Journal of Mobile, Embedded and Distributed Systems, vol. V, no. 1, 2013
ISSN 2067 – 4074

Electronic Wallet and Access Control Solution Based on RFID MiFare Cards

Stefan-Victor LEFTER
IT&C Security Master
Department of Economic Informatics and Cybernetics
The Bucharest University of Economic Studies
ROMANIA
stefan.v.lefter@gmail.com

Abstract: With the advent of Radio Frequency Identification technologies or RFID for short, different types of products and security-relevant applications have been developed for use in fields and businesses like: inventory management, product tracking, access control, passports or transport fare collection. Even though RFID has been around for quite some time, there are some types of businesses like theme parks, water parks or music festivals that haven't yet tested the benefits that this technology brings.
This paper focuses on presenting advantages and disadvantages of using an unified access control and electronic wallet system based on RFID cards like MiFare tags as an alternative to existing ticket/currency access and payment systems employed by the majority of the businesses mentioned above.

Key-Words: RFID, NFC, contactless smartcard, electronic wallet, controlled access, theme parks, music festivals

1. Introduction

Controlled access locations like theme parks, water parks or music festivals are places where large crowds of people gather to have fun and relax. Since theme parks can have on holidays around 70000 [1] visitors a day, making sure every visitor has a great time has become a real challenge for park owners and event organizers.
Without replacing the current access and payment systems based on paper tickets and local currency, the businesses mentioned above won't be able to sustain the continuous growth of visitors while at the same time maintaining a high level of customer satisfaction.
One alternative to the issues these businesses face is a RFID access control and payment system. In the next few pages we will present such a system along with its advantages and disadvantages, and offer countermeasures that can eliminate some of the disadvantages.

2. Problem Definition

On a busy day a theme park can have as many as 70000 [1] visitors. Some of the biggest music festivals accommodate even more than 100000 visitors a day [3]. At such locations people go on rides, buy merchandise of different sorts and serve foods and drinks. Thus, the use of a ticket access system combined with a currency or chips based payment system for locations that attract such large crowds has become a logistical problem. For example, queue times on theme parks attractions can reach 90 minutes per ride on the busiest of days [1]. For on-site shops and restaurants, queue times are slightly smaller but not by much. Some studies have shown that more than half the time spent by people at an amusement park will be spent on queues [4].
Long queues aren't the only problem that arises when currency is used as a payment system. The risk of theft or losing money is a problem that park visitors or festival goers must avoid. Since people go to theme parks or music festivals to enjoy themselves, having to make sure your money is safe is a concern that can reduce a visitor's satisfaction. The processing and handling of money is a problem not only to the visitors of the park or festival but also to the organizers or the owners of the venue. If money is used as a payment

system, there is also a risk that employees of the theme parks/music festivals might steal money that they receive from clients that paid for food, drinks or rides. This problem has been addressed by the introduction of tokens as a substitute for money.
If tokens are used as payment system risks to the organizer of the event/owner of the theme park are eliminated. All the risks and problems of using money still apply to customers and visitors when using tokens. Tokens don't replace money for good since visitors have to exchange money for tokens on-site and actually generate 3 more problems.
They generate an additional queue when visitors exchange money for tokens, they set a fixed price for services since a token's value is fixed and if a visitor runs out of tokens, the only way to get more tokens is by standing in line at the exchange queue.
To reduce queue times, increase customer satisfaction and provide a safe and reliable way to pay for attractions, products, food and beverages, controlled access locations like the ones mentioned above must use different access and payment solutions than the classic paper ticket and local currency.
Until now, no other payment system has met the requirements imposed by theme parks, water parks or music festivals of providing a reliable, safe, easy and fast way to pay for goods and services inside a controlled access location.

