Hacking Biometrics

Fooling A Fingerprint Scanner 1/3: Using grease stains on the scanner

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.

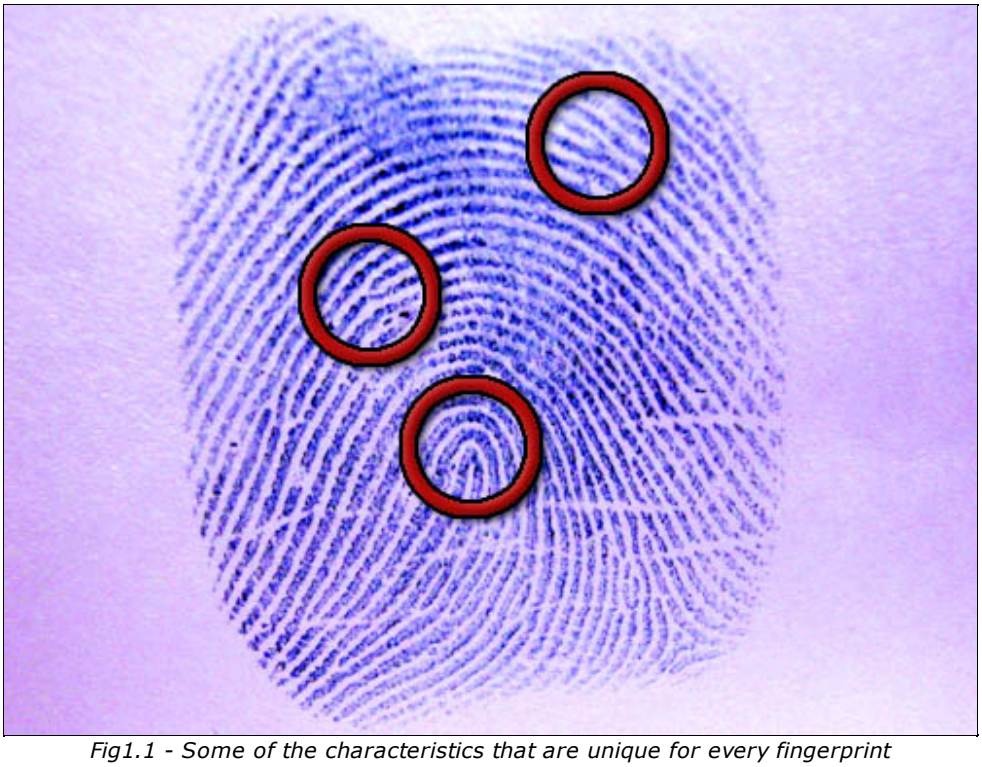

Fig1.1 - Some of the characteristics that are unique for every fingerprint

The hack itself is to re-use grease stains on the fingerprint scanner left by the previous user. Typically, a human finger contains so much grease that it leaves a non-visible mark where it touches and thus usually leaves a clear mark also on the scanner. This stain can be brought visible in many ways and even a mere breathing can show the print very clearly. 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 priviledges for the user to do whatever he wants, read and write data, send mail etc.

For this hack no specific tools are needed.

Fig 1.1 - Precise Biometrics 100 SC Smart card reader and fingerprint scanner

2. Preconditions for the attack

For using this kind of vulnerability one needs to have a clear grease stain left on the surface of the scanner. This stain has to have most of the important charasteristics of the fingerprint left on the pad so that the scanner can reliably read the same line-ends and curves that it detected on the previous user. Also for this specific scanner a smart card is required (i.e. user forgot it to the scanner).

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
- Applicable fingerprint stain on the scanner's pad left by the previous user.
- Temperature between 0-50°C (Scanner operating temperature)
- For the gummy bear attack also a gummy bear or some other jelly material (i.e flat gelatine square) is needed.
- Some privacy and a lot of perseverance

3. Analysis of the attack

For capasitive scanner the visibility of the fingerprint is not the case but it helps the intruder to see whether there is a fingerprint stain on the pad and how usable it is.

Fig3.1 - A fingerprint scanner showing the grease stain

Method 1: Moist Breath
The idea behind this scheme is to breathe gently on the surface of the scanner and produce substance that has enough capacitance to fool the scanner. As the small water particles hit the pad the grease stain left on the surface does not hold them but the moist gathers up in between the small stained fingerprint lines. This could be enough so that the scanner can measure the capasitance and faultily think that there is a finger.

How to hack it:

1. Ensure smart card is inserted.
2. Wait for login screen to prompt for finger.
3. Gently breathe at about 5-10cm distance onto the surface of the pad.
4. Try to control the amount of moist by breathing longer or shorter periods. The device will inform you that your "Finger is too wet" if you breath too much or too long.
5. 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 one time. This will reset the fault counter.

Method2 : Gummy bear
If the breathing does not work a gummy bear is to be used to represent a finger. This jello candy has nearly the same capacitance as a finger's skin (~ 20 Mohm/cm) and can be soft enough to be placed evenly on the pad and still retain the stain in form. This can also help if the device constantly informs that "Finger is too wet" as it contains much less water than moist breath.

How to hack it:

1. Ensure smart card is inserted.
2. Wait for login screen to prompt for finger.
3. Gently press the gummibear against the pad. Be careful not to ruin the stain.
4. Try to control the pressure and keep gummibear evenly flat against the pad.
5. If you press too hard you will get "Finger is too wet" error. Too light and the "finger" wont be detected.
6. 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.

Both of these techniques are quite hard to land into a successful hack. They require very much of skill and training, which makes them obsolete for a casual hacker. However, if you have access to your own scanner, you *might* be able to train yourself into a successful gummy bear hacker in a matter of just a few years ;)

The scanner used (100 SC) uses a capacitance measurement method. The pad consists of small measurement units or condensators making up a matrix at 500dpi. Each unit can measure the capacitance at that point. 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 an image of the fingerprint and use a heuristic to solve the characteristics of the finger.

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. The intruder could lurk around the subject with a bag of gummy bears or rehearse breathing. Tracing is very difficult. If there was a log-file on the users' log-ins, 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 subject's 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.

Protection against the Attack

The best way to protect against this attack is to wipe the scanner after use. To be overcautious against this attack one needs to keep the card apart from the scanner when not used. This way the data burglar has to obtain the smart card and the user must leave a stain on the scanner. Another way to make things difficult is

to use several fingers in the authentication. This way it is impossible to use one stain on the scanner to pass two different fingerprint checks.

Modifications to equipment that might help:

- Live finger detection (pulse, sugar level etc.)
- Small flap or cover over the pad that closes and clears the surface automatically after detection. Or at least scrambles it a bit.

Test results

The test was unsuccessful (security was not compromised)

Despite the furious attempts and hours of work, all that was achieved was hands full of nothing. The used scanner obviously has a heuristic for detecting this scheme as it constantly gave "Finger is too wet" error. The gummy bear technique gave a bit better results as there were also a few "Finger detection failed" errors. This means that the device was able to read the "finger" but it was not detected as the original finger corresponding to the data stored on the smart card.

Overall the test failed as no break-in was achieved and security was not compromised at any situation. However, the authors still believe, that with a good stain and a proper material found to resemble the finger, the gummy bear method might work in trained hands.

Back to index