March 2000

Body language, security and e-commerce

Norman Desmarais
Providence College, normd@providence.edu

Body Language, Security And E-Commerce

Norman Desmarais

Introduction

Security is a major concern for computer users and system administrators. Whether to protect confidential information in individual files, lock a computer system to unauthorized users, control access to an intranet or an extranet, or conduct business on the Internet, one needs to determine an appropriate level of security and the effective means to achieve the objective.

The Internet uses simple mail transfer protocol (SMTP) as the protocol to transmit electronic mail and most business transactions. These transmissions have as much privacy as a postcard and travel over insecure, untrusted lines. Anyone anywhere along the transmission path can obtain access to a message and read the contents with a simple text viewer or any word processing program. Because the transmission lines are insecure, it is easy to forge e-mail or use another person's name. Theft of identity is becoming the nation's leading incidence of fraud. A person can even claim that someone else sent a message, for example, to cancel an order or avoid paying an invoice.

Yet we continue to transmit purchase orders and other private messages via e-mail in ASCII text which is the least common denominator for electronic text. The first objective to improve security is to control physical access by limiting it to authorized individuals. The principle is that the fewer people who can get physical and administrative access to sensitive files or to server systems, the greater the security will be.

Most applications rely on passwords, cards, personal identification numbers, and keys to access restricted information or confidential files. But passwords, cards, personal identification numbers, and keys can be forgotten, stolen, forged, lost, or given away. Moreover, these devices serve primarily to identify the person. They cannot verify or authenticate that the person really is who he or she claims to be. Systems that rely on IP address verification limit access to users with a specific domain name or Internet address. Basically, this procedure identifies an individual by the machine he or she uses. Anybody using a particular computer can impersonate the rightful owner; and authorized users trying to obtain access via a different server or domain name cannot do so because the server does not recognize their address. This may require setting up a proxy server to accommodate such access; and IP spoofing has become quite common to get around these restrictions.

Because many e-commerce transactions can result in legal actions (e.g. contracts) that bind the respective parties, it is important to verify that the parties in a business transaction really are the people they purport to be and are authorized agents of the companies they represent. This article will first study some of the developments for improving security in the authentication of

individuals. It will then examine what is being done to improve the security of the content that constitutes the actual transactions and the electronic transmission of those messages.

Biometrics

Much of the effort to improve personal security focuses on what is referred to as biometrics which means “life measurement”. It is based on the principle that everyone has unique physical attributes that, in theory, a computer can be programmed to recognize. Biometrics uses mathematical representations of those unique physical characteristics to identify an individual or to verify identity. It can serve to authenticate people because everyone has unique and somewhat stable body features and ways of doing things. While passwords, cards, personal identification numbers, and keys can be forgotten, stolen, forged, lost, or given away, biology cannot be. We have all seen biometric devices used in science fiction movies. Now, they are making their way to the desktop and to personal workstations.

New developments in chip technology, lower-priced processors, and increasingly secure environments are making OEMs (original equipment manufacturers) consider biometrics as a way to differentiate their systems. These same factors are also inducing consumers to upgrade, augment, or replace their security systems with biometric-based versions. One only needs a microphone or camera, a fingerprint or eye scanner, and the corresponding software.

We can divide biometric techniques into two categories: physiological and behavioral. Common physiological biometrics include finger (fingertip, thumb, finger length or pattern), palm (print or topography), hand geometry, wrist vein, face, and eye (retina or iris). Behavioral biometrics include voiceprints, keystroke dynamics, and handwritten signatures.

For a list of biometric information sources, see the Appendix.

Fingerprints

Fingerprint technology is the most commonly used biometric, because it has been used in law enforcement for over 100 years. However, prisons and law-enforcement populations are comprised mostly of relatively uniform populations of males between the ages of 18 and 36 whose fingerprints are in relatively good condition. Some people have fingerprints that are harder to image. About 2 percent of the general population’s fingerprints baffle computers. It is often difficult to image fingerprints from people with very small

hands and fingers, people who work with their hands, or those who have injuries or scars. Also, as people age, they often lose the lipid (fat) layer in their skin and their fingerprints become worn and difficult to image.

Capacitive sensing is the most frequently used fingerprint-sensing technology. It employs a silicon integrated circuit comprising an array of capacitive sensor plates wherein a capacitive sensor measures the capacitive difference between the dead-skin layer and air space. In other words, these types of devices actually measure moisture on the finger, not a fingerprint; and it is this measure of moisture that often leads to problems when taking an image of someone's print. Consequently anyone with dirt, oil, or other contaminant on the hand or anyone with dry skin, such as older people whose skin loses moisture with age, could experience problematic readings with capacitive fingerprint sensors. One such device is FingerLoc, marketed by AuthenTec Inc. (Melbourne, FL), a spin-off of Harris Semiconductor Corp.

Other devices take images of the fingerprint itself. NEC's Touchpass system uses CCD (charged couple device) or CMOS (complementary metal oxide semiconductor) software together with optics and prisms to scan a fingerprint. Thomson Components and Tubes's FingerChip uses low cost CMOS technology in a 500-dpi fingerprint sensor that requires no optics or light source. It takes an image of the entire finger by sweeping it across the silicon sensor. While incorporating such chips and sensors into computer keyboards remains quite expensive, Thomson has a prototype chip that it expects will cut the cost for fingerprint verification from $300 to $5-10 within a year.

