Technical Note

Wi-Fi CERTIFIED Miracast™ HDCP Interoperability Issue:

HDCP 2.2 Protocol Descriptor

Version 1.0

March 24, 2015

Introduction

HDCP is a content protection mechanism that governs the transfer of media between devices that originate protected content (Sources) and displaying devices (Sinks). A common use case is a Miracast® user displaying an HDCP-protected movie from their mobile phone or tablet to a television.

This document describes an observed interoperability issue between some Miracast Source implementations with an HDCP 2.0/2.1 stack/certificate and some Miracast Sink implementations with an HDCP 2.2 stack/certificate where the content does not render correctly due to an authentication issue. If a Source fails authentication with a Sink, the user may experience errors such as:

- The Source and Sink may provide no information to the user, and it appears to the user that the connection has “failed”
- The Source may provide an audio-only connection to the Sink
- The Source may show a blank screen to the user with no other information
- The Source or Sink may indicate some kind of “Content Protection” error

Problem

Some Source implementations incorrectly assumed that Reserved bits (3087:3072) in the HDCP Receiver Public Key Certificate of [1] must always be zero (0x0000) and rely on that assumption as part of signature validation. HDCP 2.2 updated the certificate format and uses 4 of the 16 previously reserved bits (3087:3084) as the Protocol Descriptor [2], The Protocol Descriptor value can be 0x0 or 0x1. If the Source fails signature validation for Sinks supplying a certificate as part of AKE_RX_Info message of [1] with the bits set to anything other than 0x0, then it will not authenticate Sinks using HDCP 2.2 certificates, resulting in broken forward compatibility.

Similar problems may occur if an HDCP capable Sink inadequately handles the received Reserved bits within HDCP AKE messages of [2] from a Source.

Recommendation

Wi-Fi Alliance® recommends that all HDCP-capable Miracast device vendors check their devices for implementations that inadequately handle the received Reserved bits defined in the HDCP IIA 2.x specification and update any affected devices to correct this error. All 16 bits (3087:3072) shall be ignored in HDCP 2.0/2.1 implementations and the specific bits of the Protocol Descriptor shall be checked in HDCP 2.2 implementations (3087:3084).

Suggestions on providing feedback to a user after an authentication error are described in the “Best Practices Document for Wi-Fi CERTIFIED Miracast™ Devices” [3].

References

[1] "High-bandwidth Digital Content Protection System, Interface Independent Adaptation" Revision 2.0", 23 October, 2008, Digital Content Protection LLC

[2] "High-bandwidth Digital Content Protection System, Interface Independent Adaptation" Revision 2.2", 16 October, 2012, Digital Content Protection LLC

[3] "Best Practices Document for Wi-Fi CERTIFIED Miracast™ Devices", September 2014, Wi-Fi Alliance