A PIN is usually a four-digit number, which is usually composed using the decimal numerals 0 through 9. The reason for using a purely numeric entry is simply that all card terminals have only numeric keypads. The PIN is entered using the terminal keypad or a computer keyboard and then sent to the Smart Card. This compares the value that it has received with an internally stored reference value and reports the result to the terminal.

PIN entry is considered to be a security issue, especially for financial transactions, and consequently requirements relating the nature of the keypad are frequently found in this application area. Special keypads that satisfy these requirements are often called 'PIN pads'. In Germany, for example, the PIN for a Eurocheque card may only be entered using a keypad that has special mechanical and cryptographic protection. PIN pads have all the features of a security module, such as opening sensors and foils to protect against drilling, and they encrypt the PIN directly as it is entered. This provides reliable protection against tampering with a keypad in order to allow a PIN to be intercepted while it is being entered.

A distinction can be made between static and changeable PINs. A static pin cannot be changed by the user, so it effectively must be memorized by the user. If it becomes known, the user should destroy the card and obtain a new one with a different fixed PIN. A changeable PIN can be altered according to the wishes of the user, or changed to a number that the user finds easy to remember. There is a danger in this, since the numbers that many people find easy to remember are ones such as "1234", "4711" and "0815". The Smart Card does not check for the use of such trivial numbers, since there is not enough memory available to store the necessary table. It would however be perfectly conceivable for the terminal to prohibit the PIN from being changed to such a number. In order to change the PIN, it is always necessary to enter the PIN, since otherwise an attacker could replace every existing PIN with one of his own.

The situation is different with 'super PINs', or PUKs (personal unblocking keys). These usually have more digits than the actual PIN (a typical value is 6), and they are used to reset the retry counter of a PIN to zero if it has reached its maximum value. A new PIN is also entered into the card when the PUK is entered, since resetting the retry counter is of little help if the user has forgotten the PIN. This is usually the case when the retry counter has reached its maximum value.

Some applications also use transport PINs. The Smart Card is personalized with a random PIN, and the cardholder receives the PIN value by letter. The first time that the card is used, however, the user is forced to replace the PIN used for personalization of the card with one of his or her choice. In a similar procedure, called the 'null PIN' procedure, the card is preloaded with a trivial PIN, such as "0000", and the user is again forced to change the PIN the first time the card is used. Both of these procedures avoid the possibility that a PIN that has been 'spied out' when the card is personalized can later be put to good use.

According to a recommendation of the ISO 9564-1 standard, the PIN should consist of four to twelve alphanumeric characters, in order to minimize the probability of determining the correct PIN by pure trial and error. However, actual practice is often somewhat different. The entry of non-numeric characters is technically impossible at many locations, since only a numeric keypad is available.

The number of characters in a PIN depends not only on the desired level of security, but also very much on the memory of the average card user. For years, people have been accustomed to using four-digit PINs, which means that changing over to PINs with six or more digits would be very difficult. In practice, the presumed increase in security provided by a six-digit or eight-digit PIN may turn out to be purely theoretical. Many people find it

difficult to remember numbers of this length, especially if they do not use them very often, and consequently write them down on the card or on a slip of paper kept near the card. The level of security with a long PIN is then significantly lower than with a short PIN.

The perfectly well-founded insistence on periodically changing PINs meets with a similar fate. It may work in the case of a high-security application with only a few users, but it is fatal for the acceptance of a mass-market application, which aims for the simplest possible procedures in order to accommodate people with poor memories.

In this regard, there is another very important issue. In many cases, the entry and verification of a PIN does not just identify the user and demonstrate the legitimate possession of the card in question. Instead, at the same time it also represents a statement of intent by the user, who by entering the PIN declares his or her agreement to a certain transaction. A good example is entering a PIN into a cash dispenser. On the one hand, this identifies the card user by means of his of her knowledge of the secret PIN, but on the other hand it also represents a declaration by the user that he or she agrees to have a certain amount of cash paid out from his or her account. This is a very important point in connection with certain biometric features, some of which do not necessarily represent a declaration of intent since they can be tested without the explicit permission of the person involved.

The probability of guessing a PIN

The simplest attack on a PIN, aside from watching it being entered, is just guessing. The probability of success depends in part on the length of the PIN to be guessed, the characters from which it can be composed and how many attempts are allowed. The probability of correctly guessing a four-digit PIN in three tries is 0.03%, which is not particularly high. Two basic formulas for guessing passwords are presented here. They can be used in actual practice to estimate the risk associated with using a particular password.

$$x = m^n \tag{8.1}$$

$$P = i / m^n \tag{8.2}$$

Table 8.1 Definitions and descriptions of the variables in Formulas (8.1) and (8.2)

Variable	Example	Description
i	3	number of guesses
m	10	number of possible characters per position
n	4	number of positions
P	0.0003 (0.03 %)	probability of guessing the password
x	10,000	number of possible passwords

Incidentally, there is yet a fourth factor relating to guessing a PIN, which for a long time has been inexcusably neglected. This is the evenness of the distribution of the PINs within an application. It is namely much easier to guess a PIN if you know that certain PINs are more common than others. The actual significance of this important secondary factor became evident almost overnight in 1977 with regard to German Eurocheque cards. Although the detailed procedure for computing a PIN from the data stored in the magnetic

Exhibit 1017
Page 045 of 102

stripe of the Eurocheque card is still secret, at least a few general steps of the procedure became known. From this information, it could be concluded that the PINs that are generated are not evenly distributed, since the algorithm used produces the numerals 0 through 5 significantly more often than 6 through 9. It also became known that the PIN algorithm suppressed a leading zero during PIN generation. The result of this non-uniform distribution is that it is not necessary to make 3333 attempts in order to correctly guess a four-digit PIN with the permitted number of incorrect guesses (3), but only 150 [Karten 97]. With 10.5% of the cards, the distribution is so poor that only 72 attempts will suffice if the characteristics of the PIN generation algorithm are taken into account [Schindler 97]. The end result of all this is that an improved PIN generation algorithm is used with new Eurocheque cards, and the DES algorithm originally used has been replaced by a triple-DES algorithm.

Table 8.2 PINs and passwords with various lengths and codings, and the number of possible combinations

Type of PIN or password	Range of values or coding of the PIN or password	Number of possible PINs or passwords
1-digit PIN	PIN ∈ {0 ... 9}	10
1-character password	password ∈ {0 ... 9, "A" ... "Z"}	36
1-character password	password ∈ {0 ... 9, "a" ... "z", "A" ... "Z"}	62
1-character password	password ∈ {0 ... 9, "a" ... "z", "A" ... "Z", 20 arbitrary special characters }	82
4-digit PIN, no leading zero	PIN ∈ {1000 ... 9999}	9.00×10^3
4-digit PIN	PIN ∈ {0000 ... 9999}	1.00×10^4
4-character password	password ∈ {0 ... 9, "A" ... "Z"}	1.68×10^6
4-character password	password ∈ {0 ... 9, "a" ... "z", "A" ... "Z"}	1.48×10^7
4-character password	password ∈ {0 ... 9, "a" ... "z", "A" ... "Z", 20 arbitrary special characters}	4.52×10^7
5-digit PIN, no leading zero	PIN ∈ {10000 ... 99999}	8.9×10^4
5-digit PIN	PIN ∈ {00000 ... 99999}	1.00×10^5
6-digit PIN, no leading zero	PIN ∈ {100000 ... 999999}	8.99×10^5
6-digit PIN	PIN ∈ {000000 ... 999999}	1.00×10^6
6-character password	password ∈ {0 ... 9, "A" ... "Z"}	2.18×10^9
6-character password	password ∈ {0 ... 9, "a" ... "z", "A" ... "Z"}	5.68×10^{10}
6-character password	password ∈ {0 ... 9, "a" ... "z", "A" ... "Z", 20 arbitrary special characters}	3.04×10^{11}

Generating a PIN

In order to generate a PIN for a Smart Card, you need a random number generator and an algorithm that converts the random number into an ASCII-coded PIN of the necessary length. You could then use a table of known trivial combinations to recognize and discard PINs with these codes. Finally, you have to store the PIN in the Smart Card and then use the VERIFY command as necessary to compare it to a PIN that has been entered.