Veridicom Inc. (Santa Clara, CA), a spin-off from Bell Labs, uses a direct-current capacitive sensor in its FPS 100 chip. American Biometric Co.[1] and Biometric Access Corp.[2] also offer fingerprint scanning technology for less than $200 per seat. Biometric Access's SecureTouch fingerprint reader sells for $119 in bulk and can be used to authenticate individuals throughout an enterprise with products such as IBM's Global Sign-On 2.0.

Compaq provides its own fingerprint scanner, called Identicator (based on the manufacturer of the same name), as an option. It attaches to a keyboard or monitor and plugs into a PC's standard peripheral component interconnect (PCI) slot. Identicator scanners measure 43 points along the ridges and crevices of a finger, then search through a database for a match. Samsung also introduced a keyboard with a fingerprint identification device attached that plugs into a universal serial bus. Both companies see their systems particularly appropriate for environments where security is important, such as research and development, finance, and manufacturing.

Fingerprint scanners could work fine in a private security application where it may suffice to match a few locally stored prints. They are more difficult to fool than face-recognition systems because they measure the unique and complex swirls on a person's fingertip and some can even accommodate cuts. However, a public security setting, where potentially anyone's prints would need to be matched, could pose problems because current methods require large central databases. For example, if a customer makes a purchase with a credit card, his or her fingerprints might have to be matched against everyone who owns that

particular card unless there is a tamper-proof way of storing prints locally. Also, cuts and dirt can distort images. If a previous user leaves an oily latent image on the scanner, a false rejection may occur or someone with a fine brush and dry toner could "lift" fingerprints with adhesive tape. Solving these problems would open up a range of applications.

Fingerprint-chip technology will continue to improve, decreasing production costs and making it affordable to embed chip-sized finger readers in different electronic devices, such as keyboards, handheld computers, cellular phones, ATMs, television remote controls, automobiles, building security, and home lock systems. Some people even see this technology as a possible solution for gun safety. A gun with a self-contained fingerprint or handprint recognition system could restrict use to the gun's rightful owner.

Palm/hand

Palm/hand scanners, a variation of the fingerprint scanners, are better suited to sites in which the users may be working with their hands. They measure creases and/or geometry that will not be substantially altered by grime or nicks. However, these devices are also more expensive and less accurate than the fingerprint scanners, especially at sites with a large number of users.

The Handkey II reader from Recognition Systems, Inc. (Campbell, CA) which lists at $1,595 digitizes three-dimensional hand geometry, boiling down palm shapes, finger lengths, etc. to unique nine-character codes. While the system can use a cheap eight-bit processor – a member of a family that dates back to the 1970s – rather than a Pentium, the optics and algorithms account for the magic. The system is smart enough to distinguish a hand even if a person has a swollen finger or wears a bandage. William W. Wilson, president of Recognition Systems, claims an accuracy of 99.9 percent and says that his devices control the doors to 90 percent of America's nuclear reactors. He expects the US Immigration and Naturalization Service will become his next big customer. They are using hand-readers at the JFK, Toronto, Newark, and Miami airports where travelers who enroll with the INS receive cards with a magnetic stripe that they swipe through a reader. The card and handprint readers let travelers whisk through passport control lines in a few seconds.

Smart cards

Some manufacturers are relying on smart cards to control access, particularly to notebook PCs. They encode fingerprint data (128 to 512 bytes) in the smart card's microprocessor so it operates like a bank cash machine where one enters the card and a personal identification number (PIN). For example, IBM's

Smart Card Security Kit uses both a smart card and a four-digit PIN to provide access to a notebook's hard drive. Hewlett-Packard is also embracing the smart card.

Face

Face recognition also satisfies most of the criteria for the ideal biometric solution. It is easy to perform, fast, moderately convenient, and nonintrusive, except perhaps to the camera-phobic. Video camera hardware is relatively inexpensive; and some monitor manufacturers build camera lenses into their display screens to accommodate videoconferencing. With today's faster processors, even a low quality digital camera can do a pretty good job of reading digital video and can recognize individuals 78 percent of the time. These factors contribute to making face recognition one of the fastest-growing niches. However, the technology is subject to spoofing; and lighting can affect authentication.

Visionics Corp. (Jersey City, NJ) developed a "faceprint" algorithm that creates a cranial blueprint using 140 measurements of various parts of the face, such as the distance from the eyes to the nose. These devices can identify people on the basis of features inherent in the structure of their skulls – features that can't be altered except by radical plastic surgery. Consequently, if these face-recognition technologies deliver on their promises, fake beards and other disguises will no longer conceal an individual's identity. If someone wears a ski mask, for example, to obscure enough measurements to preclude a positive identification, the computer will still be able to produce a short list of possible matches. This has obvious applications for bank security systems.

Face-recognition systems can also work with people still at a distance. As one approaches, the system could recognize the face and activate the system, such as turning on a computer or unlocking a door. Visionics's technology is being tested at an airport, scanning crowds for terrorists or thieves. Scotland Yard is evaluating TrueFace, a system from rival Miros Inc. (Wellesley, MA). TrueFace is being used by a check-cashing machine operator in Texas. In less than one second, this system compares an image from a common security camera to stored images of pre-authorized individuals.

