Ad Usque Fidelis
Cabinet Louis Reynaud

Biometrics Attacks Catalog

August 2019

About Cabinet Louis Reynaud

Cabinet Louis Reynaud is a **cabinet of technological, normative and regulatory** expertise in the fields of digital trust and cyber security and a **Technology Evaluation Laboratory (Biometrics and Security) operating under the CLR Labs brand.**

We support you in your digital transformation, especially in the **evolutions and evaluation** of your products, solutions and services.

Our firm has offices in **Provence/Cote d'Azur** and in **Brussels**, close to the Telecom Valley (ETSI), the French SCS Cluster and the European institutions and the decision-making ecosystem.

We are member of the French AFNOR, French SCS Cluster, the Smart Physical Access Control association (SPAC) and the European Association Eurosmart.

Our activities revolve around four complementary axes which are:

- Mastery of key technologies and processes of digital security,
- Mastery of normative and regulatory processes,
- Mastery of security and functional certification schemes,
- Owning its own Biometrics and Security evaluation laboratory.

Our cabinet is very committed to respect for European fundamental values and the principle of sovereignty of the Member States. Its independence allows it to choose the missions in adequacy with these values.

We believe that strengthening European industries means creating a single digital market through the use of European standards and their referencing in the European acquis.

We guarantee medium and long-term support for companies, associations, local authorities, the central administration and the European institutions.

Our motto: Reflection is important, action is decisive!

More information about Cabinet Louis Reynaud and its work can be found at www.cabinet-louis-reynaud.fr.

Contact

For queries in relation to this document, please use info@cabinet-louis-reynaud.fr.

Disclaimer

The use of the information contained in this document is at your own risk, and no relationship is created between Cabinet Louis Reynaud and any person accessing or otherwise using the document or any part of it. Cabinet Louis Reynaud is not liable for actions of any nature arising from any use of the document or part of it. Neither Cabinet Louis Reynaud nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright notice

Headquarter : 3 rue plan Cavaillon 13420 Gémenos - France

CLR Labs : 2 rue Fougasse 13600 La Ciotat - France

N° SIRET 83373449400010 – TVA Intracommunautaire FR3833734494

Table of content

About Cabinet Louis Reynaud 2
Table of content 3
I. Introduction 4
II. List of known attacks 10
A. Iris 10
B. Fingerprint 17
C. Facial 42
D. Palm-vein 51
E. Voice 54
III. Conclusion 63
IV. References 64
V. Figures references 65

I. Introduction

Biometrics is a science (and sometime even an Art) through which system can uniquely identify an individual on the basis of his physiological (face, iris, fingerprint, hand geometry, retina…) and behavioral (voice, gait, signature dynamics, keystroke dynamics...) traits.

Biometrics is historically coming from the law enforcement activities (Police and Justice) and within a dedicated usage on the identification with two methods:

- One to one
- One to many

The use of biometric traits as an authentication method has become widespread from physical access control to e-commerce since the last 10 years. This generalization of the usage of biometrics technologies, within the mass market use cases, has been accelerating with the introduction in 2013 of the I-Phone 5S and now are used in several use cases:

- Electronic Identification,
- Electronic Authentication
- Electronic Signature
- Digital Identity
- NFC payment
- Cloud payment
- On-line banking
- Automatic border control

Biometrics are used in complement of the traditional authentication systems such as token based (e.g., ID cards) or knowledge based (e.g., passwords) because it alleviates the need to remember long passwords and PIN Code.

Biometric-based personal authentications system may operate in two different modes: identification and verification modes.

In identification mode, system carries out a one-to-many (1 : N) comparison to set up an individual's identity. In other words, the user's input is compared with all the templates stored in system database (such as AFIS or ABIS). The purpose of identification is to answer the question: "Who am I?".

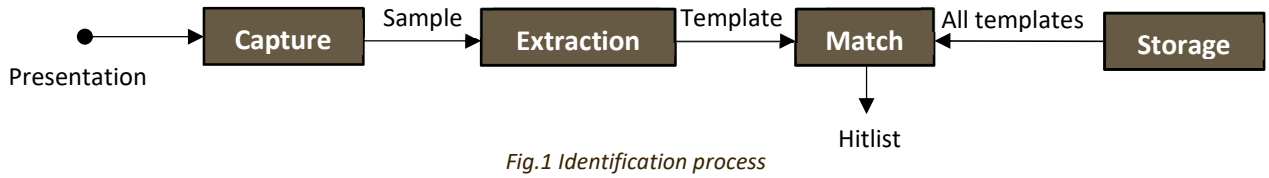


Fig.1 Identification process

In verification mode, system carries out a one-to-one (1 : 1) comparison to set up an individual's identity (e.g., a fingerprint scanner to unlock a smartphone). In other words, the user claims an identity and the system verifies whether the claim is genuine or not on the basis of validating a sample collected against a previously collected biometric sample for the individual. The purpose of verification is to answer the question "Am I who I say I am"?

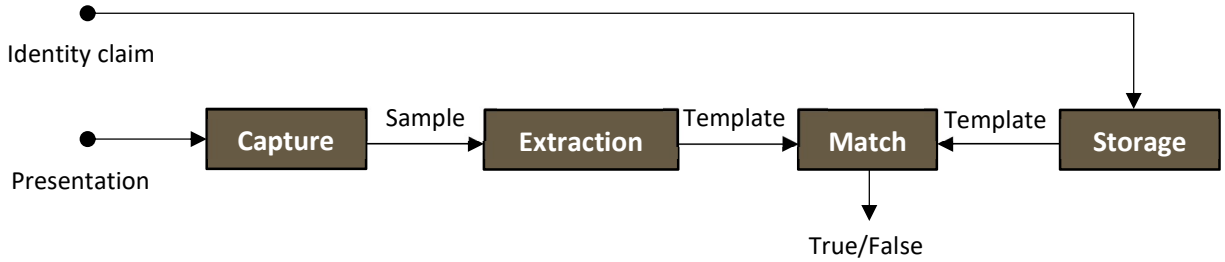


Fig.2 Verification process

All the biometric systems have four basic modules which are sensor module, feature extractor module, matcher module and decision module.

These four modules are necessary in any biometrics system to acquire and process raw biometric data and convert it into some useful information.

Sensor module

In this type of module, raw biometric data is captured by the sensor and it scans the biometric trait to convert it into digital form. After converting it to digital form, this module transmits the data to feature extraction module.

Feature extraction module

It processes the raw data captured by sensor and generates a biometric template. It extracts the necessary features from the raw data and needs much attention because essential features must be extracted in an optimal way.

It basically removes noise from the input sample and transmits the sample to input it to the succeeding module known as matcher module.

Matcher module

This module compares the input sample with the templates being stored in the database using matching algorithm and produces match score.

The resulting match score is transmitted to the decision module, which decides whether to accept the individual or not.

Decision module

After accepting the match score from matcher module, it compares the matching score against the predefined security threshold.

This module accepts or rejects the individual on the basis of predefined security threshold. If match score is greater than predefined security threshold it will accept the individual otherwise reject it.

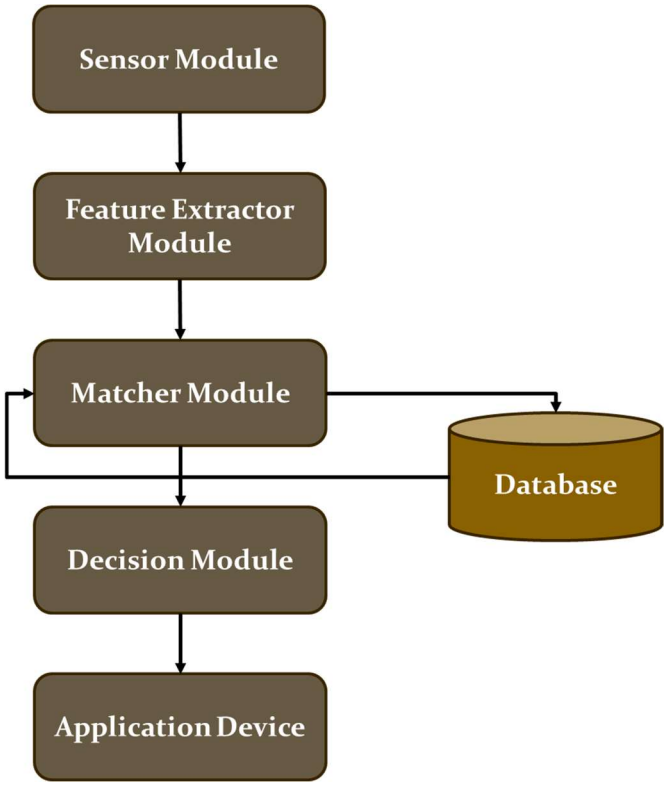


Fig.3 Biometric system

Ideal biometrics is universal, unique, permanent, collectable, acceptable and noncircumventable.

But, as all biometrics don't respond to all these criteria, they are vulnerable to attacks by malevolent people. And, of course all biometrics are not equal and do not have the same FMR (false match rate), FAR (false acceptance rate) or FRR (false reject rate).

Moreover, if biometrics respond to the identification question "Who am I?", it is important to underline, before discussing about attacks against biometrics, that it's important to use at least a two-factor authentication to create a strong authentication system.

The Biometrics technologies alone are not enough to perform a strong authentication.

The two-factor authentication should be composed by "Something that I know" or "Something that I have" or "Something that I am" for instance.

In fact, using biometrics as authentication makes sense only if you have at least a two-factor authentication.

Traditional systems are unable to distinguish between an authorized person and an intruder who can fraudulently access the system. Biometrics systems are more convenient to use because there is no need to remember any password and with a single biometric trait different, account can be secured without the burden of remembering passwords.

Biometric systems offer great advantages over traditional systems, but they are vulnerable to attacks.

There are eight attack points in biometric systems which can be attacked as shown in fig.4. These attack points are divided into two categories: direct attacks and indirect attacks.

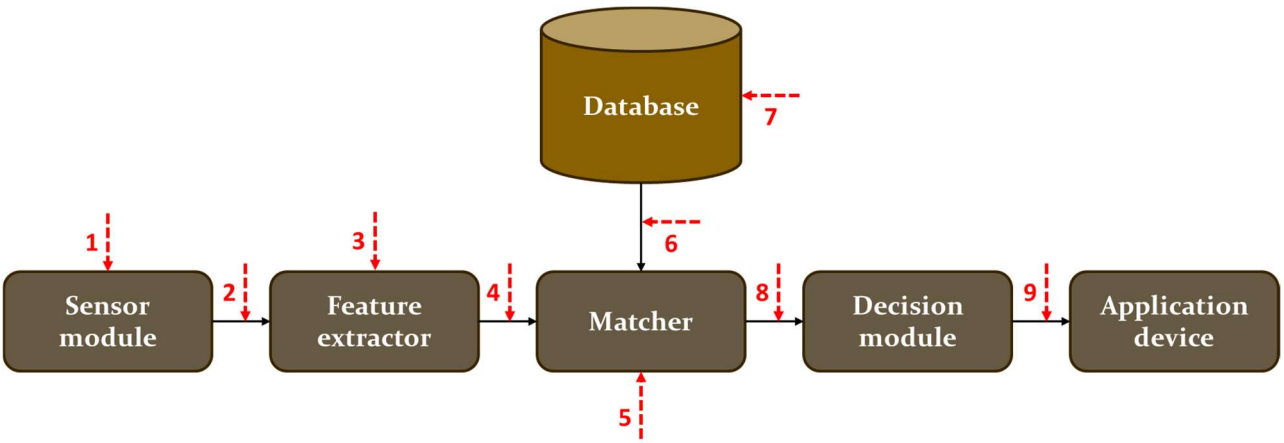


Fig.4 Attack points on biometric system

Direct attacks

It refers to the attacks that do not require any specific knowledge about the system operation such as matching algorithm used, feature vector format, etc.

1. Type 1 attack

The sensor module is vulnerable to type 1 attack which is known as "presentation attack". In this attack, a fake biometric trait such as an artificial finger or facial image is presented to the sensor by an imposter to bypass recognition systems. According to the ISO/IEC 30107-1, we call PAI (Presentation Attack Instrument) any biometric characteristic or object used in a presentation attack. In a presentation attack, an imposter can also physically damage the recognition system and flood the system with bogus access requests. It is very easy to attack at the sensor because no specific knowledge about the system operation is needed and there are no digital protection mechanisms such as watermarking, cryptography are used at the sensor level. Sensors are unable to distinguish between fake and real characteristics of an individual and can be fooled easily by using PAIs such as synthetic fingerprints and facial image of a person.

Attacks at the sensor using PAIs generally fall into one of two categories: artificial or human-based characteristics. Note that there is a third category of other natural cases such as animal-based and plant-based PAIs. Fig.5 illustrates all types of PAIs identified by ISO/IEC 30107-1.

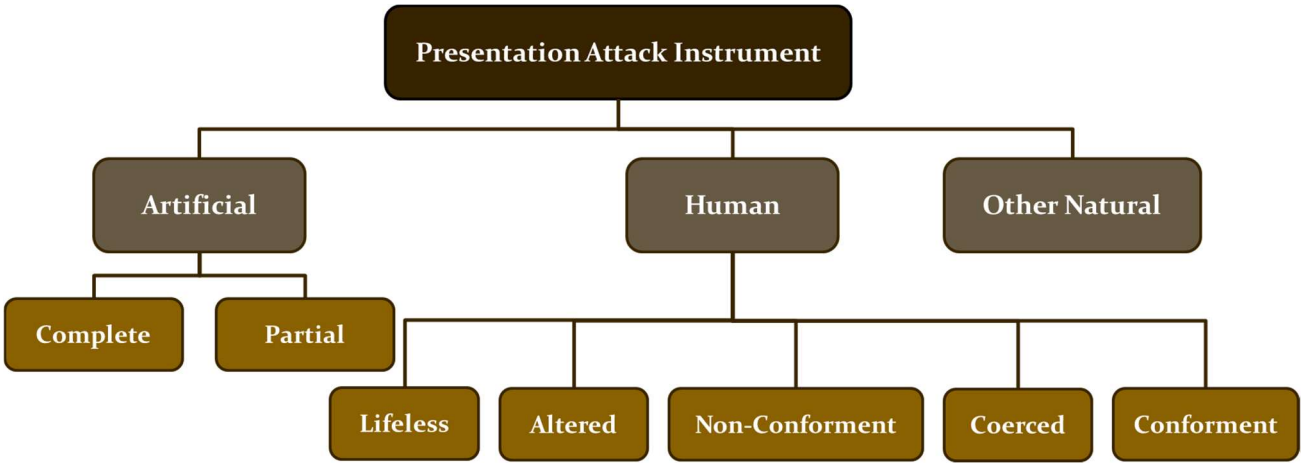


Fig.5 Types of Presentation Attack Instruments

ISO/IEC 30107-1 underlines the fact that not all coercive presentations are expected to be detectable. But, some biometrics recognition devices may enable measurement of coercion indicators, such as voice stress analysis, extreme pulse rate, or facial emotion analysis for example.

