Securing self-service telephone applications

white paper

by J. Markowitz, Consultants

Table of contents

The rise of self-service automation 2

Security in a self-service environment 3

The trouble with PINs and passwords 3

Biometric authentication 5

Securing self-service deployments 8

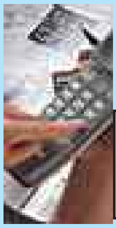
Conclusion 9

About J. Markowitz, Consultants 9

About Dr. Judith Markowitz 9

Speak or enter the tracking number of the parcel.

Say the name of the department or person you want to reach.



Enter your 16-digit card number.

The rise of self-service automation

Today's businesses compete in a fast-paced, global marketplace in which both customers and employees expect easy-to-use, 24X7 service. The e-commerce explosion has firmly established the Internet as a business-to-consumer and a business-to-business channel. Market estimates range in the billions dollars spent every year online with annual growth exceeding twenty-five percent in many parts of the world.

Similar changes have taken place within enterprises. Intranets and other corporate data networks provide service and communication channels for employees and partners.

These new channels –in combination with wireless, mobile devices – have transformed the corporate call center and technical help desk into multi-channel contact centers. These new channels are also fundamentally self-service access points to an enterprise.

Although e-commerce has helped to reshape the way businesses operate, the telephone – both wireless and wireline — remains the primary means by which customers, employees, and partners contact enterprises. Traditionally, the telephone has not been a self-service channel.

Rapid turnover of agents, soaring costs, and the need to offer 24X7 availability have driven contact centers towards increasing self-service automation. The most well-established is the automated attendant using interactive voice response (IVR) with touch-tone input. The advent of fast and accurate speech recognition in the late 1990s accelerated the move to self service by making it possible to automate operations that touch-tone cannot support or does not support well (e.g., stock quotes and directory assistance). The reach of self-service automation was further extended by the widespread adoption of VoiceXML and related standards which make it possible to interact with Web-based systems through audio dialogs. This means that self-service operations available on the corporate website can be accessed via the telephone.

A call comes in to the corporate help desk

“Who’s the supervisor on duty tonight?’
‘Oh, it’s Betty.’
‘Let me talk to Betty.’ [He’s transferred.]
‘Hi Betty, having a bad day?’
‘No, why?’
‘Your systems are down.’
‘My systems aren’t down, we’re running fine.’
‘You better sign off.’ She signed off.
‘Now sign on again.’ She signed on again.
‘We didn’t even show a blip, we show no change. Sign off again.’ She did.
‘Betty, I’m going to have to sign on as you here to figure out what’s happening with your ID. Let me have your user ID and password.’ This senior supervisor at the Help Desk tells him her user ID and password.

Figure 1: Social Engineering (Adapted from Granger, Sarah 2001 *Social Engineering Fundamentals, Part I: Hacker Tactics*. SecurityFocus, In Focus http://www.securityfocus.com/infocus/1527)

Security in a self-service environment

Services that require authentication, such as allowing customers to access their account information or permitting authorized employees to access sensitive corporate information, are either not automated or require entry of a PIN or password. This is the case whether the access mode is by Web or by telephone.

The trouble with PINs and passwords

Customers and employees have become overburdened by the number of PINs and passwords required to access the systems they need to use. This has contributed to the rise of password reset as a major employee-related service. Technical help desks spend, on average, forty to sixty percent of their time resetting passwords. Both public and private enterprise are looking for secure alternatives to the complex matrix of PINs and passwords that exists today.

Single sign-on represents an attractive solution to password overload because it consolidates the security systems protecting various systems and services within a single enterprise. It isn’t useful for consumers interested in accessing information from more than one enterprise (e.g., account status), however. Furthermore, many single sign-on systems rely on theft-resistant passwords (comprised of bizarre strings of digits and letters) that are changed every sixty to ninety days.

Unfortunately, theft of passwords is a flourishing criminal activity. Some of it is perpetrated using software (such as spyware, sniffers, and password generators) that is easily obtained on the Internet and elsewhere. Other thieves hack information repositories containing passwords and other sensitive information; still others use “social engineering.” In March, 2005 the US Treasury Department reported that inspectors posing as computer technicians used social engineering to obtain computer login codes from more than a third of the Internal Revenue Service employees and managers they called. This enabled the inspectors to log in and change the passwords to those accounts. Figure 1 shows how a social-engineering attack might work.

ChoicePoint Lexis-Nexis

These names have become synonymous with the epidemic of thefts of personal information from trusted corporate and public-sector repositories that fuel the growth of identity theft.

