Survey on passive RFID tag cryptography for nonspecialists

Seminar - Common Flaws in Protocol Security
Technical University of Munich
Munich, Germany

***Abstract*—RFID tags have seen widespread application in various facets of the industry and everyday life. They often store confidential and personal information and pose a privacy risk. Thusly, cryptography becomes a crucial aspect of the design of RFID tags. Because of limitations regarding computational and storage capabilities, intricate lightweight cryptographic methods have to be applied. In this paper, we provide a starting point for nonspecialists concerning RFID, the evaluation methods used in assessing the quality of cryptographic methods used in passive RFID tags, and discuss different cryptographic methods found in the literature.**

I. Introduction

RFID (Radio-frequency identification) tags see usage in numerous industry sectors, revolutionizing logistic and production chains, inventory management, and identification processes. Over the past decades, they have seen use in various applications, including libraries [1], healthcare [2], [3], and automated toll collection systems [4].
RFID tags are tiny electronic devices that use radio waves to emit a unique identifier. Thusly they enable the collection of data, tracking of assets, access control, and management of supply chains.
The inherent constraints of RFID tags, such as the need for lightweight and cost-effective solutions, do not leave room for robust security measures. Unlike traditional cryptographic systems with dedicated hardware support, the cryptographic systems of RFID tags need to balance the security requirements with the limitations regarding the computational and storage capabilities of the tags. Lightweight cryptographic methods are utilized in RFID tags to ensure the confidentiality, integrity, and authenticity of data transmitted between RFID tags and reader devices.
This paper first presents real-life applications for RFID technology and clarifies the functionality of RFID tags. We then discuss methods for evaluating the cryptographic protocols used in these. Subsequently, we explore different cryptographic protocols found in RFID systems before discussing the findings of the paper and concluding it.

II. Our Contributions

The main contribution of this paper is a simplified representation of surveyed papers. Additionally, the paper goes more in-depth regarding the functionality of passive RFID tags than the papers surveyed. Thus, the mechanism behind the passive RFID tags and their limitations regarding cryptography are made clear. Furthermore, we highlight methods used for the evaluation of cryptography protocols before discussing protocols found in the literature.
This paper is a starting point regarding RFID tags and the cryptographic methods used in RFID tags for someone with limited knowledge of cybersecurity and embedded systems. We achieve this through the paper's structure, exploring RFID technology from different abstractions levels.

III. Background

At the most basic level, RFID systems consist of two parts: the tag and the reader. One can compare the relation between tags and readers to the relation between a barcode and a barcode scanner: a reader reads RFID tags associated with an entity. One of the main differences between barcodes and RFID tags is that there is no need for the RFID tag to be in the line of sight of the reader. As a result, RFID technology is a more convenient solution for efficient en masse inventorying or preventing theft.
As aforementioned, the application of RFID technology in numerous sectors of the industry and everyday life is either being researched or has already taken place.

A. Usages of RFID technology

1) Libraries: By replacing barcodes with RFID tags installed inside the covers of books, the books do not need to be in the line of sight when scanned. As a result, books can be scanned faster and the efficiency of checkout and inventorying processes in libraries increases. Security gates at the exits also facilitate the detection of theft attempts [1].

2) Healthcare: In hospitals, RFID has seen usage coupled with wireless sensor networks to achieve patient tracking and vital sign monitoring. This has been done using a wristband equipped with vital sign sensors and an RFID tag [2].
RFID systems can also be used to ensure that patients are administered the correct medication by medical personnel and thus human error is minimized in a highly sensitive environment [3].

3) Automated toll collection systems: Unmanned automated toll collection systems, such as New York's E-ZPass or the FasTrack system used in California, make use of an RFID transmitter placed behind the windshield of a car and readers situated at tolling stations. When passing through the tolling stations, the toll fee can be subtracted from the account of the

driver. Thus, the need to stop the car and pay at a terminal is removed and a smoother flow of traffic is achieved [4].

B. Categories of RFID tags and readers

RFID tags can be classified into three categories: passive, semi-passive, and active tags.

