Biometric Security in the Mobile Age

Alex King
COMP 116
December 2016

Abstract

In recent years, biometric authentication has become standard on high-end consumer smartphones, most frequently in the form of discreet fingerprint readers, but also in the form of iris scanners. Manufacturers like Apple and Samsung have taken precaution when designing these features to ensure that personal biometric data remains encrypted on-device, never being sent over the internet and stored on remote servers. While these hardware and software strides are admirable in protecting this personal data, the net security effect of biometric authentication is dubious. Though its presence encourages more users to adopt some level of security rather than no security at all, there are profoundly troubling implications for authentication that, if compromised by a third party, cannot be modified by the person to prevent future breaches. This paper will survey several common biometric authentication platforms, investigate their mechanisms of operation, explore possible and proven exploits of those platforms, and evaluate their net effect on mobile security.

Introduction

To call the invention of the smartphone a *technological revolution* would be an understatement. The smartphone has rapidly transformed how humans interact with information, as well as how they interact with one another. The smartphone has also rapidly transformed what it means for a human to use a "computer". What was once tethered to a desk is now mobile, and now increasingly capable as a computer in its own right.

Much of the capability of smartphones relies on a person's ability to keep information safe on the device, restricting access to only those who have the rights to it. Countless modern uses of smartphones, such as email, personal banking, social media, and mobile wallet functionality, could not exist without robust and proven mechanisms of authentication. And just as the push for more personally-tailored functionality continues, there are consistent efforts to break these

authentication schemes to compromise private data. In that sense, it quickly becomes evident that strong and evolving mobile authentication is vital to keep the smartphone revolution proceeding smoothly. As consumers demand more features, they should hope that heightened security comes along with them.

As computer technology has increasingly become more miniaturized and powerful, so have methods of personal authentication. It's now common to find a smartphone that scans a fingerprint in a fraction of a second as a way of authenticating its owner; in fact, it's now estimated that over 600 million phones with biometric scanners are in use globally.[1] This biometric breakthrough has the capability to add a new dimension of security to the mobile universe, and in some respects, it has succeeded in doing so. But, though modern biometric authentication technologies keep personal biometric data safe and encrypted, and though they have led to an increase in the overall level of mobile of security, a closer look reveals these systems to be convenient yet incomplete security solutions that, when compromised, are rendered largely useless. This paper will examine such vulnerabilities and discuss possible remedies.

To the Community

Digital biometric tools like fingerprint and iris scanners are tantalizing in their convenience and simplicity. Initially, the average user may not stop to think about the possible security flaws inherent in a biometric-only authentication scheme, but it is vital that users understand that the use of biometrics comes with tradeoffs. In an age where more and more personal data flows through smartphones, consumers have more responsibility than ever to elect to use strong security schemes

[1] "Biometric Smartphone Update." *Acuity Market Intelligence*. N.p., 2016. Web. 30 Nov. 2016.

to protect personal information. Unfortunately, the companies that provide these smartphones and digital services do not always educate consumers on how best to accomplish this.

Action Items

A Brief Tour of Digital Biometrics

The notion of fingerprint recognition has been around for decades, with one of the first automated approaches being proposed by the Hughes Research Laboratory in 1963. In "Automatic Comparison of Finger-Ridge Patterns", author Mitchell Trauring details a mathematical mechanism for matching an introduced fingerprint to a known fingerprint in "a few seconds".[2] By the early 1980s, the Federal Bureau of Investigation had rolled out five Automated Fingerprint Identification Systems, and by the late 1990s, consumer products featuring digital fingerprint recognition became available for purchase.[3] Since that time, the technology did appear on some mainstream consumer products, (it was perhaps one of the more identifiable features of IBM's *ThinkPad* business laptop line), but the technology did not reach a wide audience until recent years, when the discreet fingerprint scanner has become a common, if not standard, feature of high-end smartphones.

Iris recognition is another biometric seeing increasing popularity, partly due to its promise of greater security. Observations about the uniqueness of the human iris go back to the mid-1930s, when ophthalmologist Frank Burch observed that iris patterns could be used to identify humans just as fingerprints do.[4] Much later, in the mid-1990s, Dr. John Daugman researched iris

---

[2] Trauring, Mitchell. "Automatic Comparison of Finger-Ridge Patterns." *Nature* 197.4871 (1963): 938-40. *Nature*. Web. 21 Nov. 2016.

