Circumvention of fingerprint scanners

Tom Fladsrud (tom@fladsrudsolutions.com)
Roar Sollie (roar.sollie@hig.no)

December 15, 2004

Abstract

One critical issue regarding the protection of confidential information or valuable items is to determine the identity of a person. Biometrics is supposed to offer this security in a user-friendly and secure way. One problem however is that there are ways to compromise systems based on biometric verification. Some of these biometrical features have known vulnerabilities. Persons with similar facial characteristics, e.g. identical twins, can fool face recognition systems. It is also stated that identical twins have similar fingerprints due to the fact that they have fingerprints that belong in the same class [1].

In this article we study other experiments and literature, describing drawbacks of these systems and some ways to fool a fingerprint verification system. Based on this, we conducted some experiments to see if we were able to circumvent fingerprint sensors by making artificial fingers with co-operation of its owner. In the experiments we tried different methods to achieve good copies (artificial fingers) of our fingerprints, using these artificial fingers to circumvent the fingerprint sensors. The experiment was conducted with the use of NISlab's[1] Authentication Workbench at HiG[2].

Keywords: biometrics, fingerprint, artificial or dummy finger, experiment

1 Introduction

Authentication based on something one knows (passwords, PINs) or has (id badge, smart card), contains known problems such as; they can be shared, borrowed,

[1]NISlab- Norwegian Information Security laboratory with different authentication technologies connected to computers installed with an application, authentication workbench, software for testing various authentication devices.

[2]HiG, Gjøvik University College, Norway

stolen, traded or guessed [2]. Biometric systems are said to be convenient because they need neither something to remember (knows) nor something to carry (has). Biometric identification systems use personal features of the user itself to check the identity. If, for example, biometric features stored on a chip card are stolen, they can not be used because the impostors biometric features do not match the features stored on the card. Fingerprint recognition is technically easier to achieve than the use of traditional authentication methods like username and password, and it has a very good balance of all the desirable properties [3]. A fingerprint is very distinctive and its details are permanent. Authentication with fingerprints is also more accepted by the public than some other biometric authentication methods like iris and retina authentication.

Fingerprint sensors have become quite small and affordable, and have therefore become more widespread. Fingerprint authentication even appears to become feasible for wallets and others small sensors. As the market of fingerprint scanners increase, it is becoming important to ensure and evaluate the security of such devices. It is important to establish how easy it is for the average criminal to circumvent the devices and how much effort, knowledge and resources are needed. This is what we will try to assess in this project.

We have conducted an experiment producing artificial fingers, trying to circumvent the two available fingerprint scanners in NISlab. There are mainly two methods to duplicate fingerprints; with and without co-operation. Duplication of a fingerprint with co-operation of its owner is of course the easiest method since it is possible to compare the dummy with the original fingerprint on all aspects and adapt it accordingly. This is why we have chosen the method of duplicating fingerprints with co-operation of its owner, and because of the limited duration of this project. Due to the limited time of this student project and the fact that the project is conducted simultaneously with the preparation for the exams, it is difficult to locate volunteers willing to set aside the amount of time needed to attend the project. This is why we chose to run the experiment with only the two authors as participants.

2 Legal and ethical issues

Implementation of technology, especially biometrics, may result in sacrificing privacy rights in the name of security [4]. Due to terrorist and criminal acts, and the September 11 terrorist attacks, it is most likely that people are willing to sacrifice some degree of privacy for protection to achieve a higher level of security.

Biometrics is often compared to an Orwellian[3] process [4] that provides more compromise of individual privacy than protection. But is biometrics the destroyer of privacy? It is stated many times with technology, that the possibility of compromise depends largely on its implementation, and how the biometric data is stored. Data segregation of personal and biometric information should apply for biometric applications, especially those stored centrally. Strict controls would be required for these systems to protect against unauthorized use or leakage of information.

One disadvantage concerning this type of experiment is the risk of contributing to educate and inform criminals. However this kind of experiment will also influence and enlighten vendors in the development of new and more secure equipment.

2.1 Other aspects

Knowledge-based authentication, in the form of passwords, is most widely used. This despite of the fact that password have many known flaws. Secure and reliable passwords are usually hard to remember and the users often have several passwords for different systems. A consequence of this is that the users often forget the passwords, and therefore must reset the password, or that they have to write them down. This require an extensive support at a huge cost [5]. Using biometrics, such as fingerprint, rules out this problem.