Some applications are focusing on a person's smile as a replacement for a security password. Other techniques based on ear or lip shape and knuckle creases are in the conceptual stages; and one startup company is trying to recognize a person's identity by body odour. However, there are no commercial products yet on the horizon for these authentication methods.

Eye scanning

Eye scanning is probably the fastest growing area of biometric research because of its promise for high scan accuracy. The hardware is several times more expensive than face, finger, or palm recognition systems; but, even though iris or retina scanners are the most expensive biometric technologies (ca. $5,000), they are the most difficult to fool. Eye scanners can even detect and utilize such personal characteristics as eye-pulsing blood vessels.

There are two types of eye scanning: retinal scanning and iris scanning. Retinal scanning uses lasers that focus on the back of the eye, while iris scanning zooms in on the front. The retina is considered unique even among identical twins In a retinal scan, one places his or her eyes two inches away from a retinal scanner, like EyeDentity, Inc.'s (Baton Rouge, LA) small video-camera, while a modulated light source scans the retina and forms an image of the unique patterns of the veins on the back of the eye. The image is matched against a central database to verify the individual and grant access.

Likewise, the iris is the most feature-rich part of the human anatomy that is constantly on view. Iris scanning developed from the research of Leonard Flom and Aran Safir, two ophthalmologists who now work for IriScan (Marlton, NJ). They proved, in the 1980s, that the iris' complex pattern of striations, freckles, and fibrous structures offered a considerably more precise means of identification than the relatively simple loops and whorls of a fingerprint.

The iris can have more than 250 distinct features, compared with 40 or 50 points of comparison in fingerprints; so iris scanning is an order of magnitude more accurate than fingerprints or even DNA analysis. Also, unique patterns in the human iris stabilize within one year of birth and remain constant throughout one's lifetime, unlike other biometrics, such as knuckle creases, voice patterns, and body odours. However, contact lens wearers or people with optical diseases like glaucoma may not easily pass an eyeball scan.

It is impossible to counterfeit the distinct iris pattern with any existing scientific technology. Iris scanning also has the advantage of being passive. A reader embedded in a teller machine, security post, or computer monitor can capture a person's image as he or she walks toward the device. Analysis takes about two seconds. The codes storing the iris information require very little computer memory – only about 256 bytes. That makes searching an archive easy. A personal computer can scan up to 100,000 records a second with a mismatch rate of less than one in 100,000.

IriScan introduced its scanner at Comdex (November 1998). The device looks a bit like a hair dryer and works by taking a video image of the iris. It breaks the image into circular grids to analyze the unique patterns within each area.

Iris and retina scanning are considered expensive and are the most uncomfortable biometric for users, psychologically, because some people see it as intrusive and inconvenient. With iris recognition, a person doesn't have to identify himself first – he just looks at the camera; and the software searches

the database to locate a matching iris. John Daugman, who developed the set of mathematical formulae underlying iris scanning technology at Cambridge University in 1994, says there has not been a false match in more than 30 million tries. However, an out-of-focus camera, mirrored sunglasses, thick contacts, and other such barriers to recognition account for system failures about 1 percent of the time, Daugman acknowledges.

Some people expect that electronic commerce will be the “killer application” for iris scanning. They see legal tender in the e-commerce age consisting of a digital certificate (more on this later) combined with a coded image of a person’s iris. While eye scanning is the most expensive and most accurate biometric, behavioral biometrics cost the least to implement; but they are less robust than physiological ones.

Voice recognition

The voice offers a less secure way to recognize an individual, but it provides the second most secure method after eye scanning. The process is slow and subject to a person’s physical or emotional state. Voice recognition software has come a long way in the past few years. No longer is it restricted to giving commands to computer programs. It is being used more and more for dictation with continually improving results. However, one must “train” the software to recognize the patterns of one’s speech. This process creates a profile of one’s vocal tract for subsequent use. The systems used for security operate in much the same way as voice recognition (discrete commands) and speech recognition (continuous speech) systems and are generally used in combination with PIN numbers to act as a password to keep systems secure. Some people worry that the voice can be recorded and played back for identification. Others think that the threshold might be too low, resulting in access systems nearly as complicated as the password approach.

Motorola’s Ciphervox system employs technology originally used in combat suits to turn on maps, infrared objects, and radios. It generates a 700-byte individual voiceprint and embeds it on a chip for use with a PIN number to allow entry into a system. Motorola, NEC, and other companies see banks, personalized content on PCs, and phones as prime applications for this technology. Other possibilities include screen savers for kids and access systems for the disabled.

Veritel Corp.’s VoiceCrypt 2.01 focuses on file security based on one’s unique voiceprint. It guarantees that only the owner can run applications encrypted with his or her personal voiceprint. Each time one accesses the VoiceCrypt program or its protected documents, the program requests a name and an answer to one of five questions asked during the enrollment process. One can also access files by typing the answer to four personal questions or by assigning a one-time password during installation for access to the program from the command line.