If magnetic-stripe cards are used in a system instead of Smart Cards, generating a PIN is somewhat more complicated. This is because it must be possible for a cash dispenser operating offline to test an entered PIN, based on data located on the magnetic stripe. Smart Cards are not actually affected by this requirement, but all debit cards (such as Eurocheque cards) presently have magnetic stripes for reasons of compatibility, even if they also have microcontrollers. The PIN generation algorithm must therefore be deterministic for hybrid cards with both a chip and a magnetic stripe, which means that it must always produce the same result for a given set of input values. A random number generator would not do this.

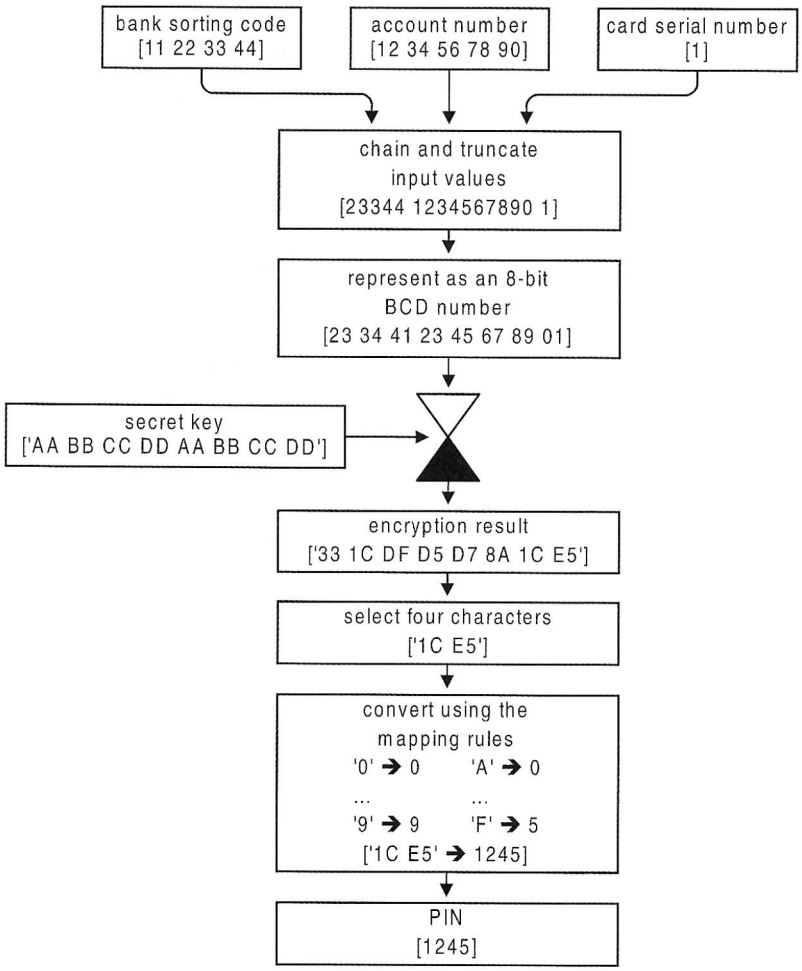


Figure 8.2 Example of generating a four-digit PIN using the DES algorithm and three card-specific data elements (bank routing code, account number and card serial number). The illustrated procedure has the disadvantage that it produces PINs that are not evenly distributed (i.e., some PINs occur more often than others), due to the mapping rule used. Example values are shown inside square brackets. This procedure is remotely similar to the procedure used for German Eurocheque cards and is based on two articles in *Die Datenschleuder* [Müller-Maguhn 97a, Müller-Maguhn 97b].

Exhibit 1017
Page 047 of 102

A procedure is thus needed that can generate a PIN based on the magnetic stripe data. In order to avoid having the security of the system depend on the procedure itself, a secret key should also be involved in the computation. Figure 8.2 illustrates an algorithm similar to the one that is used for German Eurocheque cards. Its inputs consist of the bank routing code, the account number and the serial number of the card. This algorithm uses the DES with a secret key to generate a four-digit PIN. This procedure suffers from the previously mentioned disadvantage that the generated PINs are not evenly distributed over the total possible number space ("0000" to "9999" in the case of a four-digit PIN). This is due to the mapping rule that is used to convert the hexadecimal numbers ('A', 'B', 'C', 'D', 'E', and 'F') into decimal numbers following the encryption process. This undesirable feature could however be easily avoided by using a better mapping rule. The DES is used in part because the key rather than the procedure must be kept secret, and in part due to its properties of confusion and diffusion.[1]

Testing the genuineness of a terminal

As is well known, the identity of a user is verified by the entry of a PIN. However, the user might equally well wish to be able to verify the genuineness of a terminal. For example, consider the possibility of a dummy cash dispenser. Someone with fraudulent intentions could use such a machine to collect PINs entered by unsuspecting users. If the person who set up the machine then stole the cards, he or she could use the PINs acquired using the dummy cash dispenser to withdraw money from the cardholders' accounts. This is all possible because there is no way for the user to test the genuineness of the terminal.

There is, nevertheless, a procedure that can be used to defend against this type of attack. This involves storing a password in a file in the card. This password is known only to the card user and can be changed only by the user. The Smart Card operating system allows read accesses to this file only after the terminal has been authenticated by the card. A name or a number chosen by the user can be used for this password.[2]

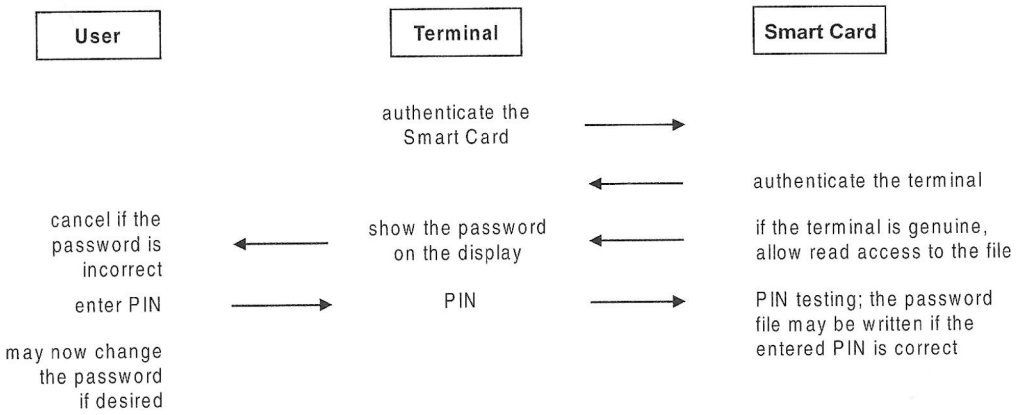


Figure 8.3 A procedure for ensuring that a PIN can only be entered using a genuine terminal. A prerequisite is that the cardholder does not enter the PIN until the password has appears on the terminal display.

