Efficient Detecting of RFID Tag Cloning Attacks using Chaos Theory

M. Babaie, H. Rahimov

Abstract—The cloning of RFID tags can lead to financial losses in many commercial RFID applications. These days, the RFID chip manufacturers are currently focused on the former by making tags hard to clone. This paper focuses on this issue by investigating a method to pinpoint tags with the same ID. This method is suitable for low-cost tags since it makes use of writing a new random number based on chaos theory and generated by chaotic logistic map on the tag’s memory, every time the tag is scanned. A back-end that issues these chaotic numbers detects tag cloning attacks as soon as both the genuine and the cloned tag are scanned. This paper describes the chaotic method and presents a mathematical modeling and calculating prevention and detection of cloning attack in this method.

Index Terms—Chaotic, Cloning Attack, RFID, Security

I. INTRODUCTION

Radio Frequency Identification (RFID) systems are composed of three main components: tags, readers, and a database and may be viewed as a means of explicitly labeling objects to facilitate their “perception” by computing devices. An RFID tag is a small device that can be attached to products and allow for unique item identification and product description. RFID tags can be active type or passive type [1]. An RFID reader, is a calculation powerful device with ability to interrogate tags and access the database, where information about individual tags and their analogous items is stored [1], [2].

Tags contain a unique identification number called an Electronic Product Code (EPC), and potentially additional information of interest to manufacturers, healthcare organizations, military organizations, logistics providers, and retailers, or others that need to track the physical location of goods or equipment [3].

All information stored on RFID tags accompanies items as they travel through a supply chain or other business process.

All information on RFID tags, such as product attributes, physical dimensions, prices, or laundering requirements, can be scanned wirelessly by a reader at high speed and from a distance of several meters [1]-[3].

RFID has seen in the central of attention in the past few years. One important reason for this is the effort of large organizations, to deploy RFID as a tool for mechanized of their supply chains. Thanks to a combination of falling tag costs and strong RFID standardization, we are revolution in RFID usage in various industrial [3], [4].

Supporters of RFID see it as a replacement of the optical barcode familiarly printed on consumer products, with these new advantages:

1. Unique identification: A barcode shows the type of object on which it is printed. An RFID tag goes a step further. It indicates a unique serial number that distinguishes among many millions of identically manufactured objects; it might indicate. The unique identifiers in RFID tags can act as pointers to a database entries containing rich transaction histories for individual items [5]-[7].

2. Automation: Barcodes, being optically scanned, require line-of-sight contact with readers, and thus careful physical positioning of scanned objects. Except in the most exactly controlled environments, barcode scanning requires human hands job. In contrast, RFID tags are readable without line-of-sight contact and without precise positioning. RFID readers can scan tags at rates of hundreds per second. In the future, point-of-sale terminals may be able to scan all of the items in passing shopping carts [7].

This paper investigates an approach to secure low-cost RFID systems against tag cloning and impersonation based on detection of cloning attacks, an approach that is far from being fully exploited today. Instead of relying on the strength
of the weakest and cheapest devices within the system, the tags, this approach relies on the visibility the tags provide. The underlying technical concept is simple and it has already been proposed for ownership transfer and access control [8], [9]. However, it has not been included in review papers, and we think that it merits recognition. Therefore our major contribution is not the idea development itself but innovative application and thorough evaluation of the concept with respect to cloning of RFID tags.

II. DATA SECURITY IN RFID

Data security is a first important issue that needs to be explained when we talk about RFIDs security. RFIDs potential wide spread implementation in systems like authorized facility access, toll payment, retail, and many others, will with it necessary bring attempts to misuse and tamper with technology. In all these applications cloning and impersonation of RFID tags could be financially lucrative for occasional hackers or professional criminals, and severely damaging for the licit companies’ revenues and reputation. The potential losses due to security breaches are furthermore amplified by the high level of automation allowed by the technology [10].

From the point of view of RFID technology, the most challenging security threats in commercial RFID applications are tag cloning and tag impersonation. The research community addresses these threats primarily by trying to make tag cloning hard by using cryptographic tag authentication protocols [10], [11]. The fundamental difficulties of this research revolve around the trade-offs between tag cost, level of security, and performance in terms of reading speed and distance; it is not very hard to protect an RF device from cloning today, but it is extremely challenging to do it using a low-cost barcode replacing RFID tag [12]-[14]. These tags will be deployed in numbers of several millions and the end-user companies have a strong financial incentive to minimize the tag cost and thus the features the tags provide.

there are three primary issues surrounding RFID and the need to protect proprietary information:

- Data stored security on the tag
- Protecting the integrity of the tag
- Securing data related to the serial number on a tag, which stored in a network database.

