



raising security to a new dimension

Multi-factor Voice Authentication For Secure Telephone And Internet Services

Abstract

Recent reports regarding the use of Internet banking in Australia (*The Australian, June 13, 2006*) indicate that Internet banking is fast maturing as the preferred channel for customers to access banking services - 42% of customers preferred online banking to going into a branch (36%) or using telephone banking (16%). However, customers are becoming increasingly concerned with the security of Internet banking - with only 35% believing that their money and personal information is safe if accessed through the Internet.

These trends correlate with trends overseas, specifically in the US where Internet banking has become a strategic channel for delivering banking services. So concerned is the US Federal Financial Institutions Examination Council (FFIEC) about the security aspects of online banking and the explosion in Internet banking fraud that they are mandating multi-factor authentication for online banking services by the end of 2006.

At the same time, the banks are 100% focused on meeting customers' ever increasing demands for fast, convenient and reliable banking services. This is no more so than in Internet banking where customers' demands for the highest standards of convenience, reliability and effectiveness have to be balanced with the equally demanding requirements for the highest level of security and privacy for personal information. Moreover, it is not just banking customers that demand the highest levels of security, but also the banking institutions themselves with their Directors and Board members legally and morally responsible for maintaining and protecting the assets of the banks along side the integrity and security of any personal information held by banking and financial institutions.

So how does a bank balance the demand of its customers for fast and convenient self-service, whilst maintaining appropriate levels of security and privacy? The key problem in deploying any self-service strategy, be it Internet or telephone

based, is in developing strong methods of authenticating the identity of users, ensuring that people accessing services really are "who they say they are"!

The Problem with PINs and Passwords

The traditional methods for authenticating identity in self-service applications are to ask the user to enter a PIN or password. PINs and passwords offer a single-factor authentication mechanism which has a number of major security problems for banking self-service.

Firstly, simply knowing a PIN or password does not necessarily mean that you are the authorised user of that service. PINs and passwords are easily stolen, copied, shared or guessed. Making PINs and passwords more complex and changing them more often does not solve these problems. Frequently, people just cannot remember complex PIN's and passwords and simply choose to write them down - thereby defeating the objective of the added complexity in the first place.

Once the security of a PIN or password is compromised there is the subsequent problem of resetting them. Most often this involves the PIN/password owner calling the organisation's help-desk and then proving to the help desk agent that they were the person who the PIN/password was originally issued to. Most often this involves the caller sharing personal information such as name, account number, address, telephone numbers, date of birth and even mother's maiden name

Yet all of this information still does not necessarily prove that you really are who you say you are. This information is often readily obtainable and can be known by a wide range of people including family members, workplace colleagues and social contacts. Furthermore, disclosing "personal information" to a help-desk agent is itself highly insecure as the help-desk agent now also knows your personal information and is in a position (if they so choose) to compromise the customer's identity



raising security to a new dimension

Multi-factor Voice Authentication For Secure Telephone And Internet Services

and privacy. (Whilst not inferring that banking help desk agents are any more dishonest than other sections of society, access to the personal information of individuals nevertheless creates a significant security risk).

Voice Authentication – A Multi-Factor Security Solution

Voice authentication provides a highly convenient yet highly secure multi-factor authentication solution for authenticating identity for both voice and internet self-service applications.

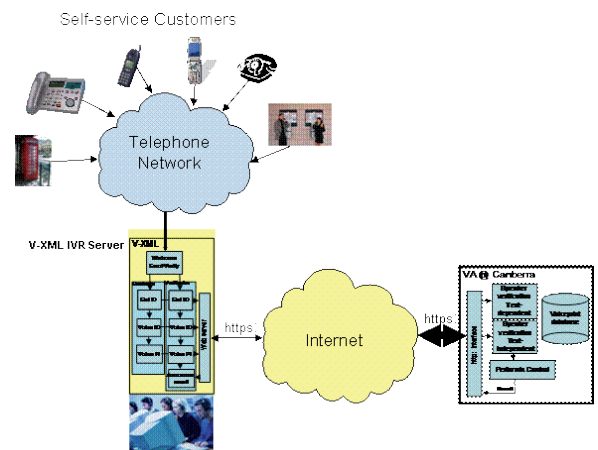
Voice authentication works by analysing the characteristics of the speaker’s voice and matching those against a template, or voiceprint, that is kept on file. Initially, the bank’s customer needs to register a sample voiceprint or voice file, but once on file, this voiceprint provides an extremely reliable process for authenticating that the customer “is who they say they are”, literally!