1 See also Section 4.10, 'Authentication'.

2 The design of a suitable Smart Card application is described in detail in Section 14.7.3, 'Testing the genuineness of a terminal'.

The first thing that happens after the user has inserted a Smart Card into the terminal is a mutual authentication process between the card and the terminal. If this is successful, then each party knows that its opposite number is genuine. The card then allows a read access to the file containing the user's secret password, which is then displayed on the terminal. The user sees his or her password, and thus knows that the terminal is genuine, since the terminal would have otherwise had no access to the file containing the password. He or she can now safely enter the PIN.

This procedure can also be used as a simple means of preventing PINs from being entered into terminals that have been tampered with. Any arbitrary word or number can be used for the password. It should be possible for the cardholder to change the password as desired, to prevent potential attackers from being able to ferret it out. This procedure can also be extended or modified as necessary to meet other demands of a similar nature.

8.1.2 Biometric methods

The steadily increasing use of passwords and PINs is producing a rising level of user resistance to this type of identification. No one has any particular difficulty with remembering a few frequently used combinations of numbers or letters. However, normal people find it difficult to remember a PIN that is used only rarely, if for example the card is used only every couple of months to obtain money from a cash dispenser. The unconscious fear that the machine will confiscate the card if the PIN is entered incorrectly three times in a row only makes matters worse.

This is certainly one of the main reasons why biometric methods are finding increasing favor in many areas. They are not necessarily faster or more secure than PIN entry, but they can make things much easier for the user. If the level of security provided by biometric methods is equivalent to that provided by PIN codes, system operators will be also prepared to use them. After all, biometric features cannot be transferred to another person as easily as a PIN. This means that the actual person is identified, rather than a secret that is shared by the user and the system operator.

8.1.2.1 Basic considerations

A biometric identification procedure is one that can unambiguously identify a person by means of unique, individual biological features. In this regard, a distinction can be made between physiological and behavioral features. If the features tested by the procedure are directly related to the person's body and are fully independent of conscious behavior patterns, they are referred to as physiological biometric features. Behavior-based biometric procedures, by contrast, utilize certain features that can be consciously changed within certain limits, but that are still characteristic of a particular person.

An essential aspect of biometric feature testing is the question of user acceptance. The more similar a procedure is to existing, well-known procedures, the more willing users will be to accept and use it. One typical example is the handwritten signature, which has been used for generations in almost all cultures for identification and indicating agreement or consent. Social aspects also play an important role. In many countries, fingerprinting is primarily used by the police and security forces. This could adversely affect the acceptance of biometric methods based on fingerprints.

Another point to bear in mind is concerns that users may have regarding medical and hygienic aspects. For example, they may be concerned about acquiring a disease from the

Exhibit 1017
Page 049 of 102

optical scanning of the retina, or be worried that the laser light will damage their eyes. Even though such fears may be fully subjective and lack any scientific basis, they can still strongly affect the behavior of the users and above all their acceptance of the procedure. Before any biometric identification method is put into use, such aspects should be fully understood.

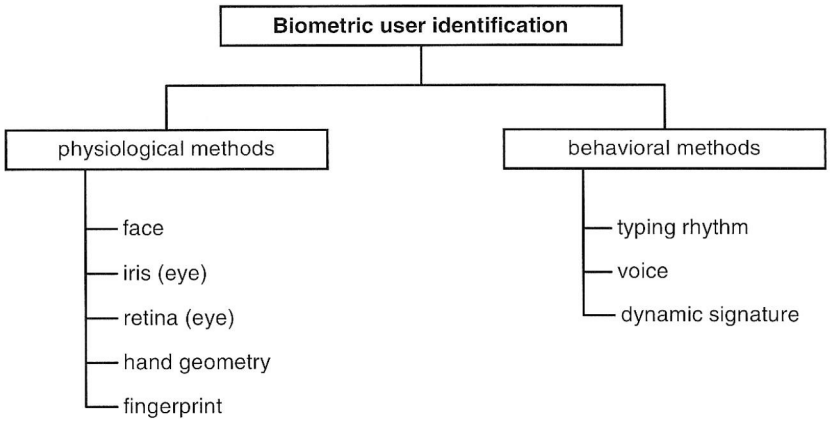


Figure 8.4 Classification of the most important biometric methods for user identification

There is yet another difference between biometric and knowledge-based identification methods, which can be considered either an advantage or a disadvantage, depending on one's point of view. This is that biological features cannot be transferred to another person. With systems that use biometric methods for identification, this means for example that it is not possible to give your card and your PIN to a trusted person who can then use the card in the intended manner. System operators naturally find such an action absolutely shocking, since revealing your PIN is forbidden in almost all systems. However, practically everyone knows how loosely such restrictions are observed in actual practice.

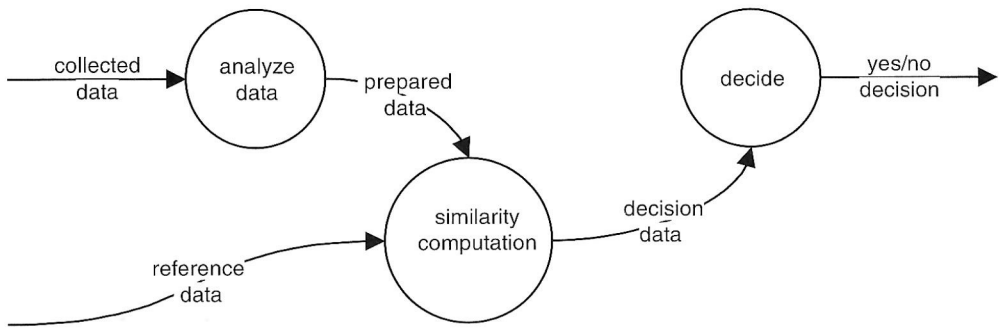


Figure 8.5 Basic data flow for the computational evaluation of a biometric feature

Entering a PIN does not just check whether the user knows a secret code; it is also a legally binding equivalent of saying, 'I consent'. This relationship is very important if some other method is to be used in place of a PIN. A test based on a retinal scan performed at a

distance of three meters, which is anyway presently not technically possible, could certainly not be considered to indicate the agreement of the individual in question to any sort of action. In almost all countries, only an intentional manual action of the user can be interpreted as an indication of consent. For instance, breaking the seal of a cardboard box containing software is an unambiguous indication that the user agrees with the printed license conditions. Biometric methods in which the testing of the person is fully passive must therefore be augmented by appropriate user instructions together with something that provides the element of consent.

Naturally, not all biological features are suitable for personal identification. A feature must satisfy at least the following criteria before it can be reasonably used:

- it can be measured effectively (in terms of the measuring method, time and costs),
- it must be capable of being uniquely associated with a particular individual,
- it must not be possible to alter the feature with fraudulent intent,
- the amount of reference data generated must be small (at most a few hundred bytes),
- natural changes to the feature over time must be so small that a satisfactory measurement is always possible,
- the measurement method and the feature must be acceptable to users.

