ENHANCING THE SECURITY OF MOBILE E-COMMERCE WITH A HYBRID BIOMETRIC AUTHENTICATION SYSTEM

Rachid Bencheikh, Luminita Vasiu
Wireless IT Research Centre, University of Westminster, 115 New Cavendish Street, London, UK

Keywords: Biometrics, Authentication, E-commerce, M-commerce, Wireless, Speech recognition.

Abstract: Mobile devices and wireless technologies seem destined to make a large and continuing impact on our lives. Mobile devices especially have been widely used in the last few years, and recent developments in wireless technologies have provided some new solutions to connectivity problems. Wireless technologies provide a new channel for implementation of mobile payments systems, the potential of short-range wireless technologies in commercial markets is enormous. Furthermore, as the popularity of m-commerce increases, so does the need for protecting personal privacy and online data. Several user authentication schemes for mobile e-commerce are starting to be introduced. This paper discusses some single factor and hybrid authentication methods currently in use, or being planned, for e-commerce and m-commerce. It also suggests a hybrid three-factor authentication scheme for mobile commerce, especially for voice-based mobile commerce, that uses speech recognition and speaker verification technology. Some issues relevant to such a scheme are also discussed.

1 INTRODUCTION

One outcome of the lack of user authentication in electronic commerce (e-commerce) is a greater incidence of identity theft and fraud. A notable attempt to reduce these problems is Secure Electronic Transactions (SET) (GPayments, 2002). SET was supported initially by Mastercard, Visa, Microsoft, Netscape, and others, SET attempts to enable participants in an e-commerce transaction to authenticate themselves to each other using public key cryptography for creating digitally signed documents that would be exchanged among the participants. SET has not been successful to date for a number of reasons, including high costs, complexity related to the supporting Public Key Infrastructure (PKI), interoperability problems, and the fact that it requires consumers to install an electronic wallet on their PCs to perform the necessary cryptographic tasks.

Visa, Mastercard and American Express have introduced some additional security measures to protect against online credit card fraud. These measures are largely based on knowledge of a password or Personal Identification Number (PIN) for user authentication during an online transaction.

Authentication based solely on knowledge or "something you know", such as a password, is typically referred to as single factor authentication. The possession of a smartcard, in addition to using a password, introduces a stronger hybrid two-factor authentication, since possession or "something you have" is also required for authentication.

Three-factor authentication, which adds "something you are", would be an even stronger and more secure form of authentication, and introduces biometrics into the scene of authentication technologies. At present, this level of security is not generally available for online commerce (Corcoran, 2002). As the performance characteristics and costs associated with biometrics becomes more widely understood, and as the underlying technology gets better, three-factor authentication could become prevalent. One area in which three-factor authentication might be especially useful is mobile commerce, which is the term used to describe commerce transactions conducted using a mobile phone or other handheld wireless device. Although not yet a widespread phenomenon in the UK, mobile commerce transactions using a mobile phone may be

Bencheikh R. and Vasiu L. (2005).
ENHANCING THE SECURITY OF MOBILE E-COMMERCE WITH A HYBRID BIOMETRIC AUTHENTICATION SYSTEM.
In *Proceedings of the Second International Conference on e-Business and Telecommunication Networks*, pages 247-253
DOI: 10.5220/0001423902470253

dependent on the additional security that three-factor authentication can provide.

Perfect authentication would be a process where every impostor is rejected, and every legitimate person is correctly authenticated, even in the scenario where the impostor knows all of the person's private information. Currently, no method of perfect authentication exists (Basu, 2003). Some methods of biometrics, such as a retinal scan, are 99.9% secure, but all biometric methods of authentication are at risk in some ways. Other methods include zero-knowledge proofs, and the use of public key cryptography in synthesis with a trusted, highly secure certification authority (Bolle, 2004).