Identity theft

The names ChoicePoint and Lexis-Nexis have become synonymous with the epidemic of thefts of sensitive consumer data stolen from corporate and public-sector repositories and individuals through a variety of criminal activities. In April, 2005 Reed Elsevier joined the growing numbers of private and public organizations when it revealed that its Lexis Nexis database had been breached and personal information, including names, addresses and Social Security and driver's license numbers for 280,000 people had been taken.

Hacking, social engineering, and other techniques for illegally capturing personal data are the first step in another mushrooming criminal activity: identity theft. According to research firm Javelin Inc., approximately 9.3 million Americans were victims of identity theft in 2004 (almost one in every 23 Americans). Cifas, the UK's credit industry's fraud-prevention association, described a "relentless rise" in identity theft cases. The approximately 120,000 UK cases reported in 2004 represent a 20 percent increase over 2003 and a 600% increase over 1999. These figures and findings for other developed countries show that identity theft is a global scourge.

Once an identity is stolen the criminals can use it to apply for loans and credit cards, withdraw large sums of money from bank accounts, use telephone calling cards, or obtain goods or privileges they couldn't get using their own identities. They can even use the identity to fund criminal activities or terrorism. The real owner of the identity ends up with a bad credit rating or worse.

The attack against ChoicePoint demonstrates that even highly-sophisticated companies can be tricked into supplying formation to criminals skilled in social engineering. ChoicePoint shared the data of 145,000 people with thieves who posed as businessmen wanting to do background checks on their own customers. ChoicePoint reported that within a month at least 750 of those people had become victims of identity theft.

These growing problems have motivated enterprises to look at biometric authentication for self-service and for single sign-on.

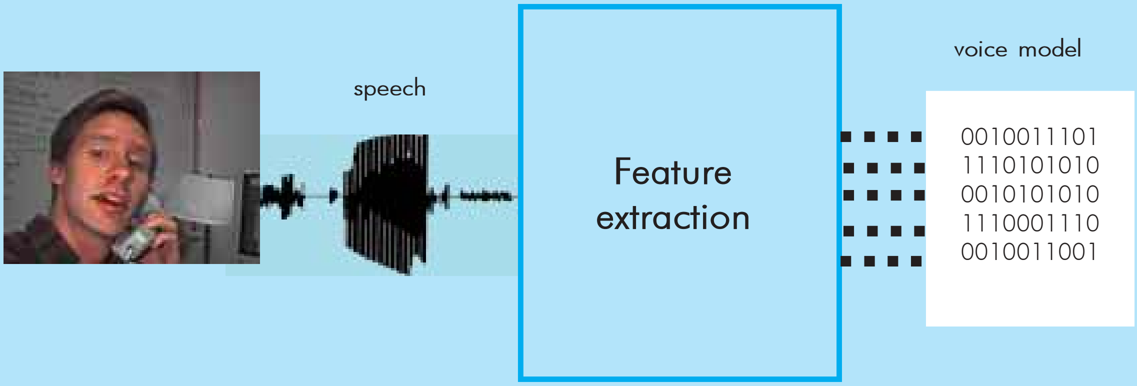


Figure 2 A biometric voice model consists of values for selected features extracted from the sample.

Biometric authentication

Biometric authentication supports the self-service model because it can be performed in real time and can be used to authenticate both local and remote users. Unlike PINs, passwords, and other kinds of authentication; which provide indirect authentication based on something a person has or knows, biometrics employ direct verification based on examination of an attribute of the person him or herself.

Biometric authentication only employs generic attributes – ones that can be used across large populations of individuals. Those attributes include DNA, fingerprints, iris patterns, and a person's voice. Face, iris, hand, and fingerprint recognition are already being employed at ATMs and kiosks and to secure login to data networks and access to secured locations, such as data centers. Speaker authentication is being used for telephone self-service operations that include password reset, RSA SecureID token administration (and as the private key of a PKI transaction), money transfer, and to provide greater security for existing PIN and password-secured applications. T-Mobile Systems, VeriSign, Volkwagen Bank, Union Pacific Railroad, and SBC Communications are among the companies that have used speaker authentication security to move sensitive applications into the self-service arena.

Biometric concepts

There are several core concepts that underlie an effective and secure biometric deployment. Among the most important are the biometric model, the two-step process, and the threshold.

Biometric model

A biometric model (sometimes called a *template*) is constructed from one or more biometric samples but it's not the same as the sample (see figure 2). It contains coded information about distinguishing features extracted from the sample. For example, many fingerprint systems encode the nature and position of minutia which include changes in the direction of the swirls in the print. Voice models used in speaker authentication include information about resonance patterns and relationships that reflect the size and shape of the mouth, nose, and throat. Since a biometric model doesn't represent the entire sample it can't be reverse engineered to recreate the original biometric sample. Nor can it be used as input to the biometric system, which expects to receive a biometric sample for analysis.

