A Comparative Literature Review on RFID Security and Privacy

Bernhard Riedl [1)], *Gernot Goluch* [2)], *Stefan Pöchlinger* [3)], *Edgar Weippl* [4)]

Abstract:
RFID provides the basis for the development of ubiquitous computing. This ever present computing environment creates new exploitable channels for adversaries. Therefore, numerous publications on RFID security appear every year, adding to the topic's diversity. Nevertheless, there are only few state-of-the-art overviews that clarify common opinions on the topic. Hence, we examined the existing literature and present our observations on privacy and security in RFID.

1 Introduction

Radio Frequency Identification (RFID) is a technology for wireless information exchange over short distances. Even though the technology itself was invented about 50 years ago, recent development in the field of low cost RFID devices began to finally show its potential [16]. The possibility of adding (minimal) computing capabilities to everyday's objects will support the development of ubiquitous computing in the near future [34]. Applying RFID transponders to consumer goods will be common [35], creating an ever present computing environment spanning all parts of everyday's life. Today RFID commerce already constitutes a vital and ever expanding market. Judging by evidence from recent years, RFID industry will continue its rapid growth during the following years [17, 35]. In such a developing market security and privacy become increasingly important.

An appropriate definition for security is given by Avizienis et al. [2]. They define security as a composite of the attributes confidentiality, integrity and availability (also called CIA). In this context, confidentiality means the absence of unauthorized information disclosure. Integrity describes the absence of improper (meaning unauthorized) system and underlying data alteration. Availability in the security context is defined as continued readiness for

[1)]Secure Business Austria, Vienna, Austria, riedl@securityresearch.ac.at
[2)]Secure Business Austria, Vienna, Austria, goluch@securityresearch.ac.at
[3)]Secure Business Austria, Vienna, Austria, poechlinger@securityresearch.ac.at
[4)]Information & Software Engineering Group, Vienna University of Technology, Austria, weippl@ifs.tuwien.ac.at

authorized actions. Hence, a system with appropriate security should maximize the balance of the three attributes' concurrent existence. Moreover, privacy is defined as a subset of confidentiality and integrity. In other words, consumers have the right to be sure that their data is not disclosed.

2 Related work

As we stated in the introduction, it is becoming increasingly difficult to ignore the importance of security and privacy aspects in research and industrial appliance of RFID [16, 34]. Nevertheless, to the best of our knowledge, there are surprisingly few literature review on RFID in a security and privacy context. Juels' survey [19] gives a good introduction and overview on some of the central topics in RFID security. Lehtonen et al. [25] limit the scope of their examination to product authentication and a discussion of the trade-off between complexity and security in different RFID authentication methods.

Moreover, there are publications on state-of-the art in RFID privacy preservation [14], as well as numerous reviews on security and privacy concerning health care, e-commerce and data mining. The latter two are especially interesting, as essential privacy questions in these fields, like "What data is collected?" and "How is data secured during transmission?" apply to RFID as well. The central factor underlying these topics in e-commerce is trust [2, 10], a topic that can easily be anticipated in an RFID context. When RFID tagged objects hit the end-user market at a large scale, consumers' willingness to provide data will likely depend on individual perceptions of trustworthiness, just as it does in e-commerce. Such perceptions will be directly based on the security and privacy provided.

3 Methodology

For our survey, we acquired publications via different search engines and libraries, i.e. ACM Portal, IEEE Xplore, SpringerLink or Goggle's scholar search. At this point, we utilized abstract reading to assess paper qualities and ensure that they cover appropriate topics for our literature review. During this selection process publications from respected scientific sources like ACM, IEEE or SpringerLink received implicit trust. When checking the bibliography of our acquired literature, we found out that many of them referenced Avoine's online bibliography [6] as an accurate source of overview. Hence, we visited this website and realized that almost all our previously selected articles where referenced there. Additionally, due to its narrow topic, this source is perfect for retrieving papers with unconventional titles that could otherwise be missed using typical terms in search engines. Therefore, we added Avoine's bibliography to our list of sources.

