

Dear members,

In this edition of our Newsletter, we focus again on the issue of security. In the past, we have already covered the use of "zero-knowledge proofs" as the basis for a reliable and acceptable scheme of RFID security. New products that have recently been presented implement this concept of zero-knowledge proofs. But to get you started, let's begin with a recap of a story we read elsewhere...

RFID hacking underground story

The online "Wired" magazine (www.wired.com) featured an article called "The RFID hacking underground" that exposed a serious weakness in some smartcard access cards. Using a device called "cloner", one hacker was able to "steal" the ID signal sent by an smartcard access card. This was done by having the "cloner" emit a signal to the smartcard, and capturing / recording the reply transmitted by the smartcard. The smartcard reacts to the signal like it was received from a regular reader, e.g. the ones connected to door locks that the whole security system is expected to protect. The recorded smart card signal is then used by the "cloner" when, in the vicinity of a locked door, it receives a reader signal asking it for its ID. The reader then "recognizes" the signal as one from a known smart card, and will unlock the door. Note: this hack was invited by the 'victim' who had some concerns about the safety of his building access control system.

For this scheme to be successful, the cloner device has to use a frequency that the smartcard will respond to. But since many commercial RFID chips use standard frequencies, this isn't very hard to do. Another prerequisite is that the hacker must be able to get the "cloner" device physically near a person who is known to have a smartcard – but obviously this can reasonably simply be done by just hanging around one of the doors that you want to open.

If the tag's chip has a writeable data area, the problem only gets worse.

From a technical point of view, the solution to this problem case is available – it's called encryption. By using an encryption scheme with session keys, an effective prevention of the "cloning" hack can be prevented. So why is encryption not used more often? The answer is economics, not technology – chips with encryption capabilities are more expensive than the ones that don't have this feature.

In another (also invited) hack, RFID tags used in a retail store and containing price information were read and changed prices were written back onto a number of tags. The device used was an ordinary PDA equipped with a PC card antenna and connected to a reader; a special software program called "RFDump" was used to review the tag data that was collected and to modify the price fields before writing them back to the relevant tags.

In a more elaborate version of this hack, it is possible to e.g. write "cookies" to smartcard tags and then use such cookies for tracking purposes, in much the same way that websites use cookies to identify returning site visitors.

In a few cases, even encrypted tags have been read and deciphered, because sometimes the encryption algorithms used by the chip manufacturers are untested – this happens mostly when 'homemade' ciphers are used. The algorithms that are in the public arena are all well-tested and commented on by

the encryption community, and their characteristics and strength are well established.

So what is the lesson here? Companies should make security a key feature on their checklist when embarking on the selection of any RFID system. And they should not take manufacturer or reseller sales pitches at face value, but get someone with adequate technical savvy involved in testing whether any proposed solution actually meets all of their security requirements. This testing includes running scenarios that are actually designed to lay bare any possible flaws. And yes, inviting a hack may be a very good way to find out about that.

RFIDsec product review/analysis

The Danish company RFIDsec recently announced their first commercial launch of a secure RFID system, aptly called "RFIDsec". The system consists of a tag containing a chip with encryption functionalities, and a protocol called "RFIDsec secure protocol" (RSP). The concepts behind this product were researched by Priway, founded by Stephan Engberg.

Recent online publications following the product launch have missed some crucial features of the product. So let's consider what are the key elements of this product, and how to evaluate them.

The RFIDsec product consists of three components:

1. an RFID chip that implements specific and essential security features
2. a specific protocol for secure communication without requiring trusted readers
3. a software platform for managing access to the chip and the data on it

The RFIDsec tag contains a chip that implements following functionalities:

- product identification, just like EPC – this is the basic concept of any RFID system. Actually, the RFIDsec chip is able to function in "normal" EPC Gen-1 mode, making it compatible for use in the supply chain next to other tag types that conform to the EPCglobal standard
- strong encryption – when in privacy or "stealth" mode, any information that is exchanged between the tag and the reader is encrypted using a 128 bit key and an algorithm that has been tested for robustness. Brute force won't work to crack the security mechanism; and passwords can be changed non-algorithmically for each session, even remotely.
- transfer of control – at the POS the customer can be given complete control of the tag's future behaviour by means of a key that the customer enters into the tag; using that key, the customer (owner of the tagged item) can control who can access data on the tag, create new data etc.
- multiple keys – the tag can hold multiple keys in order to support different types of behaviour in different security / trust domains. As an example: the manufacturer of a tagged product can have a key in order to get future access to certain data on the chip that enables him to identify the product as one that has genuinely be produced by him (e.g. in the case of warranty claims or product recall for defect repair); the retailer who sold the product could have a key in order to track products for purposes of a customer loyalty programme; and the consumer who bought the product can have a key in order to prove that he actually is the one who has legally purchased the product. However, the trust model is such that the consumer is given the final say in this – when he puts the tag in "privacy mode" all other keys can be

erased. That way, it is up to the customer to decide whether or not she or he wishes the item to be traceable for the retailer and the manufacturer. If the rewards are high enough (e.g. warranty or loyalty programme) then she might leave the tag in "normal" mode, but if he decides that the scales are not well balanced then the consumer can take full control of the tag by putting it into "privacy" mode. The consumer can also decide to disable access to information stored on the tag, or allow temporary access to be granted.

