GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Strong User Authentication For Electronic and Mobile Commerce

Robert Pinheiro
GSEC Version 1.4

Abstract

The term "electronic commerce", for most people, denotes the buying and selling of goods or services on the Internet. Payment for these Internet purchases, at least in the U.S., typically consists of providing a credit card number and expiration date at the merchant's website. No additional user authentication is usually required, although sometimes an additional security code printed on the credit card is also requested. A recent offshoot of electronic commerce, called *mobile commerce*, has similar needs for secure payment methods. Mobile commerce refers to the use of wireless, handheld devices such as cell phones and personal digital assistants to conduct commercial and financial transactions. Mobile commerce is transacted via the Internet, using technologies such as NTT DoCoMo's i-mode, and Wireless Access Protocol (WAP) to interconnect wireless devices with Internet applications. The newly emerging VoiceXML language, which provides a way to construct an automated voice interface to World Wide Web information, might also provide a way for mobile commerce to be conducted using a voice interface.

Several user authentication schemes for electronic commerce and mobile commerce are starting to be introduced. This paper discusses some single factor and two factor authentication methods currently in use, or being planned, for e-commerce and mobile commerce. It also suggests a 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.

The User Authentication Challenge

One outcome of the lack of user authentication in electronic commerce is a greater incidence of credit card fraud. A notable attempt by the credit card industry to reduce this problem is Secure Electronic Transactions (SET). SET attempts to enable participants in an electronic 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. In the U.S., credit card holders are limited in liability to only $50 for fraudulent use of

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

their card, and in many instances this is waived altogether. So the incentive for users to bother with installing these wallets on their PCs has not been great.

Visa, Mastercard, and American Express have recently 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 a purchase transaction. Authentication based solely on "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 *two factor* authentication, since "something you have" is also required for authentication.

Three factor authentication, which adds "something you are", would be an even stronger form of authentication, and introduces biometrics into the picture. At present, this level of security is not generally available for online commerce. 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 cell phone or other handheld wireless device. Although not yet a widespread phenomenon, mobile commerce transactions using a cell phone in a public place may be dependent on the additional security that three factor authentication can provide.

Single Factor Authentication for Electronic Commerce

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 enrollment, 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 PC. 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 Web sites 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 (i.e., the bank that issued the card) 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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

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 Web sites.

A somewhat different approach is taken by American Express in its Private Payments application. With Private Payments, users don't provide their credit card numbers during an online purchase. Instead, users first obtain a one-time credit card number and associated expiration date from the American Express Web site. To get this one-time number, users must provide a valid user ID and password. Since the one-time number is good for only one purchase transaction, this must be repeated each time a credit card number is needed. This approach, while still based on single factor authentication, has the advantage that users do not have to provide a "real" credit card number to the merchant. This eliminates the danger that one's unencrypted credit card number might be stolen by hackers breaking into the merchant's site.

Two Factor Authentication for Electronic Commerce

A two factor authentication scheme, based on possession of a smartcard, has been introduced by American Express with their Blue card. 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.

Mobile Commerce and User Authentication

Electronic commerce need not be restricted to PCs only. As cell phones become more ubiquitous, and their designs become increasingly more sophisticated, it is inevitable that they will be used for more than simply talking to another person. In Japan, according to some estimates, over 32 million cell phone users subscribe to NTT DoCoMo's i-mode Internet access service. This service enables users to do everything from sending and receiving text messages, to making online banking and stock trading transactions, to downloading cartoon images and personalized ringtones. While Asia may be leading the world in non-voice uses for cell phones, in the U.S. the uptake for these types of applications is much smaller. In the U.S., Internet access using a cell phone is largely based on Wireless Access Protocol (WAP), a precursor to the envisioned Third Generation[1] (3G) broadband wireless network. And depending upon who's talking, WAP is either "dead" because of its slow speed and a lack of compelling applications, or it is alive and gaining new users every day.

[1] see Welcome to 3G-Generation.com

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

There are probably several reasons for the dearth of WAP-enabled Internet applications in the U.S. Most folks in the U.S are used to getting their 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 cell 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 people. Screens on i-mode cell phones are usually somewhat larger. In any case, it is a fact that in the U.S., cell phones are largely perceived as devices intended for talking to people rather than for data applications.