The following table give examples of artificial and human presentation attack instruments.

Artificial	Complete	Gummy finger, video of face, fake hand
	Partial	Glue on finger, tape, sunglasses, artificial contact lens, non-permanent make-up, voice morphing software
Human	Lifeless	Cadaver part, severed finger/hand
	Altered	Mutilation, surgical switching of fingerprints between hands
	Non-Conformant	Facial expression/extreme, tip or side of finger
	Coerced	Unconscious, under duress
	Conformant	Zero effort impostor attempt

Tab.1 Examples of artificial and human PAIs

Most of the attacks covered in this catalog will involve type 1 attacks. Presentation attacks can be carried out by two types of attackers: a biometric imposter, where the attacker intends to be recognized as an individual other than him/herself, or a biometric concealer, where the attacker intends to evade being recognized as any individual known to the system.

Biometric imposters may perform attacks in two different ways. In the first subtype, the attacker intends to be recognized as a specific individual known to the system. In the second subtype, the attacker intends to be recognized as any individual known to the system, without specification as to which one.

In contrast, biometric concealers will be seeking to conceal his/her own biometric characteristics, as opposed to modelling the characteristics of known individuals (e.g., using an artefact or through disguise or alteration of natural biometric characteristics).

Indirect attacks

Unlike direct attacks, these are the attacks where information about the inner working of the authentication system is required to make an attack successful.

2. Type 2 attack

When the sensor acquires a raw biometric data, it sends the raw data to feature extractor module for pre-processing through a communication channel. This channel is in between sensor and the feature extractor module. It is intercepted to steal the biometric trait and is stored somewhere. The previously stored biometric trait is replayed to the feature extractor to bypass the sensor. This is known as “replay attack”.

3. Type 3 attack

The feature extractor module is vulnerable to type 3 attack which is known as “Attack on feature extractor module”. When the sensor acquires a raw biometric data, it sends the raw data to feature extractor module. An imposter pressurizes the feature extractor module to produce the feature values chosen by the intruder instead of producing the feature values generated from the original data obtained from the sensor.

4. Type 4 attack

This attack is similar to attack of type 2 but difference is in that, an imposter intercepts the communication channel between the feature extractor and matcher modules and steal the feature values of genuine user. These values can be replayed to the matcher later on. It is known as “Attack on the channel between the feature extractor and matcher”.

5. Type 5 attack

A matcher module is vulnerable to type 5th attack which is known as “Attack on matcher module”. It is attacked to generate the high matching score as selected by the imposter to bypass the biometric authentication system regardless of the values obtained from the input feature set.

6. Type 6 attack

It occurs when the imposter compromises the security of the database by adding new templates, modifying existing templates and removing existing templates. It is not an easy task to attack system database because templates are protected by digital mechanisms such as steganography, watermarking, etc. To make successful attack on system database some knowledge of inner working of the system must be needed.

7. Type 7 attack

Attack can be made possible only when template is transmitted through communication channel between system database and matcher module. It occurs when imposter modifies or tampers with the contents of the transmitted template. An imposter intercepts the channel to steal, replace or alter biometric template. It is known as “Attack on the communication channel between system database and the matcher”.

8. Type 8 attack

An imposter may override the result declared by the matcher module. In this attack, imposter may corrupt the match score (score between 0% and 100%) which is transmitted through communication channel between matcher module and decision module. It corrupts the match score to change the original decision (accept or reject) of the matcher module.

9. Type 9 attack

An imposter may override the result declared by the decision module. In this attack, imposter may tamper with the match decision which is transmitted through communication channel between decision module and application device. It tampers with the match score to change the original decision (accept or reject) of the decision module. This attack is the most critical because of the binary nature of match decision sent by the decision module to the application device. In order to protect this binary decision sent to the application device, the match score is encrypted by the decision module.

Attacks ratings

Cabinet Louis Reynaud has made another document in which it provides guidance metrics to calculate the attack potential required by an attacker to effect an attack. In this document, Cabinet Louis Reynaud associates criteria with marks in order to give a weight to each attack, to attribute then the intended level of attack (basic, substantial or high) in function of this weight. The EU Cybersecurity Act recommends three assurance levels (basic, substantial, high) to express the cybersecurity risk. These assurance levels are commensurate with the level of the risk associated with the intended use of the product, service or process, in terms of the probability and impact of an incident. Cabinet Louis Reynaud decided to use the same vocabulary to correspond to what is currently used in cybersecurity. In this catalog, each attack is associated to a level calculated thanks to the Cabinet Louis Reynaud rating's method.

This document gives a selection of cyber-attacks and hacks which is intended to raise awareness with users/operators on the risks and mitigation measures for attacks in their sector. It does so by providing a historical list of attacks per physical biometrics: fingerprint, iris, facial, voice and palm-vein.

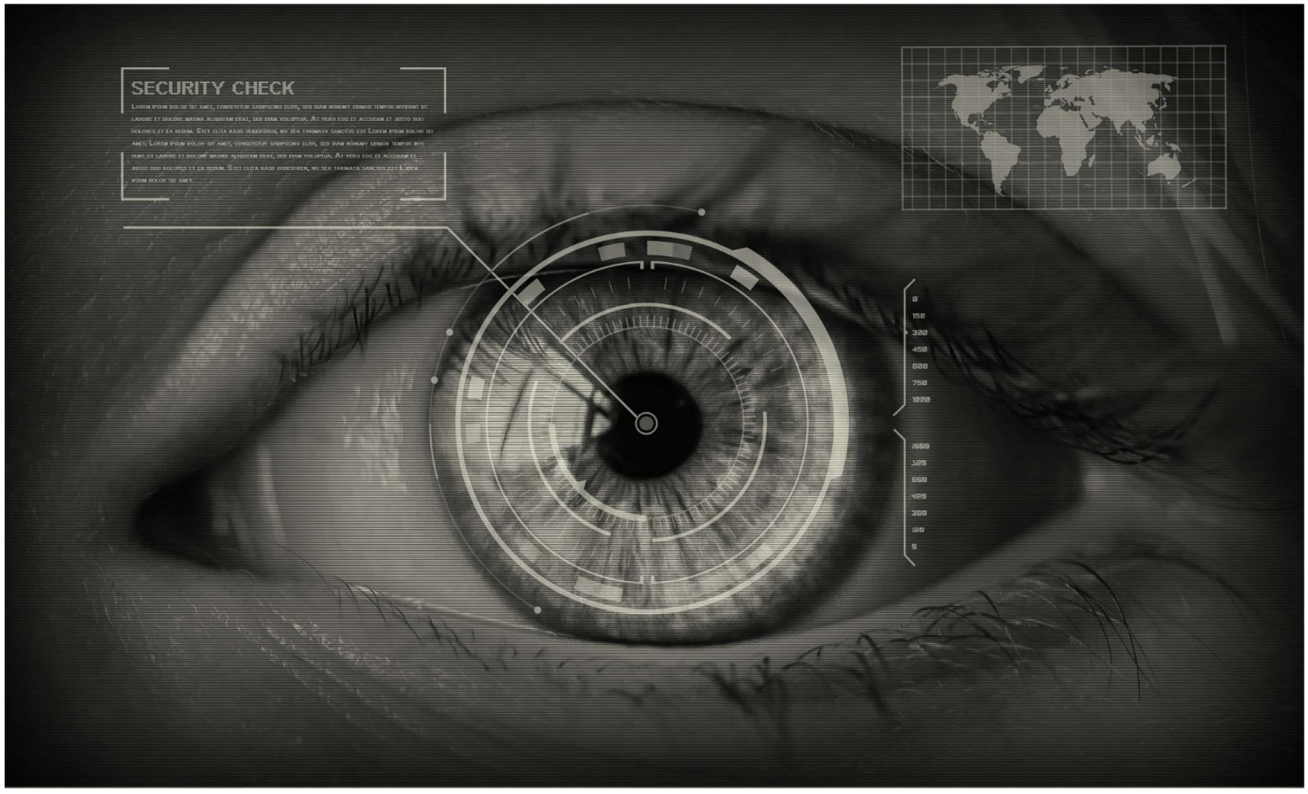
For each attack, this document gives information about the attack, the description of the attack but also a level of difficulty of the attack.

The lists are not meant to be exhaustive but are given for their relevance, their renown and for educational and awareness-raising purposes.

The content provided in this document is based on publicly available and open source information, providing specific examples of attacks and hacks. It does not provide an analysis of trends or threats.

II. List of known attacks

A. Iris



Spoofing iris recognition technology with pictures

Taxonomy of the environment

Year	2015
Country	Germany
Biometrics involved	Iris
Biometrics matching involved	(1 : 1) matcher
Biometrics inspection system involved	Iris recognition camera
Biometrics AFIS or ABIS?	None
Objective of the Fraud	Fool the iris scanner
Asset obtained by performing the attacks	Have access to what the iris recognition system was protected

Type of attack[a]: 1 **Level of attack[b]:** Basic

Author of the attack: Jan Krissler, from the Chaos Computer Club, known as Starbug

Victim of the attack: Someone who has a photo of him on internet

Description of the attack

Though iris recognition might seem secure, this form of biometrics in its various manifestations has been bypassed by some remarkably simple techniques in the past. Security researcher Jan “Starbug” Krissler, from the famous Chaos Computer Club, told Forbes at the MWC in Barcelona this kind of attack can be carried out against some iris-scanning kit just using high-resolution images found in Google searches. He believes that where photos are vivid and large enough, it’s possible to simply print copies of people’s eyes and bypass biometric authentication.

As he detailed in an upcoming talk at the CanSecWest conference in Vancouver a month later, Krissler said he can do similar work (than what he did with the clone of the thumbprint of German defense minister Ursula von der Leyen) with eyes simply using pictures gathered off the internet. To get a useful image, he had to rely on a number of factors. First, the target’s eyes must had to be bright because of the way the infrared-based system his company bought for him used light. In his tests in December, Krissler messed with Panasonic's Authenticam BM-ET200 iris recognition technology, a product that has been discontinued but the only system he said he has seen in common use in 2015.

The image also had to be large and clear enough, though Krissler didn't see that as much of a barrier. He has managed to fool a commercial system with a printout down to an iris diameter of 75 pixels. But he declared: “I did tests with different people and can say that an iris image with a diameter down to 75

pixel worked on our tests." The printout had to have a resolution of 1200 dpi too, though it's easy to find printers able to hit that specification today, and ideally at least 75 per cent of the iris was visible.

Unlike the fingerprint attack, where it was necessary to create a proper clone, all that he needed in his iris recognition hacks was the printout, the researcher claims. According to him, it's nothing more. He punched a hole in the middle, but only for orientation. But it was not needed.

Any attacker willing to carry out such a brazen attack would have to find some suitable targets first. Fortunately (or unfortunately), some of the most powerful people in the world are often pictured in high definition and happen to have lovely bright eyes. Krissler found an election poster of Angela Merkel with an iris diameter of 175 pixels that was ideal. A simple search on Google Images brought up other attractive targets from the political world, including Russian president Vladmir Putin, former Secretary of State and First Lady Hillary Clinton and UK former prime minister David Cameron.

Krissler claims to have proven it's possible to mix open source intelligence, gathered from all those high-resolution images of people's sensory organs found across the web, with biometric authentication to start hacking hardware of famous people and everyday folk alike.

Date of the attack: March 2015

Result of the attack: Successful impersonation of the user

Sources

[1] Justin Lee, "Spoofing iris recognition technology with pictures", https://www.biometricupdate.com/201503/spoofing-iris-recognition-technology-with-pictures/

[2] Ryan De Souza, "Starbug Hacker Demonstrates How To Crack Iris-Recognition Scanner", https://www.hackread.com/german-hacker-starbug-iris-recognition-scanner/

[3] Thomas Brewster, "Hacking Putin's Eyes: How To Bypass Biometrics The Cheap And Dirty Way With Google Images", https://www.forbes.com/sites/thomasbrewster/2015/03/05/clone-putins-eyes-using-google-images/#676e7a8d214a/

(a) Type of the attack is defined on pages 7 – 9

(b) Level of attack is calculated with Cabinet Louis Reynaud rating's method (more information page 9)

Hack of Samsung Galaxy S8 iris scanner

Taxonomy of the environment

Year	2017
Country	Germany
Biometrics involved	Iris
Biometrics matching involved	(1 : 1) matcher
Biometrics inspection system involved	Iris recognition camera
Biometrics AFIS or ABIS?	None
Objective of the Fraud	Fool the iris scanner
Asset obtained by performing the attacks	Unlock the phone

Samsung Galaxy S8

Type of attack: 1 **Level of attack:** Basic

Author of the attack: Jan Krissler, from the Chaos Computer Club, known as Starbug

Victim of the attack: Samsung galaxy S8 owner

Description of the attack

The iris-recognition feature in Samsung's new Galaxy S8 smartphone has been defeated by a German hacker, less than a month after it hit shelves around the world. Indeed, a video posted by the Chaos Computer Club shows the security feature being fooled by a dummy eye into thinking that it is being unlocked by a legitimate owner.

Krissler was up to the task of trying to skirt Samsung's iris scanner, and he did it in typical Starbug fashion. First, he takes a picture of the victim's eyes. In his video demonstration (link below), he used himself and had someone else take the picture. The photo does not even have to be a close-up. It can be taken from a medium distance away, so it does not even have to look like the person is the subject of the picture. The only condition is that the photo has to be an infrared image. Many inexpensive digital cameras have an IR mode, so this should not pose a problem to the dedicated infiltrator.

