P. Najera, F. Moyano, and J. Lopez, "Secure Integration of RFID Technology in Personal Documentation for Seamless Identity Validation", *3rd Symposium of Ubiquitous Computing and Ambient Intelligence 2008*, Advances in Soft Computing vol. 51/2009, pp. 134-138, 2008.
http://doi.org/http://dx.doi.org/10.1007/978-3-540-85867-6_16
NICS Lab. Publications: https://www.nics.uma.es/publications

Secure Integration of RFID Technology in Personal Documentation for Seamless Identity Validation

Pablo Najera, Francisco Moyano, Javier Lopez

Computer Science Department
University of Malaga,
E.T.S.I. Ingeniería Informática, 29071, Málaga, Spain
najera@lcc.uma.es;moyano@lcc.uma.es;jlm@lcc.uma.es

Abstract. Seamless human identification and authentication in the information system is a fundamental step towards the transparent interaction between the user and its context proposed in ambient intelligence. Due to this, the IDENTICA project is aimed to the design and implementation of a distributed authentication platform based on biometrics (i.e. voice and facial image) and personal documentation. In this paper, we present our work in this project focused on the secure integration of RFID technology in personal documentation in order to provide seamless identity validation. Our actual work status, first results and future directions are describe in detail.

Keywords: Biometry, identity verification, privacy, RFID, security.

1 Introduction

From the beginning, human identity verification has been a necessary precondition in many contexts in order to fulfil user's needs. When a person wants to withdraw some money from the bank, it must demonstrate first it is the person that it declares to be. With the adoption of electronic documents new scenarios arise. Until now, a solution has been the creation of identity documents based on a plastic support issued by a certification authority, and embedded with some biometric features, such as a photograph and a fingerprint. Spanish D.N.I (National Identity Document) based on this system has been used in Spain since 1944. However, throughout the years, new technologies (e.g. smart cards, voice recognition, and RFID tags) have arisen that could make this process more comfortable and safer without requiring human intervention.

Taking advantage of these emerging technologies, the goal of the IDENTICA project is to develop a flexible, lightweight platform in order to make easier the process of human identification in real environments. As the process of human authentication must be secure, it is necessary to provide the platform with security mechanisms that provides confidentiality and integrity of data stored inside a tag, as well as access control mechanisms in order to assure that a non-authorized part cannot retrieve personal data: this point is where UMA is interested in.

2 Technical background

2.1 RFID (Radio Frequency Identification)

The idea behind this emerging technology is providing an identity to any object in a particular environment by means of an attached RFID tag. Tag's unique identifier together with application dependent data (e.g. the name of the person if we refer to identity cards) can be read and registered by RFID readers in order to be processed by a back-end database.

Identity verification and access control based on electronic documents such as e-passports, is an interesting and promising area in which RFID is being introduced and gaining more importance day by day. One prove of its increasing importance is that since August 2006, Spanish government has been issuing *only* e-passports, and U.S. government has been demanding its possession to anyone who wants to travel there.

2.2 Biometric authentication

Biometric authentication consists of the verification of a person's identity based on the analysis and measurement of biological characteristics. In the context of identity documents, biometry can improve the security since it makes stronger the link between the document and its owner.

Nowadays, biometric information is being embedded into the RFID tags. These critical personal data (that includes facial and iris image, voice and fingerprint patterns) must be protected against adversaries and unauthorized RFID readers.

3 Focus

Provided biometry-based identity recognition techniques (i.e. facial image, iris and voice recognition), as well as optical document interpretation techniques such as OCR (Optical Character Recognition) and ICR (Intelligent Character Recognition) from other research groups, our work focuses on the integration of RFID technology in personal documentation including the secure access, storage and transference of biometrics and personal data from RFID tags to the authentication platform.

In our research on how RFID technology can be securely incorporated in the area of human authentication preserving data privacy, several matters must be kept in mind, such as eavesdropping and man-in-the-middle attacks, non-authorized access to a tag leading to data leakage or corruption, as well as counterfeited tags. In order to fulfil our task and prevent potential attacks, several steps need to be taken.

First of all, it is necessary to make a state of the art study in order to determine which security mechanisms (e.g., authentication protocols, symmetric and

asymmetric encryption algorithms, key generation algorithms or secure ID-disclosure protocols) are used nowadays in RFID technology and documents.

From this point on, we must proceed to the design and implement of the reading and writing modules that will establish the link between tag's memory and the authentication platform. In order to enhance data privacy, we must design secure tag identification mechanisms (preventing ID disclosure and later bearer tracking), mutual authentication and key generation protocols with the purpose of providing access control, preventing tag counterfeiting and securing the communication channel.

As a contribution of the project, it has been proposed to design an infrastructure to manage the keys required for access the tag and establish a secure communication channel. Until now, it has not been developed a robust, reliable key management infrastructure oriented to RFID-based infrastructures. Due to this lack, actual applications tend to apply the same key for all the RFID tags or rely on weak key generation protocols (i.e. based on predictable values) degrading the whole system security.

