Secure Symmetric Authentication for RFID Tags

Anuj kumar' Tarun mehta

Abstract- **The project ART proposes to reinforce passive RFID (Radio Frequency Identification) tags with cryptographically secure authentication. beginning with a brief introduction into common RFID systems with passive tags, we have a tendency to gift a motivation why secure authentication with standardized parallel crypto algorithms for RFID tags is important for several applications. we have a tendency to demonstrate vulnerabilities of current RFID systems Associate in Nursingd make a case for however application of an authentication mechanism will solve them. what is more we have a tendency to make a case for however authentication protocols work and the way they will be enclosed within the RFID protocol normal ISO 18000. By presenting the interim results of ART, we are going to show that the projected improvement is possible with current RIFD infrastructure and semiconductor technology used for RFID tags.**

Index Terms- **RFID, AES, Authentication, ISO 18000.**

I. INTRODUCTION

Radio Frequency Identification (RFID) is Associate in Nursing rising technology. the most plan behind it's to connect a thus referred to as RFID tag to each object during a specific atmosphere and provides a digital identity to any or all these objects. Associate in Nursing RFID tag may be a tiny micro chip, with Associate in Nursing antenna, holding a novel ID and alternative info which might be sent over frequence. the data are often mechanically browse and registered by RFID readers. the information received by the RFID reader are often after processed by a back-end info. Figure one provides a graphical summary of Associate in Nursing RFID system

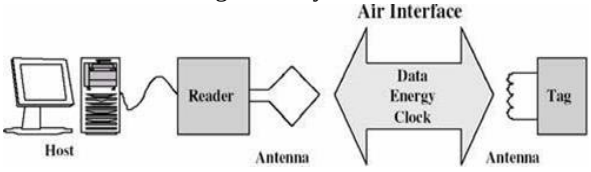

Figure 1: Overview of an RFID system.

The range of possible applications varies with the capability of the tag and is separated by different classes. Class 0 and Class 1 RFID tags are used as barcode replacement and are read-only or can be programmed only once in the field, respectively. Inventory maintenance which is used in the supply chain management can be automated using such tags. They are cheap (approximately 5 Cents) and can be used on item-level on nearly every product.

This paper is focusing on more advanced tags (Class 2)which also have a rewritable memory and additional hardware resources but do not have an active power supply on the tag. The energy for operation is pulled from the electromagnetic field provided by the reader. In addition, the reader also provides the digital clock frequency for operation. Certain modulation methods are used for communication from the reader to the tag and vice versa. Such tags cost about 50 Cents and the available silicon area is about 10,000 gates. The applications for more advanced RFID systems are manifold but especially high value products like pharmaceutical and branded goods can be protected against security vulnerabilities. In this paper, we demonstrate how the project ART (Authentication for long-range RFID systems) proposes to improve current RFID systems by providing secure authentication. The project is performed by four independent partners, two from industry and two academic partners. A major goal of the project is to enhance the functionality of current RFID tags with passive power supply.

The basic functionality of RFID systems is to provide identification of individual objects by the replies the attached RFID tag sends to a request performed by a reader. The reader uses an attached database to link the received ID number to a specific object described in the database. The major drawback of those systems is that the communication scheme does not provide a method to prove the claimed identity. Since a typical tag answers its ID to any reader (without a possibility to check whether a reader is authorized to receive the information), and the replied ID is always the same, an attacker can easily forge the system by reading out the data of a tag and duplicating it to bogus tags. Closed RFID systems with common access of all

readers to a central database, can check for illegal duplicates (bogus tags) within the database but this is not practical for many applications. Furthermore, it is impossible to distinguish the original tag from its illegal duplicates.

Strong authentication mechanisms can solve uprising security problems in RFID systems and therefore give protected tags an added value. The three main security threats in RFID systems are forgery of tags, unwanted tracking of customers, and the unauthorized access to the tag's memory. In this paper, we propose authentication protocols for RFID systems based on the ISO/IEC 9798-2 standard [6]. These protocols allow protecting high-value goods against adversary attackers. Additionally, we show that these protocols are feasible for nowadays restriction concerning data rates and compliance to existing standards as well as the requirements concerning chip area and power consumption. With authentication we mean a method to provide a proof for a claimed identity. This proof is based on a secret stored within the authenticating part of the system. As long as the secret information stays secret and the used protocol does not leak sensitive information, an attacker cannot forge a tag.

A communication system providing authentication can reject access (to information, entry, etc.) to non authorized parties. To keep the authentication secure, it is necessary that an attacker does not gain information about the secret by listening passively to successful authentications. To fulfill this requirement for strong authentication, it is necessary to use cryptographically strong computations.