The result of any measurement is not always the same, but varies from instance to instance. This effect occurs even with the simplest measurements. For example, if you measure the length of a sheet of paper several times, each result will be slightly different. There are many reasons for this, but it does not actually cause any difficulties, since the average value of the measurements will be close to the true value.

Experience shows that the amount of variation between individual measurements depends on the difficulty of the measurement process. For instance, there is a significant technical difference between determining the weight of a bar of chocolate and determining the distance between the earth and the moon. Measurements of human beings are always difficult, and are subject to a wide range of variation.

Figure 8.6 shows an example of the results of measuring a biological feature, such as the length of a finger. The range of variation in the measurement is marked on the horizontal axis, while the vertical axis indicates the probability of correct identification based on the measured biometric feature. With an ideal biometric feature and an ideal measurement method, there would be no variation, and the curve would be reduced to a vertical line. However, a real feature together with a real method produces the illustrated Gaussian bell curve. If the measurement result deviates from the reference value, it is not possible to be absolutely sure that the person to be identified has been correctly recognized.

Before a biological feature can be tested, the feature of the person in question must first be acquired. This can be achieved by making repeated measurements and computing the average value. The result is a reference value that is then stored in the Smart Card. Following this, the Smart Card can, as necessary, test whether an actual measurement value that is sent to it matches the reference pattern. Depending on the biometric method used, however, it may be necessary to use a powerful computer to process the actual measurement value into a form that the card can use for comparison. Since identification cannot be established with absolute certainty, a threshold level is needed in order to decide whether the person should be recognized as genuine. This threshold level must be set separately for each method and application.

Exhibit 1017
Page 051 of 102

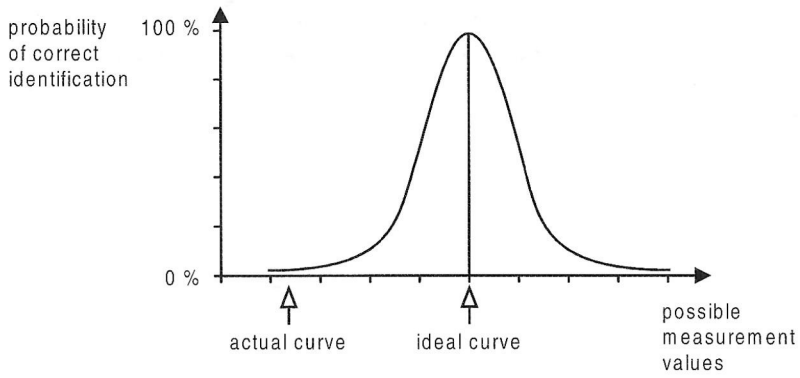


Figure 8.6 Probability distribution for repeated measurements of a biometric feature of a person

If we take our probability distribution diagram and add a curve for a second person to it, we obtain the diagram shown in Figure 8.7. The additional curve represents an arbitrary individual, whose measurement curve is close enough to that of the first individual for it to affect the identity decision. Since both curves approach the horizontal axis asymptotically, they have an intersection point. At this point, the probability that the person being tested is genuine is the same as the probability that he or she is not genuine. Biometric identification systems therefore use an adjustable threshold level, which indicates the probability above which the identity is assumed to be correct. The threshold level marked in Figure 8.7 divides the two curves into four regions. These indicate the decision to be taken regarding the identity of the person, based on the biometric feature.

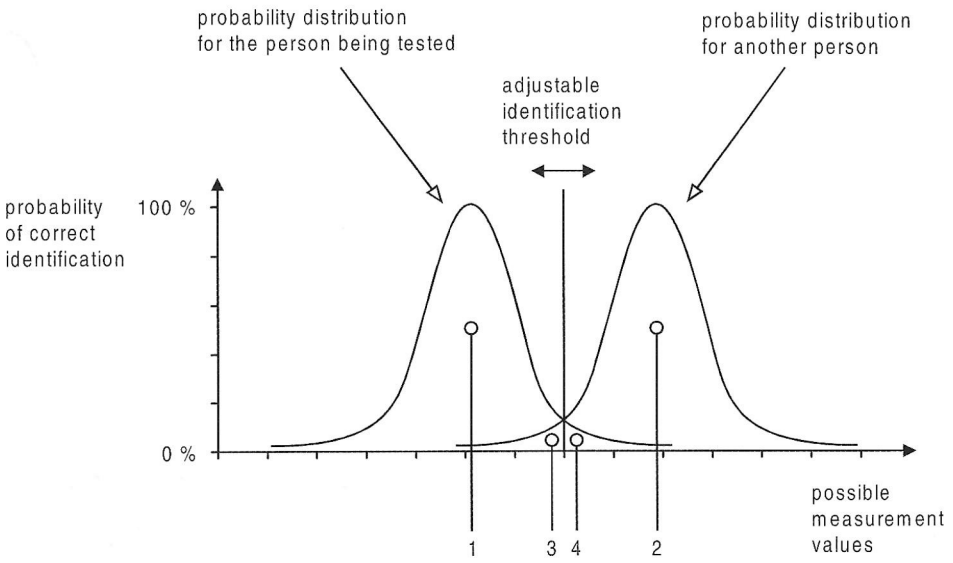


Figure 8.7 Probability distribution and decision regions for a biometric feature measurement:
1 – true positive identification (true acceptance) 3 – false positive identification (false acceptance)
2 – true negative identification (true rejection) 4 – false negative identification (false rejection)

Essentially, this diagram demonstrates that there is no such thing as an absolutely positive identification. It is only possible to assume, with a high degree of probability, that this is the right person. The level of this probability can be adjusted with the threshold value. However, in practice the threshold value cannot be set arbitrarily high, since a strict criterion for correct identification produces a large number of false rejections.

The two basic values for judging a biometric method are its false acceptance rate (FAR) and its false rejection rate (FRR). The FAR is the probability of the incorrect acceptance of the wrong person, while the FRR is the probability of the incorrect rejection of the genuine person. These two probabilities can naturally not be freely chosen, since they are properties of the biometric method that is used and can be adjusted only to a limited degree, within certain boundaries. In addition, these two values are mutually dependent, in that a low FRR produces a high FAR and vice versa.

For the user, a high FRR means that he or she may be rejected in spite of presenting a legitimate feature, which naturally affects the acceptance of the system. The system operator wants to have not only a low FRR but also a low FAR, in order to avoid false identifications.

PIN checking does not require any complicated algorithms in the Smart Card, since it involves only the comparison of the input and stored PIN values. Unfortunately, things are not this easy with biometric features. The reference value is of course stored in the card, but comparison with the measurement in question normally cannot be carried out in the card. This is due to large amount of computing power needed to evaluate biometric features. Since Smart Cards usually do not have adequate processing power for this, the computationally demanding preprocessing of the measurement values is performed externally. The result is sent to the card, which uses special algorithms that do not required a lot of memory or processing power to further evaluate the preprocessed data and then makes a yes/no decision, based on the stored reference value.

8.1.2.2 Physiological features

Additional biometric features could easily be added to the list of features described below. However, we have limited our discussion to the most important and most commonly used features in order to avoid getting lost in details.