The lack of WAP applications in the U.S. and Europe has stymied the hopes of many industry players for mobile commerce. Many service and network providers, as well as equipment makers, would love for people to be able to use their cell phones to buy stuff. Mobile commerce might consist of purchasing information that can be downloaded to the cell phone, such as games, cartoons, ringtones, or news-related items. It might include purchasing items from an online catalog, or making bids in online auctions. Other financial applications might be included as well, such as checking bank balances or funds transfer.

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 cell phone or other mobile device. Among these are:

- Visa Mobile 3D-Secure
- Mastercard Secure Payment Application
- Global Mobile Commerce Interoperability Group
- Radicchio
- 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. 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 cell phone. Users wouldn't have to fumble around looking for their credit cards when making a purchase. A mobile wallet can reside either on a cell phone itself, or at a remote wallet server accessible over

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

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 cell phone.

Mobile Wallets and Single Sign On

The concept of a server-based mobile wallet has parallels with single sign-on initiatives being developed by Microsoft and the Liberty Alliance. Both of these initiatives are concerned with developing a single user identity and authentication scheme so that users can be authenticated to multiple applications across a network by simply "signing in" only once. While Microsoft's .Net Passport is controlled by Microsoft, the Liberty Alliance is backed by over 40 companies, including Sun Microsystems, and supports the notion of "federated network identity". Federated network identity "enables users to sign-on with one member of an affiliated group of organizations, and subsequently uses other sites in the group without having to sign-on again[2]". With the advent of mobile wallets and mobile commerce, it would seem inefficient if users had to register with, and authenticate themselves to, different wallets issued by different credit card companies. The needs of mobile commerce for authentication and payment mechanisms may provide the motivation for many of the concepts being developed under the single sign–on umbrella.

Single Factor User Authentication for Mobile Commerce

To make a credit card purchase using a cell phone and a mobile wallet, users would need to authenticate themselves to the wallet. Single factor authentication based on user IDs and passwords is assumed in many of these initiatives. For instance, initial trials of Visa's Mobile 3-D Secure mobile payment scheme requires that mobile users enter their credit card information and a PIN into their cell phones during a purchase. If the wallet resides on a remote wallet server, the encrypted authentication information entered via the cell phone would reach the wallet server using WAP for data transport. The wallet then exchanges financial information with a merchant or other financial site on the Internet. This, however, may introduce the infamous "WAP gap" security breach, undermining end-to-end security between the mobile device and the wallet server.

Encryption is specified in WAP by Wireless Transmission Layer Security (WTLS) between the mobile device and the WAP gateway, and by Secure Sockets Layer (SSL) between the WAP gateway and a server on the Internet. The WAP gap refers to the fact that encrypted information traversing the WAP gateway, which converts between WAP protocols and Internet protocols, is unencrypted for a brief period of time. Although this problem exists in early WAP implementations, the WAP 2.0 specification proposes to fix this problem by allowing a WAP-enabled cell phone and a Web server (running the mobile wallet) to communicate

[2] see Liberty Alliance FAQ

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

directly using Internet protocols such as TCP/IP and HTTP. In WAP 2.0, end-to-end transport security is provided by a method for "TLS[3] tunneling", replacing the WTLS-to-SSL protocol conversion of earlier versions of WAP.

Two Factor User Authentication For Mobile Commerce

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 cell phone that has previously been registered with a mobile wallet could act as the token. (Schuba, et al) suggests that a cell phone's Mobile Station ISDN Number (MSISDN) might be used to identify a particular phone. For GSM cell 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 cell phone, be passed to the server-based mobile wallet.

A cell 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 fulfillment (i.e, shipping) information. Users would authenticate themselves to the wallet using a password, but possession of the cell phone containing the wallet itself would act as the second security factor.

Radicchio is another international consortium 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* (making sure the relevant information hasn't been tampered with), *authentication* (making sure the correct person is involved), *confidentiality* (keeping the information private), and *non-repudiation* (making sure a legitimate transaction cannot be denied later). PKI is based on establishing trusted relationships between participants, and involves the use of a private key by which an authorized 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 authorized user. This smart card may be in the form of a SIM card for GSM cell phones, or a larger card that can be inserted into a slot. The private key is then unlocked using a PIN.