None of these issues are impossible to overcome, but we can make some balance among them, and the only way to make the right decisions is to understand the options available. So discus about these issues by more detail:

A. Data stored security on the tag

In very general terms, data security is the process of protecting of data against adversaries' actions and it comprises steps of prevention, detection, and response [15]. In the following we review related work by mapping countermeasures to the three steps in the process of securing an RFID system against tag cloning and impersonation.

Detection is about minimizing the negative effects of materialized threats and increasing the adversaries' probability of getting caught. A video surveillance system is a typical example of detective measures. In some cases detection enables an immediate response that nullifies the negative effects of the materialized threat, and the result is effective prevention of the negative effects. For instance, this is the case with burglar alarms that do not immediately seize the harm from happening [17], [18].

In RFID systems, detection-based measures do not require cryptographic operations from the tags but they make use of visibility to detect cloned tags or changes in the tag ownership. The efficiency of a detection based measure is characterized by the probability to detect a threat [18].

Response is what happens after a materialized threat is detected. It comprises of all the actions that minimize the negative effects for the process owner [3] and maximize the negative effects for the adversary in terms of punishments. In commercial RFID applications this can mean, for example, confiscation of the illicit goods, prosecution of the illicit players on contract breaches and illegal activities, and ending business relationships [17], [18].

B. Protecting the integrity of the tag

Physical protection of both goods and systems predecessors of RFID was a problem that companies had to deal with for years, even before RFID. Even though this has been with us for so many years, it still inflicts great damage. Possible bad case scenarios with this issue are physical removal/damaging of the tag and 'killing' of the tag. the way to do this, is to ensure that everyone who handles these devices is educated and handles the tags with care [11]. It is also a good idea to check the material handling devices for
proper maintenance. Many box clamps or appliance clamps have rubber bumpers. These inevitably become worn and can present a hazard to your tags due to breaks in the surfaces causing “pinch points” on product. Ensuring that there is enough pressure to hold the product in these devices is critical, but this needs to be balanced with good sense. The more pressure that is applied to the product, the higher chance there is of damaging it and the attached tag [11], [12].

A carrier who is improperly handling the product can damage tags by crushing them, scrubbing them, or getting them wet. For products that are subject to rough handling during shipping, tag ruggedness should be a consideration during design selection. There are labs that perform this kind of testing, or if the time and equipment are available to the organization, limited tests can be performed internally [11].

C. Securing data related to the serial number on a tag

One of the solutions to a problem of unauthorized data reading from the tag, is to keep the information related to the product not on the tag itself but in some sort of database. This database is then connected through Internet or intranet to the readers or other devices that need access to it. Data that is stored in this database can range from usual product specifications to encryption algorithms or keys used on specific tags, and other. Most problems that could occur in this perspective are very familiar to IT experts because they are dealing with them regularly in network-databases environment that doesn’t necessarily need to be RFID related (e.g. financial service industry with its databases). The most highlighted problem is that of unauthorized access to the data in the database.

III. CHAOS THEORY AND LOGISTIC MAP

The name "chaos theory" comes from the fact that the systems that the theory describes are apparently disordered, but chaos theory is really about finding the underlying order in apparently random data.

The nonlinear dynamics researchers have observed an interesting relationship between chaotic behavior and Random number generator systems as many properties of the chaotic systems such as their sensitivity to initial conditions can be considered to the confusion in generation of secret keys. [12] Deterministic pseudorandom numbers are used for the generation of secret key in cryptography system. Thus, defining a novel PRNG with better condition can be useful in many areas including security systems simulation methods, etc.

The logistic map is a very simple mathematical model often used to describe the growth of biological populations. In 1976 May showed this simple model shows a definitely interesting behavior. The simple mathematical form of the logistic map is given as [13]:

\[ f(x_n) = x_{n+1} = r \cdot x_n \cdot (1 - x_n) \quad (1) \]

Where \( x_n \) is the state variable being in the interval \([0, 1]\) and \( r \) is system parameter which might have any value between 1 and 4. [12]

In the next section, we describe a novel chaotic method to improving data security in RFID tag and then present a mathematical model to calculate the prevention and detection of cloning attack in our proposed method.