Passive tags represent the most basic category of RFID tags. They consist of only a plain antenna connected to a load, which is used for receiving and reflecting radio waves. These are bonded to an integrated circuit (IC), also known as a microchip. A substrate is then used to encapsulate the circuitry. Semi-passive and active tags are equipped with a power supply, usually in the form of an onboard battery.

The main difference between semi-passive and active tags, which some authors do not differentiate between, is the fact that semi-passive tags do not use the power supply to amplify received and transmitted signals, relying instead on the signal of the reader to reply (interrogator driven communication). Semi-passive RFID tags only use the power supply for onboard processes, e.g. computing cryptographic functions. Active tags, additionally, use the power supply to amplify received and transmitted signals, making them capable of periodically transmitting a signal, disregarding the presence of readers (transponder-driven communication). The possibility of creating active tags that enter a power-saving mode when they find themselves outside a certain location exists, nonetheless, the delimitation between the three categories should be clear. Active and semi-passive tags come with increased size, cost, and the need for maintenance. They are as such impractical when it comes to en masse use in production chains, retail, or libraries.

RFID readers are usually categorized based on the type of tag they interact with. Further differentiation based on hardware and software is possible, although not relevant to the cryptography of RFID tags [5].

C. Functioning principle of passive RFID tags

Passive RFID tags, lacking a power supply, need to make use of the reader's signal (interrogator signal) to power the internal circuitry and communicate with the reader. As a result of the limitations regarding cost and resources, such tags only contain circuitry for power management, signal processing, memory, and the computation of basic cryptographic functions (e.g. simple hash functions [6]). To understand the functioning principle of passive RFID tags, we will describe the key components in further detail.

1) Power management: The power management circuitry inside passive RFID tags has the sole purpose of making the interrogator signal usable as a power source for the other components. This is achieved by having the reader signal received by the antenna be rectified, stored in a power storage element, and then regulating the voltage. The signal is first received by the antenna through electromagnetic induction. The rectifier then turns the alternating current (AC) electromagnetic signal received by the tag into a direct current (DC) signal [7]. The rectified signal is fed into a power storage element, such as a capacitor. Before being fed into the other components, a voltage regulator [8] is used to ensure voltage stability and circuit protection.

2) Signal processing: To enable communication between the tag and the reader, the reader's signal has to be demodulated and decoded by the tag. The signal processing circuitry is also able to use error correction codes, such as Reed-Solomon Codes (RS) [9] to correct errors. These are errors caused by noise or interference which make the received signal deviate from the signal the reader transmitted. The passive RFID tag is then able to process the data sent by the reader and respond accordingly.

Because a passive RFID tag is not able to transmit its signal, it uses a communication technique known as backscatter modulation to communicate back to the reader. Other techniques can be used, although backscatter modulation is used with the most prevalent form of passive RFID tag usage, far-field RFID [10]).

In backscatter modulation, the impedance of the load connected to the antenna is manipulated. This happens based on the data the tag is going to send back to the reader. As a result, reader signals reflected by the antenna are going to have a modulated amplitude. This reflected signal carrying the tag's data is then going to interfere with the incident signal sent by the reader and thus create the tag's response. This allows the reader to receive and interpret the tag's data [11].

3) Memory: The memory of passive RFID tags is typically integrated into the IC and usually presents itself in the form of non-volatile memory, i.e. data is stored even in the absence of a power source. The most commonly used type of memory is EEPROM (Electrically Erasable Programmable Read-Only Memory) [12]. Other types of memory, such as ROM (Read-Only Memory) or volatile memory (e.g. SRAM) can also be used in passive RFID tags: The former in the case that no need for writing data to the tag is needed and the latter in the case that session-specific information needs to be created, stored, or manipulated [13].

There is of course the possibility of storing configuration settings, such as protocol parameters or access control settings in the memory. Nonetheless, the key data stored in a passive RFID tag is the bit string it uses to identify the underlying entity. This can, for instance, come in the form of a UID (Unique Identifier) or an EPC (Electronic Product Code) that adheres to the EPCglobal Tag Data Standard. The latter is a widespread use of passive RFID tags [14].

