Application of Biometric Technology Solutions to Enhance Security

Purpose:

The purpose of this white paper is to summarize the various applications of fingerprint biometric technology to provide a higher level of security for information access via intranets, extranets, the Internet, physical access and for more secure financial and eCommerce transactions. This white paper will not address the other eight biometrics including, iris scan, retina scan, facial scan, hand geometry, voice, signature, keystroke pattern and gait. It will focus on application of Fingerprint Biometric Technology Solutions to enhance security in Corporate IT, Aviation, Banking and Financial, Healthcare and the Government sectors.

Introduction:

As organizations search for more secure authentication methods for user access, ecommerce, and other security applications, biometrics is gaining increasing attention.

What is a Biometric?

The security field uses three different types of authentication:

- Something you know—a pass-word, PIN, or piece of personal information (such as your mother's maiden name);
- Something you have—a card key, smart card, or token (like a SecurID card); and/or
- Something you are—a biometric.

Of the three different types of authentication above, a biometric is the most secure and convenient authentication tool. It can't be borrowed, stolen, or forgotten, and forging one is practically impossible. (Replacement part surgery, by the way, is outside the scope of this white paper.)

Biometrics measure individuals' unique physical or behavioral characteristics to recognize or authenticate their identity. The five physical biometrics include fingerprints, hand or palm geometry, retina, iris, or facial characteristics. The four behavioral biometric characteristics include signature, voice (which also has a physical component), keystroke pattern, and gait.

Applications:

The world would be a fantastic place if everything were secure and trusted. But unfortunately, in the real world there is fraud, crime, computer hackers, and theft. With our lives becoming more and more dependent on digital technology and automation, how do we know if people are really who they claim to be? Following the events of September 11th, there is a compelling need for a more secure future, yet it's held back due to the lack of wide deployment of authentication technology solutions for information and physical access security. How can we securely identify and authenticate who is who? The answer lies in fingerprint authentication solutions.
Fingerprints have been legally accepted for verifying identity for over a century. They cannot be altered, forgotten or cracked by hackers running a software routine. They are universally accepted as unique to each individual, and they are used in situations where there can be no mistake of identity, such as criminal proceedings and high security access control.

A fingerprint-based biometric security solution can assure people's personal identities through digital recognition. Fingerprint authentication provides a dependable, legally acceptable method for authenticating users. With focus on information security, physical access control and management, and embedded solutions, fingerprint authentication can be integrated and applied to a wide range of industries, which will be discussed later in this white paper.

Physical access

For decades, many highly secure environments have used biometric technology for entry access. Today, a major application of biometrics is in physical security: to control access to secure locations (rooms or buildings). Unlike photo identification cards, which a security guard must verify, biometrics permit unmanned access control. Today, biometric devices, such as fingerprint readers, are deployed in office buildings, hospitals, casinos and health clubs. Biometrics are useful for high-volume access control. For example, biometrics controlled access of 65,000 people during the 1996 Olympic Games, and Disney World uses a fingerprint scanner to verify season-pass holders entering the theme park.

Virtual access

For a long time, biometric-based network and computer access were areas often discussed but rarely implemented. Recently, however, the unit price of biometric devices has fallen dramatically, and several designs aimed squarely at this application are on the market. Analysts see virtual access as the application that will provide the critical mass to move biometrics for network and computer access from the realm of science-fiction devices to regular system components. At the same time, user demands for virtual access will raise public awareness of the security risks and lower resistance to the use of biometrics.

Physical lock-downs can protect hardware, and passwords are currently the most popular way to protect data on a network. Biometrics, however, can increase a company's ability to protect its data by implementing a more secure key than a password.
Using biometrics also allows a hierarchical structure of data protection, making the data even more secure: Passwords supply a minimal level of access to network data; biometrics, the next level. You can even layer biometric technologies to enhance security levels.

E-commerce applications

E-commerce developers are exploring the use of biometrics and smart cards to more accurately verify a trading party's identity. For example, many banks are interested in this combination to better authenticate customers and ensure non-repudiation of online banking, trading, and purchasing transactions. Point-of-sales (POS) system vendors are working on a cardholder verification method, which would enlist smart cards and biometrics to replace signature verification. MasterCard estimates that adding smart-card based biometric authentication to a POS credit card payment will decrease fraud by 80 percent.

