IT Security Trends

Walter Fumy

Siemens AG
ICN EN TNA 4
81737 München
walter.fumy@icn.siemens.de

Abstract This paper examines recent trends in the area of information security. It presents attacks and vulnerabilities of IT systems and networks, addresses the IT security market, and discusses the IT security hype cycle. Concerning technology trends, the paper focuses on two specific fields: cryptography, which is the basis for a large variety of security services, and user authentication, including biometric and token authentication.

1 Introduction

Absolutely secure information technology (IT) products or systems do not exist. IT security basically is an appropriate risk management strategy which identifies, controls, eliminates or minimizes uncertain events that may adversely affect IT system resources and information assets. In practice, levels of information technology security are first established through an understanding of the essential security requirements of consumers and business users. These requirements range from best practice guidelines on how to conduct a security risk assessment and evaluation of IT systems and products to the employment of specific cryptographic techniques and mechanisms. Appropriate levels of security are then achieved by implementing a suitable set of information management policies together with adequate sophisticated assurance methods and cryptographic technologies.

1.1 Attacks and Vulnerabilities

Attacks against IT systems and networks are catching the headlines. The exact vulnerabilities exploited for actual attacks change from one year to the next, as old weaknesses get fixed and new software releases new ones. Typical vulnerabilities include stack overflows and other software bugs, and weak authentication procedures and access controls. Attacks are typically tool-based, and attack tools become more and more sophisticated. Three important trends are the anti-forensic nature, the dynamic behavior, and the modularity of these tools. Also, the level of automation in attack tools continues to increase.

The CERT Coordination Center (www.cert.org) is a major reporting center for Internet security incidents and vulnerabilities. CERT statistics show that electronic crime has risen dramatically. In 1990, only 252 cyber-crime incidents have been reported, in 2000 there were 21.756 incidents, and in the first quarter of 2002 alone, there were 26.829 incidents (cf. table 1). Also, the number of newly discovered vulnerabilities reported to CERT continues to more than double each year, and new classes of vulnerabilities are discovered

each year. This makes it very difficult for administrators to keep up to date with security patches.

Year	1995	1996	1997	1998	1999	2000	2001	Q1/02
Incidents	2.412	2.573	2.134	3.734	9.859	21.756	52.658	26.829
Vulnerabilities	171	345	311	262	417	1.090	2.437	1.065

Table 1: : CERT Statistics 1995 2002

Another important source of information on attacks and vulnerabilities is the ”Computer Crime and Security Survey”, conducted each year in the United States by the Computer Security Institute (CSI) and the FBI. The findings of the latest report [CS02] confirm that the threat from IT security breaches continues to increase and that incidents are widespread and costly.

Highlights from the 2002 CSI/FBI Computer Crime and Security Survey [CS02] include

- 90% of the organizations surveyed detected security breaches within the last 12 months;
- 80% acknowledged monetary losses due to security breaches and reported losses rose by 72% compared to 2000;
- 74% cited their Internet connection as a frequent point of attack (compared to 59% in 2000);
- 33% cited their internal systems as a frequent point of attack (compared to 38% in 2000);
- 78% detected employee abuse of Internet access;
- 85% detected malicious code (e.g., computer viruses).

While internal fraud still accounts for higher losses, there has been a significant rise in losses from external attacks. Reported average losses from viruses alone were $283 million in 2002, up from just $45 million in 1999.

IT security technologies such as firewalls, anti-virus software, intrusion detection systems, strong authentication techniques, or virtual private networks help to significantly reduce vulnerabilities, however, they alone cannot thwart attacks. The security that can be achieved through technical means needs to be supported by appropriate management and procedures.

Issues to be addressed include security policies and plans, a good understanding of the security requirements, risk assessment and risk management, training and education, auditing and monitoring, and support and commitment from management. Information security requires the full organizational commitment of resources – technological, financial, and human.

1.2 IT Security Market

IT security technologies are widely used. For example, 90% of the organizations surveyed in [CS02] use anti-virus software, 89% have firewalls, 60% use intrusion detection systems, 38% have deployed digital IDs, and 10% use biometric authentication.

