IJITKM Volume 7 • Number 1 • December 2013 pp. 124-127 (ISSN 0973-4414)

Application of Biometrics in Secure Bank Transactions

Garima Yadav
Research Scholar, School of Computer Science & IT, Singhania University, Rajasthan
garima.aky@gmail.com

Abstract
The introduction and adoption of remote banking, after hour services through automatic teller machines (ATMs), phone banking, online services and electronic commerce has changed the nature of financial services, giving people the convenience and the flexibility to do so much more with their time and resources. With remote banking, the channels of transaction move outside the walls of the bank, requiring adequate protection for both bank and customer. The ability to verify the identity of a specific individual is of critical importance in reducing acts of fraud and increasing security. Traditional automated verification methods such as ATM cards cannot provide positive identification - they may be lost or stolen, while PINs, passwords and account numbers may be steal or intercepted by unauthorized users through electronic means and other ways. A concerted effort to stop this crime requires a more reliable method of identification that relies on much more than names and social security numbers. It requires a way to truly ascertain a person's identity. Biometrics can be a central component of the solution.

1. Introduction

Financial institutions engaging in any form of Internet banking should have effective and reliable methods to authenticate customers. An effective authentication system is necessary for compliance with requirements to safeguard customer information, to prevent money laundering and terrorist financing, to reduce fraud, to inhibit identity theft, and to promote the legal enforceability of their electronic agreements and transactions[1]. The risks of doing business with unauthorized or incorrectly identified persons in an Internet banking environment can result in financial loss and reputation damage through fraud, disclosure of customer information, corruption of data, or unenforceable agreements. There are a variety of technologies and methodologies that can be used by financial institutions to authenticate customers. These methods include the use of customer passwords, personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices such as smart cards, one-time passwords (OTPs), USB plug-ins or other types of "tokens". One method which is different from all above is biometric identification; here the "biometrics" is defined as "the automated means of recognizing a living person through the measurement of distinguishing physiological or behavioral traits"[2].

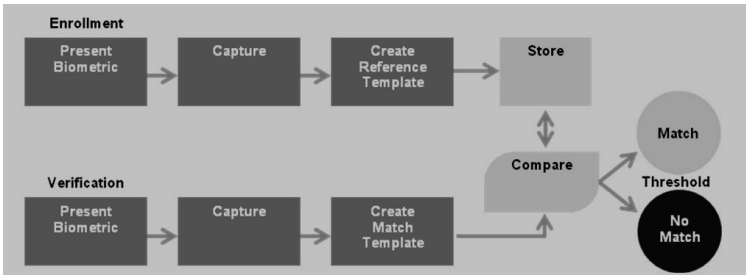

Figure1. Enrollment and Verification in Biometric System

The success or failure of a biometric system in a particular application is not dependent upon the reliability of the biometric product alone but there are many other factors also that contribute to the overall success or failure of the implementation. It is also essential to understand that no single biometric technology offers a solution to all user requirements.

Fingerprint as Biometric:

Among all the biometric techniques, fingerprint-based identification is the oldest method which has been successfully used in numerous applications. Everyone is known to have unique, immutable fingerprints. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points (Figure2). Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending. Fingerprint matching techniques

can be placed into two categories: minutiae-based and correlation based. Minutiae-based techniques first find minutiae points and then map their relative placement on the finger[2]. The matching will then hopefully become a relatively simple task of calculating the Euclidean distance will between the two codes.

Figure2. Minutiae points

We are developing algorithms which are more robust to noise in fingerprint images and deliver increased accuracy in real-time. A commercial fingerprint-based authentication system requires a very low False Reject Rate (FAR) for a given False Accept Rate (FAR). This is very difficult to achieve with any one technique. We are investigating methods to pool evidence from various matching techniques to increase the overall accuracy of the system.

2. Problem Domain

Employee Background Checks. The U.S. Federal Reserve Bank, Internal Revenue Service, ING Direct, Mellon Bank among other financial institutions in the United States use Identix live scan equipment to capture fingerprints for the purposes of conducting background checks on their applicants prior to granting employment[3]. This is a federal mandate that is designed to prevent internal fraud.

Transaction Security. Bank of Central Asia (BCA), Indonesia, uses biometrics to protect the interests of their customers, staff and the bank by ensuring that only authorized personnel could handle bank transactions. Existing methods of authorizing transactions by the bank's tellers and supervisors through the use of PINs and passwords could be opened to fraud and misuse. Replacing traditional passwords, Identix biometric system verifies the identity of employees who are authorized for withdrawals, deposits and electronic transfers over a certain amount and records an irrefutable audit trail. BCA has deployed Identix technology in more than 700 branches throughout Indonesia[4].

