Hacking Biometrics

Fooling A Fingerprint Scanner 3/3: Creating an artificial finger using a latent fingerprint

Last updated: 18th of March 2003.

The vulnerability was analyzed by:
Antti Kaseva
Antti Stén

1. Threat and Vulnerability

Fingerprint recognition is based on the fact that every human being has a unique pattern of ridges and valleys on their fingertips. The scanner makes a copy of your fingerprint and compares its characteristics to the ones stored beforehand. These characteristics are measured based on special points (such as branches and loops) on a print. In figure 1.1 can be seen some of these special points. The scanner uses these points as coordinates to define other branches, loops, beginning of lines, number of lines etc.

The scanner used in this hack stores only these special points of the user's fingerprint. The method the scanner uses to to obtain those points is explained in section 3.

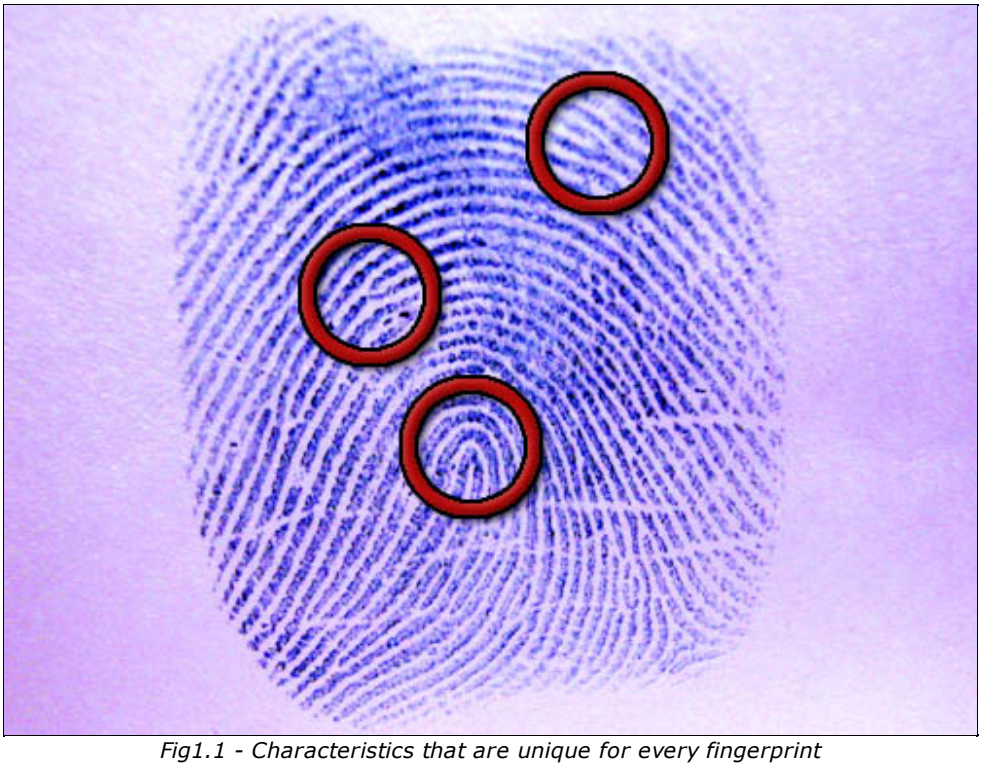

Fig1.1 - Characteristics that are unique for every fingerprint

The hack is to create an artificial finger using a mold that is manufactured from a latent fingerprint left by the legitimate user. The fingerprint can be obtained from just about anywhere, mug, door handle, rail etc. With this artificial finger the hacker should be able to intrude a system if the mandatory smart card required for logon is available and in use.

The used fingerprint scanner is Precise Biometrics 100 SC, which uses a capasitive measurement to detect finger and has a smart card reader/writer to store fingerprint info. Though in this hack only biometric aspects are to be defeated.

