Body Check: Biometric Access Protection Devices and their Programs Put to the Test

Lisa Thalheim, Jan Krissler, and Peter-Michael Ziegler

ABSTRACT: *Memorizing passwords is out. Laying your finger on a sensor or peering into a webcam can suffice to gain you immediate access to a system. There is the danger, however, that this new ease might be bought at the expense of security. How well do biometric access controls prevent unauthorized access? We have tested eleven products for you*.

According to estimates of the IBIA, the international organization of biometric devices and programs suppliers, worldwide turnover of biometric security devices and programs this year will for the first time exceed the 500 million euro limit. Though the growth is primarily being driven by large-scale orders by industrial customers and administrative bodies, nevertheless the number of products on the market designed for in-home and in-house PC use is rising.

The range of biometric security access tools for PCs meanwhile extends from mice and keyboards with integrated fingerprint scanners to webcam solutions whose software is able to recognize the facial features of registered persons to scanners that make use of the distinct iris patters of humans for identifying individuals. When the PC is booted the security software that goes with the tool writes itself into the log-on routine expanding the latter to include biometric authentication. In many instances the screen saver is integrated into the routine thus allowing for biometric authentication after breaks from work while the PC is still running. Sophisticated solutions, moreover, permit biometry based security protection of specific programs and/or documents.

The problem that all biometric security access procedures and devices still have in common, however, is the necessity of establishing fault tolerance limits: When a manufacturer - by making the appropriate hard and software efforts - decides to set his fault tolerance limits very narrowly, this increases his system's security, the user-friendliness of the system, however, is likely to decline in proportion. Should he on the other hand decide from the outset to permit considerable deviation, this will make his system easy to use, but greatly diminish its protective value.

Core Question Unanswered

The studies published to date on questions of biometric security are in the main based on evaluations of the false rejection and false acceptance rates (FRR, FAR) that are so popular with that line of business. In the event of a false rejection a user is prevented from accessing a system despite his or her access authority for the system; the reason usually being that the biometric features of the user are weakly developed, from the point of view of the system.

A false acceptance incident on the other hand allows a person whose biometric features have not been registered to log-on to the system. In most cases cheap sensor chips or badly implemented security software is responsible for a malfunction of this kind. Generally speaking, however, the statistically determined error probabilities do not give clear answers to the question of whether biometric solutions are able to protect a system even against an assailant bent on overcoming biometric protective measures. Unlike empirical scientific procedure, a hacker is scarcely likely to muster a battery of a thousand experimental subjects in the hope that one of them might perhaps be mistakenly accepted by the system. But the latter is the very core question that a security system must be made to answer.

Fig. 1 A fingerprint kit supplied by the regional Criminal Investigation Department of the German federal state of Lower Saxony stood us in good stead

Although the Fraunhofer Research Institute, based in the German city of Darmstadt, in collaboration with the German Federal Institute for Information Technology Security (BSI) conducted an extensive series of tests last year in the course of which "deliberate" searches for security loopholes in specific system were undertaken, the results, obviously due to pressure from the manufacturers, were never made public. Instead of finally laying its cards on the table, the biometrics line of business prefers to hide behind error rates it has measured itself.

There is thus only one way at present to determine how vigorously the current biometric security systems are able to resist attempts at overcoming them: test-it-, assail-it-, and outfox-it-yourself. Attempts undertaken to breach the systems can roughly be assigned to three different scenarios:

The first approach relies on tricking the biometrics system with the aid of artificially created data whilst making use of the regular sensor technology of the system; a precondition for this approach being spy-work that gets hold of more or less easily obtainable biometric features such as an image of a face or a fingerprint. After developing the appropriate photograph(s) and/or creating the artificial fingerprint(s) required, these copies of features can then be used to attempt to obtain authentication. The reactivating of

traces of fat on a fingerprint scanner- of so-called latent images - also belongs to this scenario.

The second scenario also entails tricking the biometrics system with artificial data. In this case, however, by playing back to it reference data sets, collected, for instance, with the aid of a sniffer program listening on the USB port, the system's regular sensor system is bypassed. This procedure is commonly called a replay attack. For more on USB sniffers and hardware analyzers consult the 'Attacking Via the USB Port' box.