Next Krissler prints out a zoomed image of the eye on a laser printer. The printed image does not have to include the entire face, only the eye, but it has to be zoomed sufficiently to be life-sized. The size is important because once he has a printed image of the victim's eye, he places a contact lens over it to replicate the cornea of the eye. Holding the picture with the contact lens attached to it up to the phone and aligning it with the circles opened his phone instantly.

According to Dirk Engling, the group's spokesperson, the security risk to the user from iris recognition is even bigger than with fingerprints, as we expose our irises a lot. He also warns that "under some circumstances, a high-resolution picture from the internet is sufficient to capture an iris.

But according to Samsung, it would be "impossible" to use a normal picture of an iris, however high resolution it is, to fool the security feature. In a statement, the company said the attack requires "a rare combination of circumstances" to pull off. "It would require the unlikely situation of having possession of the high-resolution image of the smartphone owner's iris with IR camera, a contact lens and possession of their smartphone at the same time. We have conducted internal demonstrations under the same circumstances, however, [and] it was extremely difficult to replicate such a result."

Date of the attack: May 2017

Result of the attack: Successful impersonation of the user

Sources

[1] Starbug, "Hacking the Samsung Galaxy S8 Iris scanner", https://media.ccc.de/v/biometrie-s8-iris-en/

[2] Alex Hern, "Samsung Galaxy S8 iris scanner fooled by German hackers", https://www.theguardian.com/technology/2017/may/23/samsung-galaxy-s8-iris-scanner-german-hackers-biometric-security/

[3] Chaim Gartenberg, "Hacker beats Galaxy S8 iris scanner using an IR image and a contact lens", https://www.theverge.com/circuitbreaker/2017/5/23/15680268/hacker-galaxy-s8-iris-scanner-ir-image-contact-lens-starbug/

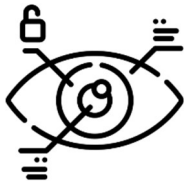
[4] Cal Jeffrey, "Samsung's Galaxy S8 iris scanner can be easily beat with a low-tech method", https://www.techspot.com/news/69431-samsung-galaxy-s8-iris-scanner-can-easily-beat.html/

Exposition of an “unhackable” USB disk password in plain text

Taxonomy of the environment

Year	2019
Country	United Kingdom
Biometrics involved	Iris
Biometrics matching involved	(1 : 1) matcher
Biometrics inspection system involved	Iris recognition camera
Biometrics AFIS or ABIS?	None
Objective of the Fraud	Obtain the Iris hash of the USB key owner
Asset obtained by performing the attacks	Get the password/hash of the device in clear text

eyeDisk



Type of attack: 7 **Level of attack:** Substantial

Author of the attack: David Lodge, researcher for Pen Test Partner

Victim of the attack: eyeDisk owner

Description of the attack

EyeDisk is a USB key that uses iris recognition to unlock the drive and that company qualifies as “unhackable”. To quote their Kickstarter campaign that raised 21000$: “With eyeDisk you never need to worry about losing your USB or the vulnerability of your data stored in it. eyeDisk features AES 256-bit encryption for your iris pattern. We develop our own iris recognition algorithm so that no one can hack your USB drive even [if] they have your iris pattern. Your personal iris data used for identification will never be retrieved or duplicated even if your USB is lost.”

But, iris biometrics-secured USB flash drive eyeDisk is not “unhackable” as it is claimed to be, as UK cybersecurity firm Pen Test Partners have discovered a way to break into the device without a spoof attack. The soft spot, security-wise, however, turns out to be the backup password. Pen Test Partners researcher David Lodge says the device matched his iris biometrics about two-thirds of the time, and was not fooled by attempts to unlock it with his children’s eyes or a picture of his own. However, he discovered he could obtain the password in plain text with a traffic-sniffing software tool. The data is passed from the host and the device during the unlocking procedure, regardless of whether the user enters the correct password or an incorrect one. The same snapshot of sniffed data also contains a string which Lodge says may be the iris hash.

According to Lodge, the software collects the password first, then validates the user-entered password BEFORE sending the unlock password.

Lodge disclosed the vulnerability on April 4, and eyeDisk responded immediately. The company acknowledged the communication and said it would provide a fix on April 9, but no further response was forthcoming, and Lodge publicly disclosed the information on May 9.

Date of the attack: April 2019

Result of the attack: Biometric information disclosure

Sources

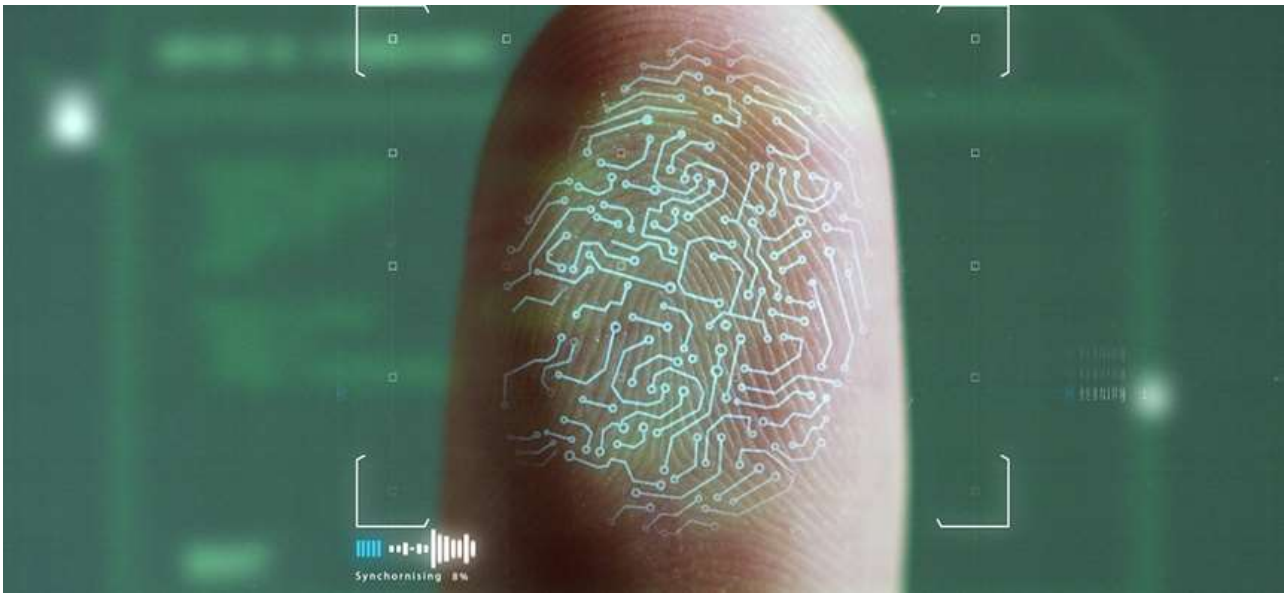
[1] David Lodge, "eyeDisk. Hacking the unhackable. Again", https://www.pentestpartners.com/security-blog/eyedisk-hacking-the-unhackable-again/

[2] Chris Burt, "Pen testing beats iris biometric USB data storage device via backup password", https://www.biometricupdate.com/201905/pen-testing-beats-iris-biometric-usb-data-storage-device-via-backup-password/

[3] "'Unhackable' USB has been hacked by a group of experts", https://www.securitynewspaper.com/2019/05/14/%EF%BB%BFunhackable-usb-has-been-hacked-by-a-group-of-experts/

[4] eyeDisk, "eyeDisk, unhackable USB flash drive", https://www.kickstarter.com/projects/eyedisk/eyedisk-unhackable-usb-flash-drive?lang=fr/

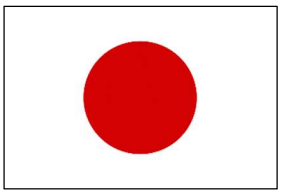
B. Fingerprint



Identification fraud at the border management

Taxonomy of the environment

Year	2008
Country	Japan
Biometrics involved	Fingerprints
Biometrics matching involved	(1 : N) matcher
Biometrics inspection system involved	Optical fingerprint scanner
Biometrics AFIS or ABIS?	AFIS
Objective of the Fraud	Cheat the central database of biometrics
Asset obtained by performing the attacks	Enter a non-authorized country



Type of attack: 1 **Level of attack:** Substantial

Author of the attack: Unknown South Korean Woman

Victim of the attack: Japanese border customs

Description of the attack

Two South Korean women have managed to bypass a cutting-edge fingerprint reading machine in Tokyo's Haneda airport in May and October 2008 and illegally enter Japan. To fool the machine, these women have paid a broker in South Korea who supply them with special tape and a fake passport.

Japan's biometric immigration system was installed in thirty airports in 2007 to improve security by keeping terrorists and foreigners with deportation records away. The Japanese began screening all foreigners entering Japan in November 2007 under which foreign nationals underwent fingerprinting and capturing digital facial images at airports and seaports nationwide to see if the data captured matched that on a 'Watch List' of deported or wanted foreign nationals.

The two women were both deported from Japan before the fraud for overstaying their visas. In order to cheat the fingerprint scanner at immigration, they used a special invisible tape on their two index which carried the fingerprints of another person and fake passports to go with it. The software was required to verify that the biometric images being presented at the fingerprint scanner did not reside in the Watch List. The image being presented to the scanner by the woman using a 'ten cent tape' fingerprint did not exist on the Watch List and the results returned were "Negative". Therefore, the system as designed met the requirements of the program. The problem was that the requirement for eliminating such a simple method for fooling the system was not included in the program requirements.

The two have reportedly laid low as nightclub hostesses but were spotted after both received deportation orders in 2008 for overstaying their visas. After that, the women have been deported in South Korea and their fingerprints have been taken again.

It is the third case of this kind of fraud known in Japan in 2009, and according to one of these women the South Korean broker used the same method to help many other foreigners illegally enter Japan.

The immigration bureau reported to the Justice Ministry that a large number of South Koreans might have entered Japan using the same technique. So, the Japanese government said it's now forced to review its antiterrorism measures at airports.

Date of the attack: May and October 2008

Result of the attack: Illegal immigration

Sources

[1] "Japanese biometric border fooled by tape", 01/29/2010, http://www.homelandsecuritynewswire.com/japanese-biometric-border-fooled-tape

[2] "Traveler fooled scanner by taping over fingerprints", 01/03/2009, https://www.seattletimes.com/life/travel/traveler-fooled-scanner-by-taping-over-fingerprints/

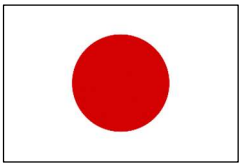
[3] Yona Flink, "Million dollar border security machines fooled with ten cent tape", https://findbiometrics.com/archive/million-dollar-border-security-machines-fooled-with-ten-cent-tape/

[4] Michael Meehan, "Biometrics Powers U.S. VISIT Program", https://fedtechmagazine.com/article/2009/12/biometrics-powers-us-visit-program/

Surgery fools Japan controls

Taxonomy of the environment

Year	2009
Country	Japan
Biometrics involved	Fingerprints
Biometrics matching involved	(1 : N) matcher
Biometrics inspection system involved	Optical fingerprint scanner
Biometrics AFIS or ABIS?	AFIS
Objective of the Fraud	Cheat the central database of biometrics
Asset obtained by performing the attacks	Enter a non-authorized country



Type of attack: 1 **Level of attack:** High

Author of the attack: Lin Rong, a Chinese woman

Victim of the attack: Japanese border customs

Description of the attack

Japan's biometric immigration system was installed in thirty airports in 2007 to improve security by keeping terrorists and foreigners with deportation records away. The Japanese began screening all foreigners entering Japan in November 2007 under which foreign nationals underwent fingerprinting and capturing digital facial images at airports and seaports nationwide to see if the data captured matched that on a 'Watch List' of deported or wanted foreign nationals. But Lin Rong, a Chinese woman, managed to enter Japan illegally by having plastic surgery to alter her fingerprints, thus fooling immigration controls.

She had previously been deported in 2007 from Japan for overstaying her visa and thus had her name and her fingerprints on the 'Watch List'. She was only discovered later when she was arrested for the crime of faking a marriage to a Japanese citizen. Upon arrest, officials noticed 'unnatural scars' on her fingers and eventually Rong confessed to her illegal entry.

According to the Tokyo police, she had paid $15,000 to have the surgery in China. Patches of skin from her thumbs and index fingers were reportedly removed and then grafted on to the ends of fingers on the opposite hand. As a result, Rong's identity was not detected when she re-entered Japan illegally.

While this is the first reported case like this of biometric fraud in Japan, experts worry that there are many more such incidents going unnoticed.

Date of the attack: December 2009

Result of the attack: Illegal immigration

Sources

[1] "'Fake fingerprint' Chinese woman fools Japan controls", http://news.bbc.co.uk/2/hi/asia-pacific/8400222.stm/

[2] Ki Mae Heussner, "Surgically Altered Fingerprints Help Woman Evade Immigration", https://abcnews.go.com/Technology/GadgetGuide/surgically-altered-fingerprints-woman-evade-immigration/story?id=9302505/

[3] Aaron Saenz, "Chinese Woman Surgically Modifies Fingerprints to Illegally Enter Japan", https://singularityhub.com/2009/12/10/chinese-woman-surgically-modifies-fingerprints-to-illegally-enter-japan/

Hack of iPhone 5S Touch ID

Taxonomy of the environment

Year	2013
Country	Germany
Biometrics involved	Fingerprints
Biometrics matching involved	(1 : 1) matcher
Biometrics inspection system involved	Capacitive fingerprint sensor
Biometrics AFIS or ABIS?	None
Objective of the Fraud	Fool the fingerprint scanner
Asset obtained by performing the attacks	Unlock the phone

Apple's security by fingerprint

Type of attack: 1 **Level of attack:** Substantial

Author of the attack: Chaos Computer Club, a German hacker collective

Victim of the attack: iPhone 5S owner

Description of the attack

German hacker collective, Chaos Computer Club, has spoofed the iPhone 5S's Touch ID fingerprint sensor with a fake fingerprint, only 24 hours after the release of the iPhone 5S.

According to the group, the jack is performed with everyday items. First, the fingerprint of the enrolled user is photographed with 2400 dpi resolution. The resulting image is then cleaned up, inverted and laser printed with 1200 dpi onto transparent sheet with a thick toner setting. Finally, pink latex milk or white wood glue is smeared into the pattern created by the toner onto the transparent sheet. After it cures, the thin latex sheet is lifted from the sheet, breathed on to make it a tiny bit moist and then placed onto the sensor to unlock the phone. This process has been used with minor refinements and variations against most fingerprint sensors on the market.