In addition, it has been proposed to apply the biometric features used in the project to develop strong key generation protocols. Thanks to this biometric information, it could be possible to establish that a reader can only access data inside a tag if the person (who it is going to be authenticated) is present at that moment. Moreover, it could be possible to generate access keys to RFID tags from biometric measures of the bearer of the document, and so in this context, there would be no need of accessing a key management infrastructure. Biometric features that will be discussed include facial recognition, iris recognition and fingerprint recognition.

3.2 Tasks performed and future work

With the purpose of defining secure mechanisms to avoid tag ID disclosure to unauthorized third parties and provide mutual authentication as well as encrypted communications between RFID tags and readers, we required to perform a through study on the RFID-related security mechanisms proposed in the literature.

As a result of this research, we have identified several protocols and techniques based on different restrictions on onboard RFID tag capabilities to fulfill the previous security requirements.

A wide range of out-of-tag techniques have been proposed in order to prevent unauthorized readers from identifying a tag. These schemes range from the Faraday cage (where a tag is confined in a physical shield to block its output) to active jamming techniques (as in the blocker tag [3] or soft blocking [4] solutions, where a device broadcasts a signal to prevent unauthorized readings). These techniques share the advantage of not forcing specific tag features, so enabling the use of low-cost security-naked RFID tags, at the cost of actively involving the user in using the mechanisms and ensuring his privacy.

In the analysis of solutions for non-cryptographic tags, we found several proposals based on tag pseudonyms (such as tags with rewritable memory [5,7] or sets of pseudonyms [6]) where the tag stores one or several alternative IDs that a

legitimate reader will be able to link to its real ID, thus avoiding identification from evil readers, but not tag tracking attacks until pseudonyms sets are refreshed. More exotic solutions for non-criptographic tags includes the error-prone approach of tags with antenna energy analysis [8], where the tag estimates reader to tag distance based on signal/noise ratio and restricts data disclosure to far-off readers.

In the area of security solutions oriented to cryptographic tags, we have identified a wide range of proposed solutions that differ in the on-board circuitery required (i.e. tag cost and suitable applications) as well as security level provided.

Among these schemes, we would like to highlight a few different or interesting ideas shared by sets of solutions. In the simpler approaches, hash-lock schemes [9] only require a tag to integrate hash functions that are used to implement access control schemes. As a reader demonstrates the knowledge of a shared secret, the tag can be unlock to read its contents and relocked to avoid future data disclosure.

Reencryption functions [11] allows a tag to provide a metaID that has been encrypt an undefined number of times, but the reader will only require to decrypt it once to recover the real ID. This scheme enables ID disclosure and tracking protection, at the cost of implementing asymmetric cryptographic circuitry onboard.

Another interesting approach pointed out in this research is based on PUF (Physical Unclonable Function) functions [10] that provide a unique fingerprint to each RFID tag thanks to the unpredictable behavior of logic gate and wire delays of each manufactured tag. Thanks to this unique signature, tag authentication schemes can be obtained that turn out to be unclonable.

Last but not least on our highlights of the security mechanisms for RFID tags research, asymmetric cryptography that seemed to be out of scope for the highly constrained RFID technology, it is turning out to be feasible thanks to elliptic curve cryptography [12] that requires only a fraction of the number of logic gates for implementation providing a similar level of security than traditional asymmetric cryptography.

Even if our study found hundreds of papers on security mechanisms for RFID, most of literature seems to focus on the higher constrained technology branch (i.e. EPC Class 1 Gen1&2 tags) mainly oriented to tagging products in the supply chain and beyond raising important privacy threats. Due to cost restrictions, these are the less capable RFID tags providing a security level non adequate to the requirements defined for personal documentation.

Actual cryptographic mechanisms standarized for ePassports cover a comprehensive range of countermeasures: Passive Authentication (i.e. data stored on tag digitally signed by the issuing country); Basic Access Control that prevents skimming and eavesdropping attacks by authenticating the reader and encrypting messages; and Active Authentication where the tag is validated proving the possession of a private key. However, key generation for BAC is based on basic owner and document data, thus enabling several attacks [1].

Regarding RFID technology branches, semi-active and active RFID tags where discarded due to size and cost reasons. In passive RFID technology, UHF (i.e. EPC Class 1 Gen1&2/ISO 18000-6), LF (i.e. ISO 18000-2, ISO 11784/11785) and

part of HF (i.e. ISO 15693) RFID branches were designed for substantially different applications and do not provide adequate cryptographic features [2]. So we concluded that passive HF tags based on ISO 14443 are the most suitable RFID tags for our purposes due to computational resources and onboard security facilities.

Further research on actual RFID tags conforming ISO 14443 standard revealed candidate choices including SmartMX P5C family from NXP, the slightly slower SLE66CLX from Infineon and the expected RF360 from Texas Instruments. The SmartMX tag was selected due to higher performance and actual availability. The SmartMX P5CT072 features a 72kB EEPROM and a cryptographic coprocessor that supports RSA, ECC, 3DES and AES functions.

