Analysis of the Vulnerabilities of the UBC RFID Parking System

Timothy Chiu, Tim Ren, Evelyn Tsai, and Kattie Tay, *EECE 412 Group 3*

***Abstract* - This report provides an analysis of the vulnerabilities in the UBC RFID parking system. As part of our analysis, we attempted a variety of attacks on the system which included duplication and cloning of the FlexPass, repeated entry into the parkade and simulation of exit by walking out with the FlexPass. From the outcomes of our attacks, we were able to conclude that the security of the UBC RFID parking system was generally secure and subject to human error rather than technical failures.**

I. INTRODUCTION

Parking at the University of British Columbia (UBC) has long been a significant issue since the construction of new buildings that replaced the surface parking lots on campus. To counter this deficiency, UBC has constructed numerous parkades around campus. These parkades are currently equipped with automatic access gates that respond to Radio Frequency Identification (RFID) tags. These tags, called the FlexPass, are used as access passes which replaced the traditional ticketing system. While RFID has proven to be an efficient access control mechanism in applications such as animal tracking, inventory management, and public transportation [1], a number of security issues have emerged and caused concerns on its use [5]. This paper will evaluate the level of security provided by the use of RFID passes at parkades at UBC. This evaluation encompasses the analysis and methods of exploiting the vulnerabilities that may exist in the parking system. Main exploits include analyzing the data contents of the FlexPass as well as simulating unauthorized access to the restricted parking area. The results obtained will illustrate the level of security of the parking system as well as the feasibility of exploiting such a system.

II. FLEXPASS TAG

The FlexPass tag used for access to parkades at UBC are a type of RFID tag. A typical RFID access control system consists of the following components: reader, transponder, and a database system which is often connected to a number of readers [2]. The following sections provide an insight of how this technology works as well as the results of our attempts at accessing data within the FlexPass.

A. How the Tag Works and its Authentication

RFID transponders, also known more commonly as RFID tags, are small portable electrical units made of simple circuits capable of storing and transmitting data via radio frequency [4]. The tag also incorporates an antenna responsible for receiving and sending information to the reader [1]. These tags are not equipped with any form of direct power supply. Instead, upon receiving a radio signal from the reader, the tags would transfer the energy from radio signal into electrical energy, and thus enabling them to perform their designed functionalities. The reader, regardless of level of complexity, requires at least an antenna and a slightly more complicated circuit design relative to the tags [1]. It usually connects to various output peripherals such as a LED display or computers with database programs. The illustration in figure 1 presents a basic, unencrypted RFID logging system.

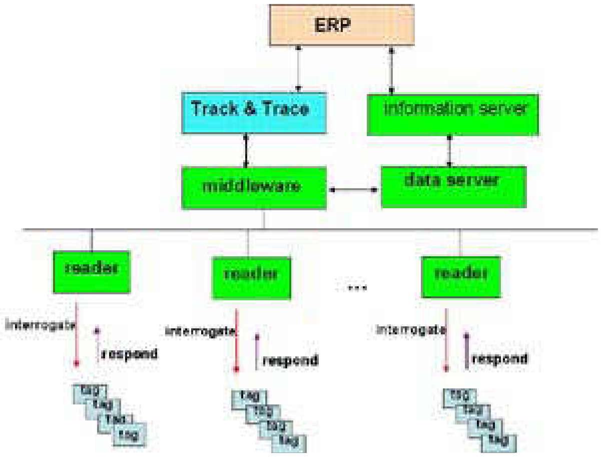

Figure 1: Authentication of typical RFID reader [3]

As per the illustration, the system may require little or almost no authentication [2]. The initial step begins when the reader continuously broadcasts signals through radio frequency and waits to receive a responding signal from any tags within its range [2]. The tags receive initializing information from the reader and become energized by the signals. The tags then respond by transmitting useful information that have been written and stored within its memory. The last authentication step requires the program to verify the information from the tag, and it does so by performing a database search and comparison [2]. Research revealed that the tag used for the UBC FlexPass was produced by Texas Instrument Ltd (TI), and was designed according to the ISO 11784 standard [8]. The FlexPass responds to signals in the 134.2 KHz frequency range, and can be energized at a range of approximately 2 meters from the reader [8].

B. Encryption

RFID technology, being an evolved version of the traditional radio transmission technology, has a more developed encryption method. For example, RFID tags capable of storing up to 120 bits of data can typically incorporate M5A encryption into part of the system design [4]. At present, however, only a minority of all ISO standardized RFID devices support encryption methods that can be used to effectively protects users' identities and personal information [1, 5]. Such limitation is a result of minimizing the production costs in order to compete with already existing technology such as the bar-code system [1].

