Ensuring authenticity and security in mobile device payment schemes

Benjamin Jones
Department of Electrical and Computer Engineering
University of Auckland
bjon083

ABSTRACT
Even though mobile technology is becoming increasingly prevalent in modern life, the population is still largely unwilling to use mobile payment systems [9]. Furthermore, the longstanding concerns over the legitimacy of users can be solved by having the remote server verify the user by using remote user authentication [10]. Thus it follows that it is worth exploring techniques for mobile device payment systems that ensure authenticity and security. This literature review will address techniques for ensuring authentication and security when dealing with mobile device payment systems and schemes. We explore the academic literature on this aspect, identifying problems and sub problems, approaches, findings and methodologies, and outlining what future work may arise from this gathered information.

INTRODUCTION
In this age of growing influence of mobile technology upon the everyday life, both in frequency of use and in ubiquity, it has become increasingly feasible to expedite the process of payment for goods by introducing the usage of cellular phones into the process. Currently, smart card-based authentication has been used due to low overall cost of implementation, and convenient portability and sale of devices. However, on the other hand, schemes that use mobile devices can provide anonymity when a user is subjected to authentication, can give the user a choice of password, and can provide the opportunity for two parties to agree on a session key, instead of the server generating the key based on its own algorithms.

Mobile device payment schemes can provide a quick, easy and efficient way of payment in theory. Instead of paying with cash, cheque or credit cards, the user can use a mobile device to pay for goods. Speeding up the process of payment will radically change the environment, and this process has become especially probable in light of the omnipresence of mobile devices in everyday life. Bluetooth LE beacons are another possible replacement for mobile devices in transactions, and are suitable in that they emit low energy signals, and do not require close proximity for information transmission to take place.

The usage of wireless payment can reduce the need for users to hold a payment card up to a terminal, or reader, but only when the requirements of sufficient authentication and security are met. Thus, an analysis of papers related to the usage of mobile phones in payment systems can provide information that will become useful for those pursuing the creation of similar projects.

The first half of this literature review highlights several key concepts that are important in explaining the details of authenticity and security in mobile device payment schemes. Grouped by topic, they represent several approaches that are commonalities of the systems mentioned in the papers. The second half of this literature review examines each of these systems in turn, having established the commonalities between each of them.

CONCEPTS

Multi-factor authentication
Multiple proofs may be required to be presented for authentication, which is the basis behind multi-factor authentication. Mobile payment services may be introduced that require multi-factor authentication [3], utilizing forms of proof such as physical objects in the possession of the user, secrets contained in the user’s knowledge base, or analysis of some physical aspect of the user, such as a fingerprint scan, or face recognition [3]. In a particular Android-based system, a USIM card was used as a unique serial number contained within each cellphone [3]. Another system used a multifactor authentication system that combined Transaction Identification Code (TIC) and SMS (Short Message Service) as two proofs needed to authenticate true login. The TIC is a code generated by the bank to be associated with a specific transaction. After this has been generated, the SMS is sent to the user’s cell phone, which will be used to verify that it is in fact the user using this service.

In an Android-based system [3], PIN code authentication, USIM card, and facial biometric authentication were used to verify the user. The user will set up their PIN with the telecommunications company, and the USIM has a unique serial code with each phone. Biometric authentication is undergone using the phone’s camera to detect facial features, using the OpenCV library on Android. The multifaceted nature of the authentication improves the robustness of the process.
FORWARD SECRECY

Forward secrecy is a concept of password authentication where the key to the session is a shared password representing a long-term secret that, if the key is compromised, will be the only secret the unlawfully accessing user gains access to. There are smart card based systems which utilize this concept [1] [2] [3] [4] [5] [6], using a password that has been agreed upon by both the user and the system as a key to exclude access by third parties. This is as opposed to the generation of a key, which cannot enable perfect forward secrecy. In order to enable forward secrecy, the protocol defines that the key must be influenced by login user, service provider and the registration centre. It is clear that forward secrecy is necessary to protect against threats to private keys.

Withstanding attacks

For some systems, there must be the need to remove the password table or verification table, so that attacks will be prevented that can leak the identity of the verifier [1]. A timestamp can also be used for authentication [2], to account for transmission delay, and discrepancies in login/registration time. This means that for attacks which require a certain amount of time to process, if the time required for the normal process has elapsed, then the system will protect itself from any attacks that may ensue after this time. Another system [4] uses bilinear pairings to reduce vulnerability to offline attacks. The bilinear pairings allow for identity-based cryptographic schemes.

Studies have shown that extracting information from patterns of power consumption from smart cards can let attackers acquire login information as well as other logs of activities that are stored on the card [1]. This is one of the evidences why a smart card’s ID, as the only factor of authentication, can leave a user open to many different kinds of attacks.