Market analysts predict that the market for IT security technology and services will continue to grow at a substantial rate. E.g., key findings of the research conducted for Datamonitor's report "Global network security markets to 2005" are [Da01]:

- the global market for network security products will rise at a CAGR[1] of 30% from $5.8bn in 2000 to $21.2bn in 2005;
- the market for security services to back up the purchase of such products will grow at a CAGR of 26% from $4.7bn in 2000 to $15.1bn in 2005;
- the fastest growing sub-markets in the area of network security are content security, Virtual Private Networks (VPNs), and Public-Key Infrastructure (PKI), growing at a CAGR of 66%, 59%, and 46% respectively;
- the traditional sales message of fear and uncertainty will be replaced by positioning IT security products and services as business enablers.

1.3 IT Security and the Technology Hype Cycle

Technologies, no matter how different they are, in general exhibit a certain pattern with respect to visibility (or hype) and time – a period of strong enthusiasm ("peak of inflated expectations") typically is followed by a phase of disillusionment, and gradual improvement of the technology ("slope of enlightenment") finally may lead to its maturity and a "plateau of productivity". This general pattern is called the *technology hype cycle* and has proven to be a very useful tool for technology assessment.

Figure 1 shows an example for an IT security hype cycle [WP01]. Quantum Cryptography and the Advanced Encryption Standard (AES) represent two new security technologies entering the cycle (both technologies will be discussed in section 2), while Single Sign-On (SSO) and Public-Key Infrastructure (PKI) are stuck in the trough of disillusionment and are labeled as unlikely to emerge from this stage quickly. Key technologies "riding the wave" of analyst and media enthusiasm include Biometrics (discussed in section 3), XML Security, and Managed Security Services.

While the Data Encryption Standard (DES) is about to leave the plateau of productivity (cf. section 2.1), Virtual Private Networks (VPNs) are reaching the plateau. A VPN emulates a private network using public networks and can provide permanent interconnection of multiple sites or dynamic dial-in capability. VPNs offer clear cost savings over alternatives such as leased lines and complete industries, such as the automotive industry, have moved to VPNs as the basis of their extranets.

[1] CAGR = compound annual growth rate.

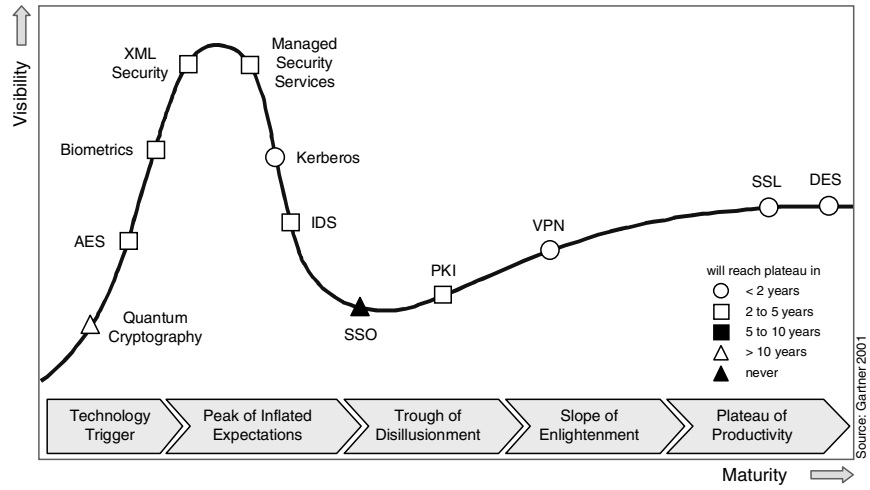

Figure 1: IT Security Hype Cycle

2 Cryptography

Cryptographic mechanisms are one of the most important tools to provide security services for IT applications, communication protocols, and infrastructures. Cryptographic techniques enable a large number of security features including data confidentiality, data integrity, entity authentication, and non-repudiation. The effectiveness of cryptographic protection depends on a variety of issues such as cryptographic key size, mechanism and protocol design, implementation aspects, and password management. All of these issues are equally important: if the key size is too small, or if a mechanism is badly designed or incorrectly implemented, or if a password is poorly protected, then the security of a IT system is at risk. Traditionally, mechanism design and the choice of key sizes get the most attention, however, the majority of successful attacks are not due to inadequate mechanism strengths or key sizes, but to other deficiencies.