[3] "Fingerprint Recognition." *Federal Bureau of Investigation*. National Science and Technology Council, n.d. Web. 21 Nov. 2016. <https://www.fbi.gov/file-repository/about-us-cjis-fingerprints_biometrics-biometric-center-of-excellences-fingerprint-recognition.pdf>.

[4] "Iris Recognition." *Federal Bureau of Investigation.* National Science and Technology Council, n.d. Web. 21 Nov. 2016. <https://www.fbi.gov/file-repository/about-us-cjis-fingerprints_biometrics-biometric-center-of-excellences-iris-recognition.pdf>.

recognition on the presumption that no two were alike. This culminated in his being awarded a patent for his recognition algorithms in 1994.[5] The algorithm, called IrisCode, has an astounding false match rate of roughly 1 in 100 billion.[6] Compared to a consumer-grade fingerprint reader false match rate of 1 in 50,000,[7] this precision wipes out concern that one person's iris may be mistaken for another.

An immediate concern to those who use digital biometric authentication is how the data is stored and secured on the mobile device. As biometrics are private and unchangeable, an easily compromised architecture could lead to grave ramifications, allowing a malicious user to masquerade as another if the biometric data were to be reconstructed. Because of this, it is crucial that both *access* to biometric data, as well as its ability to be *reconstructed*, must be reduced to the absolute minimum possible. Later in the paper, one such scheme to limit access will be discussed. Of greater importance, however, is that biometric data remains obfuscated on-device. In the event that access is breached, if biometric data is stored unencrypted, an attacker will immediately be able to view and reconstruct it. To prevent reconstruction, the data should be *encrypted* or *hashed*.

Unlike traditional passwords, biometric data generally must be encrypted rather than hashed, which introduces a new security concern that must be managed. Critically, biometric data should not be able to be reconstructed if found, and in the case of passwords, this is typically accomplished with a hash function. A hash function takes data of any size and returns a seemingly random fixed-size representation, such that it is extraordinarily unlikely that two different documents hash to the same value, but the same document will deterministically always hash to

---

[5] Ibid

[6] Daugman, J. "Probing the Uniqueness and Randomness of IrisCodes: Results From 200 Billion Iris Pair Comparisons." *Proceedings of the IEEE* 94.11 (2006): 1927-935. Web. 24 Oct. 2016.

[7] "About Touch ID Security on IPhone and IPad." *Apple Support*. N.p., 02 Nov. 2015. Web. 21 Nov. 2016.

the same value. Critically, hash functions are impossible to reverse, such that if only the hash of a document is known, there is no possible way to restore the original data. This is how text passwords are securely stored on computer systems. Unfortunately, a traditional hash function cannot work for most inputs of biometric data, because unlike a password, biometric data is not recorded the same way each time; fingerprints and irises can come in at a variety of rotations and angles, with subtle physical differences each time. This means that it's impossible to translate any biometric scan into a "true" representation that can then be hashed and compared to a database. Instead, biometric data must be encrypted, and the key to this encryption must be kept closely protected, because if the key is compromised, the data will be, too. Thankfully, modern mobile platforms go a long way in ensuring this data is kept safe.

Case Studies

Apple iPhone

Apple controls both the hardware and software of the iPhone, giving it extensive control over its entire security ecosystem. This control allows Apple to make some far-reaching security decisions, such as the inclusion of authentication chips in Lightning cables. These chips allow iOS devices to check and see if the cable is from an authorized manufacturer, reducing the chance of covert malware injection.[8] As a platform, the iPhone shines as an example of what can be done when hardware and software both cooperate for the sake of security.