ATM Security and Monitoring. Armaguard Australia, a division of Mayne Nickless Ltd, and one of the world's largest cash transport companies, was the first company to use portable biometric devices from Identix. These devices are now installed on the cash security door of over 2,000 ATMs across Australia. The guards, who replenish and service the ATMs, carry a portable sensor with them, which is used to verify identity and open the cash security door[5]. An irrefutable electronic audit trail is created, recording who was biometrically verified both at the time of opening and the time of closing the ATM while the ATM is being refilled with money or being serviced. All communication with the ATMs is done remotely using Identix software.

Customer Passbook Identification. Conavi Bank of Medellin in Colombia uses Identix biometric devices to irrefutably identify "passbook" account customers at each branch. Previous methods, which involved comparing signatures against microfiche records, were slow and insecure – in the event of fraud, the liability lay with the customer. Conavi saw the biometric solution as a unique competitive advantage as well as offering a genuine benefit to its customers.

Secure Member-Bank Database Access. To ensure the unfettered exchange of sensitive data and information without risk of unauthorized access, the Central Bank of Costa Rica has deployed Identix fingerprint security solutions to provide secure access to its databases by member banks. The Bank ensures that only authorized officers from its recognized member banks can access the Central Bank's databases by requiring verification through fingerprint biometrics prior to allowing access. The Central Bank has deployed more than 400 Identix BioTouch USB fingerprint readers to its network of member banks.

Customer Touchpoints and Remote Banking. Chile-based Banco Falabella has adopted biometric banking for its branches throughout the country. The bank has integrated Identix biometric security solutions to provide heightened security for its customers, while eliminating the need to remember cumbersome passwords. Customers are required to verify their identity via the fingerprint readers prior to performing a transaction with a teller. The bank has also installed Identix technology at its credit card centers to verify customer identification prior to making a withdrawal

on a card. Finally, the bank has integrated Identix biometrics with ATMs to replace PIN numbers for customer withdrawals.

Transaction Verification for Commodities Traders. The Brazilian Mercantile & Futures Exchange (BM&F) is the world's first stock market to implement fingerprint biometrics security for authentication and access to its electronic Global Trading System. The solution requires traders to access the electronic Global Trading System via fingerprint biometric authentication. Traders are required to verify their identity via the fingerprint readers periodically at defined time intervals throughout the period of time they are logged-on to the system[6]. This helps to guarantee the security and exclusiveness of access by authorized traders to the electronic Global Trading System.

Safe Deposit Box Security. Safety deposit box access for customers through biometric verification is proving to be popular in Switzerland because of banking regulations. Through the use of biometrics, bank clients no longer have the problems of forgetting or losing their keys. Identix access control units control access to safety deposit boxes by using the fingerprint system, which eliminates the need for a bank officer to accompany the customer to the vault. This translates into considerable savings in bank administration and staffing.

3. Risk Assessment

The implementation of appropriate authentication methodologies should start with an assessment of the risk posed by the institution's Internet banking systems. The risk should be evaluated in light of the type of customer (e.g., retail or commercial); the customer transactional capabilities (e.g., bill payment, wire transfer, loan origination); the sensitivity of customer information being communicated to both the institution and the customer; the ease of using the communication method; and the volume of transactions. An effective authentication program should be implemented to ensure that controls and authentication tools are appropriate for all of the financial institution's Internet-based products and services[7]. A comprehensive approach to authentication requires development of, and adherence to, the institution's information security standards, integration of authentication processes within the overall information security framework, risk assessments within lines of businesses supporting selection of authentication tools, and central authority for oversight and risk monitoring. This authentication process should be consistent with and support the financial institution's overall security and risk management programs. The method of authentication used in a specific Internet application should be appropriate and reasonable, from a business perspective, in light of the reasonably foreseeable risks in that application. Because the standards for implementing a commercially reasonable system may change over time as technology and other procedures develop, financial institutions and technology service providers should develop an ongoing process to review authentication technology and ensure appropriate changes are implemented.

Account Origination and Customer Verification

With the growth in electronic banking and commerce, financial institutions should use reliable methods of originating new customer accounts online. Potentially significant risks arise when a financial institution accepts new customers through the Internet or other electronic channels because of the absence of the physical cues that financial institutions traditionally use to identify persons. One method to verify a customer's identity is a physical presentation of a proof of identity credential such as a driver's license. Similarly, to establish the validity of a business and the authority of persons to perform transactions on its behalf, financial institutions typically review articles of incorporation, business credit reports, board resolutions identifying officers and authorized signers, and other business credentials[8]. However, in an Internet banking environment, reliance on these traditional forms of paper-based verification decreases substantially. Accordingly, financial institutions need to use reliable alternative methods.

