Hacking Biometrics

Fooling A Fingerprint Scanner 2/3: Creating an artificial finger using the actual finger

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 humanbeing has a unique pattern of ridges and valleys on their fingertips. A scanner makes 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 some of these special points can be seen. 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 these characteristic points of the user's fingerprint on the smart card. The method the scanner uses to to obtain those points is explained in section 3.

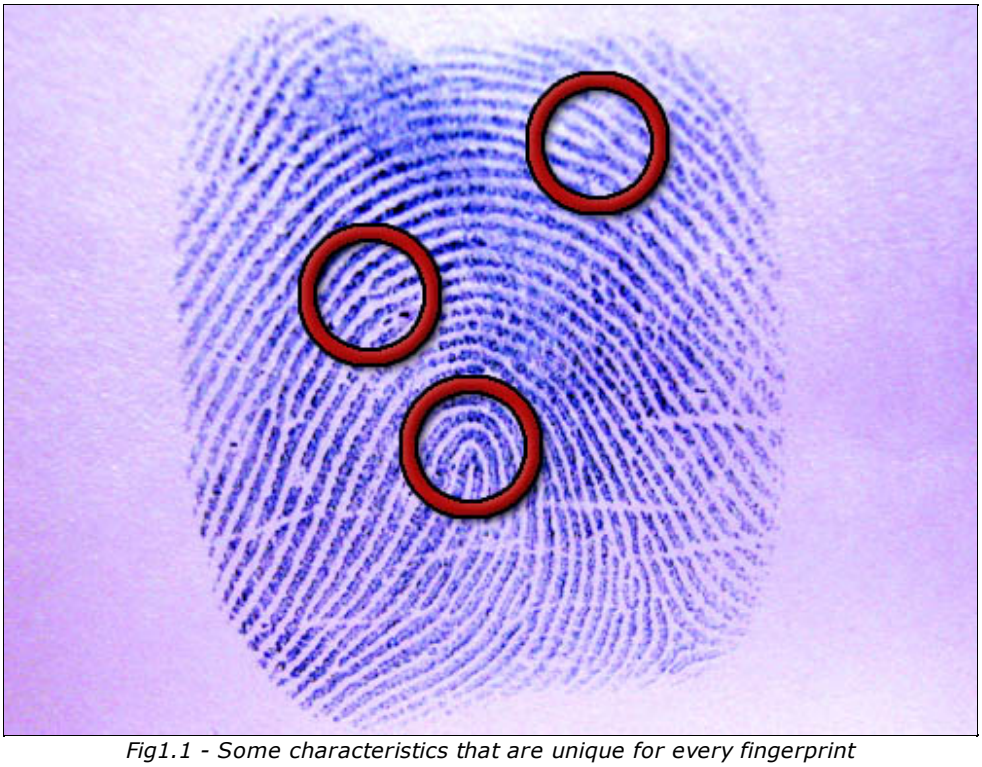

Fig1.1 - Some characteristics that are unique for every fingerprint

The hack is to create an artificial finger using a mold that is manufactured using the legitimate user's actual finger. This type of attack is not really usable in real life as people are usually wise enough not to give their fingers as a mold material. However, this hack demonstrates that the scanner can be fooled using a gelatine finger instead of a live finger and can be taken further in technology as is shown in the biometrics hack 3, "Creating a mold using a latent fingerprint".

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

If of 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 priviledges for the user to do whatever he wants, read and write data, send mail etc.

2. Preconditions for the attack

For this hack the attacker needs a legitimate user's live finger for creating the mold. Also some equipment and material is needed in the process.

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)
- Persuasive personality (AND/OR dumb user)

Things, materials and equipment:

- Live finger (enrolled to the smart card)
- Hot setting adhesive (One 100mm X 8mm bar per two molds) and a glue gun
- Gelatine leaves (40g gelatine + 1/2dl water ~= 20 fingers)
- Stowe, kettle, refrigerator

3. Analysis of the attack

The creation of the mold:

