View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by University of Strathclyde Institutional Repository

Strathprints Institutional Repository

Paul, Greig and Irvine, James (2016) IEDs on the Road to Fingerprint Authentication : Biometrics have vulnerabilities that PINs and passwords don't. IEEE Consumer Electronics Magazine, 5 (2). pp. 79-83. ISSN 2162-2248 , http://dx.doi.org/10.1109/MCE.2016.2521978

This version is available at http://strathprints.strath.ac.uk/55235/

Strathprints is designed to allow users to access the research output of the University of Strathclyde. Unless otherwise explicitly stated on the manuscript, Copyright © and Moral Rights for the papers on this site are retained by the individual authors and/or other copyright owners. Please check the manuscript for details of any other licences that may have been applied. You may not engage in further distribution of the material for any profitmaking activities or any commercial gain. You may freely distribute both the url (http://strathprints.strath.ac.uk/) and the content of this paper for research or private study, educational, or not-for-profit purposes without prior permission or charge.

Any correspondence concerning this service should be sent to Strathprints administrator: strathprints@strath.ac.uk

Fingerprint Authentication is here, but are we ready for what it brings?

Greig Paul
University of Strathclyde
Department of Electronic
& Electrical Engineering
Glasgow, United Kingdom
greig.paul@strath.ac.uk

James Irvine
University of Strathclyde
Department of Electronic
& Electrical Engineering
Glasgow, United Kingdom
j.m.irvine@strath.ac.uk

***Abstract*—Almost every 2016 flagship mobile phone, whether Android or iOS-based, is set to come with an integrated fingerprint reader. The convenience benefits of fingerprint readers are clear to users, but is the underlying technology really ready for widespread adoption? This article explores some of the background of the challenge of secure user authentication on mobile devices, as well as recent weaknesses identified in the handling of fingerprints on many consumer devices. It also considers legislatory and social implications of the widespread adoption of fingerprint authentication. Finally, it attempts to look forward to some resulting problems we may encounter in the future.**

I. Introduction

Fingerprint readers are, without doubt, one of the must-have features on almost every smartphone being launched in 2016. The Samsung Galaxy range of flagship devices have featured a fingerprint reader since the Note 4 and S5. Sony's latest Z5 range include a fingerprint reader on each device. Indeed, even newer entrants to the market such as OnePlus are including a fingerprint reader on their handsets.

Smartphone fingerprint readers are used typically to implement biometric authentication. Biometric authentication is, as the name suggests, a means of authenticating a user based on making measurements of one or more physical characteristics — in this case their fingerprint.

Fingerprint authentication on computers is not a new concept, having previously been seen on Thinkpads and other enterprise laptops, and even on some high-end Personal Digital Assistants (PDAs). A more detailed history of the use of biometrics and fingerprints was given by Corcoran in 2013 [1].

As fingerprint readers have become increasingly commonplace in smartphones, particularly following the introduction of TouchID on the iPhone 5s, there has now been time for the dust to settle on some implementations, and for security researchers to investigate their inner workings.

II. User Attitudes and the Demand for Convenience

The premise behind fingerprint authentication on mobile devices is typically as a replacement for the password or PIN. Good passwords require users to follow a multitude of rules, ensuring the length, complexity and uniqueness of every password they use. Remembering unique passwords for an ever-increasing number of services places a significant demand upon users, and leads to more easily guessable, or re-used passwords. Users now carry out 50% of their password entry operations on smartphones, where special characters are difficult to type, and long passwords are inconvenient [2].

A key selling point of biometric authentication is that it allows users to move away from passwords, both for use in authenticating to third parties, and for unlocking their own physical device. This eliminates the requirement to enter passwords, and avoids the inconvenience of forgetting passwords.

There is clear indication from previous studies that users are aware of, and willing to use, biometrics — in their 2005 survey, Clarke and Furnell found that 83% of surveyed mobile phone users would be willing to use biometric authentication [3]. Indeed, of those aware of the existence of fingerprint authentication, 99% were happy to use it. This is in clear contrast with iris recognition, where only 70% of those who were aware of it were happy to use it.