Keystrokes

Keystroke dynamics is a technique that monitors a user's fluctuating typing speed patterns. It identifies people by their unique typing rhythm, i.e. the length of time they spend pressing keys and moving their fingers around the keyboard. People move their fingers in precise, yet irregular, timing patterns during log-ins without realizing it. Even when somebody knows another's password and listens to that person enter it, one cannot imitate the keystroke speed fluctuations precisely.

NetNanny Software International Inc., makers of Internet filtering software for families, claims to eliminate the need for passwords with its BioPassword system. It is based on patented algorithms originally developed at Stanford University between 1979 and 1984 and works by measuring the timing between keystrokes.

Keystroke dynamics have not yet found their way into commercial use, primarily due to legal questions. The issues involve personal privacy and whether a company might use such techniques to monitor the hourly progress of its employees.

Signatures

Digitizing tablets can also be used as biometric devices for authenticating network users. Signature technology has a large advantage over most other behavioral biometrics because a signature is traditionally used in authorizing legal documents, bank transactions, personal file access, and so forth; but it can also be subject to a person's physical or emotional state.

Cyber Sign Inc. (San Jose, CA) has users of its Enterprise 2.0 product sign their names three times on an electromagnetic digitizing tablet to match a stored version of their signature and prove their identities. Cyber Sign supports a wide range of digitizing devices and captures the entire event of signing rather than simply comparing bitmapped images of signatures. It looks at each signature from several perspectives: the X and Y coordinates of each consecutive point; the pressure of the pen on the tablet for each stroke; the speed of the strokes; and even the off-tablet, or "air space", motion of the pen. This makes forgery virtually impossible because a user can build secrets into their signature using motions that are not visually represented. Signature technologies are also available from Wacom Technology Corp. (PenPartner tablet), PenOp Inc., and Communication Intelligence Corp. These devices focus more on document security rather than network log-ins.

Applications

Biometric devices have a bright future. Proponents foresee their use in ATMs, access control door security, computer security, and time clocks. Optimists foresee passports, drivers' licenses, mortgage loan applications, health records, safety deposit boxes, credit card transactions, e-commerce, drug, distribution, lottery tickets, and prisons as other application areas.

Biometric technologies are relatively inexpensive, requiring little or no new hardware and require nothing more than commonplace actions. This makes them attractive, especially in situations where remote users must be supported. However, more universal implementation at the desktop or workstation level will require prices to drop even further. It may require prices to drop to the $5-$10 range before consumers and employers adopt this technology. Even such low costs represent a sizeable expenditure for large companies. Cost becomes an even more important issue when one does not rely on a single security device but couples two different techniques for greater reliability.

BioAPI

To accelerate adoption of biometric technologies, the BioAPI Consortium was founded to develop a multi-level biometric API (application programming interface). The draft specification of the API specifies a set of high level programming interfaces that would allow application programmers and biometrics service providers to develop applications in a consistent manner, regardless of the platform or devices utilized. Founding members and promoters of the Consortium include Compaq, IBM, Identicator, I/O Software, Microsoft, Miros, and Novell.

Stephen Heil, the Consortium's secretary, says that the multi-level BioAPI architecture accommodates a broad range of biometric technologies, including face, fingerprint, hand, iris, and voice. It is designed to meet the diverse needs of security administrators, systems integrators, value-added resellers and application developers, as well as end users. Further details of the specification can be found on the Consortium's Web site[3].

The ideal biometric would be easy to use, fast, nonintrusive, convenient and socially acceptable. Most biometric technologies are computationally intensive; and some users see biometrics as an invasion of privacy. Biometric techniques involve trade-offs among several factors, such as accuracy, ease of use, cost, and user acceptance. While security experts may cringe at the thought of passwords, the losses from potential security breaches are usually lower than

the price of biometrics, considering the purchase price, configuration cost, and inconvenience factor.

In addition to controlling physical access to a network or to personal and confidential files, a secure extranet could defend a server without controlling the communications to and from it. To accomplish this, a firewall which isolates the internal network from the outside world could protect the server and explicitly allow specific protocol exchanges between customers and e-commerce services for example. An e-commerce server is very complex; but a firewall is relatively less so. Protecting complex systems with simpler ones makes sense and can improve reliability and reduce downtime.

Biometric devices are probably overkill for most library applications. However, they may become important tools to gain access to institutional computers. IT managers may adopt them to protect access to sensitive information, such as personnel records, salary and medical information, and academic or disciplinary records. Researchers may want to have biometric devices installed to block unauthorized access to research findings, dissertation work, or research conducted under government or foundation grants.

Librarians, among others, may be more interested in protecting the privacy of their electronic communications or in protecting the integrity of the content of the resources they provide. Library catalogs and electronic resources are exposed to increasing risks of tampering by the general public. Moreover, librarians are licensing more and more electronic materials. As license (i.e. contract) administrators, they may be held accountable for the use of those materials and be liable for contract infringements. Encryption technologies could preserve the privacy of electronic communications and transactions.

Further refinements of encryption technologies are finding their way into more and more business applications in the form of a public key infrastructure (see below). These tools aim to protect the privacy and integrity of electronic communications and transactions. They may find their way into library applications as publishers, aggregators, and electronic information providers attempt to restrict access only to authorized subscribers or licensees. Instead of having to manage a range of IP addresses or a list of valid user names and passwords for a variety of products or publishers, license administrators may find themselves managing a list of public keys.