In the area of cryptography, many alternative techniques have been proposed, each presenting its own advantages, such as performance, code size, key size, patent coverage, and standardization. Public-key cryptography, in particular, has shown itself to be an extremely valuable tool for the design and implementation of scaleable secure systems. Due to the substantial computational overhead associated with public-key algorithms, security architectures typically utilize symmetric cryptographic mechanisms for bulk encryption and integrity protection, and public-key techniques for key establishment, digital signatures, and non-repudiation services.

Today, cryptography is a well established technology; many specific algorithms and techniques have been (or are being) standardized. Major trends include

– increasing block and key sizes for symmetric ciphers (e.g., from DES to AES, cf. section 2.1),

- increasing sizes of hash codes (e.g., from SHA-1 [IS98] to SHA-256, SHA-384, SHA-512 [NI01a]),
- improvements in integer factorization and parallel processing, such that the future may demand unpleasantly large moduli for schemes like RSA or DSA (thus from RSA to elliptic curve based schemes, cf. section 2.2), and
- randomized digital signatures, and signature schemes allowing for message recovery [IS00] [IS02b].

The following sections discuss selected aspects in the area – symmetric ciphers, digital signature algorithms, equivalent algorithm strengths, and applications of quantum computers to cryptography.

2.1 Symmetric Ciphers

The Data Encryption Standard (DES), initially issued as Federal Information Processing Standard (FIPS) in 1977 [NI77], has been a worldwide standard for more than 20 years. The standard was most recently reaffirmed by NIST in 1993, until December 1998. DES is a block cipher algorithm that converts plaintext blocks of 64 bits into ciphertext blocks and vice versa using a 56-bit key, which means there are 2^{56} or approximately 7.2 x 10^{16} possible DES keys. Despite many years of research, no method has been published that breaks a DES encrypted message substantially faster than exhaustive key search, i.e., by systematically trying all different keys.

For a symmetric cipher, exhaustive key search is purely exponential in the size of the key; its time complexity can be expressed as

$$T_{(k)} = 2^{k-1}$$

where k denotes the bit-size of the cipher's key. Note that increasing k by 1 doubles the cost of attack. The expected number of trials needed to recover a DES key therefore is 2^{55}.

Ever since DES was first published, it has been criticized for its short key size. Today it is widely agreed that 56-bit keys offer only marginal protection against a committed adversary. Several studies have been performed showing that it is feasible to build a specialized machine that could crack DES-keys by exhaustive search in relatively short time. In 1999, a worldwide computing team utilized a network of nearly 100.000 PCs on the Internet and a specially designed supercomputer, the Electronic Frontier Foundation's (EFF) "Deep Crack," to win RSA Data Security's third DES Challenge. The project analyzed a DES-encrypted message in 22 hours and 15 minutes (cf. table 2).

Over the past 20 years, researchers have proposed a number of potential replacements for DES. E.g., the financial services industry has developed a standard for triple-DES encryption [AN98a]. In triple-DES, each message block is encrypted with three successive DES operations rather than one, a construction which involves two or three different keys. In typical applications, triple-DES offers an effective key size of 112 bits (cf. table 3).

Since 1997, NIST has been working with industry and the cryptographic community to develop a long-term successor for the DES. The outcome of this process is the Advanced

Encryption Standard (AES), published by NIST in 2001 as FIPS 197 [NI01b]. The AES specifies the Rijndael algorithm [DR00], a symmetric block cipher that can process data blocks of 128 bits, using keys with lengths of 128, 192, or 256 bits, and referred to as "AES-128", "AES-192", and "AES-256", respectively. Rijndael originally was designed to handle additional block sizes and key lengths, however they have not been adopted in the AES standard.

In decimal terms, the AES key sizes result in 3.4×10^{38} possible 128-bit keys, 6.2×10^{57} possible 192-bit keys, and 1.1×10^{77} possible 256-bit keys. Thus, there are more than 10^{20} times more AES-128 keys than DES keys. Assuming that one could build a machine that could recover a DES key in a second (i.e., try 2^{55} keys per second), then it would take that machine approximately 149 trillion years to crack a 128-bit AES key. [2]

2.2 Digital Signature Algorithms

Digital signature algorithms are based on public-key cryptography and are mainly used to provide entity authentication, data integrity and non-repudiation. Digital signatures typically are employed in conjunction with hash functions and may be computed on data of arbitrary length.