4) Computation of basic cryptographic functions: Using dedicated hardware and optimized cryptographic algorithms, it is possible for passive RFID tags to compute basic hash functions and symmetric [15] cryptography. There have also been architectures designed for processors compatible with passive RFID tags that can compute ECC (elliptical curve cryptography) operations [16]. The concrete design of the computing elements would not contribute to the reader's understanding of the functioning principle of passive RFID tags and is as such outside the scope of this paper.

IV. Methods for evaluating RFID cryptography protocols

Ensuring privacy in RFID tags is crucial when taking into consideration their applications. Privacy in RFID counteracts, for example, unwanted tracking of people carrying books equipped with RFID tags and the protection of the personal information stored in an RFID-enabled wristband. To provide context for the protocols we are going to discuss in the following sections, we need to establish a standard for assessing the quality of a cryptographic protocol. The adversarial model is one of the tools used in the field of cryptography to design and prove the effectiveness of cryptographic protocols. An adversary is mainly formalized through capabilities and goals. [17] In the context of passive RFID tags, this would mean that an adversary could, for instance, have the goal of retrieving sensitive information found in the memory of an RFID tag by querying it with different messages. An adversary could, additionally, have the capability of receiving and using a reader's signal before querying a tag. In the following subsections, we are going to present three methods that make use of the adversarial model to evaluate the privacy of RFID.

A. Avoine's adversarial model for RFID

Avoine's adversarial model for RFID [18] defines the adversary in the context of a specific RFID protocol as having the following capabilities: querying a tag and sending a message to it after it has received the tag's answer, sending a message to the reader, eavesdropping during an instance of the protocol between a tag and a reader, and revealing the memory contents of the tag. The latter results in the "corruption" of the tag, i.e. the other capabilities are rendered unusable after the memory contents of a tag have been revealed.
The goals of the adversary presented in Avoine's adversarial model are to "trace" an RFID tag. Avoine distinguishes between the universal, existential, and forward untraceability of an RFID protocol:

- Existential untraceability is achieved when an adversary is not able to efficiently recognize a tag it has interacted with before. The attack game proceeds as follows: First of all, three parameters are chosen. The first parameter portrays restrictions in the capabilities of the adversary. The second and third parameters dictate the maximum number of instances of the protocol in which the adversary can interact with the tags. The adversary begins by interacting with a tag chosen by the challenger in instances of the protocol chosen by them. Subsequently, they are presented with two tags, one of which is the tag from the previous step. The adversary is now able to interact with the two tags in instances of the protocol chosen by them. If the adversary can not efficiently tell the two tags apart, then the protocol is said to be existentially untraceable in regards to the parameters chosen for the attack game.
- The attack game used to prove universal untraceability is similar to the first one, although this time, the adversary is not able to choose the instances of the protocol when presented with the two tags. These will be chosen by the challenger. If the attacker is not able to efficiently tell the two tags apart, then the protocol can be said to be universally untraceable with the chosen parameters.
- Forward untraceability [19] is defined by the adversary not being able to gain information about past instances of the RFID protocol if the tag's information is revealed. This would be represented by the following attack game: the protocol instances of the tags presented to the adversary in the second step of the attack game are any instances that took place before the instances chosen by the attacker in the first step. The protocol achieves forward untraceability if the adversary is not able to achieve an advantage in distinguishing the tag they interacted with from the other one.

V. RFID Cryptography Protocols

A. OSK

Ohkubo, Suzuki, and Kinoshita [20] use randomized hash chains to achieve forward untraceability and indistinguishability of RFID tags. The protocol is based on a back-end database consisting of, for instance, the UIDs of the tags managed by the database. Whenever a reader queries the tag, the tag uses two different one-way hash functions to hash the data before it sends it. One of the hashes is then going to be sent to the reader, the other is going to overwrite the original data. This happens every time the tag is queried, leading to a different response each time. As a result of the usage of two one-way hash functions with different distributions, an attacker with knowledge of the hash functions' distributions would not be able to predict the next response of the tag or distinguish it from that of another tag. The back-end is then able to use the UIDs it stores to compute the hash chain, arriving at the data that was inside the memory of the tag. Following this, it will use the hash function the tag used before sending the response. Finally, the back-end will check if the tag's response matches that of any of its stored UIDs.

