4. Open issues in RFID security

Lot of research efforts has been put on RFID security issues during recent years. A survey conducted by CapGemini showed that consumers see RFID more intrusive than several other privacy invading technologies like loyalty cards [30]. Similarly a research conducted for IPTS in 2006 saw that the citizens social acceptance and trust of RFID is quite low, which in turn was seen as an obstacle for widespread deployment of RFID tags [29].

In 2006 Rieback et al. saw that the main security issues that require feasible solutions are On-tag Cryptography, Key revocation, legislation and standardization [21]. Since then several cryptographic solutions have been developed and evaluated by the research community [Avoine web site]. Ayoade points out that most of the solutions are theoretical and have not actually been implemented. Unfortunately even those that have been implemented have not been tested and evaluated in the real world [23]. Therefore the feasibility of the researched solutions in different applications is questionable.

While the security and privacy risks are known by the industry, so far there has not been big enough incentive to implement security solutions to the RFID tag masses. It is unlikely that security features will be implemented in the tags on the market until these features will be added in the RFID standards. Before the standards for different application areas of RFID tags will be updated, the open legal questions have to be resolved (e.g. [24]). Once the legal debates materialise into laws related to the RFID, the secure solution have to follow.

The security and privacy problems directed towards RFID systems vary quite a lot depending on the type of tag used. Similarily the solutions differ as the capabilities of the tag change. Passive tags with very little space to implement cryptographic solutions cannot use the traditional security solutions and thus a special light-weight solutions like described in previous chapter have to be developed. The bigger and more powerful the tag is the more powerful security solutions can be implemented. On the other hand more capabilities bring up new challenges that has to be solved. On simple passive tag it is enough to consentrate on protecting the tags reading process. In contrast on more powerful multipurpose active tag, the security measures have to also consider the access control from reading to writing and erasing.

Next we will go through the existing problems on physical RFID tags, security primitives and protocols for tags, and the application specific issues in general.

4.1 Physical security of RFID tag.

The RFID tag can be attacked in several ways if the attacker has a physical access to the tag. The tags circuitry can be totally demolished with sharp object or connection to antennas can be severed as was suggested by Karjoth and Moskowitz as a privacy protecting measure [20]. Tags can also be killed with electromagnetic pulse that can be created with simple items as was demonstrated in chaos communication congress. As EMP pulse does not leave any physical sign on the tag, it is not possible to visually notice if the tag is killed. The users of tagged items would prefer a method where they can easily see whether the tag is active or not. With the help of blocker tag the reading of tags can be blocked while the tag itself stays intact [22] allowing more flexibility on tag use. On some applications, possibility to kill or prevent tag reading is unacceptable and methods to protect the tag against them is required.

Tags can also be physically separated from the tagged item. A separated tag can then later on attached to a new item and thus break the identification system. It is not always possible to embed the RFID tag into the tagged item so that it cannot be physically removed. For some application areas it is important that the tags can be removed. It might be equally important that it can be seen from the tagged item, that it no longer contain valid tag. Also methods for preventing the removal of tag intact should be developed.

A physical access to the tag opens up the possibility for side channel attacks such as timing and power analysis attacks. Oren and Shamir have even developed a power analysis attack where no physical contact is required. The attack is even possible to conduct without attacker and tag transmitting any data, making it very hard to detect [33]. Solutions against these type of side channel attacks are required.

4.2 Cryptographic primitives and protocols

Lot of research have been concentrating on developing secure protocols that protect the tag against unauthorised read. Many of the suggested protocols rely on hash functions as lightweight solution. Feldhofer and Rechberger pointed out though, that existing hash functions are not feasible for protecting the simple passive tags. This is due to the requirement for storing inner vectors which requires thousands of logical gates [5]. Symmetric cipher like DESL can be used to create a hash values in many cases. Still a full-fledged hash function that can be implemented in RFID tag would be prefered due to faster performance.