Fingerprint Authentication can be integrated and applied in a wide range of sectors including:

Corporate IT

IT security is a very important and critical issue as more and more mission-critical information resides in electronic form. From product designs, business plans, client

records, financial reports, and account records, access to these electronic resources improve value and productivity; but at the cost of a higher threat to theft and fraud.

The most widely used methods of controlling access to computers and data is passwords and PIN numbers. While passwords and PIN numbers are easy to use, they provide weak proof of identity. They are rarely changed, frequently shared, often used in plain sight and easily defeated using widely available hacker programs. Since passwords do not provide the level of security necessary for an electronically networked society, the need exists for an authentication method that is easy to use, easy to connect to computer networks and legally accepted. Implementing fingerprint authentication and replacing passwords and PIN numbers makes access to corporate information more efficient and secure.

Not only will fingerprint authentication provide a means of security, it will also increase efficiency and decrease costs. Gartner Groups states that password maintenance costs $400 to $600 per user per year, and that 20 to 50 percent of all calls to company help desks are from people needing their passwords reset.[1]

The use of fingerprint authentication will:

- Eliminate password problems
- Consolidate multiple passwords to one single biometric login
- Control and manage user access to corporate network database
- Control and manage physical access to authorized areas
- Secure important confidential corporate information

Benefits:

- Higher corporate security
- Time/cost efficiencies

Aviation

The events of September 11th, 2001 have heightened security awareness and created the need to validate or identify users of a given service. Is the person boarding the plane or working at the airport indeed the person they claim to be? Airport security has been a concern for some time. Not only are airports a target for terrorism, they also are a means

of such criminal activity like theft, smuggling, and evasion from law enforcement authorities. Ensuring personal authentication and providing increased security, automating personal authentication of customers/employees using fingerprints will reduce the labor costs and increase aviation security being demanded today. With fingerprint authentication solutions, one can:

- Perform airport and airline employee background checks
- Control and manage physical access rights to all authorized areas of the airport
- Control and manage user access to airport computer network/database
- Securely identify passengers to their IDs, passports, Visas, boarding pass, and baggage.

Benefits:

- Significantly improves airport security
- Builds public trust and confidence
- Discourages terrorist and criminal activities
- Time/cost efficiencies

Banking and Financial

Theft, fraud, and embezzlement in this area has risen to alarming rates as electronic methods of conducting transactions are taking over the conventional systems of checks and balances. Traditionally, financial transactions required face-to-face interaction, but with today's technology, it is more efficient and cost effective to do it electronically.

Yet, this remote way of doing business via computers and the Internet creates an environment where fraud and identity theft is a part of the risk equation. As automated and remote methods of conducting banking and financial transactions grow, the need to know with certainty that the transaction is actually being performed by a known, identifiable, valid user at the other end grows in importance also.

The Internet has grown to great lengths, yet fraud and identity theft are the biggest deterrent to the growth of Internet commerce and banking. Consumers can see the numerous benefits of using the Internet for shopping and trading online, yet the fear of not knowing whom they are dealing with at the other end of the transaction is what keeps them from utilizing these resources. The Gartner Group forecasts that 24-30 million households will be transacting on the Internet by the end of 2004, up from 7 million in 1998.[1] Fingerprint authentication can provide security and peace of mind to these households by tackling the issue of security. A fingerprint authentication solution can provide:

- Secure online banking transactions

- Secure customer financial information
- New online services
- Non-repudiation

Benefits:

- Fraud protection
- Customer confidence and retention
- Time/cost efficiencies
- Ability to extend services to non-local customers

Healthcare

Fraud plays a significant role when it comes to government-sponsored programs focused on healthcare. According to HCFA (Health Care Financing Administration) government spending on healthcare in the U.S. exceeds $560 billion. The federal government accounts for 33 cents of every dollar spent on healthcare in the U.S. and state governments account for another 11 cents of every dollar spent. This represents over 6% of GDP annually. With recent occurrences of fraud uncovered by the federal government, where individuals in the name of deceased relatives and or friends received healthcare benefits, serious questions are raised regarding who is receiving the service or benefit on whose card. But, there is another issue of risk mitigation, as more patient data is now being kept in electronic form. HIPAA (Healthcare Insurance Portability & Accountability Act) mandates that all patient records must be protected with something stronger than a mere password by October 16, 2002.