IV. PROPOSED METHOD

The available methods to secure low-cost RFID tags from cloning are limited. In particular, cryptographic approaches proposed in the literature cannot be used with the existing standard UHF tags since they require changes in the chip’s integrated circuit, and existing detective measures do not perform well under limited visibility [14].

The presented method makes use of the tag’s rewritable memory. In addition to the static object and transponder identifiers (e.g. EPC, TID [15]), the tags store a chaotic random number that is generated by chaotic logistic map, changed every time the tag is read.

In the proposed method we use of chaotic system, that have deterministic features in the microscopic space and behave randomly in a coarse grained state space. This chaotic map is sensitive to initial conditions (cf. section 4) in this section we describe the logistic chaotic map with some properties. It’s make it optimum candidates to relate minimal critical information about the input, in the output sequence. Logistic chaotic map is fast computable and this is able to create sequence with extremely long cycle length as more accuracy in decimal number [16].

We denote this number a synchronized secret since it is unknown to all who do not have access to the tag and it can also be understood as a one-time password. A centralized back-end system issues these numbers and keeps track of which
Every time a tag is read, the back-end first verifies the tag’s static identifier. If this number is valid, the back-end then compares the tag's synchronized secret to the one stored for that particular tag. If these numbers match, the tag passes the check, otherwise an alarm is triggered. After the check, the back-end generates a new synchronized secret that the reader device writes on the tag. If a tag has an outdated synchronized secret, either the tag is genuine but it has not been correctly updated (desynchronization) or someone has purposefully obtained and written an old secret to the genuine tag (sophisticated vandalism), or the genuine tag has been cloned and the cloned tag has been scanned. Since unintentional desynchronization problems can be addressed with acknowledgments and the described form of vandalism appears somewhat unrealistic in today’s commercial RFID applications, an outdated synchronized secret is as a strong evidence of a tag cloning attack. If a tag has a valid static identifier but a synchronized secret that has never been issued by the back-end, the tag is likely to be forged. An outdated synchronized secret alone does not yet prove that a tag is cloned; if the cloned tag is read before the genuine tag after cloning attack occurred, it is the genuine tag that has an outdated synchronized secret. Therefore an outdated synchronized secret is only a proof that tag cloning attack has occurred, but not a proof that a tag is cloned.

In this paper we presented our method with a chaotic random number generator. Most of the existing (PRNGs) pseudorandom number generators are based on a linear generator that is defined by:

$$x_n = (a_1 x_{n-1} + ... + a_k x_{n-k}) \mod m$$

where the modulus $m$ and the order $k$ are positive integers and the coefficients $a_i$ belong to $\mathbb{Z}_m = \{0,1,\ldots,m-1\}$. As a result, the presented method pinpoints the objects with the same identifier but it still needs to be used together with a manual inspection to ascertain which of the objects is not genuine. In addition to knowing that a cloning attack has occurred, the back-end can pinpoint a time window and a location window where the cloning attack happened. Thus the method makes it also hard to repudiate tag cloning to parties who handle the tagged objects. This is a security service that preventive measures do not provide and it can support the responsive actions.

Now we evaluate the level of security of the presented method with a statistical model. We assume a system which consists of a population of tags that have a static identifier and non-volatile memory for the synchronized secret. The tags are repeatedly scanned by readers that are connected to the back-end. The probability that a tag will be scanned sometimes in the future at least once more is constant and denoted by $\alpha$; when a tag is scanned its synchronized secret is updated both on the tag and the back-end. The time between these updates for a tag is denoted by a random variable $I_{\text{update}}$. An adversary can copy any tag in the system and inject the cloned tag into the system. The time delay from the copying attack to when the copied tag is scanned is denoted by a random variable $I_{\text{attack}}$. In addition, an adversary can try to guess the value of the synchronized secret. In our presented method with using of logistic chaotic map to generating random numbers, the chance of guess synchronized secret in the tag by an adversary very low and it’s because of nonlinear dynamical system that there is in logistic map.