[3] Transport Layer Security

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Emergence of the Voice Web

Since WAP transactions using the small screen on a cell phone have not yet caught on, does it make sense that certain types of Internet transactions could be conducted from a cell phone using voice only? Or at least, using primarily voice, with minimal keypad interaction? Such applications could include information retrieval tasks – checking bank accounts, getting weather information – as well as interacting with an automated "personal assistant" or other commerce agent for making certain types of purchases. This possibility has led to the concept of the *voice web*, based on VoiceXML, an emerging XML markup language that aims to make certain kinds of Web-based information accessible via a voice interface. VoiceXML is being standardized by the VoiceXML Forum, as well as by the W3C Voice Browser Working Group, although these standards are still evolving. The big difference between voice applications that use VoiceXML and the more traditional Interactive Voice Response (IVR) applications is that whereas the latter presents users with various voice prompts requiring very specific responses (e.g., "Press or say 1 for Customer Service", etc.), with VoiceXML users would be able to simply say what they want ("I'd like to speak with Customer Service.").

To use the voice web, a user dials into a *voice browser*, which runs the VoiceXML code. The VoiceXML code itself is deployed on behalf of a service provider – the entity that is making its Web information available. Unlike a Web browser on a PC, which is client based, a voice browser is server based. The voice browser exchanges HTTP messages with a Web server. The security considerations for the communications between the voice browser and the Web server are essentially equivalent to that between a PC-based web browser and a Web server. That is, SSL may be used to establish a secure channel between them. Cookies may be placed on the voice browser by the Web server. The voice browser interacts with the user via various voice prompts, and accepts and interprets the user's spoken input using speech recognition technology.

A key component of VoiceXML is a "grammar" that defines the allowable speech input that the voice browser can accept and recognize from the user. Based on this input, the voice browser constructs appropriate HTTP messages that are sent to a Web server. The information contained in the HTTP messages returned from the Web server is converted by the voice browser back into speech using speech synthesis technology. The real trick is to design the grammar and the VoiceXML application so that a satisfactory user experience can be obtained with a one dimensional voice interface to a set of Web information that originally was meant to be viewed in a two dimensional space. Quite likely, only a subset of the service provider's Web site can be made available for voice browsing because of this difficulty.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The advent of VoiceXML and voice browsers, although still at an early stage in their development and deployment, provides a motivation for considering ways in which users may authenticate themselves to banking, commerce, or other types of secure voice-enabled applications that might be conducted using a cell phone. While there's no reason to believe that screen-based WAP applications couldn't also make use of the same speech-centric authentication mechanisms, speech-centric authentication seems like a natural fit to the emerging voice web.

Two Factor User Authentication for Mobile Commerce – Part II

Suppose a mobile user is interacting with a Web site using a speech interface enabled by VoiceXML. If this user needs to authenticate himself/herself to a financial or commerce application, a two factor authentication scheme based on speech processing technologies can be envisioned. The user not only provides a password or PIN, but also utters a phrase for additional authentication purposes. A voiceprint of the utterance is computed, and a comparison of the voiceprint with a previously stored voiceprint authenticates the user. Two major players in the speech processing domain (SpeechWorks and InterVoice-Brite) announced in early 2002 a joint effort to develop such a system. (Wrolstad, 2002)

This two factor authentication – based on something you know and something you are, could be extended to three factors if an additional identifier, corresponding to something uniquely bound to a token possessed by the user – such as a cell phone number – could be incorporated into the authentication process.

Three Factor User Authentication For Mobile Commerce

Three 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 - something you know - 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 cell phone or SIM card. During the authentication process, the cell 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 the user must initially enroll his/her token (i.e., cell 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 cell phone, it's possible that some cell phones in the future might contain a fingerprint reader. While that remains a possibility, we will focus only on voice biometrics here, since our motivating

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

theme is the voice web and voice-enabled mobile commerce. During enrollment, 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 enrollment process itself, such as making sure that the correct person is being enrolled, but these won't be addressed here.

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

1. I wish to order theatre tickets from my cell phone. I dial into my voice browser, and ask to buy tickets for a particular event. My phone number (or other unique identifier associated with a chip or smartcard inside my phone) is automatically transmitted to my mobile wallet, via the browser.

2. Suppose that for this particular cell phone, only my spouse and I are authorized to use it for secure financial/commerce transactions. Therefore, associated with this phone number, a small set of valid PINs and associated voiceprint templates have been pre-registered. The wallet recognizes the cell phone number, and retrieves the corresponding PINs and templates. I am prompted to supply my PIN.

3. I speak the digits of my PIN. The digits are recognized by the speech processing application, and a comparison is made against the stored PINs associated with this phone number. The PIN matches that stored against my name, and serves to identify me (and not my spouse).

4. I am prompted to speak my name. My name is recognized as an authorized user by the system, and the voiceprint of my name corresponds to the voiceprint on file for this PIN and cell phone number. My 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 my PIN, I 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, I 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 my utterance of the phrase during enrollment. If the words of the phrase and the voiceprint match, again a three factor authentication has taken place.

