DATA PRIVACY DAY 2017

A Silver BULLET

Privacy Risks With Biometrics

Powered by CYBERUSLABS

A SILVER BULLET

Many industry sectors are looking for the best access control methods. Financial, military, national security services and industry IT experts – all want to make sure that the right person has access to the right account, sensitive data or technological processes.

Passwords – the ubiquitous user login method is widely known to be the weakest link in cybersecurity today. Stolen passwords mean stolen identities.

Other user authentication/login methods such as: PIN codes, smart cards and SMSs have all been compromised. Their vulnerabilities generated efforts to search for more secure user authentication techniques. Biometric technology is becoming increasingly popular and at first glance appears to be the most secure. In its original concept only the physical presence of the authorized person would grant access to authorized accounts or other resources.

WHAT ARE BIOMETRICS?

"Biometrics refers to the automatic identifications of a person based on his or her physiological or behavioral characteristics"
Biometric recognition technology relies upon the physical characteristics of an individual, such as fingerprints, voiceprint, pattern of the iris of the eye and facial pattern. Examples of physiological biometric features include height, weight, body odor, the shape of the hand, the pattern of veins, retina or iris, the face and the patterns on the skin of thumbs or fingers (fingerprints).

Biometric technologies appear as the great opportunity for authorization and access management systems. Fascinating cutting edge technology is very appealing and seem to be a “silver bullet” that would replace all other user authentication systems. The bad news is that biometrics systems, which are starting to replace the password, come with some serious security risks of their own.

A GREAT NEW DANGER

Biometrics has been announced as the most secure and accurate user authentication technology but what seems to be its greatest strength i.e. the identification of a physical person using permanent and highly personal biometrics is also one its greatest weaknesses. Why? Because a person's biometric characteristics does not change over time. That includes the pattern in one's iris, retina or palm vein. They remain the same throughout the whole life. It also means that once stolen or compromised biometric data is unfortunately compromised forever. Every human being has a limited number of biometric features (face, fingers, eyes). In case of the authentication systems based on hardware elements (such as keys, badges), a compromised token can be revoked and replaced. Also, user IDs and passwords can be changed or reset when needed. However, when the biometric data are compromised this "reset" is not possible. In the event of biometric record leak or theft, users will have permanent and most private personal data in the hands of bad actors. The user has permanently lost control of that form of identification.

With traditional methods of user authentication – even if they are not secure or easy to use – when credentials are stolen they can be changed, but with one's iris is not the case.

> **"YOU CAN ALWAYS GET A NEW CREDIT CARD. YOU CAN ALWAYS CREATE A NEW PASSWORD. [IT'S] REALLY HARD TO GET NEW FINGERS. YOU ONLY HAVE TEN OF THEM AND ONCE THAT INFORMATION LEAKS, IT'S OUT AND THERE'S NOTHING YOU CAN DO.**
>
> Marc Goodman
> Interpol and the FBI Advisor

The same characteristics that make biometrics seemingly secure are what also make them so intrusive. When our

passwords are stolen we simply are able to change them. But we are not able so easily change our fingerprints or our faces. Or at least not without a huge effort. In this case disadvantages of using biometrics out weight profits. Recent experience shows that storing any kind of personal data presents a tantalizing bounty to cyber criminals and hackers. Jennifer Lynch, a senior staff attorney at the Electronic Frontier Foundation warns that "Data breaches are very common. If biometric information is stored on a mass scale it can be hacked into and stolen and we may lose control of it."

Billions of usernames and passwords has been already stolen and biometric data is not immune to this problem – in September 2015 fingerprints of 5.6 million US federal employees were stolen.
When the Office of Personnel Management was hacked, 5.6 million people's fingerprints were compromised. They included biometric data of secret agents. For these high security employees the result is that they are not able to work anymore. Changing their official identity will not help.

Biometric data isn't immune to the traditional techniques of cyberattacks and data theft. But there also other dangers related to biometric technologies. Some examples show how easy it may be to steal biometric data and misuse it. In his article "False sense of security spreading on a gigantic scale," Hitoshi Kokumai makes very interesting and important statement. He points out that fingerprint authentication in our smart phones are not used to make them more secure but rather as a form of convenience. What is even worse is the fact that, biometric data is stored on those devices, and they can simply be hacked. It looks that user authentication will widely relay upon biometrics and therefore they will be the targets for attacks. They will be compromised. Cyber criminals are likely already working on finding a way around protection systems.
Researchers from mobile security company Vkansee were able to break into Apple's Touch ID system with

a small piece of Play Doh in 2016 at the one of the biggest events of the technological world – a Mobile World Congress in Barcelona. This (unfortunately successful) experiment was similar to what security researcher Tsutomu Matsumoto did with a gummy bear a few years earlier to compromise another fingerprint sensor. A group of researchers at Michigan State University have published a paper in which they describe a method for spoofing a fingerprint reader with use of conductive ink printed with an ink jet printer in less than fifteen minutes. Even if some biometric systems are harder to crack than others, experience shows that no security system is impermeable. Biometric hackers from Germany's Chaos Computer Club bypassed Apple's Touch ID just days after its launch. He simply took a photo of a fingerprint on a glass surface. Later he used it to create a fake fingerprint that could unlock the smart phone.
A year later a member of the same hacking group, Jan Krissler, cloned the thumbprint of the German defense minister Ursula von der Leyen, after photographing her hand from a distance at a press conference.
Not only fingerprints can be spoofed. Some facial recognition tools can also be fooled just by use of high quality photos or videos. A team of researchers in Spain managed to trick eye-scanners with reverse engineered fake irises.

