ARTICLE:

RFID TECHNOLOGY AND THE FUTURE- OLD SCHOOL FRAUD IN A NEW WRAPPER

By **Johnny Bengtsson**

It is just a matter of time before the first RFID skimmer will reach our laboratory, and therefore the designs are as yet unknown. Based on previous experiences from magnetic stripe card skimmers, this article considers how RFID skimmers could exhibit similarities to traditional ones.

Introduction

The radio frequency identification (RFID) is a standardised contactless technology for wireless data exchange between a device (it can be a reader/writer device – the interrogator) and a data carrier (tag or transponder). The technology has its roots in transponder technology, and was rapidly developed and adopted by other industries: supply chain management, retail logistics, animal tagging, human implants, electronic toll collection, e-passports, car keys, library book, tracking, tagging and such like. An RFID device can replace the more or less obsolete magnetic stripe cards and optical bar codes, but RFID technology is not only an upgrade. RFID also provides the user or application with additional properties and functions: increased data storage space, reading and writing capability, data integrity protection (encryption, digital certificates, digital signatures and more), internal data processing – and last but not at least – tag interaction without the need for line of sight or physical contact.

Principle and related work

The interrogator is the tag reader and is also described as the transceiver. In some cases it also serves as tag writer. Basically an interrogator consists of an antenna connected to a transceiver, a signal and data processing function, internal memory storage and an interface. The interrogator also has a set of commands for tag interaction.

The RFID tag is the data carrier, also known as the transponder. It has several properties which governs the interaction of distance and data communication quality: working frequency, antenna design, RF modulation and power supply. The cheapest and probably most common in applications, such as access control and ticketing, are passive tags. These do not have an internal power supply. This is solved because the device that interrogates constantly emits an electromagnetic field induced electric current, and recharges the integrated capacitor of the tag with help from the coil within the tag. The capacitor provides a current to the circuitry, and the tag begins to send its stored data via modulated backscatter, simply described as a RF reflection and recognised by the interrogator.

An RFID tag is identified by its unique identifier (UID), a number that normally cannot (and should not) be altered. The UID is often considered to be the most important information in RFID hacking issues. There are a several countermeasures to provide for the protection of data protection, such as encrypting the data blocks and interrogator authorisation set in the tag. Several research groups and hacking communities have reported attacks to get around such obstacles, for example side-channel attacks, RF eavesdropping, man-in-the-middle and relay attacks, cryptographic algorithm attacks, reverse engineering and emulation of tags.[1] What they all seem to have in common is that the attacks take place outside the interrogator.

[1] *A great deal of material on this topic can be obtained on-line at http://www.avoine.net/rfid/.*

The perspective of the work on RFID tags

The majority of the RFID research work seems to concentrate on external attacks. The project described in this article assumes that the RFID skimming will actually take place inside the interrogator cabinet. Several advanced magnetic stripe skimmer devices or credit card skimmers adapted for point-of-sale (POS) terminals, petrol pumps and automated teller machines (ATMs) have been analysed at the Swedish National Laboratory of Forensic Science – SKL. Based on observations made during these analyses, it is predicted that RFID skimmers will be designed in similar ways.

Similarities with credit card skimmers

A functional skimmer – as recognized by SKL – acquires two essential types of information: data and authorisation. These two parts would probably be common for all kinds of skimmers. For a credit card skimmer, data would be the F/2F (two-frequency coherent-phase) data encoded card information stored on the magnetic stripe, while the PIN (personal identification number) would correspond to authorisation.

Briefly explained, the skimming devices that were analysed that were attached to or embedded inside magnetic stripe reading devices (here called hosts). They most often consist of an intercept device connected to a magnetic head or soldered on to an internal F/2F decoder unit's decoded output, with a power supply from the host or from a separate battery pack, a microprocessor for data or signal processing, commonly a flash memory for magnetic stripe data storage and an interface with the function of communicating information that is obtained by skimming, either by wire or wirelessly. The PIN is often obtained by using a video recording pin-hole camera, or a keypad tap with wires soldered on to the printed circuit board (PCB) of the keypad or by using an extra keypad membrane. Where it is thought that cabinet intrusion detectors are in place, such detectors are commonly disabled by short-circuiting bridges.