This combo of smartcard reader and fingerprint scanner can provide access to Microsoft Windows NT, 2000 and XP operating systems if account data is stored onto the smart card. This setting overrides Windows' own logon screen and user logs into his account using a smart card and a fingerprint scanner, no passwords are required. Typical hack cases occur when the legitimate user forgets his card into the reader, somewhere near it or the intruder steals the card from the user. Most threats in corporations come from the inside and this attack is most presumably performed by a fellow co-worker. Hacking thru this device usually gives all the

attack is most presumably performed by a fellow co worker. Hacking thru this device usually gives all the priviledges for the user to do whatever he wants, read and write data, send mail etc.

2. Preconditions for the attack

This hack presents the biggest threat to a fingerprint scanner as it uses an authentic and latent fingerprint. Requirements and preconditions are quite quite high in normal conditions but the threat is true and very serious.

Requirements:

- Operating system: Microsoft Windows NT, 2000 or XP
- Fingerprint scanner: Precise Biometrics SC100
- Legitimate user's enrolled fingerprint with login information on the smart card
- Temperature between 0-50°C (Scanner operating temperature)
- Fingerprint of the legitimate user

Things, materials and equipment:

- Photocopier powder
- Soft makeup brush or comparable
- Digital camera with a good macro function
- Image manipulation program
- High resolution printer with transparency printing capability
- One transparency
- Photosensitive lacquer (i.e. Positiv 20 by Kontakt Chemie)
- UV light (optional, can be replaced with a regular light bulb)
- Copper plated circuit board
- NaOH (lye) mixture (ca. 3dl)
- FeCl3 (Ferric chloride) mixture (ca. 3dl)
- Soft watercolor brush
- Gelatine leaves (40g gelatine + 1/2dl water ~= 20 fingers)
- Stowe, kettle, refrigerator

3. Analysis of the attack

Compared to hack 2 where a live finger was used to create a mold this hack is very different. A latent fingerprint is used and the procedure is divided into five sections, obtaining fingerprint, making the transparency, creation of the mold, creation of the finger and using the finger.

1. Obtaining fingerprint:

1. Spy on the user and see which finger he uses for login.
2. Spy some more and watch for suitable fingerprints (on cups, doorhandles, rails etc.)
3. Gently blow some photocopier powder on the fingerprint
4. Use makeup brush to dust the excess powder off and make the print clear.
5. Take a high resolution snapshot of the print with the camera.
6. Measure the distance between any (preferably with long distance) two characteristic points so that you can define the scale later on.
7. Clear your tracks (Wipe out the powder)

Fig3.1 - Latent fingerprint dusted visible on the side of the mug.

2. Making of transparency:

1. Use image manipulation program to edit the fingerprint image.
2. Clear out the excess dust from the sides of the print.
3. Adjust contrast so that the print has a clear pattern.
4. Scale the image according to the measurements done on the actual dusted fingerprint.
5. Convert the image to negative. (Invert)
6. Print the image on the transparency.

