New Directions in RFID Security

Erik-Oliver Blass and Refik Molva

EURECOM, Sophia Antipolis, France

Abstract. Current research in RFID security focuses on basic authentication protocols between a tag and a reader. In this paper, we claim that, in future, different new RFID-based scenarios will play an increasing role. In particular, we propose two new research directions: 1. *Multi-Tag Security*, and 2. *RFID-based Payment*. In multi-tag security, multiple tags try to jointly compute an information while using the reader either as the focal point of all communication or as a relay for tag-to-tag communication. In this scenario, the security of the computation has to be guaranteed while also privacy of individual tags must be protected. In a payment scenario, tags are used as electronic wallets similar to the notions of traditional electronic cash. Payment must be secured against malicious spending, and the privacy of tags and their payments must be protected.

1 Introduction

In Radio Frequency Identification (RFID), tags reply to the electronic prompts of a reader and are typically used for the purpose of wireless identification of objects or individuals. With advances in technology and the design of new applications, RFID tags are becoming part of our everyday life. The deployment of RFID systems unfortunately comes with a high cost due to new security exposures caused by their pervasiveness. There are many security issues associated with the use of such systems ranging from cloning to impersonation of tags through privacy violations. Clearly, industry and customers will only accept this technology if these security and privacy issues are tackled appropriately. Thus, the design of secure and privacy-preserving authentication and identification protocols for RFID systems has recently been a very attractive field for security research. The scarcity of computational resources in tags and stringent response time requirements has given researchers the opportunity to revisit traditional topics such as authentication protocols and probabilistic algorithms together with privacy as an additional motivation raised by RFID applications. Security research has abounded with lightweight authentication and identification schemes, formal security and privacy models, and analysis of RFID protocols and further refinements in forward secrecy and synchronization, cf., Avoine et al. [2], Dimitrou

This work has been supported by the RFIDAP project, grant reference ANR-07-SESU-009, funded by Agence Nationale de La Recherche as part of the SESUR 2007 call.

[8], Juels and Weis [10], Pietro and Molva [12], Tsudik [15], Vaudenay [17], Weis et al. [18], and many more. The basic tag-reader identification protocol thus hardly offers any security or privacy problem that has not already been tackled by a number of researchers.

In this paper, we suggest new directions for security research that have not been addressed yet in the context of RFID systems. First, we suggest to extend the current RFID security protocol scenario involving a tag and a reader by considering the joint relationship between several tags interacting with one or several readers. In the extended scenario involving multiple tags, we consider different cases regarding the role of the reader with respect to the overall operation. The second research direction tackles the idea of achieving functions more advanced than basic identification and authentication and discusses the security and privacy requirements raised by the micropayment problem in the context of RFID systems.

2 Multi-Tag Security and Privacy

Unlike the basic tag-reader identification protocol, new scenarios involving more than one tag and one or several readers are quite promising from the point of view of applications as well as security and privacy protocols. Imagine palettes of different goods that need to be securely identified at reception, a group of people that needs to be identified to gain access to some resource, or bags of a traveler that can only pass airport security checks together with their associated owner. In these scenarios, the goal is to achieve some computation as the result of the overall interactions between the tags and the reader while preserving security against impersonation, forging and assuring the privacy of individual tags as well as the privacy of some globally sensitive information.

Unlike the classical RFID authentication scenario, the reader and the backend system to which the former is connected are not assumed to be trusted in that they should never be in a position to identify individual tags. Rather than tag identification, the basic objective of the protocols in the multi-tag setting is to make sure that a valid computation has taken place based on the collaboration of legitimate tags.

Several computational models involving multiple, cooperating tags and readers can be envisioned: similar to an 802.11 access point, the reader can act as a simple relay between tags or be the focal point of computations performed in several tags. We analyse the multi-tag scenarios in each model with respect to the basic interactions between the tags and the reader. For each scenario, we discuss the main challenges for research based on a simple abstract model representing the data processing and security operations. All multi-tag settings discussed in this paper call for the design of some homomorphic security transform under the stringent computational limitations akin to RFID tags.