Secure content

While efforts are being made to authenticate individuals and to secure access to systems, other efforts focus on protecting the contents of electronic transmissions. A secure transaction would achieve three goals:

1. (1) to let two parties share data without risk of a third party intercepting and reading it;

2. (2) letting the receiver of a message detect whether someone has tampered with it in transit; and
3. (3) making sure both parties know they are communicating with each other and not an impostor.

The use of a value-added network with dedicated lines is one way to insure a secure transaction; but it is an expensive option which may be used with only one or two major business partners. Encryption offers another more economical option. Today's Web browsers usually include encryption and decryption capabilities. Many versions offer only 40-bit encryption while others offer 128-bit or greater encryption for added security. Encryption or cryptography is emerging from the cloak and dagger arena to become an increasingly popular tool to achieve some privacy in an increasingly public world.

Cryptography encrypts and stores information in a form that appears "scrambled" to all but authorized viewers. A software application called an encryption engine scrambles the original message, known as plaintext. The engine usually applies mathematical data (called a key) to the plaintext and creates a scrambled message, called ciphertext. The encryption process could be as simple as substituting numbers for letters, such as A = 1, B = 2, C = 3, and so on.

Modern encryption techniques generally use complex mathematical algorithms generated by computers to scramble plaintext. Theoretically, these computer-generated algorithms can only be broken by a concerted effort involving supercomputers over a long period of time. However, no encryption has proven absolutely secure. At best, we can just rely on practical security.

After encrypting a message, one needs to provide the key to the recipient to be able to unscramble the ciphertext. Getting the key to the intended recipient can pose a problem. Ideally, one would physically hand over the key; but that isn't practical in most cases, especially for commercial transactions like Internet shopping or international communications between people who have never met. To compound the problem, each transaction would require a new key to ensure that people who had a key from a previous message could not read subsequent messages intended for other parties.

Private-key or public-key

There are two broad categories of encryption algorithms – private-key (symmetric cryptography) and public-key (asymmetric cryptography). In private-key encryption, users accomplish both encryption and decryption with the same key. Whitfield Diffie and Martin Hellman invented a relatively new form of encryption in 1976 to eliminate that problem. Instead of using the same key to encrypt and decrypt a message, as in most encryption, this method, called public key encryption, splits the key into two parts: a public key

(widely distributed and available in public directories) and a private key (held as private, like an ATM PIN code). While there are other forms of encryption available, privacy advocates favor public key encryption as does a group of self-proclaimed “crypto-anarchists” who call themselves cypherpunks.

The sender uses the recipient’s public key to scramble the message to assure that only the key’s owner can read that message. A public key is an encryption code generated and stored in a key database and included with a digital signature when signing an outgoing message. Whoever receives and stores a public key can encrypt and send information to its owner.

The recipient then uses his or her private key to decrypt and display the message’s contents. A private key is a decryption code generated when one receives a certificate from a certificate issuer (signing authority). The communicating parties never have to meet or worry that they can read other messages encrypted with a public key. One can only “lock” a message he or she sends, not “unlock” it. Because messages encrypted using a public key can only be decrypted by the recipient’s private key, this creates what’s called a “digital signature” that can be used to verify the authenticity of digital exchanges. Public-key cryptography algorithms can take 1,000 times as long as private-key algorithms to encrypt or decrypt data. Public-key cryptography also requires keys up to ten times as long as those for private-key cryptography to provide an equal level of security.

Most digital commerce done over the Internet relies on encryption if it relies on any security greater than SMTP. Encryption tools haven’t been very intuitive and need to become more transparent to users to make cryptography easy to use. Standards organizations, like the Internet Engineering Task Force (IETF), that control Internet protocols are trying hard to get encryption technology built into the network operating system itself because public key encryption involves a number of components within a network, including servers and directories.

Public key infrastructure

One effort, labeled “public key infrastructure” (PKI) has been used for electronic commerce applications. Some companies, particularly larger ones, now want to use it to protect their networks to ensure that only authorized users get on the network and to provide secure e-mail capabilities for end users. Public key infrastructure is a catch-all word used to refer to all the things required to implement and use public key technology. Its main component comprises a certificate and key management system; but it also includes the applications that operate in a public key environment

The efforts to implement PKI are moving very slowly because of the cost and complexity as well as the lack of standards. Moreover, law enforcement agencies view strong encryption as a threat to their ability to investigate crimes

and terrorism. They fear that, if encryption becomes too effective and too widespread, it will prevent – or at least curtail – what they consider necessary and appropriate surveillance of terrorists, drug dealers, and other criminals. For that reason, the US government has classified the export of encryption software under the same export restrictions reserved for weapons and munitions unless the software includes a recovery, or escrow, mechanism that would ensure that keys could be accessed in the event of government subpoena or some other legitimate law enforcement reason. However, advocates for personal privacy and business interests point out that the technology is already available internationally. They say that imposing restrictions is simply "closing the barn door after the horses have gone".

While the government's role in key recovery remains controversial, the business arena encounters little debate. An employer does not want to risk losing access to e-mail or network resources if an employee becomes incapacitated in any way or leaves the company.