The third approach is made up of attacks that aim at the database directly. In general this scenario requires that one be in possession of data base administrator rights and have permission to exchange sets of data used as reference sets for recognition purposes. In the event that these data sets have no separate protection of their own the assailant has the opportunity of forging user data with a view to reactivating these at a later date in accordance with his or her designs. In the sensitive area of financial transactions this could turn out to be a ticking time bomb. Vide the hypothetical case of a former bank employee who years after leaving his firm decides to bring back to life the at one time surreptitiously created data set 'Mr. Miller's eleventh finger' with the intention of generously taking care of his retirement needs.

In our attempts at outfoxing the protective programs and devices we have concentrated on the first method: direct attempts at deceiving the systems with the aid of obvious procedures (such as the reactivation of latent images) and obvious feature forgeries (photographs, videos, silicon fingerprints). After already obtaining astonishing results by means of this approach, we conducted exemplary tests only on whether it was possible to extract biometrically relevant data by eavesdropping on the communication via the USB port between the computer and the sensor.

The Candidates

All eleven biometric protection applications tested by us are products that were presented at this year's CeBIT trade fair at the German city of Hanover and all are freely available on the market. Even though the range of products tested was not complete it did on the whole reflect market conditions: The great majority of the currently available biometrics products relies on features of the fingers for user identification. Neck-and-neck in second and third place are face recognition and iris scanning systems. All other devices and programs such as make use of language recognition, hand geometry measurement, signature recognition or keyboard touch dynamics taken together have only a marginal share of the security biometrics industry's overall turnover.

Besides six products involving capacitive fingerprint scanners (Biocentric Solutions, Cherry, Eutron, Siemens and Veridicom) two optical (Cherry, Identix) and one thermal (IdentAlink) fingerprint reader were available to us. Our tests also took in the Authenticam by Panasonic, an iris scanner that is currently being marketed in the USA and is scheduled to enter the European market in the near future, as well as FaceVACS- Logon, a technical solution for recognizing faces developed by the Dresdner Cognitec AG. Our test

environment consisted of three PCs (1-GHz-processors, 128 Mbytes of RAM, 32 Mbyte AGP graphics cards) running Windows 98 and Windows 2000, as well as of a Gericom notebook with a 14" LCD screen running Linux.

Photo Ops

Compared with other biometry-based security access procedures the marketing opportunities for facial feature recognition devices and programs are assumed to be fairly good. The technology profits especially from the fact that some of its features are already integrated into the living conditions and habits of PC users: Many people are a good deal more familiar and comfortable with gazing into a camera than, for instance, having their eyes scanned by infrared beams or their fingerprints 'taken' by a device, the latter procedure perhaps awkwardly evoking images of criminal investigations.

Cognitec's FaceVACS-Logon, which can be applied both as a authorization access solution and as a screen saver, uses as its sensor a commercially available webcam. Cognitec recommends Philips's ToUcam PCVC 740K. Authorization proceeds almost automatically: When a person approaches the PC's webcam the recognition software aided by special algorithms in a first step begins to search in the pictures it takes for eyes; once these are found it mathematically projects based on their coordinates a virtual rectangle into the picture. The following pattern recognition process in the course of which so-called Support Vector Machines (SVM) capture characteristic facial features which are subsequently compared with stored facial patterns takes place within the boundaries thus established. In the event of a positive match the authorized person is granted access to the PC immediately.
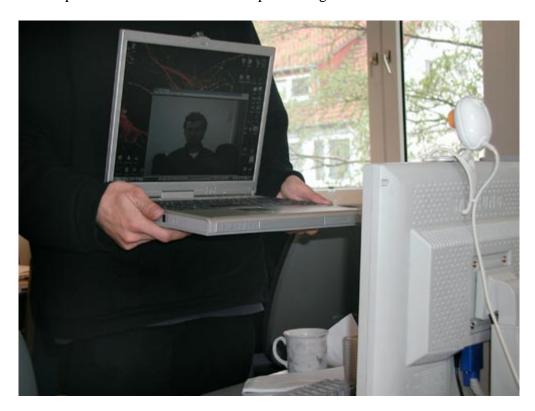
Fig. 2. Maximum security level not withstanding, FaceVACS-Logon can be outfoxed with a short video clip of a registered person.