Under "cryptographically strong" in this context we understand that it must be computationally infeasible with current computing systems to derive the secret key data from an unlimited number of known input and output message pairs.

II. SYMMETRIC AUTHENTICATION

Authentication is the mechanism that one entity proves its identity to another entity. Strong authentication protocols, such as challenge-response protocols (standardized in ISO/IEC 9798) are widely used in practice today. In challenge-response protocols, one or several messages are exchanged between the party who wants to prove its identity (the claimant) and the party who wants to verify the identity (the verifier). This is called the protocol. In a typical scenario, the verifier challenges the claimant with an unpredictable value that is used no more than once (the nonce). The claimant is required to return a response that is depending on the nonce and on the stored secret.

Using strong authentication for RFID systems leads to significant security enhancements. If readers are required to authenticate themselves to tags, attacks such as unwanted tracking and unauthorized memory access are rendered infeasible. If tags are required to authenticate themselves against readers forgery of tags is prevented. It is advantageous to use standardized protocols and algorithms because they have been rigorously cryptanalyzed and are widely used. Hence, systems based on standardized protocols and algorithms are more likely to be secure and interoperable with other well established infrastructures. Standardized challenge-response protocols are defined upon symmetric-key and asymmetric-key cryptographic primitives.

Using symmetric-key cryptography has the disadvantage that there is one secret key shared through all parties. If one key is compromised for any reason the whole systems gets insecure. However, strong asymmetric- key cryptography requires extremely costly arithmetic operations and is therefore out of question for RFID systems today. Strong symmetric-key cryptographic primitives include encryption primitives such as AES [5] which allow compact implementations [1]. In the following, a few authentication protocols based on challenge-response methods are explained.

A. Tag Authentication

Here, the tag authenticates itself against a reader. The origin of the tag are often well-tried and forgery is prevented. The protocol works as follows (we denote the concatenation of values by |):

Reader Tag: AuthRequest | ID | RR Tag Reader: EK(RR | RT) | RT

The reader sends Associate in Nursing authentication request, addressed with the ID of the tag (8 bytes). It contains a present, generated by the reader (RR, 8 bytes). The tag encrypts the present with the key key and sends the result back to the reader, which might then verify the result. To avoid chosen- plaintext attacks, i.e. that Associate in Nursing assaulter will fix the worth of

B. Reader Authentication.

This methodology is employed for genuine access to the tag's memory. The tag requests Associate in Nursing authentication from the reader before it reveals its true ID and any access to the tag. The tag takes half within the anti-collision algorithmic rule with a random ID (RT, 8 bytes). All addressed requests ar finished RT (tracking prevention). solely when self-made authorization of the reader, the tag sends its ID in plaintext and grants the reader access to the memory. Attackers will get the ID by passively taking note of the communication, though they're unable to initiate it. Another downside may be hijacking of a certified association. it's to be analyzed if this is often a sensible security threat for real-world applications.

Reader Tag: ReaderAuth | RT | EK(RT | RR) | RR
Tag Reader: ID

When respondent to the inventory request, the tag indicates with a flag that the reader should manifest itself. The reader answers to the challenge (RT, eight bytes) and sends missive of invitation to reveal the tag's ID. To avoid a chosen-plaintext attack, the reader will generate a present RR and mix it with RT before respondent the challenge.

B. Mutual Authentication.

In mutual authentication, each parties manifest themselves against one another. All 3 security threats (unwanted pursuit, unauthorized operation, and forgery) are often prevented. Like within the former protocols the tag answers the inventory request with a present (RT, 8 bytes), and requests authentication from the reader. The reader answers the challenge and sends another challenge (RR, eight bytes) for the tag. The tag answers the reader's challenge and each ar genuine . The ID is rarely sent in plain, thus unwanted pursuit is prevented.

III.NECESSITIES FOR AUTHENTICATION IN CURRENT RFID SYSTEMS

The security-enhanced RFID system is especially supported the quality ISO 18000 [7]. This normal defines the in operation conditions underneath that these RFID tags ar operated. It defines the carrier frequency that is

13.56 megahertz and defines the modulation of knowledge. The communication between the reader and also the tag uses Amplitude Shift Keying and also the response from the tag works via load modulation as a result of the tag has no active power provide. Thereby, a resistance is sporadically switched on and off employing a outlined frequency to submit information. what is more, the quality describes the information cryptography mechanisms and defines the communication theme. The tag isn't allowed the send to the reader unless information were requested. The communication is initiated by the reader with missive of invitation and also the tag responses

A.Protocol Extension.