The system’s responses can be statistically analyzed. First, the probability to successfully guess a genuine tag's synchronized secret is $1/2^H$, where $H$ denotes the length of the synchronized secret in bits. Second, when a copying attack occurs, three mutually exclusive outcomes are possible:

- **Case 1:** The genuine tag is scanned before the copied tag and an alarm is thus triggered when the copied tag is scanned.
- **Case 2:** The copied tag is scanned before the genuine tag and an alarm is thus triggered when the genuine tag is scanned.
- **Case 3:** The genuine tag is not scanned anymore and thus no alarm is triggered for the copied tag.

In Case 1 the cloned tag is detected as soon as it is scanned the first time and the negative effect of the attack can be prevented. In Case 2 the cloned tag passes a check without raising an alarm but the system detects the cloning attack when the genuine tag is scanned. In Case 3 the security fails and the cloning attack goes unnoticed [19], [20]. The system's level of security is characterized by the probability of Case 1 that tells how often threats are prevented, and by the probability of Case 1 or Case 2 that tells how often threats are detected.
\[ \text{prevention} = \text{prob(Case1)} \]
\[ \text{Detection} = \text{prob(Case1 \lor Case2)} \quad (2) \]

The probability of Case 1 equals the probability that the genuine tag is scanned at least once more, multiplied by the probability that the genuine tag is scanned before the cloned tag. Let us assume that the time when the cloning attack occurs is independent of when the genuine tag is scanned and uniformly distributed over the time axis, so the average time before the genuine tag is scanned after the copying attack is \(\frac{I_{\text{update}}}{2}\) we can establish probability of Case 1 as follows:

\[ \text{if } (T = \frac{I_{\text{update}}}{2} - I_{\text{attack}}) < 0 \quad (3) \]
\[ \text{prob}(\text{Case1}) = \alpha \cdot \text{prob}(T) \quad (4) \]

We can conclude of equation 2 that is noticed in section 3:

\[ \text{probability}(K): \{ \text{if}(x_1, x_2, \ldots, x_n \rightarrow x_{n+1}) \} \quad (5) \]

\[ \text{probability}(\text{Case1}) = \alpha \cdot \text{probability}(T) \cdot \text{probability}(K) \quad (6) \]

Assuming that \(I_{\text{update}} \sim N(\mu_{\text{update}}, \sigma_{\text{update}}^2)\)

and \(I_{\text{attack}} \sim N(\mu_{\text{attack}}, \sigma_{\text{attack}}^2)\) we can establish the probability of case 1 using a new random variable \(Z = \frac{I_{\text{update}}}{2} - I_{\text{attack}}\) as follows:

\[ \text{prob}(\text{Case1}) = \alpha \cdot \text{prob}(Z) \quad (7) \]

And, so we have:

\[ Z = N\left( \frac{\mu_{\text{update}}}{2} - \mu_{\text{attack}}, \frac{\sigma_{\text{update}}^2}{4} - \sigma_{\text{attack}}^2 \right) \quad (8) \]

Equation 3 shows that the level of security of the synchronized secrets method depends on the frequency in which the genuine tags are scanned with respect to the time delay of the attack, and on the probability that the genuine tag is scanned once more. The same finding is confirmed from equations 4 and 5 which show more clearly that, in the case of normally distributed time variables,

\[ \lim_{\mu_{\text{attack}} - \mu_{\text{update}} \to \infty} \text{probability}(\text{Case1}) = \alpha \]

After the last transaction of the genuine tag, a single cloned tag will always go unnoticed (Case 3). We assumed above a statistically average adversary who does not systematically exploit this vulnerability. However, a real world adversary who knows the system is not likely to behave in this way. Therefore this vulnerability should be patched by flagging tags that are known to have left the system.

V. CONCLUSION

Detecting cloned RFID tags appears attractive for securing commercial RFID applications since it does not require more expensive and energy thirsty cryptographic tags. This paper presents chaotic synchronized secrets method to detect cloning attacks and to pinpoint the different tags with the same ID. The presented method requires only a small amount of rewritable memory to writing random number in the tag but it provides a considerable increase to the level of security for systems that use unprotected tags. So we describe our method by mathematical modeling and calculating prevention and detection of cloning attack in this method.

ACKNOWLEDGMENTS

This article was supported by the Student’s Research center of Shahrood University of Technology.

REFERENCES


Majid Babaie was born in 1988 in Iran/Tehran and he’s a bachelor student university in SUT and Became a Member of ISC in 2010. He published some paper in creditable journals and conferences about information security and cryptography in 2010.