Only the tip of the iceberg.

There are also other dangers associated with biometrics. In addition to data theft, there are seven main points of attacks that expose vulnerabilities in biometric systems:

- Presenting fake biometrics or a copy at the sensor, for instance a fake finger or a face mask. It is also possible to try and resubmitting previously stored digitized biometrics signals such as a copy of a fingerprint image or a voice recording.
- Producing feature sets preselected by the intruder by overriding the feature extraction process.

- Tampering with the biometric feature representation: The features extracted from the input signal are replaced with a fraudulent feature set.
- Attacking the channel between the stored templates and the matcher: The stored templates are sent to the matcher through a communication channel. The data traveling through this channel could be intercepted and modified – There is a real danger if the biometric feature set is transmitted over the Internet.
- Corrupting the matcher: The matcher is attacked and corrupted so that it produces pre-selected match scores.
- Tampering with stored templates, either locally or remotely.
- Overriding the match result.

LEGAL ISSUES

Another problem is the legal status of most types of biometric data. Regulations are inconsistent and lagging today's technological capabilities. That also concerns the issue whether government agencies are allowed to collect biometric data without a person's knowledge. Recent EU regulations such as GDPR start mentioning biometric data in the legal context but they are very generic. That is a big problem from the point of view of privacy.

As a report by PricewaterhouseCoopers points out, even if new GDPR introduces the concept of biometrics in to the legal field in the EU many countries still have very different regulations in regard of the collection and transfer of biometric data. A company that holds such data – either on its own or through a third party provider in case of cloud computing systems – will find themselves in a world of serious regulatory problems in case the biometric data is stolen or misused.
Once a user's fingerprints, face, iris or DNA profile becomes a digital data it will be difficult to protect. People are becoming increasingly aware of the very thin and porous boundary between commercial gathering and use of biometric data and government's access to it.

MARKET

We cannot forget that the biometric technologies industry is a large and fast growing market, with billions of dollars-worth of investments in research and development every year. Analysts forecast the global biometrics market in the retail sector to grow at a CAGR of 21.30% during the period 2016-2020. The market is divided into segments based on biometric technology: fingerprint identification, facial recognition, hand geometry, vein recognition.

The world-wide face and voice biometric technologies market is expected to be valued at nearly USD 3bn by end of 2018. Geographically, the United States still accounts for the largest share of the global face and voice biometrics market. Nevertheless, most of the market growth is expected to come from the emerging economies, with the Asia-Pacific taking the lead.

CONCLUSION

We can't stop technological progress. However, we need to be very careful: relying only on biometrics is a bad idea – no matter how good the technology might be today or in the future. In fact, one could argue that **the better the technology the more dangerous and invasive it is for everyone's right to privacy and ability to control who has access to our private and permanent information**.

As a user identity tool, biometrics can be a convenient and accurate way to identify a person – but as with any tool can be used for good or for bad. Oz Mischli has pointed out in Adrian Bridgewater's article, that biometric features are very difficult if not impossible to change if they are stolen. If a password is compromised, it can be changed and reset; if a Client Certificate is stolen, it can be revoked and a new one issued; if a OTP device is stolen, it simply needs to be canceled and reconfigured.

Advances of biometrics should be welcomed but cautiously. People should not be forced to use biometrics to identify themselves – which has grave personal privacy dangers.

Many people refer to biometrics as the silver bullet of user authentication – easy to use and highly secure. It is not. We are a long way from either and as the use of biometrics grows – personal privacy and data security issues must be resolved. The system should be designed to be a service to people and not to control them.

SOURCES

http://biometrics.pbworks.com/

http://biometrics.pbworks.com/w/page/14811351/Authentication%20technologies#WhatIsBiometrics

https://www.ukessays.com/dissertation/examples/information-systems/advantages-and-disadvantages-of-biometrics.php

http://www.biometricnewsportal.com/biometrics_issues.asp

https://www.theguardian.com/technology/2015/dec/08/the-end-of-passwords-biometrics-risks-benefits

https://blog.digicert.com/biometric-authentication-methods/

http://fortune.com/2016/05/12/biometrics-passwords/

http://www.dawn.com/news/1154284

http://www.nbcnews.com/mach/technology/biometric-scanning-use-grows-so-do-security-risks-n593161

http://www.cse.wustl.edu/~jain/cse571-11/ftp/biomet/#sec5.1

http://www.dailymail.co.uk/sciencetech/article-3471718/Can-iPhone-s-fingerprint-sensor-hacked-using-PLAY-DOH-Researchers-claim-toy-bypass-Apple-s-security.html

https://www.scientificamerican.com/article/biometric-security-poses-huge-privacy-risks/

Business Wire (English). 04/12/2013. "Face & Voice Biometrics Market Examined by Global Industry Analysts in Insightful Study Available at MarketPublishers.com"

PR Newswire US. 02/17/2016

CYBERUS KEY

Powered by

CYBERUSLABS

Cyberus Labs Sp. z o.o.
ul. Królewska 65a/1
30-081 Kraków, Poland
e-mail: biuro@cyberuslabs.com
tel.: +48 692 437 857
www.cyberuslabs.com