CONFIDENTIAL TRADE SECRET

FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE® MEMBERS

– DO NOT COPY –

Fragment and Forge Vulnerability Detection Test Plan

Version 1.0

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

© 2021 Wi-Fi Alliance. All Rights Reserved.
This document contains confidential trade secrets intended solely for use by only authorized Wi-Fi Alliance members.
For the latest up-to-date information, please refer to the Wi-Fi Alliance website's members-only area.

WI-FI ALLIANCE PROPRIETARY AND CONFIDENTIAL – SUBJECT TO CHANGE WITHOUT NOTICE

Wi-Fi Alliance owns the copyright in this document and reserves all rights therein. This document and any related materials may only be used by Wi-Fi Alliance members for their internal use, such as quality assurance and pre-certification activities, and for their participation in approved Wi-Fi Alliance activities, such as the Wi-Fi Alliance certification program, unless otherwise permitted by Wi-Fi Alliance through prior written consent. A user of this document may duplicate and distribute copies of the document in connection with the authorized uses described above, provided any duplication in whole or in part includes the copyright notice and the disclaimer text set forth herein. Unless prior written permission has been received from Wi-Fi Alliance, any other use of this document and all other duplication and distribution of this document are prohibited. Wi-Fi Alliance regards the unauthorized use, duplication or distribution of this document by a member as a material breach of the member's obligations under the organization's rules and regulations, which may result in the suspension or termination of Wi-Fi Alliance membership. Unauthorized use, duplication, or distribution by nonmembers is an infringement of the Wi-Fi Alliance's copyright. Distribution of this document to persons or organizations who are not members of Wi-Fi Alliance is strictly prohibited. TO PREVENT UNAUTHORIZED ACCESS, DO NOT STORE ON COMPUTER ANY LONGER THAN REQUIRED.

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.

© 2021 Wi-Fi Alliance. All Rights Reserved.

Table of contents

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

List of tables

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

List of figures

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

1 Overview

1.1 Scope and purpose

This document is the test plan for validating if a device is vulnerable to fragment and forge attacks.

The identified fragment and forge vulnerabilities [2] exploit the security protocol implementation, including manipulation on unauthenticated A-MSDU Present subfield in the (plaintext) QoS Control field of the 802.11 MAC header to convert a normal non-A-MSDU to an A-MSDU, manipulation on fragments in an MSDU/MMPDU and injection of plaintext frame in a protected network. Device vulnerabilities are identified by types of attacks implemented in this test plan.

The primary goal of this test plan is to identify if a DUT implementation is susceptible to the vulnerabilities by utilizing a Fragment and Forge Vulnerability Detection (FFD) tool that has been developed to detect and report the identified 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 mitigation against A-MSDU attacks?	4.2.1, 4.2.2	Yes/No
2	Does the STAUT support mitigation against A-MSDU attacks?	5.2.1, 5.2.2	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 assumed.

[1] 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 802.11-2020

[2] Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation, Mathy Vanhoef, May 2021.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

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
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
EAPOL	EAP over LAN
PMF	Protected Management Frames
PMK	Pairwise Master Key
PTK	Pairwise Transient Key
SSID	Service Set Identifier
STA	Station

1.4.2 Definitions

This test plan contains no definitions.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

2 Test tools, methodology and approach

This section defines the tools, methodology, and approach for testing and certifying devices for Fragment and Forge 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)
- Capable of dissecting 802.11 Management, Control and Data frames

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 DUT testing in automation mode using the Wi-Fi Test Suite.

Figure 2 depicts the basic system test configuration for Fragment and Forge Vulnerability Detection DUT testing in manual mode.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

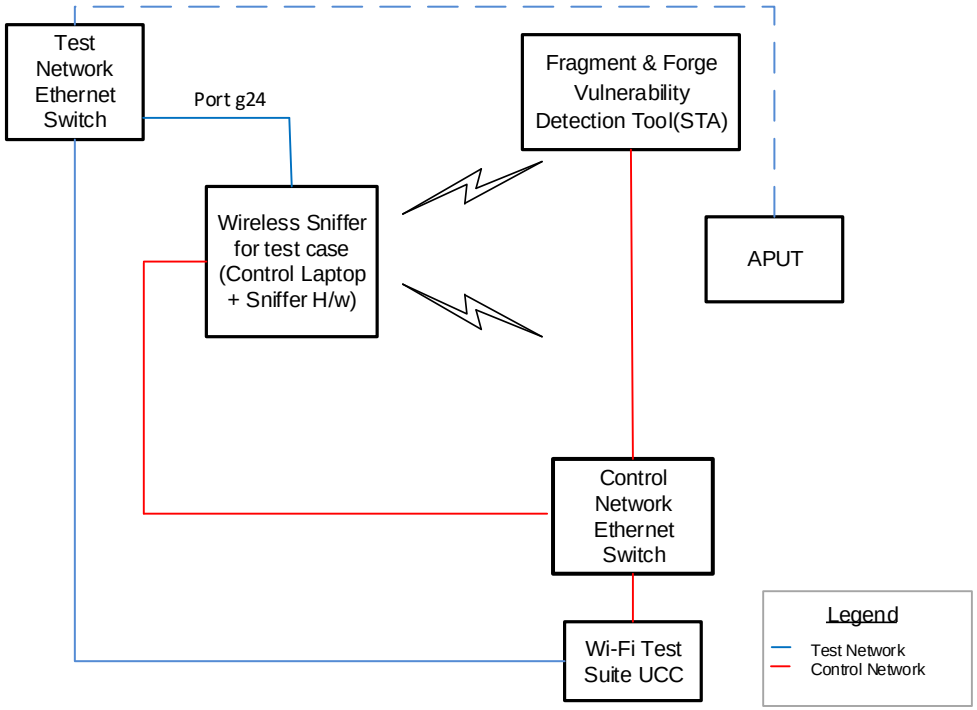

Figure 1. Fragment and Forge Vulnerability Detection test configuration for APUT

Note: The Test Network Ethernet switch needs to have mirrored port enabled. If the primary device type is declared as Mobile AP, then the connection between the sniffer and AP ethernet port(line labeled with Port g24) is not needed

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

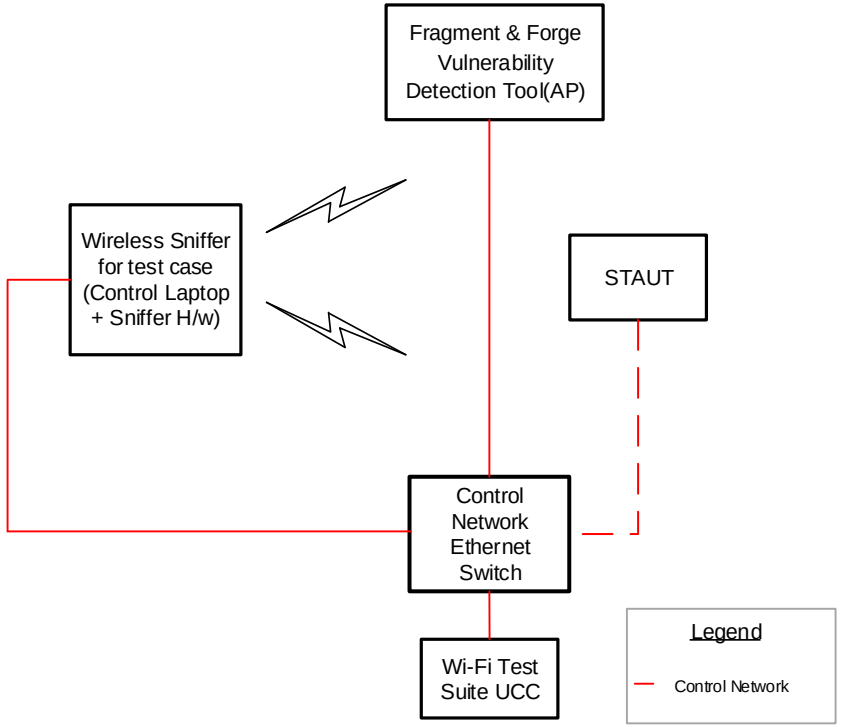

Figure 2. Fragment and Forge Vulnerability Detection test configuration for STAUT

2.4 Test bed capability requirements

2.4.1 Test bed STA requirements

Table 3 defines the general test configuration for test cases of the Fragment and Forge Vulnerability Detection tool acting as a test bed STA. If required, the following parameter values are modified for specific test cases. Current test bed tool as listed in Table 89 can only support 2.4 GHz.

Table 3. Test bed STA default parameters

Parameter	Description	Fragment and Forge Vulnerability Detection tool acting as a STA
SSID	Service Set Identifier	N/A
Security	802.11 Security method	WPA2-Personal

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Parameter	Description	Fragment and Forge Vulnerability Detection tool acting as a STA
Cipher Suite	Cipher Suite	CCMP (00-0F-AC:4)
Passphrase	Key used for encryption	12345678
PMF	Protected management frame	Enabled

2.4.2 Test bed AP requirements

Table 4 defines the general test configuration for test cases of the Fragment and Forge Vulnerability Detection tool acting as a test bed AP. If required, the following parameter values are modified for specific test cases. Current test bed tool as listed in Table 89 can only support 2.4 GHz.