Apart from papers on state-of-the-art security for RFID tags, we included papers on the use

of RFID systems as security tokens in our review. Obviously, an exploitable security leak in an RFID system intended to provide security itself, would automatically compromise the security of the protected assets. Such applications of RFID will therefore require especially strong security.

4 Observations

"The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it" [37]. This quote from Mark Weiser, who was the first to use the term "ubiquitous computing", illustrates the potential of RFID tags. But, as long as consumers have serious privacy concerns against RFID [35], we do not expect the technology to become truly "invisible" in the sense of the quotation above. Therefore, we present the observations we made during our literature review of RFID security and privacy, as we are convinced that strong security can solve many of these pressing concerns. An overview on our observations is given in Table 1.

Table 1: Observations on RFID security

Observation 1	RFID security is a complex topic comprised of several severe, interconnected problems.
Observation 2	There is no commonly accepted holistic security model.
Observation 3	Papers on new protocols and publications on weaknesses in them appear increasingly fast.
Observation 4	Perceptions on RFID differ widely regarding various involved groups.
Observation 5	Available trusted and proven cryptographic solutions are not applicable to the current generation of low cost tags.
Observation 6	There are few major development streams in the RFID security and privacy complex that drive the technology forward.

4.1 Observation 1

Much of RFID's characteristic complexity comes from its composed nature, implying several interconnected problems. We found an adequate example for this fact in Avoine's and Oechslin's [4] findings on tracking as a multilayer problem. Tracking or tracing is an RFID significant security threat. It means that adversaries can identify tags they read before (e.g. by a static identifier). This represents a serious violation of confidentiality as well as privacy.

According to Thornton et al. tracking is also the threat that customers are most aware and afraid of [35]. As a well known problem, it has received a lot of attention by the scientific

community and numerous proposals on enhanced privacy protection [20, 32, 1] have been presented to mitigate it. One of them was the previously mentioned publication by Avoine and Oechslin on tracking's multilayered nature [4]. They describe three layers of RFID communication, and show that, unlike in networking, the whole system is automatically compromised if privacy protection fails on only one of these layers.

Moreover, we can see other sources for the topic's complexity, for example in the broad range of possible attacks. As with many new technologies, RFID has its own specific vulnerabilities [23], but the obvious resource limitations of (cheap) RFID tags seemed to implicitly hinder more complex malware to be applied. This view was disproved by Rieback et al. who showed that complex exploit based malware, in this case a virus, is possible despite this limitations [31]. Therefore, we see that RFID implementers should not limit their views on core RFID topics, but be aware of all vulnerabilities discovered in information and communications technologies.

4.2 Observation 2

Another closely related observation we made is that no commonly accepted holistic security model was described so far. This makes testing and comparing new protocols and applications a complex task. Until an agreed standard model arises, we believe that security claims on mathematically proven protocols should be treated with care, as models and their related algorithms are defined by the same persons. There are however, some formalized RFID security models by Avoine [5], Juels and Weis [22] as well as Van Le et al. [24].

We observe several facts that all of the reviewed security models have in common. First they are all limited to the protocol level and do not cover operations on lower layers. Van Le et al. present a formalization of ideal wireless communication which can serve as a starting point for further examination of lower layers. However, while these models still do not cover all relevant aspects in RFID, they do already uncover weaknesses in some protocols. Avoine, as well as Juels and Weis, use their models to examine existing protocols and show that most of them do not provide formal security under them. Juels and Weis highlight that many systems do only provide security under their practically unrealistic closed system assumption [22]. Contrary, Van Le et al. find their tested protocols secure, but have tested their own self developed protocols [24]. As Gilbert et al. highlighted, a too restrictive model can make protocols look secure that are nevertheless vulnerable to realistic attacks [15]. Therefore, the lack of a standard security model for RFID shifts attention and resources from protocol comparisons to model assessments. As none of the presented models covers all aspects of RFID, we think that they will not arise as a standard to test new protocols, but they can provide valuable input for the future development of such a model. We believe that further efforts in this research direction can yield valuable results and benefit the improvement of RFID security as such.

