A Two-factor Authentication Mechanism Using Mobile Phones

Nima Kaviani, Kirstie Hawkey, Konstantin Beznosov
{nimak, hawkey, beznosov}@ece.ubc.ca

Laboratory for Education and Research in Secure Systems Engineering
lersse.ece.ubc.ca
University of British Columbia
Vancouver, Canada

Technical report LERSSE-TR-2008-03*

Last Modification Date: 2008/08/20

Abstract

Mobile devices are becoming more pervasive and more advanced with respect to their processing power and memory size. Relying on the personalized and trusted nature of such devices, security features can be deployed on them in order to uniquely identify a user to a service provider. In this paper, we present a strong authentication mechanism that exploits the use of mobile devices to provide a two-factor authentication method. Our approach uses a combination of one-time passwords, as the first authentication factor, and credentials stored on a mobile device, as the second factor, to offer a strong and secure authentication approach. We also present an analysis of the security and usability of this mechanism. The security protocol is analyzed against an adversary model; this evaluation proves that our method is safe against various attacks, most importantly key logging, shoulder surfing, and phishing attacks. Our usability evaluation shows that, although our technique does add a layer of indirectness that lessens usability, participants were willing to tradeoff that usability for enhanced security once they became aware of the potential threats when using an untrusted computer.

*This and other LERSSE publications can be found at lersse-dl.ece.ubc.ca

1 Introduction

Security is considered a secondary task [WT99]. That is to say, users usually are more focused on the main tasks that they need to accomplish (e.g., paying a bill) and are less concerned about protecting their credentials (e.g., username and password). With the development of ubiquitous computing technologies, protecting the credentials of users becomes more of a challenge. In particular, password based identification methods are vulnerable to easily implementable attacks such as key logging and shoulder surfing. Consequently, new methods of protecting users' credentials are needed for applications that may introduce risk to financial or confidential information.

Mobile devices such as mobile cell phones and PDAs are now highly personalized and distributed across a wide population of users. A recent report [mul07] shows that the worldwide unit shipments of multimedia feature rich mobile phones will exceed 300 million units in 2008. Providing usable security mechanisms that take advantage of this wide spread use of mobile devices not only would increase the level of protection for critical information, but may also enhance the chances that security considerations will be embraced by the end users.

Authentication using mobile devices is one way to bring such devices into the realm of security. However, previous research efforts that use mobile devices for authentication purposes, have employed weak authentication (i.e., only a username and password pair) using input and output features of such devices. Weak authentication is known for its vulnerability to several attacks, including shoulder surfing, phishing, and key logging. Moreover, the compact size of mobile devices imposes constraints on their efficient and consistent usability. It is unreasonable to expect a user to enter a potentially long password into a mobile device several times a day. Likewise, we cannot expect users to use small screens of mobile devices as a proper output device for their daily transactions.

We have developed a scheme that enables the use of mobile devices for authenticating users to a web service provider. The approach provides a two-factor authentication mechanism by combining one-time passwords (OTPs), as the first authentication factor, together with encrypted user credentials stored on a mobile phone as the second authentication factor. In this approach, we treated the mobile device as a trusted digital wallet to securely encrypt and store users' long term credentials. These credentials (i.e., her username and password) are encrypted using the public key of the service provider, stored on the mobile device, and are transferred to the service provider when needed. The storage of long term credentials on the mobile device enables users to use stronger passwords for their accounts, as they don't need to remember and retype the passwords for each and every login time. One-time passwords further protect the stored credentials on the cell phone, if stolen or lost, by requiring additional information at the time of log in.

In addition to a description of this authentication protocol, we present the results of security and usability evaluations of our two-factor mobile authentication system. The security analysis evaluates the mobile authentication mechanism against an adversary model. Our analysis shows that the security of our devised method is improved over similar authentication approaches that use mobile devices [MvO07, MWL04, PKP06, WGM04], due to the addition of the OTP which leads to having a strong authentication mechanism. Furthermore, the results of our usability study show that our participants were willing to adopt the new technology once became aware of the potential threats to their passwords when using untrusted computers. Participants indicated they would accept a lower level of usability in return for the higher level of security of the mobile technology. However, for this new technology to be a complete replacement to conventional username/password based systems, it should be significantly simpler.

In the rest of this paper, we focus on the details and findings of our studies. In Section 2 we review a series of related works that use mobile devices for the purpose of authentication or data protection. In Section 3, we present the developed system and describe its security protocol and implementation. Sections 4 and 5, respectively, discuss our methodology to validate the security and the usability of our developed mobile authentication mechanism. Section 7 concludes with a discussion of the opportunities for improving and extending the current technology.

2 Related Work

Enhancing the level of security by using personal mobile devices is attracting attention due to the increasing number of users adopting mobile technologies. Security researchers have started to devise approaches that may increase the level of security in accessing critical information by end users through the employment of mobile devices [MvO07, MWL04, MPR06, OBDS04, PKP06, WGM04]. Here we briefly review the closest ones to our approach. The Guardian framework [MWL04] focuses on protecting the privacy of a mobile user, including securing long-term user passwords and protecting sensitive information, from being recorded. Guardian works as a personal firewall, placed on a trusted PDA. In effect, the PDA acts as a portable privacy proxy. Guardian keeps passwords and other privacy sensitive information out of the reach of malware such as key loggers installed on an untrusted PC. Such sensitive information is displayed on the mobile device; it is up to the user to decide which information can be shown on the untrusted PC by going through them one by one and selecting the ones desired. Guardian is different from our approach in that it requires a high level of interaction with the mobile device by its users. In contrast, in our approach, the level of interaction has been simplified to pressing only a few navigational buttons on the mobile device for the purpose of authentication.

Wu et al. [WGM04] use a mobile phone as a handheld authentication token and a security proxy that allows the system to be used with unmodified third party web services. In this method, a user who wishes to use an internet kiosk to access a remote service requiring authentication would instead connect to a trusted security proxy. The proxy stores the user's passwords and can use them to login to the remote service. It also stores a mobile phone number for each user, to which a short text message (SMS) is sent to complete the authentication. Once the user responds to this message, the user's connection from the kiosk is authenticated. The proxy then operates as a traditional web proxy and mediates all aspects of the user's communication with the remote service, preventing long-term authenticators (e.g., cookies) from touching the kiosk. This approach, however, makes the trusted proxy and the mobile phone potential resources to attackers; if the phone is lost, anyone can be authenticated to the system. The proxy might be a target of DoS attacks as well. In our approach, we provide more security by using a list of OTPs as a second factor during the process of authentication. Furthermore, there is no single point of denial of service (DoS) attack implemented in our mobile authentication system.