The Apple iPhone first began using biometrics with the release of the iPhone 5S in 2013.[9] Its implementation includes both the Touch ID fingerprint sensor itself, as well as the "secure

[8] Tabini, Marco. "Five Things You Should Know about iOS Security." *Macworld*. Macworld, 28 Feb. 2014. Web. 30 Nov. 2016.
[9] Kingsley-Hughes, Adrian. "IPhone 5s with Touch ID Is a Big Win for BYOD Security." *ZDNet*. N.p., 10 Sept. 2013. Web. 21 Nov. 2016.

enclave" in Apple's processor. The enclave within each phone contains a unique digital identifier not known to Apple, meaning that Apple has no backdoor into the system.[10] The enclave boots separately from the rest of the phone, and any interactions between it and other phone components take place in encrypted memory.[11] Furthermore, Apple's custom processor is designed so that when Touch ID fingerprint data is read by the sensor, it is forwarded to the secure enclave, but Apple's processor itself is unable to read it.[12]

All of this comes together to make Touch ID on iPhone a highly secure system. Though fingerprints are not hashed, their encrypted digital representations are isolated such that they can never exit the secure enclave, ensuring that *access* to the encrypted representations is near impossible to achieve. Fingerprint data never leaves the device and is never stored unencrypted, so users should have no practical concern about the data ever being covertly stolen by malicious applications or government organizations. The hardware simply does not allow for it.

Samsung Galaxy

Samsung designs and manufactures smartphones that run Google's Android operating system, meaning that Samsung does not have the same total top-down control of the security ecosystem that Apple does. However, as Android is open source, Samsung is able to modify the platform to better suit its phones and their features. This paper will focus on Samsung's Galaxy Note 7 – which, before an international recall due to battery problems, represented Samsung's most security-focused phone to date.

The Galaxy Note 7 includes Samsung's Knox security platform, which is built on top of the Android operating system. Like Apple's iPhone, Knox on the Galaxy Note 7 builds much of

[10] Tabini, Marco.
[11] Ibid
[12] "iOS Security White Paper." *Apple*. N.p., May 2016. Web. 30 Nov. 2016.

its security and encryption from the phone's unique digital identifier.[13] It offers isolated workspaces for work and personal use, as well as a custom folder where personal apps and documents can be stored encrypted. This encrypted data cannot be decrypted by the device without user intervention. The phone has an iris scanner at the top of the device that has a similar user interface to Touch ID; it just requires a scan of the user's eye to authenticate. Samsung notes that iris scans are stored as "encrypted code", but no parallel to Apple's secure enclave exists in the processor.[14] This means that, in the unlikely event that the encryption algorithm used was cracked, the biometric data could be digitally available to an attacker, rather than being protected by physical isolation.

Ultimately, though Apple may have Samsung beat with its level of hardware support, both manufacturers have done an extremely thorough job of building a secure mobile ecosystem. Unfortunately, neither system is perfect, due in part to biometrics being easily imitable, and in part due to implementation.

Weaknesses and Defenses

In 2013, Apple's Touch ID was proven insecure by a researcher, posing questions about just how worthwhile and private fingerprints are for authentication. Marc Rogers, a security researcher, detailed his process of lifting a fingerprint and reconstructing it with a well-known method that produces fake prints made of dried glue. Rogers was successfully able to fool the Touch ID sensor on the iPhone 5S, meaning that full phone access could be achieved if a registered fingerprint of the phone's user could be lifted – an involved task, but easily doable by an assailant

---

[13] *10 Reasons to Secure Your Enterprise with Samsung Knox*. Digital image. *Samsung*. N.p., n.d. Web. 30 Nov. 2016. <http://www.samsung.com/us/system/b2b/resource/2016/02/08/Infographic_KNOX-10-Reasons-FEB16.pdf>.

[14] "Keeping an Eye on Security: The Iris Scanner of the Galaxy Note7." *Samsung Global Newsroom*. N.p., 4 Aug. 2016. Web. 30 Nov. 2016.

motivated to get into an iPhone.[15] Attacks like this are not new, with similar vulnerabilities being documented in the early 2000s.[16] Unfortunately, the current vulnerability demonstrates that in one case, consumer-grade fingerprint recognition technology doesn't do enough to prevent this sort of attack.

Iris scanning has also been cited as possibly insecure, with research demonstrating that high-resolution iris imagery can successfully pass as a real eye. Jan Krissler, a security researcher in the biometric space, has been able to break iris recognition systems using high resolution imagery of eyes found on the internet, such as those of Vladimir Putin.[17] Though the false iris print must be printed with a high number of dots per inch, the iris image itself doesn't have to be a prohibitively high resolution: "We have managed to fool a commercial system with a print out down to an iris diameter of 75 pixels," claims Krissler.[18] This means that there are plenty of normal photos on the internet that could be successfully used – photos of world leaders, celebrities, and more. Though Krissler will not speak publicly about the vulnerability until 2017, it could seriously call into question the legitimacy of naïve iris scanning for biometric security. This underscores the necessity of using smarter software mechanisms to augment biometric scanning.