B. YA-TRAP

The Yet Another Trivial RFID Authentication Protocol [21] requires the RFID tags and compute HMACs (hash-based message authentication codes) and to be able to generate pseudo-random numbers (such a construction can be achieved through the use of an HMAC). Furthermore, the tag should be initialized with a key that acts as the identifying element of the RFID and will be used for the computation of the HMAC. Additionally, the tag needs to be initialized with an initial timestamp and a maximal value for the timestamp. The message that the reader sends to initiate the protocol contains a valid timestamp. A valid timestamp is any timestamp that is greater than that stored in the internal memory of the RFID tag. The tag will use this valid timestamp to update its internal "clock". Subsequently, the tag will use the key and the timestamp to compute an HMAC. The reader will then send the tag's response to a server, which, can then use it to search in a hash table for the tag's identifier. Since the tag's

responses are based on the timestamp, the keys of the hash table need to update each time the timestamp does.

C. Hash-based access control

Using RFID tags capable of computing a one-way hash function, Weis et al. [22] describe a protocol for locking an RFID tag. The tag stores a temporary metaID, which is the result of hashing a key associated with the tag's ID, in its memory. A tag that is in a locked state only responds with its metaID, while a tag in its unlocked state can, perhaps, enable writing rights for the reader or respond with sensitive information. For a reader to be able to unlock a tag, it can use the metaID to query a database, which then sends the key to the reader. The reader sends the key to the tag, the tag hashes it and, if the result matches the metaID, it enters the unlocked state. To lock the tag again, the reader uses a new key to create a new metaID, which it then writes onto the tag's memory.

D. Pseudonym tables

Juels [23] presents a protocol in which RFID tags cycle through pseudonyms instead of having one fixed identifier. The protocol merely requires basic mathematical and logical operations to be performed by the passive RFID tag. So as not to allow trivial cloning of the pseudonyms, the protocol incorporates a mutual authentication based on one of the pseudonyms of the tags as its first step. The tag first sends one of its pseudonyms. The reader then responds with a shared key associated with the pseudonym. If the reader has successfully authenticated itself through the knowledge of the key, then the tag responds with a shared key. Finally, after both parties have identified themselves, the reader can use a one-time pad construction to update the two shared keys and the pseudonym in the tag's memory. To prevent eavesdropping, the one-time pads are transmitted over multiple protocol instances.

E. Yoking-proof using keyed hash functions and cryptographic MACs

It is also possible, in the case of a lack of trust in readers, to apply a protocol that enables two tags to prove to a trusted third party that they have been scanned together. The yoking-proof protocol using hashes and MACs [24] requires the tags taking part in the protocol to each be initialized with a secret key known by the trusted third party. At the beginning of the protocol, a reader assigns each of the tags either the role of "left proof" or "right proof". The left tag A begins by using a keyed hash function with its secret key to hash a counter value. A sends its ID, the counter, and the hash to the reader. A's response is then redirected to the right tag B, which computes a cryptographic MAC of A's response, together with its counter, using its secret key. B then sends its ID, counter, and the MAC with the assistance of the reader to A. A then computes a MAC of its response from the second step of the protocol, together with B's response, using its secret key. As a last step of the protocol, both increment their counters. Utilizing the IDs of the two tags, their tags (before incrementation), and the last MAC that was computed by A, a trusted third party would be able to recreate the protocol and check that A and B, indeed, must have been scanned together.