Some physiological features that cannot be consciously altered also do not change much over time. For example, the characteristic patterns of fingerprints never change during a person's lifetime, nor do the patterns of the retinal blood vessels. The face is certainly an exception, since even though it basically does not change, it can be transformed to a large degree by a different haircut, growing or shaving a beard, and the like. Basically, though, it is possible to say that biometric features based on adult physiology do not require ongoing adjustment of the reference pattern, since any changes are negligibly small or non-existent.

Facial features Based on everyday experience, we can assume that the human face is suitable for use as a biometric feature. Transforming this assumption into a technical implementation is however fraught with difficulty. Faces can change greatly within a short period, and their appearance depends strongly on external factors such as eyeglasses, beards, make-up, illumination and viewing angle.

If you photograph a face using visible light and suitably process the data captured by the photograph, you will often be able to make a judgement about the identity of the person behind the face. The technical toolkit for this process includes very powerful computers, fuzzy logic and neural networks, which indicate the amount of effort that it entails. In

Exhibit 1017
Page 053 of 102

addition, the stored image should be three-dimensional, or else the person should be photographed from several different angles, to prevent the system from being deceived by holding a photograph in front of its sensor. In general, this feature may prove to be a very interesting subject for future biometric methods, but presently it cannot yield a high enough probability of accurate identification to allow it to be widely used.

Retinal features Every human retina has its own unique pattern of blood vessels, with their branches and junctions. This pattern can be captured using a beam of infrared beam directed through the pupil. The light reflected by the retina is collected by a CCD camera, which in turn sends the recorded image data to a computer for analysis.

Retinal imaging is one of the very best biometric methods, since it can be used to uniquely identify a person with a very high degree of probability. However, it is not readily accepted by users, since they must place their eyes very close to the scanner in order to be identified. This often results in a fear of infection and anxiety with regard to the infrared beam. Another problem is that certain types of contact lenses strongly block light in the infrared region, which causes the measurement to fail.

Iris features The iris is a variable diaphragm that limits the amount of light that reaches the retina. Like the retina, it is a biological feature that is unique to each individual. An iris scan can be performed at a greater distance than a retinal scan, since the measurement procedure is simpler. With this method, the iris (which is located at the front of the eye) is imaged by a CCD camera using visible light. The data evaluation is similar to that used for retinal images. Here again, contact lenses can strongly influence the measurement results and thus cause problems.

Hand geometry Identification systems based on three-dimensional measurements of the hand, or parts or the hand, were already in use in the 1970s. These measurements can for example be based on finger length, finger diameter and fingertip radius. Unique individual features can be determined using very few measurement points (e.g. five). The actual measurements can be made very simply using infrared LEDs and photodiodes. The hand geometry can be determined by noting which photodiodes are fully or partially blocked by the hand. Since only a few measurements are needed for identification, the procedure is sufficiently fast and uncomplicated for the user. He or she only has to place his or her hand in an instrument, which then performs the measurements.

Fingerprints The best-known biometric identification method based on a physiological feature is without doubt fingerprinting. In the electronic version, it is naturally no longer necessary to press fingers coated with black ink onto paper. The thumb or another fingertip is placed against a transparent plate, and a camera mounted under the plate scans the skin surface without any contact. The comparison with the reference pattern is usually based on the classification scheme developed by Edward Richard Henry,[3] which marks features as arches, loops and whorls. Information about the type, position and orientation of 20 or so of these features is stored, and this information is used to generate the reference pattern.

Certain groups of users dislike this method because of the well-known fact that fingerprints have been used for years as a tool for combating crime. Small wounds on the

[3] Fingerprints were first used for identifying persons by the Bengal police in India around the end of the 19th century, under the leadership of Sir Edward Richard Henry. After returning to London, Edward Henry set up the first British fingerprint collection in 1901, and generated a classification method for fingerprint features that is still in use.

fingertips can also make unambiguous identification difficult. Many systems have sensors for measuring the temperature of the finger or the pulse rate, in addition to the optical scanner. This is designed to prevent an amputated finger from being used for identification purposes.

Despite all these problems, fingerprint systems are widely used, since they are technically relatively simple and have relatively few problems with user acceptance. The time needed to sense the fingerprint and perform the subsequent test also lies within reasonable limits. Optical and capacitive sensors based on semiconductor technology are primarily used at present. They have a resolution of around 400 dpi.

Table 8.3 Comparison of biometric methods based on physiological features

Method	Test duration (seconds)	Amount of reference data (bytes)	Probability of false rejection (FRR), percent	Probability of false acceptance (FAR), percent
Facial image	—	—	≈ 10	≈ 1
Retinal image	1.5–7	40–80	0.005	10^{-9}
Hand geometry	1–2	10–30	0.8	0.8
Fingerprint	1.5–9	300– 800	0.014	10^{-6}

8.1.2.3 Behavioral features

With many persons, biometric features based on behavior are not stable over time. Consider a signature, which can change considerably during the course of a person's life. However, it is rare for these changes to occur suddenly; instead, they are usually quite gradual and slow. Many systems therefore use adaptive procedures, which accept any changes in the feature that are detected during a correct identification as a new reference pattern that is then stored in the Smart Card.

Table 8.4 Comparison of biometric procedures based on behavioral features

Method	Test duration (seconds)	Amount of reference data (bytes)	Probability of false rejection (FRR)	Probability of false acceptance (FAR)
Voice	5	100–1000	1 %	1 %
Dynamic signature	2–4	40–000	1 %	0.5 %

Typing rhythm It has been determined that there are large differences in the manners in which different individuals type characters on a keyboard. These primarily relate to the pauses between individual letters. This can naturally be used as a biometric feature for identification. The procedure works by having the person to be identified type a prescribed character string (which is different for each test) on the keyboard. The computer to which the keyboard is attached evaluates the typing rhythm as the character string is typed. A text chosen by the user can also be used to evaluate the typing rhythm, but this requires more characters to be typed than with a prescribed text.

Exhibit 1017
Page 055 of 102

The great advantage of this method is that it does not need any additional hardware, since in most cases a keyboard and computer are already available. Unfortunately, between 100 and 150 alphanumeric characters are needed for the test, and they must be typed using the ten-finger system. This is the main disadvantage of this method.

Vocal features Like the face, a person's voice is characteristic of the person, so it can also be used for identification purposes. The person to be identified speaks one or more sentences into a microphone. These must be different for each session, since otherwise the system could be attacked very easily by playing back a previous identification session, which for example may have been recorded on magnetic tape. The waveforms of the spoken text are subjected to a Fourier analysis, which yields the characteristic frequency spectrum of the speaker. This is then compared with a reference value to determine whether the speaker's identity is genuine. The entire palette of modern computational wizardry, such as fuzzy logic, neural networks and the like, is also employed with this method.

Of course, this method also has its shortcomings. A person's voice is very strongly influenced by his or her current bodily condition. Furthermore, all background noises must be reliably filtered out to make an unambiguous spectral analysis possible in the first place. A different sentence must be spoken for each test to prevent recorded speech from being played back, which very much complicates the procedure and makes recognition more difficult. These technical difficulties are however offset by good user acceptance, which makes this a very attractive biometric identification method.

