Security Analysis of Verrus Pay-by-Phone

December 6, 2010

Paul Chiu, Tayler Hetherington, Alvin Lam, Ryan Jung

Department of Electrical and Computer Engineering
University of British Columbia
Vancouver, Canada

ppchiu@gmail.com, tayler.hetherington@gmail.com, ahflam@gmail.com,
ryanjung@interchange.ubc.ca

***Abstract*—This report outlines the methodologies and findings of our security analysis performed on Verrus' mobile authentication protocol. Several vulnerabilities were discovered and were able to be exploited through use of a free caller ID spoofing application for smart phones. This application allowed us to gain access to user accounts through the use of any generic mobile phone and change the customer's credit card information. Using this information, we were able to extract the user's PIN number and also perform a phishing scam by disguising ourselves as Verrus staff. The attack can be deterred if Verrus required customers to enter their PIN every time they used the service. However, since the system was designed to prioritize convenience over security, the system became insecure.**

I. Introduction

THE company Verrus manages a pay-by-mobile parking system utilized extensively throughout North America and parts of Europe. A customer initially creates an account with the company by supplying their mobile number, credit card information and a list of license plates; in return, the company will automatically charge their accounts whenever they are contacted by the registered mobile device to place a parking transaction. Introducing valuable assets into the system, such as financial information, increases the risk value at an exponential rate. There are now reasonable justifications for threat agents[1] to exploit vulnerabilities in the system such as the ones that we have uncovered. The risk value of leaving such a system in a vulnerable state is unacceptable which serves as our reasoning for performing this analysis. Systems that possess valuable assets such as these must be consciences of vulnerabilities.

[1] Threat Agents – entities who wish to access, abuse, and/or damage an owner's assets[1].

There have been other analyses performed on the state of the Verrus pay-by-mobile security system. Most notably, the attempt on the Verrus web site authentication protocol performed in 2008 by previous EECE412 alumni. The analysis demonstrated a weakness in the keyspace size and attempted to brute force passwords of specific accounts.

Our methodology is different from other analyses in the fundamental assumptions made about the system. By the definition of security, we assumed this system was not secure; therefore, our analysis methods focused on attempts made to circumvent or break pre-existing security mechanisms. As this report will elaborate in more detail, we deceived the authentication system employed by the call center and we used the results of this attack to circumvent the online authentication protocol. At this point in the analysis, we were ethically compelled to cease further exploitation on the system; however, hypothetical scenarios are supplied in this document for areas of further exploitation.

At the point that we halted analysis of the system, we were able to obtain complete access to the user's online account, charge their vehicles arbitrarily and deny access to the original account holder. It is possible to further the attack and register other vehicles using some social engineering techniques.

With the minimal amount of work that is required to yield the aforementioned results, there is very real reason for clients of Verrus and Verrus themselves to be concerned with the implications of our analysis. Our findings question the fundamental principles that Verrus' business model is based upon (and all future pay-by-mobile companies). There are solutions we will explore in this report; however, these solutions in the opinion of the team can only mitigate the

level of access an attacker will have after already gaining access. This analysis leads us to believe that mobile devices are simply not capable of adequately identifying an individual.

Several design principles were found to be either lacking or absent when analyzing the system. Complete mediation was not performed after gaining access to the system and in fact, the depth of the defense mechanisms employed was virtually non-existent. A mechanism to defend against our attack already exists in the system; however, it is left to the user to enable the feature. Since this feature is psychologically not acceptable with respect to convenience, the typical behavior is to leave it disabled. Finally, assumptions were not questioned; Verrus does not seem to have considered the consequences of what would happen should someone be able to replicate another user's phone number.

In our solution we propose a number of 'satisfactory' solutions that will at least deter attacks on the system; however, as mentioned there is a fundamental problem in the concept of identifying people by phone numbers. One such solution is to simply not provide the user an option of disabling security features. Another solution is to implement an effective voice recognition system.

II. Analyzed System

A. Company Overview

Verrus is an international company and pioneer in pay by phone services such as food and beverage ordering and parking[2]. Presently, they provide pay by phone parking services for 100 cities throughout North America and the United Kingdom[2]. In the lower mainland of British Columbia, Verrus provides services for meter parking on streets, parking lots managed by EasyPark (www.easypark.ca), and parking at the University of British Columbia[2]. Since customers are paying via their phones, they no longer have to worry about carrying spare change for parking. In addition, customers need not have to return to the meters to insert more coins if they will be parking for an extended period of time. Paying by phone is a convenient alternative in this day and age where people are less likely to carry change.