Other types of attacks that are possible include but are not limited to [4]:

- Replay attack
- Off-line attack
- Forgery attack
- Insider attack

These types of attacks are detailed in full below.

Replay attack

This attack is where an eavesdropper obtains the key by listening to the user provide their authentication details, and then “replaying” it back to the server, whom will not be able to ascertain the difference between the eavesdropper because they have provided the correct details, thus allowing the intruder in. To prevent replay attacks from being successful, a timestamp may be used [2] to verify that the repeat transmission is not from the user logging in twice, but that the transmission delay is too far apart for that transmission to be successful. To have timestamps is to be able to verify that the login with the correct timestamp is the correctly authenticated login, instead of the replay attack gaining unlawful access to the area.

Off-line attack

Offline algorithms work on the data set that has become available without influence of the main system. This is as opposed to online attacks, which is working with the stream of input data. In a system using bilinear pairings [4], offline attacks can be defended from, by creating cryptography using the identity that protects these data sets from being attacked.

Forgery attack

Malicious exploits can be undertaken that are performed by legitimate users, by exploiting actions that that level of user should not be able to access. Some systems [4] allow for protection from forgery attacks by creating more robust forms of authentication to correctly authenticate the user’s privileges.

Insider attack

Insider attacks are when an insider from the company modifies the network of the mobile device payment scheme, having expert knowledge from being employed in the company and being able to modify the rules as they intend. Using identity-based cryptographic schemes [4], one can prevent insider attacks of the remote server.

A phase model of the authentication process

There has been a generalized trend of the steps required for proper authentication [4], which are as follows:

1. Setup phase
2. Registration phase
3. Authentication phase – Consists of a login phase and a verification phase.
4. Password change phase – Allows the user to freely change their password, using a secure method.

In such systems [1] [2] [4] [6], Bilinear mapping will be used in the setup phase, which is essentially a cryptographic hash function that selects a secret key. The registration phase then consists of the user sending a request with their identity (ID) and password (PW). The registration service will then supply a smart card with these parameters, sending it to the user securely.

Each time the user logs into the system, he will login, then a session key agreement will take place, followed by mutual authentication and implied forward secrecy. The login is verified using the various checks involved with the specific
system. An optional password change phase is available to the user if they would like to freely change their password.

Verifying users using timestamps
In several systems [1] [4], timestamps have been used to verify transmission delay and prevent replay attacks. The payment information may include, but not be limited to: payment key, execution status, timestamp, application ID, short description, amount, currency code and mobile platform OS, among other pieces of information relevant for authentication. The idea is that once the timestamp has been recorded, the period of time which has elapsed will start running, and once it has reached the limit of time required for the average delay of transmission when a normal transaction has been assumed to take place, then that time period will expire. This time limit will reduce the chance of replay attacks occurring, which have been discussed earlier in this review.

Using both Mobile and Web channels of authentication
Several systems [5] [6] use both the mobile and web channels for authentication. The drawback of such systems is that they require a password table to refer to, which isn’t the case in certain other systems [1] that are more impervious to off-line attacks. Both systems use username/password combinations, storing identity numbers in the cell phones via SIM or other means. The combination of mobile and web authentication can be used to create forward secrecy by having the scheme utilize a key-agreement protocol for passwords.

AN ANALYSIS OF EXISTING SCHEMES

Scheme #1: An enhanced smart card based remote user password authentication scheme [1]
This is a smart-card based remote user scheme that uses password authentication, emphasizes simplicity, and provides security against several kinds of attacks. To ensure security regarding this password scheme, forward secrecy is required, and in order to achieve this, one must have a key-agreement protocol that happens during the authentication phase. This ensures that if one of the long-term keys is compromised, then the history of keys attached to that one key will not be compromised in the chain; it will only be the one piece of information that is attached to that key that will be compromised. There is no need for a password or verification table, and thus this avoids the problem of leak of verifier possibly happening. A robust authentication scheme is required to prevent information on smart cards from being extracted, such as through analyzing patterns in the power consumption.

Scheme #2: An efficient password authentication scheme for smart card [2]
This implementation uses the RSA SecurID Mobile SDK to generate software tokens, using timestamps to take into account the possibility of transmission delay, and differences in time that may be calculated between login and registration times. This reduces the chance of replay attacks occurring successfully. The system occurs in several phases: in the registration phase, the user submits their identity and password into the Key Information Centre (KIC). The KIC then issues a smart card with a unique value having been generated for the user, and the user is now enabled to insert the smart card and insert their username and password with their login request message. The server receives the login request and checks the identity and password of the user, as well as accounting for transmission delay, and checking if it is small enough, and if the timestamps are standard.