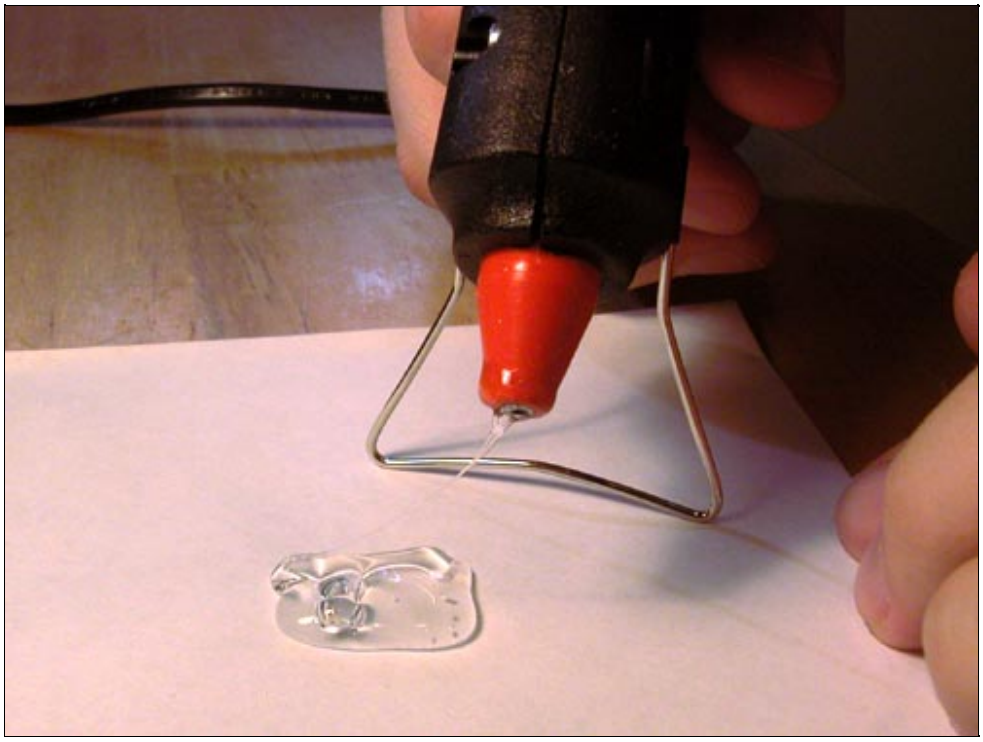

Fig3.1 - Hot setting adhesive (hot glue) gun

1. Heat up the glue gun.
2. Spread glue on a piece of paper (About the amount of one tablespoon).
3. Let it cool off slightly. Heated glue can be near 200°C!
4. Test the temperature *under* the paper using a finger.
5. When you can touch the glued area without *extreme* pain the glue is cooled off enough.
6. Moisten your finger a bit by breathing onto it or by dipping it into water and then dry it up a bit.
7. Gently press your finger in the glue. It should make a mold without excess pressure. (Too hard and the fingerprint spreads too much, too little and the print is not visible enough.)
8. Slowly lift your finger after the glue has cooled down more. (About 1 minute.)
9. Let the mold cool down to room temperature
10. You should now see the fingeprint clearly and the lines of the print should be distinctive. Watch out for any bubbles in the surface of the mold.

Fig3.2 - Gently press your finger in the glue

The creation of the finger:

Fig3.3 - Pour gelatine on the mold so that it covers the print completely

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 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.