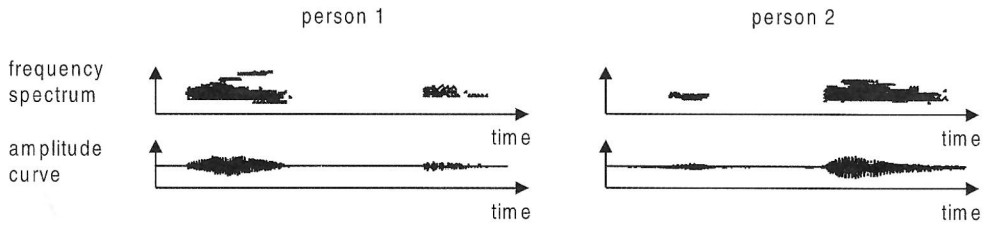


Figure 8.8 Amplitude waveform and time-dependent frequency spectrum of the name 'Wolfgang', spoken by two different people

Dynamic signatures The only identification method that is commonly used in everyday life is writing a signature. Due to its very individual character, a signature can also be used as a biometric feature. With a static method, the signature is evaluated after it has been written. In a dynamic method, however, measurements are made while the signature is being written. The static method is only of theoretical interest, since it cannot distinguish a photocopied signature from a genuine one.

The parameters measured in the dynamic method may for example be the general form of the signature, the speed, acceleration and pressure of the pen on the writing surface, and the time required to write the signature. A special pen, or a special pad that can sense the parameters to be measured, can be used to make the measurements. Figure 8.9 shows an example of a possible arrangement in which an ordinary pen is used on a special pad, and Figures 8.10 through 8.13 illustrate examples of measured signals that can be used as the basis for a biometric identification process. Pressure sensors are located at the intersections of the grid wires, and their signal amplitudes are transmitted to the computer via

conditioning logic. The computer can then use various algorithms to process the measured data into a standardized format and compare the results with a stored reference pattern.

Using a dynamic signature for purposes of identification has the highest degree of acceptance of all personal identification methods, since signatures are used daily by everybody in almost the same fashion. However, here the technical solutions are also not simple, since signatures change over time and are never completely the same. You need only consider the difference in your signature if you write it while sitting or standing to appreciate the truth of this.

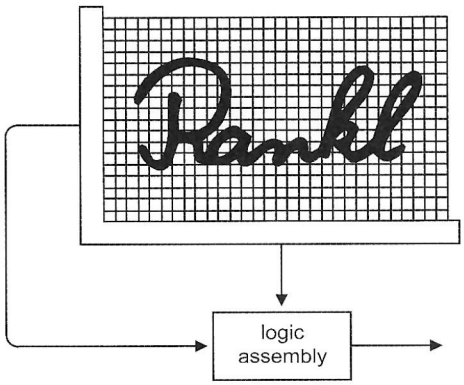


Figure 8.9 Sample measurement setup for testing a dynamically generated signature

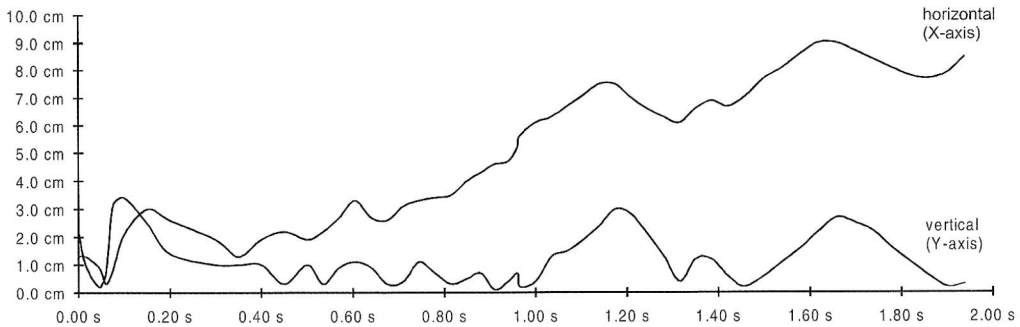


Figure 8.10 Horizontal and vertical pen position as function of time, for writing the word 'Rankl'

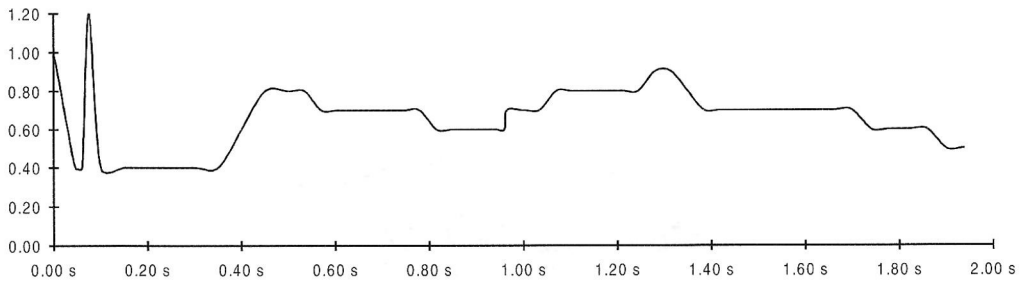


Figure 8.11 Pen pressure as function of time, for writing the word 'Rankl'

Exhibit 1017
Page 057 of 102

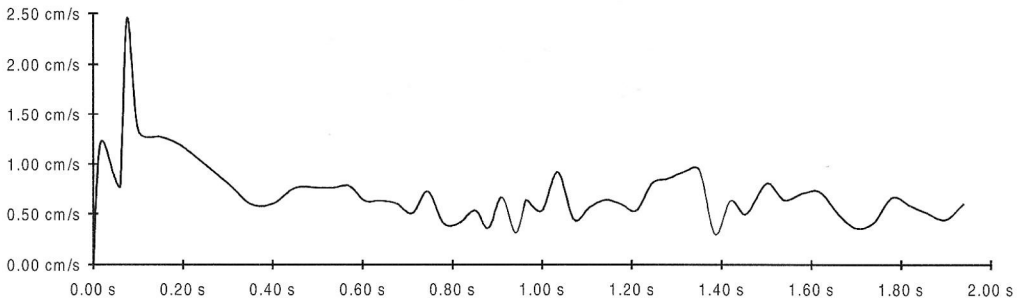


Figure 8.12 Pen speed as function of time, for writing the word 'Rankl'

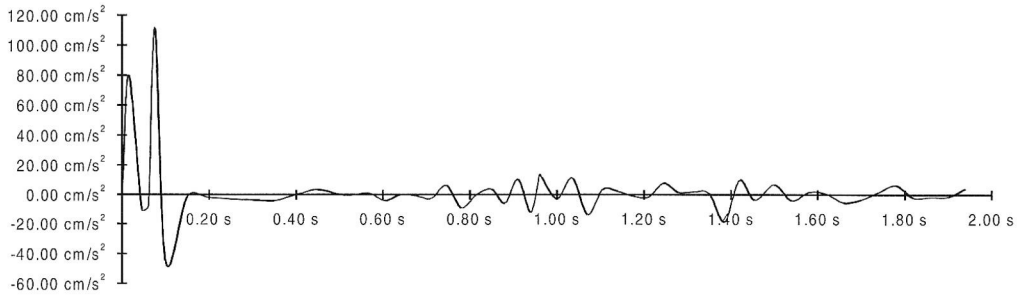


Figure 8.13 Pen acceleration as function of time, for writing the word 'Rankl'

8.2 Smart Card Security

The essential characteristic of a Smart Card is that it provides a secure environment for data and programs. If the amount of effort needed to read data from a Smart Card were not so large, it would essentially be nothing more than a diskette with a different interface.

