Detecting Cloning Attack in Low-Cost Passive RFID Tags

An Analytic Comparison between KILL Passwords and Synchronized Secrets

Obinna Stanley Okpara
(M00425161)
School of Science and Technology
Middlesex University, Mauritius Campus
OO749@live.mdx.ac.uk

Abstract **- Radio Frequency Identification (RFID) technology plays an important role in many sectors today without assuredly taking care of privacy and security issues. One of the most prevalent security issue in RFID is the cloning attack on tags. Most countries now use RFID as a means of verification in electronic passports (e-passports). A terrorist that is able to successfully clone the RFID tag on a passport document can gain unauthorized entry to a target country without detection. Hence, securing an RFID tag against cloning has become a compelling subject. The hardware limitation of low-cost passive RFID tags makes security a more difficult task. This paper analytically compared two methods to detect tag cloning. These methods are the KILL password and synchronized secret.**

Keywords — RFID, tags, cloning, Transponder ID, KILL password, synchronized secret.

I. INTRODUCTION

The potential areas of the application of Radio Frequency Identification (RFID) technology were until recently, only partially cognized. The technology has forayed into various industries as a tool for object identification. Ni [1] described how as a tracking tool, RFID can be used to track things like pet's location, goods in shopping malls, airport luggage, golf balls in a large course etc. This technology is not just a tool for tracking objects. As a facilitator of pervasive computing, RFID plays a pivotal role in connecting tangible objects to networks and databases by utilizing sensors and actuators to carry out everyday activities. Lately, it has been used as a physical access control solution in hotels [2], as an anti-theft system in Casinos [3], as a billing system in toll gates [4], as a mobile payment system in fuel stations [5] and for medication management in healthcare [6].

In all the applications of RFID technology mentioned, cloning of RFID tags is fiscally incenting to professional criminals and hackers. This could result to damage in reputation and enormous financial losses for the corporations concerned. George highlighted that the high level of automation allowed by the technology additionally intensifies the possibility of security breaches [5]. For instance, the use of RFID to transfer data wirelessly in the current biometric passport leaves serious loopholes to illicit change of ownership [3].

Therefore, security is no longer added luxury in RFID, it has become a necessity. BNP Media stated that from the RFID perspective, the most prevalent security threat in its application is tag cloning [2]. The fundamental reason for this rampant weakness lies in the trade-offs between level of security and tag cost; the distance the RFID reader can scan the RFID tag from and at what speed it can check the information on the database. Experts acknowledged that it is not difficult to secure an RFID tag from cloning, but it is an exceptional task to do it with a cheap barcode-replacing RFID tag [1]. Passive tags cost between USD0.15 to USD5.00. Companies go for low-cost passive RFID tags as a bid to minimize expenditure, so the tag's hardware constraint introduces even more complex security issues.

Mostafa and Ira developed a system to implicitly enforce RFID tag authentication using KILL passwords [7]. The KILL passwords were based on combining unique passwords with varying power levels required to "insufficiently kill" RFID tags. With the use of synchronized secrets, Mikko and Daniel [8] presented a method to identify different tags based on a unique Transponder Identifiers (TID). This paper critically analyzes these two systems to detect tag cloning by highlighting the strength and weakness of each model.

The rest of the paper is organized as follows. Section II provides a background on studies done to prevent cloning in low-cost RFID tags. A sampling of two approaches was done in Section III before objectively discussing the pros and cons of the approaches in Section IV. Finally, a conclusion will be drawn on the work done in Section V.

II. BACKGROUND

Similar to barcode technology, RFID is regarded as an Automatic Identification and Collection (AIDC) technology. Schmidt and Lars detailed that this technology is better and more efficient than barcode technology because it does not require direct line of sight to function [9]. RFID systems comprise of tags that are attached to objects, readers that scan and write data on the tags, and backend systems that store data. When a reader is in the range of a tag, a tag responds with its unique numeric identifier [3], called a transponder ID (TID). Unlike high-cost active tags that have inbuilt batteries, passive tags are powered by electromagnetic waves emitted from readers. These tags can operate on the 5.8 GHz, 2.45 GHz and a few other radio frequencies [5]. Figure 1 illustrates the architecture of an RFID system.