During enrollment, i.e. the creation of an initial reference set of facial images, FaceVACS begins by storing a number of images of the new face in the .PPM format in a log file. During each subsequent authentication procedure images, this time with a .fvi tag, are added to the collection. As these image data are neither encrypted nor otherwise particularly protected they can be read and possibly manipulated once access to the system has been acquired. Moreover, the log files allow one to ascertain which are the 'good data' sets, those, in other words, that lie above the recognition threshold. We began our attempts at outfoxing the system by transmitting the freely accessible image files to the notebook. We then presented the images upon the notebook's display to the ToUcam. Once we had found the appropriate distance between the webcam and the display, it would take but one attempt in most cases for FaceVACS-Logon to accept the image presented and hence grant us access to the system.

In the course of our next attempt at trickery we recreated a situation that could easily come about in the real world: An assailant without access to stored data attempting to overcome the obstacle of the facial recognition procedure. For this purpose we 'secretly' took three pictures in all of an authorized user with a simple digital camera under different lighting conditions. These digital images we then again transferred to our notebook, proceeding to show the various images to the webcam via the former's display. The result was that after only two images of the digital camera we had put FaceVACS's biometric protective measures out of action. From then on the system would cede control of the PC to anyone who held the notebook's display up to the webcam's scrutiny.

Playing Video Games

To prevent deception with the aid of photographs Cognitec has integrated a higher level of security known as Live-Check into the FaceVACS's software. Indeed once Live-Check has been activated all attempts at deception with stills (such as those described above) are foiled. On the downside, however, user-friendliness sinks considerably and registered users are only seldom recognized right away.

Hence we simply shot a short .AVI video clip with the webcam in which a registered user was seen to move his head slightly to left and right. As brief movements suffice for FaceVACS to consider an object alive and as the program engages in simple 3D calculations only, we were not particularly surprised about the success of our approach: Once the appropriate display-to-ToUcam distance had been found the program did in fact detect in the video sequence played to it a moving 'genuine' head with a known facial metric, whereupon it granted access to the system.

In a worst case scenario this state of affairs implies that a person without a professional background to movie making who had wielded a digital camera during a public meeting and there shot visual material of authorized personnel, to log on to a protected system, need only modify the acquired material slightly and transfer it to a portable PC.

Sleight of Finger

The most common method for distinguishing fingerprints is based on the so-called minutiae, the 'small details'. The minutiae are interruptions to the lines upon the fingertips, such as endpoints, bifurcations, whorls or islets. To identify a human fingerprint unambiguously information about the type, position and orientation of at least ten to twelve of these minutiae is required.

In the main capacitive fingerprint scanners are used to get hold of these minute details -- above all because the CMOS chips used in them have for some time now been available at a fairly reasonable price. When a finger is placed on the device the scanner's 65,000 pixels treat the surface of the skin as a capacitive pole. The capacitance of each miniature capacitor depends on whether a line or a trough is to be found above the measuring point in question. The device then converts these individual values into an 8-bit gray scale, extracts about 20 minutiae and proceeds to store these values in a reference file for future authentication purposes.

Fig. 3. Even simple breathing will do the trick of outwitting a capacitive fingerprint scanner.

In Germany the best known among the desktop fingerprint scanners is Siemens's ID Mouse, which is equipped with Infineon's capacitive FingerTIP sensor. In its current Professional V4.0 version the device can, moreover, be used as a optical USB scroll mouse. During the tests there was never a problem with installing the USB drivers and setting up the application software. Under normal conditions the enrollment as well as the subsequent authentication almost always went off quickly and without error.

It was equally easy though to outwit the ID Mouse with simple tricks. Although this according to the manufacturer's statements should have been impossible we were able several times to reactivate by simply breathing upon them traces of fat left by fingerprints upon the sensor's surface, thereby overcoming the biometric protection of the system. We cupped our hands above the scanner and within the shell thus formed breathed gently upon the sensor's surface. Meanwhile on the screen of the biometrically protected computer we were able to see the contours of an old fingerprint slowly reemerge.

Fig. 4. A fingerprint on adhesive film may suffice as a biometric ID.

It was also possible to reactivate latent fingerprints by carefully placing a thin-walled water-filled plastic bag onto the sensor's surface. The advantage of this technique is that the water spreads more evenly across the sensor's surface. When the latent fingerprint was a good quality one few attempts would normally suffice to gain us access to the system. Even when the security mode was set to its maximum (extended mode) we were able to undertake these simple latent image activations at the ID Mouse. The probable reason for this phenomenon being that the capacitors of the capacitive sensor are sensitive to humidity. Damp air that, for instance, condenses on the sensor's surface where there are residues of fat causes the relative dielectric constant on the sensor's surface to change thus leading to a change in capacitance, which the device interprets as a release signal inducing it to undertake a measurement.