While we wait for the issues related to PKI and secure encryption to get resolved, only a few commercial products exist for consumer use. A program called PGP, which stands for pretty good privacy[4], first brought public key encryption to the Internet. PGP was created by Phil Zimmerman, based on algorithms created at MIT. Zimmerman released the software over the Internet as what he called "guerrilla freeware". It spread quickly around the world and thwarted US law enforcement efforts to keep the export of encryption technology limited to less robust versions.

A cryptography company called RSA Data Security subsequently gained control of the patents to important algorithms used in public key encryption and was dismayed to find its patented algorithms included in PGP. RSA Data Security has since come to an agreement with Phil Zimmerman and his company, Pretty Good Privacy, which now sells software aimed at consumers who want to use public key encryption on their private e-mail messages.

IBM's Cryptolope

IBM's Cryptolope offered a variation of public key encryption. The technology was designed to protect intellectual property in electronic commerce. It let users wrap documents, programs, and multimedia files in an encrypted software "envelope". The cryptolope also included code to require users to pay to view or execute the cryptolope's contents.

A merchant uses a program, called the Packer, to package the contents. The server technology, called Rights Management and Payment, handles the transactions. Upon payment by credit card or online debit, the consumer receives an electronic key, called the Opener, to unlock and access the contents. The Opener is the only way to view the contents of a cryptolope. The underlying idea is to prevent pirates from gaining access to and copying digital

products while not making it difficult for paying customers. Even if a customer purchases an access key and gives a copy of the cryptolope to a friend, the friend will also have to make payment before he or she can unlock the file.

IBM announced a second version of Cryptolope, called Cryptolope Live, in the third quarter of 1997. This version, written in Java, would allow sharing documents in any electronic format, provide an audit trail, and include a tool kit for wrapping data. It would also include a digital certificate management system called Registry for secure electronic transactions (SET) and eTill, a transaction processing application to add support for the SET 1.0 specification to most commerce servers. However, within three months of the announcement, IBM announced that it would close its Databolts product group and distribute the technologies it developed to Lotus and to IBM's Internet commerce division. That was to include Cryptolope; but Cryptolope Live would be abandoned.

Other related technologies include InterTrust Technologies' DigiBox[5] and NetRights' LicensIt. DigiBox, like the cryptolope, is a secure container for online-content distribution; but it also adds complex, scalable business rules and payment terms. For example, it would let a consumer buy an article and then resell it to a friend at a discount and keep a reseller's percentage. LicensIt targets professional artists and publishers and works much like Cryptolope and DigiBox. However, instead of securing content in a container, LicensIt locks relevant copyright information into content, making compliance easier.

Wave Systems, Inc.'s (Lee, MA) WaveMeter is another competitor. The company originally introduced the WaveNet concept to the public in its electronic commerce Web site, The Great Stuff Network. Another player to watch is the Association of American Publishers[6], which hopes to develop a standard for protecting copyrights in cyberspace. With all these competitors, we cannot expect to see a universal standard adopted any time soon.

Secure transactions

The Internet uses SMTP as the protocol to transmit electronic messages. Besides having as much privacy as a postcard, these transmissions travel over insecure, untrusted lines. Nor does SMTP guarantee delivery of e-mail. Messages may get lost in cyberspace without notification or the knowledge of the sender. Some e-mail programs offer features for notification. There are also utilities that address this problem. We generally rely on security by obscurity, hoping that the sheer volume of traffic will keep our e-mail private. With more and more of our private information – from credit card data and business transactions to love letters – making its way into public places via the Internet and other digital networks, we need a way to secure information.

Secure sockets layer

RSA Data Security, which designs products like BSAfe, BCERT, and TIPEM, provides encryption technology used in software like Netscape Navigator, Microsoft Explorer, and dozens of other products that need to assure private communication over the Internet. Its new BSAFE SSL-J components suite lets developers implement the Secure Sockets Layer (SSL) v3 protocol in Java applications for use in banking, financial services, Web publishing, and consumer and electronic commerce.

Secure Sockets Layer, a protocol originally developed by Netscape is the most widely used security protocol. It has been included in Navigator since the first version and in Internet Explorer since Version 3.0. SSL defines an interface in which a client and a server can perform data encryption, assure message integrity, and validate user authentication.

The Secure Sockets Layer provides a secure channel for confidential electronic transmissions. It allows a client program and a server program to agree on encryption methods; and it supports digital certificate-based authentication for both the client and server (public and private keys). The server sends a digital certificate in unencrypted ASCII to authenticate itself to the client (authentication of the client is optional).

Digital certificates and signatures

A digital certificate is an extension of an individual's public key and works like the individual's ID card. It includes the key as well as information that vouches for the key's authenticity. Because public keys are accessible to just about anyone, a certificate authority (CA), an entity that authorizes and manages digital certificates for a group of users, verifies a user's identity prior to issuing digital certificates. A certificate then says that the person's identity has been confirmed and ensures that a particular public key actually belongs to the person who claims its ownership instead of just blindly accepting it.

A basic certificate contains:

- information about the company operating the server, such as the name the owner gave the signing authority;
- a digital signature unique to the owner;
- a public key to match the owner's private key; and
- a signature from the signing authority that issued the certificate.