One possible mechanism to increase security is the notion of *cancelable biometrics.* A cancelable biometric is one that uses uniquely identifying biometric information, along with a randomly generated transformation on that information, to create a token of authentication that can be revoked and modified, where naïve biometrics cannot. In a paper outlining possible methods of cancelable biometrics, the authors write:

---

[15] Rogers, Marc. "Why I Hacked Apple's TouchID, And Still Think It Is Awesome." *Lookout Blog*. N.p., 3 Sept. 2013. Web. 30 Nov. 2016.
[16] Leyden, John. "Gummi Bears Defeat Fingerprint Sensors." *The Register*. The Register, 16 May 2002. Web. 24 Oct. 2016.
[17] Fox-Brewster, Thomas. "Hacking Putin's Eyes: How To Bypass Biometrics The Cheap And Dirty Way With Google Images." *Forbes*. Forbes Magazine, 5 Mar. 2015. Web. 30 Nov. 2016.
[18] Ibid

> *"One of the properties that makes biometrics so attractive for authentication purposes—their invariance over time—is also one of its liabilities. When a credit card number is compromised, the is- suing bank can just assign the customer a new credit card number. When the biometric data are compromised, replacement is not possible."*[19]

The authors go on to describe possible methods of adding these "intentional, repeatable distortions" to biometric data, with the requirement that the transformation functions are one-way, similar to a hash function.[20] Complicating matters, in order for the transformations to be repeatable, the biometric signal must be positioned in the same orientation each time, meaning that "absolute" orientation of the biometric signal must be found. Finding absolute orientation is still an open area of research.[21] Lastly, the authors discuss a public cloud authentication infrastructure that could safely protect the library of transformation functions and transformed biometric data. In total, cancelable biometrics show great promise to improve the fundamental security of biometrics. Though more work is needed before systems may be implemented publicly, this technology could provide a solution to those who are apt to have biometric data compromised.

More immediate improvements to biometric security exist, such as requiring stronger passcodes and implementing *two-factor authentication*. First, it is the responsibility of operating system designers to enforce secure minimum requirements for device passcodes. Apple's own security white paper praises Touch ID's convenience, noting that it can allow a phone to be secured by a far *more* complicated passcode that will be entered *less* frequently (because Touch ID will be used in its place).[22] This is an astute observation, yet iOS currently still allows for relatively

---

[19] Ratha, N. K., J. H. Connell, and R. M. Bolle. "Enhancing Security and Privacy in Biometrics-based Authentication Systems." *IBM Systems Journal* 40.3 (2001): 614-34. Web. 24 Oct. 2016.
[20] Ibid
[21] Ibid
[22] "iOS Security White Paper."

insecure 4-digit passcodes. Until the software begins pushing users towards crafting longer alphanumeric passcodes, simple passcodes may still be the weakest link

A stronger software improvement uses two forms of authentication together, rather than requiring one authenticator or the other. This is known as two-factor authentication, where the user must present two unique tokens at the same time to prove his or her identity. Marc Rogers, the researcher who "hacked" Touch ID with false fingerprints, notes that this would be an ideal implementation of security on the iPhone, writing:

> *What I, and many of my colleagues are waiting for (with bated breath), is TouchID* [sic] *enabled two-factor authentication. By combining two low to medium security tokens, such as a fingerprint and a 4 digit pin, you create something much stronger. Each of these tokens has its flaws and each has its strengths. Two-factor authentication allows you to benefit from those strengths while mitigating some of the weaknesses."*[23]

Two-factor authentication greatly reduces the likelihood of a security breach, because it relies on not one, but two systems being compromised. Apple notes that the chance of a random fingerprint being recognized and approved by Touch ID is 1 in 50,000; when paired with even the most insecure 4-digit passcode scheme, this reduces the likelihood of random entry to 1 in 500 million.[24] Two-factor authentication is easy to implement in software, making it an excellent choice for mobile applications and services that want to increase security beyond what iOS allows by default. An example of such authentication in an iOS app is provided as supporting material for this paper.