The ID Mouse can be outfoxed even more easily by dusting the fatty residue of the fingerprint on the sensor with commercially available graphite powder (Ravenol), then stretching an adhesive film over the sensor's surface and gently applying pressure on it. Whereas we were only intermittently successful at overcoming the biometrics barrier when using the breathing or the water bag method our success rate with the adhesive film

technique when the latent fingerprints were of good quality was almost one hundred percent.

According to Siemens especially designed algorithms of the security software belonging to the package check whether the currently scanned fingerprint in terms of its position and angle coincides within certain predetermined tolerances with the last registered version of the print. This is supposed to prevent the system from being taken in by all attempts based on latent image reactivation or replay.

According to a statement from Munich the company could not conceive of a reason why their procedure should have failed when we tested it. In future, the statement went on, the company would focus even more on the problem of latent image reactivation.

In the course of a further concrete assault approach we acted out a scenario of a theft of data by more professional means, theft of a kind that people engaged in the field of industrial espionage might be thought to be capable of. With the aid a fingerprinting kit that the regional Criminal Investigation Department of the German federal state of Lower Saxony was generous enough to make available to us we took fingerprints from glasses and CDs. We dusted the prints with graphite powder, secured them with adhesive film, and then after placing them on the scanner applied gentle pressure to the surface. Our success rate with this approach was very high, regardless of whether the system was in its normal or its extended security mode.

The Cherry G83-14000 keyboard had a comparable security behavior, which was not hard to predict as the insides of the keyboard scanner and that of Siemens's ID Mouse are identical. The former was thus without much ado outfoxed by the same procedures.

Eutron's fingerprint reader Magic Secure 3100 on the other hand is a product manufactured by the South Korean firm of Hunno and includes a CMOS TouchChip by STMicroelectronics. For covering the European market the Italian firm of Eutron merely relabels this combination of fingerprint scanner and optical USB scroll mouse. It too is a capacitive scanner with properties and weaknesses comparable to the product by Siemens: Approaches to deception via the regular sensory mechanism of the device, of the kinds described above, also lead to success. Though the breathing approach was not quite as reliable, the moment graphite powder came into play we were easily able to gain access to this system also.

Fig. 5. Reactivating a latent image can also be done with a little water in a plastic bag.

The only product in the field tested to possess a special protective mechanism for the sensor surface of the capacitive scanner was Veridicom's 5th Sense Combo. A possible solution for this device that might have done away with the latent image problem once and for all after every use would have been to equip the underside of its protective spring-driven sliding cover with a miniature cleaning sponge. Besides the cover Veridicom's fingerprint reader is furnished with an integrated smart card reader. In the case of smart-card biometric-authentication applications the access check routine is no longer confined to the protected computer in question, the user can also seek authentication in relation to reference data stored on the smart card. Alas, Veridicom passed up the design opportunity for wiping away latent images on its device. We were able to outfox the device in much the same way we had outfoxed the others, expect that with the Veridicom scanner there was the slight additional difficulty that it was necessary to hold the sliding cover open with one's other hand or by sticking a matchstick in.

Security Roulette

Completely out of line during out tests were the two PDA solutions by the US American manufacturer Biocentric Solutions. To ensure their integration into the operating systems Windows CE and Pocket PC 2002 both applications make use of the program BioFamily that comes with the devices. Whereas BioHub is designed to prevent unauthorized access to a variety of these little helpers by means of a CompactFlash Card with an integrated fingerprint scanner, naught but Compaq's iPAQs will fit into the BioSentry expansion jacket with its rear FP scanner.

Even during normal use problems with both products kept popping up. Neither BioHub nor BioSentry reliably recognized registered users - a state of affairs that repeated soft- and hardware resets were unable to remedy. Sometimes it took 30 attempts for a simple authentication to succeed, then again placing the very tip of a fingertip of an unregistered user on the sensor's surface would suffice for access to the PDA to be granted. In a nutshell: Since there was no way to sensibly test either BioHub or BioSentry, we put them back where they had come from - inside their FedEx packages.

Illuminating

The second most frequent manner in which fingerprints are currently mechanically scanned is the optical one. In this case the finger which is positioned above a prism or a diffracting grid is illuminated by light from color LEDs and photographed by a CCD or a CMOS camera. An alternative technique consists of placing the finger illuminated from below upon a light-conducting fiberglass surface that is directly linked to a CMOS chip element.