B. How the System Works

To pay through Verrus, customers must first create an account with the company. Accounts can be setup through the Verrus website or through the phone. When users create their account, they are required to enter their phone number, credit card number, license plate, location, and general personal information. Users are also required to select a 4 to 6 digit PIN that will be used for authentication purposes.

After creating an account, users are able to pay for parking by calling the local Verrus phone number. Customers are identified by their phone number, and when they call Verrus, the automate system uses the caller ID to identify users. Utilizing the caller ID system for fetching a user's phone number is convenient for users as they are not required to enter their phone number every time. After users have been identified, they may be asked to enter their PIN or the last 4 digits of their credit card for authentication. Lastly, users must enter the 5 digit location number of their parking location and also the amount of time they wish to park for. Transactions are processed immediately and debited to the credit card registered to the account.

III. Related Work

In the fall of 2008, a student team led by Chris Lee, Benjamin Wai, James Wang, and Leo Wong performed an analysis on the Verrus system. They discovered the website did not limit the number of attempts for authentication and the system allowed the user to have multiple passwords. Exploiting these weaknesses, they obtained customer phone numbers and were able to perform an exhaustive key search for the last 4 digits of the credit card number to break to into the accounts. Although they were successful, their attack was based on the assumption that the system was secure.

In the area of caller ID spoofing, there have been several incidents of harassment using caller ID to mask the identity of the caller to the callee[3]. Incidents of fraud and scam have also been attributed to caller ID spoofing[3].

IV. Analysis Methodology

Our analysis of Verrus' security system began with research into pre-existing security issues. As stated in Section III, a previous EECE 412 group exposed vulnerability in Verrus' authentication process that allowed attackers to brute force any login password in a matter of minutes. We attempted to recreate this attack by repeatedly entering incorrect passwords into an existing account and recording the systems response. The results of this test are stated in the Results section of the document; however, the main findings were that Verrus had successfully corrected this vulnerability using the exponential back-off methodology. This greatly deterred, although did not eliminate, any online brute force attack. This type of attack is based on the assumption that the system is, on a whole, secure and that no back doors or shortcuts through the security system exist. Our analysis breaks away from this assumption and focuses on finding possible backdoors around the security system. This distinction in focus gives rise to the main difference in our analysis of Verrus' security system compared to previous analyses.

After discovering that the online brute force attack was handled by an update in the security system, we began by further analyzing the customer authentication method used by Verrus. On the website login page, the customer's username

is their ten digit mobile phone number. This is already an issue, however small, in its own as every customer's username is of the same format, thus allowing attackers to easily guess existing customers' usernames. The next logical step was to search for any method that would expose phone numbers currently registered with Verrus. Without requiring searching very far, Verrus' login page contains a "forgot your PIN" option for users who cannot remember their login PIN. Entering a phone number known not to be registered with Verrus resulted in an error message stating this user does not exist, however, inputting a registered phone number successfully sends an e-mail registered to the account holder including their PIN number. Although the user is notified that their forgotten password has been requested, the attacker has already gained the knowledge of the customer's username. As stated above, the online brute force attack on customer's password is no longer a reasonable method of attack; this greatly reduces the threat level that possessing usernames previously held.

The next step taken was to analyze the customer authentication method used when the customer calls in to complete a parking transaction. To start, we initially had to create an account with Verrus using one of our group member's phone numbers. We made sure to complete the account creation process using all of the default settings as a best effort to model the average user. Once we aquired an account we were immediately able to place a call to Verrus to begin the parking procedure. Once connected to Verrus' server, we were prompted to enter our 5-digit location number used to specify which parking stall we wanted to park at. This instantaneous admission into the system gave immediate rise to concern. At no point during the phone call were we prompted for a password to authenticate the customer on the other end of the phone, which will be discussed in detail later. Further navigating the on-phone interface we noticed that we were prompted for the customer's PIN for some actions, but not for others. The main actions to note that did not require a customer's PIN were parking an existing vehicle already registered to the account, and modifying the credit card information registered to the account. Other administrative actions, such as adding vehicles to the account, did require the customer's PIN for authentication purposes. At the current point in our analysis, the only security issue seemed to be related to the attacker gaining physical possession of the customer's phone, thus enabling the attacker to repeatedly place parking charges on the customer's credit card, or to change the customer's credit card information, which didn't seem to serve much purpose. However, we will show later in our analysis how this seemingly small issue gave rise to serious side effects.