Conclusion

Biometrics are a powerful mechanism for authentication, but their current implementation on mobile devices is incomplete and insecure. Biometrics can succeed because they are an

[23] Rogers, Marc.
[24] "About Touch ID Security on IPhone and IPad." *Apple Support*. N.p., 02 Nov. 2015. Web. 21 Nov. 2016.

immediate and natural way for people to carry around a personal and physically-identifying token. Unfortunately, biometrics are currently more lauded for their convenience over manual password entry rather than their heightened security promise. Engineering efforts by large smartphone manufacturers have built an excellent foundation for the secure handling of digital biometric data, so skeptical users of these features should have no fear that the data is indeed private to them and their device. Now, the same effort must be extended to software. Biometric authentication is only secure until proven falsifiable, and once that happens, it's only as secure as the secondary authentication that backs it up. In the short term, two-factor authentication should be made available as an option to encourage stronger security. In the longer term, cancelable biometrics may provide a way to keep using one's biometrics even after some are stolen or compromised. Though it is not without its drawbacks, biometric authentication has the potential to keep the evolution of consumer technology progressing smoothly.

Works Cited

"About Touch ID Security on IPhone and IPad." *Apple Support*. N.p., 02 Nov. 2015. Web. 21 Nov. 2016.

"Biometric Smartphone Update." *Acuity Market Intelligence*. N.p., 2016. Web. 30 Nov. 2016.

"Fingerprint Recognition." *Federal Bureau of Investigation*. National Science and Technology Council, n.d. Web. 21 Nov. 2016. <https://www.fbi.gov/file-repository/about-us-cjis-fingerprints_biometrics-biometric-center-of-excellences-fingerprint-recognition.pdf>.

"Galaxy Note7 Security Enhanced with Updated Knox 2.7."

"iOS Security White Paper." *Apple*. N.p., May 2016. Web. 30 Nov. 2016.

"Keeping an Eye on Security: The Iris Scanner of the Galaxy Note7." *Samsung Global Newsroom*. N.p., 4 Aug. 2016. Web. 30 Nov. 2016.

10 Reasons to Secure Your Enterprise with Samsung Knox. Digital image. *Samsung*. N.p., n.d. Web. 30 Nov. 2016. <http://www.samsung.com/us/system/b2b/resource/2016/02/08/Infographic_KNOX-10-Reasons-FEB16.pdf>.

Daugman, J. "Probing the Uniqueness and Randomness of IrisCodes: Results From 200 Billion Iris Pair Comparisons."

Fox-Brewster, Thomas. "Hacking Putin's Eyes: How To Bypass Biometrics The Cheap And Dirty Way With Google Images." *Forbes*. Forbes Magazine, 5 Mar. 2015. Web. 30 Nov. 2016.

Kingsley-Hughes, Adrian. "IPhone 5s with Touch ID Is a Big Win for BYOD Security." *ZDNet*. N.p., 10 Sept. 2013. Web. 21 Nov. 2016.

Leyden, John. "Gummi Bears Defeat Fingerprint Sensors."

Proceedings of the IEEE 94.11 (2006): 1927-935. Web. 24 Oct. 2016.

Ratha, N. K., J. H. Connell, and R. M. Bolle. "Enhancing Security and Privacy in Biometrics-based Authentication Systems." *IBM Systems Journal* 40.3 (2001): 614-34. Web. 24 Oct. 2016.

Rogers, Marc. "Why I Hacked Apple's TouchID, And Still Think It Is Awesome." *Lookout Blog*. N.p., 3 Sept. 2013. Web. 30 Nov. 2016.

Samsung Global Newsroom. Samsung, 11 Aug. 2016. Web. 24 Oct. 2016.

Tabini, Marco. "Five Things You Should Know about iOS Security." *Macworld*. Macworld, 28 Feb. 2014. Web. 30 Nov. 2016.

The Register. The Register, 16 May 2002. Web. 24 Oct. 2016.

Trauring, Mitchell. "Automatic Comparison of Finger-Ridge Patterns." *Nature* 197.4871 (1963): 938-40. *Nature*. Web. 21 Nov. 2016.

Westerman, Wayne C., Byron B. Han, and Craig A. Marciniak. Efficient Texture Comparison. Apple Inc., assignee. Patent 9135496. 15 Sept. 2015. Print.