

Fooling Fingerprint Scanners - Biometric Vulnerabilities of the Precise Biometrics 100 SC Scanner

Antti Stén, Antti Kaseva, Teemupekka Virtanen

Telecommunication Software and Multimedia Laboratory
Helsinki University of Technology
{antti.sten, antti.kaseva, [teemupekka.virtanen](mailto:teemupekka.virtanen@hut.fi)}@hut.fi

ABSTRACT

This paper looks into the security of fingerprint scanners. To do this, an example device is chosen and some attempts to break its protection are made. We analyzed some vulnerability and then three different ways to exploit these safety risks are studied and tried out. The scope of the tests is limited to fingerprints, leaving hard- and software attacks aside. At the end there are some notes about defending against these attacks. With very simple tools we managed to fool a scanner a few times out of a hundred. With more sophisticated equipment the percentage is probably higher and the result shows that fingerprint scanner alone is not, without any other security measures, secure enough to protect valuable assets.

Keywords: Fingerprint scanner, Biometrics, Authentication, Vulnerability.

INTRODUCTION

Ever since computers became containers for valuable information it has been a great task for engineers to figure out a way to secure data against thieves. Different authentication methods can be divided into three categories (Feltin, 2002): something you know (password), something you have (key, smart card), and something you are (biometrics).

In the recent years an old technique for identifying a person using fingerprints has taken a major step as it has become possible to digitize fingerprints. Fingerprint scanner is a new technology and it has made its breakthrough in the PC environment during the last few years. In the same time the technology itself has evolved to become more reliable and accurate. The scanners are used to log into operating system, replacing password authentication but many other applications are also known to consider fingerprints as an authentication method, automotive industry for one. When fingerprints and their automatic recognition are trusted in more and more areas the reliability of these systems becomes more important.

This paper gives a description about possible vulnerabilities of fingerprint scanners. The fingerprint authentication is based on the fact that everyone has an own unique fingerprint. But just like keys to your house, fingerprints can be copied and used by an unauthorized person. The procedure of such reproducing is studied and analyzed here. It becomes clear that with a little effort a fingerprint scanner can be fooled. Obviously, more effort must be put to improve the scanners before we can say goodbye to passwords.

FINGERPRINT SCANNERS

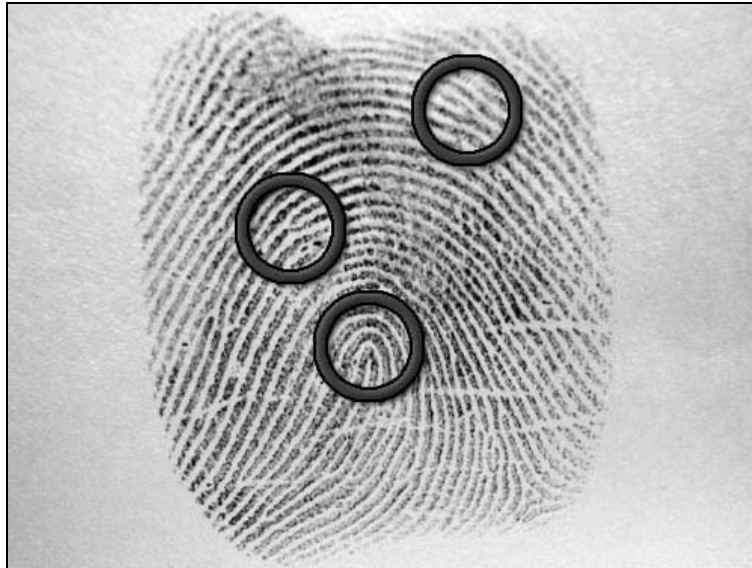


Figure 1 – Special points unique to every fingerprint

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 the 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 can be seen some of these special points. These points can be used as coordinates to navigate on the print. The scanner could, for instance, count the ridgelines between two special points or define locations of other characteristic points relative to the stored special points. This way the fingerprint generates a special kind of *'password'*, which can be used in authentication just as well as a 'normal' password.

Basically, there are two kinds of scanners: optical and capacitive. The optical scanner works in the same way as digital cameras. In the scanner, there is a matrix of photo sites (light-sensitive diodes). This composition is called *charged coupled device* (CCD). The diodes in the CCD produce an electrical pulse corresponding to the light it has received. When the finger is placed on the scanner, it illuminates the finger and thus gets an image of the print (the ridges are light and the valleys are dark).