In contrast, an earlier survey from 2000 [4], which focused more generally on authentication, rather than specifically on mobile phone authentication, found 67% of surveyed users were willing to use fingerprint authentication. While this would indicate that either user attitudes towards fingerprint authentication have changed with time, or that users consider mobile authentication a special case, a 2007 study on the uses of authentication technologies [5] found that only around 40% of users surveyed agreed biometrics were useful when accessing a computer, in contrast with 66.1% when considering financial transactions.

It is worth noting that these surveys were carried out prior to the recent widespread adoption of smartphones. Nonetheless, it is clear that users are willing to use fingerprint authentication, and that the increased portability of smartphones, combined with the large quantities of personal data stored within, is potentially a driver for the uptake of the technology. Harbach *et al.* showed that the perceived inconvenience of a secure lockscreen on a smartphone was a factor in around one third of people not enabling one, and with an average of 48 unlocks per day, there is a clear argument for convenience of unlocking frequently used devices like smartphones [6].

A. Authentication and Identification

Fingerprints, and biometrics in general, present users with a simple alternative to PINs or passwords, to which they are accustomed. We believe fingerprint authentication is viewed more favourably than alternatives, due in part to the user perception that biometrics are the most secure form of authentication [5]. In particular, we believe that users feel reassured that fingerprints are secure in part due to their relative uniqueness, and their use in criminal justice. This does raise an important distinction though when considering the use of fingerprints — the needs of an identification system are somewhat different to those from an authentication system.

In a biometric identification system, the goal is to reliably ascertain who an individual is, based upon a comparison of measurements taken from a sample, which are then matched against previous measurements. For this to work correctly, each individual in a population should be uniquely defined, and should be recognisable in future against a previous measurement. Therefore, there is considerable focus on the uniqueness of the characteristics. For example, in a criminal investigation, the aim of forensic fingerprint analysis is to recover the fingerprints of individuals who may have been present at a crime scene. Biometric identification is then carried out to ascertain if this recovered fingerprint matches that recovered from any other crime scenes, or from individuals known to have previously committed crimes.

In contrast, a biometric authentication system is designed to allow an individual asserting their identity to prove this assertion, based upon their ability to provide biometric measurements in keeping with previously enrolled values. In the authentication scenario, a rapid result and a low false-positive rate are desirable. One consideration is that a strong authentication process, per the definition from the European Central Bank, is required to be non-reusable and non-replicable, to prevent re-use of a previously valid authentication session which may have been observed. There is however an exception made for authentication based on biometric factors, since it is inherently based on static measurements of a person. The distinction between identification and authentication is also discussed in [1].

III. Limitations of Fingerprints in Authentication

A. Static and Unchangeable

The fundamental limitation of fingerprint-based authentication is that our fingerprints are the ones we were born with, and the ones we keep for life. They are, by virtue of being part of us, unchangeable. This is an advantage in one sense, as a user cannot 'forget' their fingerprints in the same way an infrequently used password can be forgotten over time. For many users, the convenience of not forgetting passwords is a significant draw of fingerprint authentication.

B. Irrevocable Identifiers

By virtue of being static in nature, there is no effective means of revocation. If your fingerprints are compromised by some means, there is no way you can prevent the compromised copies from being re-used in future. This is a limitation of the process of fingerprint authentication, since ultimately the verifier is expecting to see the same fingerprint on each occasion. Breaches of fingerprint data are now no longer a hypothetical situation, given the recent theft of 5.6 million US federal government employees' fingerprints from the Office of Personnel Management (OPM) [7].