Starbug, the hacker from the group that claimed the attack, said that Apple's sensor has just a higher resolution compared to the sensors so far. That's why the group only needed to ramp up the resolution of their fake. This declaration suggests that this method could succeed with most of the capacitive fingerprint sensors.

Date of the attack: September 2013

Result of the attack: Successful impersonation of the user

Sources

[1] Adam Vrankulj, "Chaos Computer Club claims Touch ID fake fingerprint spoof", https://www.biometricupdate.com/201309/chaos-computer-club-claims-touch-id-fake-fingerprint-spoof/

[2] "Starbug's Touch ID Attack", https://vimeo.com/75324765/

[3] Rahul Thadani, "Hacker fakes German minister's fingerprints from HD photos", https://blogs.quickheal.com/hacker-fakes-german-ministers-fingerprints-hd-photos/

Hack of Samsung Galaxy S5 fingerprint sensor

Taxonomy of the environment

Year	2014
Country	Germany
Biometrics involved	Fingerprints
Biometrics matching involved	(1 : 1) matcher
Biometrics inspection system involved	Capacitive fingerprint sensor
Biometrics AFIS or ABIS?	None
Objective of the Fraud	Fool the fingerprint scanner
Asset obtained by performing the attacks	Unlock the phone and having access to a PayPal account

Samsung Galaxy S5

Type of attack: 1 **Level of attack:** Substantial

Author of the attack: SRLabs

Victim of the attack: Samsung galaxy S5 owner

Description of the attack

The fingerprint scanner on the Samsung Galaxy S5 is one of its selling points, but it appears that the feature has fallen prey to hackers - with just a bit of wood glue and a latent print.

Indeed, showed in a video from researchers from Germany's Security Research Labs (SRLabs), a finger is enrolled on the device, which is then unlocked with the dummy print. The video shows how Samsung's implementation can be bypassed using a mold made under laboratory conditions, but it is based on nothing more than a camera phone photo of a latent print from a smartphone screen. Latent prints aren't immediately visible to the naked eye, but "can be visualized using magnesium powder, which is gently brushed over hard and shiny surfaces in order to illuminate them. In addition to unlocking the phone, the same dummy fingerprint was used to access a PayPal wallet and show that money could even be transferred using the fake print.

It took just four days for German researchers to trick the Samsung Galaxy S5's fingerprint scanner into accepting a mold of a fingerprint instead of a real finger.

Date of the attack: April 2014

Result of the attack: Success impersonation of the user

Sources

[1] Adam Vrankulj, "Samsung's Galaxy S5 falls to the same fingerprint hack as the iPhone 5S", https://www.biometricupdate.com/201404/samsungs-galaxy-s5-falls-to-the-same-dummy-print-hack-as-the-iphone-5s/

[2] SRLabs, "Samsung Galaxy S5 Finger Scanner also susceptible to ordinary spoofs", https://www.youtube.com/watch?v=sfhLZZWBn5Q/

[3] Mikael Ricknäs, "German researchers hack Galaxy S5 fingerprint login", https://www.infoworld.com/article/2607437/german-researchers-hack-galaxy-s5-fingerprint-login.html/

Hacker fakes German Defense Minister fingerprints

Taxonomy of the environment

Year	2014
Country	Germany
Biometrics involved	Fingerprints
Biometrics matching involved	(1 : 1) matcher and (1 : N) matcher
Biometrics inspection system involved	Standard biometric security software
Biometrics AFIS or ABIS?	AFIS
Objective of the Fraud	Replicate the fingerprint
Asset obtained by performing the attacks	Fool a standard biometric security software

Type of attack: 1 **Level of attack**: High

Author of the attack: Jan Krissler, also known as Starbug

Victim of the attack: Ursula von der Leyen, German Defense Minister

Description of the attack

Jan Krissler, a hacker also known as Starbug, showcased such a notewhorthy revelation at the Chaos Communication Congress, the Europe's largest association oh hackers, in Germany in 2014. Starbug demonstrated his technique for stealing fingerprints by simply analyzing a few High-Definition pictures of his target, in this case Ursula von der Leyen, the German Defense Minister.

All he needed to make this possible was a few close-range photos of his target in order to reverse engineer the fingerprints, her thumbprint in this case. He gained these photos from several press releases issued by the minister's office and another that he took himself from a few meters away. With the help of commercially available software called Verifinger he was then able to replicate her thumbprint.

With his method, Starbug explained during the conference that he was able to fool standard biometric software.

Date of the attack: December 2014

Result of the attack: Successful impersonation of the user

Sources

[1] DamnFinn, “Gefahren von Kameras für (biometrische) Authentifizierungsverfahren [31c3] von starbug/Jan Krissler”, https://www.youtube.com/watch?v=pIY6k4gvQsY/

[2] Stephen Mayhew, “German researcher reverse-engineers a fingerprint using photos”, https://www.biometricupdate.com/201412/german-researcher-reverse-engineers-a-fingerprint-using-photos/

[3] Alex Hern, “Hacker fakes German minister's fingerprints using photos of her hands”, https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands/

[4] Rahul Thadani, “Hacker fakes German minister’s fingerprints from HD photos”, https://blogs.quickheal.com/hacker-fakes-german-ministers-fingerprints-hd-photos/

Extraction of user's fingerprints on Android devices

Taxonomy of the environment

Year	2015
Country	United States of America
Biometrics involved	Fingerprints
Biometrics matching involved	(1 : 1) matcher
Biometrics inspection system involved	Capacitive fingerprint sensor
Biometrics AFIS or ABIS?	None
Objective of the Fraud	Extract the user fingerprint
Asset obtained by performing the attacks	Unlock the phone for instance

Samsung Galaxy S5

Type of attack: 2 **Level of attack**: Basic

Author of the attack: Tao Wei and Yulong Zhang from FireEye

Victim of the attack: The Android phone owner

Description of the attack

FireEye's research team has uncovered major security flaws in Android smartphones (they made their tries on Samsung Galaxy S5 and HTC One Max) that feature fingerprint sensors.

FireEye's senior staff research scientist, Tao Wei, and fellow researcher Yulong Zhang took the stage at Black Hat in Las Vegas to show all the ways they found to defeat fingerprint scanners on mobile phones. During his presentation, Zhang showed four different attacks that could allow a hacker to steal or circumvent fingerprint scanners. The first was very straightforward, but extremely important. He showed how an attacker could create a specially crafted app that mimicked a phone's unlock screen. When the victim swipes a finger to unlock the phone, they're actually using their fingerprint to seal a financial transaction.

In another attack, Zhang showed how he could pre-load fingerprint data into a phone and then prevent the user from seeing that additional fingerprints had been added. Zhang demonstrated this using an Android device. Though the Settings menu indicated only one fingerprint had been registered, he successfully unlocked the phone using two of his other fingers he'd stealthily registered. This, said Zhang, could give an attacker a backdoor into his device.

The last attack that Zhang presented was the most impressive. Normally, when an app needs fingerprint data on an Android device, that's handled by the Trust Zone, a secure environment that only talks to the outside world through go-betweens. But apps that need to know when the fingerprint scanner is being used, but without being able to see the fingerprint, have direct access to the fingerprint scanner. Zhang was able to take advantage of this and craft an attack that could grab fingerprint data any time the scanner was touched.

Though the affected phone makers have tried to segment and encrypt the information in a separate secure zone, it's possible to grab the biometric data before it reaches that protected area and create copies of people's fingerprints for further attacks. Thus, an attacker could focus on collecting data coming from the Android devices' fingerprint sensors rather than trying to break into the trusted zone. Any hacker who can acquire user-level access and can run a program as root, the lowest level of access on computers and smartphones, can easily collect fingerprint information from the affected Android phones. On the Samsung Galaxy S5, they wouldn't need to go as deep, with malware needing only system-level access.

If the attacker can break the kernel [the core of the Android operating system], although he cannot access the fingerprint data stored in the trusted zone, he can directly read the fingerprint sensor at any time. Every time you touch the fingerprint sensor, the attacker can steal your fingerprint, according to Zhang. He can get the data and from the data he can generate the image of the fingerprint of the victim. After that he can do whatever he wants.

Wei and Zhang said they had contacted Samsung, but had not heard back about any updates for users. The vulnerability is not resident on Android 5.0 Lollipop or above, that's why the researchers recommend that users should upgrade where they can.

Wei and Zhang said they had not yet gone beyond testing Android devices. Though they did not claim all Android phones below 5.0 with fingerprint authentication were affected, they said the issue is likely more widespread than just Samsung's phone. They add that the vulnerabilities uncovered in the Samsung Galaxy S5's fingerprint technology were a result of lab testing by the FireEye mobile research team. They are not aware of any customers that have actually been affected by this attack in the real world. And they declared that they believe newer Samsung models and OS updates along with security features, such as KNOX, have received improvements that exceed industry standards.

Eventually, Zhang pointed out that Apple solves this problem rather neatly with Touch ID. Like Android devices, Apple apps sometimes need to see that the fingerprint sensor is in use, like when you enroll fingerprints. But Apple encrypts all data coming out of the fingerprint sensor. This forbids the attacker from easily obtaining the fingerprint data because it is encrypted

Date of the attack: April 2015

Result of the attack: Biometric information disclosure

Sources

[1] Justin Lee, "Researchers find major security flaws in fingerprint sensors in Android phones", https://www.biometricupdate.com/201508/researchers-find-major-security-flaws-in-fingerprint-sensors-in-android-phones/

[2] Justin Lee, "FireEye researchers claim Samsung Galaxy S5 flaw allows hackers to duplicate fingerprints", https://www.biometricupdate.com/201504/fireeye-researchers-claim-samsung-galaxy-s5-flaw-allows-hackers-to-duplicate-fingerprints/

[3] Thomas Brewster, "Samsung Galaxy S5 Flaw Allows Hackers To Clone Fingerprints, Claim Researchers", https://www.forbes.com/sites/thomasbrewster/2015/04/21/samsung-galaxy-s5-fingerprint-attacks/#133a41ebaae5/

US government-related data breach

Taxonomy of the environment

Year	2015
Country	United States of America
Biometrics involved	Fingerprints
Biometrics matching involved	(1 : N) matcher
Biometrics inspection system involved	Unknown
Biometrics AFIS or ABIS?	AFIS
Objective of the Fraud	Hack the database of the OPM
Asset obtained by performing the attacks	Have access to personal data of 21.5 million individuals including 5.6 million records of fingerprints

Type of attack: 7 **Level of attack:** Not Practical

Author of the attack: A group of hackers called LulzSec Pilipinas

Victim of the attack: COMELEC (the Philippines' Commission on Elections)

Description of the attack

The United States Office of Personnel Management (OPM) reported that it has discovered that 5.6 million individual's fingerprints were stolen as part of a massive cybersecurity breaches.

In April of 2015, IT staffers within the OPM, the agency that manages the government's civilian workforce, discovered that some of its personnel files had been hacked. Among the sensitive data that was exfiltrated were millions of SF-86 forms, which contain extremely personal information gathered in background checks for people seeking government security clearances, along with records of millions of people's fingerprints. The OPM breach led to a Congressional investigation and the resignation of top OPM executives, and its full implications—for national security, and for the privacy of those whose records were stolen—are still not entirely clear today in 2019.

As the official Congressional report on the incident says, "The exact details of how and when the attackers gained entry ... are not exactly clear." Nevertheless, researchers have been able to construct a rough timeline of when the breaches began and what the attackers did.

The hack began in November of 2013, when the attackers first breached OPM networks. This attacker or group is dubbed X1 by the Congressional OPM data breach report. While X1 wasn't able to access any personnel records at that time, they did manage to exfiltrate manuals and IT system architecture information. The next month, in December of 2013, is when we definitively know that attackers were

attempting to breach the systems of two contractors, USIS and KeyPoint, who conducted background checks on government employees and had access to OPM servers (though USIS may have actually been breached months earlier).

In March of 2014, OPM officials realized they'd been hacked. However, they didn't publicize the breach at that time, and, having determined that the attackers were confined to a part of the network that didn't have any personnel data, OPM officials chose to allow the attackers to remain so they could monitor them and gain counterintelligence. OPM did plan for what they called the "big bang"—a system reset that would purge the attackers from the system—which they implemented on May 27, 2014, when the attackers began to load keyloggers onto database administrators' workstations.

Unfortunately, on May 7, 2014, an attacker or group dubbed X2 by the report had used credentials stolen from KeyPoint to establish another foothold in the OPM network and install malware there to create a backdoor. This breach went undetected and the "big bang" didn't remove X2's access or the backdoor. In July and August of 2014, these attackers exfiltrated the background investigation data from OPM's systems.

They weren't done, though: by October 2014, the attackers had moved through the OPM environment to breach a Department of Interior server where personnel records were stored, and in December 2014 another 4.2 million personnel records were exfiltrated. Fingerprint data was exfiltrated in late March of 2015; finally, on April 15, 2015, security personnel noticed unusual activity within the OPM's networks, which quickly led them to realize that attackers still had a foothold in their systems.

It's not entirely clear how X1 gained access to OPM's networks, but OPM had already been roundly criticized for poor security practices in the period leading up to the intrusion. It's also not entirely clear that X1 and X2 were the same person or group, but seeing as X1 stole information about OPM's network that would've been helpful to X2's agenda, the assumption is that they were at least working in tandem.

What is clear is that OPM's technical leadership, overly confident that they had defeated X1 with the "big bang," did not use the intrusion as a "wake up call" and failed to take measures that would have helped them detect X2. They had also largely failed to institute a number of important and recommended security measures, the most the important of which in the event was two-factor authentication. Under a two-factor authentication scheme, users need a chip-enhanced ID card that correlates with their username and password in order to log into the system. Without it, an attacker who manages to steal a valid username and password—as X2 did, using a login pilfered from KeyPoint—has free access to the system. OPM finally implemented two-factor authentication in January 2015, after X2 had already wormed their way into the network.

At any rate, once X2 had access to OPM systems, they used an Active Directory privilege escalation technique to obtain root access. This was used to install a variant of the PlugX malware, a remote access tool that allowed the attackers to navigate around OPM's systems and compress and exfiltrate data, on several of OPM servers—including, crucially, the "jumpbox," the administrative server that was used to log into other servers. Sakula, another linked piece of remote-control malware, was installed around the same time.