4.3 Observation 3

In [4], Avoine and Oechslin argued that only little work has been done on new computationally simple RFID protocols. In fact they cite only six publications on new protocols and stress that there were only two publications that exhibit weaknesses in existing protocols [3, 33]. Since this claim, an increasing number of publications appeared addressing this issue. For example, Li and Deng [26] present an attack against the recently proposed "EMAP: An Efficient Mutual Authentication Protocol" [30] and Gilbert et al. [15] present an active attack against the so-called "HB$^+$" [21]. As we've pointed out, they claim that the security model used for the mathematical proof of a protocol was too restrictive and the protocol is therefore vulnerable to practical attacks. For this reason, security proofs in RFID environments must be treated carefully. Defend, Fu and Juels [11] present attacks on two protocols by Vajda and Buttyán [36] which require only limited resources while breaking the scheme completely by uncovering the session keys. Li and Wang [27] show two attacks against the recently proposed LMAP [28] and M^{2}AP [29] protocols, which completely corrupt the concerned tags.

From this evidence, we are convinced that the lack of attention on protocol weaknesses Avoine and Oechslin experienced [4] does no longer exist. Furthermore, our review includes four publications on weaknesses, which is two times as much as Avoine and Oechslin encountered. For example, from fourteen sources added to Avoine's bibliography [6] in 2007, eight dealt with new protocols and four exposed weaknesses in existing protocols. This is additionally emphasized by the fact that three of our four above examples on weaknesses were published within less than one year. Therefore, we believe that RFID development has entered a new era where new protocols appear at a fast rate and are disproved (or sometimes improved) quite as fast.

4.4 Observation 4

We see an important aspect of the emerging RFID trust topic in the ongoing debate on further governmental or voluntary vendor regulations. To clarify the different points of involved parties, namely customers, vendors, researchers and governments, we used the efforts by the European Union's Article 29 Data Protection Working Party. This advisory body published results of a public consultation on RFID privacy [12]. In it, they state that they got results from eight private individuals, nine universities and think tanks, sixteen corporations or trade organizations, and one consumer association. Corporation in this context refers to both RFID vendors and retailers. One point of the results we find noteworthy is that most corporations see self-regulation as the adequate tool to complement the current European data protection directive in RFID related privacy issues, whereas most of the other parties suggest a need for additional guidance like RFID specific rules in the directive. The only exception from this pattern are companies providing security solutions themselves, as they do not view self-

regulation as an appropriate measure. Nevertheless, the situation is not as clear as it appears in this example.

We want to emphasize this fact by giving another example on a remarkable difference in RFID perceptions between researchers and the industry. In 2002, Garfinkel called for what he calls an "RFID Bill of Rights"[1)]. He advises that, as misuse of this new technology could easily be foreseen, the industry should voluntarily grant consumers a number of privacy rights. The EPCglobal Inc., the organization advocating the spread of the EPCglobal network, adapted very similar guidelines[2)]. The difference between the two rule sets can be seen in Table 2. Two years after proposing his "Bill of Rights", Garfinkel called the EPCglobal version of his proposals "significantly watered down"[3)]. For example, instead of guaranteeing users the right to have tags deactivated, EPCglobal Inc. simply advises that customers should be informed about the choices they have for future removal or deactivation of the tag. As Garfinkel points out, we see that the wording shows how thin these rights really are. What is remarkable about this example is that Garfinkel also opposes regulation. He points out that voluntary self regulation is useful to allay consumer concerns, but not in the way it has been done by the EPCglobal Inc.. Such minimal rights might result in a public outcry and therefore lead to even stricter mandatory regulation, which would delay RFID's further deployment.

Table 2: RFID Bill of Rights vs. EPCglobal Guidelines

RFID Bill of Rights Consumers should have...	**EPCglobal**
The right to know whether products contain RFID tags.	Tagged products should be marked with an EPC sticker.
The right to have RFID tags removed or deactivated when they purchase products.	Consumers will be informed of the choices that are available to discard or remove the tag.
The right to use RFID-enabled services without RFID tags.	Consumers shall be informed of the advantages RFID offers.
The right to know when, where and why the tags are being read.	Companies should publish policies addressing the use of collected data.
The right to access an RFID tag's stored data.	