C. Easily Observed and Captured

Fingerprints are also easily captured without the subject being aware, both with and without physical contact. As highlighted in 2013 following the highly publicised "breaking" of Apple's new Touch ID feature, a latent fingerprint was captured using a high-resolution photograph of the glass touchscreen of an iPhone. It was then used to create a mould that could form an artificial fingerprint, capable of unlocking the phone [8]. While a relatively in-depth process, this highlights one fundamental risk of relying on fingerprint authentication on smartphones — they are held and touched by the user in daily operation, and their large glass surfaces act as a magnet for the user's fingerprints.

Additionally, it was recently shown that fingerprints can also be captured without physical contact. A series of high resolution photos, including one from a press release, were used to recreate the fingerprints of the German defence minister [9]. Indeed, this is not the first occasion in which a German politician's fingerprints have been publicised; in 2008, an index fingerprint was obtained and reproduced from a water glass used by the German interior minister during an event at a University, resulting in over 4000 copies being made onto plastic foil capable of being used on various fingerprint readers [10].

D. They Can't be Turned Off

Another property of fingerprints is that they are static, and cannot easily be 'turned off'. As you go about your life, you are leaving a trail of fingerprints around. With the rise of fingerprint authentication, this could be considered tantamount to leaving a trail of sticky notes containing your username and password to every account you have, every time you touch something.

If a password is compromised or known by someone else, it is relatively straightforward to change it, therefore revoking it, with the biggest inconvenience merely having to memorise a new password. Since they remain constant at all times, this isn't possible with fingerprints. Our inability to effectively control where our fingerprints are left behind is a significant concern. You can be careful to only type your bank password in the privacy of your own home, on a system with no keyloggers, with the curtains closed to prevent onlookers, but if you use a fingerprint to authenticate with your bank (either directly or indirectly), you cannot avoid leaving those fingerprints around. There is no concept of security level with fingerprints in the same way that one can use a single low-security "throw-away" password for uninteresting accounts which don't contain any personal data of value.

IV. Limitations of Fingerprint Sensing

Smartphone fingerprint sensors have been subject to a variety of high-profile attacks, where fake fingerprints made from a variety of materials designed to have properties similar

to human skin have been accepted as valid fingerprints. Indeed, these techniques are not outwith the practical reach of private individuals [8].

More fundamentally, a fingerprint sensor within a computer system is typically designed to convey a measurement of an individual's raw fingerprint to another component of said computer system, responsible for either deriving a cryptographic key, or unlocking an existing cryptographic key held securely on the device [1]. Therefore, by identifying the input format expected by the key storage or computation module, it is possible to present a falsified (or previously-captured) fingerprint reading "on the wire", thus bypassing the need to handle the creation of a fake physical fingerprint.

V. Legislatory Concerns

A. Fingerprinting in Criminal Process

Within most countries in the world, there is a presumption of innocence for those accused of crimes, until they are convicted at a trial in a court of law. Until that point, they remain innocent and not having been convicted of any wrongdoing. In many jurisdictions, those who are under arrest, and have not been charged with, or convicted of, an offence, may be required to give fingerprints, which can be held on a database, for the purpose of identifying any linked crimes an individual may be responsible for [11].

This process, by its definition, involves the capturing of a record of an individual's fingerprints. Since fingerprints are static and irrevocable, this individual's fingerprints are now potentially on file indefinitely. If fingerprints are used as a secure means of authentication, this is equivalent to being required to hand over a full list of all your past, present, and future passwords, simply as a part of the investigatory process.

While there may be legal procedures through which individuals can appeal to have their records removed if they were not convicted of an offence, it will never be possible for that individual to be sure that their fingerprints no longer reside on a database somewhere. The same applies to those travelling to a country which stores fingerprint records of those entering as a matter of routine, such as the USA under the OBIM program (formerly US-VISIT) [12]. Large databases are not impenetrable to unauthorised access either, as was shown in the OPM breach mentioned above.