Today, three families of public-key cryptosystems are established in the marketplace:

- Integer Factorization (IF) systems are based on the computational difficulty to factor large integers. Prominent examples for IF systems include the RSA digital signature scheme [RSA78], and the Rabin-Williams scheme.
- Discrete Logarithm (DL) systems are based on the computational difficulty to solve the discrete logarithm problem over a finite field GF(p) or GF(2m) [El85]. Examples include NIST's Digital Signature Algorithm (DSA) [NI00], and Nyberg-Rueppel signatures [NR93].
- Elliptic Curve (EC) systems are based on the computational difficulty to solve the discrete logarithm problem over an elliptic curve. EC primitives are analogous to DL primitives; examples include the EC-DSA scheme and the EC-NR scheme [IS02a]. The primary advantage of elliptic curve cryptosystems is their cryptographic strength relative to the required parameter size, i.e., elliptic curves offer more security per bit (cf. table 3).

The fastest known general-purpose algorithm for either factoring large integers or for solving the ordinary DL problem for large prime fields is the so-called Number Field Sieve (NFS), invented in 1988 by John Pollard. The original version of NFS could only be used to factor numbers of a special form and therefore is referred to as Special Number Field Sieve (SNFS). The generalized version called General Number Field Sieve (GNFS or just NFS) can handle numbers of arbitrary form. Its run time depends only on the size of the number being factored, or the size of the underlying field for the discrete logarithm problem.

On heuristic grounds, NFS can be expected to require computing time proportional to

[2] The universe is believed to be less than 20 billion years old.

$$\mathrm{L}[n] = \mathrm{e}^{(1.9229+\mathrm{o}(1))*\ln(n)^{1/3}*\ln(\ln(n))^{2/3}}$$

to factor an RSA modulus n, where the o(1) term goes to zero as n goes to infinity. The amount of time it takes to factor a k-bit number is asymptotically the same as the time it takes to solve a discrete logarithm problem over a field of size k bits. However, in practice solving DL problems has been more difficult than factoring numbers of equivalent size.

The largest published factorization using the NFS is that of the 512-bit number "RSA155" which is an RSA modulus of 155 decimal digits, in August 1999. This factoring effort took less than 10^4 MIPS years and corresponds to about $3*10^{17}$ operations (cf. table 2). Note that the effort needed to factor a 1024-bit RSA modulus requires about 7 million times this effort.

Daniel Bernstein recently observed that the total cost of breaking an RSA key (i.e. the product of the amount of hardware needed and the running time) might not be as great as previously thought, at least for very large key sizes [Be01]. In particular, Bernstein suggests methods for reducing the amount of memory required to break very large RSA keys. Basically these methods are clever implementation techniques for the NFS, however, the basic number of operations required by the NFS is not reduced [Le02].

The best known attack against an Elliptic Curve system is based upon a collision attack and the birthday paradox. One expects that after computing approximately sqrt(order of the curve) points, that one can find two points that are equivalent under an algebraic relationship. From this collision, the key then can be constructed. Thus, this attack is purely exponential in the key size. Its time complexity is

$$T_{(k)} = \sqrt{\frac{\pi}{2}} * 2^{\frac{k}{2}}$$

where k is the bit size of the order of the base point. Note that increasing k by 2 doubles the cost of attack.

The largest published solution for an EC challenge is that of a 108-bit system, in April 2000. The amount of work required to solve this challenge was about 50 times the effort required to solve the 512-bit RSA cryptosystem. Solving a 160-bit Elliptic Curve challenge is estimated to require more than 60 million times the work spend to solve the 108-bit challenge.

Table 2 summarizes the state of the art concerning successful published attacks on the DES, on the RSA scheme, and on Elliptic Curve cryptosystems.

2.3 Equivalent Algorithm Strengths

Cryptographic algorithms provide different levels of security, depending on the algorithm and the key size used. In this paper, two algorithms are considered to be of equivalent strength for the given key sizes if the amount of time needed to "break the algorithms" is the same.[3]

[3] Note that other metrics for algorithm equivalence exist.

Challenge	Year	Effort (time)	Effort (machines)
ECC-108	2000	400k MIPS years (4 months)	9.500
ECC-97	1999	16k MIPS years	740
RSA-512	1999	8k MIPS years (5 months)	300
DES	1999	25k MIPS years (22 hours)	100.000

Table 2: Demonstrated Attacks – State of the Art

Table 3 summarizes equivalence guidelines for symmetric ciphers, hash functions, and digital signature algorithms. The reader should be aware that the equivalent algorithm strengths stated in table 3 are based on assessments made as of today and may need revision due to future developments.