Another assumption made by protocol developers is existence of real random numbers. The research in real number generation on the other hand has not been very active. The researchers from auto-ID labs just published their solution [28]. Since the solution has just been published, it remains open whether other researchers will find security flaws on it.

Since the lightweight security solutions have been concentrating mainly on protecting the tags identity, other possible uses for simple tags like creating digital signatures remain open. So far asymmetric cryptography seems to be out of the scope of simple passive tags.

In order to compare the feasibility of different developed primitives and protocols for variety of situations there is a need for clear evaluation criteria. How does the solution affect to the speed of reading process? Does complicating the communication affect on the reliability of identification? Is the solution feasible for reading multiple tags at same time? How many gates is required to implement the solution in tag and is additional power needed for solution? Clearly set criteria helps not only researchers to compare their solutions but also manufacturers to select fitting solution for their application area.

4.3 Back end and Application specific issues

The back end of the RFID system includes the transmission of the information from RFID reader to a database as well as the use of this database. The back end protection does not suffer from the limitations of RFID tags and thus traditional security measures for protecting the communication and databases can be used. It is good to realise though that a possibility to read a single tag is rarely a real threat towards privacy while access to a huge database containing the data of several reads of RFID tags often is. Thus protecting the back end system has to be designed carefully.

Tag reader in particular is interesting target. Attacker may try to force malware inside the reader that would leak the read data to intruder. In system relying shared secret, attacking the reader may compromise them. Temporary memory and possible temporary files inside the reader can be very attractive target for malicious person.

Combining tags with other data in database opens up new problems. In a breadcrumb threat a user is associated in the RFID tag in an item at the database [26]. When user gives the item away, the association is not necessarily changed in the database. Thus later on the user maybe associated wrongly to a location where the RFID enabled item has been seen.

As the basic cryptographic primitives suitable for the RFID environment have been developed, the focus is moving towards application specific research. Different applications have different requirements and different security threats. For example, Tags that are used for passport require much higher tamper resistant than those that are used for keeping up the product logistic.

As new areas for RFID tag use are invented, new requirements will arise. Solutions for problems like ownership transfer is required [34]. The application areas affect also on the feasibility of different solutions. Unauthorised read of passport can be prevented by selecting proper material on the passport cover that will block the read attempts. Thus only passports that are opened can be read. Of course this type of aproach is not suitable for protecting milk bottles, which require their own solution. Similarily, when the tags are used within medium organisation, solutions relying on shared secret are feasible. Tags that has to be readable by several organisation should not rely on shared secrets due the risen risk of compromising the secret.

Several threats towards privacy can be identified when RFID tags are used, all of them are not real threats in all application areas. Rao et al. have developed simple model that can be used for analysing the extent of threat by given case [27]. This threat assessment model although superficial, can be used as a basis for further research to develop better threat analysis methods in different environments.

Garfinkel et el. see that customers should know about the RFID tags in products and how these tags work. They suggest defining public policies for the RFID tag behavior in different cases [26]. Such policies would give the customers information that they can use to evaluate the risk given tag will provide against their privacy. Ayoda suggests that RFID readers could make sound when reading a tag in similar manner than digital cameras make sound when picture is taken [23]. Thus customers would know when the tag is read and could ease the acceptability of technology.

4.4 The future of RFID security

Since the basic cryptographic primitives and security protocols have been developed it is time to get them implemented and tested in real life. Real life testing will show if it is possible to use challenge-response authentication to tens of tags at the same time and how much burden a non-deterministic authentication will put on the RFID reader.

As the basic security primitives and protocols are getting lightweight enough the emphasis on security development will move towards application specific issues. The more complicated tags will likely open up new types security threats that in turn that need new solutions. The possibility to write into tag has opened up a possibility to insert malware inside the tag that can affect the tag reader [31].

The research results will also bring up new ideas of protecting security and privacy that will further open up the field of RFID security research. For example Rifkin and Roy suggested that the tag would provide more information to the readers that are closer to it, than those who are farther away. [32] The feasibility of the concept and how it would survive from different kind of specialised devices that attackers could create is open.