A typical ISO 11784 RFID tag supports 120-bit information storage capacity. However, according to the data sheet provided by TI, the FlexPass used for the UBC parking system only reserves 80-bits of memory for data storage [8,9]. It is thus unfeasible to implement secure encryption since 8 bits out the 80-bit memory is used for the hand-shaking and initializing procedure, and another 16 bits for error bit detection. This design leaves no more than 60 bits of memory for actual data storage within the transponder. These findings show that the UBC FlexPass is not encrypted and is susceptible to data theft when the data is broadcasted between the reader and the tag. In general, RFID access or management control systems have been proven to behave poorly against Denial of Service (DoS) attacks such as signal jamming [1] or Man-in-the-Middle (MiM) attacks such as unauthorized duplication of transponders [3]. Research has also exposed other effective methods to compromise some of the software authentication methods such as hash calculation [6].

C. Attempt at Duplicating FlexPass Contents

There are numerous RFID transponder duplication attempts by computer specialists that have proven successful [4]. Our intentions were to attempt a similar exploit by utilizing a reader to send and receive signals at the desired frequency. We would then be able to intercept the response of a tag during operation and then analyze and transfer the read data onto blank tags to create a viable duplicate tag to bypass the system [5]. Logically, the broadcasting nature of RFID and lack of secure authentication make attacks such as MiM especially effective, due to the inability of the real reader to detect the presence of other intercepting readers [7].

However, after we acquired a lower-end reader at the cost of $80, we encountered a number of technical difficulties in our attempt to duplicate the FlexPass. Our lab-tests showed that the reader generates a waveform that varies in amplitude according to the distance in between the tag and the antenna of the reader, indicating a generated response. Obtaining readable data turned out to be a great challenge as the RFID reader that we purchased was not the genuine TI RFID reader and thus was incompatible with the tag. At a price of over $300 from Digikey, the genuine reader was above our budget of $100. We attempted to extract meaningful information from the tags by implementing programs in various computing languages including C, C++, and Java (RXTX); none of the programs generated a successful data read and thus our attempt was put on hold. Even if the tag duplication could be carried out without having to analyze the intercepted data, only primitive attacks such as DoS can be performed and is unlikely for attackers to utilize such attacks to their benefit. Despite our unsuccessful attempt to create a duplicate FlexPass, we believe that proper equipment such as the authentic TI reader will make it realistic to create a duplicate.

III. WEAKNESSES IN SECURITY INFRASTRUCTURE OF PARKADE

The infrastructure of the parkades itself plays a key role in ensuring the security of the entire parking system. In UBC, the parkades are equipped with RFID readers at both entrances and exits that are used with the FlexPass. To enter or exit the parkade using the FlexPass, users are required to scan their FlexPass at the RFID reader in order to activate the gate at the parkade to open. Also, a FlexPass that had been signed into the parkade has to be signed out of the parkade before it can be used again. The following sections will describe our attempts at testing the robustness and effectiveness of the infrastructure in the UBC parkades.

A. Attempt 1: Simulation of Entry and Exit by Walking Past RFID Reader with FlexPass

Our first attempt was to determine if the UBC RFID parking system would allow us to park more than one car in the parkade at the same time. This was done by walking past the RFID reader at the entrance and exit of the parkade with the FlexPass in hand to simulate the process of signing the FlexPass in and out of the parkade.

We first drove into the parkade and used the FlexPass to let ourselves in. We then walked past the reader at the exit of the parkade and scanned our FlexPass to sign it out. However, the gate did not open as expected. To confirm if the FlexPass had indeed been signed out, we proceeded to drive into the parkade using a second car and attempted to open the gate with the same FlexPass but were unsuccessful.

From walking past the RFID reader at the exit, we noticed there were three squares cut into the ground: two before the gate and one after it. We speculated that these squares were ground weight sensors and the purpose of them was to detect whether it was an actual car that was exiting or entering the parkade. This meant that a car would have to actually drive past all three sensors in order for the FlexPass to be signed in or out.

B. Attempt 2: Repeated Entry into Parkade

Our second attempt was to sign out our FlexPass by making use of any random car that was exiting the parkade at that time. This was done by standing at the exit with our FlexPass while the random car was exiting. Two uncertainties we had was if the RFID reader would be able to sign us out with both our FlexPass and the other car's FlexPass present, and which one would it sign out.