Fingerprints may also be handled differently from a legal perspective than something which is known to a person, such as a password or PIN. In the US state of Virginia, a judge found that requiring the disclosure of a password or PIN would be in breach of the 5th Amendment, but that requiring a person suspected of committing a crime to use their fingerprint to unlock a device was constitutional [13]. It highlights an interesting situation on some devices, such as the iPhone, where a fingerprint can only be used within 48 hours of the last successful fingerprint login, after which the PIN must be used.

VI. Current Implementations

A. Smartphone Implementation

Today's consumer devices featuring fingerprint authentication technology typically make use of the ARM TrustZone Trusted Execution Environment (TEE), which allows for isolated *secure world* code to be executed on the regular CPU, separate from untrusted user code, such as that of a mobile device's operating system.

Recent research by Zhang *et al.* has nonetheless highlighted the problem of poor implementational security of fingerprint readers on many mobile devices. In their paper, a number of security issues with implementations of fingerprint sensors in mainstream phones were identified [14]. In the most extreme case of the HTC One MAX, the user's enrolled fingerprint was stored in a world-readable file. This meant that any unprivileged application running on the phone could read the file containing a user's fingerprint, without the user being aware.

While the established best practice for implementation of fingerprint readers involves the use of the ARM TrustZone to hold, validate and handle all fingerprint data, Zhang *et al.* highlighted that even with this in place, there have been exploits against TrustZone, and the fingerprint reader device is often exposed to the regular, non-TrustZone operating system of the mobile phone. This allows the fingerprint reader to be accessed by software running on the phone, provided it is able to elevate its privileges sufficiently to do so.

In addition, there have been numerous publicly documented exploits of TrustZone technology [15], [16], [17]. All of these allowed for arbitrary code execution within the secure environment, and the latter specifically gives a proof of concept to show how the user's raw fingerprint can be captured and retrieved from the reader, despite only code running in the TrustZone being able to read from the fingerprint reader on the device in question.

B. Reader Trust

Another, more general consideration with today's implementation of fingerprint authentication is that of trust of the capture device. Since, by definition, fingerprint data is constant, it is necessary for the reader or capture device to be trustworthy, and not store or transmit it for use or storage by unauthorised parties. This raises the questions of who is authorised to receive the data, how the biometric data may be used, and the manner in which it may be stored and processed. Specifically when a device holds biometric data (such as a smartphone), a question arises over if the company who manufactures the smartphone has, or should have, any right (or ability) to access that data. In the case of Android devices, for example, there is also the question of whether or not Google (the developer of the core operating system) has the ability or right to access the data.

A rise in the use of fingerprint authentication on smartphones would also likely fuel a rise in the use of fingerprint authentication in other areas. For example, Poland has installed bank ATMs featuring fingerprint authentication since 2010, where a fingerprint is used in conjunction with a PIN to withdraw cash [18]. Significantly, this requires users to provide their fingerprints to an unverifiable device operated by a third party. Fake (or real, with unauthorised modifications) ATMs have been a popular way for criminals to "skim" cards and obtain PINs via fake keypads and card readers.

If users become comfortable with providing their fingerprint to equipment requesting it, without being familiar with it (to identify signs of tampering or illegitimacy), they may find their fingerprint data is stolen by criminals. While the same is completely true of bank card numbers and PINs as used presently at ATMs, there is little long-term impact of such details being compromised; the bank freezes the account and reverses the transactions, and issues a new card to the account holder, who sets a new PIN. In the case of biometric authentication, it is not possible to change or revoke the biometric.

C. Other Uses

Biometric data is potentially of huge value to advertisers and other businesses, as it allows for theoretically globally unique identification of users, simply based upon their use of a product or service. If fingerprint readers become a common feature of consumer electronic devices such as smartphones, undoubtedly the question over rights to use such data will emerge and need answered.

Whether it is legal, ethical or acceptable for fingerprint data to be used to pervasively track a user is a question which should be answered before such technology becomes widespread, otherwise we may find ourselves in a situation like we face with internet-based services, where users have relatively limited technical controls and restrictions over the use and sharing of their personal data, and websites carry out widespread tracking of user activity and actions across the wider internet.