In many ways its is analogous to the bank keeping a signature on file and using it to check that you are indeed the account holder. When the caller enters the system, they are asked for their identity credential, for example their account number. This is then used to reference their voiceprint. Their identity can be confirmed by comparing their voice, i.e. the way they say their account number, against the voiceprint held on file. This confirms that the voice quality matches; providing a two-factor authentication credential in a single utterance: first, the information must match i.e. information known by the caller knows, such as the account number; and secondly, the voice quality must match. This is something the caller is (the voice biometrics authentication component). Security can be further enhanced by asking additional questions, such as “please say your password or name”. Again the caller not only has to get the password or name right, but must say it with the correct voice quality.

Voice authentication is most commonly used in telephone services to confirm a caller’s identity before allowing access to secure Interactive

Voice Response (IVR) speech recognition and call centre services. However, the same voiceprint and authentication process can be used for multi-factor authentication for secure Internet self-service, such as Internet banking.

The diagram below shows the architecture developed by 3SH for secure telephone services. The architecture comprises of a VoiceXML IVR connected via https: (secure communications protocol) to a voice authentication server.



Contact Centre, IVR or Speech Recognition Applications

In the model, the VoiceXML IVR implements the call flow for the authentication process, whilst the voice biometric server provides the authentication process. Voice data logged by the VoiceXML IVR (for the purpose of authentication) is encrypted and relayed to the voice authentication server for processing. This system, in turn returns a value back to the IVR based on how well the voice data matched the associated voiceprint stored in the identity management database. Based on this information the IVR can then authorise access to a secure service or pass the call to a contact centre agent based on business rules set by the bank.



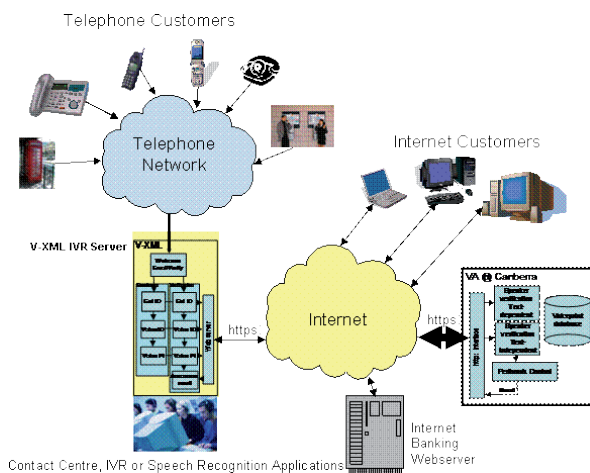
raising security to a new dimension

Multi-factor Voice Authentication For Secure Telephone And Internet Services

Given that the architecture is already based on an established web services model, extending it to support secure multi-factor authentication for secure Internet self-services is relatively straight forward.

The diagram below shows the extensions required. This amounts to connecting the Internet banking server, via appropriate firewalls and security systems to the Internet to enable connection by Internet customers.

At the receiving end the speech data is decrypted, unpacked and processed by the speaker verification technology using the voiceprint information from the database. The authentication system computes a verification score based on how well the spoken information (both information and biometric content, i.e. two-factor authentication) matches the voiceprint information on file. The score is passed to the Internet banking server, which like in the voice channel, uses business rules to either allow or decline access to the service.



In this model an Internet customer accesses the Internet banking server (as usual) over the Internet as with any other service. To access secure services, customers enter their ID/ customer or account number into the website (as they do currently). The Internet banking server copies this information to the voice authentication server which, in the same way that the Voice-XML server, uses this information to retrieve the associated “authorised customer’s voiceprint” from the voiceprint database.

At this point, the Internet customer, in response to instructions that appear on their monitor, would speak their ID number and passphrase into the system using either the built in PC microphone or a microphone connected to their PC, just like people do when they use Internet telephony. The voice data is packaged and encrypted using software running on the PC and sent to the voice authentication server using secure Internet protocol (https://) for verification.



raising security to a new dimension

Multi-factor Voice Authentication For Secure Telephone And Internet Services

Alternative Configuration and Benefits

The solution can be configured in several different ways to enable banks to effectively and conveniently authenticate the identity of users with little or no modification to their current Internet banking services.