Mannan and van Oorschot [MvO07] propose an approach to counter attacks like phishing, key logging, and session hijacking. Their method cryptographically separates a user's long-term secret input from a (typically untrusted) client PC; the client PC performs most computations but has access only to temporary secrets. The user's long-term secret (typically short and low-entropy) is input through an independent personal trusted device such as a cell phone. The mobile device provides the user's long-term secrets to a client PC only after encrypting the secrets using a pre-installed, correct public key of a remote service (the intended recipient of the secrets). The proposed protocol (MP-Auth) realizes such an approach, and is intended to safeguard passwords from key loggers, other malware (including rootkits), phishing attacks, and pharming, as well as to provide transaction security to foil session hijacking. This method is similar to our approach; however, we store the long term username and password on the mobile device. Furthermore, we provide additional security by using a list of OTPs; this protects the user accounts even if the mobile device gets lost or stolen.

Finally, it should be noted that, in contrast to our approach, none of the above mechanisms present a usability evaluation of the devised security solution; making the usability of such systems questionable.

3 Two-factor Authentication Using Mobile Phones

We propose a two-factor authentication system that employs a mobile device to authenticate a user to a web server (i.e. an on-line banking site) through a potentially untrusted personal computer (i.e., a client). The first factor is the combination of username and password that are usually required by web servers. The second factor is a one-time password that would be typed into the browser of the untrusted client and sent to the web server. The username and the password, as the long time credentials of the user, are encrypted and stored on the cell phone and are then transferred to the web server upon a request by the user. The list of OTPs can be provided to the user as an RSA SecureID token [rsa] or following any OTP generation algorithm [Hal94, Rub96]. In our implementation of OTPs, we provide the users with a list of randomly generated OTPs following Rubin's *independent one-time passwords* [Rub96], as it offers improved security features, including independence of generated OTPs and security against shoulder surfing attacks. Storing the long term credentials on the mobile device prevents from repetitive entry of potentially long username and passwords into a mobile device and enables the users to use long and possibly more complicated passwords for their accounts. Furthermore, using an OTP as a secondary authentication credential changes the whole authentication process from weak authentication to strong authentication, thus bringing more security for the users. We have implemented this authentication mechanism using JAVA Mobile Information Device Profile (MIDP) [jav] and the Security and Trust Services API (SATSA) for J2ME [sat] on a Nokia N80 smart phone equipped with a Symbian S60 [sym] operating system (see Appendix B).

While describing the mobile authentication mechanism, we use the following conventions for presenting the entities of our protocol. The pair (u, p) refers to the username and password related to particular service S that a user U needs to use. The pair (K_s, K_{s-1}) refers to the RSA key pair that belongs to the service provider, with K_s being the public key and K_{s-1} being the private key. N represents a randomly generated nonce on the mobile device in order for the user to identify the server. T represents the timestamp generated on the cell phone to mark the time when an authentication request has been made by the user. $h(x)$ represents the hashed value of x and OTP_i represents the i^{th} one-time password. R_{OTP_i} stands for a request R from the service provider for the i^{th} one-time password. The symbol || stands for a concatenation function which usually connects a series of string data. Finally, the symbol $\{\ \}_{K_s}$ is used to represent the results of an encryption by a key K_s, while the symbol $[\ ]_{K_s}$ is used to represent the results of a decryption using the key K_s.

Our authentication protocol comprises the following steps:

1. The public key K_s of the web server is stored on the user's mobile device.

2. The user is required to enter a pair of username and password (u, p) into the mobile device at the time of initialization. The cell phone generates that hashed password $h(p)$, and concatenates it with the username u and then encrypts the pair using the public key of the service provider, thus generating the cipher $\{u||h(p)\}_{K_s}$.

3. At each login time, a time-stamped token T, and a random nonce string N are generated on the cell phone and are then concatenated together with the cipher text $\{u||h(p)\}_{K_s}$ to create a string of the form $\{u||h(p)\}_{K_s}||N||T$.

4. The mobile device encrypts the above string using the public key K_s of the service provider creating $\{\{u||h(p)\}_{K_s}||N||T\}_{K_s}$.

5. The cipher $\{\{u||h(p)\}_{K_s}||N||T\}_{K_s}$ is sent from the cell phone to a bridging client application on the personal computer. Meanwhile nonce N is shown on the screen of the mobile device.

6. The bridging client on the personal computer receives the cipher message over a TCP/IP connection and immediately forwards it to a Firefox extension listening on another TCP/IP port.

7. The Firefox extension receives the cipher text $\{\{u||h(p)\}_{K_s}||N||T\}_{K_s}$, opens an SSL connection with the service provider, and sends the cipher to the server

8. The server decrypts the cipher by applying the RSA deciphering algorithm using its private key twice; once by applying $[\{\{u||h(p)\}_{K_s}||N||T\}_{K_s}]_{K_{s-1}}$, and then by applying $[\{u||h(p)\}_{K_s}]_{K_{s-1}}$ which leads to extracting the deciphered string $u||h(p)||N||T$.

9. The timestamp T is checked to protect against replay attacks, the pair $(u, h(p))$ is checked against the existing set of usernames and passwords, and if a proper match is found, the random nonce $N' = N$ is returned to the desktop client through the SSL channel and is presented to the user on the browser.

10. A request R_{OTP_i} for the i^{th} one-time password is also sent to the browser together with nonce N'.

11. The user should check the nonce N' shown on the browser page with the nonce N shown on the screen. In case there is no nonce shown on the browser or if N' doesn't match N chances are that the user is redirected to a phishing website. Otherwise the user enters the one-time password to the server.

12. In case of a successful match between the OTP_i sent by the user and the OTP_i on the server, the server authenticates the user to the system.

13. The user is also assured of a correct connection with the server, first off, because the cipher text cannot be accessed without the correct private key which is kept on the server. Also the equality of the nonce number shown on the browser page with the one shown on the screen of the mobile device guarantees against session hijacking.

Figure 1 shows the step by step authentication method in our system according to the description above. As can be seen, the user needs to interact with the system at two points. First she initiates the whole scenario by choosing an appropriate service on her cell phone for which she has the credentials already encrypted and stored. Then, once the long time credentials are evaluated by the web server, the user will be prompted to enter one of the OTPs to the personal computer from the list of OTPs that she has already been provided with.

The security of this type of authentication is determined by how well the whole approach guarantees the confidentiality and integrity of exchanged credentials. The usability of the system, however, depends on how easy it is for the user to interact with the system and provide the required credentials at the right time during the process of authentication. The users need to be able to