Biometric security, such as speaker authentication, is the only form of authentication that uses direct verification based on examination of an attribute of the person him or herself.

Biometric concepts (continued)

Two-Step Authentication Process Biometric authentication requires two steps: enrollment and authentication. During enrollment, the system creates a biometric model from one or more biometric samples provided by an individual and stores the model (sometimes, called the *reference model*) in a secured database. Enrollment is generally a facet of the other security procedures that comprise acceptance of an individual as an authorized user.

The second step is authentication which involves a claim by an unknown individual to be a specific enrolled user. That claim is accompanied by a biometric sample. The act of providing a sample is generally quick and easy. A typical speaker authentication system requires a single authentication utterance. It may ask the individual to say their account number or other identifier. Speech recognition is used to access the reference model for that identifier. Then the utterance is converted into a biometric model that is compared with the reference model. If the two models are sufficiently similar the system accepts the claim of identity as true. If they differ significantly from each other the system rejects the unknown person as an impostor.

Threshold Biometric systems are statistical systems. They expect that no two samples will be exactly the same. This is true for all biometrics. Two fingerprint samples from the same person, for example, may differ slightly in pressure, orientation, dryness, and other factors that affect the codes used to construct the model. Voice, iris, face, hand, and other models vary in the same way. Consequently, a biometric system expects there to be differences between the reference model and another sample provided by the same person. The threshold determines how much variability it will allow before the identity claim is questioned or actually rejected.

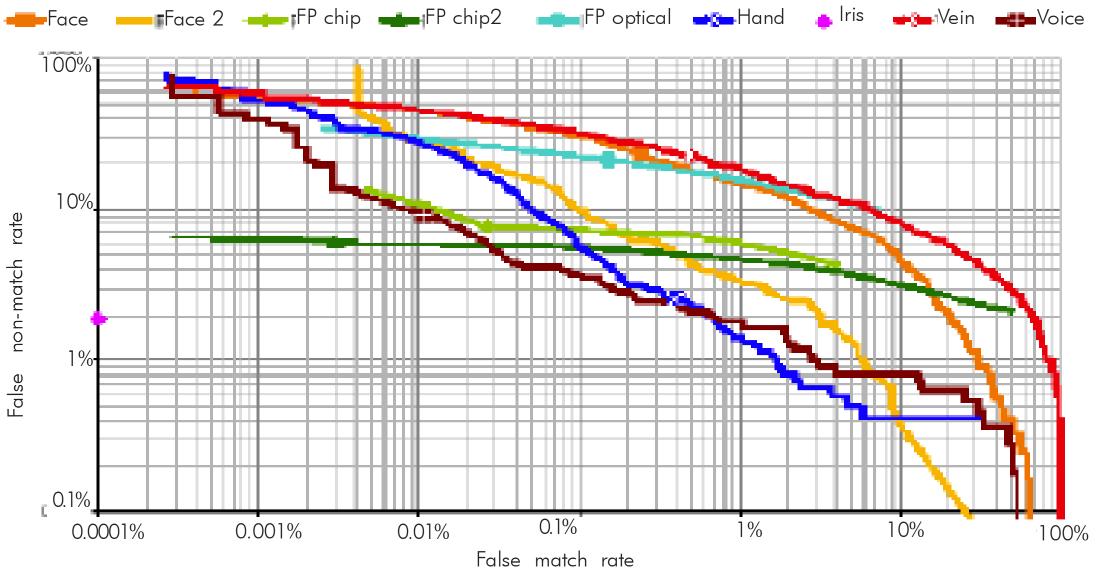


Figure 3: Biometrics Product Testing - Final Report (March 2001) Centre for Mathematics & Scientific Computing, National Physical Laboratory United Kingdom

Accuracy

Biometrics has been called the Holy Grail of security. Although it's a valuable and effective tool for securing self-service operations no biometric is foolproof. In addition to the variation described earlier (see Threshold) fielded applications must contend with variability in the following areas: user behavior (e.g., between novice and expert users as well as intra-user variability), changeable environmental conditions (e.g., lighting), input devices that become dirty or damaged, telephones or cameras that differ in the way they process input, and transmission channels that can be "noisy." These and other sources of variability may cause a biometric system to fail to recognize a sample provided by an authorized user. This kind of error is called *false rejection* or *false non-match*. A system may accept an impostor's claim as legitimate. Errors of this kind are *false acceptance* (also called *false match*). Placement of the threshold affects the ratio between false match and false non-match errors. Errors made when the threshold is set to require a stricter correspondence between the reference model and the new model tend to be false non-match errors. Correspondingly, systems allowing less correspondence between the two models are more likely to make false match errors than false non-match errors. Consequently, proper setting of the threshold is part of building an effective biometric system.