Date of the attack: April 2015

Result of the attack: Biometric information disclosure

Sources

[1] Jason Chaffetz, Marc Meadows and Will Hurd, “Report from the Committee on Oversight and Government Reform on the OPM Breach”, September 2016

[2] Andrea Peterson, “OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought”, https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/?noredirect=on&utm_term=.922509b0eaba/

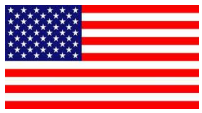
Hack mobile phones using 2D printed fingerprints

Taxonomy of the environment

Year	2016
Country	United States of America
Biometrics involved	Fingerprints
Biometrics matching involved	(1 : 1) matcher
Biometrics inspection system involved	Capacitive fingerprint scanner
Biometrics AFIS or ABIS?	None
Objective of the Fraud	Fool the fingerprint scanner
Asset obtained by performing the attacks	Unlock the phone

Huawei Honor 7

Samsung S6



Type of attack: 1 **Level of attack:** Basic

Author of the attack: Kai Cao and Anil K. Jain, researchers from Michigan State University

Victim of the attack: The phone owner

Description of the attack

Michigan State (MSU) researchers, Anil Jain and Kai Cao, have discovered an inexpensive and quick method to unlock a mobile phone protected by fingerprint biometrics using an off-the-shelf printer and special photo paper.

In their report, Anil Jain and Kai Cao talk about the hack on the iPhone 5S and the Samsung Galaxy S6 by the German hacker known as Starbug who used photograph of the fingerprint of the genuine user and created a spoof fingerprint with latex milk or white wood glue. According to them, there are two limitations of above method of hacking mobile fingerprint reader: the spoof is fabricated manually, where the hacker experience may affect the quality of spoof fingerprint and the accuracy of spoof attack, and it takes significant amount of time to create a spoof; for example, wood glue takes around 20~30 minutes to get dry.

Their report presents a simple yet effective method for spoofing the fingerprint sensor embedded in a mobile phone using a 2D fingerprint image printed on a special paper. The spoof fingerprint is generated automatically. In order to make a successful spoof fingerprint, they installed three AgIC4 silver conductive ink cartridges as well as a normal black ink cartridge in a color inkjet printer (they used Brother MFC-J5910DW printer). According to them, a better conductivity can be achieved if a brand new (unused) printer is used. Then, they scanned the target fingerprint image (of the authorized user) at 300 dpi or higher resolution. Eventually, they mirrored (reverse the image in the horizontal direction) and printed the original or binarized fingerprint image on the glossy side of an AgIC special paper.

In their spoofing experiment, they selected Samsung Galaxy S6 and Huawei Honor 7 phones as examples. They enrolled the left index finger of one of the authors and used the printed 2D fingerprint of this left index finger to unlock the fingerprint recognition systems in these phones.

They tried several fingers of different subjects and all of them can successfully hack these two phones. But, they noticed that Huawei Honor 7 is slightly more difficult to hack (more attempts may be required) than Samsung Galaxy S6.

In summary, they have proposed a simple, fast and effective method to generate 2D fingerprint spoofs that can successfully hack built-in fingerprint authentication in mobile phones. Furthermore, hackers can easily generate a large number of spoofs using fingerprint reconstruction or synthesis techniques which is easier than 2.5D fingerprint spoofs (the Starbug's solution).

Date of the attack: February 2016

Result of the attack: Successful impersonation of the user

Sources

[1] Kai Cao and Anil K. Jain, "Hacking mobile phones using 2D printed fingerprints", February 2016

[2] Stephen Mayhew, "Researchers at MSU spoof a fingerprint protected smartphone using an inkjet printer", https://www.biometricupdate.com/201603/researchers-at-msu-spoof-a-fingerprint-protected-smartphone-using-an-inkjet-printer/

Philippines' government-related data breach

Taxonomy of the environment

Year	2016
Country	Philippines
Biometrics involved	Fingerprints
Biometrics matching involved	(1 : N) matcher
Biometrics inspection system involved	Unknown
Biometrics AFIS or ABIS?	AFIS
Objective of the Fraud	Hack the database of the COMELEC website
Asset obtained by performing the attacks	Have access to personal data of 55 million registered voters including 15.8 million records of fingerprints

Type of attack: 7 **Level of attack:** Not Practical

Author of the attack: A group of hackers called LulzSec Pilipinas

Victim of the attack: COMELEC (the Philippines' Commission on Elections)

Description of the attack

According to a report by Trend Micro, a massive breach of the database of the Philippines' Commission on Elections (COMELEC) has leaked a huge number of voter's personal identifiable information, including passport information and fingerprint data.

Following the defacement of the COMELEC website on March 27 by a hacker group, a second hacker group, called LulzSec Pilipinas, posted COMELEC's entire database online. Within the day, they added three more mirror links where the database could be downloaded.

While COMELEC officials claim that no sensitive information was stored in the database, Trend Micro research showed that the data dumps include 1.3 million records of overseas Filipino voters, which included passport numbers and expiry dates, 15.8 million record of fingerprints and list of people running for office since the 2010 elections. In some tables of the database, even the name, birth date, VIN fields and current residence were not encrypted. Worse, for some records, the names of the parents, birthplace and passport numbers could be identified by just knowing the names of the overseas voters. Banks usually use these details to verify the identity of a person.

With 55 million registered voters in the Philippines, this leak may turn out as one of the biggest government-related data breaches in history.

Date of the attack: May 2016

Result of the attack: Biometric information disclosure

Sources

[1] Trend Micro, "Data Protection Mishap Leaves 55M Philippine Voters at Risk", https://blog.trendmicro.com/trendlabs-security-intelligence/55m-registered-voters-risk-philippine-commission-elections-hacked/

[2] Stephen Mayhew, "Fingerprint and passport data leaked in Philippines voter database breach", https://www.biometricupdate.com/201604/fingerprint-and-passport-data-leaked-in-philippines-voter-database-breach/

[3] Michael Bueza and Wayne Manuel, "Experts fear identity theft, scams due to Comelec leak", https://www.rappler.com/newsbreak/in-depth/127870-comelec-leak-identity-theft-scams-experts/

Possible attack against (1 : N) matching fingerprint security systems

Taxonomy of the environment

Year	2018
Country	United States of America
Biometrics involved	Fingerprints
Biometrics matching involved	(1 : N) matcher
Biometrics inspection system involved	Capacitive fingerprint scanner
Biometrics AFIS or ABIS?	AFIS
Objective of the Fraud	Fool the fingerprint scanner
Asset obtained by performing the attacks	Access to restricted area or user accounts

Type of attack: 1 **Level of attack:** Substantial

Author of the attack: Researchers from New York University and Michigan State University

Victim of the attack: People linked to the (1 : N) matching fingerprint security system

Description of the attack

New findings from computer scientists at New York University's Tandon School of Engineering and Michigan State University could raise the stakes of biometrics security significantly. Researchers have used a neural network to generate artificial fingerprints that work as a “master key” for biometric identification systems and prove fake fingerprints can be created.

According to a paper presented at a security conference in Los Angeles [2], the artificially generated fingerprints, dubbed “DeepMasterPrints” by the researchers from New York University, were able to imitate more than one in five fingerprints in a biometric system that should only have an error rate of one in a thousand.

The researchers, led by NYU’s Philip Bontrager, say that “the underlying method is likely to have broad applications in fingerprint security as well as fingerprint synthesis.” In order to work, the DeepMasterPrints take advantage of two properties of fingerprint-based authentication systems.

The first is that, for ergonomic reasons, most fingerprint readers do not read the entire finger at once, instead imaging whichever part of the finger touches the scanner. Crucially, such systems do not blend all the partial images in order to compare the full finger against a full record; instead, they simply compare the partial scan against the partial records. That means that an attacker has to match just one of tens or hundreds of saved partial fingerprint in order to be granted access.

The second is that some features of fingerprints are more common than others. That means that a fake print that contains a lot of very common features is more likely to match with other fingerprints than pure chance would suggest.

Based on those insights, the researchers used a common machine learning technique, called a generative adversarial network, to artificially create new fingerprints that matched as many partial fingerprints as possible. The neural network not only allowed them to create multiple fingerprint images, it also created fakes which look convincingly like a real fingerprint to a human eye.

The researchers compare the method to a "dictionary attack" against passwords, where a hacker runs a pre-generated list of common passwords against a security system. Such attacks may not be able to break into any specific account, but when used against accounts at scale, they generate enough successes to be worth the effort.

Against a moderately stringent setting, the researcher team's master prints matched with anywhere from two or three percent of the records in the different commercial platforms up to about 20 percent, depending on which prints they tested.

Overall, the master prints got 30 times more matches than the average real fingerprint—even at the highest security settings, where the master prints didn't perform particularly well. Think of a master print attack, then, like a password dictionary attack, in which hackers don't need to get it right in one shot, but instead systematically try common combinations to break into an account. The researchers note that they did not make capacitive printouts or other replicas of their machine learning-generated master prints, which means they didn't attempt to unlock real smartphones.

However, it is important to notice that most small area sensors today **are not** minutiae matchers, that's why even if the method developed by these researchers looks pretty efficient, the scope of that attack is more limited than it appears.

Date of the attack: November 2018

Result of the attack: Successful impersonation of the user

Sources

[1] Alex Hern, "Fake fingerprints can imitate real ones in biometric systems – research", https://www.theguardian.com/technology/2018/nov/15/fake-fingerprints-can-imitate-real-fingerprints-in-biometric-systems-research/

[2] Philip Bontrager, Nasir Memon, Arun Ross, Aditi Roy, Julian Togelius, "DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution"

[3] Lily Hay Newman, "Machine Learning Can Create Fake 'Master Key' Fingerprints", https://www.wired.com/story/deepmasterprints-fake-fingerprints-machine-learning/

[4] « Des empreintes digitales qui déverrouillent tous les téléphones », https://fr.metrotime.be/2018/11/18/must-read/des-empreintes-digitales-qui-deverrouillent-tous-les-telephones/

Hack of Samsung Galaxy S10 ultrasonic fingerprint sensor

Taxonomy of the environment

Year	2019
Country	Unknown
Biometrics involved	Fingerprints
Biometrics matching involved	(1 : 1) matcher
Biometrics inspection system involved	Ultrasonic fingerprint scanner
Biometrics AFIS or ABIS?	None
Objective of the Fraud	Fool the fingerprint scanner
Asset obtained by performing the attacks	Unlock the phone

Samsung Galaxy S10

Type of attack: 1 **Level of attack:** High

Author of the attack: A security researcher going by the name of Darkshark on Imgur

Victim of the attack: Samsung galaxy S10 owner

Description of the attack

One of the big new feature announcements with the launch of the Samsung Galaxy S10 smartphone was the all new “in-display” fingerprint scanner for the S10 and S10+ models. But, unlike all the other 2019 flagship Android models, the additional security offered by the ultrasonic fingerprint sensor was the unique selling point highlighted by Samsung.

The difference with the ultrasonic fingerprint scanner in the Galaxy S10 and S10+ smartphones compared to the more traditional capacitive scanners is that it can capture a 3D image rather than a 2D one. By using very high-frequency ultrasonic soundwaves, the scanner can map a fingerprint in quite astonishing detail which includes things like ridges and pores as well as just the 'flat' patterns we are more used to seeing. With this technology, the Samsung device is capable of creating an intricate 3D map of the owner’s fingerprint. A map that captures depth data across different points on the scanner, making the resulting map very detailed in all dimensions.

The scanner has been hacked in April 2019 by a security researcher, going by the name of darksark on Imgur, with a 3D-printed copy of his thumbprint from a photograph of a latent print on a wine glass. Indeed, the researcher was able to use a photograph of his fingerprint from a wine glass and, using Photoshop, create an alpha mask from it. This mask was then exported to 3ds Max software in order to create a geometry displacement to get highly detailed and raised 3D model. It was then just a matter of printing that model from his AnyCubic Photon LCD resin printer which has an accuracy-level down to 10 microns. This ensured all the

ridges of the fingerprint were properly rendered. The time to print was 13 minutes, after which the resulting fake fingerprint unlocked the Galaxy S10 every time.

However, the hack shouldn't have been successful as the ultrasonic sensor is supposed to detect liveness by sensing blood flow, which darkshark points out seems not to be the case, perhaps due to changes made when Samsung updated the software for the in-display sensor to deal with performance issues a few weeks before the hack attempt. The researcher says that the technique could be replicated to steal latent prints from distance and break into a stolen phone, as well as biometrically secured accounts such as a bank account for instance.

Date of the attack: April 2019

Result of the attack: Successful impersonation of the user

Sources

[1] Darkshark, "I attempted to fool the new Samsung Galaxy S10's ultrasonic fingerprint scanner by using 3d printing. I succeeded.", https://imgur.com/gallery/8aGqsSu/

[2] Davey Winder, "Samsung Galaxy S10 Fingerprint Scanner Hacked - Here's What You Need To Know", https://www.forbes.com/sites/daveywinder/2019/04/06/samsung-galaxy-s10-fingerprint-scanner-hacked-heres-what-you-need-to-know/#6a0c2bc45d42/

[3] Chris Burt, "Hack of Samsung Galaxy S10 ultrasonic fingerprint sensor suggests no liveness detection", https://www.biometricupdate.com/201904/hack-of-samsung-galaxy-s10-ultrasonic-fingerprint-sensor-suggests-no-liveness-detection/

Hack of OnePlus 6T and 7 Pro “in-display” fingerprint sensors

Taxonomy of the environment

Year	2019
Country	United States of America
Biometrics involved	Fingerprints
Biometrics matching involved	(1 : 1) matcher
Biometrics inspection system involved	Optical fingerprint scanner
Biometrics AFIS or ABIS?	None
Objective of the Fraud	Fool the fingerprint scanner
Asset obtained by performing the attacks	Unlock the phone

One Plus 7 Pro

Type of attack: 1 **Level of attack:** Basic

Author of the attack: Max Tech (name of the YouTube channel)

Victim of the attack: One Plus 6T or 7 Pro owner

Description of the attack

The brand new One Plus 7 Pro is equipped with an optical “in-display” fingerprint sensor. This technology has the advantage to be very fast compared to other smartphones.