Table 4. Test bed AP default parameters

Parameter	Description	Fragment and Forge Vulnerability Detection tool acting as an AP
SSID	Service Set Identifier	testffd
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	1 in 2.4 GHz
PMF	Protected management frame	Enabled

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

3 Requirements for Wi-Fi Alliance certification

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

3.1 General requirements

3.1.1 Prerequisite certification requirements

There are no prerequisite certification requirements for an APUT or STAUT to pass Fragment and Forge 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.

3.1.2.1 Disable power save mode

A DUT's power save mode shall be disabled. If it is impossible to disable power save mode, then it is recommended to increase the test repetition to ten times to avoid false positive result.

3.1.2.2 Verification for test tool

- APUT testing
  - To validate the test tool STA environment is setup correctly, a DUT needs to achieve pass results for test cases as described in A.2.1 before proceeding to the test cases in section 4.
- STAUT testing
  - To validate the test tool environment is setup correctly, a DUT needs to achieve pass results for cases as described in A.2.2 before proceeding to the test cases in section 5.

3.1.2.3 IP address assignment

The IP address of the STAUT can be obtained by automatic assignment and shall be in the range 192.165.100.0/24 except 192.165.100.254. This is because the test tool AP's IP is fixed at 192.165.100.254.

The IP address of the APUT does not have the limitation as the STAUT. Thus, a user can choose based on the network setup.

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 and Table 6 list the applicable tests for the APUT and STAUT.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

"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 Fragment and Forge 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 shall 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

Table 5 summarizes the Fragment and Forge Vulnerability Detection APUT tests.

Table 5. APUT test applicability

Test case description	Test plan section	Applicability: Mandatory (M) /Optional (O) / Conditional (C)	Associated CVE [2]
Frame aggregation attack test	4.2.1	O	CVE-2020-24588
Frame aggregation attack with a malformed packet test	4.2.2	O	CVE-2020-24588
Mixed key fragment attack with non-consecutive PN test	4.3.1	M	CVE-2020-24587

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Test case description	Test plan section	Applicability: Mandatory (M) /Optional (O) / Conditional (C)	Associated CVE [2]
Mixed key fragment attack with consecutive PN test	4.3.2	M	CVE-2020-24587
Cached fragment attack with reassociation test	4.4.1	M	CVE-2020-24586
Cached fragment attack with reassociation with a time delay test	4.4.2	M	CVE-2020-24586
Cached fragment attack with de-authentication test	4.4.3	M	CVE-2020-24586
Cached fragment attack with de-authentication and reconnection with a time delay test	4.4.4	M	CVE-2020-24586
Non-consecutive Packet Number attack test	4.5.1	M	CVE-2020-26146
Encrypted fragment followed by plaintext fragment attack test	4.6.1	M	CVE-2020-26147
Multiple mixed fragment attack test	4.6.2	M	CVE-2020-26147
Plaintext fragment followed by encrypted fragment attack test	4.6.3	M	CVE-2020-26147

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Test case description	Test plan section	Applicability: Mandatory (M) /Optional (O) / Conditional (C)	Associated CVE [2]
Plaintext frame attack test	4.6.4	M	CVE-2020-26140
Plaintext fragment attack test	4.6.5	M	CVE-2020-26143
Broadcast plaintext fragment attack after connection test	4.7.1	M	CVE-2020-26145
Broadcast plaintext fragment attack during 4-way handshake test	4.7.2	M	CVE-2020-26145
Faking A-MSDUs as EAPOL after a secure connection test	4.8.1	M	CVE-2020-26144
Faking malformed A-MSDU as EAPOL after a secure connection test	4.8.2	M	CVE-2020-26144
Faking A-MSDUs as EAPOL during 4-way handshake test	4.8.3	M	CVE-2020-26144
Faking Malformed A-MSDU as EAPOL during 4-way handshake test	4.8.4	M	CVE-2020-26144

3.2.2 STAUT tests

Table 6 summarizes the Fragment and Forge Vulnerability Detection STAUT tests.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Table 6. STAUT test applicability

Test case description	Test plan section	Applicability: Mandatory (M) / Optional (O) / Conditional (C)	Associated CVE [2]
Frame aggregation attack test	5.2.1	O	CVE-2020-24588
Frame aggregation attack with a malformed packet test	5.2.2	O	CVE-2020-24588
Mixed key fragment attack with non-consecutive PN test	5.3.1	M	CVE-2020-24587
Mixed key fragment attack with consecutive PN test	5.3.2	M	CVE-2020-24587
Cached fragment attack with reassociation test	5.4.1	M	CVE-2020-24586
Cached fragment attack with reassociation with a time delay test	5.4.2	M	CVE-2020-24586
Cached fragment attack with de-authentication test	5.4.3	M	CVE-2020-24586
Cached fragment attack with de-authentication and reconnection with a time delay test	5.4.4	M	CVE-2020-24586

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Test case description	Test plan section	Applicability: Mandatory (M) / Optional (O) / Conditional (C)	Associated CVE [2]
Non-consecutive Packet Number attack test	5.5.1	M	CVE-2020-26146
Encrypted fragment followed by plaintext fragment attack test	5.6.1	M	CVE-2020-26147
Multiple mixed fragment attack test	5.6.2	M	CVE-2020-26147
Plaintext fragment followed by encrypted fragment attack test	5.6.3	M	CVE-2020-26147
Plaintext frame attack test	5.6.4	M	CVE-2020-26140
Plaintext fragment attack test	5.6.5	M	CVE-2020-26143
Broadcast plaintext fragment attack after connection test	5.7.1	M	CVE-2020-26145
Broadcast plaintext fragment attack during 4-way handshake test	5.7.2	M	CVE-2020-26145

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Test case description	Test plan section	Applicability: Mandatory (M) / Optional (O) / Conditional (C)	Associated CVE [2]
Faking A-MSDUs as EAPOL after a secure connection test	5.8.1	M	CVE-2020-26144
Faking malformed A-MSDU as EAPOL after a secure connection test	5.8.2	M	CVE-2020-26144
Faking A-MSDUs as EAPOL during 4-way handshake test	5.8.3	M	CVE-2020-26144
Faking Malformed A-MSDU as EAPOL during 4-way handshake test	5.8.4	M	CVE-2020-26144

3.3 Configuration requirements

The DUT parameters that require manual configuration are listed below.

1. SSID
2. Wireless operational mode (a/n/ac/ax)
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 7 lists the default APUT configuration values that a technician shall set within a test procedure. Specific test cases may impose additional configuration requirements.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Table 7. APUT default configuration requirements

Parameter	Description	APUT
SSID	Service Set Identifier	testffd
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	1 in 2.4 GHz
PMF	Protected management frame	OOB

3.3.2 STAUT configuration requirements

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

Table 8. STAUT default configuration requirements

Parameter	Description	STAUT
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
PMF	Protected management frame	OOB

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 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. Test failure in any one of the iterations results in an immediate test case failure and remaining iterations will be skipped.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

4 APUT tests

4.1 APUT configuration requirements validation test

This section is not applicable to an APUT undergoing Fragment and Forge Vulnerability Detection testing.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

4.2 Frame aggregation attack tests

4.2.1 Frame aggregation attack test

Objective

This test is to verify that an APUT rejects an A-MSDU frame with a valid LLC/SNAP header.

Applicability: Optional. This test is only executed if the APUT declares support for A-MSDU attack mitigation indicated in Table 1.

References

Section 3.2, [2]

Test configuration

Table 9 defines the specific parameter values required for this test case.

Table 9. Frame aggregation attack test configuration

Parameter	APUT value	Fragment and Forge Vulnerability Detection tool acting as a STA value
Vendor	N/A	Refer to Appendix A
SSID	testffd	N/A
Operating channel	1	N/A
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 10 provides the test procedure and expected results for this test case.

Table 10. Frame aggregation attack test procedure and expected results

Step	APUT1	STA	Expected result
1	Configure APUT with the parameters listed in Table 7 and Table 9.		
2		Configure the STA as in Table 3 and Table 9. Trigger the STA to associate to APUT.	

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Step	APUT1	STA	Expected result
3		Trigger the STA to inject ICMP Echo Requests using A-MSDU with a valid LLC/SNAP header to the APUT. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: amsdu-inject	If the Fragment and Forge Vulnerability Detection tool detects that APUT responds to the ICMP Echo Requests via ICMP Echo Response, then FAIL, else PASS.

4.2.2 Frame aggregation attack with a malformed packet test

Objective

This test is to verify that an APUT rejects an A-MSDU frame with a valid LLC/SNAP head in a malformed Data frame.