The digital-certificate issuer "signs" the certificate by generating a code that gets encrypted with the issuer's private key. This signature essentially means that the issuer has investigated the company operating the server and believes

it to be legitimate. If the client trusts the issuer, then it can trust the server and already knows the issuer's public key. The digital certificate then lets users create digital signatures for their electronic messages and files.

Individuals could set up their own private certification service or use a third-party certificate authority such as RSA Data Security; CertCo, Inc.; Entrust Technologies; or Verisign, Inc. VeriSign announced a non-exclusive agreement with Netscape Communications in February 1999 that will lead to tighter integration of Verisign's OnSite product with Netscape's Certificate Management System, making VeriSign the premier provider of Internet trust services for Netscape's customers. The two companies will also team to build an Internet security Web site; and VeriSign is also working on an insurance policy to protect users of its digital certificates.

Transport layer security

The Internet Engineering Task Force is currently trying to use SSL 3.0 as a basis for a proposed open standard called transport layer security (TLS) which is supported by most major Web server vendors. The protocol derives its name from the IETF working group charged with developing an Internet standard for a secure, authenticated channel between hosts. Version 1.0 of the TLS protocol was presented to the IETF in May 1998. Although based on SSL, TLS is incompatible with SSL 3.0 due to the differences introduced into the protocol. Netscape believes that the IETF will soon make TLS an Internet standard. Although vendors will not be obliged to implement it, there will be a standard for secure transactions to serve as the basis of comparison for other protocols.

Another proposed standard, private communications technology (PCT), requires fewer messages to negotiate a compatible set of protocols. It supports more encryption algorithms and provides additional security by using different keys for authentication and encryption.

Secure electronic transactions

Visa and MasterCard International, Inc. both support the use of SSL encryption until the secure electronic transactions (SET) standard which they co-developed becomes more widely used. SET wouldn't eliminate the need for protocols such as TLS, focusing instead on confidentiality and authentication. SSL provides encryption for transmitting credit card numbers on the Internet. SET goes further, using digital certificates to verify the identities of both the consumer and the merchant.

When consumers are ready to make an online purchase, they'll be informed that they're about to perform a SET. They'll then select, from an on-screen "wallet", the credit card they want to use. The wallet, which resides on the hard drive of the consumer's PC, will have a graphic representation of each type of card. After selection of the type of payment, the order information will go to the merchant; but the credit card data will go to the participating financial institution for verification. The merchants do not receive the actual credit card number but only a credit card authorization. In theory, this increases security by avoiding card numbers sitting on servers connected to the Internet. But, in practice, most major retailers quickly transfer the numbers to a more secure server.

With SSL or other technologies, the merchants must absorb the cost of any fraud. With SET, credit card companies will cover the merchants in cases of consumer fraud just as they do with in-person transactions. However, they are hoping the number of fraudulent transactions will drop, along with their liability, because SET enables them to authenticate the credit card holder. Also, consumers don't have to worry about typing errors or the credit card information falling into the wrong hands. The numbers are kept in that encrypted "wallet" on the hard drive.

While SET offers more security, it is also more complicated, requiring merchants to have special software. Also, each SET purchase requires multiple encrypted transactions; and consumers need digital certificates and special "wallet" software to make a SET purchase. This wallet software has made SET slow to take off. (SSL just requires a credit card number.) Besides finding it annoying to download and install another piece of software, consumers cannot move the wallet and its money from one computer to another. But right now the technology is still in the pilot stage.

Secure sockets layer has made digital-cash vendors unnecessary. Companies like First Virtual, CyberCash (Cybercoin), and DigiCash, in Amsterdam have all but disappeared as has Digital/Compaq's Millicent. These companies aimed at enabling "microtransactions" when merchants required a minimum $10 purchase. All the banks offering online services currently use secure servers and assure their customers that transmitting personal data, like credit card numbers, is much less risky than giving the card to a minimum-wage server in a restaurant and having him or her disappear with it for five or ten minutes.

Bank of America and Lawrence Livermore National Laboratory, in a pilot program to test financial electronic data interchange (EDI), determined that it is viable to transmit sensitive information securely and reliably over the Internet. They found that none of the messages were lost in transit during the pilot. Any problems encountered were due to nonrecurring software and procedural issues, not to any breach of the network or tampering with the messages being transmitted. Any problems with message reliability occurred within the internal systems of the pilot partners and were eventually resolved. Despite delays and problems, information on payment instructions, acknowledgments, and payments remained consistent, suggesting that the Internet has the capability of transmitting crucial data like payment instructions accurately, even with existing security measures.

The Open Financial eXchange (OFX)[7] is also working on developing online financial standards and solutions. Their efforts focus on integrating XML into the client and server. This will enable anybody with a computer and a Web browser to engage in electronic commerce. While OFX is laying the groundwork for the future of electronic commerce, the Financial Services Technology Consortium[8] is creating an electronic commerce messaging format. This format uses XML and intends to make XML the standard for electronic check processing via the Internet.

Whom do you trust?

While credit card companies like Visa and Mastercard have not publicly or actively encouraged consumers to use their credit cards for Internet purchases, they do not perceive the Internet as posing any greater financial risk than "normal" transactions. After all, the most serious risk with credit cards occurs when an employee in some company steals or copies a database of customer records that includes credit card data, not when the numbers are being transmitted over the Internet. Dishonest employees and lax corporate operating procedures usually account for this type of fraud and theft rather than inadequacies of the Internet or other computer technologies. Moreover, all major credit card issuers offer their customers essentially the same liability protection they provide when the cards are lost or stolen.