2.1 Similar businesses solutions

A business similar to theme parks or music festivals is represented by the ski industry. Ski resorts have similar needs as theme parks or music festivals. Ski-lift access is granted only to skiers that pay for this type of service. Some skiers want more lifts while other want fewer lifts. Controlled access to ski-lifts was put in-place through the use of access turnstiles much like the systems used at theme park rides. Since skiing takes place on mountains, in the winter season, the use of money to grant access on lifts wasn't an option. Ski resorts needed a way to grant ski-lift access without forcing skiers to remove their gloves. The solution was using a RFID system. RFID tags can be kept in skier's pockets while access turnstiles are fitted with tag readers. Since tags have non-volatile memory for storing information, the number of lifts bought by a skier is kept on the tag. When the skier comes close enough to the access turnstiles the tag is read by the readers. If the skier has ski lifts on the tag, the access turnstile folds and lets the skier access the lift. When the tag is read by the reader the information on the tag is also updated. The reader acts as a writer and deducts a lift from the skier's total number of lift rides.
The system has proven so successful that you rarely find a ski resort that still uses barcode tickets for ski lift access.
Urban transport fare collection is another use case where RFID systems have had many successful implementations. Most urban transport systems have been using paper tickets since the beginning of their service proving it to be a reliable and secure system. The reasons why this system was replaced by RFID systems are based on economic and ecological grounds. A paper ticket can be used a limited number of times, thus generating recurring fixed costs for the transport authority. A RFID tag can be rewritten an unlimited number of times, so it can be used as a ticket without generating recurring costs. Since tags are made of plastic they are more environmentally friendly than paper tickets. The RFID fare collection systems are organized as an electronic wallet system that can be filled with transport fares time and time again. Based on the transport vehicle in use, collection readers are placed either in vehicles or at transport stations.
Having all of the enumerated advantages and being implemented with great success in similar businesses, RFID systems represent a great opportunity for theme parks and music festivals to resolve the problems we have identified.

3. Proposed solution

What we have to offer to businesses like theme parks and music festivals is an RFID system based on MiFare Classic 1k

ISSN 2067 – 4074

tags that unifies the access control and electronic wallet components.
The full hardware layer consists of the following components:

- MIFARE Classic 1k tags
- ACR122U RFID readers
- Host PCs

The software layer of the system is made up of:

- An Access Microsoft Windows desktop application
- A Wallet Microsoft Windows desktop application
- An Admin Microsoft Windows desktop application
- A SQL Server 2012 Express Edition instance.

3.1 The Access Application

The places where the parks and music festivals are located usually have gates where tickets are verified and visitors are granted access. Usually, tickets are bought online and send by post to customers. Instead of tickets, tags can be sent in their place, with their electronic wallet preloaded with points bought on the park's/festival's website. At the entrance of the park/festival access will be smoother as the gates will be fitted with tag readers. Ticket checking is a manual job through which the anti-counterfeit measures like serial number or holograms are verified. This is a process that is more cumbersome than approaching a tag to a reader, and the automatic process of verifying on the back-end server, that the tag is valid and belongs to its rightful owner. One of the three applications of our system is the access control application through which customers will be granted access to the grounds of the park or of the music festival.

Figure 1. The access application UI

A customer only has to approach his tag to the reader and after the tag has been identified by the system, he can enter the access code that was generated at the moment when the tag was bought. Even if it is a desktop application it was designed to be easily used on touch-screen panels as well.

3.2 The Wallet Application

Inside the grounds of the park/music festival, every ride, merchandise, food or beverage stand will be fitted with a PC and tag reader that will be connected to a back-end server. Since the locations where such businesses operate have an average size of 50 hectares [7] a local area network that connects all the PCs to a back-end server is feasible.
To pay for merchandise, food and beverages and to access rides, customers will use the points loaded on the electronic wallet of their tag.
This operation will be done through the use of the wallet application.
To perform a transaction, the customer will approach his tag to the reader of the stand. After the tag has been identified by the system, the application will read the balance on his tag. After the transaction is made the new balance is written on the tag. An image of the Wallet Application User Interface is presented in Figure 2.

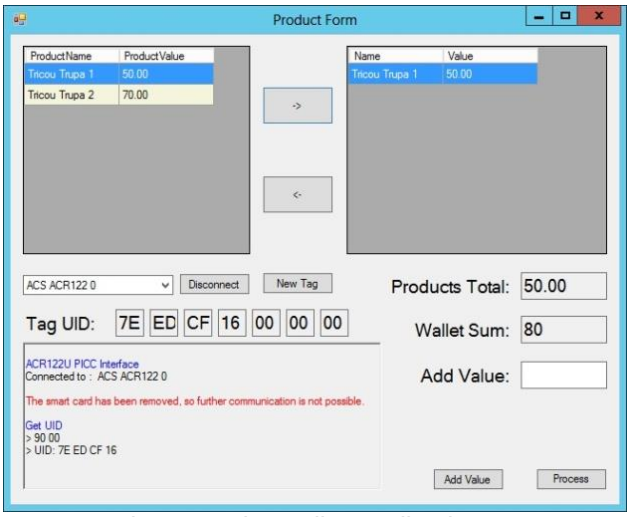

Figure 2. The wallet application UI

Through the use of a wallet application, our system will speed up queues.
since using an electronic wallet removes the cumbersome process of manually handling money change or tokens. If people run out of points on their wallets they refill their electronic wallet from any stand.