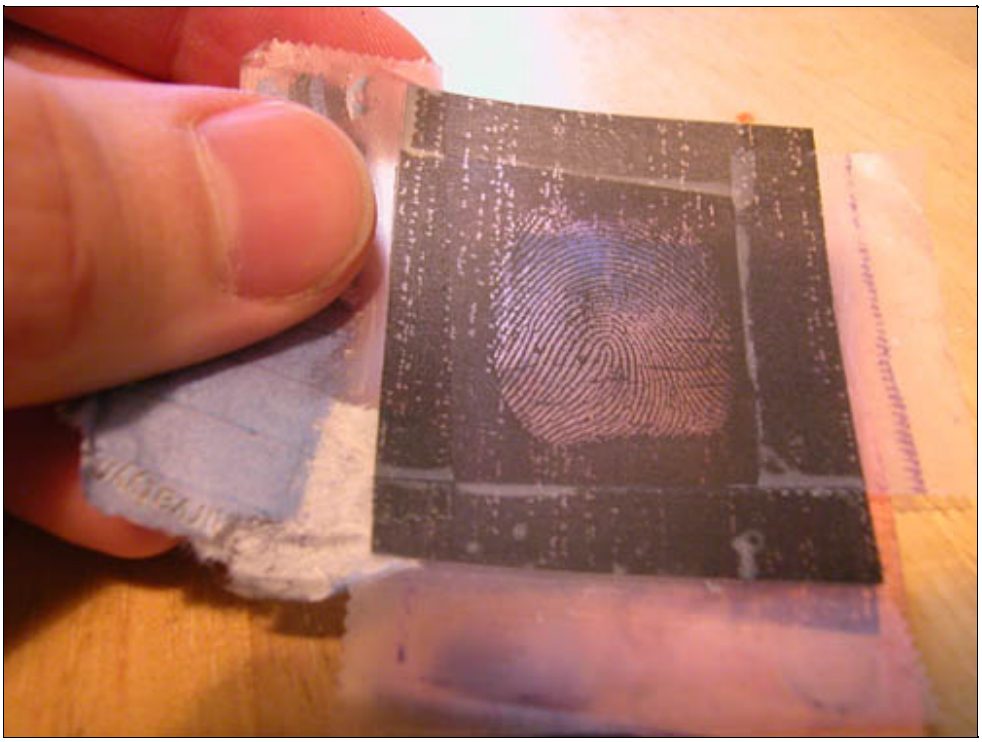

Fig3.2 - Finished transparency showing negative image.

3. The making of the mold:

In this section it is adviced to follow instructions stated on the containers of the materials as they might vary depending on the brands used. Some testing is probably needed to calibrate all materials together. (i.e. dilution of the acid for the circuit board used)

1. Spray the photo sensitive lacquer on the circuit board and let it dry for a while.
2. Place the transparency on the circuit board with tape.
3. Expose the board through transparency with UV-light for 5-15 minutes. (Normal light bulb can also be used but the exposure time is much longer.)
4. Take off the transparency
5. Develope the lacquer using NaOH-solution. Use watercolor brush to brush the lacquer. Be careful not to rub off all the lacquer. (NaOH is used to wash off the lacquer in non-exposed areas and to develope the rest)
6. When you see the fingerprint wash the board with water.
7. Corrode the board using FeCl3-solution. (Hang the board copper side down in the solution.)
8. Once the copper is corroded off wash the board throughly with water.
9. Use soap or alcohol to rinse any remaining lacquer off the board.

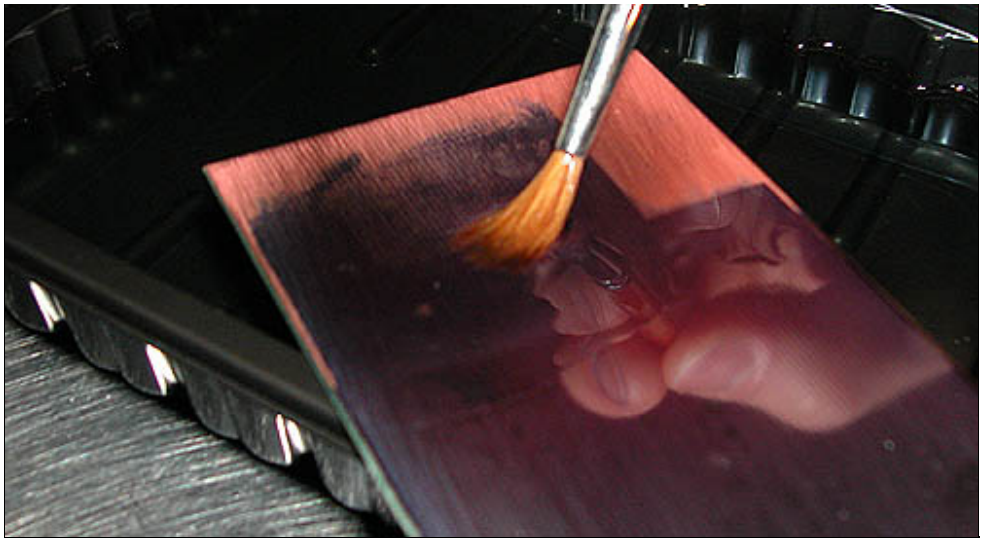

Fig3.3 - NaOH is used to wash off the lacquer in non-exposed areas.