The most vital command is that the anti-collision sequence that may be a command each tag should implement. Thereby, the reader sends Associate in Nursing initial inventory command. All tags within the atmosphere create a response that is that the tag's distinctive ID. If only 1 tag answers to the request the ID are often retrieved by the reader and every one resultant commands are often addressed victimization the ID that addresses one single tag. If 2 or a lot of tags create a solution to missive of invitation a collision happens. this will be detected at the reader. The reader then uses a changed inventory request wherever it adds a district of the tag's ID to the request. solely tags that have this a part of the ID ar allowed to answer. Once the ID of 1 tag is known, the reader sends a "stay quiet" command to the tag with the known ID. This methodology is employed as long as there are not any a lot of collisions and every one tags inside the atmosphere ar known.

Adding Associate in Nursing authentication command to the ISO 18000 normal works by employing a custom command which might be outlined. The challenge-response protocol fits ideally to the request-response protocol. once authenticating a tag, the reader sends a challenge inside the request and also the tag answers per the given authentication protocol.

B. Interleaved Authentication Protocol.

The authentication protocol mentioned higher than solely works once the results of the cryptologic primitive is on the market inside the time outlined for the tag's response. As this point is extremely short a modification of this authentication theme was projected wherever the calculation time for the algorithmic rule is of minor importance. For this

purpose, authentication is split into 2 elements. the primary half is that the authentication request (AR), that tells the tag to inscribe the challenge and doesn't expect any response. The second half is that the response request (RR), that collects the authentication response, once the result's offered. For one tag, the temporal order overhead is massive, however with quite one tag, the reader will use the idle time (during the tag is busy calculating) to send authentication requests (or alternative requests) to alternative tags. This mechanism is printed in figure a pair of.

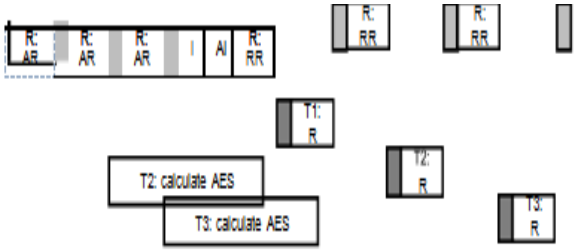

Figure 2: Interleaved authentication protocol.

C. cryptologic Hardware Module.

Computation of the cryptologic algorithmic rule AES (Advanced cryptography Standard) is computationally terribly advanced compared to alternative tasks of tags. The implementation of the AES that fulfils the necessities regarding low power consumption and low die size is way far from being trivial. this consumption of extra hardware parts on Associate in Nursing RFID tag should not exceed 10μA to avoid reduction of the in operation vary.

The AES algorithmic rule may be a block cipher that 128 bits of knowledge the thus referred to as State. to boot, the cipher key that has additionally 128 bits should be keep and new spherical keys have to be compelled to be derived. To inscribe with AES, a spherical transformation is performed 10 times iteratively, wherever one spherical consists of the operations SubBytes, MixColumns, ShiftRows, and AddRoundKey. To decrypt, the inverse operations InvSubBytes, InvMixColumns, InvShiftRows, and AddRoundKey ar applied.

Most hardware implementations of the AES specialise in high information output. the information rates in RFID systems ar terribly slow. Therefore, our implementation tries to arrange operations such the mean current consumption is decreased . we have a tendency to selected Associate in Nursing 8-bit implementation with a flip flop primarily based RAM that holds the State and one spherical key. additionally, the datapath consists of Associate in Nursing S-Box implementation, a MixColumns multiplier factor with 3 temporary registers and a few minor combinatory logic. The controller may be a finite state machine to cut back the chip space and also the current consumption

D.Random range Generation.

Some of the protocols given in section II would like some quite random numbers (nonces). Thereby, it's vital that not very true random numbers ar necessary. the sole vital factor is that the numbers aren't foreseeable and that they should not be duplicated. The implementation on Associate in Nursing RFID tag may be a linear feedback register (LSFR) wherever the seed price is applied from Associate in Nursing genuine reader.

IV.THE PROJECT ART & INTERIM RESULTS

The FIT-IT funded research ART (Authentication for Long- range RFID Technology) is directed on the subsequent objectives within the space of RFID:

1. Raise existing protocol standards for RFID technology with reference to security measures.
2. style and implement tags with sturdy cryptologic algorithms and implement a example tag and a reader.
3. Improve long-range readers in terms of in operation vary by victimization innovative architectures.
4. Investigate potential new application fields.
5. analysis the role of secure sensible tags as a part of a world of close intelligence.

The intermediate results of ART are often directly allotted to the outlined objectives. ranging from a close study of the ISO 18000 protocol, we have a tendency to extended the protocol to permit sturdy cryptologic authentication victimization AES as cryptologic primitive.