To estimate how the computing power available to attackers may change over time, typically Moore's law is used. Moore's law states that the density of components per integrated circuit doubles every 18 months, which is interpreted that the computing power per chip doubles every 18 months.[4]

Symmetric Cipher	Hash Function	RSA Scheme	Elliptic Curve
56 (DES)	112	512	112
80 (SKIPJACK)	160 (RIPEMD-160)	1.024	160
112 (Triple-DES)	224	2.048	244
128 (AES-128)	256 (SHA-256)	3.072	256
192 (AES-192)	384 (SHA-384)	7.680	384
256 (AES-256)	512 (SHA-512)	15.360	512

Table 3: Commensurate Security Levels

Based on Moore's law and the steady growth of the Internet, it is safe to assume that the computing power available for attacks doubles every 12 months, which can be interpreted as a steady loss of cryptographic strength. Under this assumption, the following conclusions hold:

– Symmetric ciphers "lose" 1 bit of security per year;

[4] There is some skepticism as to whether this law will hold much longer because new technologies will eventually have to be developed to keep up with it.

- Hash functions and Elliptic Curve based schemes "lose" 2 bits of security per year; and
- RSA schemes "lose" about 20 to 30 bits of security per year.

In addition, unanticipated advances in breaking algorithms may occur.

2.4 Quantum Cryptanalysis and Quantum Cryptography

Quantum computing is a relatively new field that has developed with the increased understanding of quantum mechanics. It promises computing devices that are exponentially faster than conventional computers, at least for certain problems. The story of quantum computing started in the 1980's with the publication of a theoretical paper that first described a universal quantum computer [De85].

In a classical computer, a bit has a discrete range and can represent either a zero or a one – consequently a register composed of L physical bits can be in one out of 2^L possible states. In a quantum computer, a quantum register composed of L quantum bits (or *qubits*) can store in a given moment of time all 2^L numbers in a quantum superposition, i.e. at once. Because of superposition, a quantum computer can in one computational step perform the same operation on 2^L different numbers encoded in L qubits. In order to accomplish the same task, a classical computer has to repeat the same computation 2^L times or has to employ 2^L processors working in parallel. Therefore, quantum computers promise to offer an enormous gain in the use of the computational resources time and memory.

Several of the unique features of quantum computers have applications to cryptography. In 1994, Peter Shor published a quantum algorithm that, in principle, can very efficiently factor large integers or compute discrete logarithms [Sh94]. Shor's algorithm runs in polynomial-time. Another quantum algorithm published by Lov Grover achieves searching an unsorted list of N items in only about sqrt(N) steps [Gr96]. An important application of this algorithm is the cryptanalysis of symmetric ciphers, such as the DES or the AES. Grover's algorithm can be used for speeding up exhaustive key search – however, its running time is still exponential.

How a quantum computer could be built is known in principle. However, as the number of quantum logic gates in a network increases, one quickly runs into serious practical problems. One main reason is a phenomenon called quantum decoherence, which is due to the influence of the outside environment on a quantum computer. Therefore, the development of practical quantum computers still remains an open question. In the event that a sufficiently large quantum computer can be built, public-key cryptography may have to be abandoned, and for symmetric cryptosystems key sizes may have to be doubled.

On the other hand, quantum mechanics can be utilized for the establishment of shared secrets over an insecure channel. This technology is referred to as *quantum cryptography* [Be92] [Br93]. Photons have a polarization, which can be measured in any basis consisting of two orthogonal directions. If a photon's polarization is read twice in the same basis, the polarization will be read correctly and will remain unchanged. If it is read in two different bases, in the second basis a random result will be obtained and the polarization will be

changed randomly. Based on this observation, several quantum key establishment protocols have been designed. These protocols enjoy the property that their security is based on the fundamental laws of quantum mechanics, rather than on computational assumptions.

3 User Authentication

Authentication assures one party of the identity of a second party and that the second party was involved at the time the evidence was created. Several alternative authentication techniques have been proposed, which require different capabilities of the entity being authenticated. For authentication mechanisms based on cryptographic techniques, these include the ability to store a cryptographic key and the ability to perform cryptographic operations with acceptable speed and accuracy. Unfortunately, human beings have neither of these two capabilities.