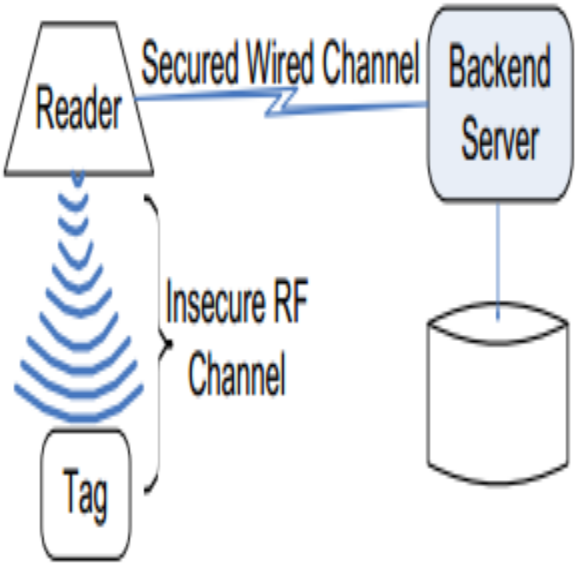

Figure 1: RFID System Architecture *[10]*

When data on a genuine tag is copied to an empty tag, a false identity is created. This is known as the tag cloning attack. In the absence of extra security measures, low-cost passive RFID systems are highly susceptible to cloning attacks. An RFID tag that can be easily modified or cloned without detection is said to lack integrity [10]. Integrity can be easily sabotaged if the verification scheme has been wrongfully eschewed or bypassed. In reaction to this, a lot of research has been done on how to detect and prevent tag cloning in an RFID system.

Quite a number of papers proposed to counter the earlier stated threat by implementing cryptographic protocols in the RFID system. One paper, proposed a model called Semi-Randomized Access Control (SRAC) [11]. SRAC relies on the reader and backend having sufficient resources to utilize strong symmetric or asymmetric key algorithms to secure the reader-backend communication. The flaw with this system is that it cares only about the tag-reader communication because it assumes that the reader and backend are one. However, this is not so in most RFID systems. So even though the system makes use of a cheap tag, the reader and backend integrated into one will be more costly than a normal split system.

Lee came up with a hash-lock protocol, where a tag is programmed to reply to a reader's query by generating a hashed value of its TID [12]. The reader will then check with the backend to verify if the tag replied with the correct value. It can be reasoned that this approach has a tag-reader, reader-backend synchronization problem. Scalability was another issue associated with this method. Furthermore, because of the hardware limitation, using symmetric and asymmetric key encryption will badly slow down an RFID system. So using cryptographic protocols did not meet the security or operational requirements of passive low-cost RFID tags.

Luck and Jacky developed a technique to detect tag cloning called Deckard [13]. This system uses the paradigm of Intrusion Detection System (IDS). Deckard applies statistical methods to look for anomalies. Anomalies in the card holder's behavior. The system however, does not necessarily detect if a tag has been cloned, it focuses on if a genuine tag is being used by an authorized person. The main shortcoming is its high false alarm rate. For example, if an employee is replaced by another employee, even though the old employee's tag was legitimately given to the new employee, Deckard will still raise an alarm.

A method that applies digital watermarks was proposed [14]. This technique applies the concept of watermarking in multimedia where information can be embedded in a document to prevent and detect copying and modification. It has potentials to detect cloning of RFID tags. Watermarking does not only have the ability to detect cloning in RFID tags, it is capable of detecting data manipulation in a genuine tag. The underlying watermark is undetectable by merely looking at the tag. The cost of creating such a tag is the main concern. The higher cost of production means watermarked tags do not directly fall under the category of low-cost passive tags.

Having looked at various works that have been done to detect tag cloning in low-cost passive tags, two techniques stood out. These techniques are the KILL Password [7] and Synchronized Secret [8]. The two methods do not require any change in the normal RFID infrastructure or extra system resources. Additionally, neither symmetric nor asymmetric cryptographic key algorithms were used. This means the problem of speed and feasibility do not apply to these methods. The next section of this paper samples these approaches in detail.