Voice Authentication for Internet Banking Activation - voice authentication could be used to activate an Internet banking account. In this configuration, the Internet banking service is not available until activated. A banking customer telephones the bank's voice authentication system to confirm their identity and authority to access Internet banking. Authentication activates their account and they have a period of time to log-in. (If they do not log-in in time the account then becomes inactive again and they will need to telephone again to re-activate.) Once logged-off the customer then has to call again to confirm identity to re-activate their Internet banking account.

The benefits are that:

- it is simple to implement and does not impose any complication or change to current Internet banking processes, and
- It can be available for selected accounts, such as high value accounts, including business accounts.

The disadvantage compared to the Internet solution is that there is a cost involved in making the telephone call to authenticate and, whilst the process significantly enhances security through cutting down the time available for an impostor to break into an account, it is not completely secure as stolen PINs and passwords could be used whilst the account is active. At the moment all Internet banking accounts are active 24 hours a day 7 days a week leaving them open to attack at anytime.

Voice authentication for One-time passwords - a variation on the above configuration is to use a voice authentication system to issue one-time passwords. In this

configuration the bank customer telephones the voice authentication system to obtain a one-time password which they have a limited time to use to access their Internet banking services as they do now.

The benefits are that:

- it is more secure as it uses different one-time passwords for different Internet banking sessions, and
- it does not matter if they write it down as once it has time out it will be useless and once used cannot be used a second time.

Telephone Voice authentication during the log-on process - a variation on this configuration is to ask the customer to confirm by telephone their identity during the log-on process by repeating information displayed on the screen during the log-on process. A further variation is for the internet banking application to telephone them to obtain a voice authentication credential to authorise a transaction.

These configurations, whilst offering higher levels of security are more complex (and expensive) to implement as they require a telephony application to be integrated into the (existing) Internet banking application which is currently not the case.

The benefits of the approach are as follows:

- As there are now no PINs or passwords for the customer to remember, the solution provides banks with a multi-factor authentication solution for Internet banking services that is as convenient (if not more convenient) than current methods.
- The convenience is enhanced, as banking customers can use the same multi-factor authentication mechanism for both the telephone and Internet channels.
- The solution offers enhanced security as it enables on-line transactions to be confirmed using a multi-factor biometric authentication credential. In



raising security to a new dimension

Multi-factor Voice Authentication For Secure Telephone And Internet Services

effect, customers can “sign” financial transaction using their voice. This not only strengthens security of online services, it also enables banks to offer a far wider range of high value services on the Internet (and voice channel) as they now have a multi-factor biometric security mechanism available to them.

The solution is also extremely cost-effective to implement and manage as:

- there is no need to purchase and issue any token or special devices to banking customers. They use a device, the PC microphone which they either already have built into their system or would purchase for other tasks, such as VoIP telephony, voice recording or personal speech recognition, and
- as a device or token has not been issued, costs associated with supporting issued token or device decreases significantly, and
- lastly there is the problem about what happens when customers invariably loses or have their tokens or devices stolen, misplaced, damaged or they become faulty. In these circumstances, there is then the problem of re-confirming that the “*customer is who they say they are*” before re-issuing a token or device.

There is also the opportunity for banks holding voiceprints on file to authorise third party transactions; such as Internet credit-cards transactions. The voice authentication security credential ensures that the person making an Internet credit card transaction is indeed the authorised credit card holder and not an impostor using stolen credit card information, personal information or stolen cards.

About the Author

Dr Clive Summerfield is CEO of 3SH. Clive has been driving the adoption of speech recognition and voice authentication since the 1980s, with a key focus on massively scalable carrier-grade projects.

In 1990 Clive founded Syrinx Speech Systems where he implemented AT&T’s USA based Customer Care application as well as applications for Commonwealth Bank’s Australian Stock trading system. He introduced voice biometrics to Australian government agencies such as Parliament House and has recently undertaken an evaluation on voice authentication technologies sponsored by Australia’s Centrelink.

Please visit www.3sh.net for more information.