Applicability: Optional. This test is only executed if the APUT declares support for A-MSDU attack mitigation indicated in Table 1.

References

Section 3.2, [2]

Test configuration

Table 11 defines the specific parameter values required for this test case.

Table 11. Frame aggregation attack with a malformed packet test configuration

Parameter	APUT value	Fragment and Forge Vulnerability Detection tool acting as a STA value
Vendor	N/A	Refer to Appendix A
SSID	testffd	N/A
Operating channel	1	N/A
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 12 provides the test procedure and expected results for this test case.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Table 12. Frame aggregation attack with a malformed packet test procedure and expected results

Step	APUT1	STA	Expected result
1	Configure APUT with the parameters listed in Table 7 and Table 11.		
2		Configure the STA as in Table 3 and Table 11. Trigger the STA to associate to APUT.	
3		Trigger the STA to inject ICMP Echo Requests using A-MSDU format with a valid LLC/SNAP header in a malformed frame to the APUT. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: amsdu-inject-bad	If the Fragment and Forge Vulnerability Detection tool detects that the APUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

4.3 Mixed key fragment attack tests

4.3.1 Mixed key fragment attack with non-consecutive PN test

Objective

This test is to verify that an APUT denies fragments encrypted under different keys and with non-consecutive Packet Numbers (PN).

Applicability: Mandatory.

References

Section 4, [2]

Test environment

- APUT
- STA: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 13 defines the specific parameter values required for this test case.

Table 13. Mixed key fragment attack with non-consecutive PN test configuration

Parameter	APUT value	Fragment and Forge Vulnerability Detection tool acting as a STA value
Vendor	N/A	Refer to Appendix A

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Parameter	APUT value	Fragment and Forge Vulnerability Detection tool acting as a STA value
SSID	testffd	N/A
Operating channel	1	N/A
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 14 provides the test procedure and expected results for this test case.

Table 14. Mixed key fragment attack with non-consecutive PN test procedure and expected results

Step	APUT	STA	Expected result
1	Configure APUT with the parameters listed in Table 7 and Table 13.		
2		Configure the STA as in Table 3 and Table 13. Trigger the STA to associate to APUT.	
3		Trigger the STA to inject ICMP Echo Requests in two fragments encrypted with different keys and with non-consecutive PNs to the APUT. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: ping I,F,BE,AE --rekey-request	If the Fragment and Forge Vulnerability Detection tool detects that the APUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

4.3.2 Mixed key fragment attack with consecutive PN test

Objective

This test is to verify that an APUT denies fragments encrypted under different keys and with consecutive Packet Numbers (PN).

Applicability: Mandatory.

References

Section 4, [2]

Test environment

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

- APUT
- STA: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 15 defines the specific parameter values required for this test case.

Table 15. Mixed key fragment attack with consecutive PN test configuration

Parameter	APUT value	Fragment and Forge Vulnerability Detection tool acting as a STA value
Vendor	N/A	Refer to Appendix A
SSID	testffd	N/A
Operating channel	1	N/A
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 16 provides the test procedure and expected results for this test case.

Table 16. Mixed key fragment attack with consecutive PN test procedure and expected results

Step	APUT1	STA	Expected result
1	Configure APUT with the parameters listed in Table 7 and Table 15.		
2		Configure the STA as in Table 3 and Table 15. Trigger the STA to associate to the APUT.	
3		Trigger the STA to inject ICMP Echo Requests in two fragments encrypted with different keys and with consecutive PNs to the APUT. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: ping I,F,BE,AE --pn-per-qos --rekey-request	If the Fragment and Forge Vulnerability Detection tool detects that the APUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

4.4 Poisoning the fragment cache

4.4.1 Cached fragment attack test with reassociation

Objective

This test is to verify that an APUT denies combination of cached fragment and a new fragment after reassociation.

Applicability: Mandatory.

References

Section 5, [2]

Test environment

- APUT
- STA: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 17 defines the specific parameter values required for this test case.

Table 17. Cached fragment attack test with reassociation configuration

Parameter	APUT value	Fragment and Forge Vulnerability Detection tool acting as a STA value
Vendor	N/A	Refer to Appendix A
SSID	testffd	N/A
Operating channel	1	N/A
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 18 provides the test procedure and expected results for this test case.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Table 18. Cached fragment attack test with reassociation procedure and expected results

Step	APUT	STA	Expected result
1	Configure the APUT with the parameters listed in Table 7 and Table 17.		
2		Configure the STA as in Table 3 and Table 17. Trigger the STA to associate to APUT.	
3		Trigger the STA to inject ICMP Echo Requests with following steps: 1. Injecting a fragment 2. Try triggering a reassociation 3. Inject second fragment to the APUT Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: ping I,E,R,AE	If the Fragment and Forge Vulnerability Detection tool detects that the APUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

4.4.2 Cached fragment attack with reassociation with a time delay test

Objective

This test is to verify that the APUT denies combination of cached fragment and a new time-delayed fragment after reassociation with a time delay.

Applicability: Mandatory.

References

Section 5, [2]

Test environment

- APUT
- STA: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 19 defines the specific parameter values required for this test case.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Table 19. Cached fragment attack with reassociation with a time delay test configuration

Parameter	APUT value	Fragment and Forge Vulnerability Detection tool acting as a STA value
Vendor	N/A	Refer to Appendix A
SSID	testffd	N/A
Operating channel	1	N/A
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 20 provides the test procedure and expected results for this test case.

Table 20. Cached fragment attack with reassociation with a time delay test procedure and expected results

Step	APUT	STA	Expected result
1	Configure APUT with the parameters listed in Table 7 and Table 19.		
2		Configure the STA as in Table 3 and Table 19. Trigger the STA to associate to APUT.	
3		Trigger the STA to inject ICMP Echo Requests with following steps: 1. Injecting a fragment 2. Try triggering a reassociation 3. Wait for a time delay of 1 second 4. Inject second fragment to the APUT Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: ping I,E,R,E	If the Fragment and Forge Vulnerability Detection tool detects that the APUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

4.4.3 Cached fragment attack with de-authentication test

Objective

This test is to verify that an APUT denies combination of cached fragment and an injected fragment after de-authentication and reconnection.

Applicability: Mandatory.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

References

Section 5, [2]

Test environment

- APUT
- STA: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 21 defines the specific parameter values required for this test case.

Table 21. Cached fragment attack with de-authentication test configuration

Parameter	APUT value	Fragment and Forge Vulnerability Detection tool acting as a STA value
Vendor	N/A	Refer to Appendix A
SSID	testffd	N/A
Operating channel	1	N/A
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 22 provides the test procedure and expected results for this test case.

Table 22. Cached fragment attack with de-authentication test procedure and expected results

Step	APUT	STA	Expected result
1	Configure APUT with the parameters listed in Table 7 and Table 21.		
2		Configure the STA as in Table 3 and Table 21. Trigger the STA to associate to APUT.	
3		Trigger the STA to inject ICMP Echo Requests with following steps: 1. Injecting a fragment 2. Try triggering de-authentication and then reconnect 3. Inject second fragment to the APUT	If the Fragment and Forge Vulnerability Detection tool detects that the APUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Step	APUT	STA	Expected result
		Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: ping I,E,R,AE --full-reconnect	

4.4.4 Cached fragment attack with de-authentication and reconnection with a time delay test

Objective

This test is to verify that an APUT denies combination of cached fragment and a new time-delayed fragment after de-authentication and reconnection.

Applicability: Mandatory.

References

Section 5, [2]

Test environment

- APUT
- STA: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 23 defines the specific parameter values required for this test case.

Table 23. Cached fragment attack with de-authentication and reconnection with a time delay test configuration

Parameter	APUT value	Fragment and Forge Vulnerability Detection tool acting as a STA value
Vendor	N/A	Refer to Appendix A
SSID	testffd	N/A
Operating channel	1	N/A
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 24 provides the test procedure and expected results for this test case.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Table 24. Cached fragment attack with de-authentication and reconnection with a time delay test procedure and expected results

Step	APUT	STA	Expected result
1	Configure APUT with the parameters listed in Table 7 and Table 23.		
2		Configure the STA as in Table 3 and Table 23. Trigger the STA to associate to APUT.	
3		Trigger the STA to inject ICMP Echo Requests with following steps: 1. Injecting a fragment 2. Try triggering de-authentication and then reconnect 3. Wait for a time delay of 1 second 4. Inject second fragment to the APUT Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: ping I,E,R,E --full-reconnect	If the Fragment and Forge Vulnerability Detection tool detects that the APUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

4.5 Non-consecutive Packet Number Attack

4.5.1 Non-consecutive Packet Number attack test

Objective

This test is to verify that an APUT denies encrypted fragments with non-consecutive Packet Numbers (PN).

Applicability: Mandatory.

References

Section 6.2, [2]

Test environment

- APUT
- STA: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 25 defines the specific parameter values required for this test case.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Table 25. Non-consecutive Packet Number attack test configuration

Parameter	APUT value	Fragment and Forge Vulnerability Detection tool acting as a STA value
Vendor	N/A	Refer to Appendix A
SSID	testffd	N/A
Operating channel	1	N/A
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 26 provides the test procedure and expected results for this test case.