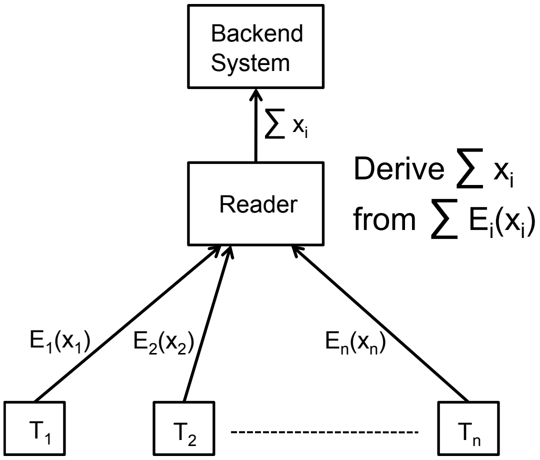

Fig. 1. Aggregation Protocol

2.1 Reader as a Focal Point

In the focal point model, various scenarios can be envisioned. In the first scenario, called aggregation, the reader collects and combines data computed by tags based on some data aggregation operation such as sum, average, etc.. One of the challenging security research problems raised by this scenario is the design of aggregation operations compatible with security transforms in the context of the RFID systems.

The second scenario that lends itself to an interesting research problem with RFID tags is matching of tags based on their secret attributes.

2.2 Aggregation

The goal of the aggregation model depicted in Figure 1 is to allow each tag T_i to send the value x_i of some private attribute to the reader and to let the reader or the backend system compute the aggregate $\sum x_i$ of the values transmitted by several tags while the privacy of the tags and the confidentiality of individual x_i values are preserved with respect to the reader, the backend system and potential intruders. Typical applications for this model are computation of statistics (sum, average, etc.) over private data, such as visitors' origin, gender, age, etc. at the entrance of some event, or the type of disease(s) contracted by patients in a hospital. The value x_i of the private data may be represented by a single bit or decimal value in case of a simple attribute or by a vector of bits or decimal values in case of a multivariate attribute. The main challenge in this model is to allow the reader or the backend system to compute the aggregate of the values using the encrypted samples $E_i(x_i)$ transmitted by each tag. This basically requires an encryption operation that is homomorphic with respect to the aggregation operator whereby the cleartext aggregate value $\sum x_i$ can be derived from the aggregate $\sum E_i(x_i)$ of the encrypted samples. The reader might notice a strong similarity between this requirement and the secure data aggregation problem in sensor networks. Nonetheless the design of a homomorphic encryption mechanism as required by the multi-tag aggregation model is definitely made harder by the additional requirement for tag privacy. Thus secure aggregation mechanisms based on end-to-end sharing of keys between individual contributors and the focal point, such as the ones suggested by Castellucia et al. [5], Girao et al. [9], Önen and Molva [11] are not suitable for the multi-tag setting. Furthermore, another desirable property deriving from tag privacy is unlinkability through the aggregation protocol. In order to assure unlinkability, the encrypted values transmitted by the same tag must be different and uncorrelated for each execution of the protocol. On the other hand, most homomorphic encryption algorithms that lend themselves to the solution of the multi-tag aggregation problem are based on complex operations that are definitely not suitable for the limited computational environment of RFID tags. Asymmetric approaches whereby the complexity of the operations are supported by the reader or the backend server seem to offer a promising avenue for tackling this problem.

2.3 Matching

The goal of matching with RFID tags as shown in Figure 2 is to allow a reader to determine whether two or more tags possess some attributes a_i that jointly fulfill some boolean constraint $g(a_1, a_2, \ldots, a_n)$ while keeping the attributes of each tag private not only with respect to third party intruders but also with respect to the reader. Identity of the attributes held by the tags or their matching with respect to some operation can be considered as part of the constraint.

Such a mechanism can be used in implementing safety regulations that forbid the transport of some set of hazardous goods in the same shipment while the content of each individual container is kept secret for obvious reasons due to the potential risk of misuse or theft.