Biometrics increases the security since the problem with weak passwords is avoided. Often such biometrics as fingerprints is combined with passwords, but does not require the same strength of the password as systems based only on password authentication. Further the use of biometrics prevents users from lending out their authentication devices. However there are also downsides using biometrics such as if the fingerprint is compromised there are no way of replacing it.

3 The rules of the competition

To establish the security of fingerprint scanners, we have conducted an experiment using artificial fingers trying to circumvent the fingerprint scanners. By doing this we hoped to be able to evaluate the security strength, using the False Acceptance Rate (FAR) of different fingerprint authentication devices, when using artificial

[3] Orwellian means the power of holding two contradictory beliefs in one's mind simultaneously, and accepting both of them.

fingers. Before this test could be executed we made some rules of the competition.

3.1 Rules

The test will be performed using NISlab's "Authentication Workbench v4.0.2" at HiG, with two different fingerprint sensors. All tests will be performed offline with the same population and in the same environment. Any adjustment to the devices and the environment for optimal performance must take place prior to the experiment [6]. In our experiments we use the default settings in the

This experiment involves time-consuming activities not suitable for participation of several volunteers. Fingerprint samples will be collected from a small group, consisting of the two authors. A potential expansion of the experiment includes volunteers. These will, in accordance with [6], have to sign a volunteer consent form that states the purpose of the experiment and where the volunteer consent to the biometric data being used for experiment purpose only.

We acknowledge that this delimitation would not make the experiment representative for the world population, but this is also not the intent of the experiment. The purpose of this experiment is to see how easy it is to fool a fingerprint system, and from that discuss the security strength based on how much time, resources, and knowledge and costs that is required for a successful attack.

3.2 Resources available to the adversary

In [7], attacks on biometric systems are grouped in eight sources of attack:

- Fake biometric at the sensor, such as a fake finger, a copy of a signature or holding a image in front of a camera used in face recognition authentication.
- Reply attack of digitally stored biometric signal, such as an old copy of a fingerprint image.
- Override feature extract, for instance by using a Trojan horse.
- Tampering with the feature representation.
- Override matcher so that it always directly produce an unnaturally high or low match score.
- Tampering with stored templates that could result in authorization of a fraudulent individual.

- Attack the channel between the stored template and the matcher and change the contents of the templates before they reach the destination.
- Override the result. For instance if the system returns access denied, the hacker overrides this and gains access. In this case, even if the performance of the recognition system were excellent it would will useless.

Schneier [8] additionally describes other abuses of biometrics such as the problem with humans leaving their fingerprints on surfaces, also called latent fingerprint, and that once the biometric is compromised there is no way of changing the biometric data.

Most of the attacks mentioned earlier require substantial knowledge and resources. The purpose of this project is to find out how little effort and knowledge is needed to be able to compromise the fingerprint sensor. An attack that is realistic to successfully accomplish in this context is the use of an artificial biometric at the sensor, for instance the use of an artificial finger that contains the fingerprint of a legitimate user.

There are two methods of obtaining the biometric data, with and without the help of the owner. A real attack situation would mostly involve non co-operative owners, which involves added time and resources for obtaining the biometrics. However, to avoid spending too much time on collecting the biometrics, and because of the legal issues involved in obtaining biometrics without the owners consent, we will base our experiment on the help of the owner of the biometric.

Due to the limited funds and time available for conducting this experiment we will use low cost equipment and the use of Internet for recipes [9, 10, 11]. See Appendix B for detailed list of equipment used.

4 Counterfeiting fingerprints

Based on a literature study and recipes found on the Internet, we have conducted seven different experiments making dummy fingers to circumvent the two available fingerprint sensors. These sensors are the capacitive fingerprint sensor "Biliionton FP reader", and the optical sensor "U are U DigitalPersona 4000" (Fig.1, see Appendix C for detailed information about the scanners used).

These sensors are connected to a computer in the NISlab environment. The authentication workbench used in NISlab lets us create and register a test person. This test person then enrolles the fingerprints, in turn placing the chosen fingers

Figure 1: "U are U DigitalPersona 4000" (at the top) and "Billionton FP reader".

on the selected fingerprint sensor. When we conducted the experiment, we used a function called "Quick Verify", to see if the dummy or attempt of fooling the selected fingerprint sensor succeeded. Then the workbench displays if the identification failed or was accepted, and the level of similarity.

After several attempts we discovered that it was difficult to both enroll and verify using a legitimate finger as well as an artificial finger on the capacitive reader "Billionton FP reader".