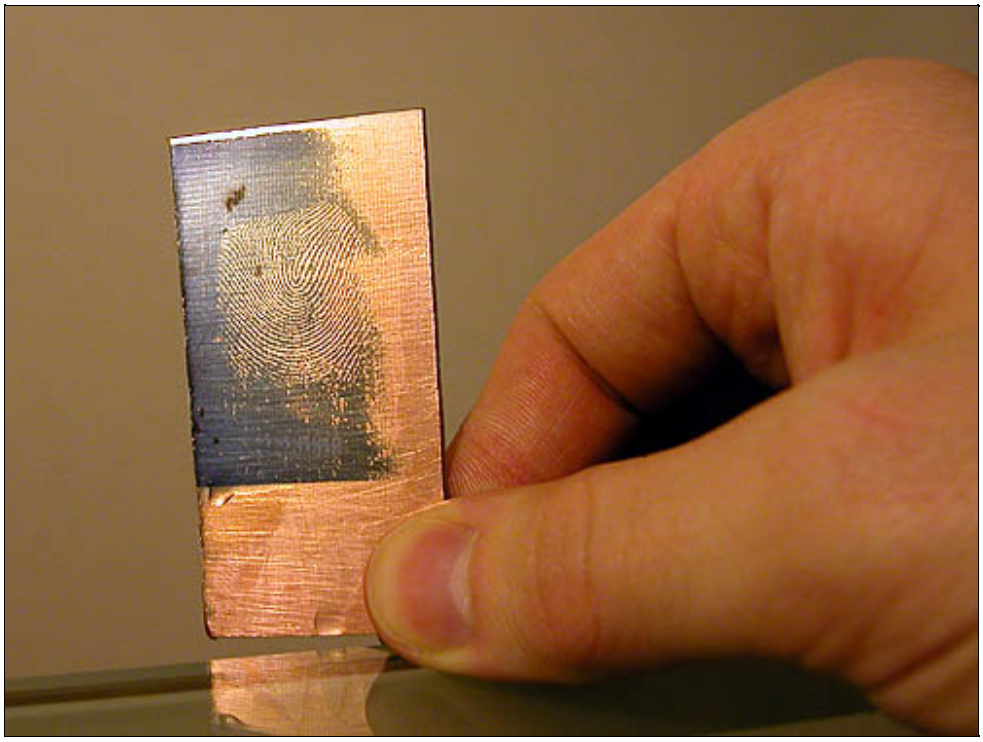

Fig3.4 - The board ready to be corroded.

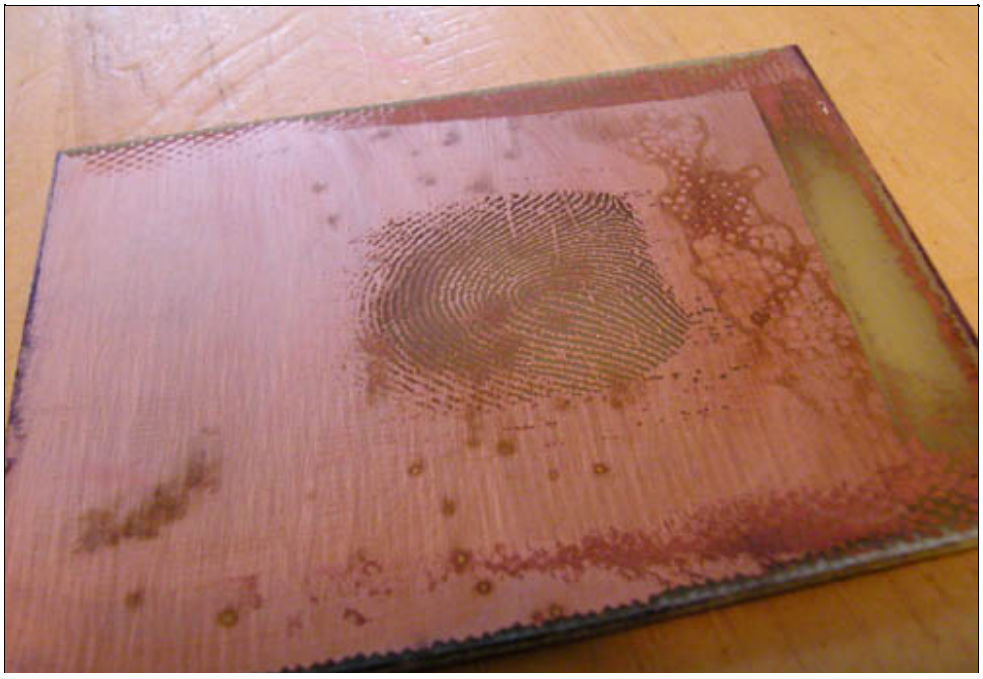

Fig3.5 - Finished board (mold).