The main challenge in this model is to allow the reader or the backend system to compute the constraint using the encrypted attributes $E_i(a_i)$ transmitted by each tag. This again calls for an encryption function that is homomorphic with respect to the constraint function whereby the cleartext value of the constraint function $g(a_1, a_2, \ldots, a_n)$ can be evaluated based on some function f computed over the encrypted attributes. There is a strong similarity between tag matching and the secret matching problem as addressed by Ateniese et al. [1], Balfanz et al. [3], Sorniotti and Molva [13]. Unfortunately a straigthforward transposition of these computationally expensive secret matching mechanisms in the RFID setting does not seem feasible mainly due to the stringent limitations of the RFID environment. Like the previous scenario, the most promising approach for tackling the tag matching problem seems to be the combination of an asymmetric protocol with an unbalanced sharing of computational burden between tag and reader.

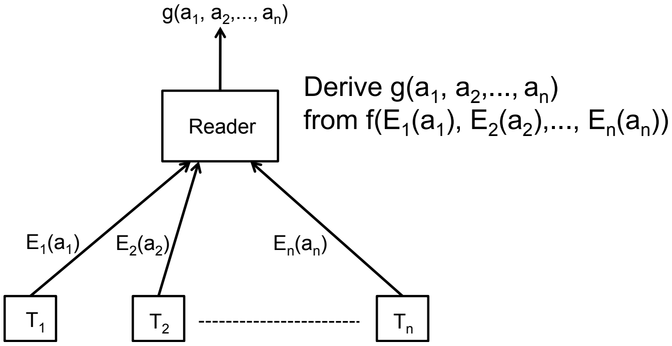

Fig. 2. Tag Matching Protocol

2.4 Reader as a Relay

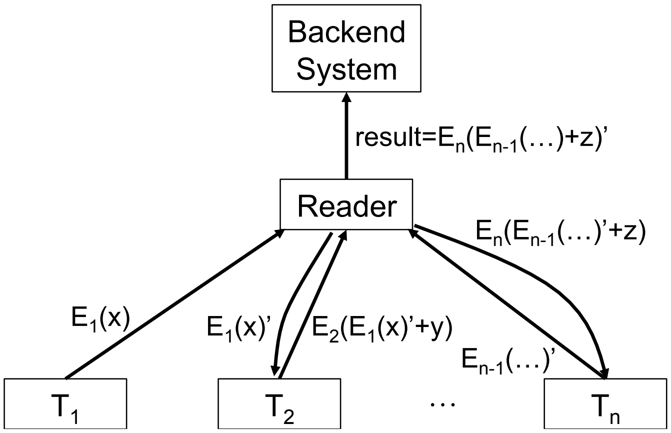

Fig. 3. Distributed authentication of tags, reader acts as relay

In the relay model, similar to traditional multi-party computation, the reader conveys the messages originating from the tags to one another. The tags do not trust the reader in the sense that they do not want to reveal their individual privacy to the reader. Within that model, based on the privacy requirements, the reader may be required to perform some transform over protected messages, thus calling, e.g., for some homomorphic security transform like computing with encrypted functions or data. The basic setup of the relay communication model is depicted in Figure 3. A total of n tags, $T_1, \ldots, T_n$ want to simultaneously authenticate to the reader. Not only an outside adversary, but maybe even the reader must not be able to identify individual tags. Still, the reader should be convinced in the end that there a n valid tags authenticating. Randomly, one tag T_1 launches the protocol by sending a credential x to the reader using a privacy-preserving obfuscator E. The reader receives $E_1(x)$ and forwards $E_1(x)$ to T_2. T_2 responds by appending its own credential y to $E_1(x)$: $E_2(E_1(x) + y)$.

Eventually, T_n sends $E_n(E_{n-1}(\ldots) + z)$ to the reader. The reader or some kind of backend system will now be able to verify whether n valid tags, maybe belonging to the same kind of group, participated in the authentication. One typical application for such a setup if the aforementioned scanning of bags belonging to the same traveler during airport security checks.

The operation $'+'$ can be any append-operation, with a focus of being lightweight. To protect privacy or traceability of individual tags, credentials such as x, y, z should change over time. They might even be updated separately by the reader. Also, to shift computation to the reader, we could allow the reader to do a transformation of received obfuscated credentials $E_i(j)$. As shown in Figure 3, the reader might transform $E_i(j)$ to $E_i(j)'$ before relaying this to the next tag.