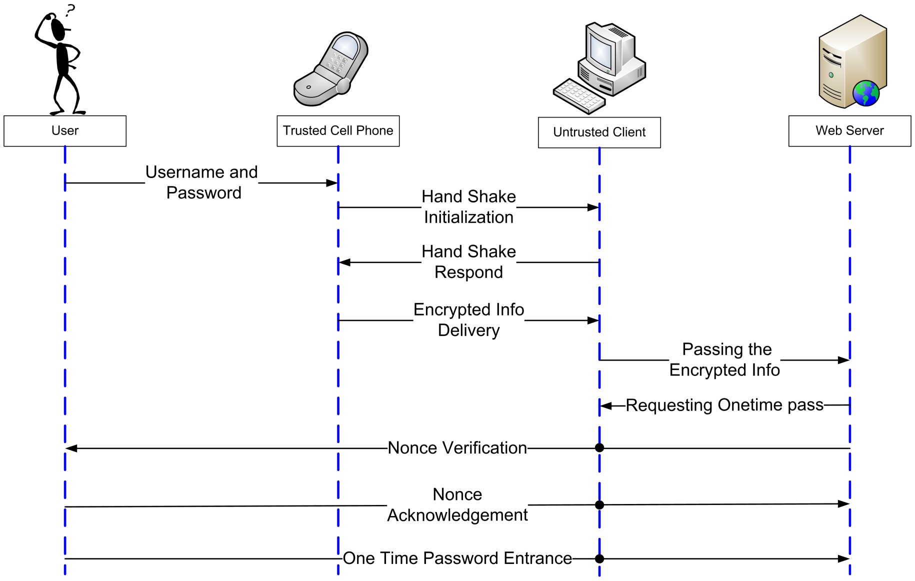


Figure 1: Step by step authentication protocol in our two-factor mobile authentication mechanism

login to the web servers with very small cognitive overhead compared to what they usually do by typing in the username and password to an authentication system at a service provider. In the next two sections, we elaborate on how the security and usability of the approach were evaluated.

4 Security Evaluation of the Mobile Authentication Mechanism

There are a variety of attacks that require to be considered while analyzing the security of our method. In this section, we provide an analysis of the major known attacks to the confidentiality and integrity of users' credentials when using our mobile authentication protocol. We discuss the points of strength and potential weaknesses in our protocol.

4.1 Key Logging Attacks

Our authentication protocol is secure against any key logging attack on a potentially untrusted desktop computer. First of all, as we described earlier, the password p is hashed on the mobile device. Furthermore, the cell phone generates a cipher text $\{\{u||h(p)\}_{K_s}||N||T\}_{K_s}$, which once sent to the desktop computer, is impossible to decrypt as long as the private key K_{s-1} is securely preserved by the service provider. Hence, there is no way for any key logging program of any type, even ones that can capture the screen of a desktop computer, to obtain the long term credentials of the user.

4.2 Lost or Stolen Mobile Device

The mobile device, now carrying confidential information that may lead to financial gains, becomes an important target for theft. A malicious attacker could steal the cell phone and attempt to login to various user accounts. As we discussed earlier, however, the stored long term credentials of the user are not the only credentials required to access an account. The user is also provided with a list of OTPs that are required to be provided to the authentication system during the process of login. Although a stolen mobile device opens the door for possible brute force attempts to find the stored username and password on the cell phone, an attacker needs to also have an OTP to be able to access an account. This gives the user enough time to act to revoke and renew the credentials so as to foil any attacks that may occur at a later time. This does, however, assume that users keep their list of OTPs separate from their cell phones and do not keep the OTPs on the cell phone or in its close proximity.

4.3 Lost or Stolen List of OTPs

Similar to a lost or stolen mobile device, a list of OTPs on its own will be of no use to the attacker. The attacker needs to also have the mobile device to be able to initiate a login process; not having the device is equal to not having the major factor in the process of authentication. As before, this does assume that users keep their mobile devices and OTP list separate.

4.4 Shoulder Surfing

Shoulder surfing implies the ability of an attacker to obtain all or part of a user's credentials by peeking at the information provided by the user during login time. In our authentication mechanism, we provide the user with a list of OTPs, each associated with an index number i. When logging into the system, the user is prompted to provide OTP_i to successfully be authenticated to the system. The attacker could try to peek at the list of OTPs and find out the next few OTPs and then try to use them with a stolen or lost mobile device. In our authentication mechanism, however, the next OTP to be asked from the user is randomly selected from the list of available OTPs. As a result, the malicious user will not be able to determine the next OTP that the server is going to require. This in turn foils attacks that may happen as a result of shoulder surfing. Of course, using specialized devices (e.g., SecureID [rsa]) would reduce the concerns about shoulder surfing even more.

4.5 Phishing Man-in-the-Middle Attack

Phishing is a special type of social engineering in which the attacker resides in between the user and the intended service provider and tries to resemble the behavior of the original service provider in order to fool the user into revealing the required credentials. In our case a phishing attack can happen when the desktop PC is sending the cipher $\{\{u||h(p)\}_{K_s}||N||T\}_{K_s}$ to the service provider. The attacker can try to find a couple of OTPs from the user and try to combine the cipher string and the appropriate OTP to authenticate himself to the service provider. However, the use of nonce enables the user to readily check the conformance and equality of the returned nonce N' from the server with the nonce N generated on the cell phone, thus verifying the correctness and the reality of the contacting server. The use of an SSL connection between the server and the client prohibits from any eavesdropping of the communication channel by the attacker during exchange of the credentials.

4.6 Passive Man-in-the-Middle Attack

In a passive Man-in-the-Middle (MiM) attack, the attacker obtains the cipher text $\{\{u||h(p)\}_{K_s}||N||T\}_{K_s}$ and tries to reuse it on a different occasion (i.e., when he has been able to gain the list of OTPs). This type of attack is not applicable to our authentication protocol, as the cipher text $\{\{u||h(p)\}_{K_s}||N||T\}_{K_s}$ has a timestamp for its generation. The timestamp is checked by the server whenever the message is deciphered by the service provider. If the difference between the timestamp and the current clock of the service provider is greater than a threshold of δ seconds, the server revokes the request and closes the session. System administrators can define the appropriate value of δ. This prevents the attacker from performing a passive MiM attack.

4.7 Active Man-in-the-Middle Attack

In an active MiM attack, the attacker combines passive MiM and phishing to obtain the credentials of the user. From the untrusted computer, the user is first redirected to a compromised server which receives and stores the long term and encrypted credentials of the user. This malicious host then sends the information of the user to the desired service provider and receives the information about the nonce as well as the request R_{OTP_i}. The attacker then creates a phishing website to collect OTP_i. Once OTP_i is obtained, it is sent to the service provider and the attacker can impersonate the user. This represents a sophisticated attack which requires an in-depth understanding of the communication protocol between the modules in our mechanism. However, according to Kirckhoff's law, secrecy as a result of obscurity does not guarantee security and is not intended in our mechanism either. One way to foil this attack is for the user to check the certificate of the host with which an SSL connection is established. Analyzing the certificate of the target host would help the user understand whether the target site is truly the one it claims to be, or whether it is forged. Even though checking the validity of the certificate reduces the usability of the system, it considerably helps to minimize the possibility of an active MiM attack.

4.8 Session Hijacking and Parallel Session Hijacking

In a session hijacking attack, malware or an attacker can take over a session already opened by the user, and use the stored information in the session to perform other transactions or alter the transactions. Our current implementation of the protocol does not prevent against such type of attacks as the main intention behind our protocol is to protect the credentials of the user during the process of authentication and there is no mechanism to preserve the integrity of transactions in our system. However, a solution to this problem can be obtained by implementing a transaction integrity check that requests a user confirmation once a transaction happens. According to [MvO07], a proper chaining of protocol messages between the mobile device and the personal computer may also help with preventing a parallel session hijacking attack.