4. The creation of the finger:

1. Soften gelatine sheets in cold water for about 5 minutes.
2. Heat up the water (1/2dl) so it boils.
3. Put the softened gelatine sheets into the hot water. Do not boil!
4. Stir for 10 minutes.
5. Let the mixture cool down a bit. You can try to reduce the amount of bubbles with a gentle stir.
6. Pour some of the gelatine mixture on the mold so that it covers the print completely. Do not make too thick finger.
7. Put the mold in the refrigerator and let it congeale for at least 15 minutes. The longer the better, but keep the mold in a humid place or the gelatine will dry up.
8. After the gelatine has congealed you can separate it from the mold. Using a knife peel off a bit from the corner and then slowly lift the rest of the finger.
9. The finger should now have a distinctive fingerprint.
10. You can handle the finger in room temperature but be careful not to warm it too much as it will start to melt again.

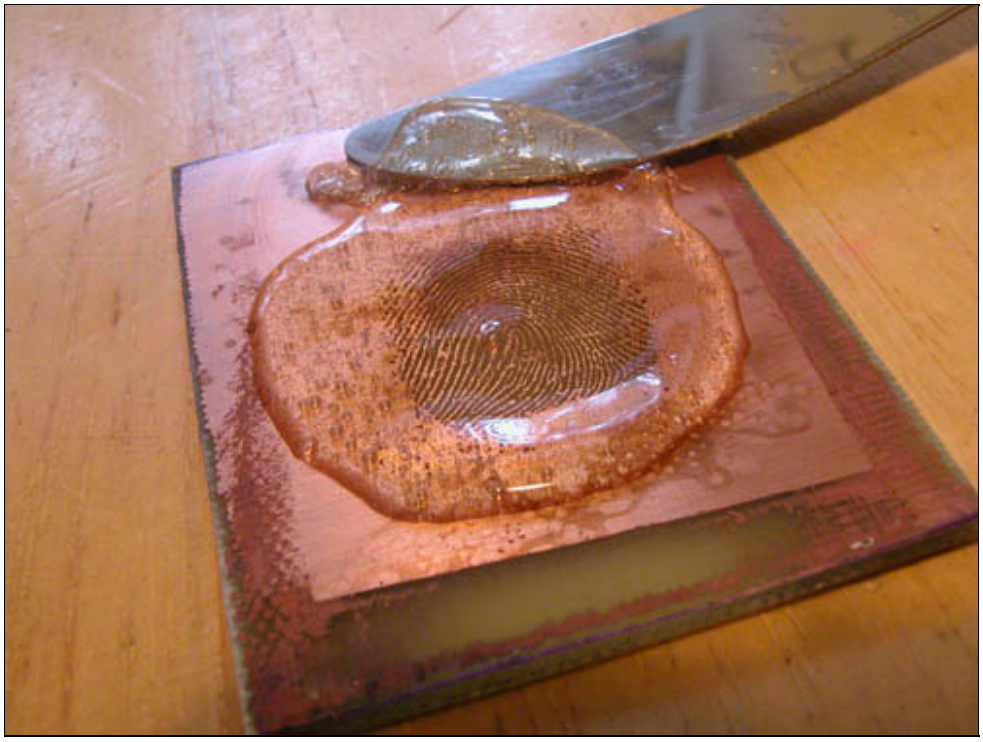

Fig3.6 - Gelatine spread on the board as a thin layer.

5. The usage of the finger:

1. You should now have a gelatine finger that feels like a soft real finger.
2. Ensure the smart card is inserted into the reader.
3. Wait for the login screen to prompt for the finger.
4. Place the gelatine finger on the tip of you finger.
5. Gently press the gelatine finger on the scanner.