The result of all this effort be privacy of individual tags and authentication as a group of valid tags. Also, these scheme could support tolerance against a fraction of broken or compromised tags. However, classical, traditional solutions to these problems are not suitable for RFID. The challenge for research here is to find new, lightweight solutions for these problems, designed under the specific constraints of the RFID environment.

3 Secure and Private Electronic Payment with Tags

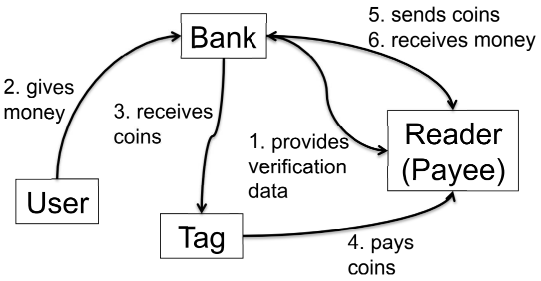

Fig. 4. RFID based payment

The Oyster Card [14] is a prominent example of another important application of RFID tags: electronic payment. While the Oyster Card is a centralized setup with only one payee, large contactless smartcards are used, and security mechanisms have already been bypassed, there will be a need for RFID-based payment systems.

In contrast to the Oyster Card setup, customers will, however, have a strong demand for privacy, untraceability, or unlinkability of their payments. There is also an increasing emphasis in several countries on regulations for the protection of user privacy and security within RFID-based payment systems.

Neither the bank nor different payees, e.g., London's Public Transportation System, should be able to follow and link subsequent payments. So, the system will not only have to protect against malicious tags trying to illegally spend money, but also to protect against potentially "malicious payees" trying to reveal someone's privacy.

In general, payment protocols and the micropayment variant thereof are not a new research topic at all, cf., research on electronic cash [4, 6, 7] and its many extensions, or see van Tilborg [16] for an overview. Still, the payment problem in the constrained RFID environment raises very challenging research problems. One of the main challenges will be to design a solution for a payment scheme which is suited for constrained tags, but still protects the privacy of payers, in particular their payments' untraceability or unlinkability. The design of payment schemes in the RFID setting has to address several issues as follows:

1. Blind signatures that are one of the main building blocks of classical payment schemes are infeasible in the RFID environment due to their computational complexity. However, to achieve privacy and untraceability of payments against the bank, there is a strong requirement for lightweight techniques for achieving similar privacy purposes as blind signatures.
2. Tags are also constrained in terms of storage; straigthforward solutions trading-off precomputing of complex operations by powerful readers with storage in tags are therefore not suitable. Also, coins of the virtual currency cannot be stored on the tag, as there is not enough non-volatile memory available. To overcome this problem, tags would need to be able to "generate" valid coins on the fly during payment. Still, payees must be able to verify validity of generated coins and in doing so not reveal the identity of the paying tag or trace the tag.
3. Digital signatures also are not feasible in RFID tags, thus calling for lightweight approaches to prevent forging of currency and double spending. In this context, it is important to point out that, as with electronic cash, different payees (readers) are typically not synchronized with each other and also not online connected to some kind of joint backbone system. They are "offline" and thus need to verify payments offline. Still, it should eventually be detected if a tag tries to double spend money.
4. Often readers – representing payees – are embedded devices with restricted hardware. While readers' hardware capabilities are higher than those of tags by orders of magnitude, still payment might possibly require lightweight protocols on the reader side, too.

The setup in a tag based payment scenario is shown in Figure 4. In an initial step, the bank provides payees with information how distinguish between valid and invalid coins. Then, as with electronic cash, tags are "charged" at the bank. The user of a tag hands in real money, and in return the bank sends coins or information on how to create coins to the tag.

Therewith, the tag can now generate coins during payment and send them to the payee. After successful verification of these coins, the payee forwards coins to the bank and gets reimbursed.

4 Conclusion

As RFID-systems are entering our daily life, there is a strong demand for appropriate security and privacy-preserving mechanisms. Today's research mainly focuses on traditional applications, such as secure identification and mutual authentication between a tag and a reader. While this is without doubt important, we claim that most problems in this field are already understood or about to be understood. Future research results will most likely offer only marginal improvements and eventually result in what is currently worked on: privacy-preserving authentication between a tag and a reader. However, we claim that with the omnipresence of RFID-tags, there are many other promising applications that need to be worked on: the two examples presented in this paper are 1.) multi-tag applications, where there we can have benefit from multiple tags cooperating and using a reader only as a relay, and 2.) payment applications, where tags are used similar to electronic wallets in electronic cash.