Accordingly, during our tests we were unable by reverting to simple latent image activation to get the better of our candidate, Identix's Bio-Touch USB 200 - with systems of this kind to trigger the recognition procedure at all it is necessary that, prior to the CMOS camera taking the picture presented to it via a concave mirror, the light from the red LED source be reflected by an object on the scanner's surface.

For the first time we thus had to avail ourselves of an 'artificial finger.' An intruder with even minor manual skills might, for example, with the aid of photo-sensitive lacquer fashion the image of a fingertip into a mould for a three-dimensional likeness of the fingertip in question. As these steps are obvious we felt free under laboratory conditions to take a somewhat simpler approach: We took small common tea-warming candles, removed their wicks, pressed fingertips into the warm wax and proceed to fill the troughs with commercially available silicon.

The moment we placed the thus fashioned 'fingertips' on the scanner's surface BioTouch's resistance collapsed: The DFR-200 optical sensor accepted the silicon copies without hesitation, during authentication as well as during enrollment. The reverse of the deception also worked: When in possession of a silicon copy of a fingerprint of a registered person we were able to log on to the computer 'incognito'.

Moreover, in the course of further experiments we also detected that even without the aid of an 'artificial finger' it was possible to deceive the optical sensor. For we were again able to gain access with our tried-and-tested adhesive film technique. In this case, however, though it was not enough to simply place the film with the graphite pattern on the scanner's surface, once a halogen lamp was made to shine on the scanner from a distance of about 30 centimeters, that too worked. Apparently, the intense back-lighting on the one hand enhanced the contrastive properties of the graphite powder on the scanner's surface whilst on the other inducing a kind of snow blindness in the sensor.

The G81-12000 keyboard made available to us by Cherry is likewise equipped with Identix's optical fingerprint scanner, hence its results vis-à-vis our attempts at deception were more or less identical.

Hot Spots

A lot less frequently than those with capacitive or optical systems are fingerprint scanners with thermal recognition systems deployed. The latter systems measure the minimal temperature differences between the 'hills' (the lines of fingertips) and the 'valleys' (the furrows in between) that the sensor registers on the fingertip's surface.

IdentAlink's Sweeping Fingerprint Scanner FPS100U works on the basis of Atmel's CMOS-Finger-Chip-Sensor FCD4B14, which consists of a total of eight rows, placed one after the other, with 240 sensor pixels each. To trigger the scanning procedure one moves one's finger, applying gentle pressure, slowly across the only about half a centimeter wide thermal sensor. Located right next to it is a small heating unit that raises the temperature of the lines of the finger while they are moving across the sensor. Immediately after it has been switched on the device cannot supply usable images, only after a short heating-up period can high quality images of fingers be generated.

If the BioLogon software that goes with the device hadn't repeatedly stymied our attempts at getting to grips with it - on occasion the system crashed five times during enrollment and was only 'forced' back into cooperating with us by our pulling the USB plug - IdentAlink's Sweeping Fingerprint Scanner might have made a comparatively good impression during the tests. Because unlike the case with the capacitive and optical sensors owing to the thermal sensors minute surface area it was not possible to reactivate latent images or make use as before of our otherwise so successful adhesive film technique.

Only on the basis of silicon copies of authentic fingerprints were we able to score some successes: With their aid we repeatedly surmounted the biometric-access protection barrier. With a little bit of practice we were able to use silicon copies to create reference data sets and thereafter to gain access with the original finger as well as with the copy of the same.
In conclusion it must be said, however, that the amount of effort required to trick the sensor mechanism of a thermal fingerprint scanner with artificial data is significantly higher than that required in the other cases described above. Nevertheless, even the FPS100U is still a long way off from guaranteeing secure access.

The Highlight

Biometric applications that make use for access control purposes of individual features of a person's eyes, such as those of his or her retina or iris, are somewhat tainted by their cliché association with secret service activities in high-security bunkers. Even though a handy iris scanner for the home already exists: Panasonic's Authenticam BM-ET100, which with its separately operating webcam is not much lager than a pocket-size edition of Shakespeare's sonnets.