Based on the description of a typical credit card skimmer, the work outlined in this article proposes that ideas from such devices are applicable to potential RFID skimmers, internally mounted inside an interrogator to conceal the electronics. For example, the wiretapping device would probably be attached to a RFID transponder decoder unit instead of a F/2F decoder circuit and so forth.

Discussion

To date, the Swedish National Laboratory of Forensic Science has not observed any attacks or attempted attacks on RFID related systems in Sweden. There is no clear answer for this; the technology behind RFID is still new or unknown to the law enforcement authorities in Sweden. The laboratory is currently running a project to gain advanced knowledge in hi-tech RFID technology, including standards, hardware and related work. The project also aims to develop new forensic analysis methods and best practice recommendations for potential RFID technology related crimes.

Conclusion

There are reasons to believe that unmonitored RFID devices are likely to become targets for embedded RFID skimmers in the future, located inside interrogator device cabinets. The level of fraudulent electronic design has reached a point where miniaturisation for concealment, advanced signal processing and wireless communication is no longer an issue. This is experienced from the large number of magnetic stripe card (credit card) skimming device analyses undertaken at SKL. Suggestions on potential RFID systems to be attacked are access card keys, transponders, electronic toll collection and asset tracking. Payment card readers on self service terminals and petrol pumps are also considered to be at risk for possible embedded RFID skimmers.

However, tag emulators in plastic card form would probably be a limiting factor for RFID skimmers. No such cards that enable the UID to be altered have been seen on the market yet. It might be less feasible to expose an electronic tag emulator instead of a plastic card on RFID terminals monitored by humans (commercial stores, border controls or on public transportation systems).

This article was prepared from a presentation given by the author at the 5th European Academy of Forensic Science Conference, EAFS 2009, held in Glasgow between 8 – 11 September 2009. The project is run by the author at Statens kriminaltekniska laboratorium.

johnny.bengtsson@skl.police.se

The reader will find the following list of papers to be of interest and a general introduction to the available literature:

Gerhard de Koning Gans, Jaap-Henk Hoepman and Flavio D. Garcia, 'A Practical Attack on the MIFARE Classic', in G. Grimaud and F.-X. Standaert, editors, Eighth Smart Card Research and Advanced Application Conference: CARDIS 2008, Lecture Notes in Computer Science, Volume 5189 (Springer Verlag, 2008), pp 267-282,

Gerhard P. Hancke, 'A Practical Relay Attack on ISO 14443', (February 2005)

Gerhard P. Hancke, 'Eavesdropping Attacks on High-Frequency RFID Tokens', (RFIDSec'08, July 2008)

Michael Hutter, Stefan Mangard, Martin Feldhofer, 'Power and EM Attacks on Passive 13.56 MHz RFID Devices', Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, 10-13 September 2007

Timo Kasper, David Oswald and Christof Paar, 'New Methods for Cost-Effective Side-Channel Attacks on Cryptographic RFIDs', RFIDsec09 (2009)

Michal Krumnikl, 'Unique (EM4001) RFID Emulator', (August 2007)

Karsten Nohl, Henryk Plötz, Mifare, 'Little Security, Despite Obscurity', 24th Chaos Communication Congress (2007)

Karsten Nohl, David Evans, Starbug and Henryk Plötz, 'Reverse-Engineering a Cryptographic RFID Tag', Proceedings of the 17th conference on Security symposium, San Jose, CA (USENIX Association, 2008), pp 185-193

Melanie R. Rieback, 'Security and privacy of Radio Frequency Identification', 2008