When conducting these experiments the participants must wash their fingers with soap to make the different substances flow more easily through the valleys of the print. This way the captured fingerprint is of best possible quality.

4.1 Experiment 1

Some fingerprint sensors described in the literature, are so bad that one can fool it by enrolling the actual fingerprint first and then breathe on it [12]. The breath is supposed to activate the sensor ones more using the latent fingerprint on the sensor, verifying the user last (recently) identified by the sensor. After several attempts, none of the sensors we used was fooled. Obtained FAR data on the "U are U DigitalPersona 4000" and the "Billionton FP reader" are 0 %. Time consumed for this experiment was five minutes and the cost was equal to zero.

An advancement of this experiment is the use of a plastic bag filled with hot water [12]. This plastic bag is then placed on top of the sensor to active the latent fingerprint of the previous captured user. The results of this scheme were the same as for the previous one.

4.2 Experiment 2

In a lecture in the Authentication course, we were introduced to a movie made by Frank Rosengart in 2004. This movie describes how he was able to make a dummy fingerprint using a latent fingerprint on a bottle. This fingerprint was made by Rosengart himself, which refers to the method of co-operation. However this method could also be used to obtain fingerprints of non co-operative individuals, i.e. from glasses in a restaurant. He made superglue evaporate on the latent fingerprint, making it easier to capture. He took a picture of this fingerprint using a digital camera, transmitted it to his computer, and used image processing to remove some noise in the picture. This picture was then printed out on a transparency, on which the printer made a mark of the fingerprint. He made a thin layer of glue on top of this fingerprint, waited till it was dry and then drew it off. This glue containing his fingerprint, was used to verify his identity, using a fingerprint sensor he had available.

Based on the method used by Rosengart we conducted an experiment using a ink pad to attain a good fingerprint with low level of noise. This fingerprint was copied on to a transparent, on which we placed a thin layer of glue and waited until it was dry. When we tried to pull of the glue, it was stuck on to the transparent and could not be taken off without getting stretched or broken. Thus the use of several types of glue and attempts, they all carried the same result; no visible or useable dummy fingerprint. Therefore we were not able to fool the fingerprint sensors. Obtained FAR data on the "U are U DigitalPersona 4000" and the "Billionton FP reader" are 0 %. Time consumed for this experiment was one hour at a total cost of 46 NOK.

4.3 Experiment 3, 4, 5 and 6

In experiment 3, 4, 5 and 6 we used modelling clay to form the fingerprint in four samples. We used four different substances to make the dummy fingerprint; adhesive glue, silicon, filler and wood cement (wood glue). When the samples had dried, we tried to separate the substances from the modelling clay. The problem in this process was that all the samples where stuck in to the modelling clay, such way that the fingerprints in the substances was covered by modelling clay. Therefore it was not possible to achieve any results from these experiments. Obtained FAR data on the "U are U DigitalPersona 4000" and the "Billionton FP reader" are 0 %. It took approximately two hours at a total cost of 135 NOK.

Figure 2: Dipping the finger in plaster

Figure 3: Dry the plaster with hair dryer

Figure 4: Take the mould off the finger.

Figure 5: Place silicon in the mould.

4.4 Experiment 7

[9] describes, step by step, how to create a wafer-thin silicon dummy of a fingerprint if the owner of the fingerprint is willing to co-operate. It is said that the method requires only a limited amount of time (a few hours) and limited means. We tried to conduct a similar experiment with some small modifications. Mainly, the modification is the way we make the fingerprint in the plaster, which consist of a repeatable process of dipping the finger in the liquid plaster and drying it with a hair dryer. The process is described in this sequence:

1. Beforehand, the finger should be washed with soap to make the plaster flow more easily through the valleys of the print.

2. Make a liquid plaster mixture in a bowl. Preferably the plaster should be of good quality, such as plaster available in hobby shops.

3. Dip the chosen finger in the plaster, and dry the plaster onto the finger using a hair dryer. Repeat this process until the fingertip is covered with a solid and strong plaster sample (Fig. 2 and 3).

4. When the plaster is dry, carefully remove the plaster from your finger (Fig.4).

5. A thin layer of silicon waterproof cement is placed in the mould, covering the inside of the mould (Fig.5).

6. When the silicon has hardened, the dummy should be carefully removed. Before use the artificial fingertip must harden to ensure ridges and valley from smoothing.