For user authentication there are three basic techniques:

- Something you know (e.g., password, PIN);
- Something you have (e.g., physical key, smart card, USB token); and
- Something you are (e.g., fingerprint, voice characteristics).

For reasons of cost, most systems authenticate their users based on user IDs and passwords. However, user IDs and passwords are cumbersome – most people find passwords hard to remember[5], and managing passwords has turned out to be a serious challenge. Also, as people get accounts on more and more systems and for more and more applications, they reuse passwords in ways that may expose vulnerabilities.

3.1 Biometric Authentication

The term biometrics applies to a wide range of techniques that employ the physical or behavioral characteristics of human beings as a means of authentication ("something you are"). A large variety of biometric techniques have been proposed for use with IT systems. These include fingerprint readers, iris scanners, retina scanners, face imaging devices, hand geometry readers, keystroke analysis, and voice recognition.

Advantages of biometric authentication include that biometric characteristics are almost impossible to lose or forget, and that biometric authentication eliminates the management of forgotten and expiring passwords. Usage of biometric authentication techniques is often recommended in conjunction with other user authentication methods, rather than as a single, exclusive method.

Since no two biometric templates are exactly alike, verifying a template is not a simple yes/no outcome. Thus, biometric systems can decide incorrectly. The trial template might be matched incorrectly against another person's reference template, or the trial template might not be matched even though the user is enrolled. The accuracy of biometric authentication is measured by the false acceptance rate (FAR) and the false rejection rate (FRR).

[5] According to several studies, forgotten passwords account for 25-50% of all calls to IT help desks.

The lower the FAR, the better is the security. The lower the FRR, the easier the system is to use (see figure 2).

In the following, three attractive biometric authentication technologies are discussed in more detail: finger-scan, iris-scan, and voice-scan.

Finger-scan technology is the most prominent biometric authentication technology today. Applications include physical access, computer and network access, and public services. Finger-scan is considered a relatively accurate biometric authentication technology, however, more accurate technologies exist (cf. figure 3). Its acceptance rate among users is very high, although the technology still bears a slight stigma from the use of fingerprinting for criminal investigations.

The human fingerprint is comprised of various types of ridge patterns. The discontinuities that interrupt the flow of ridges are called minutiae and form the basis for most finger-scan authentication solutions. Many types of minutiae exist, including ridge endings, bifurcations (points at which a ridge divides), dots (very small ridges), islands (ridges between two temporarily divergent ridges), and ponds (empty spaces between two temporarily divergent ridges).

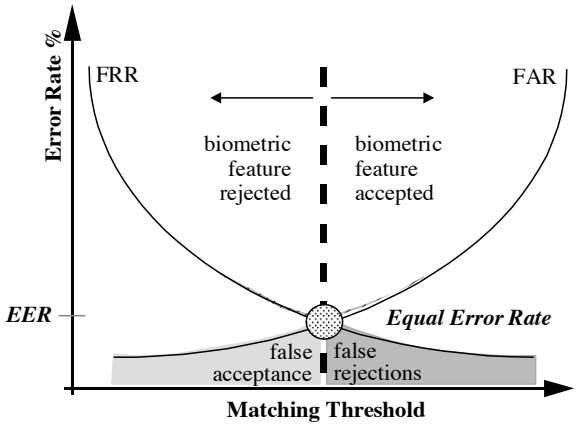

Figure 2: Accuracy of Biometric Authentication

Finger-scan biometrics does not store full finger images but only particular data about the fingerprint in a template typically requiring about 500 bytes. Therefore, the fingerprint itself cannot be reconstructed from the finger-scan template. The technologies in use today to capture the fingerprint image are optical, silicon, and ultrasound.

- Optical technology is the most widely used. The finger is placed on a platen and typically a charged coupled device (CCD) converts the image of the fingerprint into a digital signal.
- Silicon technology was introduced in the late 1990's and is mostly based on DC capacitance. The silicon sensor acts as one plate of a capacitor, the finger as the other

one. The capacitance distribution between the platen and the finger is then converted into a digital image. Silicon sensors are small enough to be integrated into a variety of devices, including smart cards and USB tokens.