4.9 Denial of Service Attack

Depending on the method of communication between the mobile device and the personal computer, a DoS attack might be possible to carry out. If a wireless or Bluetooth communication method is used between the mobile device and the personal computer, an attacker might be able to intercept or destroy the actual packets and thwart a proper communication between the mobile device and the PC. Similarly, it is possible for an attacker to perform DoS attacks during the process of message exchange between the PC and the service provider. Nonetheless, as mentioned earlier, our authentication method is more concerned with preserving the confidentiality and integrity of users' long term credentials, and DoS does not really compromise the confidentiality of these credentials, rather it downgrades the quality of service.

4.10 Formal Analysis of the Security Protocol

Further to the above analysis of the adversary model defined for our authentication mechanism, we also analyzed and evaluated the security of our authentication protocol using the AVISPA tool. AVISPA (Automated Validation of Internet Security Protocols and Applications) [arm05], is a widely used verification and validation tool that helps with automatically analyzing an internet security protocol by simulating various attacks against the protocol. In order for our protocol to be implemented in AVISPA, we delegated the role of the user partly to the mobile device (to verify the correctness of the returned nonce), and partly to the PC, (to send the OTP to the server). We coded our protocol in AVISPA's High-Level Protocol Specification Language (HLPSL) and tried the three existing AVISPA tests, namely `OFMC`, `CL-AtSe`, and `SATMC`, on the implemented protocol. All three tests evaluated our protocol as `SAFE`. We did not check our protocol with the `TA4SP` backend as it was not supported by our implementation of the protocol. The HLPSL code for our implementation can be found in Appendix A.

5 The Usability Evaluation of the Mobile Authentication Mechanism

In Section 4, we analyzed the security of our devised authentication mechanism by defining an adversary model and evaluating our authentication approach against the defined attacks. In this section we report on a formative evaluation of our protocol. We conducted the evaluation to determine how users might respond to adopting the mobile authentication mechanism for their purpose of authentication to an on-line financial account, in particular when accessing such accounts on an untrusted computer. It is important to conduct a usability study of the approach, as the new mechanism has added complexity of authentication as compared to a traditional login mechanism.

5.1 The Study Design

Our main research goals for this study were *1) to investigate the usability of our two-factor authentication scheme using mobile devices for the purpose of authentication*; and *2) to investigate the factors that would impact willingness to employ the mobile authentication system, given the additional cognitive burden in contrast with traditional authentication mechanisms.*

Research in the area of usable security shows that obtaining observational data about users' security practices is challenging [EKM+07]. Interviews and surveys have been successfully used to get a sense of participants' security concerns and usual security preserving actions [FHH+02, DHC06]; however, participants may report making particular security decisions, when in reality their actions may differ [GCEA06]. Usability studies of secure systems are also challenging as participants of such studies may not be motivated to protect study data as if it is their own [WI05, WT99]. However, conducting a similar study with real financial information may violate participants' privacy. We, therefore, opted to have participants login to a simulated bank server using a provided user name and password.

For our evaluation, we chose a within subject lab study in which the participants used both traditional authentication and our new mobile authentication technique to login to a simulated bank server on the study computer in the lab. This allowed participants to reflect on their security and comfort when using both protocols. Our authentication mechanism is particularly valuable when an untrusted computer must be used to perform online transactions. According to Technology Acceptance Model (TAM) [JPB+06], a perceived need for security also influences user acceptance. We therefore needed to ensure that participants understood the risks of using such computers. This was achieved by showing to the participants, half way through the study, that there was a key logger installed on the untrusted PC that was recording all key strokes made. We refer to this change in the participants' mental model as *risk priming*. Hence, our conditions comprise the four combinations of using two authentication systems both before and after risk priming.

5.2 Methodology, Data Collection, and Analysis

We provided participants with a pre-task questionnaire in order to obtain an understanding of their general attitudes towards using their online financial accounts, and their level of safety and concern when dealing with their accounts. In order to measure the participants' feeling of safety or concern, we provided them with five Likert-scale responses (ranging from very little to very much) which were then converted to numeric values (i.e., 1 = very little and 5 = very much). When analyzing the responses, we calculated the mean of the numeric values for the responses to get a sense of the overall perceptions of the participants.

The study was conducted in two sets of two authentication tasks (traditional authentication, mobile authentication). In the first set, the users were asked to play the role of *John Smith* and use his associated username and password to login to a virtual bank account on a bank server (set up locally in the security lab at the university). For the first task, the users were asked to login to the bank server using the traditional login mechanism to enter the given username and password into the PC. For the second task, the users were asked to use the mobile authentication mechanism and the stored credentials on the cell phone (i.e., the username and the password) to login to the bank account. The participants were asked to imagine that it was their own cell phone, their real bank account, and their real username and password. Throughout the study, the participants were provided with an instruction sheet explaining how to use both authentication mechanisms. The participants were able to look at the instructions and ask for clarification from the researcher at any time during the study.

Once the first set of tasks was complete, the participants were provided with a questionnaire asking about their experience with each authentication method. The goal of the questionnaire was to measure the level of comfort, satisfaction, and usability of both authentication methods. We then primed our participants' minds to the risks of using an untrusted computer, showing the log file from the key logger installed on the computer. The log showed that for traditional authentication mechanism, the full username and password of John Smith were recorded, but when using the mobile authentication system, only the one-time password was saved.

For the second set of authentication tasks, we asked the participants to redo the two authentication tasks keeping the untrusted nature of the computer in mind. We allowed them to opt out of either of the authentication mechanisms if they did not feel secure using it. Seven of the participants opted out of using the traditional login mechanism, but all were willing to re-login to their accounts using the mobile authentication mechanism. After this second set of authentication tasks, we asked the participants to again fill out the questionnaire.

At the end of the experiment, we conducted a 15 minute long semi-structured interview with the participants asking three major questions: *i) what are your perceptions of the mobile authentication approach? ii) If it were your real username and password for your bank account, would you be willing to participate in the study?*, and *iii) If it was your real bank account and your real cell phone with your account credentials stored on it, would you be willing to participate?*

We measured several factors that may impact users when adopting mobile authentication technology through the above mentioned questionnaires. These include *users' perceived level of trust* in using the new mechanism, their *level of comfort* with giving control of their passwords to a program, *perceived ease of use*, *perceived necessity and acceptance*, *security awareness*, *location awareness*, and *physical control* over the device. We also considered *time-to-completion* of the authentication tasks as another measure for the usability of our approach. Our post-session interviews provided a richer interpretation of the quantitative results. The Wilcoxon matched-pairs single ranks test was used for pair wised comparisons of the significance of changes in users' attitudes for traditional and mobile authentications before and after risk priming.

