Fooling Fingerprint Scanners

Biometric vulnerabilities of the Precise Biometrics 100 SC scanner

Helsinki University of Technology
Course Tik-110.452

2003-03-24

Antti Kaseva - Antti Stén

TEKNILLINEN KORKEAKOULU
TEKNISKA HÖGSKOLAN
HELSINKI UNIVERSITY OF TECHNOLOGY

Abstract

There are many ways to authenticate a user. Different methods can be divided in three categories [5]:

- Something you know (password)
- Something you have (key, smart card)
- Something you are (biometrics)

This paper gives a description about the vulnerabilities of fingerprint scanners. The fingerprint authentication falls in the third category, since everybody *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.

After the basics of fingerprints have been explained the vulnerabilities are analyzed. They are first explained in general and then three different ways to exploit these safety risks are studied. At the end there are some notes about defending against these attacks and how the attacker might get caught. The three ways studied here are explained more thoroughly in the report papers [1].

It becomes clear that even with little effort a fingerprint scanner can be fooled. Therefore most scanners today don't come even close to meet the safety requirements of an average corporation. Clearly more effort must be put to improve the scanners, before we can say goodbye to passwords.

Biometrics – Just another easy challenge for intruders.

Table of Contents

Introduction to Fingerprints and Recognition 3
Tested Vulnerabilities and Analysis 4
  Hardware and General Preconditions 4
  Using Grease Stains Left on the Pad 4
  Creating a Mold Using a Live Finger 5
  Creating a Mold Using a Latent Fingerprint 6
Detection and Defense 8
  Detection 8
  Defense and improvement suggestions 8
  The Risks of a Hacker 8
References 9

Introduction to Fingerprints and Recognition

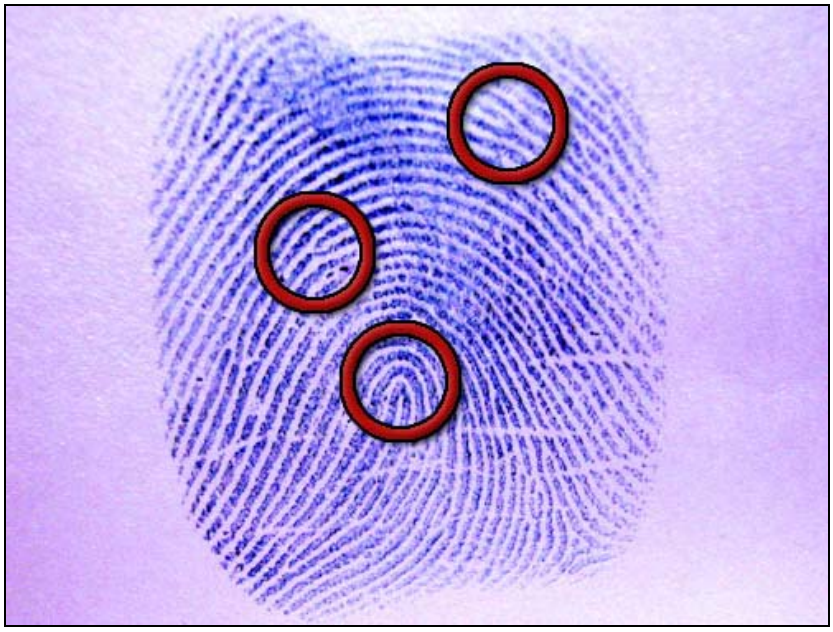

Figure 1 – Special points unique to every fingerprint

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 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 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 photosites (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 certain kind of circuit in the scanner 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.

For more information see [8].

Tested Vulnerabilities and Analysis

Fingerprint scanner is a new technology and it has made its breakthrough in the PC environment during the last few years. Even the technology itself has evolved in the couple of years to become more reliable and accurate. The scanners are nowadays usually used to log into operating system, replacing password authentication. This gives a titillating idea of hacking biometrics. Thus we decided to try to hack one of these devices and here are the vulnerabilities that were tested during the study and the analysis of the results.

Hardware and General Preconditions

The hardware used in the tests consisted of a fingerprint scanner made by Precise Biometrics (model 100 SC) [10], a typical laptop and a valid smart card for the scanner. The scanner is based on capacitive measurement, a technique described in detail in the chapter *"Vulnerabilities of Fingerprint Scanners"*. It is an USB connected and has a smart card reader/writer which it uses to store 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.