Table 26. Non-consecutive Packet Number attack test procedure and expected results

Step	APUT1	STA	Expected result
1	Configure APUT with the parameters listed in Table 7 and Table 25.		
2		Configure the STA as in Table 8 and Table 25. Trigger the STA to associate to APUT.	
3		Trigger the STA to inject ICMP Echo Requests in two fragments encrypted with non-consecutive PNs to the APUT. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: ping I,E,E --inc-pn 2	If the Fragment and Forge Vulnerability Detection tool detects that the APUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

4.6 Accepting plaintext fragments or plaintext frames in a protected network

4.6.1 Encrypted fragment followed by plaintext fragment attack test

Objective

This test is to verify that an APUT denies a fragmented MSDU/MMPDU that includes an encrypted fragment followed by a plaintext fragment after a secure connection.

Applicability: Mandatory.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

References

Section 6.3, [2]

Test environment

- APUT
- STA: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 27 defines the specific parameter values required for this test case.

Table 27. Encrypted fragment followed by plaintext fragment attack test configuration

Parameter	APUT value	Fragment and Forge Vulnerability Detection tool acting as a STA value
Vendor	N/A	Refer to Appendix A
SSID	testffd	N/A
Operating channel	1	N/A
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 28 provides the test procedure and expected results for this test case.

Table 28. Encrypted fragment followed by plaintext fragment attack test procedure and expected results

Step	APUT	STA	Expected result
1	Configure APUT with the parameters listed in Table 7 and Table 27.		
2		Configure the STA as in Table 8 and Table 27. Trigger the STA to associate to APUT.	
3		Trigger the STA to inject ICMP Echo Requests in two fragments: encrypted fragment followed by plaintext fragments to the APUT. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: ping I,E,P	If the Fragment and Forge Vulnerability Detection tool detects that APUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

4.6.2 Multiple mixed fragment attack test

Objective

This test is to verify that an APUT denies a fragmented MSDU/MMPDU that includes encrypted and plaintext fragments after a secure connection.

Applicability: Mandatory.

References

Section 6.3, [2]

Test environment

- APUT
- STA: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 29 defines the specific parameter values required for this test case.

Table 29. Multiple mixed fragment attack test configuration

Parameter	APUT value	Fragment and Forge Vulnerability Detection tool acting as a STA value
Vendor	N/A	Refer to Appendix A
SSID	testffd	N/A
Operating channel	1	N/A
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 30 provides the test procedure and expected results for this test case.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Table 30. Multiple mixed fragment attack test procedure and expected results

Step	APUT	STA	Expected result
1	Configure APUT with the parameters listed in Table 7 and Table 29.		
2		Configure the STA as in Table 8 and Table 29. Trigger the STA to associate to APUT.	
3		Trigger the STA to inject ICMP Echo Requests in following fragments to APUT: 1. An encrypted fragment 2. An encrypted 2nd fragment 3. A plaintext fragment Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: linux-plain	If the Fragment and Forge Vulnerability Detection tool detects that APUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

4.6.3 Plaintext fragment followed by encrypted fragment attack test

Objective

This test is to verify that an APUT denies a fragmented MSDU/MMPDU that includes a plaintext fragment followed by an encrypted fragment after a secure connection.

Applicability: Mandatory.

References

Section 6.3, [2]

Test environment

- APUT
- STA: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 31 defines the specific parameter values required for this test case.

Table 31. Plaintext fragment followed by encrypted fragment attack test configuration

Parameter	APUT value	Fragment and Forge Vulnerability Detection tool acting as a STA value
Vendor	N/A	Refer to Appendix A
SSID	testffd	N/A

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Parameter	APUT value	Fragment and Forge Vulnerability Detection tool acting as a STA value
Operating channel	1	N/A
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 32 provides the test procedure and expected results for this test case.

Table 32. Plaintext fragment followed by encrypted fragment attack test procedure and expected results

Step	APUT	STA	Expected result
1	Configure APUT with the parameters listed in Table 7 and Table 31.		
2		Configure the STA as in Table 8 and Table 31. Trigger the STA to associate to APUT.	
3		Trigger the STA to inject ICMP Echo Requests in two fragments: plaintext fragment followed by encrypted fragments to the APUT. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: ping I,P,E	If the Fragment and Forge Vulnerability Detection tool detects that APUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

4.6.4 Plaintext data frame attack test

Objective

This test is to verify that an APUT denies a plaintext data frame after a secure connection.

Applicability: Mandatory.

References

Section 6.3, [2]

Test environment

- APUT
- STA: Fragment and Forge Vulnerability Detection tool

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

- RF shielded room

Test configuration

Table 33 defines the specific parameter values required for this test case.

Table 33. Multiple plaintext fragment attack test configuration

Parameter	APUT value	Fragment and Forge Vulnerability Detection tool acting as a STA value
Vendor	N/A	Refer to Appendix A
SSID	testffd	N/A
Operating channel	1	N/A
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 34 provides the test procedure and expected results for this test case.

Table 34. Multiple plaintext fragment attack test procedure and expected results

Step	APUT	STA	Expected result
1	Configure APUT with the parameters listed in Table 7 and Table 33.		
2		Configure the STA as in Table 8 and Table 33. Trigger the STA to associate to APUT.	
3		After connection, trigger the STA to inject ICMP Echo Requests in plaintext frame to the APUT. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: ping I,P	If the Fragment and Forge Vulnerability Detection tool detects that APUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

4.6.5 Multiple plaintext fragment attack test

Objective

This test is to verify that an APUT denies a fragmented MSDU/MMPDU that includes multiple plaintext fragments after a secure connection.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Applicability: Mandatory.

References

Section 6.3, [2]

Test environment

- APUT
- STA: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 35 defines the specific parameter values required for this test case.

Table 35. Multiple plaintext fragment attack test configuration

Parameter	APUT value	Fragment and Forge Vulnerability Detection tool acting as a STA value
Vendor	N/A	Refer to Appendix A
SSID	testffd	N/A
Operating channel	1	N/A
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 36 provides the test procedure and expected results for this test case.

Table 36. Multiple plaintext fragment attack test procedure and expected results

Step	APUT	STA	Expected result
1	Configure APUT with the parameters listed in Table 7 and Table 35.		
2		Configure the STA as in Table 8 and Table 35. Trigger the STA to associate to APUT.	
3		After connection, trigger the STA to inject ICMP Echo Requests in two plaintext fragments to the APUT.	If the Fragment and Forge Vulnerability Detection tool detects that APUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Step	APUT	STA	Expected result
		Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: ping I,P,P	

4.7 Broadcast plaintext fragment attack

4.7.1 Broadcast plaintext fragment attack after connection test

Objective

This test is to verify that an APUT denies fragment with a broadcast receiver address in a unicast frame after being connected.

Applicability: Mandatory.

References

Section 6.4, [2]

Test environment

- APUT
- STA: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 37 defines the specific parameter values required for this test case.

Table 37. Broadcast plaintext fragment attack after connection test configuration

Parameter	APUT value	Fragment and Forge Vulnerability Detection tool acting as a STA value
Vendor	N/A	Refer to Appendix A
SSID	testffd	N/A
Operating channel	1	N/A
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Table 38 provides the test procedure and expected results for this test case.

Table 38. Broadcast plaintext fragment attack after connection test procedure and expected results

Step	APUT	STA	Expected result
1	Configure APUT with the parameters listed in Table 7 and Table 37.		
2		Configure the STA as in Table 3 and Table 37. Trigger the STA to associate to APUT.	
3		Trigger the STA to inject plaintext ICMP Echo Requests with a broadcast Receiver Address in 2nd fragment to APUT after connection succeeds. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: ping I,D,P --bcast-ra	If the Fragment and Forge Vulnerability Detection tool detects that APUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

4.7.2 Broadcast plaintext fragment attack during 4-way handshake test

Objective

This test is to verify that an APUT denies fragment with a broadcast receiver address in a unicast frame during 4-way handshake.

Applicability: Mandatory.

References

Section 6.4, [2]

Test environment

- APUT
- STA: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 39 defines the specific parameter values required for this test case.

Table 39. Broadcast plaintext fragment attack during 4-way handshake test configuration

Parameter	APUT value	Fragment and Forge Vulnerability Detection tool acting as a STA value
Vendor	N/A	Refer to Appendix A
SSID	testffd	N/A
Operating channel	1	N/A

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Parameter	APUT value	Fragment and Forge Vulnerability Detection tool acting as a STA value
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 40 provides the test procedure and expected results for this test case.