5.3 Participants

Nine participants (7 males, 2 females) took part in the user study. One of our participants was older than 35, five of them were between 25 and 35, and the other three were between 20 and 24. All participants were graduate students recruited from two Canadian universities: six of the participants were majoring in computer science, one in information technology, one in civil engineering, and one in digital media. For this preliminary formative evaluation, we used a convenience sample; a future evaluation with a more mature version of the technique will incorporate a broader range of potential users. It should be noted that five of the participants had a background in computer security. We hoped to get feedback on the usability of the mechanism from both security experts and potential non-expert users of the mobile authentication system.

All of the participants indicated that they used computers and accessed the internet on a daily basis. Seven used their cell phones every day, and the other two used it a couple of times a week. When questioned about their financial activities, all participants stated they made online financial transactions (67% of them doing so a couple of times a week). Almost all participants (88%) reported conducting online banking, while 66% reported making online credit card transactions, and 55% made online bill payments.

5.4 Results

We now present some of the results that were obtained in the usability evaluation. Due to space limitations, we focus only on the most significant results.

5.4.1 General Security Attitudes for Financial Transactions

As shown in Figure 2, participants were more concerned about accessing their on-line financial accounts compared to their email accounts. Participants' indicated that their level of concern was highly dependent on the computer that they need to use for accessing their accounts, particularly when accessing their financial accounts. However, they indicated that their level of concern was not as dependent on the Internet connection that they use (e.g., wireless or wired), or the location (e.g., school or internet café) where they access their information. As for their perceived level of safety for using different computers for financial transactions, as shown in Figure 3, the participants indicated a higher level of safety when using their personal computers, as compared to the computers at the lab or at work. The computers at an internet café or a kiosk were considered very unsafe by the participants. Interestingly, as their perceived level of safety with the computer decreased, so did the degree that the perceived safety depended on the internet connection. At an internet café or a kiosk, participants indicated that their perceived level of safety did not depend at all on the internet connection; it was low whatever the connection.

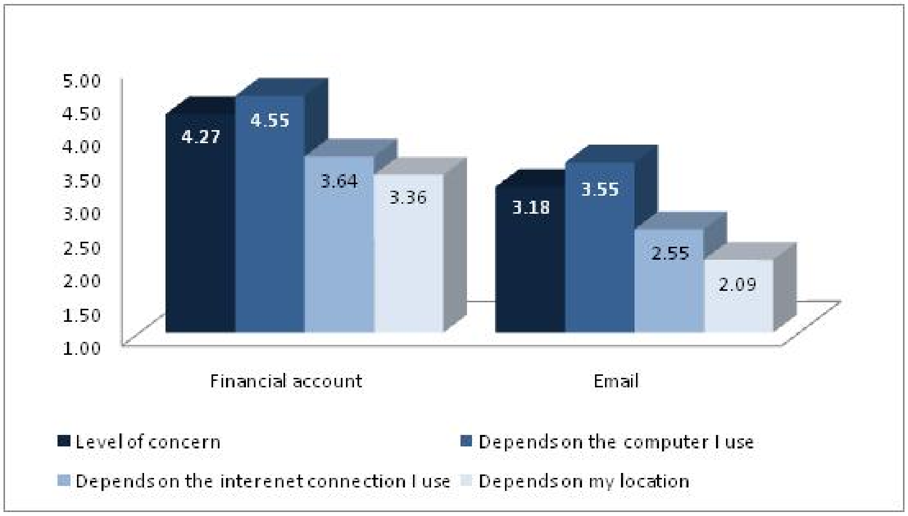


Figure 2: Responses to: Are you concerned about the security of your online financial accounts? Participants indicated a level of concern, and whether that concern is affected by the computer in use, the internet connection, or the location (1=Not at all; 5=Very Much).

5.4.2 Comparative Usability of the Authentication Techniques

We next compare the usability of the two authentication techniques. We first present results of the time to completion for each authentication task (Figure 4).

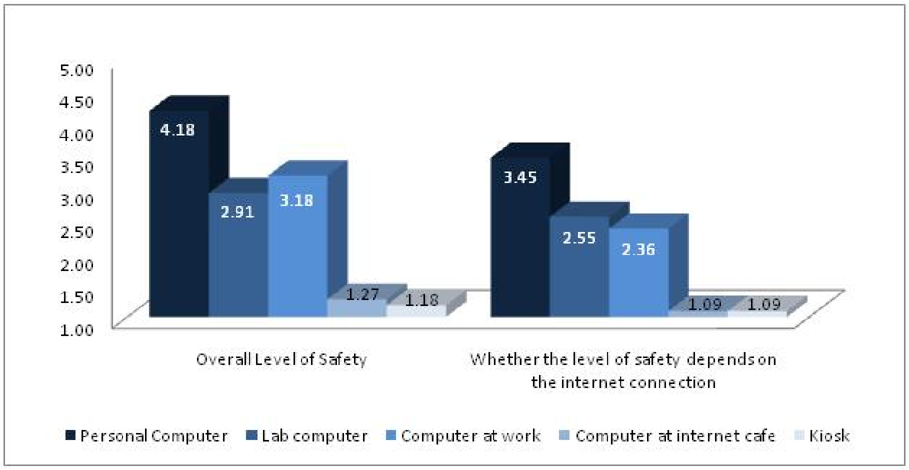
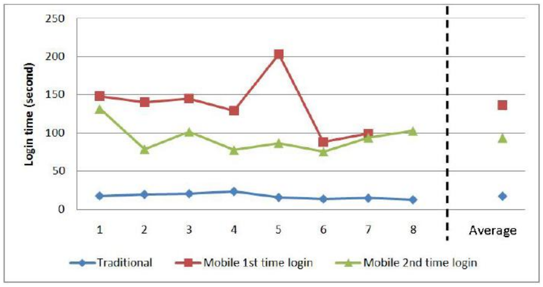


Figure 3: Responses to: How safe do you feel when you use each computer for financial transactions? Participants indicated a level of safety, and whether that perception of safety is affected by the internet connection in use (1=Not at all; 5=Very Much).

Due to some technical issues we lost the time-to-completion data for one of our participants. Here we report only on the eight obtained results. It took only 17.4 seconds on average for participants to login to their account using the traditional authentication method for the first login task (as noted above, only two participants elected to login with the traditional method after the risking priming). Login with the traditional mechanism is likely even faster once users know their username and password by heart and can type it rapidly into the computer. For the mobile authentication mechanism, however, login was much slower (136 seconds for the first task; 94 seconds for the second task). This is significantly longer than traditional login mechanism even in the best case. However, the considerable time reduction between sets makes us believe that once users practice the mobile authentication method and get familiar with the device interactions, their efficiency will improve.

We also asked participants which authentication mechanism they found more usable. As expected, both before and after risk priming all participants indicated that the traditional authentication mechanism was more usable compared to the mobile authentication mechanism. It is likely due to its noticeably faster time-to-login and its reduced number of steps. However, as will be discussed next, the mobile authentication mechanism was considered more secure than the traditional mechanism by all our participants.