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

very good, a speaker verification system may not be able to tell the difference between the recording and a live response. One way around this problem is to use a rotating challenge/response scheme that helps to ensure that a "live" person is seeking 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 enrollment 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 enrollment.

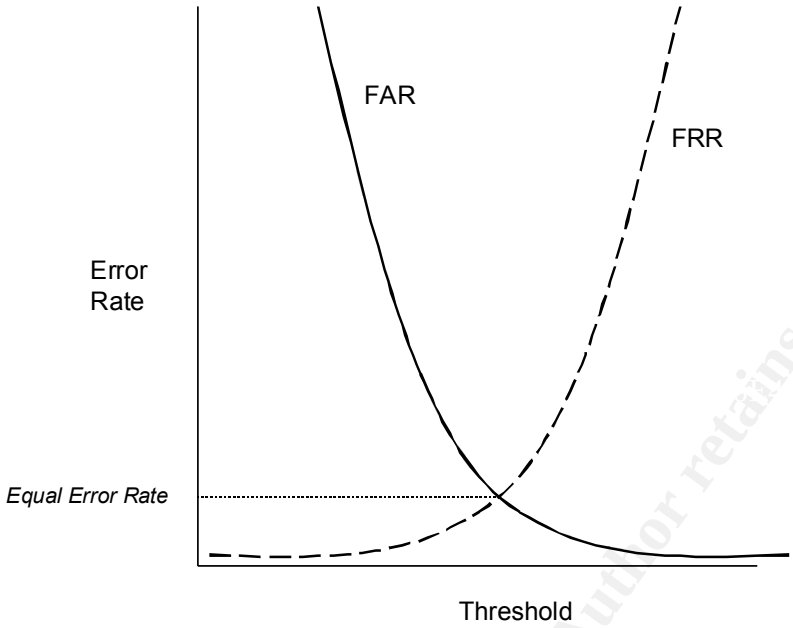
Convenience versus Security

During authentication, a matching algorithm is used to compare the voiceprint(s) of the person seeking to be authenticated, with those templates stored during enrollment. Since the voiceprint created during authentication will never exactly match the templates of a legitimate user created during enrollment, 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. 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).

Which is worse – a financial or commerce application that sometimes authenticates an imposter, or one that occasionally rejects a legitimate user? For highly secure financial and commerce applications, it would be worse 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 unauthorized 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. But as in life itself, there is no free lunch.

A diagram of the error rate versus threshold illustrates the tradeoff between security and convenience. As the diagram 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.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



False Rejection Rate (FRR) vs False Acceptance Rate (FAR)

(Mansfield, et al) contains a performance analysis of a leading speaker verification system, including a discussion of these error rates and the factors that affect them. One thing to note is that the actual shape of these curves will depend on the actual design and implementation of the speaker verification system. Also, longer utterances will usually provide greater accuracy, since longer utterances provide more information about an individual's speech patterns.

Is Speaker Verification Ready for Prime Time?

It is generally believed that current speech technology is not as accurate for biometric applications as other technologies, such as fingerprint and iris scans. This is probably true if a voiceprint is used for identification purposes; that is, performing a one-to-many comparison with many other stored voiceprints to find a match. The reason is because any given voiceprint, when compared against thousands or millions of other people's voiceprints, may be too close to someone else's for the matching algorithm to detect a difference. But when voiceprints are used for authentication/verification, a voiceprint is compared only against the stored voice template of the person being authenticated – a one-to-one comparison. Because it is much easier to detect a true difference under those conditions, speaker verification is competitive with other biometric authentication methods.

Of course, the human voice may sound different under different circumstances – such as when the speaker has a cold or other nasal obstruction, for instance.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

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 enrollment 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.

Speaker verification via cell phone is vulnerable to these problems. One approach to addressing some of these difficulties is distributed speech processing (DSR). With DSR, some of the speech processing itself can take place on a cell phone equipped with a sufficiently powerful processor – such as may be available with cell phones designed for the emerging third generation (3G) wireless networks. DSR allows noise reduction and feature extraction to take place on the cell phone, so that the speech signal itself doesn't have to traverse the cell phone network for processing at a central location. Instead, a compact set of numbers representing the extracted characteristics of a particular individual's voice is transmitted for additional processing at a central site. Because data rather than speech is transmitted across the wireless network, the integrity of the information contained in the initial speech utterance is protected by the standard error correcting codes used for data transmission. This is an example of a situation where some combination of WAP and VoiceXML might be used for secure wireless Internet applications: WAP for transmission of the voiceprint data, and VoiceXML for the speech interface to a mobile commerce application.