For proper analysis that the urged protocol extension is usable in realistic environments, we have a tendency to developed an RFID system simulation tool for protocol analysis (PETRA – Protocol analysis tool for RFID application). This tool emulates the communication between Associate in Nursing RFID reader Associate in Nursingd an arbitrary range of tags. thanks to the Associate in Nursingti- collision theme an RFID reader performs

to handle one tag when the opposite, the communication procedure between a reader and also the tags within the field isn't settled, however looking on many protocol parameters, the precise tag's IDs and sequence of the tags coming into the sector. victimization PETRA we will emulate a high range {of
{different|totally completely different|completely different}|of various} things (varying range of tags within the field; different length of tags within the field; different time of entry into the field) during a cycle correct manner. we will so confirm realistic timings for typical and worst case eventualities of the communication in RFID systems.

As cryptologic primitive for the parallel authentication we have a tendency to chosen AES. One vital criteria for choice of the AES algorithmic rule was its structure that permits economical implementation in hardware. we have a tendency to analyzed the chances for the simplest fitting implementation design to supply AES-128 cryptography practicality that accommodates the demanding necessities for passive RFID systems (average current consumption below 10μA) with presently used semiconductor technology (Philips zero.35μm process). victimization ULP (Ultra Low Power) techniques on each level throughout the planning cycle, we have a tendency to achieved to offer AES-128 cryptography and decipherment together with spherical key computation with a mean power consumption of but 4μA. A complete version with a microcontroller interface was enforced and made (TINA – small AES) as ASIC, that is thus far the littlest and most power-efficient implementation of AES celebrated worldwide. Our style uses around zero.25 mm² semiconductor space that permits production of security increased RFID tags while not a serious increase of the prices. To demonstrate the authentication of Associate in Nursing RFID tag with AES practicality a programmable example tag victimization Associate in Nursing FPGA was developed.

The analog front-end (receiver a part of a tag) is combined with a XILINX FPGA (Field-Programmable Gate Array) on atiny low PCB to figure as full operational tag example. All digital elements of the planning, the non volatile memory block, the controller for computing the extended ISO 18000 communication protocol (implemented as finite state machine) and also the AES module ar organized in programmable hardware. In contrary to plain tags, this example uses Associate in Nursing on board power provide (battery), since FGPA technology's power consumption is far on top of a specialised low power style on RFID capable ASIC technology

V.CONCLUSION

In this paper we have a tendency to started with a brief introduction to current RFID systems. we have a tendency to showed however the fundamental principles work and that we motivated the improvement of actual RFID systems with authentication practicality with standardized strategies and algorithms. when a short section concerning the goals of the project ART we have a tendency to given the interim results. the most result thus far is that we have a tendency to showed, that secure parallel authentication is possible for current RFID technology while not vital extra prices.

RFID with authentication isn't solely necessary to use RFID technology in security relevant applications however additionally if the tags contain personal information, consistent to Article seventeen of the eu commission's information protection directive (see [5]).

VI.ACKNOWLEGDMENT

The project ART is funded underneath the initiative FIT-IT, that was established by the Austrian ministry BM:VIT. The given solutions ar results of the total syndicate, consisting of Philips Semiconductors, Siemens, FH Joanneum Kapfenberg, and IAIK TU metropolis. beside Philips, TU metropolis can establish Associate in Nursing initiative for coordinated analysis and teaching of RFID topics at TU metropolis within the close to future. One goal of this initiative is to ascertain TU metropolis as on of the eu leading centers of excellence for analysis and teaching in RFID topics.

REFERENCES

[1] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. sturdy Authentication for RFID Systems victimization the AES algorithmic rule. In Conference of cryptologic Hardware and

Embedded Systems, 2004. Proceedings. Pages 357-370. Springer 2004.

[2] M. Feldhofer. Associate in Nursing Authentication Protocol during a Security Layer for RFID sensible Tags. within the twelfth IEEE Mediterranean Electrotechnical Conference – MELECON 2004. IEEE Proceedings. Pages 759-762, May 2004

[3] EC ARTICLE twenty nine information Protection unit. operating document on information protection problems associated with RFID technology. offered on-line at: http://europa.eu.int/comm/ internal_market/privacy/docs/wpdocs/2005/wp105_en.pdf

[4] Bundesamt für Sicherheit in der Informationstechnik– BSI. Risiken und Chancen des Einsatzes von RFID-Systemen. 2004, ISBN-3-922746-56-X.

[5] National Institute of Standards and Technology (NIST). FIPS- 197: Advanced cryptography normal (AES). Nov 2001. offered on-line at http://www.itl.nist.gov/fipspubs/.

[6] International Organization for Standardization (ISO). ISO/IEC 9798-2: info Technology – Security Techniques – Entity authentication mechanisms – half 2: Mechanisms victimization parallel encipherment algorithms. 1993.