Scheme #3: Android-based mobile payment service protected by 3-factor authentication and virtual private ad-hoc networking [3]
This scheme uses multifactor authentication revolving around a pair of mobile payment devices, a reader and a client. It combines PIN code, USIM card and facial biometric authentication. The USIM card is designed to provide the opportunity for mutual authentication, and modern day SIM cards usually contain a SIM and USIM application. The unique serial code contained within the USIM, along with the forward-facing camera provided to undergo biometric analysis, and the PIN authentication as provided as a key-agreement protocol between the two parties, provides three levels of authentication to the process. The Ad Hoc application on the mobile phone utilizes the Ad-Hoc-Mode WiFi driver module, which is located inside the Linux Kernel. PIN Authentication is executed using an Android-based WebKit library. Card authentication relies on the RIL driver module. The face authentication uses an open-source OpenCV library for the Android OS. These robust and multifaceted authenticity checks use Ad-Hoc networking to provide multifactor authentication with usage of the smart phone and the applications that are available on it.

Scheme #4: An improved remote user authentication scheme with smart cards using bilinear pairings [4]
This proposes an extension to an existing system developed by Das et al. [7], which receives a login request of a user and, if the login request is valid, allows the user to log in. Flexible password change is also allowed, to users who have already registered. However, in the improved scheme, general vulnerabilities in types of off-line attacks are fixed. In this version also, is the option to change password by the user’s own choice, without need of help from a remote server. This is achieved by bilinear pairings, specifically the Weil or Tate pairings, which allow construction of identity-based cryptographic schemes. They review Feng et al.’s authentication scheme for smart cards [8], which consisted of the setup phase, the registration phase, the login phase and the verification phase. However, in this case, it is simplified by combining the login and verification into an authentication phase, and adding a password change phase. The timestamp verification is used in this scheme, avoiding
replay attacks, withstandung forgery attacks, insider attacks and offline attacks. The added flexibility of a possible password change also makes this service valuable.

**Scheme #5: A multi-factor security protocol for wireless payment-secure web authentication using mobile devices [5]**

Most services only use either the Web channel of authentication, or the Mobile channel, but very few use both channels. This is an example of a system that uses both the Web and Mobile channels to confirm the identity of a user who is trying to log into the system. It combines a Transaction Identification Code (TIC) and SMS (Short Message Service) to provide security. The TIC is used to identify singular transactions which are user specific, and issued by the bank to the user. When the user inputs their username and password, the identification code (TIC) is generated, and used to authenticate the transaction. Once this has happened, an SMS is sent to the user’s phone, for further verification purposes. The user specific code generated for each transaction serves as a key to make data available to the user, but only for this transaction. The transaction time required for SMS to take place is a cost worth considering. This form of two way authentication is completely secure, and rather easy to implement. It is the bank’s duty to handle the TIC generation algorithms for key generation.

**Scheme #6: User authentication using mobile phones for mobile payment [6]**

Much like in Tiwari et Al. [5], this scheme also uses both the Mobile and Web channels in combination to confirm the identity request. The differing factor of Sung et Al [6] from Tiwari et Al. is that the paper proposes Transaction Certificate Mode (TCM) for this. This is a form of offline approval, with the TCM representing a payment gateway to ensure the security of sensitive information against attacks. There are three main security risks that are addressed in this scheme: stolen device, borrowed device, and infected device. An International Mobile Equipment Identity Number, or IMEI number, is used to identify which devices are valid and which are not. It can be used to stop stolen phones from accessing the network if they are from a country which is invalid. Thus, offending phones can be blacklisted by the server, and since the IMEI number is stored on the SIM, it can be used to render the mobile payment device effectively useless.

**SUMMARY**

There are many forms of user authentication that are possible when creating a scheme that can secure and protect against attacks. It is important to take into consideration various types of attacks when designing the scheme, as well as enabling a key-agreement protocol in order to ensure forward secrecy of the key. Designing the scheme without the need for a verification or password table can also make sure that sensitive information from the verifier will not be leaked. The scheme is to be designed so that the user can safely have a transaction with the information being as secure as possible.

**FUTURE WORK**

More research particularly in the areas of the kinds of password input types would be valuable. Fingerprint analysis and other forms of authentication with regard to mobile payment systems could be explored in literature, as well as more information about attacks based on extracting information based on patterns in power consumption.

Further research could be made into other forms of biometric analysis such as fingerprint, palm print, iris recognition, or voice.

More research into applications for mobile devices that are OS-specific may be helpful, especially if we are looking at the internals of Android (as explored in [3]), or iOS, or other mobile operating systems.

**REFERENCES**


NOTE TO THE MARKER
In my literature review I have used additional references to support my main arguments. The main six references I draw on are [1], [2], [3], [4], [5] and [6].