Next we began to analyze the reasoning behind the absence of a PIN requirement during the customer parking procedure. We started at the account creation page to view the information in more detail. Very quickly, we noticed that there was a checkbox stating "Skip requirement to enter PIN when caller ID is detected", which was preselected by default. Thus, the average user (one who would not change any of the advanced account settings) would likely create an account that required no further authentication than a phone number when wanting to park their vehicle. It should be noted that this setting is also a convenience. The requirement to be prompted with a password at the time of parking can be time consuming, cumbersome, and even frustrating in a situation when it is forgotten. Thus, even advanced users may stay with this default setting which has higher focus on convenience over security.

The next stage in our analysis focused on other possible ways that an attacker could possess a customer's phone without physically requiring it. Caller ID spoofing has been widely available for many years; it allows users to change their caller ID to another ID for the duration of a phone call. All that is needed is a mobile phone capable of running applications or a computer with an internet connection. Without going into detail of the internal workings of a caller ID spoofing application, we were able to obtain free software for a smartphone (namely callerID Faker), which allowed us to masquerade as any phone number by masking our real phone number with any number of interest. After testing that the application worked between two of our group member's phones, we began the test with Verrus' server by placing a call and masking the phone number with a different, registered phone number. Unexpectedly, we were immediately prompted with the same message to enter our 5-digit location number, which signified that we had gained access into another user's account. We had the same limitations and privileges as if we had direct access to the customer's physical phone, which allowed us to park and charge an existing car to the account holder's credit card or change the credit card information. The first of these two options was of little interest as it was deemed only to cause mischief, but the latter option gave rise to a serious flaw.

At the login page, the user is prompted to enter their username and PIN number. They are also provided with the option to enter, in place of their PIN number, the last four digits of the registered credit card. As shown above, we have gained the ability to change the registered credit card on any account by spoofing their phone number. The conjunction of these two seemingly harmless properties becomes severe as we are now able to indirectly gain access to any customer's password and therefore possess the ability to login to their account.

Once falsely gaining access to a customer's account, we were able to view all of the customer's personal information,

parking transaction history, and registered vehicles. Although we had full access to the account, we were missing the two most important pieces of customer information; the PIN and the credit card, as we were required to change the credit card number to gain access to the account. The next stage in our analysis was to gain insight on how these two valuable pieces of information could be uncovered.

We recalled that the login screen contained a "forgot your PIN" option that e-mailed the customer's PIN to the registered e-mail address. As we were already logged into the customer's account using the credit card number, we were able to modify the e-mail address to anything we wanted, notably our own. After changing the e-mail address to one of interest, we logged out, pressed the "forgot your PIN" button, and entered the customer's phone number. In seconds we had a confirmation e-mail containing the customer's PIN. At this point we no longer need the fake credit card number to log in to the account as we possessed the actual PIN for the account. The next step was to find a way to restore the customer's credit card information.

Introducing social engineering into the analysis, a simple phishing scam would allow us to regain the correct credit card information for the account. As we had received an e-mail from Verrus in response to the "forgot your PIN" scenario, we had access to the e-mail address used by Verrus for customer support and the format used in their support e-mails. Using these two pieces of information, we created an SMTP client capable of specifying any source e-mail address, and used the freely available mail server, hMailServer. These allowed us to create a copy of Verrus' e-mail, send it from the exact same e-mail address (support@verrus.com), and notify the customer that their account information seems to be incorrect and may need to be modified. The main aspect to notice in this phishing scam is that in no point is the customer required to respond to a malicious third party mistakenly giving out their personal information, but instead they're are able to use all of the legitimate services provided by Verrus to access their account and modify the information. The reason this type of phishing attack would work is due to the fact that the attacker is able to obtain all of the required information prior to involving the customer. This minimizes any suspicion the customer might have if they were dealing with an illegitimate third party as from this point, they are dealing directly with Verrus. Once the user has updated their credit card information back to its original state, we are able to log in to the account using the original PIN we obtained and now have full access to add and remove cars, change information, delete the entire account, and view full transaction history.