2 SINGLE FACTOR AUTHENTICATION

Credit card companies are beginning to introduce single factor authentication schemes based on information known to a cardholder in order to help reduce fraudulent online credit card transactions. Visa International has introduced 3-D Secure, which requires users to first register their Visa cards for the service. During enrolment, users select a password to be used when shopping online. During the purchase transaction, users enter their Visa card numbers as well as their passwords, which provides the additional layer of security. Mastercard has a somewhat different version, called Secure Payment Application (SPA), which requires that a kind of electronic wallet be downloaded to a user's machine (Shi, 2004). This wallet is a "thin" client and is different from the wallet required by SET in that it is not part of a PKI, and does not perform cryptographic computations. When a user visits websites that have been enabled to handle SPA payments, the wallet pops up on the user's screen, and a user ID and password must be provided for authentication. This information is encrypted by the browser and sent to the card issuer for authentication. Once the user is authenticated to the wallet, transaction specific information as well as credit card and customer information is exchanged between the wallet, the merchant's site, the card issuer's site, and the acquirer's site (i.e., the bank that processes the merchant's credit card transactions). This goes a step beyond 3-D Secure in that the user does not have to specifically provide credit card and shipping information to the merchant, since this is provided by the SPA. Authentication is performed once per session with SPA. Once the user is authenticated to the wallet, no further authentication is required if purchasing at different Websites.

3 TWO-FACTOR AUTHENTICATION

A two-factor authentication scheme, based on possession of a smartcard, has been introduced by American Express with their Blue card (GPayments, 2002). Visa and Mastercard also have smartcard payment schemes in the works. Since the Blue card has an embedded chip, users must have an appropriate card reader attached to their PCs. This approach is similar to the single factor Private Payments process in that users are provided with a one-time card number to use for each purchase transaction. The difference is that, in addition to a password, the user's Blue card must be inserted in the card reader in order to be assigned the one-time number. While providing a greater level of security, this two-factor authentication scheme has the drawback that a card reader must be available.

4 MOBILE COMMERCE AND USER AUTHENTICATION

E-commerce needs not be restricted to PCs only. As mobile phones become more ubiquitous, and their designs become increasingly more sophisticated, it is inevitable that they will be used for more than voice communication. In Japan, according to some estimates, over 32 million mobile phone users subscribe to NTT DoCoMo's i-mode Internet access service (Sharaf, 2004). This service enables users to do everything from sending and receiving text messages, to making online banking and stock trading transactions, to downloading images. While Asia may be leading the world in non-voice uses for mobile phones, in the UK the uptake for these types of applications is less significant. In the UK, internet access using a mobile phone is largely based on Wireless Access Protocol (WAP), a precursor to the envisioned 3G broadband wireless network. WAP has slow downloading speeds and lacks of compelling applications.

There are probably several reasons for the unpopularity of WAP-enabled Internet applications

in the UK. Most users are used to high speed internet access via PC-based web browsers, which are not as common in Japan. So there may be less interest generally in web access via mobile phone. The low data speeds available using today's circuit switched wireless networks are probably a factor, although the emerging always-on, packet-switched 3G wireless systems are supposed to provide bandwidths up to 2 Mbps. Another possibility is the user interface itself. Having to negotiate multiple tiny screens to complete simple Web transactions is clumsy and uncomfortable for many users. Screens on i-mode mobile phones are usually somewhat larger. In any case, it is a fact that in the UK, mobile phones are largely perceived as devices intended for voice communications rather than for data applications.

Despite the lack of mobile commerce activity today, there are several industry initiatives that seek to address the problem of secure financial or commerce transactions from a mobile phone or other mobile wireless devices. Among these are (Radicchioi, 2002): Visa Mobile 3D-Secure, Mastercard Secure Payment Application, Global Mobile Commerce Interoperability Group, Mobile Electronic Transactions (MeT), Mobey Forum, Mobile Payment Forum, Paycircle. These initiatives focus on the larger questions of mobile payment alternatives, without focusing specifically on user authentication. The concept of a mobile wallet is important in many of these mobile payment alternatives. The mobile wallet allows the storage of information about a purchaser, such as shipping address, as well as information about multiple credit cards (Corcoran, 2002). Unlike PC-based wallets, mobile wallets provide a value-added service to a mobile user, since they eliminate the need to provide credit card and shipping details via the limited interface capabilities of the mobile phone. A mobile wallet can reside either on a mobile phone itself, or at a remote wallet server accessible over the internet. There are several advantages to a server-based wallet, including efficiencies related to upgrades and additional functionality that can be added by the service provider. A server-based wallet can also be accessed by more than one mobile phone.