III. SAMPLING OF APPROACHES

A. KILL Password

Tag killing was developed because of consumers' privacy concerns. There were complaints from the public that large commercial outfits like Wal-mart and Shoprite can track customers with the tags attached to goods [15]. So the idea to kill tags after purchasing products that have RFID tags was born. According to electronic product code global (EPCGlobal), which is the universal RFID standard, killing a tag permanently disables the tag [5]. However, a study revealed that when a reader issues the KILL command, it only zeroes out a tag's memory bank [3]. Furthermore, it is possible for programmers to reprogram the tag and bring it back to life. Researchers [7] saw it as a possibility of using this feature to prevent and detect tag cloning in low-cost RFID tags.

During the process of killing a tag, any error detected will either take the tag back to an arbitrary state or keep the tag in its current state. If no errors are identified during this process, the tags moves on to be killed. Figure 2 below depicts this procedure.

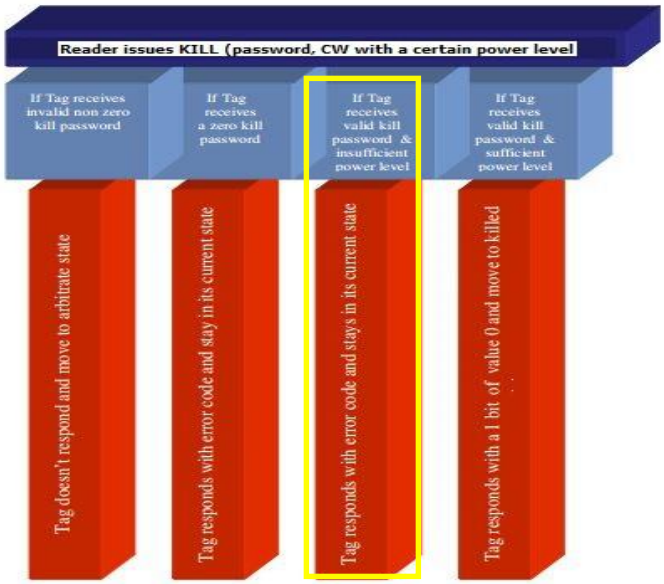

Figure 2: KILL Command Operation *[7]*

The EPCGlobal standard implied that when an RFID tag receives a correct password with a power level that is insufficient to kill a tag, it replies with an error code [7]. Hence, the reader's response tacitly verifies the tag's authenticity. If a tag sends a wrong password through the KILL command operation, the reader will not respond at all. The key in this technique is that the tag must be programmed with the correct password and just about the right amount of power to *insufficiently kill* the tag. Mostafa and Ira described that for tag authentication to take place instead of the actual killing of the tag, the tag needs to request the appropriate amount of power from the reader [7]. This is even more owed to the fact that different tags require different power levels to effectively carry out this authentication. Figure 3 below shows a snapshot of GV RFID software.

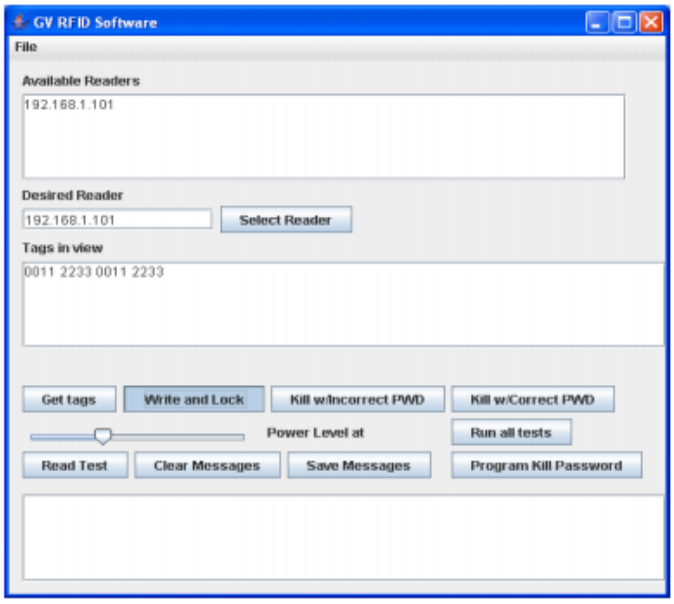

Figure 3: Tag Programming Interface *[7]*

GV RFID software, a Java Application Programming Interface (API) can be used to program a reader to authenticate tags with a certain password and proper power level.This technique has two phases, the first takes place in the RFID reader side, the second takes place in the RFID tag side. Both sides have to be configured to match.