Speaker verification is usually combined with other factors in a multifactor authentication model, rather than acting as the sole authentication mechanism. Just as users who provide an incorrect PIN are usually given a second and possibly third chance to provide the correct value, a speaker verification algorithm that cannot match a voiceprint with the stored template the first time could allow the user to make one or two more attempts. The best of the three attempts could then be matched against the template. Or, if templates were created for several utterances, a text-prompted system could prompt the user to speak a different phrase.

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 cell 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 cell phone. The ability to distribute some of the speech processing functions to the cell phone itself offers a way to alleviate some of the potential problems with speaker verification used

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

in conjunction with a cell phone, including noise reduction and problems related to the transmitting a speech sample over a wireless cell phone network.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

World Wide Web Consortium (W3C), "Voice Browser Activity – Voice Enabling the Web", URL: http://www.w3.org/Voice/

Trintech Inc., "Preparing for the m-Commerce Revolution: Mobile Payments, 2002", March 2002,
URL: http://www.epaynews.com/downloads/mpayment_paper.pdf

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

Mansfield, T., Kelly, G., Chandler, D., Kane, J. "Biometric Product Testing – Final Report, March 19, 2001", Center for Mathematics and Scientific Computing, National Physics Laboratory, U.K.
URL: http://www.cesg.gov.uk/technology/biometrics/media/Biometric Test Report pt1.pdf

Ratha, N., Senior, A., Bolle, R. "Automated Biometrics", IBM Watson Research Center
URL: http://www.research.ibm.com/ecvg/pubs/ratha-auto.pdf

Hennessy, D. "The Value of the Mobile Wallet", November, 2001
URL: http://www.network365.com/downloads/whitepaper_88.pdf

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

Bionetrix Corp., "The Evolving Role of Authentication in the Financial Services Industry", 2001 URL: http://www.bionetrix.com/pdf/Financeb.pdf

WAP Forum, "WAP 2.0 Technical White Paper", January 2002
URL: http://www.wapforum.org/what/WAPWhite_Paper1.pdf

Osborne, M. "WAP, m-Commerce, and Security", KPMG
URL: http://www.kpmg.co.uk/kpmg/uk/image/mcom5.pdf

Ankari, Inc., "The Challenge of User Authentication" URL:
http://www.systempros-cordless.com/resource/UserAuthentication.pdf

Schuba, M., Wrona, K. "Security for Mobile Commerce Applications"
URL:http://www.medialabeurope.org/people/k-wrona/pub/mskw_miv01.pdf

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

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

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

Financial Services Technology Consortium, "New Authentication Services", URL: http://www.fstc.org/discussions/transcript/2002-01-23-Transcript-V1.html

Mobey Forum, "The Preferred Payment Architecture – Technical Documentation", Version 1.0, 2001
URL: http://www.mobeyforum.org/public/material/PPATechnical.pdf

Pearce, D. "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

Houlding, D. "VoiceXML and the Voice-Driven Internet", Dr. Dobb's Journal, April 2001
URL: http://www.ddj.com/documents/s=868/ddj0104g/0104g.htm

Jewson, R. "E-Payments: Credit Cards on the Internet", October 2001
URL: http://www.aconite.net/Epayments_Whitepaper.pdf

Sam, M., Down, K., Clements, J., Rabin, J., "The Services and Technology of the Wireless Internet: Costs and Benefits", Dundee Securities Corp. Global Wireless Industry Report Part 2, December 20, 2000
URL: http://www.ecommercescotland.org/mbusiness/wps/GlobalWirelessIndustry_2.pdf

VoiceXML Forum, URL: http://www.voicexmlforum.org/

Welcome to 3G-Generation.com, URL: http://www.3g-generation.com/

Wrolstad, J. "Voice Recognition Employed for M-Commerce Security", Wireless Newsfactor, February 1, 2002
URL: http://www.wirelessnewsfactor.com/perl/story/16123.html

American Express Private Payments FAQ,
URL: http://www26.americanexpress.com/privatepayments/faq.jsp

Liberty Alliance Project, FAQs, URL: http://www.projectliberty.org/faq.html

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Last Updated: April 24th, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GA	May 30, 2017 - Jun 04, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor