Usage of all-zero key detected. Client is vulnerable to installation of an all-zero key in the 4-way handshake!
```

6. For test case 5.3.1, if the STAUT device has implemented the patch to fix the identified vulnerability on group key reinstallation and the Security Vulnerability Detection tool still reports the STA as vulnerable to group key reinstallations: Received 5 unique replies to replayed broadcast ARP requests. STA is vulnerable to group key reinstallations (or STA accepts replayed broadcast frames), the STAUT vendor should code inspect to ensure that the STA has implemented, and enabled replay protection feature on the STAUT.
7. For test case 5.3.1, if the STAUT implementation as part of fixing the group key reinstallation vulnerability does not respond to Group Key Handshake Message 1 from the AP, the Security Vulnerability Detection tool may still report the STAUT as vulnerable to group key handshake vulnerability.

4 APUT tests

4.1 APUT configuration requirements validation test

This section is not applicable to an APUT undergoing Key Reinstallation Vulnerability Detection testing.

4.2 802.11r Fast Transition handshake vulnerability tests

4.2.1 Key reinstallation vulnerability test on 802.11r AP test

Objective

This test determines whether a Fast BSS Transition capable APUT is vulnerable to key reinstallation.

This test is repeated with PMF enabled and PMF disabled. If the APUT supports FT using WPA2-Enterprise operation, the test is repeated using EAP-TTLS.

Applicability: Optional. This test shall be executed only if the APUT vendor declared support for the Fast BSS Transition (802.11r) feature in Table 1.

References

Section 13 [2]

Test environment

- APUT1 device that supports FT protocol (802.11r)
- APUT2 device that supports FT protocol (802.11r)
- Wireless sniffer
- STA: Security Vulnerability Detection tool emulating an FT capable STA (DHCP client is enabled)
- DHCP server
- RF shielded room
- AAA server for FT enterprise test

Test configuration

Table 10 defines the specific parameter values required for this test case.

Table 10. Key reinstallation vulnerability test on 802.11r AP test configuration

Parameter	APUT1 value	APUT2 value	Security Vulnerability Detection tool acting as a STA value
Vendor	N/A	N/A	Qualcomm - refer to Appendix A
SSID	FTtest	FTtest	N/A
Operating channel	36 for APUT supporting 5 GHz, else 1	48 for APUT supporting 5 GHz, else 6	N/A
Security	Run 1: WPA2-Personal Run 2: WPA2-Ent (EAP-TTLS/MSCHAPv2)	Run 1: WPA2-Personal Run 2: WPA2-Ent (EAP-TTLS/MSCHAPv2)	Run 1: WPA2-Personal Run 2: WPA2-Ent (EAP-TTLS/MSCHAPv2)
Passphrase	12345678	12345678	12345678
PMF	Run 1a: Enabled Run 1b: Disabled Run 2a: Enabled	Run 1a: Enabled Run 1b: Disabled Run 2a: Enabled	Run 1a: Enabled Run 1b: Disabled Run 2a: Enabled

Parameter	APUT1 value	APUT2 value	Security Vulnerability Detection tool acting as a STA value
	Run 2b: Disabled	Run 2b: Disabled	Run 2b: Disabled

Test procedure and expected results

Table 11 provides the test procedure and expected results for this test case.

Table 11. Key reinstallation vulnerability test on 802.11r AP test procedure and expected results

Step	APUT1	APUT2	STA	Expected result
1	Configure APUT1 with the parameters listed in Table 8 and Table 10.	Configure APUT2 with the parameters listed in Table 8 and Table 10.		
2	Start the Sniffer.			
3			Configure the STA to emulate an FT capable STA device and trigger the STA to associate to APUT1. Command to execute on STA tool device: sudo ./vdt_agent --4.2.1 ../wpa_supplicant/wpa_supplicant -D nl80211 -i <wireless interface name> -c <configuration file>	
4	Wait 30 seconds. Stop the Sniffer.			SN: If the association and 4-way handshake are successful with APUT1, then CONTINUE else FAIL.
5	Start the Sniffer in APUT2's operating channel to capture the FT handshake and data traffic.			
6			Trigger the STA to roam from APUT1 to APUT2 using FT authentication. sudo ./wpa_cli -i <interface name> > status > scan_results > roam <bssid of APUT2> The STA continues to replay (Re)Association Request frame to the APUT.	