3.3 The Admin Application

The clients who will use our system will have a dedicated application through which they will be able to add locations, location stands, products, stand products, tags, customers and access codes.
The admin application will feature even a tag transactions viewer, in order to see the details of each transaction.

3.4 NDEF Support

The MiFare Classic tags operate on high-frequency radio waves, more specifically on the 13.56 Mhz frequency. This is the same frequency on which Near Field Communication (NFC) enabled devices operate.
This standard of radio communication has been adopted by almost all of today's mobile phone manufactures, and you rarely find a new smartphone up for sale without a NFC chip inside it.
In order to future proof our system, and make it easily extensible we have adopted a common data format defined by the NFC Forum, the NFC Data Exchange Format (NDEF). In doing so our tags are formatted according to the specifications set for NFC Forum Enable Tags.
By implementing NDEF data formats our system can easily implement smartphones support. Most other RFID systems in use that utilize MiFare tags ignore NFC standards and use proprietary data formats in order to offer better security. As we will see MiFare Classic tags have some security flaws that even proprietary data formats aren't able to fix.
If the implementation of NDEF as a data format enables our system to easily adopt smartphones, the security of the system will actually grow. RFID tags lack a microprocessor and a secure element capable of authentication measures, while most smartphones have both. The use of NDEF data format will be the competitive advantage that our system will have over other RFID solutions, as their systems won't be able to easily implement smartphone support.
Next we will inspect the security issues of the MiFare tags and present countermeasures that our system has implemented in order to eliminate those security issues.

3.5 Security issues of MiFare based RFID systems and countermeasures

The MiFare RFID tags have been introduced by NXP Semiconductors in 1995 and more than a billion tags have been sold worldwide since then [9].
Acting as access control and electronic wallet systems, the tags have attracted the attention of research groups, who have taken numerous studies concerning the security that the tags offer.
The MiFare Classic tags implement a NXP proprietary cryptographic algorithm called CRYPTO-1. It is a stream cipher with a 48-bit secret key that is used to assure data confidentiality and mutual authentication between the tag and reader. By applying reverse engineering techniques directly on the silicon implementation, security researchers Karsten Nohl and Henryk Plötz have uncovered the CRYPTO-1 algorithm. In the research paper Dismantling MIFARE

ISSN 2067 – 4074

Classic, a team of researchers from the Radboud University in Nijmegen, the Netherlands, led by Flavio D. Garcia, have fully disclosed the entire algorithm.
Based on these vulnerabilities a number of attacks have been identified. To facilitate a thorough understanding of RFID security and thus, implement effective countermeasures we will discriminate attacks based on the security properties that they affect, which are confidentiality, integrity and availability.

- **Confidentiality** ensures that information or services cannot be accessed by unauthorized parties. Attacks that can affect the confidentiality of a system are:

a. **Side-Channel Analysis** is a non-invasive type of attack that may be conducted when the attacker measures fluctuations in timing delays, power consumption or emitted signals and radiation - information that may reveal critical data about the input and the internal states of the RFID devices. A Differential Electro-Magnetic Analysis (DEMA) is a type of side-channel analysis that measures the electromagnetic field variations caused while an RFID device performs cryptographic operations. Performing such an attack on our system, given the fact that the cryptographic algorithm of the MiFare cards is known, will result in the retrieval of the secret keys with which the the data found on the tags is encrypted. To perform a SCA, an attacker needs special equipment that can intercept the electromagnetic field generated by a reader of our system. The analysis of the captured signal is carried on a computer so a person with this type of equipment on himself would be easily noticed by the security personnel of a theme park or music festival. As this attack requires lab equipment, it isn't a feasible attack on our system.

b. **Physical tampering** was the type of attack that managed to break the CRYPTO-1 algorithm. The two researchers that conducted the attack dismantled the MiFare card to check its internal components, and through careful examination managed to reverse engineer the algorithm. This type of attack would render the tag unusable so it isn't an issue for our proposed system.