The capacitive scanner has a more materialistic approach. It measures the capacitance in different points on the scanner. If capacitance is high, then at that point there is a ridge, if small, there is a valley of the fingerprint. There is a circuit in the scanner whose 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. For more information see (Harris, 2002).

TESTED VULNERABILITIES

Hardware and General Preconditions

The hardware used in the tests consisted of a fingerprint scanner made by Precise Biometrics (precise, 2003), a typical laptop and a valid smart card for the scanner. The scanner is based on capacitive measurement. It is an USB connected device and has a smart card reader/writer, which it uses to store the fingerprint characteristics and Windows logon information. Although these properties give a

broader scale of possible attacking points, only biometric interfaces are taken into tests and analysis to make the scope narrow enough and more generic approach for other capacitive scanners also.

Method 1: Using Grease Stains Left on the Pad

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 breath can show the print very clearly. The scheme is to use this stain by breathing on the scanner and making the scanner think that there is a live finger pressed against its pad. A variation of this idea is to use a finger-like substance that has a flat surface and press it against the pad leaving the grease stain under it.

Grease is also known as a method of lubrication and corrosion guard. This is based on the fact that grease rejects water and that it is not a very good conductor. When there is a grease stain left on the surface of the pad, it can be used to prevent water or moist breath attaching that point. Water on the other half has a decent conductance and approximately the same capacitance of the skin. When we breathe, the moist gathers up in the valleys of the fingerprint and makes an inverted duplicate of the finger. Despite this inversion, the relations of the characteristic points are the same as in the enrolled fingerprint and so it could be detected as legitimate user's print.

When substance (e.g. gummy bear (Leyden, 2003b) is pressed on the scanner's pad, the grease stain isolates the material from the pad and capacitance is measured at the same points as by breathing on the scanner.

In our tests, either of the techniques described did not work in the way they were supposed to. The scanner was very picky when detecting a finger, even with a live enrolled finger it was occasionally hard to log in. For the breathing, the scanner notified "Finger is too wet" and for the gummy bear attack there was also the "Invalid finger" error presented.

Method 2: Creating a Mold Using a Live Finger

Some typical household items carry the properties of a real finger when it comes to capacitance, conductivity and flexibility. One of the easiest ways to imitate human finger is to create a gelatine finger from gelatin sheets or powder. When using a mold, this material can be formed into a shape of the legitimate user's finger. The mold itself can also be manufactured using equipment commonly available, such as hot setting adhesive.

This method 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 the 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.

First, the mold must be created. In our test we used hot glue. It is important to stick the finger in the glue when it is still liquid but not too hot. It is a good idea to moisten the finger beforehand. After the mold is ready and cooled down, some liquid gelatine is poured on it. To get the best result, it is advised to use gelatine sheets mixed in hot water. Boiling should be avoided to reduce the amount of bubbles. After the gelatine is congealed (to speed up the process, the mold with the gelatine on it, can be cooled down in a refrigerator), the fake finger is ready to be used. Same rules apply here as it did with the gummy bear; the right amount of pressure must be found.

This method was proven to be successful and thus security was compromised. After several tryouts and many trial-error experiments a suitable way to manufacture a usable mold was found. As a result, we were able to create a fake finger that was used to fool the scanner. The result is not a hundred percent proof solution as only few times out of hundred ended up in a successful detection of the

finger. With this success rate it is not easy to go and break into someone's computer, because after a few failed detections the scanner locks the smart card and PUK-code is needed to unlock the card.

This method is not very usable for real life situations, as it needs a live finger for the mold creation. Though this method is further developed in the next method and thus brought into more usable form. Yet, it shows that a fingerprint scanner can be fooled with a pretty simple scheme and a very low budget.

Method 3: Creating a mold using a latent fingerprint

The most usable and also the most probable form of attacking a fingerprint scanner is by using a real fingerprint left by the legitimate user. Now that security of the scanner has been compromised, it is time to try preparing the mold without any help from the target. Typically we leave fingerprints anywhere we touch, mugs, door handles, stair rails and of course keyboards. These latent prints can be brought visible and then used to make a mold and a fake finger. The creation of the mold is different than in the previous attack, but the usage of the finger follows the same path.