We tried this out by hiding behind the scanner while a random car exited the parkade. The result was that the gate opened but we still needed to determine if the reader had indeed signed out our FlexPass or if it had only been able to detect that of the random driver's. To confirm our suspicions, we attempted to drive into the parkade in a second car using the same FlexPass. The FlexPass successfully activated the gate and we were able to enter the parkade using the same FlexPass in a different with the first car still parked inside. This method demonstrated that such an exploit was actually viable.

C. Implemented Countermeasures by UBC parkades

Looking at the above two attempts at exploiting the system, although the second method worked, however both of them were generally unfeasible. The weight sensors deployed in the ground of the parkades' entrances and exits minimized the chances of anyone trying to walk out of the parkade and passing the FlexPass to another person. During our experiments at the parkades, we also discovered at least three surveillance cameras installed at the entrances and exits of the parkades. A booth where a parking attendant sat in was also strategically located at the parkades overlooking both entrances and exits. All these countermeasures implemented by UBC acted as deterrents to anyone attempting any sort of foul play. Thus, it can be said that the infrastructure of the UBC parkades was generally secure and that the risks of it being exploited was relatively low or insignificant.

IV. VIGILANCE OF SECURITY PERSONNEL

The human factor is frequently described as the weakest part of a security system. Despite the best efforts of engineers in designing a technical security solution for the parking system, the system is still fallible if not implemented and operated accordingly. In the case of the security system in the parkades at UBC, the human factor in particular consideration is the vigilance of the parking attendant on duty. Users who intend to abuse the system could ultimately be successful if the security personnel who operate the system elect to be negligent. The following section will illustrate our attempts at deceiving the parking attendant by using a replica of an authentic FlexPass tag which we produced ourselves.

A. FlexPass Duplication

Our intention was to duplicate the appearance of an authentic FlexPass onto a non-usable tag and assess if a parking attendant on duty would be able to observe the difference between the tags as we enter and exit the parkade. To create this replica, we scanned and printed a high resolution image of the FlexPass tag onto sticker paper. We then attached the sticker onto the blank RFID tag that we purchased from Digikey for $25. We intentionally changed the tone of colour of the replica tag so that it would be distinguishable from the authentic tag when held side by side (See Figure 2). This would examine the parking attendant's ability to observe and recognize the subtle differences and thus helping us to determine if the attendant is sufficiently vigilant when handling the tags.

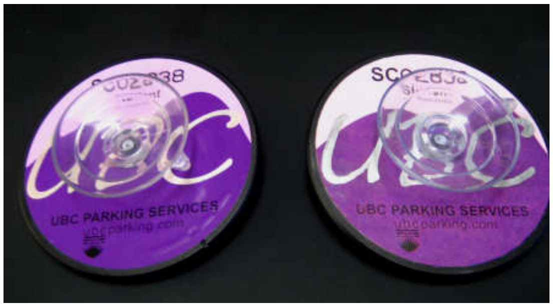

Figure 2: Authentic FlexPass and its Replica

B. Attempt at Deceiving Parking Attendant

The strategy in carrying out this experiment was to use the created replica pass to gain access and exit into and out of one of the parkades at UBC. We conducted our trial by first driving up to the parkade entrance and scan the pass, resulting in the failure to open the gate. We then went to the parking attendant booth to describe the problem, at which he prompted us to obtain a parking ticket from the machine. We then parked the car and returned an hour later to test the exit process. During the exit process, we proceeded to the gate and told the parking attendant about our difficulty in entering. He then took our replica pass and input the serial number from the pass into the computer to retrieve user information from the database. After verifying that the serial number of the pass corresponded to that of a working FlexPass, the parking attendant allowed us to exit from the parkade.

C. Results and Feasibility of Exploitation

Although we were successful in displaying that the parking attendant was negligent, this method of exploiting the security system is not feasible due to the variability in the human factor error. One careless parking attendant is indeed not a complete representation of the behaviour of the other parking attendants. The susceptibility of vehicle and driver recognition through the repeated encounter with the same parking attendant will also create suspicion in attempting this exploit. Unless the user decides to only use the replica pass occasionally, he or she should not attempt this method because there is a considerable risk of identification by the parking attendant.

V. SECURE SYSTEM DESIGN VIOLATIONS

From our analysis of the UBC RFID parking system's security, we were able to note a few design flaws in the system. These flaws could potentially increase the vulnerability risks of the system which might lead to future exploitations.