7		Initiate arping from the STA to the APUT2. Note: Downlink (DL) ping traffic from a console in the		

Step	APUT1	APUT2	STA	Expected result
		APUT2's wired network to the STA device can also be initiated to perform this step.		
8	Wait 30 seconds. Stop the Sniffer.			SN: (MANUAL VERIFICATION STEP) If the association, and 4-way handshake are successful with APUT2, then CONTINUE else FAIL. If the sniffer detects reuse of CCMP PN in frames transmitted by the APUT2, then FAIL else CONTINUE. If the SVD tool reports the APUT as not vulnerable to key reinstallation vulnerability, then PASS else FAIL.

4.3 Fast Initial Link Setup Shared Key authentication tests

4.3.1 Key reinstallation vulnerability test for FILS SK authentication test

Objective

This test determines whether an AP supporting FILS SK authentication is vulnerable to key reinstallation.

Applicability: Optional. This test shall be executed only if the APUT vendor declared support for FILS SK authentication feature in Table 1.

References

IEEE Std 802.11ai-2016 [3]

Test environment

- APUT device that supports FILS SK authentication
- Wireless sniffer
- STA: Security Vulnerability Detection tool emulating a FILS SK capable STA (DHCP client is enabled)
- AAA server supporting FILS SK authentication
- DHCP server
- RF shielded room

Test configuration

Table 12 defines the specific parameter values required for this test case.

Table 12. Key reinstallation vulnerability test for FILS SK authentication test configuration

Parameter	APUT value	Security Vulnerability Detection tool acting as a STA value
Vendor	N/A	Qualcomm - refer to Appendix A
SSID	FILStest	N/A
Operating channel	6 if the APUT supports 2.4 GHz, else 36	N/A
FILS Realm	wfa.oce.test (Hash value = 93C1)	N/A
FILS AKM Suite Selector	14	14
FILS Configuration	FILS SK Authentication without PFS enabled	FILS SK Authentication without PFS enabled
Security	WPA2-Enterprise	WPA2-Enterprise
EAP method (WPA2-Enterprise)	EAP-TTLS/MSCHAPV2	EAP-TTLS/MSCHAPV2

Security credentials (WPA2-Enterprise)		username=ttls-user@wfa.oce.test
		password="password"

FILS HLP Configuration	HLP disabled	HLP disabled

Parameter	APUT value	Security Vulnerability Detection tool acting as a STA value
PMK caching	Disabled	Disabled

Test procedure and expected results

Table 13 provides the test procedure and expected results for this test case.

Table 13. Key reinstallation vulnerability test for FILS SK authentication test procedure and expected results

Step	APUT	STA	Expected result
1	Configure the APUT with the parameters listed in Table 8 and Table 12.	Configure the STA with the parameters listed in Table 3 and Table 12.	
2	Start the Sniffer and the AAA server.		
3		Configure the STA to emulate a FILS SK capable STA device and trigger the STA to associate to APUT. Command to execute on STA tool device: sudo ./vdt_agent --4.3.1 ../wpa_supplicant/wpa_supplicant -D nl80211 -i <interface name> -c ../wpa_supplicant/fils-supplicant.conf	
4	Wait for 30 seconds. Stop the sniffer.		SN: If the initial association and 4-way handshake are successful with the APUT, then CONTINUE else FAIL.
5		Initiate a ping from the STA to the ping server.	SN: If the ping is successful, and packets are sent via the APUT, then CONTINUE else FAIL.
6		Trigger the STA to disassociate from the APUT. Command to execute on STA tool device: sudo ./wpa_cli -i <interface name> > disconnect	
7	Wait for 10 seconds for the APUT to clear its state.		
8		Trigger the STA to associate to the APUT using FILS SK authentication. Command to execute on STA tool device: sudo ./wpa_cli -i <interface name> > reconnect The STA continues to replay (Re)Association Request frame to the APUT.	
9		Initiate arping from the STA to the APUT. Note:	

Step	APUT	STA	Expected result
		Downlink (DL) ping traffic from a console in the APUT's wired network to the STA device can also be initiated to perform this step.	
10	Wait for 30 seconds. Stop the sniffer.		SN: (MANUAL VERIFICATION STEP) If the FILS SK authentication and association are successful with the APUT, then CONTINUE else FAIL. If the tool detects reuse of CCMP PN in the frames transmitted by the APUT, then FAIL else CONTINUE. If the SVD tool reports the APUT as not vulnerable to key reinstallation vulnerability, then PASS else FAIL.