[1)] see http://www.technologyreview.com/Infotech/12953/

[2)] see http://www.epcglobalinc.org/public/ppsc_guide/

[3)] see http://www.technologyreview.com/Infotech/13902/

4.5 Observation 5

Conventional cryptography, which is common on platforms where resources (processing capacity, memory) are less scarce, is not applicable to the current generation of low cost tags. When reviewing RFID security related literature, we found that this point was quite common among involved researchers. For instance, Juels [18] projects that upcoming five cent tags will only perform simple computational operations, excluding conventional cryptography. In his view, the best security provided will likely be PIN controlled data access. Moreover, Sarma et al. explicitly call strong symmetric key encryption "a challenge in short term" [34]. Until advancements are made, implementations of conventional cryptography on RFID tags like the AES implementation by Feldhofer et al. [13] require more then the computational resources available on EPC tags [7].

From this sample, we conclude that this view is common among the scientific community, and nevertheless can't be overstated in its importance for RFID development. We fear that a lack of security in newly created RFID applications will cause further consumer concerns and might seriously delay RFID's further development. There is also some practical evidence against this. Some of the already deployed RFID applications find widespread acceptance despite their proven lack of security [35]. Nevertheless, in our view this observation provides a good explanation for some driving issues in RFID and therefore, we will start our examination of the current main development streams in RFID research from this point.

4.6 Observation 6

As we've seen, current RFID tags cannot execute conventional cryptography. Therefore, one of the most important aspects in RFID research is the development of new, less computationally complex security algorithms that are feasible for cost critical tags, like the EPCs. An important value in that context is the notion of "minimalist cryptography", formulated by Juels [18]. We see one of his major contributions in the demonstration that standard cryptography is not a necessary prerequisite for providing security. Since then, numerous proposals on computationally simple authentication protocols and privacy protection mechanisms have been published (see Observation 3). All these protocol suggestions and all exposed weaknesses mentioned before [30, 36, 28, 29], can be seen as work in this area as well. Therefore, at the time being, this race for computationally simpler protocols covers the biggest quantity of RFID security publications.

As RFID tags can be expected to provide more resources in the future, implementations of standard and complex security algorithms still present valuable findings for further research. Moreover, not all applications of RFID are equally cost critical. Tags containing mandatory sensitive information are usually deployed in far smaller numbers than EPCs. Therefore, costly

stronger tags might be economically justifiable for such applications. As typical advancements in this research direction, we see efforts to adapt standard cryptography to RFID limitations, like Feldhofer et al.'s previously mentioned AES implementation [13]. Furthermore, there are some initial efforts to make public key cryptography (PKC) available on RFID systems, as well that might lead to feasible RFID PKC features in the future. This is indicated by the various publications on elliptic curve cryptography (ECC), which appeared recently. For example, Batina et al. present an elliptic curve generator for RFID tags in [8] and adaptations of RFID protocols for elliptic curve cryptography in [9]. At the time being, protocols and suggestions for ECC implementations on RFID systems exist [9], but to the best of our knowledge no experimental implementations. Therefore, these advancements have yet to prove their practical feasibility.

Undoubtedly, there are some publications which fall into neither of these categories. These deal with topics like non protocol specific attacks [23], malware [31] or integration of different solutions [32]. We believe that the last topic will grow in importance when the current solutions for security issues are incorporated into the next generation of RFID tags.

5 Conclusion

In this paper, we examined the sources for RFID's complexity, described the need for a wholistic security model and emphasized the increasing dynamics in RFID research. Furthermore, we highlighted the different perceptions by RFID users, researchers and vendors and showed the current development streams in RFID research starting from the commonly accepted fact that the current generation of RFID tags cannot execute conventional cryptograpy.

We have seen that there are some important issues that keep RFID from fulfilling Weiser's quotation on ubiquitous technologies at the moment. Nevertheless, RFID researchers have already presented numerous solutions to some of the most pressing concerns. It will be fascinating to see which of these proposals (and when) are incorporated into the next generations of industrial RFID systems. Finally, we see that RFID's individual advantages adhere perfect to the idea of ubiquitous computing and look out for further development of this complex topic.