- removal of product ID – when the tag is put into "privacy mode" the product ID is deleted. This is an essential feature, because consumer acceptance will necessarily be based on trust, and there must be absolute assurance that there is no "back door". Using the 'access management platform' software (see below) the wary customer could be shown to his eyes what data still resides on the chip after it has been put into "privacy" mode by him, and can thus be convinced that the system is secure and trustworthy.
- anti-cloning – when the product serial number is absent then cloning is useless, as there is only a random and meaningless key to be read from the tag
- zero knowledge – when in privacy mode or "stealth mode", the RSP protocol for data exchange with readers does not leak any identifiers; there is a single step identification mechanism that the RSP protocol uses, which ensures that the tag does not start communicating until the reader has been authenticated as a trustworthy one. Therefore, an untrusted reader does not even sense the tag's presence, since it won't start sending any signals until after successful authentication. Adding to the anti-cloning feature discussed above, this means that "cloning" of the tag (see first chapter of this Newsletter) is also physically impossible.
- 1 Kb of memory that can be rewritten
- compatible with ISO-14443 (on physical operation of contactless smart cards), and hence:
- RF operation at 13.56 MHz

The RFIDsec Secure Protocol implements following features:

- compliant with EPC Gen-2 specifications operating in the standard protocol custom command space
- strong encryption – all communications can be encrypted, making "listening in" a useless activity
- one-step authentication – the tag can remain silent, and hence unnoticed, until the reader that emits the "wake up" signal has been authenticated
- support for advanced access management – making it possible to "partition" the chip memory and define different access rights for different parties for different parts of that memory. It is essential to mention here that a "master key" is part of this functionality, making it possible to transfer full access control of the tag and all data on it to the customer at the POS when a tagged item is bought by him.

The Access Management Software Platform implements following features:

- the platform has a defined API through which external applications can make use of the functions that are available in the management software
- the owner of the tag gets full control of it, and can grant access rights, effectively deciding who may have access to what part of the data on the chip.

Having described all the features and functionalities of the RFIDsec products in some detail, where does this all lead us? Let's consider the concepts underlying this product, and then evaluate what role the RFIDsec could play in the spread of RFID.

The fundamental requirements in designing and developing the product have been to provide trust and to provide control over the use of the tag. Furthermore, the idea of flexibility has been key. And finally, the idea has been to implement these concepts in such a way that it would be possible to explain the benefits to a non-technical audience. From the "psychology of public acceptance" perspective, the importance of this latter requirement can hardly be overstated.

So here is what the product is all about:

- transfer of control to the owner of the tag – when a consumer buys a tagged product, then full control of the tag can be transferred to her at the POS and from that point on it is up to him to decide who is granted access to (the data on) the chip
- multimodality; the tag can operate in various modes, suited to the needs of the environment of use in the relevant phase of the lifecycle of a tagged product. Therefore, the tag can provide security and control and trust in both B2B and B2C environments.
- robust security; through encryption, one-step authentication, and a specific protocol for communications with reader devices. The owner of the tag can rely on the security mechanism to protect the data on the chip against any unauthorised access or use.

As secondary features we could mention:

- controlled access through a specific software platform
- generic useability through compatibility with EPC Gen-1

In the B2B environment these are important, but in the average B2C situations these features won't be very conspicuous or interesting.

When we arrive at a final evaluation of the RFIDsec product, we know of no other commercially available product that really has the potential to solve the key issue of consumer trust in RFID. Ofcourse this solution must be proven in practice, and therefore we are very keen to hear about actual projects where RFIDsec has been implemented. What are the findings here? Does the product effectively hold up to its promises?

On a final note, we believe that RFIDsec holds a great promise for the future of RFID. Because of it's (as yet) unique capabilities, it is well positioned to gain a headstart. The marketing approach will probably determine any large-scale commercial success to a great deal. As stated above, getting a message across to the general public that has no technology bias at all, will be of paramount importance. Because RFIDsec chooses to work with a partner network for reselling and deploying, orchestrating the marketing message will be an important job determining the chances of success. Since the company comes from an R&D background, the greatest challenge might be in the area of psychology and communication. After all, it is superior marketing that wins the

market, not superior product quality... and we all know more than one example of that elementary truth.

Which brings us to the main advantage of RFIDsec: it was developed from a consumer requirement perspective, and therefore it can be communicated to the consumer from that perspective. Let's just hope that the sales and marketing people at RFIDsec keep this in mind all the time.