Fingerprints consist mainly of grease and are usually latent but with e.g. photocopier powder they can be made visible. With a digital camera a visible fingerprint can be ported to a computer and retouched to a suitable form. Using a technique that is widely used with do-it-yourself circuit boards, a negative image of this fingerprint is printed on a transparency. A photosensitive layer of lacquer is applied to a copper plated circuit board and transparency is placed over that. When UV-light hits the surface, the black-printed areas of the transparency protect the lacquer and the rest react with the light. After a few minutes the lacquer is washed off with a lye dilution and a fingerprint should be visible on the circuit board. Now this board is corroded with ferric chloride and the result is a flat mold of the fingerprint. Gelatine liquid can be poured on to the mold as a thin layer and after congealing we have a fake finger. This finger is used between an intruder's finger and a fingerprint scanner. A fake finger is placed between the pad and a human finger in order to fool the scanner.

Compared to method 2 where a live finger was used to create a mold, this approach 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.

First, a clear and flawless picture of the target's fingerprint must be obtained. The fingerprint must of course match the finger that is enrolled to the smart card. When a suitable print is found a good way is to use photocopier powder to dust the print visible and then use a digital camera to take a snapshot of it. It is important to make some measurements to get the scale of the print correct, i.e. measure the distance between two characteristic points.

Making of transparency step-by-step:

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. Invert the image to negative.
6. Print the image on the transparency.

The making of the mold step-by-step:

1. Spray the photosensitive 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.
4. Take off the transparency
5. Develop the lacquer using NaOH-solution. Use watercolor brush to brush the lacquer. Be careful not to rub off all the lacquer.
6. When you see the fingerprint, wash the board with water.
7. Corrode the board using FeCl₃-solution.
8. Once the copper is corroded off, wash the board thoroughly with water.
9. Use soap or alcohol to rinse any remaining lacquer off the board.

The creation of the finger:

1. Soften 40g of gelatine sheets in cold water for about 5 minutes.
2. Heat up the water (1/2dl) to boiling and take the kettle off the stove.
3. Put the softened gelatine sheets into the hot water. Be careful not to boil them.
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. About 2mm is a good layer thickness.
7. Put the mold in the refrigerator and let it congeal 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.



Figure 2 – Gelatine spread on the board as a thin layer

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 advised to stop trying after about 5-10 tryouts or you will get the smart card locked and thus increase the risk of getting caught. Try again after the legitimate user has successfully logged on one time. This will reset the fault counter.

This technique was proven to be successful and security was compromised although the success rate was not that high. Only a few out of a hundred tryouts ended up in a successful detection of the finger. But this is not a bad sign. It merely shows that the break-in can be done and improved. The most critical part of the mold manufacturing is the transparency creation. It takes a skilled image manipulator to create a usable fingerprint if the print itself is not of a very high quality. With a professional dusting kit the fingerprint is probably much better than with a photocopier powder. With a good mold this method could be extremely effective.

All this can be achieved within one day and thus the attack is not very expensive considering the time used. If the contents of the target computer are very valuable, then this method can be very usable indeed.

INTERPRETING THE RESULTS

In the light of the tests done, it is shown that fingerprint scanners do not provide a completely secure way to authenticate a user although together with the smart card and PIN it can be quite good indeed. The protection that only a fingerprint would give is not sufficient at all.

The first method implicates that the 100 SC scanner can detect when there is a material that does not have proper ridges and valleys in it, such as a real finger would. The breathing technique failed probably because the moist breath spread all over the pad, whereas, a real finger would have made only a round circle. In either case the stain was probably not voluminous enough to have the desired effect.

The other two approaches show that the security of the scanner can be compromised with a fairly low effort in a usable way. In our tests the rate of successful logins with the phony finger was rather low. Only about one out of fifty attempts succeeded, but still a great danger lies beneath these results. It is only a question of how much effort is put to the fake finger manufacturing. The better the mold, the better the results are. Possible improvements are using a circuit plate with thicker copper plating, measuring the gelatine dilution for capacitance and adding e.g. salt to it or a better fingerprint dusting method.

There is always room for improvement in the scanner. The scanner can test the finger in many ways to make sure that it is a real and live finger detection could be used to make it harder to make a phony finger that passes the test (test for pulse, sugar percentage etc.). A relatively simple way to increase protection is to define a number of failed attempts before the scanner locks the users account. Something between three and ten could be a reasonable amount.