References

[1] G. Ateniese, J. Camenisch, and B. de Medeiros. Untraceable rfid tags via insubvertible encryption. In *CCS '05: Proceedings of the 12th ACM conference on Computer and communications security*, pages 92–101, New York, NY, USA, 2005. ACM Press.

[2] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. *Dependable and Secure Computing, IEEE Transactions on, Vol.1, Iss.1*, pages 11–33, 2004.

[3] G. Avoine. Privacy issues in RFID banknote protection schemes. In *International Conference on Smart Card Research and Advanced Applications – CARDIS*, pages 33–48, Toulouse, France, August 2004. IFIP, Kluwer Academic Publishers.

[4] G. Avoine and P. Oechslin. RFID traceability: A multilayer problem. In *Financial Cryptography – FC'05*, volume 3570 of *LNCS*, pages 125–140, Roseau, The Commonwealth Of Dominica, February–March 2005. IFCA, Springer-Verlag.

[5] Gildas Avoine. Adversary model for radio frequency identification. Technical Report LASEC-REPORT-2005-001, Swiss Federal Institute of Technology (EPFL), Security and Cryptography Laboratory (LASEC), Lausanne, Switzerland, September 2005.

[6] Gildas Avoine. Bibliography on security and privacy in RFID systems. Available Online at http://lasecwww.epfl.ch/~gavoine/rfid/, 2007.

[7] D. Bailey and A. Juels. Shoehorning security into the EPC standard. In *International Conference on Security in Communication Networks – SCN 2006*, volume 4116 of *LNCS*, pages 303–320, Maiori, Italy, September 2006. Springer-Verlag.

[8] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede. An elliptic curve processor suitable for RFID-tags. Cryptology ePrint Archive, Report 2006/227, 2006.

[9] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede. Public-key cryptography for RFID-tags. In *International Workshop on Pervasive Computing and Communication Security – PerSec 2007*, pages 217–222, New York, USA, March 2007. IEEE Computer Society Press.

[10] F. Belanger, J. S. Hiller, and W. J. Smith. Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *Journal of Strategic Information Systems, Vol. 11*, pages 245–270, 2002.

[11] B. Defend, K. Fu, and A. Juels. Cryptanalysis of two lightweight RFID authentication schemes. In *International Workshop on Pervasive Computing and Communication Security – PerSec 2007*, pages 211–216, New York, USA, March 2007. IEEE Computer Society Press.

[12] European Union ARTICLE 29 Data Protection Working Party. Results of the public consultation on article 29 working document 105 on data protection issues related to RFID technology. *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp111_en.pdf*, 2005.

[13] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. Strong authentication for RFID systems using the AES algorithm. In *Workshop on Cryptographic Hardware and Embedded Systems – CHES 2004*, 2004.

[14] Simson L. Garfinkel, Ari Juels, and Ravi Pappu. Rfid privacy: An overview of problems and proposed solutions. *IEEE Security and Privacy, Volume 3, Number 3*, pages 34–43, 2005.

[15] H. Gilbert, M. Robshaw, and H. Sibert. An active attack against HB^+ – a provably secure lightweight authentication protocol. Manuscript, July 2005.

[16] EPCglobal Inc. Epc radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 mhz 960 mhz version 1.0.9, 2005.

[17] Sixto Ortiz Jr. How secure is RFID? *Computer, Volume 39, Number 7*, pages 17–19, 2006.

[18] Ari Juels. Minimalist cryptography for low-cost RFID tags. In *International Conference on Security in Communication Networks – SCN 2004*, volume 3352 of *LNCS*, pages 149–164, Amalfi, Italia, September 2004. Springer-Verlag.

[19] Ari Juels. RFID security and privacy: A research survey. Manuscript, September 2005.