Table 40. Broadcast plaintext fragment attack during 4-way handshake test procedure and expected results

Step	APUT	STA	Expected result
1	Configure APUT with the parameters listed in Table 7 and Table 39.		
2		Configure the STA as in Table 3 and Table 39. Trigger the STA to associate to APUT.	
3		Trigger the STA to inject plaintext ICMP Echo Requests with a broadcast Receiver Address in 2nd fragment to APUT during 4-way handshake. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: ping D,BP --bcast-ra	SN: If APUT responds to each ICMP Echo Request with an ICMP Echo Response, then FAIL, else PASS. If the primary device type is declared as Mobile AP, then skip the following step: If the APUT forwards the ICMP Echo Requests to its Eth port, then FAIL, else PASS.

4.8 Faking A-MSDU as EAPOL handshake frames

4.8.1 Faking A-MSDUs as EAPOL after a secure connection test

Objective

This test is to verify that after a secure connection is successful, an APUT denies A-MSDUs, with each containing an EAPOL subframe followed by a plaintext ICMP Echo request subframe.

Applicability: Mandatory.

References

Section 6.5, [2]

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Test environment

- APUT
- STA: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 41 defines the specific parameter values required for this test case.

Table 41. Faking A-MSDUs as EAPOL after a secure connection test configuration

Parameter	APUT value	Fragment and Forge Vulnerability Detection tool acting as a STA value
Vendor	N/A	Refer to Appendix A
SSID	testffd	N/A
Operating channel	1	N/A
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 42 provides the test procedure and expected results for this test case.

Table 42. Faking A-MSDUs as EAPOL after a secure connection test procedure and expected results

Step	APUT	STA	Expected result
1	Configure APUT with the parameters listed in Table 7 and Table 41.		
2		Configure the STA as in Table 3 and Table 41. Trigger the STA to associate to APUT.	
3		After a secure connection is successful, trigger the STA to inject A-MSDUs, with each containing one EAPOL subframe followed by a plaintext ICMP Echo Request subframe to APUT. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: eapol-amsdu I,P	If the Fragment and Forge Vulnerability Detection tool detects that APUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

4.8.2 Faking malformed A-MSDU as EAPOL after a secure connection test

Objective

This test is to verify that after a secure connection is successful, an APUT denies A-MSDUs, with each containing a malformed EAPOL subframe followed by a plaintext ICMP Echo request subframe.

Applicability: Mandatory.

References

Section 6.5, [2]

Test environment

- APUT
- STA: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 43 defines the specific parameter values required for this test case.

Table 43. Faking malformed A-MSDU as EAPOL after a secure connection test configuration

Parameter	APUT value	Fragment and Forge Vulnerability Detection tool acting as a STA value
Vendor	N/A	Refer to Appendix A
SSID	testffd	N/A
Operating channel	1	N/A
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 44 provides the test procedure and expected results for this test case.

Table 44. Faking malformed A-MSDU as EAPOL after a secure connection test procedure and expected results

Step	APUT	STA	Expected result
1	Configure APUT with the parameters listed in Table 7 and Table 43.		

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Step	APUT	STA	Expected result
2		Configure the STA as in Table 3 and Table 43. Trigger the STA to associate to APUT.	
3		After a secure connection is successful, trigger the STA to inject A-MSDUs, with each containing one malformed EAPOL subframe followed by a plaintext ICMP Echo Request subframe to APUT. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: eapol-amsdu-bad I,P	If the Fragment and Forge Vulnerability Detection tool detects that APUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

4.8.3 Faking A-MSDUs as EAPOL during 4-way handshake test

Objective

This test is to verify that during 4-way handshake, an APUT denies A-MSDUs, with each containing an EAPOL subframe followed by a plaintext ICMP Echo request subframe.

Applicability: Mandatory.

References

Section 6.5, [2]

Test environment

- APUT
- STA: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 45 defines the specific parameter values required for this test case.

Table 45. Faking A-MSDUs as EAPOL during 4-way handshake test configuration

Parameter	APUT value	Fragment and Forge Vulnerability Detection tool acting as a STA value
Vendor	N/A	Refer to Appendix A
SSID	testffd	N/A
Operating channel	1	N/A
Security	WPA2-Personal	WPA2-Personal

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Parameter	APUT value	Fragment and Forge Vulnerability Detection tool acting as a STA value
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 46 provides the test procedure and expected results for this test case.

Table 46. Faking A-MSDUs as EAPOL during 4-way handshake test procedure and expected results

Step	APUT	STA	Expected result
1	Configure APUT with the parameters listed in Table 7 and Table 45.		
2		Configure the STA as in Table 3 and Table 45. Trigger the STA to associate to APUT.	
3		During the 4-way handshake, trigger the STA to inject A-MSDUs, with each containing one EAPOL subframe followed by a plaintext ICMP Echo Request subframe to APUT. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: eapol-amsdu BP	SN: If APUT responds to each ICMP Echo Request with an ICMP Echo Response, then FAIL, else PASS. If the primary device type is declared as Mobile AP, then skip the following step: If the APUT forwards the ICMP Echo Requests to its Eth port, then FAIL, else PASS.

4.8.4 Faking malformed A-MSDU as EAPOL during 4-way handshake test

Objective

This test is to verify that during 4-way handshake, an APUT denies A-MSDUs, with each containing a malformed EAPOL subframe followed by a plaintext ICMP Echo request subframe.

Applicability: Mandatory.

References

Section 6.5, [2]

Test environment

- APUT
- STA: Fragment and Forge Vulnerability Detection tool

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

- RF shielded room

Test configuration

Table 47 defines the specific parameter values required for this test case.

Table 47. Faking malformed A-MSDU as EAPOL during 4-way handshake test configuration

Parameter	APUT value	Fragment and Forge Vulnerability Detection tool acting as a STA value
Vendor	N/A	Refer to Appendix A
SSID	testffd	N/A
Operating channel	1	N/A
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 48 provides the test procedure and expected results for this test case.

Table 48. Faking malformed A-MSDU as EAPOL during 4-way handshake test procedure and expected results

Step	APUT	STA	Expected result
1	Configure APUT with the parameters listed in Table 7 and Table 47.		
2		Configure the STA as in Table 3 and Table 47. Trigger the STA to associate to APUT.	
3		During the 4-way handshake, trigger the STA to inject A-MSDUs, with each containing malformed EAPOL subframe followed by a plaintext ICMP Echo Request subframe to APUT. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: eapol-amsdu-bad BP	SN: If APUT responds to each ICMP Echo Request with an ICMP Echo Response, then FAIL, else PASS. If the primary device type is declared as Mobile AP, then skip the following step: If the APUT forwards the ICMP Echo Requests to its Eth port, then FAIL, else PASS.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

5 STAUT tests

5.1 STAUT configuration requirements validation test

This section is not applicable to a STAUT undergoing Fragment and Forge Vulnerability Detection testing.

5.2 Frame aggregation attack

5.2.1 Frame aggregation attack test

Objective

This test is to verify that a STAUT rejects an A-MSDU frame whose start is also a valid LLC/SNAP header.

Applicability: Optional. This test is only executed if the STAUT declares support for A-MSDU attack mitigation indicated in Table 1.

References

Section 3.2, [2]

Test environment

- STAUT
- AP: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 49 defines the specific parameter values required for this test case.

Table 49. Frame aggregation attack test configuration

Parameter	STAUT value	Fragment and Forge Vulnerability Detection tool acting as an AP value
Vendor	N/A	Refer to Appendix A
SSID	N/A	testffd
Operating channel	N/A	1
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Table 50 provides the test procedure and expected results for this test case.

Table 50. Frame aggregation attack test procedure and expected results

Step	STAUT	AP	Expected result
1		Configure AP with the parameters listed in Table 4 and Table 49.	
2	Configure the STAUT as in Table 8 and Table 49. Trigger the STAUT to associate to AP.		
3		Trigger the AP to inject ICMP Echo Requests using A-MSDU with a valid LLC/SNAP header to the STAUT. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: --ap amsdu-inject	If the Fragment and Forge Vulnerability Detection tool detects that STAUT responds to the ICMP Echo Requests via ICMP Echo Response, then FAIL, else PASS.

5.2.2 Frame aggregation attack with a malformed packet test

Objective

This test is to verify that a STAUT rejects an A-MSDU frame whose start is also a valid LLC/SNAP head in a malformed Data frame.

Applicability: Optional. This test is only executed if the STAUT declares support for A-MSDU attack mitigation indicated in Table 1.

References

Section 3.2, [2]

Test environment

- STAUT
- AP: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 51 defines the specific parameter values required for this test case.

Table 51. Frame aggregation attack with a malformed packet test configuration

Parameter	STAUT value	Fragment and Forge Vulnerability Detection tool acting as an AP value
Vendor	N/A	Refer to Appendix A
SSID	N/A	testffd

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Parameter	STAUT value	Fragment and Forge Vulnerability Detection tool acting as an AP value
Operating channel	N/A	1
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 52 provides the test procedure and expected results for this test case.