In a real life situations there are some preconditions that need to be satisfied before any of the tests can be executed. These are shortly described in the following chapters and found in more detail in the hack reports[1]. Also equipment needed in the tests and instructions how to execute hacks are described with more detail in the reports and it is advised to read the reports before reading this chapter.

Using Grease Stains Left on the Pad

The Key Idea

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 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.

Technical Background

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. Now, 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. As we breath, the moist gathers up in the valleys of the fingerprint making a somewhat duplicate of the finger. Only that it is the "negative image" of the finger's topology. Still, almost the same points are detected as a characteristic points in the fingerprint and so this could be detected as an enrolled finger.

The variation should do technically the same miracle. When substance (i.e. gummy bear [4]) 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.

Preconditions

For the hack to work, a hacker has to find a scanner with a proper stain left on it. For the 100 SC scanner a hacker also needs the smart card with the legitimate user's finger enrolled to it. A real life situation could be when a user leaves his desk for a minute and leaves his card into the reader. When the screen saver starts the user or hacker has to present a finger to gain access again. Other ways of obtaining the card is by stealing or by a mere fluke of finding it.

Test Results and Analysis

In our tests neither of the techniques described did not work in the way they were supposed to. The scanner was very picky when detecting finger, even with a live enrolled finger it was occasionally hard to log in. For the breathing the scanner reviled "Finger is too wet" and for the gummy bear attack there was also the "Invalid finger" error presented.

This implicates that the scanner can detect when there is a material that does not have proper ridges and valleys in it such as a real finger would have. 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 neither case the stain was probably not enough solid to have the desired effect. A user with a very greasy finger is a very unexpected event and in our tests logging on with a wet or greased finger the scanner failed to read the print.

All this implies that more sophisticated hacks are needed to penetrate the shiny surface of the scanner.

Creating a Mold Using a Live Finger

The Key Idea

Some typical household items carry the properties of a real finger when it comes to capacitance, conductivity and flexibility. One of the easiest way to imitate human finger is to create a gelatin 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 the most common equipment available to anyone, such as hot setting adhesive (hot glue).

Technical Background

Finger's ridges and valleys are clearly visible to human eye but they are not very distinctive when it comes to creating a mold. There are several types of materials that can be used to create a mold candidate but a few present truly capable properties for this hack. Plaster is usually too rough to copy a fingerprint completely, fine clay has a nasty habit of loosing its smoothnes when heated and suitable plastic is hard to come by. Our cunning idea of using hot setting adhesive started as a sideshow but soon became apparent that it was more than a good option. This adhesive is very hot (can be nearly 200 of degrees Celsius!) but after it cools down a bit it can copy the finger pressed against it with a very good detail. It also presents a good surface for gelatin as the congealed material is easy to detach from the mold. In addition it is a fast material to work with.

Preconditions

For the hack to work, a hacker needs to find a user that is dumb enough to give his finger as a mold resource. Also the smart card is needed to access fingerprint scanner and to logon into Windows.
Some work and time is required to manufacture the fake finger using the mold.

Test Results and Analysis

The hack 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. Also the gelatin solution gave a few gray hairs when the perfect ratio and thickness was sorted out. 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 hack someone's scanner because after 5-10 failed detections (exact number is not known) the scanner blocks the smart card and PUK-code is needed to unblock the card.
This hack 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 hack 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.

Creating a Mold Using a Latent Fingerprint

The Key Idea

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. 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.

Technical Background

Our fingerprints consist mainly of grease. This grease stain is usually latent but with i.e. photo copier powder it can be made clearly visible. After that with a digital camera it can be taken into a computer and retouched. Using a technique that is widely known at Do-It-Yourself circuit board scene, 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. Gelatin 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 a hacker's finger and a fingerprint scanner. Fake finger sets on the pad just like a normal finger and fools the scanner.

Preconditions

In this hack a fingerprint is needed and it has to be in such a good conditions that all the key characteristics are shown well enough or can be repaired. Quite a long list of equipment is needed [1] along with the basics of chemical handling. Also the hacker has to know which finger he is hunting for. And probably the most important aspect, the hacker has to find his way to the computer itself. This might mean getting through the security check at the lobby.

Test Results and Analysis

This technique was proven to be successful and security was compromised though 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 hack 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. This is crucial for the hack to work. With a good mold the hack could be extremely effective.