B. **Synchronized Secret**

This method utilizes the tag's rewritable memory during the authentication process. Along with the static object and TID, the tag saves a pseudorandom number that changes every time the reader does a scan. This randomly generated number is unknown to persons that do not have physical access to the genuine tag. Since it has to be the same on the tag and the backend, Mikko presented it with the term "synchronized secret" [8]. Mikko went further to liken this number to a one-time password. In this technique, a centralized backend database issues and keeps track of these secrets. To avoid tag management errors, a location and time stamp is used to track which digits are written on which tag.

First of all, a reader scans a tag and verifies the TID with the backend. If the tag provides a valid TID, the backend goes ahead to check if the tag's synchronized secret matches with the one associated with that particular tag. If these two numbers match, i.e. the TID and synchronized secret, the tag is genuine. In other words, the tag passed the authentication process. If the numbers are not valid, then the reader will detect an error that will trigger an alarm. The principle of detecting tag cloning with synchronized secrets is illustrated in Figure 4.

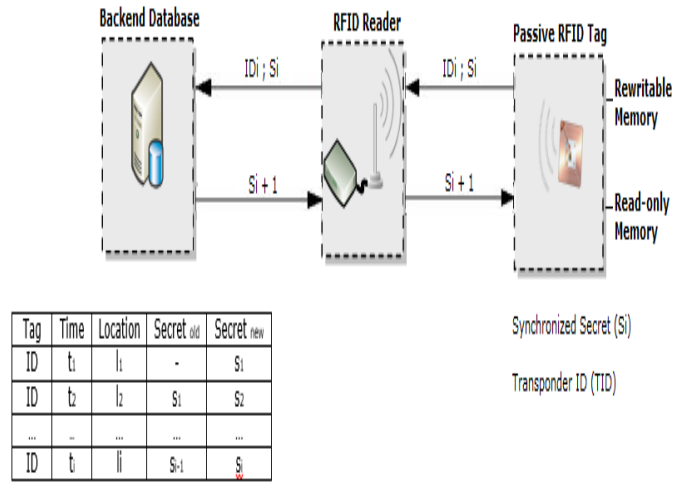

Figure 4: Illustration of Synchronized Secrets *[8]*

After successful passing the check, a new secret is generated and stored by the backend. The backend does not wipe off the old secret. This is done to check if a tag failed to pass because

it is cloned or simply because of a synchronization error. After authentication, a new synchronized secret is written on the tag by the reader. Although a possibility, outdated synchronized secrets do not outrightly mean cloning has occurred.

One possibility can be that the reader did not complete the writing process (update) of the new secret on the tag. In such a scenario, even if the tag is genuine, it will still have an old secret (this is known as de-synchronization). To address this defect, it was decided to implement acknowledgments (ACKs) to confirm that the tag secret update occurs successfully. After verification, a tag sends an ACK to the reader that it has synchronized and has the new secret. In response, the reader sends an ACK to the backend that it got the ACK message from the tag. Finally, the backend sends its ACK message to the reader to confirm the whole acknowledgement process has been successfully completed. This can be somewhat likened to the Transport Control Protocol (TCP) three-way handshake. See Figure 5 below.