However, even if the sensor is very fast, it can be hacked with some tinfoil and glue in few minutes. The process itself is rather simple. It basically entails creating a rudimentary mold of a fingerprint using aluminum foil, a dab of hot glue, and a little bit of Elmer's glue. It's a cheap hack, in other words, albeit an effective one on the OnePlus 7 Pro. Incidentally, the same method was proven to work on the previous generation OnePlus 6T, which also equipped with an optical “in-display” fingerprint sensor.

YouTube channel Max Tech demonstrated the hack. All it entailed was putting a dab of hot glue on a piece of aluminum foil, wetting the thumb, and pressing a fingerprint into the glue. After it dries, it can be filled in with Elmer's glue, then gently peeled off the aluminum foil. The result is a mold of a fingerprint that is detected by the OnePlus 7 Pro.

It's a rather quick and easy hack, at least in principal. To put this to use, however, it becomes far more difficult. After all, it's not as though OnePlus 7 Plus owners are going to volunteer their fingerprints to a hacker. So, in that regard, this is not really a practical hack.

Incidentally, the same method is ineffective on Samsung's Galaxy S10+. That's likely because Samsung implemented an ultrasonic fingerprint sensor. It's slower than the optical sensor in the OnePlus 7 Pro, but captures additional depth data for a 3D scan that is a bit more secure.

Date of the attack: May 2019

Result of the attack: Successful impersonation of the user

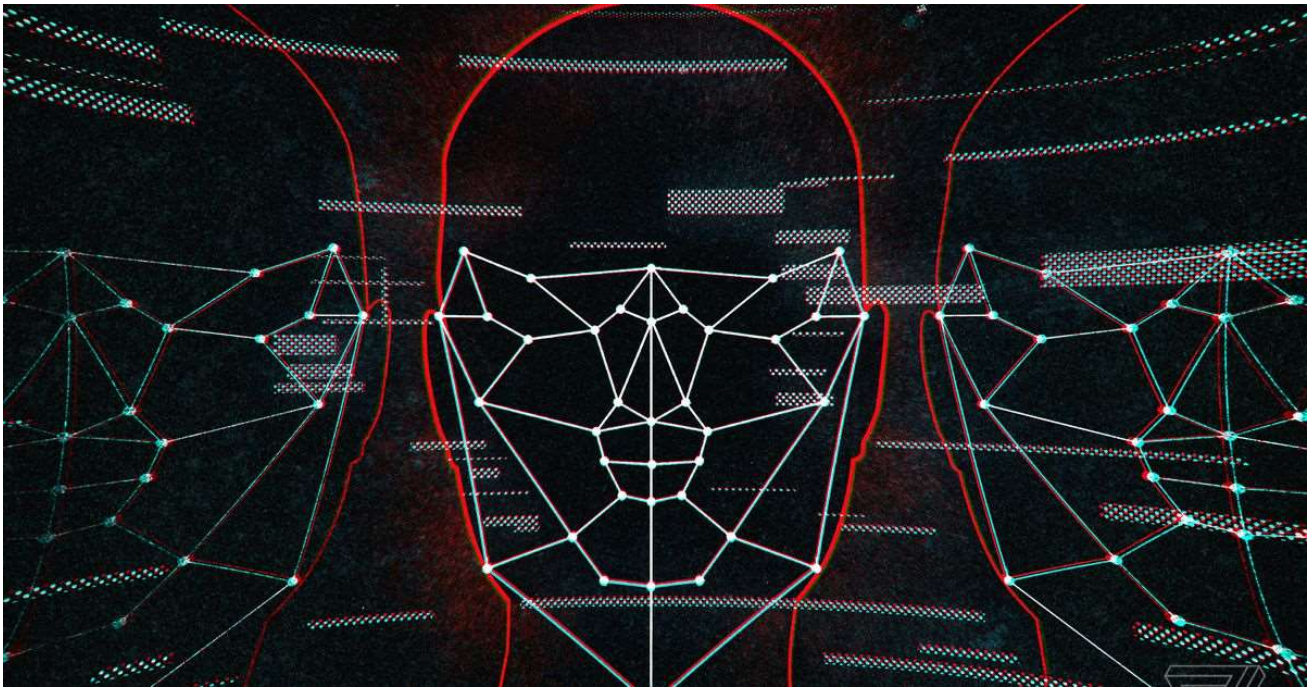
Sources

[1] Chris Burt, "OnePlus 7 Pro optical in-display fingerprint sensor easily spoofed, Apple selects acoustic sensing",https://www.biometricupdate.com/201905/oneplus-7-pro-optical-in-display-fingerprint-sensor-easily-spoofed-apple-selects-acoustic-sensing/

[2] Paul Lilly, "OnePlus 7 Pro In-Display Fingerprint Sensor Hacked In Minutes With Glue", https://hothardware.com/news/oneplus-7-pro-fingerprint-sensor-hacked-minutes-glue/

[3] Max Tech, "OnePlus 7 Pro Fingerprint Scanner HACKED!", https://www.youtube.com/watch?v=TJ6H-Ww22Kw/

C. Facial



Ice Cream Sandwich Face Unlock feature compromised

Taxonomy of the environment

Year	2011
Country	Malaysia
Biometrics involved	Face recognition
Biometrics matching involved	(1 : 1) matcher
Biometrics inspection system involved	Face recognition camera
Biometrics AFIS or ABIS?	None
Objective of the Fraud	Fool the face recognition scanner
Asset obtained by performing the attacks	Unlock the phone

Samsung Galaxy Nexus

Type of attack: 1 **Level of attack:** Basic

Author of the attack: SoyaCincau

Victim of the attack: Samsung Galaxy Nexus owner

Description of the attack

The Face Unlock feature in Android 4.0 for the Galaxy Nexus unlocks the phone using facial recognition software. According to Google, the "Face Unlock" feature in Ice Cream Sandwich can't be fooled by images.

A video demonstration created by mobile blogger from SoyaCincau shows that the Face Unlock feature can be fooled by showing it a mere image of the face used to set up the locking mechanism. The video shows someone unlocking a Galaxy Nexus running Android 4.0, also known as Ice Cream Sandwich, by holding in front of the device a digital photo taken of him that is displayed on another phone.

A Google representative contacted by CNET said the feature is considered low security and experimental. Even the interface warns users that "Face Unlock is less secure than a pattern, PIN, or password" and that “someone who looks similar to you could unlock your phone”.

Skeptics are claiming the blogger registered the photo in the Galaxy Nexus’ Face Unlock, and not his actual face. Facial recognition technology requires a straight-on view of your face for both registration and recognition. A typical photo of you probably will not fit that parameter (unless you take a lot of mugshots). That appears to be what they did with the Galaxy Nexus at SoyaCincau. It looks unintentional as they appear to have established the test on the spot. Furthermore, it is normal to look directly at the front camera when taking a self-photo, which is also required to register your face for recognition.

Date of the attack: November 2011

Result of the attack: Successful impersonation of the user

Sources

[1] SoyaCincau, "Ice Cream Sandwich Face Unlock feature compromised", https://www.youtube.com/watch?time_continue=5&v=BwfYSR7HttA/

[2] Elinor Mills, "Digital image can dupe Android face-based lock", https://www.cnet.com/news/digital-image-can-dupe-android-face-based-lock/

[3] Sumocat, "Android Ice Cream Sandwich Face Unlock Tricked by Photo", https://www.gottabemobile.com/android-ice-cream-sandwich-face-unlock-tricked-by-photo-but-its-only-a-trick/

Logging into a bank account with a high-quality video

Taxonomy of the environment

Year	2015
Country	United States of America
	Face recognition
Biometrics matching involved	(1 : 1) matcher
Biometrics inspection system involved	Face recognition system
Biometrics AFIS or ABIS?	None
Objective of the Fraud	Fool the face recognition scanner
Asset obtained by performing the attacks	Have access to a bank account

Type of attack: 1 **Level of attack:** Basic

Author of the attack: Dan Moren

Victim of the attack: Himself

Description of the attack

After seeing that the Chinese retail giant Alibaba decided to let the customers purchase goods and authorize payments using facial recognition, the journalist Dan Moren from Popular Science decided to see if it would be hard to trick a facial recognition system.

As he writes in his article, it is easy today with social media to find high quality images or videos of someone's face. So, he tried to see if pictures of himself could give him access to his bank account that uses face recognition as authentication. Fortunately, the face recognition system of his bank gets a liveness detection based on blinking, so a simple image of himself did not give him access to his bank account.

For his second try, he printed out an 8-by-10 glossy photograph of his face, then took a razor and cut out the eyes. He then peered through the holes and tried to fool his phone into recognizing him, but it didn't succeed. According to him, the scale wasn't quite right, so he couldn't get his eyes to line up perfectly. For him, it's possible that a better photo might succeed.

His last try was the good one to fool his bank app. He shot a quick video of himself, blinking included. When the banking app prompted him to look into the camera for the facial authentication-based login, he positioned the phone's front-facing camera in front of a monitor displaying the video. The spoofing tactic successfully logged Moren into his banking account. In doing so, Moren makes a convincing argument that facial recognition should not be used for biometric authentication since photos and videos of faces can be easily found on the Internet.

Date of the attack: March 2015

Result of the attack: Successful impersonation of the user

Sources

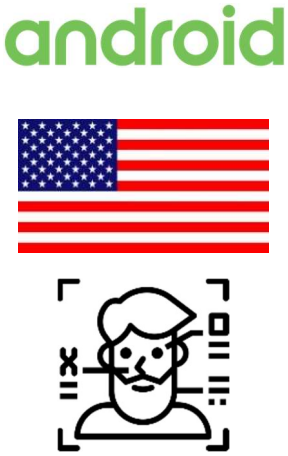
[1] Dan Moren, "Face Recognition Security, Even With A 'Blink Test,' Is Easy To Trick", https://www.popsci.com/its-not-hard-trick-facial-recognition-security/

[2] Justin Lee, "Can facial recognition systems be spoofed using high quality video?", https://www.biometricupdate.com/201503/can-facial-recognition-systems-can-be-spoofed-using-high-quality-video/

Hack of facial recognition systems with liveness detection

Taxonomy of the environment

Year	2016
Country	United States of America
Biometrics involved	Face recognition
Biometrics matching involved	(1 : 1) matcher
Biometrics inspection system involved	Face recognition system
Biometrics AFIS or ABIS?	None
Objective of the Fraud	Fool the face recognition scanner
Asset obtained by performing the attacks	Unlock the phone



Type of attack: 1 **Level of attack:** High

Author of the attack: Researchers from University of North Carolina

Victim of the attack: Phone owner

Description of the attack

At the Usenix security conference, security and computer vision specialists from the University of North Carolina presented a system that uses digital 3-D facial models based on publicly available photos and displayed with mobile virtual reality technology to defeat facial recognition systems. A VR-style face, rendered in three dimensions, gives the motion and depth cues that a security system is generally checking for. The researchers used a VR system shown on a smartphone's screen for its accessibility and portability.

Given one or more photos of the target user, they first automatically extract the landmarks of the user's face. These landmarks capture the pose, shape, and expression of the user. Next, they estimate a 3D facial model for the user, optimizing the geometry to match the observed 2D landmarks. Once they have recovered the shape of the user's face, they use a single image to transfer texture information to the 3D mesh. Transferring the texture is non-trivial since parts of the face might be self-occluded (e.g., when the photo is taken from the side). The texture of these occluded parts must be estimated in a manner that does not introduce too many artifacts. Once the texture is filled, they have a realistic 3D model of the user's face based on a single image. However, despite its realism, the output of stage is still not able to fool modern face authentication systems. The primary reason for this is that modern face authentication systems use the subject's gaze direction as a strong feature, requiring the user to look at the camera in order to pass the system. Therefore, they must also automatically correct the direction of the user's gaze on the textured mesh. The adjusted model can then be deformed to produce animation for different facial expressions, such as smiling, blinking, and raising the eyebrows. These expressions are often used as liveness clues in face authentication systems, and as such, they

need to be able to automatically reproduce them on their 3D model. Finally, they output the textured 3D model into a virtual reality system. Using this framework, an adversary can bypass both the face recognition and liveness detection components of modern face authentication systems.

The researchers tested their virtual reality face renders on five authentication systems—KeyLemon, Mobius, TrueKey, BioID, and 1D. All are available from consumer software vendors like the Google Play Store and the Apple Store and can be used for things like protecting data and locking smartphones. To test the security systems, the researchers had the subjects program each one to detect their real faces. Then they showed 3-D renders of each subject to the systems to see if they would accept them. In addition to making face models from online photos, the researchers also took indoor head shots of each participant, rendered them for virtual reality, and tested these against the five systems. Using the control photos, the researchers were able to trick all five systems in every case they tested. Using the public web photos, the researchers were able to trick four of the systems with success rates from 55 percent up to 85 percent.

For the UNC researchers, the most challenging part of executing their 3-D replica attack was working with the limited image resources they could find for each person online. But their study proved that with enough work, a hacker is able to use limited image that he could find on Facebook for instance, and fool a face recognition, even if it uses liveness detection.

Date of the attack: August 2016

Result of the attack: Successful impersonation of the user

Sources

[1] Yi Xu, True Price, Jan-Michael Frahm and Fabian Monrose, “Virtual U: Defeating Face Liveness Detection by Building Virtual Models from Your Public Photos”, *Proceedings of the 25th USENIX Security Symposium*, August 2016

[2] Justin Lee, “Facebook photos could be used to dupe facial recognition”, https://www.biometricupdate.com/201608/facebook-photos-could-be-used-to-dupe-facial-recognition/

Break into a bunch of Android phones

Taxonomy of the environment

Year	2018
Country	United States of America
Biometrics involved	Face recognition
Biometrics matching involved	(1 : 1) matcher
Biometrics inspection system involved	Face recognition camera
Biometrics AFIS or ABIS?	None
Objective of the Fraud	Fool the face recognition scanner
Asset obtained by performing the attacks	Unlock the phone

Type of attack: 1 **Level of attack:** Not Practical

Author of the attack: Thomas Brewster, a Forbes journalist

Victim of the attack: Android phones owners

Description of the attack

Thomas Brewster, a journalist from Forbes, tried to break the facial recognition systems of the hottest handsets running Apple's and Google's operating systems, namely a iPhone X, a Samsung S9, a Samsung Note 8, a LG G7 ThinQ and a OnePlus 6. He also tried to fool the Microsoft Hello facial recognition.