In fact, Visa, MasterCard, American Express, Discover, and other credit card companies may emerge as the most important enablers of electronic commerce because they fulfill the important role of validating or certifying that the parties in a given transaction are both who they say they are and are good for the economic exchange. These institutions already command a level of trust that they hope to transfer to new purchasing channels like the Internet. The use of a credit card in a purchase means essentially that the card issuer has "preapproved" the merchant as a valid place of business and that the consumer has passed a basic test of credit worthiness (or at least the bank that issued the credit card will stand behind the transaction and guarantee payment to the merchant).

Excite, the builder of a popular search engine and Web site, has a certified merchant program that not only protects consumers for the first $50 not covered by credit card companies in a fraudulent transaction, but will put a red ribbon on merchant sites that meet its encryption and electronic-mail notification requirements. Companies that are able to build trust, whether through the strength of their brand or trusted technology solutions, will have an edge with the consumer.

The American Institute of Certified Public Accountants (AICPA) has also identified the need to build trust for electronic commerce. Seeing an opportunity to capitalize on the need for assurance, the group formed a committee of roughly 20 accountants from the "Big six" and other companies to

establish standard policies and procedures for auditing Web businesses. They launched a fledgling business, CPA WebTrust[9], in mid-1998 to analyze transactional Web sites. They assess how Web businesses authorize users, encrypt information, and store confidential data, such as credit card information, and that buyers get what they paid for. Retailers who satisfy the criteria can post the seal of the AICPA WebTrust on their site. Having a trusted intermediary, such as the AICPA, bless Web sites with a seal of approval should make consumers and businesses feel more comfortable with Internet transactions.

Summary

Network security demands attention at multiple levels. We looked at various physiological and behavioral biometrics for the authentication of individuals. These technologies have broader applications than network security. They can be used to control access to personal computers, private files and information repositories, building access control, and many other applications. While still relatively expensive and immature, these technologies vary in accuracy and reliability. They may be most effective when used in tandem with other security measures.

We then considered attempts to improve the security of the content of electronic transactions. We examined encryption methodologies, particularly public key encryption. We also looked at IBM's cryptolope and related technologies. We then surveyed some techniques to secure the electronic transmission of messages, such as the secure sockets layer and digital certificates. We also covered some of the proposed standards for secure transmissions, such as transport layer security and secure electronic transactions.

Strong encryption is not the answer to every security issue. Buggy software, human error and greed, and poor server administration provide opportunities for unscrupulous hackers. The increasing number of private communications over the Web, particularly business transactions, will require a higher level of security. If a problem occurs with a business transaction or a Web company is accused of bad business practices, it may become very difficult to establish liability. Who should be held accountable – the business, the ISP, the bank, or the trust intermediary? Having an agency like a credit card company or the AICPA vouch for the integrity of the parties may go further than establishing and promoting the infrastructure for Web commerce. This authentication may become an important condition of conducting business electronically.

Notes

1. www. abio.com
2. www.bio metricaccess.com
3. www.bioapi.org
4. www.pgpi.com
5. www.intertrust.com
6. www.publishers.org
7. www.ofx.net
8. www.fstc.org
9. www.cpawebtrust.org

Further reading

Brown, C. (1998), "Self-contained fingerprint IDs forgo PCs, networks", *Electronic Engineering Times*, pp.61.

Dawley, H (1998), "A program that never forgets a face", *Business Week*, pp.81.

(1998), "For your eyes only: biometrics", *The Economist*, Vol. 346 No.8055, pp.80.

Hooman, B. (1998), "Passwords could be past tense by 2002", *Computer Weekly*, .

Karv, A (1997), "Certifying your Internet identity", *LAN Magazine*, .

Karv, A (1997), "Lesson 104: public key cryptography", *LAN Magazine*, .

Karv, A (1997), "Public key infrastructures", *Network Magazine*, pp.69.

Karv, A (1999), "PKI options for next-generation security", *Network Magazine*, pp.30-5.

McCooey, E. (1999), "Security becomes a priority. Compaq, Dell, others adding security hardware to PCs", *Windows Magazine*, .

Neil, S (1999), "Arming the network with digital IDS", *PC Week*, pp.123, 129..

Phillips, K (1998), "Not everybody's HA-API", *PC Week*, Vol. 15 No.5, pp.95.

Phillips, K (1998), "New options in biometric identification", *PC Week*, Vol. 15 No.36, pp.95..

Sullivan, K.B (1999), "Digital certificates grow up", *PC Week*, pp.143.

Surkan, M (1998), "Biometrics: all the way or not at all; implementing new security technologies", *PC Week*, .

Ware, J.P (1998), *The Search for Digital Excellence*, McGraw-Hill, New York, NY,

.

Appendix: biometric information sources

Biometric Consortium www.biometrics.org is the US government's biometrics site. It contains publications, research, databases, events and government activities.

International Biometric Group www.biometricgroup.com contains biometric news and consulting and offers information free or by subscription.

International Computer Security Association www.ncsa.com/ contains information on security and cryptography.