5. Gently press the gelatine finger on the scanner.
6. If you press too hard you will get "Finger is too wet" error. Too light and the "finger" wont be detected.
7. If you continually get "Finger detection failed!" then it is adviced to stop trying after about 5-10 tryouts (exact amount is not known) or you will get the smart card locked and thus increase the risk of getting caught. Try again after the legitimate user has succesfully logged on one time. This will reset the fault counter.

Fig3.7 - Press the gelatine gently on the pad with the finger.

This hack is based on the fact that gelatine finger has about the same capacitance as a real finger (~20Mohms/cm) and thus the scanner is unable to distinguish these two. Now all that is needed is a gelatine finger that corresponds to the real finger at an accuracy level of the scanner. For the 100 SC scanner this resolution is 500dpi, each dot representing a small point for measuring the capacitance. If capacitance is high, then at that point there is a ridge, if small, there is a valley of the fingerprint. There is a certain kind of circuit in the scanner of which voltage output depends on the capacitance on the scanner surface. Therefore the voltage in the ridge area is different from that in the valley area. This way the scanner can obtain the characteristics of the finger.

When the gelatine finger is pressed against the scanner's pad, the ridges touch the surface and the valleys stay intact. Now the scanner measures the capasitance between it's matrix of dots and creates an image of the fingerprint. An intelligent heuristic is used to detect typical charasteristics for each unique fingerprint.

4. Detection and tracing

This hack is very difficult to detect. If the intruder does not get caught redhanded, the only way to detect this kind of attack is to notice the damage afterwards. A data burglar could dust for fingerprints anywhere and wait for an opportunity to attack a scanner. Tracing is very difficult. If there was a log-file on the users logins, you might find some information about the break-in (e.g. the time). Surveillance cameras might catch the data burglar on tape or some person could just as well see the man in action. But there are no any "real" ways to track the intruder down, because the break-in is done on the subjects own computer. The things used in the break can be disposed easily (thrown in garbage, melted or even eaten), so even if the burglar is caught there might be no evidence left.

5. Protection against the Attack

There are no any fool proof ways to protect against this attack. If you are not wearing gloves all the time, you leave fingerprints everywhere for evil intruders to duplicate. To diminish the probability of a succesful break-in is to use a smart card protection for the scanner (and keep the card apart from the scanner when not used). This way the databurglar has to obtain both the smartcard and a copy of the users fingerprint. Another way to make things difficult is to use several fingers in the authentication. Then to break in to the system the breaker needs more than one print, which is more difficult to get especially when the authentication is done using fingerprints from different hands.

6. Test results

The test was succesfull (security was compromised)

The test was successful! (security was compromised)

The real fingerprint was obtained from the side of mug using the technique described above. Though the successful test rate was not that high, only a few times out of a hundred the scanner detected the finger correctly. Vast majority of the recognitions ended up in a false fingerprint. This means that the scanner thought there was a finger but it was not interpreted as an authorized finger that is enrolled onto the smart card. This fact itself has a very positive side too (from the hacker's viewpoint) as it tells that the mold just needs to be done with a higher quality. So how to make the procedure better:

- Use professional fingerprint duster kit to get better image of the fingerprint
- Take your time to manipulate the image so the printed transparency is top quality
- Use lower dilution when developing the circuit board. This will leave a better layer for the corrode-phase

Even though this process is time consuming and complex it is much more usable technique than hack 2 (Using a live finger to create a mold). This way the hacker can obtain everything needed by himself (excluding the smart card) and operate in privacy when creating the mold itself. If the data on the computer is very valuable then this method is still very cost effective and worthwhile. Total time for the hack taken is about 3-5 hours with preparation. (Without hunting the usable fingerprint and waiting for the right time to attack.)

This hack is probable to work on a wide variety of different scanners even though they are not tested. Precise Biometrics 100 SC gave the feeling of a quality scanner as it was sometimes giving a hard time even for the legitimate user. This is due to strict marginals in finger humidity, temperature and pressure settings set by the vendor. There is no apparent reason why the technique that was used would not work on other scanners also.

Back to index