Finally it is important to solve the legal issues surrounding the RFID tags. With tags it is easy to generate huge databases about information of people and their behaviour. Clear rules are needed who is allowed to create such databases, and how the people affected about this will be properly informed. Responsibility issues should also be clarified. For example, what would be the legal implications if the store does not kill RFID tag in item after the customer has purchased it? [35] If the killing fails, is the intrusion to customer privacy in responsibility of tag manufacturer or the store? Finding out the legal problems will likely bring up new research opportunities for engineers to develop new solutions that enable secure and feasible use of RFID tags in the future.

[20] Karjoth G., Moskowitz P., Disabling RFID tags with visible confirmation: clipped tags are silenced, WPES '05: Proceedings of the 2005 ACM workshop on Privacy in the electronic society, pp. 27-30, Alexandria, VA, USA, 2005, isbn 1-59593-228-3

[21] Rieback M., Crispo B., Tanenbaum A., The Evolution of RFID Security, IEEE Pervasive computing, Volume: 5, Issue: 1 pp. 62-69, IEEE, January-March 2006

[22] A. Juels, R. L. Rivest and M. Szydlo, The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, 2003

[23] J. Ayoade, Roadmap to solving security and privacy concerns in RFID systems, Computer Law & Security Report, Volume: 23, Issue: 6, pp. 555-561, Elsevier,2007

[24] D. Flint, RFID tags, security and the individual, Computer Law & Security Report, Volume: 22, Issue: 2, pp. 165-168, Elsevier,2006

[26] S.L. Garfinkel, A. Juels, R. Pappu, RFID privacy: an overview of problems and proposed solutions, IEEE Security & Privacy Magazine, Volume: 3, Issue: 3, pp.: 34-43, IEEE, May-June 2005

[27] S. Rao, N. Thantry, R. Pendse, RFID Security Threats to Consumers: Hype vs. Reality, The 41st Annual IEEE International Carnahan Conference on Security Technology, pp. 59-63, October 8-11, 2007, Ottawa, Ontario, Canada

[28] W. Che, H. Deng, X. Tan, and J. Wang, A Random Number Generator for Application in RFID Tags, Networked RFID Systems and Lightweight Cryptography, pp. 279-288, Springer, 2008

[29] M. van Lieshout L. Grossi, G. Spinelli, S. Helmus, L. Kool, L. Pennings, R. Stap, T. Veugen, B. van der Waaij, C. Borean, RFID Technologies: Emerging issues, Challenges and Policy Options, IPTS, Sevilla, 2006, Available at: http://ftp.jrc.es/eur22770en.pdf

[30] RFID and Consumers - What European consumers think about radio frequency identifications and implications for businesses. Capgemini report, 2005 Available at: http://www.capgemini.com/news/2005/Capgemini_European_RFID_report.pdf

[31] M. R. Rieback, P.N.D. Simpson, B. Crispo and A. S. Tanenbaum, RFID malware: Design principles and examples, Pervasive and Mobile Computing, Volume 2, Issue 4, pp. 405-426, November 2006, Elsevier

[32] K.P. Fishkin and S. Roy. Enhancing RFID privacy via antenna energy analysis. Technical Report Technical Memo IRS-TR-03-012, Intel Research Seattle, 2003.

[33] Y. Oren, A. Shamir, Remote Password Extraction from RFID Tags, IEEE Transactions on Computers, Volume: 56, Issue: 9, pp. 1292-1296, IEEE, September 2007

[34] K. Osaka, T. Takagi, K. Yamazaki, O.Takahashi, An efficient and Secure RFID Security method with Ownership Transfer, International Conference on Computational Intelligence and Security, pp. 1090-1095, IEEE, 2006

[35] E. P. Kelly, G. S. Erickson, RFID tags: commercial applications v. privacy rights, Industrial Management & Data Systems, Volume 105, Issue 6, pp. 703 – 713, 2005, Emerald Group Publishing Limited