For real life purposes this hack presents more challenging tasks than one might think at first. Firstly, the hacker needs to know which finger to hunt for so some spying is needed to obtain this information. Then a suitable fingerprint is needed and thus the legitimate user needs to be observed some more. After that some privacy is required to get an image of the print and some time is needed for the manufacturing of the mold.

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

Conclusions

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 (Passwords are proven to have many weaknesses [9]). Even so, the scanner can be set to 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 alone. For instance, a hacker can steal a laptop and then read the contents of the hard drive without any difficulties. So the fingerprints protection in this case is suited for preventing "in and out" – hackers that merely log on to the computer, do their businesses and leave. Also the smart card and USB-interface provide more commonly known access points for hack attempts that are not covered here.

Detection and Defense

Detection

Detection of this kind of attack depends highly on the damage done. If the intruder does not leave any obvious signs of break-in (such as forgetting the phony finger at the crime-scene) then the only real way to detect an intrusion is to notice some changes within the data on the computer. If there is some kind log of users logged in to the system, it can be seen whose ID is used to break the protection. Other than that, there are no practical ways to detect the break-in.

However, if the data burglar is amateurish, there are some trivial ways of detection. E.g. the person, whose finger is being copied with hot glue, can easily realize that something weird is going on. Just as well someone can find some powder on mugs and railings. This happens when the burglar forgets to wipe the stains left from dusting the fingerprints.

Also, because this kind of attack must be done at the computer to be hacked (because the authentication is done in place) it is possible to catch the intruder red handed.

Defense and improvement suggestions

There are a lot of ways to improve the safety of a fingerprint scanner. You can use a smart card protection on the scanner, so the device does not work unless a valid card is inserted. This way the burglar must obtain the card in addition to the valid fingerprint. 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. To use a capacitive detection rather than an optical increases the safety a bit. Live finger detection can be used to make it harder to make a phony finger that passes the test (test for pulse, sugar percentage etc.).

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 might be enough so it cannot be used again. 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 basic ways to defend against this attack is to avoid giving your prints for molding, not to forget the smart card in the device and keep on eye on possible fingerprint hunters (with a little help from guards and surveillance cameras).

The Risks of a Hacker

The highest risk for the intruder is to get caught in action. This is because the break-in must be done in place. Of course if the system allows remote login, this is not an issue. And if you are hunting and dusting for fingerprints in a public place, someone might see you and find it suspicious. Other than that, there aren't many risks afterwards (unless you are caught on surveillance camera).

There is a possibility that someone might find the equipment used to make phony fingers in the burglar's possession. This is small risk if the intruder is smart enough to dispose all related objects and keep a straight face when asked about it. After all, the equipment used in the hacks consist of commonly available items.

References

[[1] A Kaseva, A Stén. Hacking Biometrics, Fooling a Fingerprint Scanner. 03/3003, [Referenced 24.03.2003]. Available:
http://www.hut.fi/~akaseva/l337h4x0r/

[2] Lisa Thalheim, Jan Krissler, Peter-Michael Ziegler. Body Check. c't heise online. 11/2002, page 114 [Referenced 04.02.2003]. Available:
http://www.heise.de/ct/english/02/11/114/

[3] John Leyden. Biometric sensors beaten senseless in tests. The Register. 1/2003. [Referenced 04.02.2003]. Available:
http://www.theregister.co.uk/content/archive/25400.html

[4] John Leyden. Gummi bears defeat fingerprint sensors. The Register. 1/2003. [Referenced 04.02.2003]. Available:
http://www.theregister.co.uk/content/55/25300.html

[5] Bryan Feltin, 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

[6] Bruce Schneier. Crypto-Gram Newsletter. Biometrics: Truths and Fictions. 8/1998. [Referenced 04.02.2003]. Available:
http://www.counterpane.com/crypto-gram-9808.html#biometrics

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

[8] Tom Harris. HowStuffWorks: How Fingerprint Scanners Work [Referenced 4.2.2003]. Available:
http://computer.howstuffworks.com/fingerprint-scanner.htm

[9] Ross Anderson. 2001. Security Engineering. 1. p. Ch 3. Wiley. Canada. 612 pages. ISBN 0-471-38922-6.

[10] Precise Biometrics 100 SC scanner data sheet [Referenced 25.03.2003], Available:
http://www.precisebiometrics.com/data/content/DOCUMENTS/12112002_171152_619122Precise_100SC_web.pdf