- **Integrity** guarantees that information or services are not modified by unauthorized parties. The attacks that can affect the integrity of our system are**:**

a. **Impersonation** of RFID tags can be achieved by tag cloning or by tag reprogramming. The discovered vulnerabilities of the MiFare tags mostly enable these types of attacks.

b. **Tag cloning** can only be done with the help of a special device called an emulator. Since the businesses we have designed our system for have personnel near any of the systems readers, the use of an emulator won't go unnoticed. By using tags that have the shape of bracelets, the emulators couldn't go unnoticed. To make sure these types of attacks wouldn't be successful in the event that attackers would bypass the personnel's vigilance, we have implemented a two stage authentication for in the access control application. At the entrance of the location, besides validating the tag, the visitors will need to enter a 4 digit pin code. This pin code is unique to a tag and is entered once the tag is assigned to a customer through the admin app. An attacker with an emulator could manage to clone a valid tag but in order to get access to the location he would also need to know the pin code. If an attacker tries to use an emulator on the electronic wallet part of the system, his attack would succeed only once. Every transaction will be checked with the back-end server. On each transaction verification on the unique id of the tag will be made, and the person

whose tag has been cloned would notice the balance on the electronic wallet has been changed by the transaction that was performed by the attacker. The tag will then be blacklisted and the next time the attacker uses the emulator, the personnel will be warned by the system that the respective emulated tag can't perform the transaction.

c. When talking about **tag reprogramming** attacks, in the case of MiFare tags we actually refer to a card state replication attack. A card state replication attack could affect the electronic wallet part of the system. Because of the vulnerabilities of the MiFare tags, an attacker can read the contents of the tag after he has discovered the secret keys used to encrypt the data on the tag. By reading and storing the contents of a valid tag that has just been filled with points, the attacker has a card state at his disposal. After depleting the points on the tag, the attacker can rewrite the tag with the stored state, managing to have his wallet filled without paying for the points. To mitigate such an attack, our system uses a hash-based transaction validation process. When a tag is added to our system, the admin application will concatenate the UID of the tag with a salt value. This resulting text is then hashed with the SHA-256 cryptographic function in order to obtain the transaction validation value.

The salt value is actually the number of transactions that have been processed on the tag plus one.

The hash value is written on the tag and in the database of the back-end server, and it will serve to validate the next transaction that the respective tag will perform.

After a transaction is validated, the hash on the tag is updated. This process uniquely identifies each transaction. If a state replication attack would be performed, the state copied onto the tag would have a different validation hash than the one currently found in the database, and the next transaction that the attacker would try to perform would be refused.

- **Availability** ensures that information and/or services should be always available to all legitimate parties. From an availability point of view, the list of attacks that can be performed are jamming of RFID frequency or destruction of tags or readers. These types of attacks either aren't feasible in controlled access locations like theme parks and music festivals or an attack of this type can be dealt with very quickly by the personnel of the locations. These types of attacks wouldn't generate something of value for the attackers so there aren't many reasons why such attacks would be implemented.

4. Conclusion

Knowing the vulnerabilities of the MiFare tags and implementing security measures that deal with the types of attacks that can be performed because of those vulnerabilities assures that our access control and electronic wallet RFID based system offers a great security/cost ratio. Businesses like theme parks or music festivals that what to improve their services and their customer satisfaction can start taking into consideration the solution that we have developed.

References

[1] Disneyland, What time of year to visit Disneyland and Walt Disney World, available at http://www.scottware.com.au/theme/feature/atend.htm

[2] Wikipedia, List of amusement park rankings, available at: http://en.wikipedia.org/wiki/List_of_amusement_park_rankings

[3] Wikipedia, Rock in Rio, available at: http://en.wikipedia.org/wiki/Rock_in_Rio (2013)

ISSN 2067 – 4074

[4] Chris Koseluk, Are we there yet? Amusement Business 116, no. 25, 2004, pp. 14-17.
[5] Wikipedia, Radio-frequency identification, available at: http://en.wikipedia.org/wiki/Radio-frequency_identification
[6] Datamars, RFID Competencies, available at: http://www.datamars.com/default.aspx/MenuItemID/258/MenuGroup/_RFID+Competencies.htm
[8] Orlando Theme Parks News, Comparing the Size of Disney's Theme Parks, 2012, available at: http://www.orlandoparksnews.com/2012/02/fun-fact-comparing-size-of-disneys.html
[9] NXP, NXP Consolidates No. 1 Position in Worldwide ID Market , available at: http://www.nxp.com/news/press-releases/2011/07/nxp-consolidates-no-1-position-in-worldwide-id-market.html
[10] Mifare, MIFARE® Milestones, available at: http://www.mifare.net/aboutmifare/history/