The ability for an advertiser to tell with certainty that the current visitor to a website, or user of an application, is the same one as in a previous browsing session, would be of incredible value — this would persist across devices and browsing sessions. It would also be effective against attempts to prevent such tracking, such as a user clearing their cookies. While the suggestion not to provide fingerprints to such websites may well be the obvious one, ensuring this is enforced with technical (rather than legislatory) measures is essential. With current fingerprint reader implementations generally "black box" systems, not open to scrutiny by researchers or experts, this is difficult to achieve.

D. Action Verification

In contrast to a PIN or password, where a user is prompted to enter a particular one for a given service or action, fingerprints remain constant between services. This means that the contextual information as to the action being carried out following fingerprint verification is critical. Since the same fingerprint may be used to unlock a device, as well as authorise a high-value bank transfer, it is important to ensure users have a reliable and trustworthy way to understand the operation they are approving via their fingerprint.

Entering a PIN requires a user to understand the action they are authorising — presuming a user follows good practice and doesn't have the same PIN on all of their bank cards, they can easily detect that they are carrying out a transaction on the wrong card due to the PIN being rejected. Likewise, while not fool-proof against malicious attack [19], the screen on an EMV chip-and-PIN payment terminal confirms the value of a transaction being carried out, or the recipient and value of a transfer. On a smartphone featuring fingerprint authentication, simply providing a fingerprint is sufficient to carry out a variety of operations. These can extend from merely unlocking the device, to logging into an app or website, to initiating a bank transfer. Indeed, smartphone apps from major banks now allow for the use of fingerprints to authenticate transactions [20].

VII. Future Considerations

A. Avoiding the Reader

With the rise in smartphone fingerprint sensors, it is interesting to note that, while early devices with such sensors (such as the Motorola Atrix) featured their sensor on the rear of the device, where it could be avoided or covered by a case, more recent implementations (such as the iPhone and Samsung's Galaxy range of devices) feature the fingerprint reader on the front, within the device's physical home button. This presents usability benefits for consumers, since authentication can be carried out using a button they already use for other tasks. Additionally, for the purpose of unlocking the device, the same button which was used to wake the phone can then be immediately used as a fingerprint reader to verify the user's fingerprint. On the other hand, this also makes it easier for a user to unintentionally authenticate a request, simply through over-familiarity with the process.

Continuing this trend, it is conceivable that in the future, the need for a fingerprint reader in itself may be eliminated, given a recent patent application by Apple [21], to include a fingerprint reader within the screen. At that point, and arguably also today, with the reader a component of one of the major buttons on the phone, the question arises over if a user has a choice as to whether they wish to be fingerprinted or not while using a device. While users can avoid using the reader for the purpose of authentication, it is much more difficult with the current "black-box" style fingerprint authentication systems to verify that the fingerprint data isn't being read or stored. With sensors embedded in screens, it may not be clear to a user when they are authenticating a request, since the authentication process may no longer be a clear distinct action, thus bypassing the careful consideration that should be taken before proceeding.

B. Fingerprint Payments

The latest, and potentially one of the most visible, consumer application of fingerprint-based authentication on smartphones is for the authentication of payments carried out via a mobile device. By placing their smartphone against a contactless reader, a user is able to select the card to use for payment, and authenticate the payment by simply placing their finger against their smartphone's fingerprint reader.

Early implementations which we see on today's consumer devices, such as Apple Pay, appear to have a number of weaknesses, as exhibited in their own demonstration. Specifically, there is no authentication of the transaction amount visible — as seen in their product demonstration, an Apple Pay user simply knows that they are being asked to approve a transaction with the selected card, but there is no indication of the value of the transaction being carried out [22].