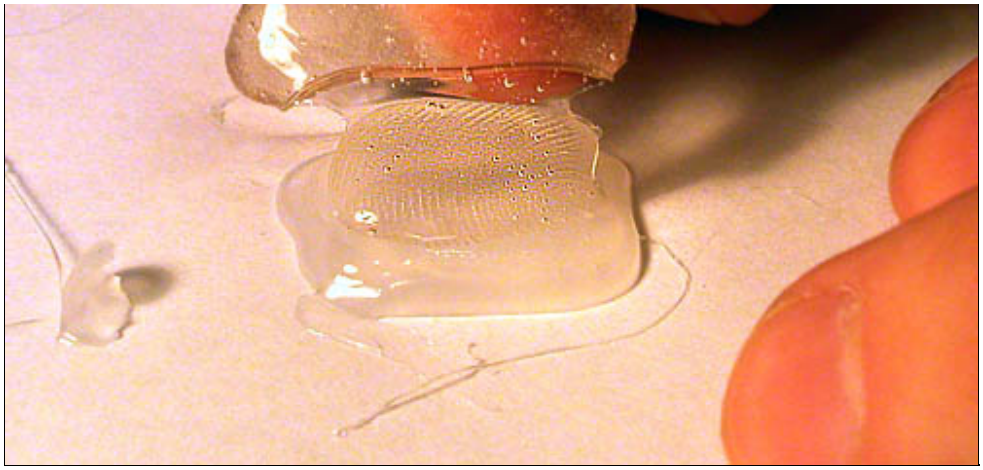

Fig3.4 - The congealed gelatine must be carefully separated

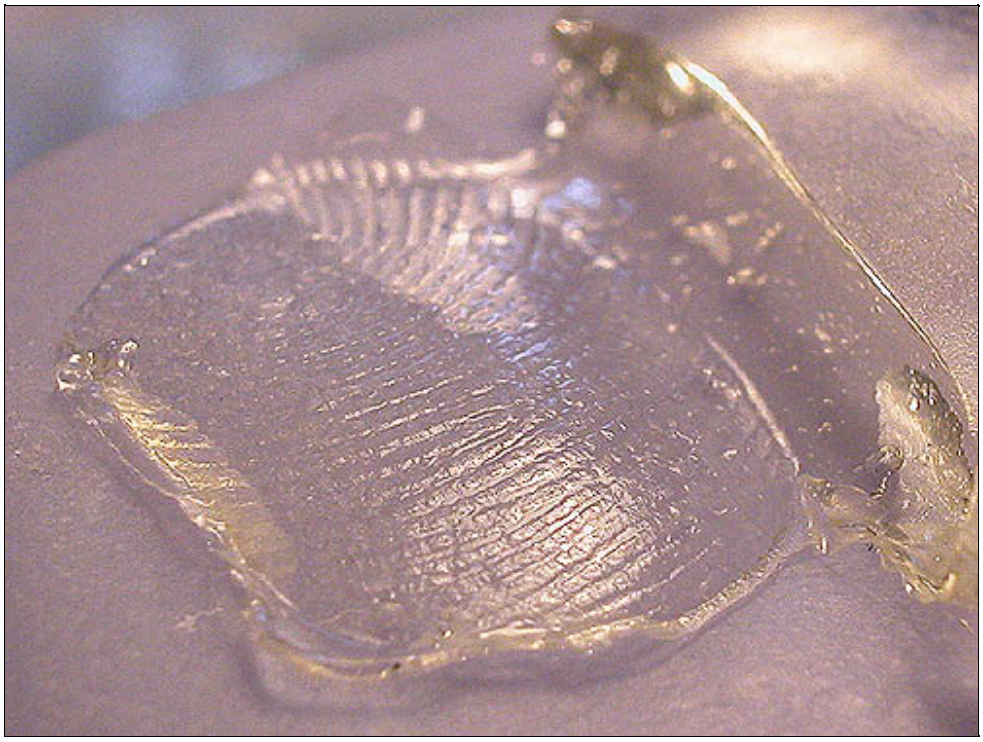

Fig3.5 - A ready gelatine finger

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 your finger.
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.

Fig3.6 - Press the gelatine gently on the pad with a 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 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 can be quite easily detected by the user whose finger is being copied. A person planning to break into a system using a fingerprint scanner should have a very credible story to convince someone to stick his or her finger in hot glue. If someone could get a mold without the subject's perception, it would be very difficult to trace a break-in using the phony finger. 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 just as well some person could 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 (throw in garbage, melt or even eat), so even if the burglar is caught there might be no evidence left.

5. Protection against the Attack

The easiest way to protect against this attack is to avoid giving a mold of your fingers. To diminish the probability of a succesful break-in is to use a smartcard protection for the scanner (and keep the card apart from the scanner when not used). This way the data burglar has to obtain both the smart card and a mold of the users finger. 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 mold, which is much harder than getting just one mold by fluke.

6. Test results

The test was successful! (security was compromised)

The break was succesful when using hot setting adhesive (hot glue) to produce the mold and gelatin leaves to make the fingerprint. The test rate was not very high until proper mold was made and a good technique to do it was learned. The key to success is to make a finger that is thin enough to lay evenly flat on the scanner's pad.

How to make the hack work best:

- Use a thick gelatine solution.
- Try to reduce the amount of bubbles in both the mold and the finger.
- Use more than one mold to create different fingers, then you will see what type of mold works the best for you.

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