To fool the scanners, he used a 3D-printed head of one of them. The head was printed at Backface in Birmingham, U.K., where the journalist was ushered into a dome-like studio containing 50 cameras. Together, they combine to take a single shot that makes up a full 3D image. That image is then loaded up in editing software, where any errors can be ironed out. Backface then constructs the model with a 3D printer that builds up layers of a British gypsum powder. Some final touch-ups and colorings are added, and the life size head is ready within a few days, all for just over £300.

For all four Android phones, the spoof face was able to open the phone, though with differing degrees of ease. The iPhone X was the only one to never be fooled. Microsoft appeared to have done a fine job too. It's new Windows Hello facial recognition also didn't accept the fake head as real.

There were some disparities between the Android devices' security against the hack. For instance, when first turning on a brand new G7, LG warns the user against turning facial recognition on at all. "Face recognition is a secondary unlock method that results in your phone being less secure," it says, noting that a similar face can unlock your phone. The journalist precised that there was no surprise then that, on initial testing, the 3D-printed head opened it straightaway.

There's a similar warning on the Samsung S9 on sign up. Whilst iris recognition wasn't duped by the fake head's misted-over eyes, facial recognition was tricked, albeit with a need to try a few different angles and lighting first. The result was the same for Note 8.

The OnePlus 6 came with neither the warnings of the other Android phones nor the choice of slower but more secure recognition. And, despite some sci-fi style face scanning graphics when registering a face, the phone instantly opened when presented with the fake head. It was, undoubtedly, the least secure of the devices Thomas Brewster tested.

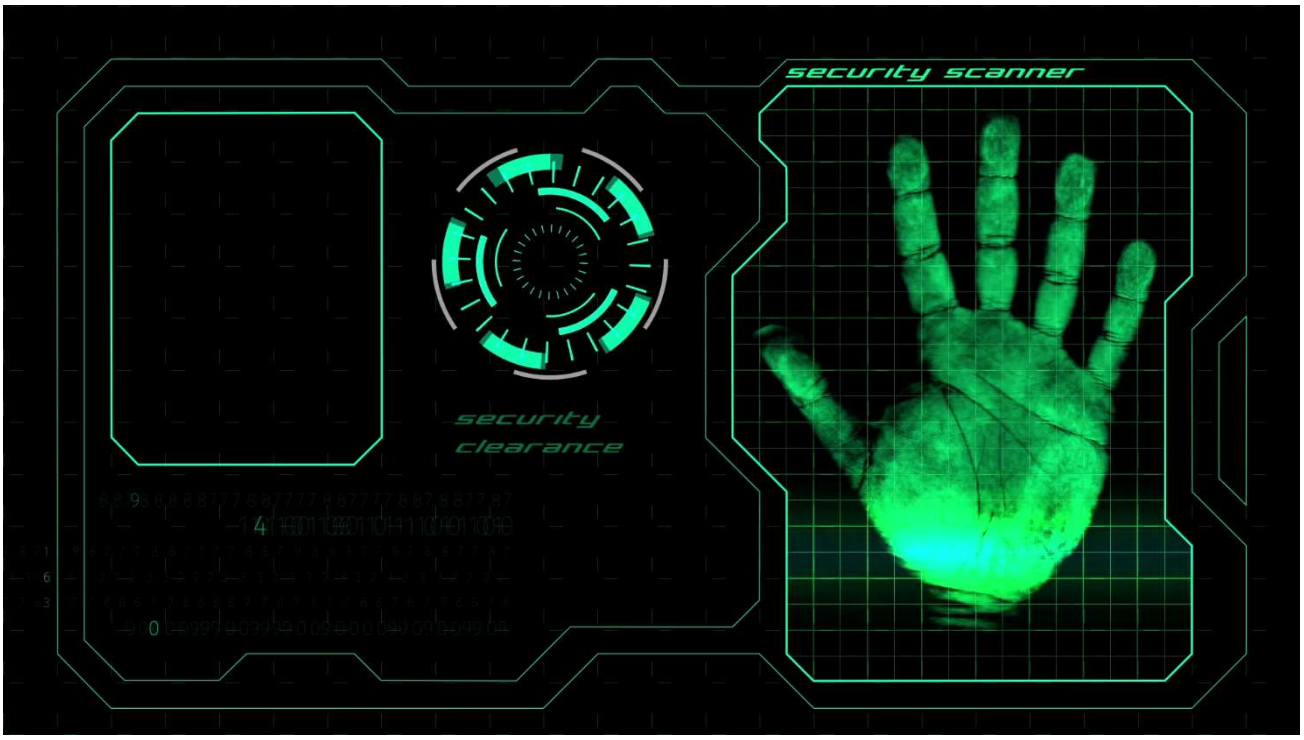
Date of the attack: December 2018

Result of the attack: Successful impersonation of the user

Sources

[1] Thomas Brewster, "We Broke Into A Bunch Of Android Phones With A 3D-Printed Head", https://www.forbes.com/sites/thomasbrewster/2018/12/13/we-broke-into-a-bunch-of-android-phones-with-a-3d-printed-head/#981872d13307/

D.Palm-vein



Spoof of Hitachi and Fujitsu palm vein recognition systems

Taxonomy of the environment

Year	2018
Country	Germany
Biometrics involved	Palm vein
Biometrics matching involved	(1 : 1) matcher or (1 : N) matcher
Biometrics inspection system involved	
Biometrics AFIS or ABIS?	ABIS
Objective of the Fraud	Fool the palm vein recognition system
Asset obtained by performing the attacks	Enter an unauthorized area

Type of attack: 1 **Level of attack:** High

Author of the attack: Jan Krissler and Julian Albrecht from the Chaos Communication Club

Victim of the attack: Companies which use palm vein recognition system from Hitachi or Fujitsu

Description of the attack

Security researchers at Chaos Communication Congress in Leipzig, Germany have demonstrated a successful spoof attack on a hand-vein biometric reader using a modified camera and a fake hand made out of wax.

Jan Krissler, also known as Starbug, and Julian Albrecht, also known as Motherboard, created the fake by removing the infrared filter from an SLR camera, and taking 2,500 pictures over 30 days to capture a useable image of veins under the subject's skin. Krissler says the photos can be taken from 5 meters away. They used the image to create a vein pattern in a model hand made out of wax, which was accepted by two different biometric from Hitachi and Fujitsu, which cover around 95 percent of the vein authentication market.

Even the demonstration didn't go entirely to plan; the researchers had to put one of the scanners underneath a table to stop the hall's lights from interfering with the hack. However, now that the method has been proven to work, other researchers will likely build upon it to create a process that's more efficient and reliable.

Vein authentication isn't currently used in any mainstream smartphones (today there is only the LG 2019 flagship which own this recognition system). Instead it is more commonly used to control access to buildings such as Germany's signals intelligence agency.

The researchers disclosed the details of their research to Fujitsu and Hitachi. According to Krissler they presented their research to employees from Hitachi while Fujitsu did not reply back to them in length.

In a statement provided to Heise Online, a Fujitsu spokesperson sought to downplay the implications of the hack and said that it could only succeed under laboratory conditions and that it wouldn't likely work in the real world.

But, Krissler and Albrecht only spent around a month working on this research. A well-funded and resourced adversary, perhaps a state that is trying to break into an area secured with vein authentication, could likely replicate this research on a larger and more efficient scale. That may be particularly worrying when the sort of targets protected with vein authentication are sometimes exactly the ones that a state may want to target.

Date of the attack: December 2018

Result of the attack: Successful impersonation of the user

Sources

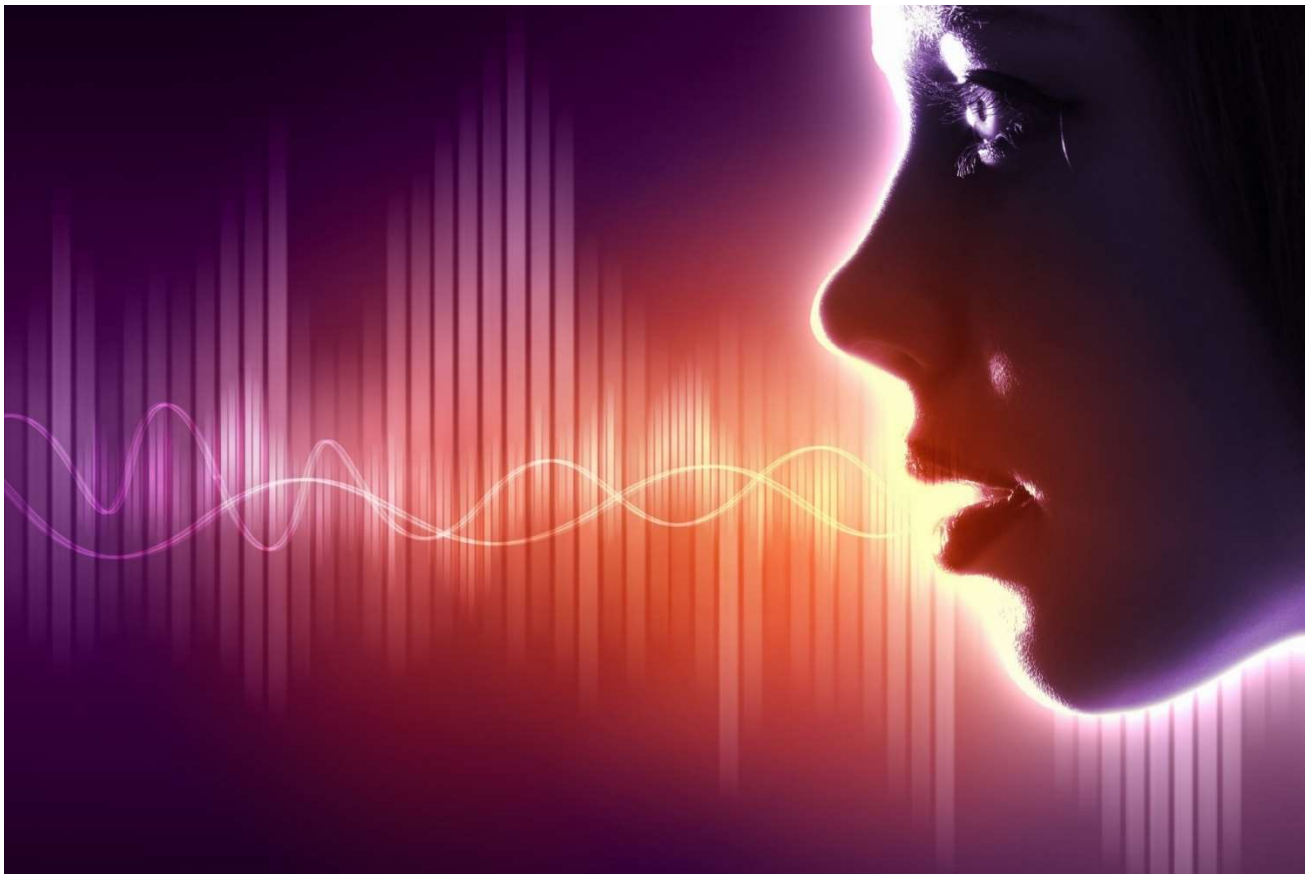
[1] Chris Burt, "Researchers spoof biometric palm vein recognition system with inexpensive fake", https://www.biometricupdate.com/201901/researchers-spoof-biometric-palm-vein-recognition-system-with-inexpensive-fake/

[2] Joseph Cox and Max Hoppenstedt, "Hackers Make a Fake Hand to Beat Vein Authentication", https://www.vice.com/en_us/article/59v8dk/hackers-fake-hand-vein-authentication-biometrics-chaos-communication-congress/

[3] Jon Porter, "Hackers use a fake wax hand to fool vein authentication security", https://www.theverge.com/2018/12/31/18162541/vein-authentication-wax-hand-hack-starbug/

[4] "35C3: Mit Venenbild auf Handattrappe Geld abheben oder beim BND einbrechen", https://www.heise.de/newsticker/meldung/35C3-Mit-Venenbild-auf-Handattrappe-Geld-abheben-oder-beim-BND-einbrechen-4259637.html/

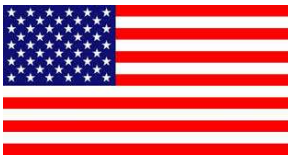
E. Voice

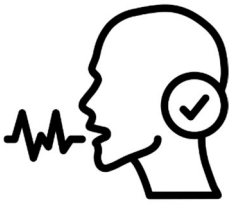


Spoof of voice authentication systems with automated voice imitation

Taxonomy of the environment

Year	2015
Country	United States of America
Biometrics involved	Voice
Biometrics matching involved	(1 : 1) matcher or (1 : N) matcher
Biometrics inspection system involved	Voice recognition system
Biometrics AFIS or ABIS?	ABIS
Objective of the Fraud	Fool the voice recognition system
Asset obtained by performing the attacks	Voice impersonation of an individual





Type of attack: 1

Level of attack: Substantial

Author of the attack: Dibya Mukhopadhyay, Maliheh Shirvanian and Nitesh Saxena from University of Alabama at Birmingham

Victim of the attack: A lambda user of voice recognition system

Description of the attack

A research team at University of Alabama at Birmingham has discovered that voice impersonation can be applied to trick both automated and human verification for voice authentication systems.

The research was authored by UAB graduate students Dibya Mukhopadhyay and Maliheh Shirvanian, researchers in UAB's Security and Privacy in Emerging computing and networking Systems (SPIES) Lab, along with Nitesh Saxena, Ph.D., the director of the SPIES Lab and associate professor of computer and information sciences at UAB.

The team recently presented the research, which explores how attackers equipped with audio samples of another person's voice could compromise their security, safety and privacy, at the European Symposium on Research in Computer Security (ESORICS) in Vienna, Austria.

Using an off-the-shelf voice-morphing software, the researchers were able to develop a voice impersonation attack for the purpose of breaching automated and human verification systems.

A would-be attacker could record a person's voice using a few techniques, including being in close proximity to the speaker, conducting a spam call, by scouring the Internet for audiovisual clips, and by hacking into cloud servers that store audio data.

Using software that automates speech synthesis such as voice morphing, allows attackers to create a near-duplicate of an individual's voice by using just few audio samples. The technology can then transform the attacker's voice to state any arbitrary message in the voice of the victim.