4.1 Two-Factor User Authentication

Two-factor authentication for mobile commerce may be based not only on a PIN or password, but also on user possession of a token. A specific mobile phone that has previously been registered with a mobile wallet could act as the token. Shi et al (Shi, 2004) suggests that a mobile phone's Mobile Station ISDN Number (MSISDN) might be used to identify a particular phone. For GSM mobile phones containing a SIM card holding identifying information such as a phone number, it is actually the SIM card that acts as the token. The authentication process would require that not only the password or PIN, but also the identifying information contained on an internal chip or SIM card in the mobile phone, be passed to the server-based mobile wallet.

A mobile phone might also contain an internal chip containing the wallet, or it might have a slot into which a smartcard containing the wallet can be inserted. The Mobey Forum, whose members are mainly European banks and other international companies, endorses a scheme based on a bank-issued chip card that can be inserted into the mobile device. Embedded within the chip is a wallet containing payment and fulfilment (i.e., shipping) information. Users would authenticate themselves to the wallet using a password, but possession of the mobile phone containing the wallet itself would act as the second security factor.

Radicchio is another international consortium (Radicchioi, 2002) concerned with secure mobile commerce. The Radicchio approach is based on a wireless PKI, which ensures that mobile commerce transactions satisfy several important security-related criteria. These are: integrity, authentication, confidentiality and non-repudiation. PKI is based on establishing trusted relationships between participants, and involves the use of a private key by which an authorised user can encrypt a message that can only be decrypted with the corresponding public key. This establishes the user's digital signature. However, the authentication part of the PKI paradigm depends on a mechanism, which ensures that only the correct party can gain access to their private key. Radicchio uses a two-factor approach to authentication. Private keys are stored on a smart card that must be in the possession of the authorised user. This smart card may be in the form of a SIM card for GSM mobile phones, or a larger card that can be inserted into a slot. The private key is then unlocked using a PIN.

4.2 Three-Factor User Authentication

Three hybrid factors taken together: something you know, something you have, and something you are, are generally acknowledged to provide the most secure form of user authentication. The first factor would correspond to a PIN, the user could either speak the digits of the PIN, or enter it via the keypad. The second factor "something you have" would correspond to a token possessed by the user, which would be the user's mobile phone or SIM card. During the authentication process, the mobile phone would have to transmit a unique identifier to the application performing the authentication. This identifier might correspond to the telephone number assigned to the phone, and (for GSM phones) would be contained within the phone's SIM card. This scheme implies that users must initially enroll their token (i.e., mobile phone or SIM card) with the authenticating system.

The third factor "something you are" would correspond to the user's voice biometric, or voiceprint. Although voice seems like a natural and obvious biometric to use when speaking on a mobile phone, it is now possible to use mobile phones that have an embedded fingerprint reader or a camera. While that remains a possibility, we will focus only on voice biometrics here. During enrolment, the user creates one or more voiceprint templates that will be matched later with voiceprints generated during the authentication process. There are also security issues involved with the enrolment process itself, such as making sure that the correct person is being enrolled, but these will not be addressed here.

A user authentication scenario for voice-enabled mobile commerce might therefore work like this:

User wishes to order cinema tickets from his mobile phone. He dials into his voice browser, and asks to buy tickets for a particular event. His phone number or other unique identifier associated with a chip or smartcard inside phone, is automatically transmitted to mobile wallet, via the browser.

Suppose that for this particular mobile phone, only two users are authorised to use it for secure financial or commerce transactions. Therefore, associated with this phone number, a small set of valid PINs and associated voiceprint templates have been pre-registered. The wallet recognises the mobile phone number, and retrieves the corresponding PINs and templates. User is prompted to supply PIN.

User speaks the digits of my PIN. The digits are recognised by the speech processing application, and a comparison is made against the stored voice template associated with this phone number. The PIN matches that stored against user's name, and serves to identify him.

User is prompted to speak his name. The name is recognised as an authorised user by the system, and the voiceprint of user's name corresponds to the voiceprint on file for this PIN and mobile phone number. User's identity has now been authenticated to the financial/commerce wallet.