Monitoring and Reporting

Monitoring systems can determine if unauthorized access to computer systems and customer accounts has occurred. A sound authentication system should include audit features that can assist in the detection of fraud, money laundering, compromised passwords, or other unauthorized activities. The activation and maintenance of audit logs can help institutions to identify unauthorized activities, detect intrusions, reconstruct events, and promote employee and user accountability. Financial institutions should rely on multiple layers of control to prevent fraud and safeguard customer information. For example, a financial institution can analyze the activities of its customers to identify suspicious patterns. Financial institutions also can rely on other control methods, such as establishing transaction dollar limits that require manual intervention to exceed a preset limit[9]. Adequate reporting mechanisms are needed to promptly inform security administrators when users are no longer authorized to access a particular system and to permit the timely removal or suspension of user account access.

Customer Awareness

Financial institutions have made, and should continue to make, efforts to educate their customers. Because customer awareness is a key defense against fraud and identity theft, financial institutions should evaluate their consumer

education efforts to determine if additional steps are necessary. Management should implement a customer awareness program and periodically evaluate its effectiveness[10]. Methods to evaluate a program's effectiveness include tracking the number of customers who report fraudulent attempts to obtain their authentication credentials (e.g., ID/password), the number of clicks on information security links on Web sites, the number of statement stuffers or other direct mail communications, the dollar amount of losses relating to identity theft, etc.

4. Conclusion

As biometrics continues to advance scientifically and technologically, its use and acceptability as a means of security and authorization across various sectors also grows. Biometrics would be a useful solution to the issue of security for mobile banking in developing countries, particularly to address the unique needs of the unbanked in rural areas. Technically, the use of biometrics is entirely feasible in mobile applications. The main issue to address with any biometric system is that the performance will only be as good as the quality of the data captured, so that environmental controls and user training are of paramount importance. For purposes of mobile phone banking, fingerprint recognition appears to be the best technology to use today. Fingerprints are already being used for several rural banking applications around the world, with acceptable performance and security results. Fingerprint recognition security could either interface directly with a bank's online banking system, an approach that will often require costly systems integration (and result in an undesirable one-off solution), or it could interface with a separate mobile banking platform. The mobile banking platform would act as a "black box" intermediary between the cellphone and the bank, receiving the identity and biometric authorization data from the user's handset and, once verifying the information, sending a pre-authorized signal to the banking system, using standard ISO banking protocols, telling the bank to go ahead with the transaction at hand. Recent advances in biometric technology have resulted in increased accuracy at reduced costs, biometric technologies are positioning themselves as the foundation for many highly secure identification and personal verification solutions. Today's biometric solutions provide a means to achieve fast, user-friendly authentication with a high level of accuracy and cost savings. Many areas will benefit from biometric technologies. Highly secure and trustworthy electronic commerce, for example, will be essential to the healthy growth of the global Internet economy. Many biometric technology providers are already delivering biometric authentication for a variety of web-based and client/server based applications to meet these and other needs. Continued improvements in technology will bring increased performance at a lower cost. While biometric authentication is not a magical solution that solves all authentication concerns, it will make it easier and cheaper for you to use a variety of automated information systems.

5. References

[1] John C. Dvorak, Forbes.com, SmartCards Get Smarter 06.01.01, 3:00 PM ET http://www.forbes.com/2001/06/01/0601dvorak.html

[2] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. Springer- Verlag, 2003.

[3] N. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in *Proc. Audio and Video-based Biometric Person Authentication (AVBPA)*, pp. 223–228, (Halmstad, Sweden), June 2001.

[4] American Express Announces Winners of 'Code Blue' Contest - Global Competition Spurs Innovation in Java(TM) Technology-Based Smart Card Development http://www.SmartCardcentral.com/news/pressrelease/may2001/amex_052301.asp

[5] Scottson & Michaels, Inc. has been in the business of Credit Card Fraud Verification Processing since 1994. http://www.scottson-michaels.com/ccfraudhistory.htm

[6]"Army's New Password: 'Biometrics'", USA Today, Thursday, June 22, 2000, Section, "The Nation," page 3A. Microsoft, Others Unveil Tools To Protect Online Privacy By Linda Rosencrance 06/21/2000 http://it.idg.net/crd_fraud_69160.html

[7] The following list of articles very nicely explains simple applications available. Although dated, if someone is looking for a quick solution, updated features and prices could be found at the vendor's sites.

[8] http://www.zdnet.com/pcmag/features/biometrics/387164.html

[9] PC Magazine: Compaq Fingerprint Identification Technology By Stephen W. Plain, February 23, 1999 http://www.zdnet.com/pcmag/features/biometrics/387165.html

[10] Preface, By Ira S. Somerson, BCFE, CFE, CPP, President, Loss Management Consultants, Inc., Blue Bell, Pa. http://www.securitymagazine.com/whitepaper.htm