In its research, the UAB team investigated the consequences of stealing voices in two voice authentication-dependent applications and scenarios. The first application involved a voice biometrics system that uses the so-called unique features of a person's voice for authentication purposes. Researchers found that once the study's participants were able to fool the voice biometrics system by using fake voices, they could gain full access to the device or service.

The second application explored how stealing voices affected human communications, in which the researchers used voice-morphing tool to imitate Oprah Winfrey and Morgan Freeman in a controlled study environment. The study's participants were able to make the voice morphing system speak nearly any phrase in the victim's tone and vocal manner to launch an attack that could potentially jeopardize their reputation and security. The results clearly showed how automated verification algorithms were largely ineffective in blocking any of the attacks developed by the research team, with the average rate of rejecting fake voices being less than 10 to 20 percent for most victims.

In two online studies with about 100 participants, researchers found that participants rejected the morphed voice samples of celebrities as well as somewhat familiar users about half the time.

Their research showed that voice conversion poses a serious threat, and their attacks can be successful for a majority of cases, according to Saxena. Saxena made a few recommendations on ways that people can prevent their voice from being stolen, which included increasing their awareness of these potential attacks, and being wary of uploading audio clips of their voices on social media.

Date of the attack: September 2015

Result of the attack: Successful impersonation of the user

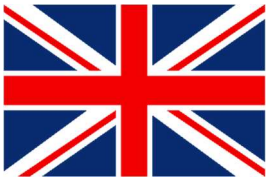
Sources

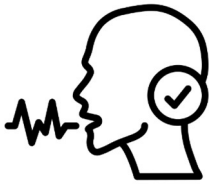
[1] Justin Lee, "UAB researchers find that automated voice imitation can spoof voice authentication systems", https://www.biometricupdate.com/201509/uab-researchers-find-that-automated-voice-imitation-can-spoof-voice-authentication-systems/

HSBC voice recognition ID system tricked by twins

Taxonomy of the environment

Year	2017
Country	United Kingdom
Biometrics involved	Voice
Biometrics matching involved	(1 : 1) matcher
Biometrics inspection system involved	Voice recognition system
Biometrics AFIS or ABIS?	ABIS
Objective of the Fraud	Fool the voice recognition system
Asset obtained by performing the attacks	Access to the bank account of his twin brother





Type of attack: 1 **Level of attack**: Basic

Author of the attack: Joe Simmons, twin brother of Dan Simmons

Victim of the attack: Dan Simmons, a BBC reporter

Description of the attack

Security software designed to prevent bank fraud has been fooled by a BBC reporter and his twin. BBC reporter Dan Simmons set up an HSBC account and signed up to the bank's voice ID authentication service. But the bank let Dan Simmons' non-identical twin, Joe, access the account via the telephone after he mimicked his brother's voice.

HSBC claims is secure due to each person having a unique voice, measured through 100 different characteristics. The BBC reported that while Simmons' twin was not able to withdraw any money over the phone, Joe could check the balance and recent transactions of his brother's account and had the option to transfer money between accounts.

HSBC was informed of the potential hole in its voice identification system and told the BBC that it would "review" ways to make the voice ID system more sensitive so that it could not be tricked by inquisitive twins. According to a spokesman from HSBC, twins do have a similar voiceprint, but the introduction of this technology has seen a significant reduction in fraud, and has proven to be more secure than PINs, passwords and memorable phrases.

However, there appear to be a few flaws in HSBC's system, with a BBC reporter having found that it allowed them to still attempt to access their HSBC account after deliberately failing the voice ID check on 20 separate occasions over a 12-minute period.

Date of the attack: May 2017

Result of the attack: Successful impersonation of the user

Sources

[1] Dan Simmons, "BBC fools HSBC voice recognition security system", https://www.bbc.com/news/technology-39965545/

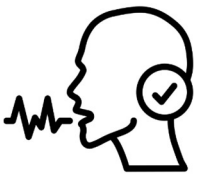
[2] Patrick Collinson, "HSBC voice recognition system breached by customer's twin", https://www.theguardian.com/business/2017/may/19/hsbc-voice-recognition-system-breached-by-customers-twin/

[3] Roland Moore-Colyer, "HSBC Voice Recognition ID System Tricked By Twins", https://www.silicon.co.uk/security/hsbc-voice-recognition-212519/

Voice recognition systems easily tricked by impersonators

Taxonomy of the environment

Year	2017
Country	Finland
Biometrics involved	Voice
Biometrics matching involved	(1 : 1) matcher or (1 : N) matcher
Biometrics inspection system involved	Voice recognition system
Biometrics AFIS or ABIS?	ABIS
Objective of the Fraud	Fool the voice recognition system
Asset obtained by performing the attacks	Voice impersonation of an individual



Type of attack: 1 **Level of attack:** Basic

Author of the attack: Researchers from University of Eastern Finland

Victim of the attack: A lambda user of voice recognition system

Description of the attack

Researchers from University of Eastern Finland have published a study in which they demonstrate that skillful impersonators are able to fool high tech voice recognition systems. These systems generally aren't efficient yet in recognizing voice modifications, a vulnerability that poses significant security concerns, according to the researchers.

The researchers did not indicate which products they tested, although many mobile brands are increasingly equipped with applications that function with voice commands, such as Apple's Siri or Microsoft's Cortana for instance.

The widespread use of electronic services has increased the demand of applications that use voice to recognize the speaker either for authentication purposes or for public safety.

Voice attacks against speaker recognition can be done using technical means, such as voice conversion, speech synthesis and replay attacks. The scientific community is systematically developing techniques and countermeasures against technically generated attacks. However, voice modifications produced by a human, such as impersonation and voice disguise, cannot be easily detected with the developed countermeasures, according to the research.

The study finds that voice impersonation is common in the entertainment industry, with professionals and amateurs alike copying the voice characteristics of speakers, particularly public figures.

The practice of "voice disguise", whereby speakers alter the way they speak in order to avoid being recognized, can frequently occur in situations that don't require face-to-face communication. As a result, criminals can blackmail unsuspecting people or conduct threatening calls. These threats call for a need to improve the accuracy of voice recognition systems so that they aren't susceptible to human-induced voice modifications.

The researchers analyzed the speech of two professional impersonators mimicking eight Finnish public figures, as well as acted speech from 60 Finnish speakers who participated in recording sessions. The speakers were asked to alter their voices to make themselves sound older or younger, and many of them were able to successfully fool the speech systems.

Date of the attack: November 2017

Result of the attack: Successful impersonation of the user

Sources

[1] R. González Hautamäki, M. Sahidullah, V. Hautamäki, and Tomi Kinnunen, "Acoustical and Perceptual Study of Voice Disguise by Age Modification in Speaker Verification"

[2] Justin Lee, "Researchers find voice recognition systems easily tricked by impersonators", https://www.biometricupdate.com/201711/researchers-find-voice-recognition-systems-easily-tricked-by-impersonators/

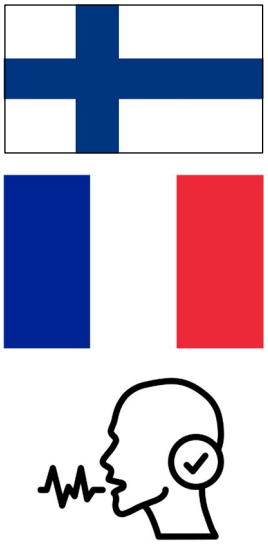
[3] "New university research warning over voice recognition biometric security", https://www.computing.co.uk/ctg/news/3021015/voice-impersonators-can-fool-speaker-recognition-systems-easily-says-study/

[4] "Research Says Impersonators Can Fool Voice Recognition Systems", https://www.securitymagazine.com/articles/88494-research-says-impersonators-can-fool-voice-recognition-systems/

Voice mimicry attacks assisted by ASV

Taxonomy of the environment

Year	2019
Country	Finland and France
Biometrics involved	Voice
Biometrics matching involved	(1 : N) matcher
Biometrics inspection system involved	Automatic Speaker Verification (ASV)
Biometrics AFIS or ABIS?	ABIS
Objective of the Fraud	Fool the voice recognition system
Asset obtained by performing the attacks	Use one ASV system to emulate the broad speaker ranking of another targeted ASV system



Type of attack: 1 **Level of attack:** High

Author of the attack: Researchers from University of Eastern Finland and Université de Lorraine

Victim of the attack: A lambda user of voice recognition system

Description of the attack

Researchers from University of Eastern Finland and Université de Lorraine realize a study in which they simulate a scenario, where a publicly available ASV (Automatic Speaker Verification) system is used to enhance mimicry attacks against another closed source ASV system. In specific, ASV technology is used to perform a similarity search between the voices of recruited attackers and potential target speakers (7,365) from VoxCeleb corpora to find the closest targets for each of the attackers.

Their goal is to gain insight how well similarity rankings transfer from the attacker's ASV system to the attacked ASV system, whether the attackers can improve their attacks by mimicking, and how the properties of the voices of attackers change due to mimicking. For the ASV experiments, they use i-vector technology in the attacker side, and x-vectors in the attacked side. For the listening tests, they recruit listeners through crowdsourcing.

Biometric data uploaded to the Internet in large quantities, including human voice samples, open up potential for misuse whenever the same biometric identifiers are adopted for strong user authentication to regulate access to personal data records, bank accounts and other services. Their study addressed a potential risk related to combination of public-domain automatic speaker verification (ASV) technology and public-domain voice data. The former is used as a search tool to identify potential target speakers to be mimicked. Their results suggest that human mimicry is a rather special skill and less effective in spoofing modern ASV systems

compared to voice conversion, text-to speech, and replay. In specific, none of their six attackers received high detection scores for their attacks from their simulated public-domain or attacked ASV systems. Similar negative findings have been reported in earlier studies and are often speculated to be due to difficulty of humans to mimic accurately low-level spectral cues employed by ASV systems.

One of their motivations was to re-assess whether speech mimicry—one of the weakest known attacks against ASV — might be made substantially stronger (or more practical) when the target speakers are selected using ASV. They approached this question from two perspectives. On the one hand, they wanted to find out how the score ranges associated with broad target speaker rank (closest, median, further) transfer from the attacker's ASV to the attacked ASV. This is the technology dimension of their attack model. On the other hand, they wanted to isolate the effect of the mimicry effort by collecting attackers' voice samples both 'before' (zero-effort attack) and 'after' (mimicry attack) listening to the target speaker's voice. This allows them to analyze the changes in attacker-to-target log-likelihood ratio (LLR) scores due to mimicry effect alone. This is the human dimension of their attack model.

Concerning the broad target speaker rank, the score relations generalize well from the attacker's ASV system to the attacked ASV system: LLR(closest target) > LLR(median target) > LLR(furthest target) relationship was retained both for Finnish and non-Finnish targets. This suggests that one could, indeed, use one ASV system (here, i-vector PLDA) to emulate the broad speaker ranking of another, targeted ASV system (here, x-vector PLDA).

That's why they underlined that, with an increasing number of video and voice samples posted online, it is not only the security, but user privacy, that deserves attention.

Date of the attack: 2019

Result of the attack: Successful impersonation of the user

Sources

[1] V. Vestman, T. Kinnunen, R. Gonzalez Hautamäki, M. Sahidullah, "Voice Mimicry Attacks Assisted by Automatic Speaker Verification", *Computer Speech & Language,* 2019

III. Conclusion

This catalog gives a cartography of known biometrics attacks.

It is also demonstrating the need to evaluate the resistance to potential attacks on the different parts of biometrics system before going live with a project implementing Biometrics.

It allows Cabinet Louis Reynaud to highlight the universe in which it is expert.

We work with mastery in performance (ISO/IEC 19795) and attack detection (ISO/IEC 30107), thanks to the knowledge of our senior experts on technical expertise on biometrics and on PAIs.

Thanks to our technology evaluation laboratory located at La Ciotat, in Provence/Cote d'Azur - FRANCE, we are able to make or identify PAIs but also to make performance evaluation (FAR/FRR).

Moreover, Cabinet Louis Reynaud is able to make test plans and integrations of all biometrics and technologies embedding these biometrics (Server, computer, smart phone, smart card, secure element, smart watch, IOT Devices).

To be more precise, our laboratory, associated with our expertise, allows us to do:

- Performance testing:
  - Biometric recognition engine (e.g. FAR/FRR)
  - Liveness detection
- Conformance and functionality testing:
  - International standards
  - API's
- Security testing:
  - Template protection
  - Algorithms integrity
  - Secure application programming against side channel attacks
- Test plan definition
- Test targets: Server, computer, smart phone, smart card, secure element, smart watch, IOT

Devices

Hope that you have enjoyed the reading of our Biometrics attack catalog. Should you have any feedback that you would like to provide us, please send them @ info@cabinet-louis-reynaud.fr

IV. References

Rubal Jain, Chander Kant, “Attacks on biometric systems: an overview”, *International Journal of Advances in Scientific Research,* 2015; 1

Tiwalade O. Majkodumni, Francis E. Idachaba, “A review of the fingerprint, speaker recognition, face recognition and iris recognition based biometric identification technologies”, *World Congress on Engineering,* 2011; 2

Jain Anil K., Ross Arun and Salil Prabhakar, “An introduction to biometric recognition”, *IEEE Transactions on circuits and systems for video technology,* 2004; 14

Abdulmonam Omar Alaswad, Ahlal H. Montaser, and Fawzia Elhashmi Mohamad, “Vulnerabilities of Biometric Authentication “Threats and Countermeasures”, *International Journal of Information & Computation Technology*, 2014; 4

U. Latha and K. Rameshkumar, “A Study on Attacks and Security Against Fingerprint Template Database”, *International Journal of Emerging Trends & Technology in Computer Science*, 2013; 2

Joseph Mwema, Michael Kimwele, Stephen Kimani, “A Simple Review of Biometric Template Protection Schemes Used in Preventing Adversary Attacks on Biometric Fingerprint Templates”, *IJCTT*, 2015; 20

ISO/IEC 30107-1, Information technology — Biometric presentation attack detection — Part 1: Framework

Cabinet Louis Reynaud, “Biometrics attacks ratings”, August 2019

V. Figures references

Fig.5, ISO/IEC 30107-1, Information technology — Biometric presentation attack detection — Part 1: Framework

Tab.1, ISO/IEC 30107-1, Information technology — Biometric presentation attack detection — Part 1: Framework