Table 52. Frame aggregation attack with a malformed packet test procedure and expected results

Step	STAUT	AP	Expected result
1		Configure AP with the parameters listed in Table 4 and Table 51.	
2	Configure the STAUT as in Table 8 and Table 51. Trigger the STAUT to associate to AP.		
3		Trigger the AP to inject ICMP Echo Requests using A-MSDU format with a valid LLC/SNAP header in a malformed Data frame to the STAUT. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: --ap amsdu-inject-bad	If the Fragment and Forge Vulnerability Detection tool detects that STAUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

5.3 Mixed key fragment attack tests

5.3.1 Mixed key fragment attack with non-consecutive PN test

Objective

This test is to verify that a STAUT denies fragments encrypted under different keys and with non-consecutive Packet Numbers (PN).

Applicability: Mandatory.

References

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Section 4, [2]

Test environment

- STAUT
- AP: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 53 defines the specific parameter values required for this test case.

Table 53. Mixed key fragment attack with non-consecutive PN test configuration

Parameter	STAUT value	Fragment and Forge Vulnerability Detection tool acting as an AP value
Vendor	N/A	Refer to Appendix A
SSID	N/A	testffd
Operating channel	N/A	1
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 54 provides the test procedure and expected results for this test case.

Table 54. Mixed key fragment attack with non-consecutive PN test procedure and expected results

Step	STAUT	AP	Expected result
1		Configure AP with the parameters listed in Table 4 and Table 49.	
2	Configure the STAUT as in Table 8 and Table 53. Trigger the STAUT to associate to AP.		
3		Trigger the AP to inject ICMP Echo Requests in two fragments encrypted with different keys and with non-consecutive PNs to the STAUT. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via	If the Fragment and Forge Vulnerability Detection tool detects that STAUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Step	STAUT	AP	Expected result
		command: --ap ping I,F,BE,AE --rekey-request	

5.3.2 Mixed key fragment attack with consecutive PN test

Objective

This test is to verify that a STAUT denies fragments encrypted under different keys and with consecutive Packet Numbers (PN).

Applicability: Mandatory.

References

Section 4, [2]

Test environment

- STAUT
- AP: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 55 defines the specific parameter values required for this test case.

Table 55. Mixed key fragment attack with consecutive PN test configuration

Parameter	STAUT value	Fragment and Forge Vulnerability Detection tool acting as an AP value
Vendor	N/A	Refer to Appendix A
SSID	N/A	testffd
Operating channel	N/A	1
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 56 provides the test procedure and expected results for this test case.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Table 56. Mixed key fragment attack with consecutive PN test procedure and expected results

Step	STAUT	AP	Expected result
1		Configure AP with the parameters listed in Table 4 and Table 55.	
2	Configure the STAUT as in Table 8 and Table 55. Trigger the STAUT to associate to AP.		
3		Trigger the AP to inject ICMP Echo Requests in two fragments encrypted with different keys and with consecutive PNs to the STAUT. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: --ap ping I,F,BE,AE --pn-per-qos --rekey-request	If the Fragment and Forge Vulnerability Detection tool detects that STAUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

5.4 Poisoning the fragment cache

5.4.1 Cached fragment attack with reassociation test

Objective

This test is to verify that a STAUT denies combination of cached fragment and a new fragment after reassociation.

Applicability: Mandatory.

References

Section 5, [2]

Test environment

- STAUT
- AP: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 57 defines the specific parameter values required for this test case.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Table 57. Cached fragment attack with reassociation test configuration

Parameter	STAUT value	Fragment and Forge Vulnerability Detection tool acting as an AP value
Vendor	N/A	Refer to Appendix A
SSID	N/A	testffd
Operating channel	N/A	1
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 58 provides the test procedure and expected results for this test case.

Table 58. Cached fragment attack with reassociation test procedure and expected results

Step	STAUT	AP	Expected result
1		Configure AP with the parameters listed in Table 4 and Table 57.	
2	Configure the STAUT as in Table 8 and Table 57. Trigger the STAUT to associate to AP.		
3		Trigger the AP to inject ICMP Echo Requests with following steps: 1. Injecting a fragment 2. Wait for a reassociation 3. Inject second fragment to the STAUT Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: --ap ping I,E,R,AE	If the Fragment and Forge Vulnerability Detection tool detects that STAUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

5.4.2 Cached fragment attack with reassociation with a time delay test

Objective

This test is to verify that a STAUT denies combination of cached fragment and a new time-delayed fragment after reassociation with a time delay.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Applicability: Mandatory.

References

Section 5, [2]

Test environment

- STAUT
- AP: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 59 defines the specific parameter values required for this test case.

Table 59. Cached fragment attack with reassociation with a time delay test configuration

Parameter	STAUT value	Fragment and Forge Vulnerability Detection tool acting as an AP value
Vendor	N/A	Refer to Appendix A
SSID	N/A	testffd
Operating channel	N/A	1
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 60 provides the test procedure and expected results for this test case.

Table 60. Cached fragment attack with reassociation with a time delay test procedure and expected results

Step	STAUT	AP	Expected result
1		Configure AP with the parameters listed in Table 4 and Table 59.	
2	Configure the STAUT as in Table 8 and Table 59. Trigger the STAUT to associate to AP.		

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Step	STAUT	AP	Expected result
3		Trigger the AP to inject ICMP Echo Requests with following steps: 1. Injecting a fragment 2. Wait for a reassociation 3. Wait for a time delay of 1 second 4. Inject second fragment to the STAUT Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: --ap ping I,E,R,E	If the Fragment and Forge Vulnerability Detection tool detects that STAUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

5.4.3 Cached fragment attack with de-authentication test

Objective

This test is to verify that a STAUT denies combination of cached fragment and an injected fragment after de-authentication and reconnection.

Applicability: Mandatory.

References

Section 5, [2]

Test environment

- STAUT
- AP: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 61 defines the specific parameter values required for this test case.

Table 61. Cached fragment attack with de-authentication test configuration

Parameter	STAUT value	Fragment and Forge Vulnerability Detection tool acting as an AP value
Vendor	N/A	Refer to Appendix A
SSID	N/A	testffd
Operating channel	N/A	1
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Parameter	STAUT value	Fragment and Forge Vulnerability Detection tool acting as an AP value
PMF	Enabled	Enabled

Test procedure and expected results

Table 62 provides the test procedure and expected results for this test case.

Table 62. Cached fragment attack with de-authentication test procedure and expected results

Step	STAUT	AP	Expected result
1		Configure AP with the parameters listed in Table 4 and Table 61.	
2	Configure the STAUT as in Table 8 and Table 61. Trigger the STAUT to associate to AP.		
3	If STAUT does not reconnect automatically, trigger STAUT to reconnect.	Trigger the AP to inject ICMP Echo Requests with following steps: 1. Injecting a fragment 2. Try triggering de-authentication 3. Wait for STAUT to reconnect 4. Inject second fragment to the STAUT Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: --ap ping I,E,R,AE --full-reconnect	If the Fragment and Forge Vulnerability Detection tool detects that STAUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

5.4.4 Cached fragment attack with de-authentication and reconnection with a time delay test

Objective

This test is to verify that a STAUT denies combination of cached fragment and a new time-delayed fragment after de-authentication and reconnection.

Applicability: Mandatory.

References

Section 5, [2]

Test environment

- STAUT

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

- AP: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 63 defines the specific parameter values required for this test case.

Table 63. Cached fragment attack with de-authentication and reconnection with a time delay test configuration

Parameter	STAUT value	Fragment and Forge Vulnerability Detection tool acting as an AP value
Vendor	N/A	Refer to Appendix A
SSID	N/A	testffd
Operating channel	N/A	1
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 64 provides the test procedure and expected results for this test case.

Table 64. Cached fragment attack with de-authentication and reconnection with a time delay test procedure and expected results

Step	STAUT	AP	Expected result
1		Configure AP with the parameters listed in Table 4 and Table 63.	
2	Configure the STAUT as in Table 8 and Table 63. Trigger the STAUT to associate to AP.		
3	If STAUT does not reconnect automatically, trigger STAUT to reconnect.	Trigger the AP to inject ICMP Echo Requests with following steps: 1. Injecting a fragment 2. Try triggering de-authentication 3. Wait for STAUT to reconnect 4. Wait for a time delay of 1 second 5. Inject second fragment to the STAUT	If the Fragment and Forge Vulnerability Detection tool detects that STAUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Step	STAUT	AP	Expected result
		Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: --ap ping I,E,R,E --full-reconnect	

5.5 Non-consecutive Packet Number Attack

5.5.1 Non-consecutive Packet Number attack test

Objective

This test is to verify that a STAUT denies encrypted fragments with non-consecutive Packet Numbers (PN).

Applicability: Mandatory.

References

Section 6.2, [2]

Test environment

- STAUT
- AP: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 65 defines the specific parameter values required for this test case.

Table 65. Non-consecutive Packet Number attack test configuration

Parameter	STAUT value	Fragment and Forge Vulnerability Detection tool acting as an AP value
Vendor	N/A	Refer to Appendix A
SSID	N/A	testffd
Operating channel	N/A	1
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Table 66 provides the test procedure and expected results for this test case.