Some minor changes can also increase the safety significantly. A simple flap or cover over the scanning surface can scramble the grease stain left on it. To require multiple fingerprints in authentication prevents the re-use of the grease stain. It also decreases the probability of a successful reproduction of phony fingers (since there are more prints to produce).

Some other basic ways to defend against these attacks is to avoid giving your prints for molding, not to forget the smart card in the device, and keep an eye on possible fingerprint hunters (with a little help from guards and surveillance cameras). Particularly interesting fact is that user leaves his fingerprints just about everywhere and on to just about anything, including the smart card and the scanner itself. The case covering of the Precise Biometrics scanner is good in the way that it does not gather prints due to its matte surface. Instead the smart card has a glossy surface, thus being an excellent place to look for fingerprints. This is very crucial as the card and fingerprint should be kept apart.

CONCLUSIONS

We made three attacks against a fingerprint scanner, two of which were more like testing an idea. The third one was a real attack. Using simple equipment, we managed to pass a fingerprint authentication in 2 % of the tries.

The tests done show that a fingerprint scanner does not provide the ultimate protection and it cannot be trusted to guard a system by itself. As is the case with the tested 100 SC scanner, the additional security comes in the form of a smart card that is required for every action. The fingerprint scanners are typically used to replace passwords that users are unable to remember and, thus, write them visible somewhere. Even so, the scanner can be set to a mode where it asks the user for the card's PIN, whenever it is used. This type of protection fulfills all three types of authentication, something that you own (card), something that you know (PIN) and something that you are (fingerprint).

With the additional protection features, this scanner gives a pretty good level of security for a typical user. This type of fingerprint scanner is not meant to protect a highly valuable computer all by itself.

For instance, a malicious user can steal a laptop and then read the contents of the hard drive without any difficulties. So the fingerprint protection in this case is suited for preventing “in and out” – intruders that merely log on to the computer, do their business and leave. Also the smart card and USB-interface provide more commonly known access points for break-in attempts that are not covered here.

With all this in mind, fingerprint scanners cannot be thought as password replacements or a silver bullet to security. Rather, they can be considered as additional security items by making it easier to improve safety a bit.

REFERENCES

Precise (2003) Precise Biometrics 100 SC scanner data sheet [Referenced 25.03.2003], Available: http://www.precisebiometrics.com/data/content/DOCUMENTS/12112002_171152_619122Precise_10_SC_web.pdf.

Thalheim, L., Krissler, J., Ziegler, P. (2002) Body Check. *c't heise online*. 11/2002, page 114 [Referenced 04.02.2003]. Available: <http://www.heise.de/ct/english/02/11/114/>.

Leyden, J. (2003) Biometric sensors beaten senseless in tests. *The Register*. 1/2003. [Referenced 04.02.2003]. Available: <http://www.theregister.co.uk/content/archive/25400.html>.

Leyden, J. (2003b) Gummi bears defeat fingerprint sensors. *The Register*. 1/2003. [Referenced 04.02.2003]. Available: <http://www.theregister.co.uk/content/55/25300.html>.

Feltin, B. (2002) Information Assurance Using Biometrics, Global Information Assurance Certification (GIAC) Program. 6/2002. [Referenced 04.02.2003]. Available: http://www.giac.org/practical/Bryan_Feltin_GSEC.doc.

Schneier, B. (1998) Crypto-Gram Newsletter. Biometrics: Truths and Fictions. 8/1998. [Referenced 04.02.2003]. Available: <http://www.counterpane.com/crypto-gram-9808.html#biometrics>.

Schneier, B. (1999) Counterpane Labs. Biometrics: Uses and Abuses. 8/1999. [Referenced 04.02.2003]. Available: <http://www.counterpane.com/insiderisks1.html>

Harris, T. (2002) HowStuffWorks: How Fingerprint Scanners Work [Referenced 4.2.2003]. Available: <http://computer.howstuffworks.com/fingerprint-scanner.htm>.

Anderson, R. (2001) Security Engineering. 1. p. Ch 3. Wiley. Canada. 612 pages. ISBN 0-471-38922-6.

COPYRIGHT

[Antti Stén, Antti Kaseva, Teemupekka Virtanen] © 2003. The author/s assign the AIWSC03 & University of South Australia a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to the AIWSC03 & UniSA to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.