Traditional 1^{st} Login	Mobile 1^{st} Login	Mobile 2^{nd} Login
17.4	136	93.9

Figure 4: Time-to-Completion for each authentication method

5.4.3 Perceptions of Security for the Authentication Mechanisms

We analyzed the post task set questionnaire responses (before and after risk priming) to evaluate participants' security perceptions for both the traditional and mobile login mechanisms (Table 1). One pair of questions asked them to reflect on their trust for the security of each of the two authentication techniques. Level of trust in using the traditional authentication mechanism went down significantly ($z = -2.271,\ p < 0.023$) after risk priming. However, level of trust for the mobile authentication mechanism stayed pretty much the same both before and after risk priming. Figure 5 compares participants' level of trust in each of the two authentication methods before and after risk priming.

We also asked participants how much trust they would have when using each of the techniques on a public computer (Table 1). Their comapred level of trust between mobile and traditional login mechanisms changed from a marginal difference ($z = -1.897,\ p < 0.058$) before priming to a significant difference ($z = -2.719,\ p < 0.007$) after priming. Interestingly, their level of trust for both techniques on a public computer were not affected by the risk priming ($z = -0.816,\ p < 0.414$). What is key is that, independent from risk priming, participants' level of trust for the traditional technique on a public computer was significantly lower than for the general case (before priming, $z = -2.428,\ p < 0.015$; after priming, $z = -2.333,\ p < 0.020$). No significant change was found in their level of trust in the security of the mobile technique when considering an untrusted computer rather than the general case (before priming, $z = -1.730,\ p < 0.084$; after priming, $z = -1.342,\ p < 0.180$).

5.4.4 Evaluation of the Usability/Security Tradeoff

While participants preferred the usability of the traditional authentication mechanism, the increased security of the mobile authentication technique was considered important, particularly for financial transactions on untrusted computers. As shown in Table 1, after the first set of authentication tasks, participants indicated a strong preference for using the traditional login for all their authentications (72% for financial transactions, 100% for non-financial transactions). However, after risk priming, participants' preferences drastically changed for

Table 1: Responses, before and after risk priming, when participants reflected on their trust for the security of the two authentication techniques in general and when using a computer other than their own. They also indicated their preferred login technique for both financial and non-financial activities.

Questions	**Before Risk Priming**		**After Risk Priming**	
(1 = very little, 5 = very much)	**Traditional**	**Mobile**	**Traditional**	**Mobile**
Trust for the security of the technique	3.56	4.22	2.33	4.11
Level of trust when using a computer other than their own	1.78	3.78	1.56	4.00
	% of Participants Preferring Technique			
Preferred login for financial activities	72%	28%	11%	89%
Preferred login for non-financial activities	100%	0%	72%	28%

financial transactions, with 89% of them now indicating a preference for the mobile authentication for financial transactions despite their low rating of its usability. Furthermore, 28% would now prefer to use it for non-financial transactions as well. The preference for the mobile login for authentication to financial accounts was unanimous when we specifically asked participants to consider untrusted computers. However, both before and after risk priming, participants were still willing to use the traditional authentication mechanism when using their own computers, apparently trusting that their personal computers are not compromised.

5.4.5 Perceptions of Viability of Mobile Approach in the Wild

Our quantitative analysis of the results showed that the users are willing to sacrifice on the usability of authentication when they become aware of the potential threats to the system. The new mobile authentication technology was widely accepted by the users in order to login to an unknown and potentially malicious PC. Our post-session interview allowed us to gain insight about participants' perceptions of the long-term viability of the mobile authentication approach.

Our interviews revealed that, although they appreciated the mobile technique for its ability to bypass the untrusted computer when authenticating, they did not completely feel safe with storing their username and password on their mobile devices. For example, they commented: *"... I wouldn't want to keep the password on the cell phone, I would rather keep it in my mind ...* [P7]", *"... I am not very comfortable to save my information on the phone ...* [P8]", and *"... Not familiar with the security of stored information on the phone ... I don't feel comfortable ...* [P3]". One participant was also concerned about safeguarding the OTP: *"... you are now concerned about protecting the mobile and this [one-time passwords] sheet ...* [P5]".

On the other hand, there was some support for the convenience of not having to enter the information each time. One participant felt that their laziness would result in the acceptability of the technology in a long run: *"... I would end up*

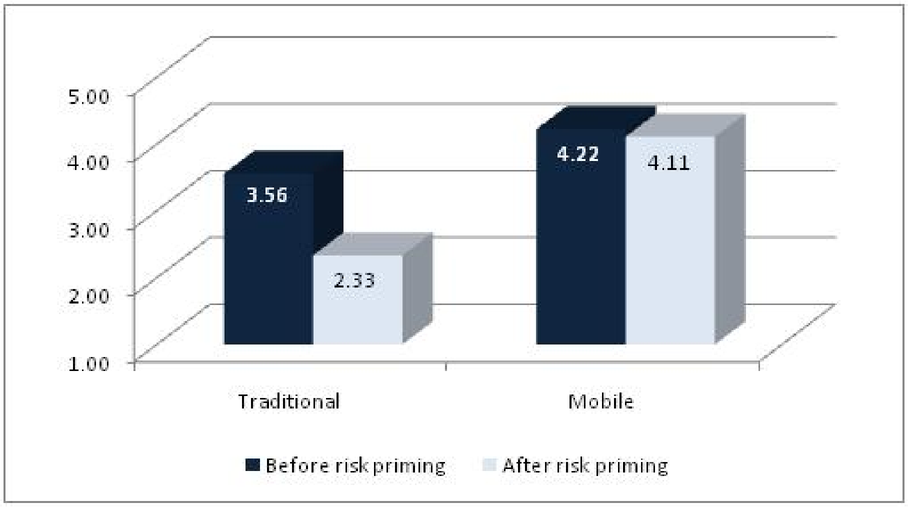


Figure 5: Level of trust in using each authentication method before and after risk priming

saving it, because I am lazy ... [P7]". This participant even compared this technology with using credit cards.: "*... I usually keep [my cell phone] with me all the time and treat it as my credit card ...* [P7]". This quote illustrates that users will have to first learn the culture of using the new mechanism before they feel totally comfortable with using it. Indeed, those participants with some previous background on using two-factor authentication were more comfortable with using the system compared to those without having any background in using the system. For example, one participant mentioned "*...before, I have a similar device like that provided by bank, so I feel more safe if I have the second [factor] ...* [P6]".

According to Anderson [And01], there needs to be a positive feedback for each new technology before it takes off. This also applies to any new technology that requires consent from the users to be adopted. This can be done by providing enough training and support from the institutions that are promoting the use of the new technology. For a new technology to be accepted by the community of users, it should be supported by a reputable authority, so that the users can be reimbursed with their lost assets in case of a loss or a breach in the security of the new technology. This important concept was acknowledged by our participants: "*... The brand name is more important than explaining to the user why [this mechanism] is important ...* [P6]", or "*... if the bank tells me it is something safe, I [will] try it ...* [P9]".