The whole process of making the mould took 20 minutes, after placing the silicon into the mould it took one hour until the silicon has hardened so that the dummy could be removed. When using the dummy finger for identification, the "Billionton FP reader" did not even register that the dummy was placed on the sensor, but when we tried the "U are U DigitalPersona 4000" we actually succeeded. The identification was accepted, and the fingerprint sensor also produced a similarity rate. When conducting the verification 20 times, the average similarity rate retrieved using the artificial thumb was 231.65 and 525.05 using the real thumb (see Appendix A for detailed results). All 20 attempts succeeded. Obtained FAR data on the "U are U DigitalPersona 4000" using this dummy finger is 100 % and 0 % using the "Billionton FP reader". Total cost for this experiment was 80 NOK.

4.5 Extended version of experiment 7

Due to the fact that this was the only experiment with successful outcome, we extended the experiment using several samples of artificial fingers. We made ten artificial fingers, five from each of us, from now on referred to as person A and B, to obtain FAR data. The artificial fingers from person A, resulted in an average similarity rate considerably lower than from person B (approximately 100 vs. 230). When taking a closer look at these artificial fingers, we notice that the person B has deeper valleys than person A, making his fingerprints easier to capture.

One of the artificial fingers was damaged during the process of separating the silicon fingertip from the plaster. This finger was not accepted by the recognition system, making the total FAR at 90 %.

4.6 Summary of experiments

The experiments were conducted using the default settings in "NISlab Authentication Workbench". Because the "Billionton FP reader" had no available information about the threshold, we had no option but to use the default settings. The "U are U DigitalPersona 4000" had a default similarity threshold value of 47, and it was possible to adjust this value to a minimum threshold of 22 or a maximum

threshold of 63. These similarity values for minimum, default and maximum settings refers to a FAR threshold of 0.1 %, 0.01 % and 0.001 %. A presentation in a DET curve or ROC curve would not be appropriate for the results obtained from these experiments because only one of the experiments contains FAR different from zero. However we believe that in this case an representation of the results in a table will give a better overview of the results. Table 1 summarizes the results of the experiments.

Experiment #	**# Attempts** B/U	**# false acceptances** B/U	**# false rejections** B/U	**% FAR** B/U	**% FRR** B/U
1	10/10	0/0	0/0	0/0	0/0
2	10/10	0/0	0/0	0/0	0/0
3	10/10	0/0	0/0	0/0	0/0
4	10/10	0/0	0/0	0/0	0/0
5	10/10	0/0	0/0	0/0	0/0
6	10/10	0/0	0/0	0/0	0/0
7	20/20	0/20	0/0	0/100	0/0
7 ext.	20/20	0/2	0/0	0/90	0/0

Table 1: Results of the experiments using "Billinton FP reader" and "U are U DigitalPersona 4000". The two sensors is represented in the table with ’B’ and ’U’ respectively.

5 Conclusion

The experiments conducted in this project produced some interesting results concerning the ease of making an artificial finger with co-operation of its owner. None of the fingerprint scanners tested by us was designed for use in a high-security environment. Experiment seven, describes how we managed to make a dummy finger using plaster and silicon. This artificial finger fooled the optical "U are U DigitalPersona 4000"- fingerprint sensor. If an amateur can produce good results with limited equipment and resources, an experienced forger will not do worse with better materials.

The scanners used in this experiment do not include liveliness detection. Several manufacturers claim that they have mechanisms detecting heartbeat in the tip of the finger. This might prevent a successful verification of our artificial fingers.

As mentioned earlier a fingerprint is difficult to verify on the "Billionton FP reader", even with a real finger. The reason for the unsuccessful attempt with one of the artificial fingers in experiment seven, might be due to the fact that the surface is so small that we were unable to place the dummy on it. The artificial fingertip made in [11] might be able to fool this fingerprint sensor.

We have compared the results achieved in this project with other similar experiments, like [11] and [12], and came up with some conclusions:

- [11] have similar results, as to the fact that we both succeeded. One other aspect of these experiments is the quality of the sensors. These may or may not be more secure. The artificial finger produced by Sandström, was of better quality and less visible, making it usable in controlled and secure environments. Our artificial finger made in experiment seven, is also usable in an environment without human monitoring. The intension of our project was to see how much time and effort needed to circumvent a fingerprint scanner. Due to this, we chose some less time-consuming experiments. This was not the case in [11].
- Others, i.e. [12], have succeeded in experiments that we did not. This does not necessarily mean that our experiment was of poorer quality, but might be a result of the quality of the fingerprint scanners. This implies that the technology is evolving and improving.