Taking into consideration the design of smartphone-based payment systems, which are now deployed and operational in the USA and UK, we believe there is a risk of early users being victims of fraud, as a result of innovative fraudsters, given the reliance of these systems on fingerprint authentication. Even putting aside the limitations of fingerprints being unchanged and potentially known to third parties, and the ease with which they can be captured, a fingerprint reader is ultimately used to authenticate to a "trusted" area of the smartphone, often based on ARM TrustZone technology, as discussed earlier.

If the contents of this TrustZone were to be compromised, the user's fingerprint would most likely no longer be necessary in order to authorise transactions on behalf of a user. The presentation of a permitted fingerprint is used by the semi-isolated Trusted Execution Environment (TEE) to permit the use of cryptographic keys, which are themselves only accessible by the TEE. In the event of the TEE being compromised (as discussed earlier), these keys may be exfiltrated from the device, or otherwise abused by a malicious user (such as by forcibly enrolling a new fingerprint).

VIII. Potential Mitigations

Despite many of the potential risks and challenges of the use of fingerprints in secure authentication, it is clear that consumers feel it is secure enough, and products incorporating fingerprint readers are now reaching the market in significant quantities. In this section, we consider some ways in which these risks can potentially be mitigated or reduced, to allow for a practical solution to the clear user demand for a simpler means of authentication.

A. Legislation

We firstly believe that strong legislation is necessary to govern how biometric information may be used, and shared. Where such legislation exists, it often covers only government or official use of biometric information [23], rather than commercial or third party use of, and gathering of, biometric information.

When a user voluntarily provides their fingerprints to a piece of consumer electronic equipment, they are no longer engaging with a legislated entity. Indeed, in many jurisdictions, the handling of electronic or personal data (which may include biometric data) is left to self-regulation and loose oversight, rather than legislation [24].

Given the unique way in which biometric information cannot be changed, we believe that legislation governing the technological protection of biometric data is necessary, to ensure that consumer technology utilising it is designed to reduce the risk of compromise as much as possible.

B. Transparent Implementations

In order to mitigate many of the risks of current implementations (such as TrustZone exploits and similar), we believe it would be advisable for implementations of biometric authentication to be designed and documented publicly, with all relevant source code as to the operation of the authentication mechanism made available for review. With fingerprint authentication set to become near-ubiquitous in the short-term, there would be considerable benefit in ensuring that the technology is secure, on account of the hesitations people hold about the use of biometric authentication, and the significance with which end users place on trust and resistance to attack [25]. Ensuring that implementations are transparent and open to independent scrutiny would facilitate verification of correct implementation, and the identification of security weaknesses. While it could be argued that such disclosure would make attacks easier, a lack of source code has not held researchers back in finding vulnerabilities in TrustZone and other fingerprint reader implementations, as discussed earlier.

C. Trusted Software

If a product offers a consistent and predictable user interface for the request of fingerprint authentication, it is important to ensure that this interface is trustworthy. For example, it is critical that the application or service requesting identifying information is clearly and correctly identified to the user, to prevent social engineering attacks, or falsely generated prompts from overriding the system prompt to change the appearance of the prompt (making it appear a different application is requesting authentication).

We also recommend that at each opportunity, the user be clearly presented (using a trusted software implementation, which is again open to scrutiny and security testing by independent researchers) with a summary of the action being carried out at each point. A separate cryptographic key should be used for each application using biometric authentication, to prevent a rogue application from generating a valid authentication message in response to its own request, which would be accepted by another service as an attestation that the user had agreed to an operation. This would be a risk in a scenario where a service accepted a signed random value as an attestation — another application could request the same random value, and replay the token, unless a unique key is used for every application.

D. Avoiding Over-use

One factor we have identified is that the over-use of fingerprint authentication may well pose a risk. Consumers seek convenience, and the convenience of fingerprint authentication is attractive, compared with the task of typing lengthy passwords on a small on-screen keyboard. Despite this, repetitive authentications result in people becoming lazy, as is seen in their use of short or simple passwords for which they are asked for regularly. If fingerprint authentication is over-used, we believe it likely that people may become overly comfortable with simply approving everything that is requested, rather than validating the precise request. Especially when a fingerprint reader is located on the home key of a product, the natural reaction will be to approve the action, rather than to scrutinise it further and verify that it is indeed the action which should be carried out. By encouraging users to pause and consider the request, perhaps even enforcing this via a short on-screen time-out, this would go some way to ensuring that users are aware of the action they are providing authentication for.

