March 2015

Technical Note
Removal of TKIP from Wi-Fi® Devices

Version 1.0

Effective Date: March 16, 2015

WI-FI ALLIANCE PROPRIETARY – SUBJECT TO CHANGE WITHOUT NOTICE

This document may be used with the permission of Wi-Fi Alliance under the terms set forth herein. By your use of the document, you are agreeing to these terms. Unless this document is clearly designated as an approved specification, this document is a work in process and is not an approved Wi-Fi Alliance specification. This document is subject to revision or removal at any time without notice. Information contained in this document may be used at your sole risk. Wi-Fi Alliance assumes no responsibility for errors or omissions in this document. This copyright permission does not constitute an endorsement of the products or services. Wi-Fi Alliance trademarks and certification marks may not be used unless specifically allowed by Wi-Fi Alliance.

Wi-Fi Alliance has not conducted an independent intellectual property rights ("IPR") review of this document and the information contained herein, and makes no representations or warranties regarding IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions.

Wi-Fi Alliance owns the copyright in this document and reserves all rights therein. A user of this document may duplicate and distribute copies of the document in connection with the authorized uses described herein, 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. Unauthorized use, duplication, or distribution is an infringement of Wi-Fi Alliance's copyright.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY WI-FI ALLIANCE AND WI-FI ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF THIS DOCUMENT AND ANY INFORMATION CONTAINED IN THIS DOCUMENT.

Introduction

This technical note will provide important information to network administrators and equipment vendors on the importance of using WPA2™, and on potential considerations when evaluating whether to disable WPA™. This document describes the current problems encountered when using TKIP/WPA, the barriers encountered by the industry, the recommended solution by Wi-Fi Alliance®, and changes to the Wi-Fi CERTIFIED™ program to discourage the use of TKIP/WPA. Implementation of the recommendations in this technical note will accelerate the retirement of TKIP/WPA and encourage the industry-wide transition to WPA2.

Problem

WPA, which uses Temporal Key Integrity Protocol (TKIP), no longer provides sufficient security to protect consumer or enterprise Wi-Fi® networks. TKIP is an older security technology with known vulnerabilities to some cryptographic attacks. TKIP and WEP use the same underlying cipher, and, consequently, they are vulnerable to a number of similar attacks. TKIP was designed as a transitional mechanism in 2004 for devices equipped with WEP and unable to support AES. Due to the known vulnerabilities of TKIP, networks utilizing it may be more susceptible to attack.

Recommendations

1. **Network administrators should purchase or deploy equipment that supports WPA2.**

   WPA2, based on the 802.11 standard, includes the Advanced Encryption Standard (AES). WPA2 with AES offers an overall higher level of security to consumer and enterprise users. Wi-Fi Alliance has required WPA2 on all Wi-Fi CERTIFIED products since 2006.

2. **Network administrators should configure their APs to be WPA2 only.**

   Despite the continued ability to configure "TKIP-only" and WPA / WPA2 mixed mode networks in Wi-Fi CERTIFIED devices, Wi-Fi Alliance strongly discourages their use because of known vulnerabilities in TKIP. Network administrators should regularly evaluate their need to operate "TKIP-only" or WPA / WPA2 mixed mode networks. If TKIP is required to support legacy devices on their networks, then network administrators should take additional protective measures such as keeping TKIP devices on networks that are firewalled or independent of other networks. As organizations retire legacy (certified prior to 2004) client devices that needed "TKIP-only" networks, they should also retire "TKIP-only networks." Similarly, administrators should consider disabling or removing WPA / WPA2 mixed mode support from WPA2 networks as their need to support legacy (certified prior to 2006) devices that do not support WPA2 declines.

3. **Equipment vendors should proactively transition away from TKIP support by discouraging its use to their customer base, and removing the functionality in products as internal research indicates when their market no longer needs it.**

   For equipment vendors, Wi-Fi Alliance recommends that they discourage the use of TKIP in the short term, and ultimately remove TKIP from all Wi-Fi devices when their market no longer needs it. At a minimum, vendors should remove TKIP and any "TKIP-only" mode configurations from the primary device interface. Access to the "TKIP-only" configuration mode via a secondary configuration interface is acceptable. The requirement to go to a secondary interface is a mechanism used to restrict TKIP usage to only those deployments with legacy devices; other deployments will typically use the primary configuration interface (e.g. web or graphical interface), where the “TKIP-only” option is not present. This approach balances the needs of the deployed base with the goal of reducing the use of “TKIP-only” modes by making selection of these modes less prominent.

Impact on Wi-Fi Alliance Certification

Wi-Fi Alliance prohibits a Wi-Fi CERTIFIED device from offering a “TKIP-only” configuration option through the device’s primary interface. Wi-Fi CERTIFIED devices may continue to offer a “TKIP-only” mode through a secondary user interface to support legacy devices, when needed.

Wi-Fi CERTIFIED devices are allowed, but discouraged to offer use of WPA / WPA2 mixed mode on the primary interface.