References

[1] Anil K. Jain, S. Prabhakar, and Sharath Pankanti. Can identical twins be discriminated based on fingerprints? Technical Report MSU-CSE-00-23, Department of Computer Science, Michigan State University, East Lansing, Michigan, October 2000.

[2] Gerrit Bleumer. Biometric yet privacy protecting person authentication. *Lecture Notes in Computer Science*, 1525:99–110, 1998.

[3] Maio D. Jain A.K. Prabhakar S. Maltoni, D. *Handbook of Fingerprint Recognition*. Series : Springer Professional Computing, 2003.

[4] Wayne Penny. Biometrics: A double edged sword - security and privacy. *GSEC Certification Practical*, 2002. SANS Institute.

[5] S.Brostoff and A.Sasse. Are passfaces more usable than passwords? A field trial investigation., 2000. `http://oneman.cs.ucl.ac.uk/brostoff\_sasse.pdf`.

[6] A.J. Mansfield and J.L. Wayman. Best practices in testing and reporting performance of biometric devices, version 2.01, August 2002. `http://www.cesg.gov.uk/site/ast/biometrics/media/BestPractice.pdf`.

[7] J.H Connell N.K Ratha and R.M. Bolle. An analysis of minutiae matching strength, 2001.

[8] Bruce Schneier. The uses and abuses of biometrics. *Comm. ACM*, 42(8):136, August 1999.

[9] Ton van der Putte and Jeroen Keuning. Biometrical fingerprint recognition: Don't get your fingers burned, . *IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications*, pages 289–303, 2000. `http://www.keuning.com/biometry/Biometrical\_Fingerprint\_Recognition.p%df`.

[10] Johan Blomme. Evaluation of biometric security systems against artificial fingers. Exam, Linköpings tekniska högskola, 2003. `http://www.ep.liu.se/exjobb/isy/2003/3514/exjobb.pdf`.

[11] Marie Sandström. Liveness detection in fingerprint recognition systems. Msc thesis, Linköpings tekniska högskola, 2004. `http://www.ep.liu.se/exjobb/isy/2004/3557/exjobb.pdf`.

[12] Peter-Michael Ziegler Lisa Thalheim, Jan Krissler. Body check. *c't magazine 11/2002*, page 114, 2002. http://www.heise.de/ct/english/02/11/114/.

[13] *Billionton fingerprint reader specification*. http://www.eaonline.com.my/product/pcmciaproduct/A006.htm.

[14] *Billionton Inc.* http://www.billionton.com.tw.

[15] *digitalPersona Inc.* www.digitalpersona.com/products/hardware/resources/reader.pdf.

Appendix A- Similarity scale

Trial Number	Similarity Artificial Finger	Similarity Real Finger
1	205	627
2	142	559
3	181	798
4	196	785
5	272	683
6	217	776
7	288	315
8	272	433
9	162	523
10	217	413
11	228	385
12	264	346
13	306	497
14	216	523
15	235	348
16	245	403
17	251	569
18	199	216
19	263	630
20	274	672
Average	231.65	525.05

Appendix B- Material

This appendix contains a detailed description of the material used in the experiments. The material used is available at any hardware stores.

- Different types of glue
  - Wood cement - "Tundra Ikea trelim"
  - Contact glue - "Bison Tix"
  - Hobby glue - "Casco Skolelim"
- Plaster - "Borup Model-Gips"
- Different types of silicon
  - Silicon - "Metylari Easy Fix Filler"
  - Silicon - "Acrylic AcrylFinish"
  - Silicon - "Bostik Akrylmasse(inne) vannbasert"
- Bowl
- Modelling clay
- Hair dryer
- Transparent

Appendix C- Fingerprint scanner specification

"Billionton FP reader" [13] from Billionton System Inc. [14]:

- Capacitive scanner.
- The sensor matrix is comprised of 16,384 individual elements arranged in a 128x128 Square Pattern (500 pixels per inch,ppi).
- Environment operating ranges is from $0 - 55°\mathrm{C}$.
- It has a false acceptance rate (FAR) at 0.015 % and a false rejection rate (FRR) at 2.3 %.
- The sensing area size is 6.5mm x 6.5mm.
- The physical size of the scanner: 70x53.9x19.5 mm (LxWxH).

"U are U DigitalPersona 4000" from DigitalPersona inc. [15]:

- Optical sensor
- Pixel resolution is 512 dpi.
- The image capture area is 14.6mm x 18.1 mm.
- The fingerprint is represented with a 8-bit grayscale (256 levels of gray).
- The physical size of the scanner: 79x49x19 mm (LxWxH).