Sometimes systems cannot analyze the sample. If this occurs during enrollment, it's called *failure to enroll;* if it happens during authentication, its called *failure to verify*. This problem can be handled by having the system ask the user to provide another sample but might, for example, be the result of a dirty or poorly-functioning input device.

Most vendors will supply testing data they've conducted on their own products but there are few publicly-available independent performance tests for speaker authentication. Figure 3 shows the results of one assessment run by the National Physical Laboratory of the United Kingdom. It shows that the speaker-authenticatin tool (brown line) performed very well at a range of threshold levels when compared with the other biometricss.

Securing self-service deployments

Performance tests of technology reveal that biometrics are highly accurate but they do not speak to the issue of how secure a specific biometric self-service solution or product is – nor how well a biometric deployment is safeguarded against hacking. The level of security provided by a self-service deployment resides at the application level – in the security-component of the application as a whole. This section addresses three measures that support the deployment of effective and secure biometric applications. Multi-factor authentication is an element of the application design, Common Criteria Certification refers to the level of security that a product or solution offers, and the ANSI X9.84 standard provides guidance for protecting a biometric deployment.

Multi-factor authentication

The use of two-factor and multi-factor authentication can enhance the performance of any security system – no matter how powerful it already is. For speaker authentication, two-factor authentication can be as simple as asking the user to supply an account number or other identifier. In that case, the two factors are the identifier (something the person knows) and the person's voice (a biometric). Some speaker authentication systems store a series of questions to ask when the results of the biometric matching are close to the threshold and, therefore, questionable. Some of those questions may be tied to recent activities. For example, a system deployed by a financial institution might ask the amount or date of the person's most recent deposit.

Common Criteria certification

The *Common Criteria* standard (also called *Evaluation Criteria for Information Technology Security*) is an approved standard of the International Standards Organization (ISO) for evaluating IT security. It is intended to be used as the basis for evaluating the security properties of information technology products and systems. Common Criteria evaluation assigns a level of confidence to the security offered by a product or solution (not just raw technology). That level is based on the results of a battery of tests that may take several months to complete. The certification level that is assigned indicates whether the solution is secure enough for a specified type of application. The assessment includes protection from unauthorized disclosure of information (confidentiality), modification of data (integrity), and disruption of access (availability). It considers security threats that arise from human activity and other sources that may or may not be malicious, such as power interruptions and denial of service.

The only product using speaker authentication that has successfully undergone a Common Criteria evaluation is the VOICE.TRUST Server Version 4.1.2.0. It received Common Criteria Certification in 2005 at the EAL 2 level. This means that it is applicable to self-service operations that require up to moderate levels of independently assured security. The product also supports multi-factor authentication. Information about Common Criteria evaluation can be downloaded from www.commoncriteria.org.

Securing the security – ANSI X9.84

The American National Standards Institute (ANSI) has a standard called X9.84, *Biometric Information Management and Security for Financial Services.* Despite its name, it applies to biometric applications in any industry. ANSI X9.84 specifies the minimum security requirements needed for effective management of biometrics data throughout the life cycle of a deployment and describes methods for securing biometric data and systems during enrollment and authentication. It can be purchased and downloaded from the ANSI standards store at www.ansi.org.

Conclusion

The move to self service over the telephone is strong but it has been hampered by the lack of easy-to-use, effective security. PINs and passwords are compromised far too easily to support the migration of sensitive operations to self service. Biometrics, notably speaker authentication, provides an effective, easy-to-use solution that supports the deployment of secured self-service implementations for the telephone. But, simply using a biometric will not ensure that a deployment provides adequate security nor that the biometric system is protected from being compromised. The use of a multi-factor authentication design provides stronger authentication, especially when the results of biometric matching are inconclusive. Common Criteria evaluation of products and solutions specifies the security level that those products can provide and ANSI X9.84 is a guideline for developing secure biometric applications.

About J. Markowitz, Consultants

J. Markowitz, Consultants is a sole proprietorship formed in 1990 for the purpose of promoting development of creative and profitable speech recognition, voice-biometrics, and knowledge-based businesses. We have become one of the leading independent industry analysts in speech-processing and biometrics.

About Dr. Judith Markowitz

J. Markowitz, Consultants was founded by Judith A. Markowitz, PhD. Dr. Markowitz is recognized internationally as one of the foremost experts on the speech processing and voice-biometrics industries.

JC
M

J. Markowitz, Consultants
5801 N. Sheridan Road, Suite 19A
Chicago, IL 60660 USA
+1-773-769-9243
www.jmarkowitz.com