The bottom section of the scanner's casing contains three infrared light sources. The two outer and somewhat weaker ones illuminate the iris while the user adjusts his or her distance to the device. When the user gazes straight into the camera from a distance of about half a meter (48 to 53 cm), a mark detectable in the opening of the lens changes from orange to green, at the same time the infrared light source in the middle begins to shine brightly and a sufficiently high quality picture of the iris is taken by the camera.

At first the AuthentiCam presented us with quite a challenge. During our first attempts at trickery we offered digitally-shot iris images via the notebook display as well as via a head-mounted display (HMD) to the black and white video camera of the scanner; owing to the too intense reflection of light on the displays without success, however. Due to the overexposure that resulted the system was also unable to recognize the features of iris images that had been printed on normal paper.

What was interesting though was that all iris images taken by the system showed a bright spot in the middle of the pupil. This fact gave us the idea that - besides fulfilling the requirement of acquiring a green light by the system - we might in our next attempt at outwitting it show the system's camera human digital iris images printed on paper that had a small hole cut into the middle and behind which were placed the hidden pupils of actual human beings.

Fig. 6. A sight for sore eyes perhaps, but very effective: achieving authentication with someone else's iris by hiding your own pupil behind it.

It quickly became apparent that this would be the way to success. As an opening to its calculations the PrivateID software by Iridian that comes with the device requires the in-depth aperture of the pupil, upon the center of which it bases its computations of the iris. By doing the deed we had at least initiated the taking of images by the system.

The only thing that was still missing was a printed picture of an iris with an appropriate degree of quality. Hence we presented to the Authenticam a digital image of a human eye that had been sprayed onto mat inkjet paper with a resolution of 2400 x 1200 dpi and into which we had previously cut a miniature hole. This was enough to overcome Authenticam's resistance: We were granted access to the system under the assumed identity of 'Master False Eye'.

It was also possible to enroll with the aid of the 'artificial' eye. From that point onwards anyone in possession of the eye pattern was able to log on to the system. Moreover, the person whose eye had been used to create the pattern was also able to acquire authentication in relation to the picture-generated reference data set with his own live iris.

Panasonic on account of these results, as was to be expected, proved to be 'not amused'. We were told that the product made available to us for our tests was a prototype which would be redesigned prior to its introduction to the German market. As the system has been marketed in the USA for some time now, we suspect that without our tests no such redesigning would have been contemplated. It has to be said in favor of the iris scanner, however, that under real life conditions it would not be easy to obtain iris images of authorized persons. With such images at one's disposal, however, creating a deceptive eye-patch can no longer be thought of as much of a problem as high resolution inkjet printers and mat paper cannot today be considered high-tech equipment.

Conclusions

For the sake of fairness we need to emphasize again at this point that according to their manufacturers' statements none of the products tested by us was designed for use in a high-security environment. Nevertheless, the question can be put whether a security application whose protective measures can be foiled with the simplest of tricks is an investment of 300 euros worth making.

A question also raised by our tests is whether the expensive systems are really more secure than the ones tested by us - or whether it is simply the case that no one has yet seriously tested them? After all, the weaknesses are in part those of the algorithms used and not those of the sensors applied. Should better algorithms already exist, why do the manufacturers not use these for their low-priced products also? The development cost argument does not apply to software that already exists.

Even though manufacturers of biometric products can scarcely avoid for marketing reasons extolling their applications as mature and secure: The technology suitable for mass consumption for identifying and authenticating the identity of persons on the basis of their physical features is obviously still in its infancy.

That much remains to be done, before any abolition of passwords or PINs in favor of biometric procedures can even be contemplated, our tests have shown: We were able, aided by comparatively simple means, to outwit all the systems tested. Whether silicon or a notebook constitute the kind of unusual 'high-tech weaponry' that some company statements made in response to our results claimed we had used, is up to the reader to decide. The fact remains, however, that the products in the versions made available to us were more of the nature of toys than of serious security measures. If it does not want to gamble away the trust in biometric technology right from the start, the line of business should not treat the security needs of its customers quite so thoughtlessly.

As long as adequate security cannot be guaranteed through biometric solutions the use of these products should always be coupled when possible with the assigning of additional PINs or passwords: For most of the solutions doing so is a standard option. When capacitive fingerprint scanners are being used the sensors' surfaces should be cleaned after every use to prevent possibly present latent images from being reactivated. Moreover, anyone using biometric access protection procedures in a Windows 98 or Windows ME

environment, should immediately block all avenues whereby regular enrollment might be bypassed.

