

[Full-disclosure] RFID access control tokens widely open to cloning

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2006-12/msg00239.html>

- *From:* Adam Laurie <adam.laurie@xxxxxxxxxxxxxx>
 - *Date:* Mon, 11 Dec 2006 17:51:40 +0000
-

Too many systems to itemize here rely on the 'unique ID' of an RFID token to grant access to a system or building, and, in the case that these tokens are based on 125kHz or 134.2kHz standard tags, many of them may be vulnerable to relatively simple cloning attacks.

In a way this is nothing new – several researchers have previously presented attacks whereby RFID tags were emulated by custom built circuits which were able to fool readers into thinking that a genuine tag had been presented. However, the industry response was normally that this was not a 'real' threat, as it required specialist knowledge and equipment, and the resulting device was not a 'true clone' as it didn't have the same form factor as the original.

The difference here is that the 'clone' may actually follow the same form factor as the original, and is therefore indistinguishable not just to the reader, but also to the human eye. In addition, no specialist equipment or custom circuitry is required, and the 'clones' can be produced using off the shelf equipment, software and blank tags purchased perfectly legally over the Internet. In fact, the tags are only doing what they were designed to do in the first place: implement industry standards.

The problem is that many security system suppliers are integrating industry standard tag readers, and promoting the 'uniqueness' of the tag ID as a guaranteed certainty when it isn't, and thereby compromising the security of the entire system.

The two specific tag types I've looked at are:

Trovan 'Unique', aka EM4x02

FDX-B, aka EM4x05 – ISO-11784/5 (animal tags)

The description of the 'Unique' tag, from the Trovan website is as follows:

"The TROVAN UNIQUE" Read-Only System is well-suited to applications that require a high level of data security. Unlike other vendors' factory preprogrammed lines, the protocol of the TROVAN UNIQUE" line is

[Full-disclosure] RFID access control tokens widely open to cloning

patented, providing unmatched protection against unauthorised third-party cloning. Each transponder is programmed with a unique 10-digit ID code during manufacture. Comprehensive automatic test methods ensure that no code exists in duplicate in any of the TROVAN UNIQUE" transponder types, and that codes are programmed correctly in a readable manner. Once the code is programmed at the time of the transponder's manufacture, it cannot be counterfeited or tampered with. A total of 550 billion unique ID codes is available."

Q5 are general purpose, multi-standard tags, that are capable of emulating other devices. I found that it was a standard feature of the Q5 chip to emulate a 'Unique' tag, and it was trivial to program a duplicate ID into one. The resulting tags were tested against three different systems that I have access to, and all three systems were unable to distinguish between the original and the 'clone'.

In response to my questioning the security of the Unique tags, the response I got from Trovan was: "There are a variety of H4102 versions, some of which can be emulated by a Q5 tag. Our tags are a custom version of the H4100 tag."

It should be noted that I am not pointing the finger at Trovan devices here, but the 'Unique' standard some of their tags implement and which are generally available as a generic tag type – it is sometimes hard to tell exactly who's devices or tags are used in a specific installation, but suffice it to say that I have found 3rd party systems (one at a very recent security systems show in London) that were vulnerable to EM4x02 style cloning. The equipment required to do this was a laptop and off the shelf RFID reader/writer, but it could just as easily have been a small handheld, and so a credible threat exists of simply swiping an access tag ID in a 'walk-by' of someone leaving a building, and then producing a clone which will give full access.

I am also able to produce what seem to be accurate clones of FDX-B tags (such as the one in my dog), and also VeriChip tags, in as much as a standard FDX-B reader such as you might find at your local vet will not be able to tell the difference. I have not been able to test if a genuine VeriGuard system would also be fooled, but VeriCorp's response when I took it up with them was:

"You can take a write once and re-writeable chip and put the VeriGuard ID number on this chip, and a lot of readers will read the ID and including the VeriGuard reader. I can not tell you every but their three things that tell are unit that it is a VeriChip 16 digits not 15, timing and one other thing. We call it copying not cloning because the can't get all the information need to send to the VeriGuard reader at the right time."[sic]

The latest release of the open source python library, RFIDIOt (v0.1h), contains tools for programming both EM4x02 and EM4x05 tag IDs to Q5 or Hitag2 tags, and I would suggest that if you own (or supply) systems

[Full-disclosure] RFID access control tokens widely open to cloning

based on either of these standards, that you use them to audit for this vulnerability.

Full details here:

<http://rfidiot.org>

cheers,

Adam

--

Adam Laurie Tel: +44 (0) 1304 814800

The Bunker Secure Hosting Ltd. Fax: +44 (0) 1304 814899

Ash Radar Station <http://www.thebunker.net>

Marshborough Road

Sandwich <mailto:adam@xxxxxxxxxxxxx>

Kent

CT13 0PL

UNITED KINGDOM PGP key on key servers

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>