Table 66. Non-consecutive Packet Number attack test procedure and expected results

Step	STAUT	AP	Expected result
1		Configure AP with the parameters listed in Table 4 and Table 65.	
2	Configure the STAUT as in Table 8 and Table 65. Trigger the STAUT to associate to AP.		
3		Trigger the AP to inject ICMP Echo Requests in two fragments encrypted with non-consecutive PNs to the STAUT. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: --ap ping I,E,E --inc-pn 2	If the Fragment and Forge Vulnerability Detection tool detects that STAUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

5.6 Accepting mixed plaintext and encrypted fragments or frames

5.6.1 Encrypted fragment followed by plaintext fragment attack test

Objective

This test is to verify that a STAUT denies a fragmented MSDU/MMPDU that includes an encrypted fragment followed by plaintext fragment after a secure connection.

Applicability: Mandatory.

References

Section 6.3, [2]

Test environment

- STAUT
- AP: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 67 defines the specific parameter values required for this test case.

© 2021 Wi-Fi Alliance. All Rights Reserved.

Table 67. Encrypted fragment followed by plaintext fragment attack test configuration

Parameter	STAUT value	Fragment and Forge Vulnerability Detection tool acting as an AP value
Vendor	N/A	Refer to Appendix A
SSID	N/A	testffd
Operating channel	N/A	1
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 68 provides the test procedure and expected results for this test case.

Table 68. Encrypted fragment followed by plaintext fragment attack test procedure and expected results

Step	STAUT	AP	Expected result
1		Configure AP with the parameters listed in Table 4 and Table 67.	
2	Configure the STAUT as in Table 8 and Table 67. Trigger the STAUT to associate to AP.		
3		Trigger the AP to inject ICMP Echo Requests in two fragments: encrypted fragment followed by plaintext fragments to the STAUT. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: --ap ping I,E,P	If the Fragment and Forge Vulnerability Detection tool detects that STAUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

5.6.2 Multiple mixed fragment attack test

Objective

This test is to verify that a STAUT denies a fragmented MSDU/MMPDU that includes encrypted and plaintext fragments after a secure connection.

Applicability: Mandatory.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

References

Section 6.3, [2]

Test environment

- STAUT
- AP: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 69 defines the specific parameter values required for this test case.

Table 69. Multiple mixed fragment attack test configuration

Parameter	STAUT value	Fragment and Forge Vulnerability Detection tool acting as an AP value
Vendor	N/A	Refer to Appendix A
SSID	N/A	testffd
Operating channel	N/A	1
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 70 provides the test procedure and expected results for this test case.

Table 70. Multiple mixed fragment attack test procedure and expected results

Step	STAUT	AP	Expected result
1		Configure AP with the parameters listed in Table 4 and Table 69.	
2	Configure the STAUT as in Table 8 and Table 69. Trigger the STAUT to associate to AP.		

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Step	STAUT	AP	Expected result
3		Trigger the AP to inject ICMP Echo Requests in following fragments to STAUT: 1. An encrypted fragment 2. An encrypted 2nd fragment 3. A plaintext fragment Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: --ap linux-plain	If the Fragment and Forge Vulnerability Detection tool detects that STAUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

5.6.3 Plaintext fragment followed by encrypted fragment attack test

Objective

This test is to verify that a STAUT denies a fragmented MSDU/MMPDU that includes a plaintext fragment followed by encrypted fragment after a secure connection.

Applicability: Mandatory.

References

Section 6.3, [2]

Test environment

- STAUT
- AP: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 71 defines the specific parameter values required for this test case.

Table 71. Plaintext fragment followed by encrypted fragment attack test configuration

Parameter	STAUT value	Fragment and Forge Vulnerability Detection tool acting as an AP value
Vendor	N/A	Refer to Appendix A
SSID	N/A	testffd
Operating channel	N/A	1
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Test procedure and expected results

Table 72 provides the test procedure and expected results for this test case.

Table 72. Plaintext fragment followed by encrypted fragment attack test procedure and expected results

Step	STAUT	AP	Expected result
1		Configure AP with the parameters listed in Table 4 and Table 71.	
2	Configure the STAUT as in Table 8 and Table 71. Trigger the STAUT to associate to AP.		
3		Trigger the AP to inject ICMP Echo Requests in two fragments: plaintext fragment followed by encrypted fragments to the STAUT. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: --ap ping I,P,E	If the Fragment and Forge Vulnerability Detection tool detects that STAUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

5.6.4 Plaintext data frame attack test

Objective

This test is to verify that a STAUT denies a plaintext MSDU/MMPDU after a secure connection.

Applicability: Mandatory.

References

Section 6.3, [2]

Test environment

- STAUT
- AP: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 73 defines the specific parameter values required for this test case.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Table 73. Plaintext data frame attack test configuration

Parameter	STAUT value	Fragment and Forge Vulnerability Detection tool acting as an AP value
Vendor	N/A	Refer to Appendix A
SSID	N/A	testffd
Operating channel	N/A	1
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 74 provides the test procedure and expected results for this test case.

Table 74. Plaintext data frame attack test procedure and expected results

Step	STAUT	AP	Expected result
1		Configure AP with the parameters listed in Table 4 and Table 73.	
2	Configure the STAUT as in Table 8 and Table 73. Trigger the STAUT to associate to AP.		
3		After connection, trigger the AP to inject ICMP Echo Requests in plaintext frame to the STAUT. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: --ap ping I,P	If the Fragment and Forge Vulnerability Detection tool detects that STAUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

5.6.5 Multiple plaintext fragment attack test

Objective

This test is to verify that a STAUT denies a fragmented MSDU/MMPDU that includes multiple plaintext fragments after a secure connection.

Applicability: Mandatory.

References

© 2021 Wi-Fi Alliance. All Rights Reserved.

Section 6.3, [2]

Test environment

- STAUT
- AP: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 75 defines the specific parameter values required for this test case.

Table 75. Multiple plaintext fragment attack test configuration

Parameter	STAUT value	Fragment and Forge Vulnerability Detection tool acting as an AP value
Vendor	N/A	Refer to Appendix A
SSID	N/A	testffd
Operating channel	N/A	1
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 76 provides the test procedure and expected results for this test case.

Table 76. Multiple plaintext fragment attack test procedure and expected results

Step	STAUT	AP	Expected result
1		Configure AP with the parameters listed in Table 4 and Table 75.	
2	Configure the STAUT as in Table 8 and Table 75. Trigger the STAUT to associate to AP.		
3		After connection, trigger the AP to inject ICMP Echo Requests in two plaintext fragments to the STAUT. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: --ap ping I,P,P	If the Fragment and Forge Vulnerability Detection tool detects that STAUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

5.7 Broadcast plaintext fragment attack

5.7.1 Broadcast plaintext fragment attack after connection test

Objective

This test is to verify that a STAUT denies fragment with a broadcast receiver address in a unicast frame after being connected.

Applicability: Mandatory.

References

Section 6.4, [2]

Test environment

- STAUT
- AP: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 77 defines the specific parameter values required for this test case.

Table 77. Broadcast plaintext fragment attack after connection test configuration

Parameter	STAUT value	Fragment and Forge Vulnerability Detection tool acting as an AP value
Vendor	N/A	Refer to Appendix A
SSID	N/A	testffd
Operating channel	N/A	1
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 78 provides the test procedure and expected results for this test case.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Table 78. Broadcast plaintext fragment attack after connection test procedure and expected results

Step	STAUT	AP	Expected result
1		Configure AP with the parameters listed in Table 4 and Table 77.	
2	Configure the STAUT as in Table 8 and Table 77. Trigger the STAUT to associate to AP.		
3		Trigger the AP to inject plaintext ICMP Echo Requests with a broadcast Receiver Address in 2nd fragment to STAUT after connection succeeds. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: --ap ping I,D,P --bcast-ra	If the Fragment and Forge Vulnerability Detection tool detects that STAUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

5.7.2 Broadcast plaintext fragment attack during 4-way handshake test

Objective

This test is to verify that a STAUT denies fragment with a broadcast receiver address in a unicast frame during 4-way handshake.

Applicability: Mandatory.

References

Section 6.4, [2]

Test environment

- STAUT
- AP: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 79 defines the specific parameter values required for this test case.

Table 79. Broadcast plaintext fragment attack during 4-way handshake test configuration

Parameter	STAUT value	Fragment and Forge Vulnerability Detection tool acting as an AP value
Vendor	N/A	Refer to Appendix A
SSID	N/A	testffd

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Parameter	STAUT value	Fragment and Forge Vulnerability Detection tool acting as an AP value
Operating channel	N/A	1
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 80 provides the test procedure and expected results for this test case.

