Education IT Government IT
blogs

George Ou

August 21, 2006

RFID passports and VeriChip security podcast

Posted by **George Ou** @ 4:45 pm

Digg This!

Download the MP3 | **Subscribe** | **More Podcasts**

–

I had the opportunity to interview Kevin Mahaffey who is the Director of Development for **Flexilis Inc**. Kevin and his team of researchers presented a **video** at Black Hat 2006 illustrating improperly shielded RFID (Radio Frequency Identifier) passports that can potentially be used to trigger a bomb.

It turns out that RFID passwords were originally designed to transmit in clear text but that was determined to be too risky for people's personal data and privacy. An encryption mechanism was added and the keying material needed to decrypt the RFID signal was printed on the passport and had to be read by an optical reader. If a good encryption algorithm with sufficient key length is used, the user's personal data on their passports would be protected. But we want to avoid bad RFID implementations like the Dutch passport which according to Mahaffey was extremely simple to break because it had an effective entropy of 30 bits in the encryption key.

The issue of RFID cloning came up because Lukas Grunwald recently demonstrated the cloning of an RFID chip from an RFID passport. This has unfortunately led to lot of misinformation going around the web that the RFID passports have been cloned and therefore is totally ineffective. This misunderstanding has unfortunately led to some misdirected anger at having any kind of chip technology on our ID systems. But just because the passport is cloned doesn't mean it's been compromised because there is a digital signature on the passports. If anyone attempts to modify any of the information on that passport such as the name or the photograph, it would immediately invalidate the checksum on the digital signature. As Mahaffey pointed out, current passports only have a "hologram that looks pretty and therefore must be real". No digital signatures on conventional passports means that the pictures and names on the passport can be modified or a complete forgery can be produced with an arbitrary name and photo. So there is a definite advantage to having a digital signature component in a chip on a passport, but only if it's implemented in a way that doesn't compromise a user's privacy or security.

But encryption only hides the content of the passport and not the presence of the passport. There is no reason people should be forced to beacon the fact that they are carrying passports which could potentially give away clues about a person's country of origin. High powered RFID readers could still read the RFID passports from several feet away so a metal shield was added to the RFID passports to prevent leakage of the RFID signal. But Flexilis has determined that the shielding was inadequate even when the passport is opened a quarter of an inch. To demonstrate the potential dangers, Flexilis **conducted field tests** showing an RFID passport triggering a simulated bomb.

I also asked Mahaffey about the new human implantable chips from **VeriChip** being proposed for various applications including **Access Control**. To my surprise, Mahaffey stated that the VeriChip implants didn't

use any kind of cryptography to protect the unique ID stored on the chips! I asked Mahaffey how easy it would be to clone these chips and it turns out to be trivial. Not only is there no encryption going on, but the VeriChip implants are so simple to replicate that in fact, someone has already demonstrated how easy it is to clone a VeriChip. I then asked what would happen if someone clones your VeriChip implant? As Mahaffey put it: "it's time to go under the knife" (to get the chip replaced).

But even if the VeriChip implants were using strong cryptography, would it then be wise to implant an authentication device in your body? While I have always supported the use of strong authentication devices such as smartcards and cryptographic tokens, I don't want it inside my body. No material item on this Earth is worth life or limb and I would rather hand over my key rather than have it cut out of me. So the only thing these VeriChip implants seem to be good for is my cat or someone who would voluntarily rather have an implant instead of wearing a medical ID tag for emergency care. But in the end, both Mahaffey and I agree that any technology should be voluntary and users should always be able to opt out without consequence.

11 Comments | **Blog This** | **E-mail This** | **Print This** | **Permalink**

Categories: Security, Infrastructure, Mobile/Wireless, News, Podcasts
Previous Post **Next Post**

LATEST **Message has been deleted.**
(**Read the rest**)

a practical addition George.. Arnout Groen -- 08/22/06 **Technology is lots of fun** WiredGuy -- 08/22/06 **Implants** beepster -- 08/24/06 **VeriChip is a from of Tyranny NOT Security** ciociario -- 08/25/06 **Message has been deleted.** ciociario -- 08/25/06 **Message has been deleted.** ciociario -- 08/25/06 **Message has been deleted.** ciociario -- 08/25/06 **Message has been deleted.** ciociario -- 08/25/06 **Message has been deleted.** ciociario -- 08/25/06 TALKBACK **Add your opinion**

Trackbacks

The URI to TrackBack this entry is: *http://blogs.zdnet.com/Ou/wp-trackback.php?p=301*

No trackbacks yet.