[20] Ari Juels, Ronald L. Rivest, and Michael Szydlo. The blocker tag: selective blocking of rfid tags for consumer privacy. In *CCS '03: Proceedings of the 10th ACM conference on Computer and communications security*, pages 103–111, New York, NY, USA, 2003. ACM Press.

[21] Ari Juels and Stephen Weis. Authenticating pervasive devices with human protocols. In *Advances in Cryptology – CRYPTO'05*, volume 3126 of *LNCS*, pages 293–308, Santa Barbara, California, USA, August 2005. IACR, Springer-Verlag.

[22] Ari Juels and Stephen Weis. Defining strong privacy for RFID. Cryptology ePrint Archive, Report 2006/137, 2006.

[23] Z. Kfir and A. Wool. Picking virtual pockets using relay attacks on contactless smartcard. In *SECURECOMM '05: Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, pages 47–58, Washington, DC, USA, 2005. IEEE Computer Society.

[24] Tri van Le, Mike Burmester, and Breno de Medeiros. Forward-secure RFID authentication and key exchange. Cryptology ePrint Archive, Report 2007/051, 2007.

[25] M. Lehtonen, T. Staake, F. Michahelles, and E. Fleisch. From identification to authentication - a review of RFID product authentication techniques. Printed handout of Workshop on RFID Security – RFIDSec 06, July 2006.

[26] T. Li and R. Deng. Vulnerability analysis of EMAP - an efficient RFID mutual authentication protocol. In *Second International Conference on Availability, Reliability and Security – AReS 2007*, Vienna, Austria, April 2007.

[27] Tieyan Li and Guilin Wang. Security analysis of two ultra-lightweight RFID authentication protocols. In *IFIP SEC 2007*, Sandton, Gauteng, South Africa, May 2007. IFIP.

[28] P. Peris-Lopez, J. C. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda. LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags. Printed handout of Workshop on RFID Security – RFIDSec 06, July 2006.

[29] P. Peris-Lopez, J. C. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda. M2AP: A minimalist mutual-authentication protocol for low-cost RFID tags. In *International Conference on Ubiquitous Intelligence and Computing*, volume 4159 of *LNCS*, pages 912–923. Springer-Verlag, September 2006.

[30] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda. EMAP: An efficient mutual authentication protocol for low-cost RFID tags. In *OTM Federated Conferences and Workshop: IS Workshop – IS'06*, volume 4277 of *LNCS*, pages 352–361. Springer-Verlag, November 2006.

[31] M. Rieback, B. Crispo, and A. S. Tanenbaum. Is your cat infected with a computer virus? In *PERCOM '06: Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications*, pages 169–179, Washington, DC, USA, 2006. IEEE Computer Society.

[32] M. Rieback, G. Gaydadjiev, B. Crispo, R. Hofman, and A. Tanenbaum. A platform for rfid security and privacy administration. In *Proc. USENIX/SAGE Large Installation System Administration conference*, pages 89–102, Washington DC, USA, December 2006.

[33] J. Saito, J.-Ch. Ryou, and K. Sakurai. Enhancing privacy of universal re-encryption scheme for RFID tags. In *Embedded and Ubiquitous Computing – EUC 2004*, volume 3207 of *LNCS*, pages 879–890, Aizu-Wakamatsu City, Japan, August 2004. Springer-Verlag.

[34] S. Sarma, S. Weis, and D. Engels. RFID systems and security and privacy implications. In *Cryptographic Hardware and Embedded Systems – CHES 2002*, volume 2523 of *Lecture Notes in Computer Science (LNCS)*, pages 454–469, Redwood Shores, CA, USA, August 2002.

[35] F. Thornton, B. Haines, A. M. Das, H. Bhargava, and A. Campbell. *RFID Security*. Syngress Publishing, Inc., Rockland, MA, USA, 2006.

[36] I. Vajda and L. Buttyán. Lightweight authentication protocols for low-cost RFID tags. In *Second Workshop on Security in Ubiquitous Computing – Ubicomp 2003*, Seattle, WA, USA, October 2003.

[37] Marc Weiser. The computer for the 21st century. *Scientific American Volume 265, Number 3*, pages 94–104, 1991.