It is naturally practically impossible to set up a complete system, or even a Smart Card, such that it has perfect security that is proof against everything and everybody. If the effort expended on the attack is raised to a high enough level, it is possible to force your way into any system or tamper with it. However, every potential attacker makes a conscious or unconscious benefit analysis for himself and his targets. The rewards of breaking into a system must be worth the time, money and effort that he must expend to achieve the goal. Regardless of whether the reward is money or prestige within a peer group, if it is not worth the effort, no one will invest all too much energy in breaking a system or a Smart Card.

The security of a Smart Card is guaranteed by four components. The first component is the card body, in which the microcontroller is embedded. Many of the security features that are used for the card body are not only machine-readable, but they can also be visually checked by humans. The techniques that are used for these features are not specific to Smart Cards, but are also used with other types of cards. The remaining components – the chip hardware, the operating system and the application – protect the data and programs in the Smart Card microcontroller.

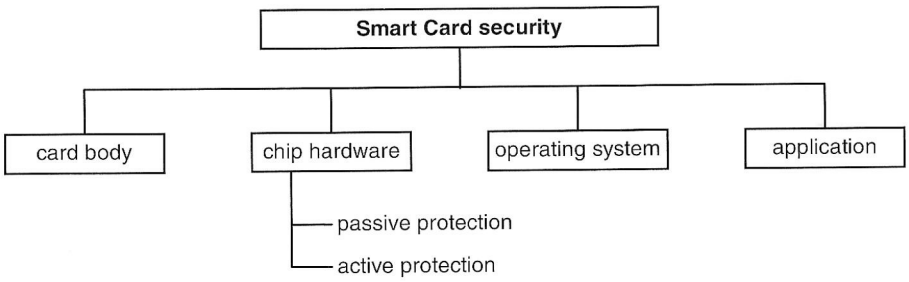


Figure 8.14 Classification of Smart Card security components

The security of a Smart Card is guaranteed only when all of these components are present and their defense mechanisms are working properly. If the card is used exclusively within a realm where it is not subject to human verification, the card body component is not necessary. The three components that are independent of the card body, however, are indispensable for the physical and logical security of a Smart Card against attacks. If any of these components fails, or if any one of them does not meet the applicable requirements, the Smart Card is no longer secure, since these components are coupled to each other in a logical AND relationship.

8.2.1 A classification of attacks and attackers

A major problem with all information technology systems that are subject to attack is the 'avalanche effect', which is often seen after a successful attack. If a printer (for example) succeeds in counterfeiting good-quality bank notes in sufficient quantity, this is naturally a matter of concern for the affected national bank, but in practice, it never leads to an inflation of the national currency. In the first place, the counterfeiter would never be able to produce a sufficient number of false bank notes for this, and in the second place, it is very risky to bring large numbers of counterfeit notes into circulation.

With electronic money, on the other hand, the situation is somewhat different. Since this consists of nothing more than immaterial information, it is in practice impossible to distinguish between an original and a copy. In addition, if a new counterfeiting method becomes known, this can lead to an avalanche effect, as other people copy the original technique. This effect can be very clearly seen by examining what has happened due to counterfeit prepaid telephone cards, which have been produced in very large numbers. Some network operators can still only defend themselves against this attack by restricting the calling destinations for cardphones.

In the following material, we attempt to systematically classify possible types of attack and attackers. The emphasis naturally lies on the information-technological side of Smart Cards, rather than on security features of the card body that can be checked by humans. This classification allows potential attacks to be evaluated, so that suitable measures can be taken against them. As is well known, it is easier to defend against a known type of attack than against an unknown one.

We have based our arrangement of the different types of attack on the ISO 13491-1 standard, which describes the concepts, requirements and evaluation methods for cryptographically secure equipment in the banking sector.

Exhibit 1017
Page 059 of 102

Classification of attacks

There are several different approaches to the systematic classification of attacks on Smart Cards. To conduct a security evaluation, for example, all possible types of attack are grouped and formally described according to each phase of the card's life cycle [IC Protection 97, Isselhorst 97]. This results in multipage lists that identify all conceivable attacks for each phase in turn. In the actual evaluation, each item is checked to see if the system or the Smart Card can defend against it. In this book, a different type of classification is used, in order to present the subject in as realistic a manner as possible, and also to illustrate the pong-pong game of attacks and defenses. In addition, it is our intention to present a general summary of methods of attack and defense, which is not specific to any particular system.

In principle, attacks on Smart Cards can be divided into three different types: attacks on the social level, attacks on the physical level and attacks on the logical level. Naturally, mixed types also occur in practice. For example, an attack at on the physical level could prepare the way for a subsequent attack on the logical level, which is for example the case with differential fault analysis.

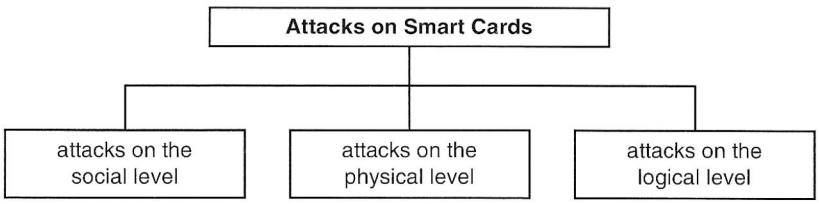


Figure 8.15 Classification scheme for attacks on Smart Cards

Attacks on the social level are attacks that are primarily directed against people that work with Smart Cards. These can be chip designers working for semiconductor manufacturers, software designers or, later in the life cycle of the card, cardholders. These attacks can only partially be parried by technical measures; they must primarily be defended against by organizational measures. Surreptitiously acquiring a PIN by watching it being keyed in can easily be prevented by providing visual shields on either side of the keypad. Attacks on the social level against Smart Card programmers are rendered pointless by making the procedures that are used public, and also by having third parties evaluate the program code that they produce. In this case, security depends only on secret keys, and the knowledge of the software developers is of no use to an attacker.

Attacks on Smart Cards on the physical level usually require technical equipment, since it is necessary to obtain physical access to the Smart Card microcontroller hardware in one way or another. The attacks can be either *static*, which means that no power is applied to the microcontroller, or *dynamic*, with the microcontroller operating. Static physical attacks impose no timing restrictions on the attacker, who can do his job at his own pace. With a dynamic attack, however, sufficiently fast data acquisition and measuring equipment must be available.

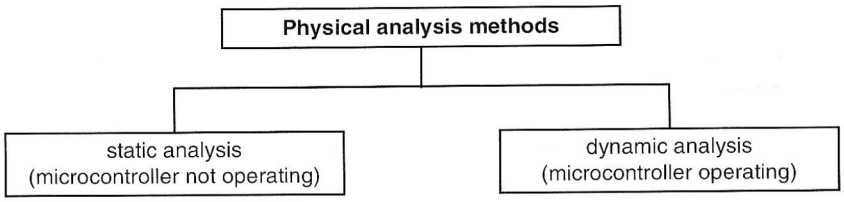


Figure 8.16 Classification of physical methods that can be used to analyze Smart Card microcontrollers

Up to now, most known successful attacks on Smart Cards have been on the logical level. These attacks arise from pure mental reflection or computations. This category includes classical cryptoanalysis, as well as attacks that exploit known faults in Smart Card operating systems and Trojan horses in the executable code of Smart Card applications.