One of the principles of designing secure systems that was violated was the Least Privilege principle. Currently, FlexPass users are allowed to register as many vehicles as they wished under their account. The purpose of this was to encourage people to carpool to UBC by sharing a FlexPass. However, this could backfire in a situation where a user cloned multiple tags and distributed them to other people. All the user had to do was ensure that the other people's vehicles were registered under his account which could be easily done via the UBC Parking Services website. By giving users the ease of adding/removing vehicle registration information from their accounts, UBC Parking Services has made it easier for users to use duplicate tags as they did not need to go through any approval procedure before being allowed to register new vehicles.

The UBC RFID parking system also violated the Fail-Safe Defaults principle. In one of our attacks described in an earlier section, we successfully tricked a parking attendant into letting us in and out of the parkade using a look-alike but non-functioning FlexPass. The parking attendant had found our car registered under the FlexPass and assumed that it was the system or FlexPass malfunctioning rather than suspecting that we had malicious intent. If the Fail-Safe Defaults principle had been followed, the parking attendant should have denied us exit and instead made us pay before we were allowed to leave the parkade. By letting people exit for free on the basis that they owned a FlexPass but it was malfunctioning, UBC could potentially lose thousands of dollars in revenue if this attack was repeated frequently.

In addition, the Complete Mediation principle was violated since at no point during our attacks did they ask for identification to prove that we were indeed the registered user of the FlexPass. The FlexPass contained no indication of our identity i.e. photo, driver's license, student number, or vehicle license plate, which meant that once we had a hold of someone else's FlexPass, we could do anything with it. Also, there were no parking attendants at work on weekends which meant that there was no one monitoring the cars entering and exiting the parkade. The FlexPass account on the UBC Parking Services website is also easily accessible since only the student number and driver's license is required to access it. Someone with malicious intent would have no trouble obtaining such information and this could lead to an infringement of the user's privacy.

One other principle not followed was the Question Assumptions principle. UBC Parking Services probably did not expect anyone to attempt to hack their system. Therefore, parking attendants were not trained to identify users with malicious intent like us who used a look-alike tag instead of a real one. UBC Parking Services also had probably not thought of the possibility that the FlexPass could be forged since the FlexPass did not contain any special security features such as holograms. Instead, the FlexPass was merely a readily available RFID tag with a normal printed sticker on it.

VI. CONCLUSION

The FlexPass is used by thousands of people daily throughout the different parking lots in UBC. Each year, it generates tens of thousands of dollars in revenue for UBC Parking Services. Any exploitation or malicious attack on the system would no doubt cost loss of revenue to UBC Parking Services as well as cause inconvenience to users of the FlexPass.

Through our analysis of the system, we were able to conclude that the UBC RFID parking system did not have any major vulnerability issues. Our simulation of exit and repeated entry attacks proved that the methods were not feasible and the risks of someone successfully attempting those attacks were low. Our FlexPass forgery proved successful as it preyed on the human error factor but would become evident if the same exploit was used too frequently. Our attempt to clone a FlexPass turned out to be unsuccessful due to lack of time and resources; however, research on the FlexPass itself indicates that cloning of the FlexPass is possible.

While we were working on our project, we received tremendous support from our peers to succeed. This was a result from the high prices that students were required to pay for UBC parking which were deemed unreasonable and unaffordable. As such, most were eager and supportive of our attempt to hack the system. From this, it highlights the potential of someone exploiting the system in exchange for monetary gains. Given the sufficient time and resources, a malicious person would definitely be able to create a functioning clone of the FlexPass and thus pose a threat to the UBC RFID parking system.

VII. REFERENCES

[1] R. Malenle et al., The Evolution of RFID Security, *IEEE CS and IEEE ComSoc, pp 62-69, March 2006.*

[2] A. Sharif and V. Potdar, A Survey of RFID Authentication Protocols, IEEE CS and IEEE ComSoc, pp 1346-1350, 2008

[3] I. Syamsuddin et al., A Survey of RFID Authentication Protocols Based on Hash-Chain Method, IEEE CS and ComSoc, pp 559-564, 2008

[4] H. S. Kim et al., Formal Verification of Cryptographic Protocol for Secure RFID System, IEEE CS and IEEE ComSoc, pp 470-477, August 2008

[5] H. Knospe and H. Pohl, RFID Security

[6] M. S. Hossain and S. I. Ahamed, Towards a Simple Secured Searching Protocol for Future RFID Applications, IEEE CS and ComSoc, pp 151-157, August 2008

[7] E. J. Yoon and K. Y. Yoo, Two Security Problems of RFID Security Method with Ownership Transfer, IEEE Cs and ComSoc, pp 68-73, August 2008

[8] RI-TRP-R9UR 85mm Disk Transponder, Texas Instruments Inc.

[9] Wikipedia Encyclopedia, www.wikipedia.org : key word ISO 11784