5 STAUT tests for 60 GHz

5.1 STAUT configuration requirements validation test

This section is not applicable to a STAUT undergoing Key Reinstallation Vulnerability Detection testing.

5.2 4-way handshake vulnerability tests

5.2.1 Removed

5.2.2 Removed

5.2.3 Immediate retransmission of encrypted EAPOL M3 during pairwise rekey handshake test

Objective

This test determines if the STAUT is vulnerable to PTK and GTK key reinstallation using immediate retransmission of an encrypted EAPOL M3 message during the pairwise rekey handshake.

Applicability: Mandatory for a 60 GHz STAUT device

References

Section 12 [2]

Test environment

- STAUT with DHCP client enabled
- Wireless sniffer
- AP: Security Vulnerability Detection tool emulating an AP
- RF shielded room

Test configuration

Table 14 define the specific parameter values required for this test case.

Table 14. Immediate retransmission of encrypted EAPOL M3 during pairwise rekey handshake test configuration (60 GHz)

Parameter	STAUT value	Security Vulnerability Detection tool acting as an AP value
Vendor	N/A	Qualcomm
SSID	N/A	encryptedM3
Operating channel	N/A	2
Security	WPA2-Personal GCMP	WPA2-Personal
Passphrase	12345678	12345678
DHCP	Enabled	n/a

Test procedure and expected results

Table 15 provides the test procedure and expected results for this test case.

Table 15. Immediate retransmission of encrypted EAPOL M3 during pairwise rekey handshake test procedure and expected results

Step	STAUT	AP	Expected result
1	For 60 GHz: Configure the STAUT with the parameters listed in Table 9 and Table 14		
2	Start the Sniffer.		
3		Configure the AP to test 4-way handshake vulnerability.	
4		The AP starts to transmit Beacon frames.	
5	Configure the STAUT to scan and associate to the AP using WPA2-Personal security.		SN: If the association exchange and 4-way handshake are successful, then CONTINUE else FAIL.
6		The AP initiates a pairwise rekey handshake with the STAUT. Note that no user intervention is required. During the pairwise rekey, the AP transmits repeated encrypted EAPOL M3 messages at regular intervals to verify pairwise key reinstallation on the STAUT. The AP also transmits Broadcast ARP Request frames at regular intervals to check for group key reinstallation.	
7	Wait for 30 seconds. Stop the Sniffer.		For 60 GHz: Manual SN: If the rekey between the STA and the AP is successful, then CONTINUE else FAIL. If the STAUT device is reusing GCMP PN in the transmitted frames, then FAIL else CONTINUE. If the STAUT is accepting replayed group addressed frames, then FAIL else PASS. Verify using tcpdump on the AP tool.

5.2.4 Removed

5.2.5 Removed

5.3 Group key handshake vulnerability tests

5.3.1 Group key handshake vulnerability test

Objective

This test determines if the STAUT is vulnerable to GTK key reinstallation.

Applicability: Mandatory for a 60 GHz STAUT device

References

Section 12 [2]

Test environment

- STAUT with DHCP client enabled
- Wireless sniffer
- AP: Security Vulnerability Detection tool emulating an AP
- DHCP server
- RF shielded room

Test configuration

Table 16 define the specific parameter values required for this test case.

Table 16. Group key handshake vulnerability test configuration (60 GHz)

Parameter	STAUT value	Security Vulnerability Detection tool acting as an AP value
Vendor	N/A	Qualcomm
SSID	N/A	testGTK
Operating channel	N/A	2
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
DHCP	Enabled	N/A

Test procedure and expected results

Table 17 provides the test procedure and expected results for this test case.

Table 17. Group key handshake vulnerability test procedure and expected results

Step	STAUT	AP	Expected result
1	For 60 GHz: Configure the STAUT with the parameters listed in Table 9 and Table 16		
2	Start the Sniffer.		
3		Configure the AP to test Group Key handshake vulnerability.	
4		The AP starts to transmit Beacon frames.	
5	Configure the STAUT to scan and associate to the AP using WPA2-Personal security.		SN: If the association, 4-way handshake and DHCP exchange are successful, then CONTINUE else FAIL.