Our analysis so far has been under the assumption that the customer had created the account using the default settings, which has the effect that a PIN is not required at the time of making a parking transaction. If, however, the customer selects to require a PIN when paying for parking, the possibilities for attack are reduced, but not eliminated. In the final stage of our analysis we found that although Verrus had eliminated the plausibility of an online brute force attack, an on-phone brute force attack of the password is very possible. We found that Verrus allows three incorrect password attempts before disconnecting the current phone session, however, does not keep a record of this failed login attempt. When we called back, we were allotted the same three failed attempts before being disconnected. Thus, an attacker with very few required resources, such as three or four phones, is able to perform the brute force attack, on average, in less than an hour. For example, We were able to try approximately 24 different passwords per minute, 96 passwords per minute spread over 4 phones. Assuming the customer has chosen a 4 digit PIN, there are 10,000 possible combinations for the password. On average, we only need to try half of these passwords, thus attempt 5000 different passwords. To aid the attack even further, since the last 4 digits of the credit card is also a valid password, we only need to attempt 2500 different passwords on average. Spread over 4 phones, it would only take 2500/96 =~ 26 minutes on average.

V. Results

Attempting a brute force attack on the system yielded negative results as the system discourages this type of attack by enforcing an exponential back-off policy when an incorrect password is entered more than three times.

With the vulnerabilities that we discovered, we were able to conduct a number of attacks on Verrus' internet and telephone system. To begin, we were able to gain access to a targeted Verrus account. This enabled us to charge the account on behalf the user, delete car(s) associated with the account, alter the account's credit card information, and also change the account's password to revoke the account owner's access.

In Section IV, we mentioned that original access to the customer's phone account yielded little aside from enabling us to perform other vulnerability attacks elsewhere in the system. It was briefly mentioned that DOS (denial of service) attacks could be performed by arbitrarily charging a vulnerable account to parking stalls. This was passed off as little but mischief; however, with very little effort the ramifications that both Verrus and effected customers would incur if an attacker elevated the attack to multiple targets would become enormous.

Similarly, it would be trivial to harass Verrus' customers by simply changing information in their accounts, or even deleting the account in its entirety.

With the ability to spoof one's caller ID, it is possible for a malicious user to create an account with incorrect phone number and license plate information and start using Verrus' services with their own credit card. At the end of the month, the user can claim that his/her credit card had been compromised as no other account information belongs to the user and theoretically be able to deny any charges.

VI. Discussion

A. *Risk Management*

1. Assets

One of the assets put at risk by the vulnerabilities that we've found is the company's reputation. If users knew there were significant vulnerabilities in Verrus' system, we believe a large number of users would be deterred from using Verrus' services. This would amount to a large monetary loss for Verrus as their system is currently deployed in over 100 cities over North American and the United Kingdom[2].

Moreover, as we mentioned in the results section, we gained full access to the targeted account, thus providing us all the personal information that is recorded in the account such as the account owner's postal code, previous parking history, as well as partial credit card information. As we are able to make charges to the user's account, the user's finance is also put at risk. Given the vast user base Verrus has, the monetary value associated with this risk would be unimaginable.

2. Vulnerabilities

The biggest vulnerability that we have found during our analysis is that by default, Verrus authenticates the user with the phone's caller ID system. As we have detailed in this report, this type of authentication is not nearly sufficient enough to verify a user, as it is comparable to authenticating the user by simply asking them who they are.

Another vulnerability we found is that the key space Verrus uses for password login is too small. Limited by the lack of alphabet keys on the phone, a Verrus login must only contain numbers and is restricted to a maximum length of 6 digits. This means that there are only 10^6 possible combinations for a key. On average, an adversary would only need to go through half the key space to find a match. To make matters worse, Verrus also uses the user's last 4 digits of their credit card as a valid login which only has 10^4 possible combinations. Assuming that the user's login is different from their last four digits of their credit card, the probability that the adversary can find a match is greatly increased.