– Ultrasound technology is the most accurate finger-scan technology. It transmits acoustic waves and measures the distance based on the impedance of the finger, the platen, and air. Ultrasound is capable of penetrating dirt and residue, countering a main problem of the other sensor technologies.

Iris-scan technology leverages the unique features of the human iris to provide user authentication. The visible patterns of a human iris contain a large amount of randomness. The iris is formed between the third and eighth month of gestation; the mechanisms forming it appear to be chaotic. The iris patterns are phenotypic – the two eyes of a person are different, as are the irises of identical twins.

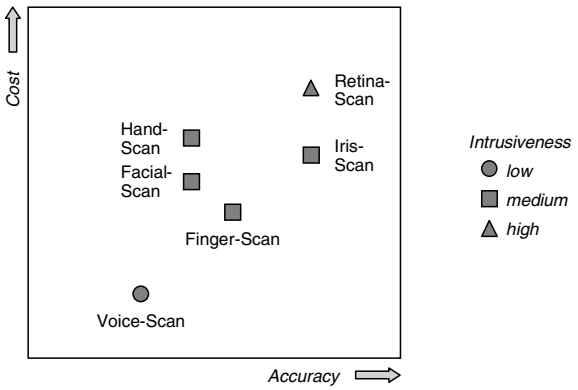

Figure 3: Strengths and Weaknesses of Some Biometrics

A primary visible characteristic of the iris is the colored ring of tissue that surrounds the pupil and appears to divide the iris in a radial fashion. Other characteristics include rings, furrows, freckles, and the corona. A specific signal processing technique extracts these characteristics and converts them into a template of typically 512 bytes.

The iris is relatively small; getting a high quality iris picture without being too intrusive is the main practical problem with iris-scan technology. Typically, the iris is located by a dedicated camera within a distance of at most 3 feet from the eye. The algorithms used in iris recognition appear to be extremely accurate (cf. figure 3).

Voice-scan technology, also known as voice or speaker verification, is a biometric authentication technology often deployed in environments where the voice is already captured, such as telephony and call centers. Speaker verification utilizes the distinctive qualities of a person's voice. Some of these characteristics are behaviorally determined, some are physiologically determined. Voice-scan appears to be less accurate than other biometric authentication technologies; on the other hand, deployment costs are relatively low and the acceptance rate among users is very high (cf. figure 3).

Figure 3 illustrates comparative strengths and weaknesses of some biometric technologies. It compares the characteristics deployment cost, accuracy, and intrusiveness (i.e., how intrusive the users perceive an authentication technology to be).

Despite the obvious benefits of biometric authentication, the technology has so far been limited to a relatively small number of applications. User acceptance – a combination of ease of use and invasiveness – is seen as one of the key stumbling blocks to mass acceptance.

3.2 Token authentication

An authentication token is a physical device that a user carries around and uses for authentication ("something you have"). Examples for tokens in use today include physical keys, badge IDs, chip cards, and USB tokens. Since tokens can be lost or stolen, they typically are supplemented with at least a second authentication factor – in general a PIN or a password.

Tokens with an embedded CPU and memory are suitable for authentication mechanisms based on cryptographic techniques. These typically have the capability to securely store cryptographic keys and to perform cryptographic operations with acceptable speed. Additional benefits may include that cryptographic keying material can be generated on board and thus secret keys never have to leave the secure environment of the token.

Thus cryptographic tokens can enhance PKI technology – smart cards or USB tokens can provide secure computing platforms and secure storage for public key certificates and private keys. Combined with biometrics, the device protecting the private key can authenticate the user using biometric data to activate the private key for signature generation.

Potential issues with authentication tokens include denial of service attacks based on failed authentication attempt lock-out mechanisms. These mechanisms may be used by malicious code to lock a token.

4 Conclusion

Technology development never stands still. Attacks and attack tools will continue to advance, as will security technologies and security controls. In the area of IT security, technology development tends to be not linear, but to go in leaps. Also, disruptive technological innovation may occur, e.g., due to unanticipated advances in hardware design and algorithms, or in quantum computing.

IT security markets will continue to show above average growth rates. New laws and regulations will impose information security requirements, and often all enterprises in a particular industry (e.g., healthcare) must comply with these regulations. In addition, insurance companies are expected to establish baseline security standards (e.g., ISO 17799, BSI-Grundschutz-Zertifikat) for any policies that include IT liability.