Appendix A: A Need for Clarification with Regard to Biometric Applications

The government of the Federal Republic of Germany continues to consider biometric procedures important tools in the fields of identity ascertainment and criminal prosecution. This emerges from the answer given on April 24th to the official question posed to the government by the speaker on domestic policy of the parliamentary group of the PDS (the Party of Democratic Socialists, Germany's reformed ex-communists), Ms. Ursula Jelpke. Referring explicitly to the report on biometrics by c't magazine (c't edition 5/02) Ms. Jelpke had sought to determine the attitude of the federal government to the error rates of these recognition systems and the current state of affairs with regard to the possible introduction of biometric data to identity cards.

Responding to the official question, the ministry of the interior declared that no bill on the introduction of biometric features to and storage of the latter upon identity documents would be introduced to parliament until the requisite preliminary work had been completed. As a first step the procedures in question would have to be tested 'in pilot projects of considerable scope that as to their environmental features simulate as closely as possible the actual later environment of use of the applications.' According to the ministry, there is thus no fixed date for the introduction of the bill. The use of biometric procedures with regard to identity documents had, however, already been discussed at a ministerial level within the EU, the ministry's statement continued, and for June 2002 a conference on this topic of all EU member states was planned.

As there are presently at least five totally different biometrics approaches vying for the customers' favor and the scale of a later application at a total of 70 million owners of German ID documents is clearly defined, the testing is likely, from a technical point of view at least, to take up some time yet.

The assessment of the situation by the Office of Technology Assessment (TAB) of Germany's lower chamber of parliament, the bundestag, is similar: 'An assessment of the capabilities of the available biometric systems on the basis of the - at times highly contradictory - items of information regarding them cannot reliably be undertaken,' thus the office summarizing its insights. The confusion were compounded, according to the office, by the unclear distinctions frequently made between the possible potential and the actual current capabilities of the devices and programs. The TAB, founded in 1990, is an institution that, upon a request by the parliamentary committee on research, furnishes the members of parliament with topic-related reports on and analyses of scientific and/or technical developments, whilst supplying them with information on the related options for political action available. To accomplish its tasks it normally relies on the expertise of independent, external experts.

Appendix B: Attacking Via the USB Port

Taking account of security concerns is not a forte of the protocol of the USB, the Universal Serial Bus. It allows users to swap devices hooked up to a computer while the computer is running; thereby, giving potential assailants something of a break: It allows them to exchange the biometric scanner for a deceptive device of their own and play back to the computer data gathered while eavesdropping on a login event.

The simplest eavesdropping tool is a filter driver like USB Snoop for Windows. USB Snoop interposes itself between the driver of the USB adapter and the actual device driver. After being presented by Windows with all the data exchanged between the USB and the device driver, USB Snoop then writes these into a log file of its own. These data the snooping party can then analyze at its leisure. Filter drivers are quite easy to detect though and in addition require administrator rights to be installed under Windows 2000 and Windows XP. Nevertheless, they would permit studies of a biometric scanner of the same kind as the one to be tricked to be undertaken at one's own PC.

On the other hand, the workings of a hardware analyzer like the USB Agent by Hitex (see page 69), which eavesdrops on the USB cable directly, are virtually invisible. A USB Agent latched on to the cable records all transmitted data, transferring these to a foreign PC. An assailant can then with the aid of the software that goes with the device analyze on the foreign PC the protocols used by the target PC and filter out the relevant data packages. After exporting the data to a text file it is then possible to generate within it the data required to accomplish a login.

Fig. 7. With the aid of data packets gathered by eavesdropping and some lines of Perl script we were able to reconstruct complete fingerprints.

With regard to the ID Mouse by Siemens we were able with the aid of USB data packets and a few lines of Perl script to reconstruct the image of a fingerprint. All one requires to replay the data gathered by eavesdropping is a micro controller with USB support and some storage capacity. Together these then constitute a device capable of impersonating towards the target PC the previously removed biometric scanner. The firmware required to do so is fairly easy to program: The device, upon configuration requests, simply needs to respond with answers identical to those of the actual scanner and then at the right moment play back the stored biometric data.

The way to foil attacks of this kind with certainty would be to use so-called challenge-response procedures in the course of which the biometric scanner and the application mutually authenticate one another and thereafter communicate with one another exclusively in an encrypted fashion.

Translated by Robert W. Smith