Lastly, although Verrus now implements an exponential backoff policy for their internet login, there is no lockout policy for their phone login. An adversary is simply disconnected if he/she has entered more than 3 incorrect passwords. The adversary is able to call back right away to attempt another 3 passwords. Through our analysis, we found that it was reasonable to make 24 password attempts in a minute and assuming that it would only take the adversary about 2500 attempts, the adversary would be able to gain access to the account in just under 2 hours.

3. Threat Agents

The vulnerabilities that we have found do not require the adversary to be technically savvy. In fact, any person with a smart phone that can obtain a caller ID spoofing application would be able to carry out the attacks we found in our analysis.

B. *Secure System Design Principles*

When Verrus designed the security aspect of their system, they neglected the principle to "Question Assumptions" as they assumed that caller ID spoofing was not possible and therefore was a secure form of authentication.

They also failed to consider the "Complete Mediation" principle as they did not re-check the credentials of the user on every access to an important option in the phone interface.

The mechanism to defend against our attack already exists in the system; however, it is left to the user to enable the feature. Since this feature is psychologically not acceptable with respect to convenience, the typical behavior is to leave it disabled.

Lastly, the system designers neglected to implement multiple layers of defense to make it more difficult for adversaries to compromise an account.

C. *Solutions*

To avoid the vulnerabilities that we found in our analysis, Verrus could have removed the option to authenticate the user by caller ID alone. This would have prevented us from modifying the account's credit card information and using our generated information to log into the system.

This may not be a practical solution for some people as the addition of the mandatory security device would be somewhat psychologically unacceptable with respect to convenience. As a compromise, a less effective but more convenient solution would be to verify users using biometrics. Specifically, a voice recognition system could be used to authenticate the user's voice to recorded records.

The inclusion of smart phone technology would have deeply impacted the findings of our analysis[4]. As technology evolves problems that involve older technology can be solved when designing the foundation for newer technology. As an example, society on a whole is moving towards the utilization of so-called smart phones that can run applications. Verrus could easily develop an application on a smart phone that stores the encrypted information of a user and sends the information back to Verrus utilizing technology such as 3G or even 4G. To propose a solution to caller ID spoofing is difficult in that there is an inherent flaw in the very foundation of older technology like mobile phones; however, changing the foundation entirely allows us to very easily solve the problem.

In addition, Verrus should implement exponential back-off for the phone's system as well to discourage brute force attacks from the phone interface.

VII. Conclusion

In this report, we have outlined the security vulnerability in the authentication system of Verrus' call center. Using a commercially available program "CallerID Faker", we were able to show that an attacker can disguise their phone number as another number and due to the lack of authentication past this point we were able to break into a user's account. From there we were able to either harass the user of the account, or change their credit card information to something of our own creation. We showed that using this step we were able to intrude into the user's account on the website and using various social engineering techniques, persuade the user to restore their original credit card information and grant us unlimited access to their account.

The results of this report question the fundamental principles of pay by mobile services. Personal information was able to be read as well as moderate access to the user's credit card. A more malicious attacker could replicate our results to a further extent. Using transaction histories, auto thieves would have information to track a user's typical day to day activities. Additionally, any random phone number could become a target to this attack as shown in the vulnerability in the PIN recovery system. Verrus' and various credit card companies could quickly become overwhelmed by the number of charge-backs that would ensure if an attacker decided to steal completely random accounts and charge them arbitrarily.

Acknowledgment

The group would like to thank the creators of CallerID Faker for the use of their phone spoofing application. Without their program it would not have been possible to perform the attack.

The group would like to thank James F. Kurose and Keith W. Ross for their SMTP (simple mail transfer protocol) mail client depicted in the book "Computer Networking - A Top Down Approach". This was used to craft and prove our phishing attempt when recovering credit card information.

The group would like to thank the creators of hMailServer for providing a program to host our fake Verrus email domain for our social engineering proof of concept.

References

[1] Common Methodology for Information Technology Security Evaluation, ISO/IEC International Standard 15408-2006.
[2] Verrus. "Verrus Mobile Payment", www.verrus.com, Dec. 5, 2010.
[3] Wikipedia. "Caller ID spoofing", en.wikipedia.org/wiki/Caller_ID_spoofing Dec. 5, 2010.
[4] K. Beznosov, private communication, November 2010.