Table 80. Broadcast plaintext fragment attack during 4-way handshake test procedure and expected results

Step	STAUT	AP	Expected result
1		Configure AP with the parameters listed in Table 4 and Table 79.	
2	Configure the STAUT as in Table 8 and Table 79. Trigger the STAUT to associate to AP.		
3		Trigger the AP to inject plaintext ICMP Echo Requests with a broadcast Receiver Address in 2nd fragment to STAUT during 4-way handshake. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: --ap ping D,BP --bcast-ra	SN: If STAUT responds to each ICMP Echo Request with an ICMP Echo Response, then FAIL, else PASS.

5.8 Faking A-MSDU as EAPOL handshake frames

5.8.1 Faking A-MSDUs as EAPOL after a secure connection test

Objective

This test is to verify that after a secure connection is successful, a STAUT denies A-MSDUs, with each containing an EAPOL subframe followed by a plaintext ICMP Echo Request subframe.

Applicability: Mandatory.

References

© 2021 Wi-Fi Alliance. All Rights Reserved.

Section 6.5, [2]

Test environment

- STAUT
- AP: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 81 defines the specific parameter values required for this test case.

Table 81. Faking A-MSDUs as EAPOL after a secure connection test configuration

Parameter	STAUT value	Fragment and Forge Vulnerability Detection tool acting as an AP value
Vendor	N/A	Refer to Appendix A
SSID	N/A	testffd
Operating channel	N/A	1
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 82 provides the test procedure and expected results for this test case.

Table 82. Faking A-MSDUs as EAPOL after a secure connection test procedure and expected results

Step	STAUT	AP	Expected result
1		Configure AP with the parameters listed in Table 4 and Table 81.	
2	Configure the STAUT as in Table 8 and Table 81. Trigger the STAUT to associate to AP.		
3		After a secure connection is successful, trigger the AP to inject A-MSDUs, with each containing one EAPOL subframe followed by a plaintext ICMP Echo Request subframe to STAUT.	If the Fragment and Forge Vulnerability Detection tool detects that STAUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Step	STAUT	AP	Expected result
		Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: --ap eapol-amsdu I,P	

5.8.2 Faking malformed A-MSDU as EAPOL after a secure connection test

Objective

This test is to verify that a secure connection is successful, a STAUT denies A-MSDUs, with each containing a malformed EAPOL subframe followed by a plaintext ICMP Echo Request subframe.

Applicability: Mandatory.

References

Section 6.5, [2]

Test environment

- STAUT
- AP: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 83 defines the specific parameter values required for this test case.

Table 83. Faking malformed A-MSDU as EAPOL after a secure connection test configuration

Parameter	STAUT value	Fragment and Forge Vulnerability Detection tool acting as an AP value
Vendor	N/A	Refer to Appendix A
SSID	N/A	testffd
Operating channel	N/A	1
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 84 provides the test procedure and expected results for this test case.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Table 84. Faking malformed A-MSDU as EAPOL after a secure connection test procedure and expected results

Step	STAUT	AP	Expected result
1		Configure AP with the parameters listed in Table 4 and Table 83.	
2	Configure the STAUT as in Table 8 and Table 49. Trigger the STAUT to associate to AP.		
3		After the secure connection is successful, trigger the AP to inject A-MSDUs, with each containing one malformed EAPOL subframe followed by a plaintext ICMP Echo Request subframe to STAUT. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: --ap eapol-amsdu-bad I,P	If the Fragment and Forge Vulnerability Detection tool detects that STAUT responds to the ICMP Echo Requests with ICMP Echo Responses, then FAIL, else PASS.

5.8.3 Faking A-MSDUs as EAPOL during 4-way handshake test

Objective

This test is to verify that during 4-way handshake, a STAUT denies A-MSDUs, with each containing a malformed EAPOL subframe followed by a plaintext ICMP Echo Request subframe.

Applicability: Mandatory.

References

Section 6.5, [2]

Test environment

- STAUT
- AP: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 85 defines the specific parameter values required for this test case.

© 2021 Wi-Fi Alliance. All Rights Reserved.

Table 85. Faking A-MSDUs as EAPOL during 4-way handshake test configuration

Parameter	STAUT value	Fragment and Forge Vulnerability Detection tool acting as an AP value
Vendor	N/A	Refer to Appendix A
SSID	N/A	testffd
Operating channel	N/A	1
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 86 provides the test procedure and expected results for this test case.

Table 86. Faking A-MSDUs as EAPOL during 4-way handshake test procedure and expected results

Step	STAUT	AP	Expected result
1		Configure AP with the parameters listed in Table 4 and Table 85.	
2	Configure the STAUT as in Table 8 and Table 85. Trigger the STAUT to associate to AP.		
3		During the 4-way handshake, trigger the AP to inject A-MSDUs, with each contains with each containing one EAPOL subframe followed by a plaintext ICMP Echo Request subframe to STAUT. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: --ap eapol-amsdu BP	SN: If STAUT responds to each ICMP Echo Request with an ICMP Echo Response, then FAIL, else PASS.

5.8.4 Faking malformed A-MSDU as EAPOL during 4-way handshake test

Objective

This test is to verify that during 4-way handshake, a STAUT denies A-MSDUs, with each containing a malformed EAPOL subframe followed by a plaintext ICMP Echo Request subframe.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Applicability: Mandatory.

References

Section 6.5, [2]

Test environment

- STAUT
- AP: Fragment and Forge Vulnerability Detection tool
- RF shielded room

Test configuration

Table 87 defines the specific parameter values required for this test case.

Table 87. Faking malformed A-MSDU as EAPOL during 4-way handshake test configuration

Parameter	STAUT value	Fragment and Forge Vulnerability Detection tool acting as an AP value
Vendor	N/A	Refer to Appendix A
SSID	N/A	testffd
Operating channel	N/A	1
Security	WPA2-Personal	WPA2-Personal
Passphrase	12345678	12345678
PMF	Enabled	Enabled

Test procedure and expected results

Table 88 provides the test procedure and expected results for this test case.

Table 88. Faking malformed A-MSDU as EAPOL during 4-way handshake test procedure and expected results

Step	STAUT	AP	Expected result
1		Configure AP with the parameters listed in Table 4 and Table 87.	
2	Configure the STAUT as in Table 8 and Table 49. Trigger the STAUT to associate to AP.		
3		During the 4-way handshake, trigger the AP to inject A-MSDUs, with each containing	SN:

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Step	STAUT	AP	Expected result
		malformed EAPOL subframe followed by a plaintext ICMP Echo Request subframe to STAUT. Note: Fragment and Forge Vulnerability Detection Tool injects the fragments via command: --ap eapol-amsdu-bad BP	If STAUT responds to each ICMP Echo Request with an ICMP Echo Response, then FAIL, else PASS.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Appendix A (Normative) Test bed products

A.1 Approved test tool equipment

Table 89 lists the approved test equipment required to execute the test cases in this test plan.

Table 89. Approved test equipment

Vendor	Product	Contact
Alfa	Alfa-AWUS036NHA	support@wi-fi.org

Table 90 lists the additional test tools required to execute the test cases in this test plan.

Table 90. Additional test tools

Device	Product	Other certification programs using this device	Contact
Wireless Sniffer	Sniffer/Intel AX200 NGWG.NV	Wi-Fi 6	support@wi-fi.org

A.2 Test bed verification

A.2.1 Test bed verification tests for APUT

Following tests are designed to validate test bed STA setup before proceeding to APUT tests. Each test is labeled with distinct test case ID in Wi-Fi Test Suite as listed below:

- **Test ID 4.0.1**: This test is to verify that the testbed STA can successfully connect with APUT, send an ICMP Echo Request and receive ICMP Echo Response from APUT.
- **Test ID 4.0.2**: This test is to verify that the testbed STA can successfully connect with APUT, send a fragmented ICMP Echo Request and receive ICMP Echo Response from APUT.
- **Test ID 4.0.3**: This test is to verify that the testbed STA can successfully connect with APUT, send an ICMP Echo Request enclosed in a normal (non SPP protected) A-MSDU frame and receive ICMP Echo Response from APUT.

A.2.2 Test bed verification tests for STAUT

Following tests are designed to validate test bed AP setup before proceeding to STAUT tests. Each test is labeled with distinct test case ID in Wi-Fi Test Suite as listed below:

- **Test ID 5.0.1**: This test is to verify that the testbed AP can successfully connect with STAUT, send an ICMP Echo Request and receive ICMP Echo Response from STAUT.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

- **Test ID 5.0.2**: This test is to verify that the testbed AP can successfully connect with STAUT, send a fragmented ICMP Echo Request and receive ICMP Echo Response from STAUT.
- **Test ID 5.0.3**: This test is to verify that the testbed AP can successfully connect with STAUT, send an ICMP Echo Request enclosed in a normal (non SPP protected) A-MSDU frame and receive ICMP Echo Response from STAUT.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.

Appendix B (Informative) Document revision history

Table 91. Document revision history

Version	Date YYYY-MM-DD	Remarks
1.0	2021-05-11	Initial release.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2021 Wi-Fi Alliance. All Rights Reserved.