Maintaining confidentiality and security of a patient's record by allowing controlled access to selected parts of a patient's electronic record to only those authorized clinicians who absolutely need to access the patient information to deliver services, presents a huge issue for hospitals and physicians. It is in this healthcare environment, that a convenient and secure method of "just-press-here" fingerprint authentication solution, can lead to the achievement of the level of confidentiality and security of patient's electronic records, required by hospitals and physicians.

With the implementation of HIPAA, healthcare organizations are challenged to contain escalating administrative and security costs, while also ensuring patient privacy and

security of patient records. One of the proposed standards is the use of digital signatures
in HIPAA-specified transactions to:

- Improve the efficiency and effectiveness of the healthcare system by standardizing the interchange of electronic data for specified administrative and financial transactions.
- Protect the security and confidentiality of electronic health information.[2]

The integration and use of fingerprint authentication can:

- Support HIPAA standards
- Provide accurate patient history
- Authenticate hospital employees for remote information access to patients record
- Control and manage physical access rights to authorized rooms
- Perform staff background checks
- Extend medical services like online prescriptions or telemedicine

Benefits:

- Reduce hospital errors and operating costs
- Higher level security
- Time/cost efficiencies

Government

The government has the largest and most complex information system that exists today,
having influence on every part of our daily lives. With Federal, State, local, and foreign
government organizations, an important concern is protecting classified and sensitive
information, ensuring integrity of the information, and controlling access to the information and systems that process and transport this information. Now with all this
precious information residing in electronic form, there is a necessity for it to be secure
and confidential, yet maintain its efficiency and convenience.

Biometric verification can greatly reduce the cost of delivering essential services by government agencies and other non-profits. These cost savings take two major forms:
reduced overhead for delivering the service and fraud reduction. In the case of egovernment
usage the major feature fingerprint authentication offers is personal authentication. Namely,
that an individual or benefit recipient is indeed who they claim to be and who the government thinks they are.

Fingerprint verification can greatly reduce costs for distributing social services.

Distribution of funds from entitlement programs can be linked to the rightful recipient.
This can help ensure timely delivery of these services while reducing the possibility of
fraud and theft. Also, the use of fraudulent identities to gain access to government services can be reduced.

- Connecticut's Department of Social Services has saved the state $9 billion by using fingerprint verification in its welfare benefit program. (Gartner Group)
- Los Angeles County employs a fingerprint identification system to identify welfare recipients. Along with savings of $18 million in a three-year period, the county reports that the number of individuals receiving payments has dropped by
  3,000. This is thought to be due to the elimination of people enrolled under multiple names. (Gartner Group)

Fingerprint verification can also be an enabling technology that allows broader egovernment
initiatives such as electronic voting, voter registration, vehicle registration
and other online services. Current studies show that the administrative costs for voting
generally range from $2 to $7 per vote with some special elections costing significantly
more than this. The cost savings of the digital age will only be realized to their fullest by
local, state and federal governments when the authentication of a delivered service takes
place as part of the solution.

Therefore, from law enforcement, military, judicial, education, and social services, the
use of fingerprint authentication can be integrated and applied to many government services:

- Identifying and validating the correct person in government entitlement programs.
  Fraud in government entitlement programs estimated by the General Accounting
  Office is at over $10 billion a year.[3]
- In law enforcement in identifying criminals or access control in jails and prisons
- In education with distance learning and Internet based classes
- In military and personnel authentication to classified information, physical access
  to authorized areas, and military equipment control
- In government services such as electronic voting, voter registration, vehicle registration, and other online services

Main benefits:

- Fraud reduction
- Time/cost efficiencies

Biometric technology has been around for decades but has mainly been used in highly secretive environments requiring extreme security measures. This white paper has addressed application and benefits of fingerprint biometric authentication in a variety of industries and in the government sector. The events of September 11, 2001 have significantly increased security concerns of both private citizens and of governments around the world, and are likely to accelerate the deployment of fingerprint biometric security solutions for information access via intranets, extranets, the Internet, physical access and for more secure financial and eCommerce transactions.

REFERENCES

1 Gartner Research Group. 25 April 2002. http://www.gartner.com
2 Health Insurance Portability and Accountability Act Executive Summary. 25 April. 2002. http://www.hipaa-iq.com/summary.htm
3 Campbell, Joseph, Lisa Alyea, and Jeffery Dunn. Government Applications and Operations. Biometric Consortium. 25 April. 2002. http://www.biometrics.org