VI. Evaluation

The OSK protocol has been shown to not be able to defend against denial of service in the case that the number of communication steps is limited because then it is possible to send so many queries to a tag that it breaks [25]. YA-TRAP is itself prone to a trivial denial of service attack because an adversary could guess a valid timestamp and thus send the tag's "clock" into the future, making it unresponsive to well-meaning readers. Additionally, if the timestamp (and therefore the hash table) is not updated often enough, it could become a probable scenario that a reader tries to read a tag that has already been read since the last update of the timestamp. As a possible solution, the RFID tag could answer with the HMAC for a limited amount of times when it is queried by the same timestamp, although this would allow for (limited) tracing of the tag. Using Hash-based access control a spoofing attack is possible. An adversary that queries the tag and then sends its metaID to a legitimate reader would be sent the key. This can not be prevented, although by checking the information that the tag sends after the unlocking process, it is possible to detect such a spoofing attack.

VII. Related Work

For a deeper dive into passive RFID tag cryptography, we would suggest Juels' survey of RFID security and privacy [26] as a first step. This survey has as its main focus so-called "basic RFID tags", which have even more limited computational capabilities when it comes to cryptography. As a result, solutions such as physical buttons that "kill" or let an RFID tag enter a sleeping-mode, have been proposed. Furthermore, we would recommend this 2014 survey by Mujahid and Islam [27] for gathering insight into more recent and advanced protocols for passive RFID tags. Finally, this inductive method [28] expands the adversary models presented in this survey by making the privacy proofs work for cases in which the number of communication steps grows to infinity.

VIII. Conclusion

In this survey, we offer a starting point for people inexperienced regarding RFID systems and the cryptography therein. Starting from the highest level we work our way down by firstly showcasing some applications of RFID systems in everyday life and discussing the circuitry inside passive RFID tags. After highlighting the limitations of passive RFID tags we discuss the attack games used to formalize definitions of privacy and security concerning RFID systems. Finally, we elaborated on some of the cryptographic protocols that brought RFID cryptography to life and discussed their strengths and shortcomings.

REFERENCES

[1] N. K. Singh and P. Mahajan, "Rfid and it's use in libraries: A literature review," *International Journal of Information Dissemination and Technology*, vol. 4, no. 2, pp. 117–123, 2014.

[2] T. Adame, A. Bel, A. Carreras, J. Melià-Seguí, M. Oliver, and R. Pous, "Cuidats: An rfid–wsn hybrid monitoring system for smart health care environments," *Future Generation Computer Systems*, vol. 78, pp. 602–615, 2018.

[3] M. Martinez Perez, G. Vazquez Gonzalez, and C. Dafonte, "The development of an rfid solution to facilitate the traceability of patient and pharmaceutical data," *Sensors*, vol. 17, no. 10, p. 2247, 2017.

[4] R. Want, "Rfid: A key to automating everything already common in security systems," *Scientific American*, vol. 290, no. 1, pp. 56–65, 2004. [Online]. Available: http://www.jstor.org/stable/26172655

[5] S. Preradovic, N. C. Karmakar, and I. Balbin, "Rfid transponders," *IEEE microwave magazine*, vol. 9, no. 5, pp. 90–103, 2008.

[6] M. Feldhofer and C. Rechberger, "A case against currently used hash functions in rfid protocols," in *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops: OTM Confederated International Workshops and Posters, AWeSOMe, CAMS, COMINF, IS, KSinBIT, MIOS-CIAO, MONET, OnToContent, ORM, PerSys, OTM Academy Doctoral Consortium, RDDS, SWWS, and SeBGIS 2006, Montpellier, France, October 29-November 3, 2006. Proceedings, Part I*. Springer, 2006, pp. 372–381.

[7] A. Ashry, K. Sharaf, and M. Ibrahim, "A simple and accurate model for rfid rectifier," *IEEE Systems Journal*, vol. 2, no. 4, pp. 520–524, 2008.

[8] J. Heidrich, D. Brenk, J. Essel, M. Heinrich, M. Jung, G. Hofer, G. Holweg, R. Weigel, and G. Fischer, "Design of a low-power voltage regulator for rfid applications," in *2010 IEEE Region 8 International Conference on Computational Technologies in Electrical and Electronics Engineering (SIBIRCON)*. IEEE, 2010, pp. 552–557.