5.4.6 Study Data vs. Real User Data

At the end of the interview, when we asked if the users would be willing to participate the study using their real username and password, all but one participant rejected the suggestion, primarily because we had informed them of a key logger application on the unknown computer. On the other hand, when we asked if participants would like to participate the study with their real username and passwords stored on the mobile device, most of them agreed as they felt safer against potential key logging or shoulder surfing of their credentials. It should be noted that these responses were likely a result of risk priming. If the participants were not aware of the key logger on the PC, and if they had not observed that the username and password stored on the mobile device was not captured by the key logger, we could have received different responses.

One aspect of security built into the mobile authentication technique was not utilized during the authentication tasks; the use of a verification code to prevent from phishing was unsuccessful. Participants were almost always negligent about checking the verification code shown on their mobile device against the one shown on the bank's website and they usually trusted the web server when they saw the page that they expected to see. Whether or not users would be as careless with their own data remains to be seen.

6 Future Work

Evaluating the results of our security and usability studies identified directions for our future research. In terms of improving the security of the designed system, we are considering adding another layer of security to the mobile device to protect the authentication process in case both the mobile device and the OTP list are lost or stolen together. Although the username and password are encrypted on the device, an attacker with both the mobile device and the OTP list could initiate the authentication mechanism and gain access to the confidential information stored on the device. One possibility is to encrypt the stored information with a symmetric master key, potentially generated from a user defined pin code or users' biometric information. Considering that mobile devices incorporate many peripherals which can be used as input devices for collecting biometric information (e.g., facial, iris, voice, and fingerprint information), the latter option of generating a symmetric key from such information should be feasible. Additionally, adding this layer of security to the mobile device should give more confidence to the users with respect to storing their usernames and passwords on the mobile device.

A further line of investigation is motivated by our observation that users were quite negligent about checking the verification code generated on the device against the one shown on the monitor of the untrusted PC. We will investigate methods of bringing this verification code to the attention of users. One possibility is using CAPTCHA [vABHL03], but with a user-oriented interpretation as opposed to its current challenge-response protection against nonhuman attackers.

Finally, we would like to simplify the process of data exchange with the untrusted computer. Using Bluetooth data communication rather than TCP communication is one potential point of investigation. This would exempt users from having to deal with various IP addresses and port numbers when they interact with multiple untrusted machines. By using Bluetooth, they can simply search for and connect to the nearby PC using its given name, which may increase the usability of the technique by simplifying the process of data exchange. However, Bluetooth has its own security and usability problems that require further investigation of this area.

7 Conclusion

We have described our mobile two-factor authentication mechanism for the purpose of protecting long term credentials of users, particulary when they must authenticate while using an untrusted computer. This approach uses a combination of stored credentials on mobile devices and one-time passwords to assure the confidentiality of long term credentials. We analyzed and discussed the potential security threats to our devised authentication technique and provided an analysis of the security protocol using AVISPA to formally prove the security of the protocol. However, as mentioned before, the main advantage of our mechanism is not only its comparative security to other existing approaches, although the two factor authentication does lead to a stronger authentication. We believe that our method of storing encrypted long time credentials on the mobile devices will increase the usability of mobile authentication mechanisms, by reducing the need for input on small handheld devices. Furthermore, users may opt to use more robust user names and passwords if the burden of input is reduced.

Our formative usability study with 9 participants demonstrated that the participants preferred the use of our mobile authentication mechanism compared to the traditional login mechanism when dealing with untrusted computers. The study showed an increase in the level of trust and security of mobile authentication system when the users are primed about the potential threats to their long term credentials. However, for the users to better accept the technology, it should be supported by a reputable authority and they will need to be well trained about how to use the system and the benefits of using the system. Given the overhead of using the system and the minimal perception of risk for personal computers, it should be easy for the users to switch between traditional authentication mechanisms and the new mobile technology according to which is more appropriate given their usage environment. We have identified several directions of future work to improve both the security and usability of our mobile authentication technique. Once these improvements have been incorporated, we will conduct a more rigorous usability study.

8 Acknowledgements

Abdullah Alqattan, David Lewis, Nicholas Pearson contributed to the initial work on the system. Students of the EECE 412 class (Fall 2007) and the LERSSE lab provided feedback throughout its development and evaluation. Thanks also to the anonymous participants in our usability study. This research has been supported by Grant in Aid from the Ministry of Labour and Citizens' Services, British Columbia, Canada.

References

[And01] Ross J. Anderson. Why Information Security is Hard-An Economic Perspective. In *ACSAC*, pages 358–365. IEEE Computer Society, 2001.

[arm05] The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications. In Kousha Etessami and Sriram K. Rajamani, editors, *CAV*, volume 3576 of *Lecture Notes in Computer Science*, pages 281–285. Springer, 2005.

[DHC06] J.S. Downs, M.B. Holbrook, and L.F. Cranor. Decision strategies and susceptibility to phishing. pages 79–90. ACM Press New York, NY, USA, 2006.

[EKM$^+$07] Serge Egelman, Jennifer King, Robert C. Miller, Nick Ragouzis, and Erika Shehan. Security user studies: methodologies and best practices. In Mary Beth Rosson and David J. Gilmore, editors, *CHI Extended Abstracts*, pages 2833–2836. ACM, 2007.

[FHH$^+$02] Batya Friedman, W. David Hurley, Daniel C. Howe, Edward W. Felten, and Helen Nissenbaum. Users' conceptions of web security: a comparative study. In Loren G. Terveen and Dennis R. Wixon, editors, *CHI Extended Abstracts*, pages 746–747. ACM, 2002.

[GCEA06] J. Gideon, L. Cranor, S. Egelman, and A. Acquisti. Power strips, prophylactics, and privacy, oh my! pages 133–144. ACM Press New York, NY, USA, 2006.

[Hal94] N. Haller. The s/key (tm) one-time password system. *Symposium on Network and Distributed System Security*, pages 151–157, 1994.

[jav] http://java.sun.com/products/midp/.

[JPB$^+$06] T. James, T. Pirim, K. Boswell, B. Reithel, and R. Barkhi. Determining the Intention to Use Biometric Devices: An Application and Extension of the Technology Acceptance Model. *Journal of Organizational and End User Computing*, 18(3):1–24, 2006.

[MPR06] Jonathan M. McCune, Adrian Perrig, and Michael K. Reiter. Bump in the Ether: A Framework for Securing Sensitive User Input. In *USENIX Annual Technical Conference, General Track*, pages 185–198. USENIX, 2006.

[mul07] Multimedia Mobile Phone Shipments Surpass TV Shipments in 2008 According to MultiMedia Intelligence. MultiMedia Intelligence, 2007.

[MvO07] M. Mannan and P.C. van Oorschot. Using a personal device to strengthen password authentication from an untrusted computer. Technical report, 2007.

[MWL04] Boris Margolin, Matthew Wright, and Brian Neil Levine. Guardian: A Framework for Privacy Control in Untrusted Environments. Technical Report 04-37, University of Massachusetts, Amherst, June 2004.

[OBDS04] Alina Oprea, Dirk Balfanz, Glenn Durfee, and Diana K. Smetters. Securing a Remote Terminal Application with a Mobile Trusted Device. In *ACSAC*, pages 438–447. IEEE Computer Society, 2004.