This is an example of a text dependent approach, since it is based on the user providing a fixed password or PIN. A few permutations on this scheme are possible. Instead of speaking the PIN, a user could enter it on the phone's keypad, which would prevent someone else from overhearing it. Another possibility is that no PIN needs to be entered in this way. Instead, the user utter a secret phrase, which has two purposes. The words of the phrase constitute a password, and the computed voiceprint is matched against a stored template of the user's utterance of the phrase during enrolment. If the words of the phrase and the voiceprint match, again a hybrid three-factor authentication has taken place.

5 REPLAY ATTACKS

One weakness of this type of authentication is the possibility of replay attacks. In a replay attack, the attacker records the response of a valid user, and then replays it back to the system at a later time. If the quality of a voice recording is very good, a speaker verification system may not be able to tell the difference between the recording and a live response (Basu, 2003). One way around this problem is to use a rotating challenge/response scheme that helps to ensure real time authentication. Such a challenge/response design would require the user to respond to a challenge that changes each time. This would tend to discourage replay attacks, since the attacker presumably would have difficulty recording all possible responses. For instance, during enrolment the user might be asked to provide the answers to a number of questions known only to the user. During authentication, a challenge would prompt for the answer to one of these questions. Another way to overcome the possibility of a replay attack is with a text prompted approach. For example, a user may be prompted to utter a

randomly chosen string of digits. The voiceprints of the user speaking these digits would be matched against templates provided during enrolment (CCIR) (Pearce, 2000).

6 CONVENIENCE VERSUS SECURITY

During authentication, a matching algorithm is used to compare the voiceprint(s) of the person seeking to be authenticated, with those templates stored during enrolment. Since the voiceprint created during authentication will never exactly match the templates of a legitimate user created during enrolment, a threshold must be defined for determining what is an acceptable match. If the matching algorithm produces a measure greater than the threshold, the user is accepted, if not, the user is rejected (Roussos, 2004). This leads to two types of errors: the false acceptance of an imposter, and the false rejection of a legitimate user. The frequency of occurrence of the first type of error is known as the False Acceptance Rate (FAR), whereas the frequency of the second type of error is known as the False Rejection Rate (FRR) (Bolle, 2004).

For highly secure financial and commerce applications, it would be critical to allow an imposter to gain access. Such systems would need to have a very low FAR. On the other hand, a system that requires less stringent security might occasionally grant access to an unauthorised person, but should almost never reject a legitimate user. For instance, authentication of valid ticket holders to a sporting event might fall under this category. Such a system would therefore require a very low FRR. Ideally, authentication schemes should have both very low FARs and FRRs.

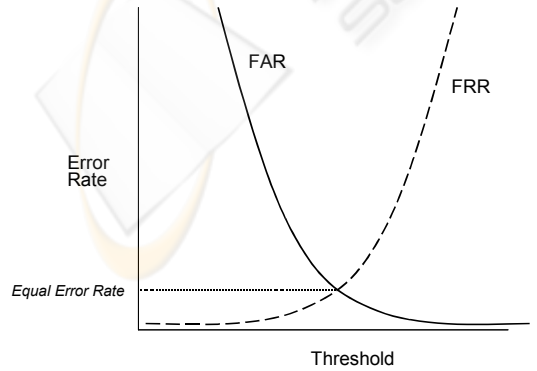

Figure 1: False Rejection Rate (FRR) vs False Accept Rates

A diagram (Figure 1) of the error rate versus threshold illustrates the tradeoff between security and convenience. As Figure 1 shows, there is an inverse relationship between FAR and FRR. As the threshold becomes larger, FAR decreases, while FRR increases. As the threshold becomes smaller, the opposite is true. There is thus a certain threshold where FRR equals FAR. The error rate at which the FAR equals the FRR is known as the equal error rate, and is often used as a performance measure for speaker verification systems.