[9] H. Dong, J. He, A. Kang, C. Zhang, and T. Han, "Implementation of error-correcting encoded saw rfid tags," in *2011 IEEE International Ultrasonics Symposium*. IEEE, 2011, pp. 581–583.

[10] R. Want, "An introduction to rfid technology," *IEEE pervasive computing*, vol. 5, no. 1, pp. 25–33, 2006.

[11] P. Sorrells, "Passive rfid basics," *Microchip Technology Inc*, vol. 7, 1998.

[12] J. Hu, D. Wang, and J. Wu, "A 2 kbits low power eeprom for passive rfid tag ic," *Chinese Journal of Electronics*, vol. 31, no. 1, pp. 18–24, 2022.

[13] D. E. Holcomb, W. P. Burleson, and K. Fu, "Power-up sram state as an identifying fingerprint and source of true random numbers," *IEEE Transactions on Computers*, vol. 58, no. 9, pp. 1198–1210, 2008.

[14] F. Thiesse and F. Michahelles, "An overview of epc technology," *Sensor review*, 2006.

[15] J.-W. Lee, D. H. T. Vo, Q.-H. Huynh, and S. H. Hong, "A fully integrated hf-band passive rfid tag ic using 0.18- μm cmos technology for low-cost security applications," *IEEE Transactions on Industrial Electronics*, vol. 58, no. 6, pp. 2531–2540, 2011.

[16] D. Hein, J. Wolkerstorfer, and N. Felber, "Ecc is ready for rfid–a proof in silicon," in *Selected Areas in Cryptography: 15th International Workshop, SAC 2008, Sackville, New Brunswick, Canada, August 14-15, Revised Selected Papers 15*. Springer, 2009, pp. 401–413.

[17] Q. Do, B. Martini, and K.-K. R. Choo, "The role of the adversary model in applied security research," *Computers & Security*, vol. 81, pp. 156–181, 2019.

[18] G. Avoine, "Adversarial model for radio frequency identification," *Cryptology ePrint Archive*, 2005.

[19] G. Avoine and P. Oechslin, "A scalable and provably secure hash-based rfid protocol," in *Third IEEE International Conference on Pervasive Computing and Communications Workshops*. IEEE, 2005, pp. 110–114.

[20] M. Ohkubo, K. Suzuki, S. Kinoshita *et al.*, "Cryptographic approach to "privacy-friendly" tags," in *RFID privacy workshop*, vol. 82. Cambridge, USA, 2003.

[21] G. Tsudik, "Ya-trap: Yet another trivial rfid authentication protocol," in *Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06)*. IEEE, 2006, pp. 4–pp.

[22] 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: First International Conference, Boppard, Germany, March 12-14, 2003. Revised Papers*. Springer, 2004, pp. 201–212.

[23] A. Juels, "Minimalist cryptography for low-cost rfid tags," in *Security in Communication Networks: 4th International Conference, SCN 2004, Amalfi, Italy, September 8-10, 2004, Revised Selected Papers 4*. Springer, 2005, pp. 149–164.

[24] ——, "" yoking-proofs" for rfid tags," in *IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second*. IEEE, 2004, pp. 138–143.

[25] A. Juels and S. A. Weis, "Defining strong privacy for rfid," *ACM Transactions on Information and System Security (TISSEC)*, vol. 13, no. 1, pp. 1–23, 2009.

[26] A. Juels, "Rfid security and privacy: A research survey," *IEEE journal on selected areas in communications*, vol. 24, no. 2, pp. 381–394, 2006.

[27] U. Mujahid and M. Najam-ul Islam, "Ultralightweight cryptography for passive rfid systems," *International Journal of Communication Networks and Information Security*, vol. 6, no. 3, p. 173, 2014.

[28] D. Liu, G. Yang, Y. Huang, and J. Wu, "Inductive method for evaluating rfid security protocols," *Wireless Communications and Mobile Computing*, vol. 2019, pp. 1–8, 2019.