6		The AP initiates a group rekey handshake with the STAUT. Note that no user intervention is required. After completing the initial 4-way handshake and DHCP exchange the AP starts to transmit repeated Group rekey handshake EAPOL M1 messages and Broadcast ARP Request frames at regular intervals to check for group key reinstallation.	
7	Wait for 30 seconds. Stop the Sniffer.		For 60 GHz: Manual SN: If the rekey between the STAUT and AP is successful, then CONTINUE else FAIL. If the STAUT is accepting replayed group addressed frames, then FAIL else PASS. Verify using tcpdump on the AP tool.

5.4 Group key reinstallation with WNM sleep mode tests

5.4.1 Removed

5.5 Replay protection tests

5.5.1 Removed

Appendix A (Normative) Test bed products (2.4 and/or 5 GHz)

A.1 Approved test tool equipment

Table 18 lists the approved test equipment required to execute the test cases in this test plan.

Table 18. Approved test equipment

Device	Vendor	Product	Contact
Security Vulnerability Detection tool	Qualcomm	AR5BxB-00114A (ath9k) or AR5BXB-0092DA (ath9k)	support@wi-fi.org
QuickTrack tool		See [4]	support@wi-fi.org

Table 19 lists the additional test tools required to execute the test cases in this test plan.

Table 19. Additional test tools

Device	Vendor	Product	Contact
Wireless Sniffer	Qualcomm	CA-65-Y9345-LCT	support@wi-fi.org
AAA server		HostAPD for FT and FILS-SK tests (separate packages)	support@wi-fi.org

Appendix B (Normative) Test bed products (60 GHz)

B.1 Approved test bed equipment

Table 20 lists the approved test equipment required to execute the test cases in this test plan.

Table 20. Approved test equipment

Device	Vendor	Product	Contact
Security Vulnerability Detection tool	Qualcomm	CA-65-YA181	support@wi-fi.org

Table 21 lists the additional test tools required to execute the test cases in this test plan.

Table 21. Additional test tools

Device	Vendor	Product	Contact
Wireless Sniffer	Qualcomm	CA-65-YA181	support@wi-fi.org

These devices are not currently available for purchase. Any member interested in having their 60 GHz device tested for key reinstallation vulnerabilities, please contact Wi-Fi Alliance at support@wi-fi.org.

Appendix C (Informative) 60 GHz Security Vulnerability Detection tool setup guide

Please see the WiGig KRACK Testing User Manual which can be downloaded from ftp://wlabs.wi-fi.org/testbeds/WiGig/WiGig-KRACK/document. To obtain userid and password for the FTP site, follow this link. If needed, copy and paste the URL into your browser. https://groups.wi-fi.org/apps/org/workgroup/gmdocs/download.php/91690/WLABS%20FTP%20Site%20Passwords.htm

Appendix D (Informative) Document revision history

Table 22. Document revision history

Version	Date YYYY-MM-DD	Remarks
1.0	2017-10-16	Initial release.
1.1	2017-10-19	1. Added Appendix C to provide additional information on the detection tool output 2. Updated the detection tool execution commands for all test cases 3. Added a note to section 4 4. Editorial fixes
2.0	2017-11-29	1. Added APUT FILS SK authentication test case - test case 4.3.1 2. Added PASS/FAIL criteria for all APUT and STAUT test cases 3. Renumbering of test case IDs 4. Editorial fixes
2.1	2018-05-18	1. Updated test case 4.3.1 procedure with additional instructions to control test bed STA 2. Updated Appendix A
2.2	2018-07-05	1. Added 60 GHz testing (test cases 5.2.3 and 5.3.1)
2.3	2018-12-07	1. Added test case 5.5.1 for STAUT replay protection test 2. Other fixes to test configuration tables to be in sync with the VDT/test setup configuration 3. Editorial cleanup, added basic system test configurations for automation and manual modes 4. Removed Intel 7260 and added Intel 8265 in Appendix A 5. Added test case assignments in Appendix A.2
2.4	2019-09-03	1. Updated Appendix C to refer to the WiGig KRACK Testing User Manual
2.5	2021-05-24	1. Section 5 STAUT test cases for 2.4 and 5 GHz removed 2. References added to QuickTrack STAUT test cases for 2.4 GHz 3. Updated applicability of tests in section 3.2 to reflect FlexTrack and QuickTrack certification path 4. Editorial updates to incorporate QuickTrack certification path