In order to implement the security mechanisms defined in the project on a tag, writing data through a RFID reader it is not enough. Instead, a complete implementation of internal tag operating system is required. The resulting ROM mask has to be provided to NXP in order to manufacture the final ICs. To achieve this goal, Keil's PK51 developing environment and SmartMX DBox testing box have been selected. Similar alternatives like Ultra-SmartMX from Ashling did not allow squeezing the full range of IC features according to providers.

In a first approach, a ROM mask conforming ICAO 9303 standard that fulfils reader authentication and secure messaging defined in Basic Access Control mechanism is being implemented. Further work will include new security schemes defined in the context of the project.

In particular, robust key generation algorithms for authentication and encryption derived from owner's biometrics, instead of basic personal and document data (i.e. birth day, passport number and expiration date) as used in actual ePassports, are expected.

A different approach will work on an adequate infrastructure for RFID key management in the proposed scenario. This infrastructure would provide pre-established high entropy keys without requiring on-reader robust key generation algorithms.

5 Conclusions

As computing evolves and gets pervasive, new scenarios arise where automatic identity validation is required in order to allow system access and grant pertinent privileges to a user without human intervention. In this context, the IDENTICA project has born with the goal of provide a distributed authentication platform based on biometrics and personal documentation. RFID technology embedded in electronic documentation will provide the link between real-world identity documents with biometric data stored inside and the context-aware system.

But automatic management of human presence and his identity by means of RFID technology in personal documentation may lead to individual tracking and personal data leakage, thus adequate security mechanisms for this purpose are required.

We have shown the first steps and results of our work in this direction where a biased effort towards the most constrained RFID technology branches, not suitable for personal documentation, has been detected in actual proposed solutions and specific mechanisms for electronic documentation have turned up to be present weaknesses. Also future directions have been exposed oriented to the design of an adequate key management infrastructure for RFID systems and key generation protocols based on biometric data that will potentially solve the deficiencies in actual solutions.

Acknowledgements. This work has been partially supported by the Spanish Ministry of Industry through the IDENTICA project (FIT-360503-2007-3) and the Spanish Ministry of Science and Education through the National F.P.U. Program.

References

1. Avoine, G., Kalach, K. and Quisquater, J. "ePassport: Securing International Contacts with Contactless Chips", in Tsudik, G., ed.,'Financial Cryptography and Data Security - FC'08', IFCA, Springer-Verlag, Cozumel, Mexico, 2008.
2. Phillips, T., Karygiannis, T. and Kuhn, R. "Security standards for the RFID market," Security & Privacy Magazine, IEEE (3:6), 2005, pp. 85--89.
3. A. Juels, R. Rivest, M. Szydlo, The blocker tag : Selective blocking of RFID tags for consumer privacy, In Porceedings of the 10th ACM Conference on Computer and Communications Security, Oct. 27-30, ACM Press, New York, 2003, 103-111.
4. A. Juels and J. Brainard, “Soft Blocking: Flexible Blocker Tags on the Cheap,” Workshop on Privacy in the Electronic Society, ACM Press, 2004, pp. 1–7.
5. S. Kinoshita, F. Hoshino, T. Komuro, A. Fujimura, M. Ohkubo, Low-cost RFID privacy protection écheme, IPS Journal 45, 8, Aug, 2004, pp. 2007-2021 (in Japanese).
6. A. Juels, “Minimalist Cryptography for RFID Tags,”4th Conf. Security in Comm. Networks, C.Blundo and S. Cimato, eds., Springer-Verlag, 2004, pp.149-164.
7. P. Golle et al., “Universal Re-encryption for Mixnets,” Proc. RSA Conference Cryptographer’s Track, T.Okamoto, ed., Springer-Verlag, 2004, pp. 163–178.
8. K.P. Fishkin and S. Roy, “Enhancing RFID Privacy via Antenna Energy Analysis,” IRS-TR-03-012, Intel Research Seattle, 2003.
9. Weis,S. “Security and Privacy in Radio-Frecuency Identification Devices”, Masters Thesis, mayo 2003.
10. Pim Tuyls y Lejla Batina, “RFID-Tags for Anti-Counterfeiting”, Topics in Cryptology - CT-RSA 2006, The Cryptographers' Track at the RSA Conference 2006, febrero 2006.
11. Shingo Kinoshita, Miyako Ohkubo, Fumitaka Hoshino, Gembu Morohashi, Osamu Shionoiri y Atsushi Kanai, “Privacy Enhanced Active RFID Tag”, Proceedings of ECHISE 2005, mayo 2005.
12. S.Martínez, M. Valls, C. Roig, F. Giné y J.M. Miret, “An elliptic curve and zero knowledge based forward secure RFID Protocol”, RFIDSec 2007, Julio 2007.