OpenSource Security Ralf Spenneberg

Am Bahnhof 3-5

48565 Steinfurt

info@os-s.net

OS-S Security Advisory 2016-02

Date: January 1st, 2016

Updated: January 1st, 2016

Authors: Oguzhan Cicek, Hendrik Schwartke, Ralf Spenneberg

CVE: Not yet assigned

CVSS: 6.2 (AV:L/AC:L/Au:S/C:C/I:C/A:N)

Title: Weak authentication in NXP Hitag S transponder allows an attacker to read, write and clone any tag

Severity: Critical. All applications relying only on the Hitag S security are broken.

Ease of Exploitation: Trivial

Vulnerability: Weak authentication using 48 bit key and 24 bit password

Product: NXP Hitag S transponder

Abstract

The Hitag S transponder supports a crypto mode. In crypto mode the transponder requires a bilateral authentication before the transponder may be read or written. This authentication uses a 48 bit key and a 24 bit password. The underlying algorithm is not publicly documented. We determined that the Hitag S transponder uses the same crypto algorithm as the Hitag 2 which was published already in 2006 by Wiener [1]. The algorithm may be broken using a crypto-analytic attack published at Usenix 2012 [2] and using SAT-Solvers. The cryptoanalytic attack requires 150 sniffed authentication challenges between a valid reader and a corresponding transponder. The attack using SAT solver requires 2 such challenges because every authentication challenge provides only 40 bits encrypted data with known plaintext. To deduct the 48 bits of the used key more data is required.

Using SAT solvers the key can usually be retrieved within 5 days.

The Hitag S may read-protect the areas where the key and a password is stored. While the key may be broken and is thus known to the attacker the password send by the transponder during the authentication. Although the password is send encrypted the attacker may decrypt the password using the broken key.

Impact

The attacker may read and write all not-protected areas of the transponder. The applications using the transponder need to implement there own mechanisms to protect the integrity and confidentiality of the stored information.

The attacker may emulate the transponder (using for example the proxmark 3) since the protocol and crypto algorithm is now known and the attacker has access to the full content of the transponder to be emulated.

Vendor Contact

The vendor NXP was first contacted July 17th 2015 using [info|security|abuse]@nxp.com. We did not receive any response. We contacted NXP a second time using psirt@nxp.com on November 17th 2015. This time we received a response and communicated the vulnerability to the vendor.

[1] https://web.archive.org/web/20120127012528/http://cryptolib.com/ciphers/hitag2

[2] https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/verdult