7 LIMITATIONS OF VOICE RECOGNITION

One problem with using voice recognition is the robustness of this biometric technique to variable environmental conditions and to impersonation. It is possible to reduce the effect of these factors considerably by employing face and voice recognition concurrently and co-operatively. Such multimodal systems can be shown to be less sensitive to variations in speech patterns of a particular individual, to background noise, poor transmission conditions in remote applications and to determined attacks by impostors. Furthermore, the human voice may sound different under different circumstances, such as sickness for instance. Background noise is also a problem, since it can affect the voiceprint, although algorithms able to subtract noise from speech signals are being developed. Voiceprints are sensitive to differences in microphones used during enrolment and authentication. In addition, the quality of the transmission channel between the microphone and the voice processing application may degrade or distort the speech signal, resulting in an inferior voiceprint (Varshney, 1997).

Speaker verification via mobile phones is vulnerable to these problems. Several approaches can be adopted for combining the different modalities. The two main approaches are called feature fusion and decision fusion; also called early and late fusion respectively. The term layered biometric is also used to describe forms of late or decision fusion. Each layer is one biometric modality and these can be combined to alter the performance parameters of the overall system (FRR, FAR) .

A simple approach to decision fusion will be to treat the two modalities independently. For example,

in an access control application, voice verification can be performed and if successful face verification can follow. If the latter is also successful then access can be granted. In such a sequential layer arrangement the latter layers will only be invoked if the earlier verification layers are successful. In this way the combined FAR of the system is the product of the FAR of each of the layers (Varshney, 1997).

Alternatively, both biometric technologies can be invoked, possibly concurrently, in a parallel-layered system. The system can be arranged so that if the any of the modalities produce an acceptance then the user is accepted and the other layers need not be invoked. In this way the FRR is reduced to be the product of the FRR of all the layers. It is also possible to have a logical operation performed at the final stage to combine the decisions at the parallel layers. In a layered approach several modalities of biometric information may be integrated.

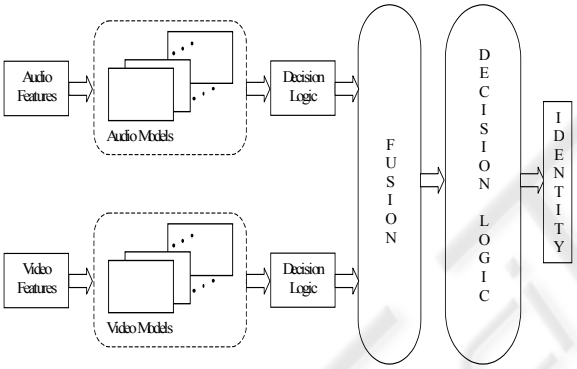

Figure 2: An example of a decision fusion system

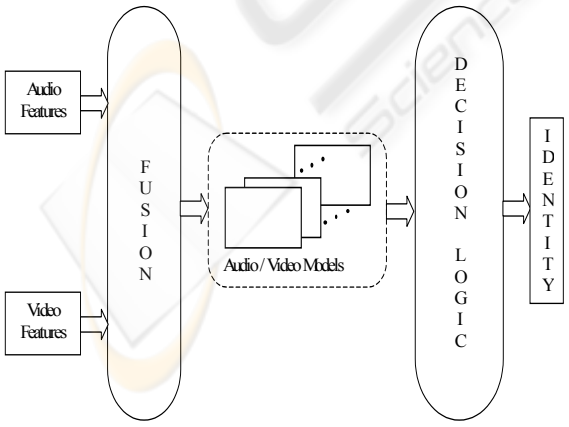

Figure 3: An example of feature fusion system

A more sophisticated version of decision fusion will hold information about the performance of individual classifiers; their strengths and weaknesses in identifying/verifying particular individuals or under particular circumstances. When it comes to combining the decisions from the different classifiers these additional performance information is combined in an optimal way to give appropriate weighting to the different biometric modalities. Figure 2 shows an example of this multimodal biometric configuration.

Alternatively in feature fusion the feature vectors obtained from the live samples are used together to train a combined classifier. This has the advantage that all the feature information is present at the classification stage; the disadvantage is that the classification stage becomes very sensitive to training data. Figure 3 shows an example of a feature fusion system .

The issue of efficient and effective combination of biometric modalities is still outstanding and attracts significant research attention.