Just as with the cryptoanalysis of cryptographic protocols, these attacks can be divided into passive and active types. In a passive attack, the attacker analyzes the ciphertext or cryptographic protocol without modifying it, and may for example make measurements on the semiconductor device. In an active attack, by contrast, the attacker tampers with the data transfer or the microcontroller.

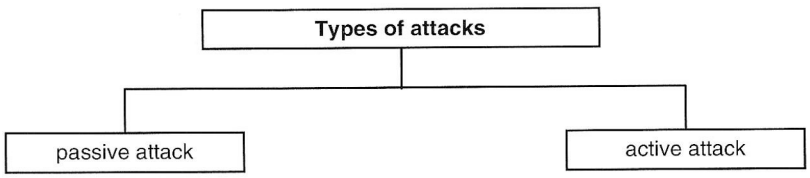


Figure 8.17 Classification of types of attacks on Smart Cards

The phases of the life cycle of a Smart Card as defined by the ISO 10202-1 standard[4] could be used with regard to the timing of possible attacks. However, this would result in verbose and long-winded descriptions, so for the sake of readability we have undertaken a simplification and classified the attacks into three intervals: (a) development, (b) production and (c) card usage.

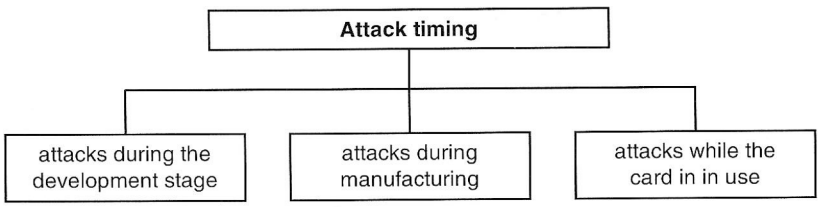


Figure 8.18 Classification of the timing of possible attacks

4 See also Chapter 10, 'The Smart Card Life Cycle'.

Exhibit 1017
Page 061 of 102

Attacks during development relate to system design, chip development, operating system development and the generation of applications. The term 'production' is used here to refer in general to all processes used to produce hardware. This covers the whole range from wafer production by the semiconductor manufacturer to card personalization and sending cards to their ultimate users. Card usage refers to the stage in which the Smart Cards are in the field, which means that they are being used by cardholders.

The consequences of an attack and the classification of attackers

In order to be able to realistically estimate the strengths and weaknesses of attacks on the security of a Smart Card, it is important that we first have at least a rough idea of the possible types of attackers. We can also use this information to help us devise defensive strategies and mechanisms.

As a rule, typical attackers have one of two basic motivations for their activities. The first of these is just plain greed, while the second is the desire for fame and status within a particular 'scene'. These two motivations have different consequences for the system operator. An attacker that seeks a financial reward for his activities can take the risk of becoming a 'card issuer' in his own right,[5] or he may attempt to blackmail the system operator. Both of these approaches can be combated using the usual judicial measures. If details of the attack become public, the reputation of the Smart Card system will be damaged. The worst damage to the reputation of the system operator occurs when a large number of cardholders lose money as a result of an attack.

The reputation of a Smart Card system is similarly impaired when an attack is prompted by a compulsion to perform scientific research rather than criminal tendencies. An attacker in this profession will consider his or her activities to be successful only if the results can be published in a suitable manner. The attacker is also under extreme pressure to publish these discoveries as quickly as possible, since in this trade, as is well known, only the first one past the post wears the laurels. The end result is that the system operator, with little or no warning, is faced with the publication of a detailed description of an attack on his system. Following this, the attack that has been made public is refined layer by layer by other interested parties, and also explained in terms that can be grasped by outsiders. The ultimate blow comes when programs that carry out the attack in a fully automated manner are published on the Internet.

A number of GSM network operators found themselves confronted with a similar series of events in the spring of 1998. However, here the attack on the COMP128 cryptographic algorithm had no large negative effects on normal network operation. From the point of view of the attacker, this manner of working also held a very large and very significant benefit. He was seen as the successful discoverer of a security leak, and thus as one of the 'good guys', and never had any serious concerns about any judicial consequences of his actions.

The quintessential conclusion that can be drawn from these scenarios is that it ultimately does not particularly matter to a system operator whether an attack comes from a 'good guy' or a 'bad guy'. With truly dangerous attacks, the financial damage and the damage to the reputation of the system are most often rather significant. In the worst case, the system must be shut down, all cards must be blocked and new cards that are immune to the attack must be issued. With large systems that have several million cards in use, such a process can take more than half a year.

---

5 This is the usual approach for producing self-reloading telephone cards.

The classification chart in Figure 8.19 shows the various types of attackers, based on experience and the previously described aspects. All four types can be equally dangerous to a Smart Card system, but they have different capabilities and options. The typical hacker has a moderate level of system knowledge, good creative ideas and usually a similar group of friends. He normally does not have an extensive amount of equipment, and his financial means are also limited. However, if he is competent and employs a suitable approach, he can certainly obtain access to a large amount of computing power, for example by means of an Internet campaign.

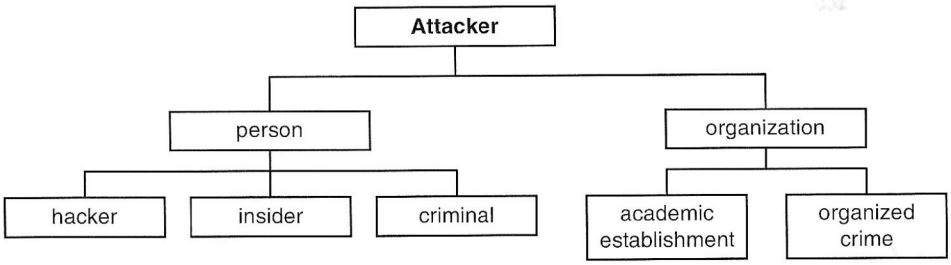


Figure 8.19 Classification of the possible types of attackers

All insiders form a special class of attackers, assuming in the first place that they have very good system knowledge. They may have access to hardware and software components, and the may know about weak points in the system. As long as only single individuals are involved, they are equivalent to hackers in terms of their resources and options. However, since insiders are neither anonymous nor especially numerous, it is usually possible to retrace their attacks.

The third group of individuals that can be regarded as potential attackers is criminals. They usually do not have a high level of technical knowledge, but they do have a lot of energy when it comes to achieving personal advantages (primarily financial) via their activities.

A potential source of attack that cannot be ignored in practice consists of academic institutions such as universities and technical institutes, with all their students and professors. They do not necessarily have special knowledge of specific Smart Card microcontrollers or applications, but they do have a large amount of generally useful knowledge. In addition, they have access to a large pool of qualified and inexpensive labor in the form of students and graduates, as well as adequate technical equipment in their laboratories. Many of these institutions also house a plentiful amount of computing power and highly motivated people with an experimental bent.

Organized criminal organizations naturally represent a completely different source of attacks on Smart Card systems. The amount of money that they have available allows them to acquire all the knowledge and tools necessary for a successful attack, either by purchasing it or by criminal means.

Classification of the attractiveness of an attack

In order to allow effective perimeter defense measures to be put in place, you should investigate the attractiveness of an attack for all of the candidate weaknesses of the system. This can be done in an objective mathematical manner by means of value analysis, in order to compute a prioritized list of probable attack targets. The scheme that is presented here is