As experts agree, the major challenge for enterprises and the public sector today is not the security technology itself, but how to establish appropriate procedures, management,

and controls for achieving IT security. Human beings – this is a fact, not a trend – will continue to be less reliable and less easy to predict than security technologies. Training and education, as well as support and commitment from top management will continue to be key issues.

References

[AN01] American National Standards Institute: ANSI X9.84 Biometric Information Management and Security, 2001.

[AN98a] American National Standards Institute: ANSI X9.52 Triple Data Encryption Algorithm Modes of Operation, 1998.

[AN98b] American National Standards Institute: ANSI X9.62 Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 1998.

[Be01] Bernstein, D.J.. Circuits for Integer Factorization: A Proposal. Manuscript, November 2001 (available at http://cr.yp.to/papers.html#nfscircuit).

[Be92] C. Bennett, F. Bessette, G. Brassard, L. Savail, and J. Smolin, Experimental quantum cryptography, Journal of Cryptology (1) 5 (1992), 3-28.

[Br93] G. Brassard, Cryptography column - Quantum cryptography: A bibliography, Sigact News (3) 24 (1993), 16-20.

[CS02] Computer Security Institute: CSI/FBI 2002 Computer Crime and Security Survey, 2002.

[Da01] Datamonitor: Global network security markets to 2005, Reference Code DMTC0730, 2001.

[De85] Deutsch, D.: Quantum Theory, the Church-Turing Principle, and the Universal Quantum Computer, Proceedings of the Royal Society of London, Series A, Vol. 400 (1985), 97-117.

[DH76] Diffie, W.; Hellman, M.E.: New Directions in Cryptography, IEEE Transactions on Information Theory, 22 (1976), 644654.

[DR00] Daemen, J.; Rijmen, V.: The Block Cipher Rijndael. In: J.-J. Quisquater and B. Schneier, eds: Smart Card Research and Applications, LNCS 1820, Berlin: Springer (2000), 288-296.

[El85] ElGamal, T.: A Public-Key Cryptosystem and a Signature Scheme based on Discrete Logarithms, IEEE Trans. on Information Theory 31, No. 4 (1985), 469472.

[Gr96] Grover, L.K.: A Fast Quantum Mechanical Algorithm for Database Search, Proceedings of the 28^{th} Annual ACM Symposium on the Theory of Computing (1996), 212219.

[IS00] International Organization for Standardization: ISO/IEC 9796-3 Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms, 2000.

[IS02a] International Organization for Standardization: ISO/IEC 15946-2 Cryptographic techniques based on elliptic curves Part 2: Digital signatures, 2002.

[IS02b] International Organization for Standardization: ISO/IEC 9796-2 Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms, 2002.

[IS98] International Organization for Standardization: ISO/IEC 10118-3 Hash-functions Part 3: Dedicated hash-functions, 1998.

[Le02] Lenstra, A.; Shamir, A.; Tomlinson, J.; and Tromer, E.: Analysis of Bernstein's Factorization Circuit (available at http://www.cryptosavvy.com)

[LV02] Lenstra, A.; Verheul, E.: Selecting Cryptographic Key Sizes, Journal of Cryptology 14 (2001), 255-293.

[NI00] National Institute of Standards and Technology: FIPS 186-2 Digital Signature Standard (DSS), 2000.

[NI01a] National Institute of Standards and Technology: Draft FIPS 180-2 Secure Hash Standard (SHS), 2001.

[NI01b] National Institute of Standards and Technology: FIPS 197 Advanced Encryption Standard (AES), 2001.

[NI77] National Institute of Standards and Technology: FIPS 46 – Data Encryption Standard (DES), 1977.

[NR93] Nyberg, K.; Rueppel, R.A.: A new Signature Scheme based on the DSA Giving Message Recovery, 1st ACM Conference on Computer and Communications Security, Fairfax, VA, November 1993.

[RSA78] Rivest, R.L.; Shamir, A.; Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM 21 (1978), 120126.

[Sh94] Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring, Proceedings of the 35th Annual IEEE Symposium on the Foundations of Computer Science (1994), 124-134.

[WP01] Wheatman, V.; Pescatore, J.: The Information Security Hype Cycle, Gartner Note DF-14-8426, November 2001.