8 CONCLUSION

Although single factor and two factor user authentication schemes for mobile commerce are under consideration by several emerging bodies concerned with mobile payment options, a well-designed three factor scheme that combines a biometric with a PIN and an enrolled mobile phone acting as a token would offer the most security. A speaker's voiceprint is a natural biometric to consider when envisioning secure payments being made from a mobile phone. The ability to distribute some of the speech processing functions to the mobile phone itself offers a way to alleviate some of the potential problems with speaker verification used in conjunction with a mobile phone, including noise reduction and problems related to the transmitting a speech sample over a wireless mobile phone network.

REFERENCES

Basu, A., Muylle, S., 2003. Authentication in e-commerce, *Communications of the ACM archive*, Volume 46 , Issue 12 (December 2003), Mobile computing opportunities and challenges, Pages: 159 – 166, ACM Press New York, NY, USA.

Bolle, R. , Connell, J. and S. Pankanti, 2004. Guide to Biometrics, Springer Professional Computing Publishers, New York.

CCIR - Center for Communication Interface Research, 2000. Large Scale Evaluation of Automatic Speaker Verification Technology, University of Edinburgh. URL: http://spotlight.ccir.ed.ac.uk/public_documents/technology_reports/Verifier_report.pdf

Chen, J. J., Adams, C. , 2004. Short-range wireless technologies with mobile payments systems, *Proceedings of the 6th international conference on Electronic commerce*, Delft, The Netherlands, ACM International Conference Proceeding Series; Vol. 60. ACM Press New York, NY, USA.

Corcoran, D., Sims, D., Hillhouse, B., 2002. Smartcards and Biometrics: Your Key to PKI, URL: http://www.biowebserver.com/downloads/Smartcards.pdf

Fui-Hoon Nah, F., Siau, K., Sheng , H. , 2005. The value of mobile applications: a utility company study, *Communications of the ACM*, February 2005, Volume 48 Issue 2, ACM Press.

GPayments, Ltd., 2002, Visa 3-D Secure vs. MasterCard SPA: A Comparison of Online Authentication Standards, URL: http://www.gpayments.com/pdfs/GPayments_3-D_vs_SPA_Whitepaper.pdf

Pearce, D., 2000. Enabling New Speech Driven Services for Mobile Devices: An Overview of the ETSI Standards Activities for Distributed Speech Recognition Front Ends, AVIOS 2000, May 22-24, 2000, San Jose CA, URL: http://portal.etsi.org/stq/kta/DSR/Avios DSR paper.pdf

Radicchio White Paper, 2002. Wireless PKI Opportunities, Version 1.00 URL: http://www.radicchio.org/downloads/smd_002.pdf

Ravi, S., Raghunathan, A., Kocher, P., Hattangady, S., 2004. Security in embedded systems: Design challenges. *ACM Transactions on Embedded Computing Systems*, Volume 3 , Issue 3 (August 2004) Pages: 461 – 491, ACM Press New York, NY, USA.

Roussos, G. , Moussouri, T., 2004. Consumer perceptions of privacy, security and trust in ubiquitous commerce, *Personal and Ubiquitous Computing* Volume 8 , Issue 6 (November 2004) Pages: 416 – 429, Publisher Springer-Verlag London, UK.

Schwiderski-Grosche S. and Knospe, H., 2002. Secure Mobile Commerce, In: C. Mitchell (editor): Special issue of the IEE Electronics and Communication Engineering, *Journal on Security for Mobility*, Volume 14 Number 5, pages 228-238, October 2002.

Sharaf, M. A., Chrysanthis, P. K., 2004. On-demand data broadcasting for mobile decision making, Mobile Networks and Applications, Volume 9 , Issue 6 (December 2004) Pages: 703 - 714 2004. Publisher Kluwer.

Shi, Y., Cao, L., Wang, X., 2004. A security scheme of electronic commerce for mobile agents uses undetachable digital signatures. *Proceedings of the 3rd international conference on Information security*, Pages: 242 – 243, ACM Press New York, NY, USA.

Tarasewich, P., 2003. Designing mobile commerce applications, *Mobile computing opportunities and challenges*, Pages: 57 – 60. ACM Press New York, NY, USA.

Varshney, P. K., 1997, Multisensor Data Fusion. *Electronics and Communications Engineering Journal*, IEE, pp 245-253, December 1997.