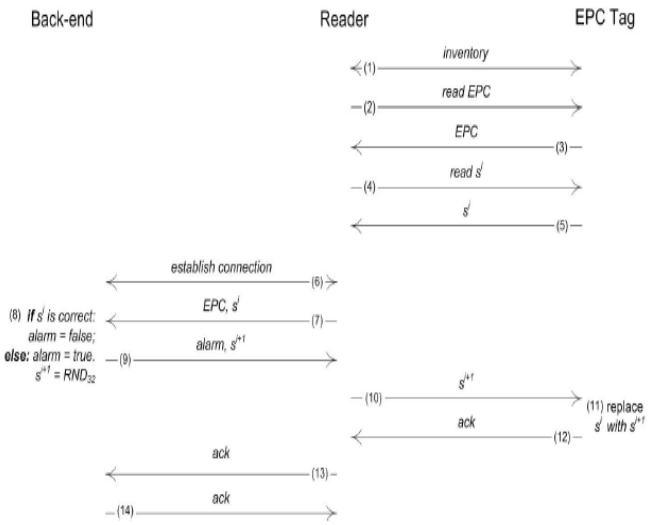

***Figure 5: Tag Synchronized Secret Update with ACK** [8]*

Another likelihood is that an individual has intentionally written an old secret to a genuine tag. Such an attack is known as sophisticated vandalism. This scenario is seemingly impractical for some reasons. If an external attacker or a disgruntled employee gets hold of a genuine tag that has the new secret written on it, it will be senseless to try to write an old secret on the tag. The attacker would rather write the new secret on a fresh tag. Due to the elimination of synchronization errors by ACKs and the impracticality of sophisticated vandalism in the application of RFID today, an outdated secret is proof that tag cloning has occurred. Additionally, a tag is likely to have been forged if it has a secret that has never been generated by the backend.

IV. DISCUSSION

In the synchronized secret technique, it takes time for a tag's new secret update to take place. This time is known as Tupdate [8]. In a system that caters for only a few tags, this might not be an issue. On the other hand, there will be noticeable delay in an RFID system that needs to authenticate a large number of tags within a short period of time. It can be said that the introduction of ACK messages has eliminated the possibility of de-synchronization errors, but it still does not ensure that the ACKs will be received in minimum time. Factors like the distance between the reader and backend, the presence of electromagnetic interference (EMI) can affect the ACK transmission time. In essence, synchronized secrets will not be an efficient method in RFID applications where high rate of tag authentication occurs. One of these RFID applications is the RFID tolling system. Still, making the ACK packet as short as possible can go a long way in resolving this issue.

In the KILL password method, the communication between the tag and reader occur at a faster rate compared to the synchronized secret. The reader has to check for the accuracy of the password from the backend only once in a single authentication process. After that, the backend is no longer directly involved in the tag authentication and KILL command process [7]. This results in a relative increase in authentication rate.

One of the hardware constraints of a low-cost passive tag is that it does not have a user defined memory space. So for a system to use the synchronized secret methodology in a cheap tag, one has to overwrite the 4bytes reserved for the access-password with a synchronized secret [8]. The access-password can be completely or partly overwritten, depending on the length of the desired synchronized secret. The longer the secret, the more secure the system, but the more time it will take to transmit. A decision has to be made based on the area of use and the administrator's preferences. In other words, synchronized secret requires a certain level of configuration to function properly.

KILL passwords also require a degree of configuration. As a security measure, an administrator might decide to change the default passwords on the tags. Overwriting is not needed since the technique makes use of the tag's access-password. The main configuration in KILL passwords takes place when selecting the appropriate power level to activate the KILL command. It was inferred that different tags require different power levels to respond with the "insufficient to kill" message [7]. Therefore the administrator needs to know the amount of decibels (dB) to configure on the tag. The configuration will enable the reader know how much power to emit to produce the required response from the tag.

In terms of downright security, it can be argued that the KILL password is more secure to tag cloning attacks. This is because the KILL command technique carries out authentication based on three criteria. These are the TID, the password and the power level. In comparison, synchronized secrets make use of only the TID and a secret. The extra layer of security in the KILL technique suggests that it can be more resistant to cloning attacks. However, an extra layer of security does not necessarily guarantee more security.

If weak passwords are used an RFID system that uses KILL passwords and the attacker is able to determine the required power level, the added security layer might not be able to detect or prevent the attack. Therefore, the KILL password largely depends on the strength of the password used and the unpredictability of the required power level. The area the RFID system is to be used impacts the question of which approach is more secure. The approaches discussed have different pros and cons. Table 1 below summarizes their strengths and weaknesses.