Bibliography

[1] G. Ateniese, M. Blanton, and J. Kirsch. Secret handshakes with dynamic and fuzzy matching. In *Network and Distributed System Security Symposium*, pages 159–177, 2007.

[2] G. Avoine, E. Dysli, and P. Oechslin. Reducing time complexity in rfid systems. In *Proceedings of Selected Areas in Cryptography*, pages 291–306, Kingston, Canada, 2005. ISBN 978-3-540-33108-7.

[3] D. Balfanz, G. Durfee, N. Shankar, D. K. Smetters, J. Staddon, and H.-C. Wong. Secret handshakes from pairing-based key agreements. In *IEEE Symposium on Security and Privacy*, pages 180–196, 2003.

[4] S. Brands. Untraceable off-line cash in wallets with observers. In *Proceedings of Annual International Cryptology Conference*, pages 302–318, Santa Barbara, USA, 1993. ISBN 3-540-57766-1.

[5] C. Castellucia, E. Mykletun, and G. Tsudik. Efficient aggregation of encrypted data in wireless sensor networks. In *2nd Annual International Conference on Mobile and Ubiquitous Systems, Mobiquitous*, 2005.

[6] D. Chaum. Blind signatures for untraceable payments. In *Proceedings of Annual International Cryptology Conference*, pages 199–203, Santa Barbara, USA, 1982.

[7] D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. In *Proceedings of Annual International Cryptology Conference*, pages 319–327, Santa Barbara, USA, 1988. ISBN 3-540-97196-3.

[8] T. Dimitrou. rfiddot: Rfid delegation and ownership transfer made simple. In *Proceedings of International Conference on Security and privacy in Communication Networks*, Istanbul, Turkey, 2008. ISBN 978-1-60558-241-2.

[9] J. Girao, D. Westhoff, and M. Schneider. Cda: Concealed data aggregation for reverse multicast traffic in wireless sensor networks. In *IEEE ICC05*, 2005.

[10] A. Juels and S.A. Weis. Defining strong privacy for rfid. In *PerCom Workshops*, pages 342–347, White Plains, USA, 2007. ISBN 978-0-7695-2788-8.

[11] M. Önen and R. Molva. Secure data aggregation with multiple encryption. In *EWSN 2007, 4th European conference on Wireless Sensor Networks, January 29-31, 2007, Delft, The Netherlands — Also published as LNCS Volume 4373*, Jan 2007.

[12] R. Di Pietro and R. Molva. Information confinement, privacy, and security in rfid systems. In *Lecture Notes in Computer Science, Volume 4734*, pages 187–202, 2007. ISBN 978-3-540-74834-2.

[13] A. Sorniotti and R. Molva. A provably secure secret handshake with dynamic controlled matching. In *IFIP SEC 2009, 24th International Information Security Conference, May 18-20, 2009, Pafos, Cyprus*, May 2009.

[14] Transport for London. Oyster online, 2009. https://oyster.tfl.gov.uk/oyster/entry.do.

[15] G. Tsudik. Ya-trap: yet another trivial rfid authentication protocol. In *Proceedings of International Conference on Pervasive Computing and Communications Workshops*, Pisa, Italy, 2006. ISBN 0-7695-2520-2.

[16] H.C.A. van Tilborg, editor. *Encyclopedia of Cryptography and Security*. Springer Verlag, 2005. ISBN 038723473X.

[17] S. Vaudenay. On privacy models for rfid. In *Proceedings of ASIACRYPT*, pages 68–87, Kuching, Malaysia, 2007. ISBN 978-3-540-76899-9.

[18] S.A. Weis, S.E. Sarma, R.L. Rivest, and D.W. Engels. Security and privacy aspects of low-cost radio frequency identification systems. In *Security in Pervasive Computing*, pages 201–212, Boppard, Germany, 2003. ISBN 3-540-20887-9.