< note: updated from emailed version with feedback from RFIDsec >

Events

- The Institute of Validation Technology organises the event **RFID Technology within Healthcare and Pharmaceuticals** on August 22-24, 2006 at the Crowne Plaza - San Francisco, CA, USA. With two industry specific tracks, plus networking opportunities. You may register at www.ivthome.com/conferences, and download a brochure at www.ivthome.com/pdf/ivt0806_rfid.pdf.
- GDS International organises the **Extended Retail Solutions Symposium** on 7-8 September 2006 in the hotel Bayerischer Hof, Munich, Germany. RFID will be a hot topic to be addressed in this conference. You can visit the organisers' website at www.erseurope.com. Members as well as business partners of RFID Society are eligible to a 15% discount.
- World Trade Group organises the **2nd Annual Asia Pacific Supply Chain & Logistics Summit** on 11-13 September 2006 in the Pan Pacific Hotel, Singapore. This is the premier supply chain and logistics forum in Asia Pacific, hosting over 350 senior supply chain professionals. This three day event will discuss the supply chain and China, re-engineering your Asia Pacific supply chain, improving manufacturing agility and consumer focus, harnessing your biggest asset, maintaining the best talent and leadership, re-thinking risk, mastering the uncertainty inherent in the Asia Pacific supply chain and exploiting technology. Members of RFID Society are entitled to a 10% discount up until 31st August 2006; quote "RFSAP" on the delegate booking form. Visit www.scmapp.worldtradeco.com for more information.
- Simply Group Ltd organises the **Air & Port Security Expo Europe** on 13-14 September 2006 in Brussels. APS Europe covers passenger, cargo and terminal security. You may visit <http://www.aps-expo.com/> for more information. RFID Society members are eligible to a 20% discount on the entrance fee.
- IQPC is organising the **5th RFID, Barcoding and Emerging Technologies for Hospitals and Health Systems** event on 18-21 September 2006 in Hilton Philadelphia City Avenue, Philadelphia, PA, USA. Members of RFID Society are eligible to a 10% discount on the entrance fee. To obtain this please use code IUS_10333 when registering. Visit www.iqpc.com/cgi-bin/templates/singlecell.html?topic=233&event=10357 for more information.
- IDTechEx organises the **RFID Smart Labels Europe 2006 Conference** on 19-20 September in London, UK. This conference is concerned with how to make money out of RFID, particularly looking at the tags – how to make them and where to sell them. There is special focus on sectors where prices are not in free fall, yet adoption is rapid, like healthcare and the air industry. You may visit rfid.idtechex.com/smartlabelseurope06/en/exhibitors.asp for more information. RFID Society members are eligible to a 10% discount on the entrance fee, mention code 'SOC6' at registration.

- Advanced Learning Institute organises the **RFID for Government Conference** on 4-5 October in Washington, USA. For more information, visit www.aliconferences.com/conferences/rfidgovernment/1006.html. Members of RFID Society are eligible to a 15% discount on the entrance fee.
- Terrapinn organises the **SCMLogistics World 2006** on 16-19 October 2006 in the Suntec Exhibition & Convention Centre, Singapore. SCMLogistics World is an established Asian logistics & supply chain management conference and exhibition. There are visitors from High-Tech to Chemical, Auto, CPG, Retail, Oil and Gas and Pharmaceutical industry. SCMLogistics exhibition will be held in conjunction with Material Handling and Industrial Automation Asia. You may visit www.terrapinn.com/2006/scmlog for more information, or you may contact wendy.mah@terrapinn.com.
- IQPC organizes the **Pharma Secure Chain** conference on November 13 - 16, 2006 in Thistle Marble Arch, London, UK. Focus is on practical supply chain integrity and traceability measures to protect patients, products and IP against counterfeiting and diversion. Members of RFID Society are eligible to a special offer - use priority code RFISOC when registering to claim your complimentary masterclass worth 399 GBP. This offer is only open to RFID Society members and can only be claimed by entering this code. Simply follow the normal registration procedure online, selecting the conference package and masterclass you wish to attend then enter the code when prompted. When you preview your registration you will see 399 GBP has been deducted from the total registration fee. Visit <http://www.iqpc.co.uk/GB-2777/RFISOC> for more information.
- World Trade Group organises the **4th Annual North American Supply Chain & Logistics Summit** on 4-5 December 2006 in the Horseshoe Bay Resort Marriott Hotel, Austin, Texas, USA. This summit is the premier supply chain and logistics forum in North America. This two day event will discuss the key issues including: Driving the lean supply chain, fostering leadership in the supply chain, managing global supply chain security, supply chain outsourcing and benchmarking the latest RFID implementation strategies. Members of RFID Society are entitled to a 10% discount up until 24th November 2006. To register, please visit <http://www.scmna.worldtradeco.com> quoting RFSNA on the delegate booking form.
- Access Events organizes the **5th Global RFID ROI Summit** on January 29-30, 2007 in London (UK). Visit www.rfid-roi.com/ for more information.
- The Awareness Group in association with the Supply-Chain Council, AMR Research & CILT (UK) organizes the **Extended Supply Chain 2007 (ESC2007)** on March 26-27, 2007. The venue is Riverbank Park Plaza, London, UK. Topics focus on improving customer service, simultaneously driving productivity and eliminating waste. Visit <http://www.esc2007.com/> for more information.

As always we welcome your feedback and your comments.

Best regards,

Ralph Goossens
Frans Lambi
Founders, RFID Society