Table 1: Comparing KILL password and Synchronized Secret

	KILL password	**Synchronized Secret**
Speed	Fast	Slow
Config ease	More Complex	Less Complex
Cloning resistance	More Secure	Less Secure

Due to the unique setup of each approach in the process of detecting tag cloning, both might leave the system vulnerable to one or more other possible attacks. Table 2 below shows the level of vulnerability using both methods exposes an RFID system to.

Table 2: Vulnerability Table

Vulnerability	**KILL password**	**Synchronized Secret**
Denial of Service (DoS)	Less Susceptible	More Susceptible
Timing Analysis	Less Susceptible	More Susceptible
Replay attack	More Susceptible	Less Susceptible
Malicious code injection	More Susceptible	Unsusceptible
KILL command attack	Susceptible	Unsusceptible

V. CONCLUSION

RFID systems are now used in very sensitive areas like Immigration Services. As a result, the issue of securing RFID systems can longer be ignored or over emphasized. Cloning attacks have been prevelant amongst others over the years. This paper critically analyzed the two main methods of detecting cloning of low-cost passive RFID tag which are KILL passwords and synchronized secrets. Several factors where considered to determine which method will work best in which scenario. The area the RFID system is to be used largely determines the effectiveness of the chosen method.

VI. REFERENCES

[1] L. M. Ni, D. Zhang and M. R. Souryal, "Mobile RFID Tracking System," *IEEE Wireless Communications*, vol. 18, no. 2, pp. 45-51, 2011.

[2] BNP Media, "Profile: CityCenter hotels opt for Kaba's RFID lock systems," *Casino Journal*, vol. 25, no. 2, p. 34, 2012.

[3] R. M. Chris, "Radio frequency identification (RFID)," *Computers & Security*, vol. 25, no. 1, pp. 18-26, 2006.

[4] Internet of Things (IOT), Internet of Things: International Workshop, Changsha: Springer, 2012.

[5] R. George, Networked RFID: systems, software and services, London: Springer, 2008.

[6] W. Yao, W. Yao, C.-H. Chu, C.-H. Chu, Z. Li and Z. Li, "The use of RFID in healthcare: Benefits and barriers," in *IEEE International Conference on RFID-Technology and Applications*, Orlando, 2010.

[7] M. Mostafa, E. Said, I. Woodring, "An Empirical Study for Protecting Passive RFID Systems against Cloning," in *Sixth International Conference on Information Technology*, Las Vegas, 2009.

[8] D. O. A. I. a. F. M. Mikko Lehtonen, "Securing RFID systems by detecting tag cloning," *Pervasive Computing*, pp. 291-308, 11-14 May 2009.

[9] S. Malte and T. L. a. S. Matthias, "RFID and barcode in manufacturing logistics: interface concept for concurrent operation," *Information systems management*, vol. 30, no. 2, pp. 100-115, 2013.

[10] J.-l. A. M. S. Y. Mohd Faizal Mubarak, "Trusted anonymizer-based RFID system with integrity verification," in *7th International Conference on Information Assurance and Security (IAS)*, Melacca, 2011.

[11] I. H. E. A. C. A. K. a. H. D. Jalal Awed, "RFID protocols," in *International Conference on Innovations in Information Technology*, Al Ain, 2008.

[12] L. Kaleb, "A Two-Step Mutual Authentication Protocol Based on Randomized Hash-Lock for Small RFID Networks," in *Fourth International Conference on Network and System Security*, Melbourne, 2010.

[13] L. M. a. J. Hartnett, "Deckard: A System to Detect Change of RFID Tag Ownership," *International Journal of Computer Science and Network Security*, vol. 7, no. 7, pp. 89-98, 2007.

[14] Kim. J. a. Kim. K, "Anti-counterfeiting solution employing mobile RFID environment," *World Academy of Science, Engineering and Technology*, vol. 8, no. 1, pp. 141-144, 2005.

[15] G. Michael, "Walmart reading RFID tags in Texas" *Supermarket News*, vol. 52, no. 19, p. 61, 2004.