[PKP06] Bryan Parno, Cynthia Kuo, and Adrian Perrig. Phoolproof Phishing Prevention. In Giovanni Di Crescenzo and Avi Rubin, editors, *Financial Cryptography*, volume 4107 of *Lecture Notes in Computer Science*, pages 1–19. Springer, 2006.

[rsa] http://www.rsasecurity.com.

[Rub96] Aviel D. Rubin. Independent one-time passwords. *Computing Systems*, 9(1):15–27, 1996.

[sat] http://developers.sun.com/mobility/apis/articles/satsa2/.

[sym] http://www.s60.com/.

[vABHL03] L. von Ahn, M. Blum, N.J. Hopper, and J. Langford. CAPTCHA: Using hard AI problems for security. *Proceedings of Eurocrypt*, 2003, 2003.

[WGM04] Min Wu, Simson Garfinkel, and Rob Miller. Secure Web Authentication with Mobile Phones. In *DIAMCS Workshop on Usable Privacy and Security Systems*, July 2004.

[WI05] Tara Whalen and Kori M. Inkpen. Gathering evidence: use of visual security cues in web browsers. In *Graphics Interface*, pages 137–144. Canadian Human-Computer Communications Society, 2005.

[WT99] Alma Whitten and J.D. Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *The 9th USENIX Security Symposium*, pages 169–183, 1999.

APPENDIX A
The AVISPA Code for the Mobile Authentication Protocol and the Analysis Results

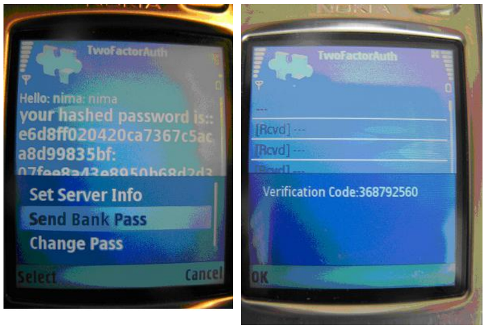
```
role mobile(M, PC, S : agent,
  Es : public_key,
  H  : hash_func,
  P  : text,
  SND, RCV : channel (dy)) played_by M def=

  local State   : nat,
        T, N    : text,
        U, HSD  : message

  init State := 0

  transition
    0. State   = 0 /\ RCV(start) =|>
       State' := 2 /\ T' := new ()
         /\ N' := new ()
         /\ SND(M.PC.{{H(M.P)}_Es.T'.N'}_Es)
         /\ secret({H(M.P)}_Es, u, {M, S})
         /\ witness(M, S, pass, H(M.P))
end role

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

role pc(M, PC, S : agent,
  OTP_i    : text,
  SND, RCV : channel (dy)) played_by PC def=

  local State : nat,
    N : text,
    X : {{message}_public_key.text.text}_public_key

  init State := 1

  transition
    1. State   = 1 /\ RCV(M.PC.X') =|>
       State' := 3 /\ SND(M.PC.S.X')

    3. State   = 3 /\ RCV (PC.S.N') =|>
       State' := 5 /\ SND (PC.S.OTP_i)
       /\ witness (PC, S, otp_ver, PC.OTP_i)
end role

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

role server(M, PC, S : agent,
  Es : public_key,
  H  : hash_func,
  OTPs : (agent.text) set,
  Pass : (agent.text) set,
  SND, RCV : channel (dy)) played_by S def=
  local State    : nat,
        P , T, N : text,

  init State := 0

  transition
    0. State   = 0
         /\ RCV(M.PC.S.{{H(M.P')}_Es.T'.N'}_Es)
         /\ in(M.P', Pass) =|>
       State' := 2
         /\ secret(H(M.P'), v, {M, S})
         /\ SND(PC.S.N')
         /\ wrequest(S, M, pass, H(M.P'))

    2. State   = 2
         /\ RCV(PC.S.P')
         /\ in (PC.P', OTPs) =|>
       State' := 4
         /\ wrequest(S, PC, otp_ver, PC.P')
end role

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

role session(M, PC, S : agent,
   Es : public_key,
   H : hash_func,
   P, OTP_i : text,
   OTPs : (agent.text) set,
   Pass : (agent.text) set) def=

  local S_S, R_S, S_M   : channel (dy),
        R_M, S_PC, R_PC : channel (dy)

  composition
    mobile(M, PC, S, Es, H, P, S_M, R_M)
 /\ pc    (M, PC, S, OTP_i, S_PC, R_PC)
 /\ server(M, PC, S, Es, H, OTPs, Pass, S_S, R_S)
end role

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

role environment() def=

  local OTPs : (agent.text) set,
        Pass : (agent.text) set
  const
    m, s, pc : agent,
    es : public_key,
    h : hash_func,
    u, v, nonce : protocol_id,
    pass, otp_ver : protocol_id,
    pm, otp, ipm, iotp : text

  init    Pass := {m.pm, i.ipm}
       /\ OTPs := {pc.otp, i.iotp}

  intruder_knowledge = {m, s, pc, h, ipm, iotp}
  composition
    session(m, pc, s, es, h, pm, otp, OTPs, Pass)
 /\ session(m, i, s, es, h, pm, iotp, OTPs, Pass)
 /\ session(i, pc, s, es, h, ipm, otp, OTPs, Pass)
end role

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

goal
  secrecy_of u, v
  weak_authentication_on pass
  weak_authentication_on otp_ver
end goal

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

environment()
```

AVISPA Evaluation Results of our Protocol

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  mas.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 1.22s
  visitedNodes: 918 nodes
  depth: 10 plies

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

% CL-AtSE
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  mas.if

GOAL
  As Specified
```

```
BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 320583 states
  Reachable  : 159108 states
  Translation: 0.01 seconds
  Computation: 11.48 seconds

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

% SATMC
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  BOUNDED_SEARCH_DEPTH
  BOUNDED_MESSAGE_DEPTH

PROTOCOL
  mas5.if

GOAL
  %% see the HLPSL specification..

BACKEND
  SATMC

COMMENTS

STATISTICS
  attackFound               false     boolean
  upperBoundReached         true      boolean
  graphLeveledOff           4         steps
  satSolver                 zchaff    solver
  maxStepsNumber            30        steps
  stepsNumber               5         steps
  atomsNumber               1531      atoms
  clausesNumber             8708      clauses
  encodingTime              1.05      seconds
  solvingTime               0.001     seconds
  if2sateCompilationTime    0.11      seconds

ATTACK TRACE
  %% no attacks have been found..
```

APPENDIX B
The Implemented Prototype



Hello: nima: nima
your hashed password is::
e6d8ff020420ca7367c5ac
a8d99835bf:
07fee8a43e8950b68d2d3

[Rcvd] ---
[Rcvd] ---

Verification Code:368792560

Figure 6: Snapshots of our Java MIDlet prototype, implemented on a Nokia N80 with a Symbian S60