E. Awareness of Risks

We believe that it is important for service and application implementers to be aware of the risks of fingerprint authenti-

cation, particularly around those whose fingerprints may be known to, or have been captured by, third parties. While today's payment solutions allow fingerprint authentication as a means of proof the card-holder is present, this ultimately relies on the integrity of the TrustZone implementation used to hold these keys. If these keys were extracted, or a man-made fingerprint was presented to the reader, the proof that a customer was present to authorise a transaction is less robust. With the ease with which an unwilling party can be compelled to give their fingerprints, it is also likely that people may be forced to unlock fingerprint-authenticated equipment against their will, to authorise transactions or simply for their fingerprints to be captured for future use.

F. Plan for Compromise

Finally, in light of the previous point, we believe it is necessary to begin to plan for a future where fingerprint and other biometric authentication is readily subverted by malicious use of, or threat of, force. While the same is true for today's passwords and PINs, we are always capable of selecting and using a new password. Early adopters of biometric authentication technologies will be at risk of emerging threats, and we should be prepared for a time where people's fingerprints are widely known. For this reason, we believe it important to consider this risk in future, when deploying biometric technology, and for companies relying on it to be aware that the presence of a seemingly biometrically-verified signature does not necessarily indicate the user has agreed or given their consent. This may also have implications on the legal status of biometrically-authenticated signatures.

IX. Conclusion

Biometric user authentication, in the form of fingerprint authentication, is becoming increasingly mainstream, seen on almost all present or upcoming flagship mobile handsets. Despite its wide reach, we have highlighted a number of concerns around the fundamental security of the use of fingerprints for authentication purposes. The permanent, irrevocable nature of fingerprints means that their compromise or capture is a life-long concern. We also leave fingerprints behind on almost everything we touch, including specifically the screens of the products we use in our day-to-day lives. Researchers have shown the ease with which a fingerprint can be cloned from photographs, or simply a glass which has been touched by an individual. We also explored the risks of implementations of today's fingerprint authentication technology, specifically surrounding some of the risks of TrustZone-based implementations of key storage and fingerprint verification, and exploits which have previously allowed for arbitrary code execution, compromising the supposedly-secure execution environment. We have also explored the risk of improper implementation of fingerprint readers in commercially available smartphones, including those which expose fingerprint data to any app running on the phone.

Fingerprint authentication looks set to continue to grow, despite the warnings of the security industry. While the convenience it offers is clearly of interest to consumers, the ability to replace passwords with something that is faster and unforgettable is clear to users, albeit with the caveat it can also never be changed. The next few years will likely dictate how biometric authentication will work in the future — could we end up in a position where muggers simply take fingerprints of their victims, knowing they now hold that user's keys for life? We have made a series of recommendations towards improving the technical implementation of biometric security on current consumer devices, and enhancing trust of their software, although these will not address some of the fundamental concerns of the static nature of biometric identifiers and their use in authentication.

Acknowledgment

This work was funded by EPSRC Doctoral Training Grant EP/K503174/1.

References

[1] P. Corcoran, "Biometrics and consumer electronics: A brave new world or the road to dystopia? [soapbox]," *Consumer Electronics Magazine, IEEE*, vol. 2, no. 2, pp. 22–33, April 2013.

[2] C. Foxx. How to pick the perfect password. [Online]. Available: http://www.bbc.co.uk/news/technology-34221843

[3] N. L. Clarke and S. M. Furnell, "Authentication of users on mobile telephones–a survey of attitudes and practices," *Computers & Security*, vol. 24, no. 7, pp. 519–527, 2005.

[4] S. M. Furnell, P. Dowland, H. Illingworth, and P. L. Reynolds, "Authentication and supervision: A survey of user attitudes," *Computers & Security*, vol. 19, no. 6, pp. 529–539, 2000.

[5] L. A. Jones, A. I. Antón, and J. B. Earp, "Towards understanding user perceptions of authentication technologies," in *Proceedings of the 2007 ACM workshop on Privacy in electronic society*. ACM, 2007, pp. 91–98.

[6] M. Harbach, E. von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith, "Its a hard lock life: A field study of smartphone (un) locking behavior and risk perception," in *Symposium on Usable Privacy and Security (SOUPS)*, 2014.

[7] A. Greenberg. OPM now admits 5.6m feds fingerprints were stolen by hackers. [Online]. Available: http://www.wired.com/2015/09/opm-now-admits-5-6m-feds-fingerprints-stolen-hackers/

[8] Chaos computer club breaks Apple TouchID. [Online]. Available: http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid

[9] A. Hern. Hacker fakes German minister's fingerprints using photos of her hands. [Online]. Available: http://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands

[10] D. Goodin. Get your German interior minister's fingerprint here. [Online]. Available: http://www.theregister.co.uk/2008/03/30/german_interior_minister_fingerprint_appropriated/

[11] Being arrested: your rights. [Online]. Available: https://www.gov.uk/arrested-your-rights/giving-fingerprints-photographs-and-samples

[12] Office of biometric identity management. [Online]. Available: http://www.dhs.gov/obim

[13] Virginia judge: Police can demand a suspect unlock a phone with a fingerprint. [Online]. Available: http://arstechnica.com/tech-policy/2014/10/virginia-judge-police-can-demand-a-suspect-unlock-a-phone-with-a-fingerprint/

[14] "Fingerprints on mobile devices: Abusing and leaking." [Online]. Available: https://www.blackhat.com/docs/us-15/materials/us-15-Zhang-Fingerprints-On-Mobile-Devices-Abusing-And-Leaking-wp.pdf

[15] Full TrustZone exploit for MSM8974. [Online]. Available: http://bits-please.blogspot.co.uk/2015/08/full-trustzone-exploit-for-msm8974.html

[16] D. Rosenberg, "QSEE TrustZone kernel integer over flow vulnerability," in *Black Hat conference*, 2014.

[17] D. Shen, "Exploiting Trustzone on Android," in *Black Hat conference*, 2015.

[18] Poland installs Europe's first biometric fingerprint-scanning ATM machine. [Online]. Available: http://www.popsci.com/technology/article/2010-05/poland-installs-europes-first-biometric-fingerprint-scanning-atm-machines

[19] I. Ion and B. Dragovic, "Don't trust POS terminals! Verify in-shop payments with your phone," *Proceedings of SMPU*, vol. 8, 2010.

[20] Bank of Melbourne enables fingerprint login for Apple iOS users. [Online]. Available: http://www.arnnet.com.au/article/555819/bank-melbourne-enables-fingerprint-login-apple-ios-users/

[21] M. Yousefpor, J.-M. Bussat, B. B. Lyon, G. Gozzini, S. P. Hotelling, and D. Setlak, "Fingerprint sensor in an electronic device," Aug. 4 2014, US Patent App. 14/451,076.

[22] Apple. Apple pay. [Online]. Available: https://www.apple.com/apple-pay/

[23] *Protection of Freedoms Act 2012*. [Online]. Available: http://www.legislation.gov.uk/ukpga/2012/9

[24] W. E. Agin, "The new regime for treatment of customer data in bankruptcy cases," *J. BANKR. LAW & PRAC.*, vol. 10, p. 365, 2001.

[25] M. El-Abed, R. Giot, B. Hemery, and C. Rosenberger, "A study of users' acceptance and satisfaction of biometric systems," in *Security Technology (ICCST), 2010 IEEE International Carnahan Conference on*, Oct 2010, pp. 170–178.