Is Secure and Usable Smartphone Authentication Asking Too Much?

Alexander De Luca, Ludwig-Maximilians-Universität München

Janne Lindqvist, Rutgers University

There's nothing wrong with having multiple smartphone authentication systems—each adapted to different device capabilities and mobile contexts—as long as they're complementary and don't detract from the user experience.

Smartphones have become nearly ubiquitous, enabling users to access communication, payment, banking, entertainment, social networking, and other services previously available only on desktop computers anytime, anywhere. However, this convenience comes with considerable security and privacy risks. Smartphones contain intimate details of our lives: who we talk to and spend time with, where we go, and, increasingly, how we spend our money. With a stolen phone, an attacker can acquire much of the owner's personal and financial data—not only what the device itself contains but also what is accessible through the Internet.

Unfortunately, smartphones are still mostly secured with authentication mechanisms that predate mobile devices—namely, personal identification numbers, which originated with the development of automatic teller machines in the late 1960s, and passwords, which were in use long before computer systems. However, typing a PIN or password on a small handheld device, especially if you're walking or engaged in another activity, is more cumbersome than doing so on a stationary, relatively larger ATM keypad or computer keyboard.

The first attempt to adapt user authentication to the smartphone's small form factor came in 2008, when Android introduced its optional pattern lock system, which requires users to swipe a finger across a particular sequence of dots to unlock the device, as Figure 1 shows. Despite being more error-prone and slower than traditional PIN/password entry, many users prefer pattern lock due to its playfulness and ease of use.[1] On the downside, the

0018-9162/15/$31.00 © 2015 IEEE

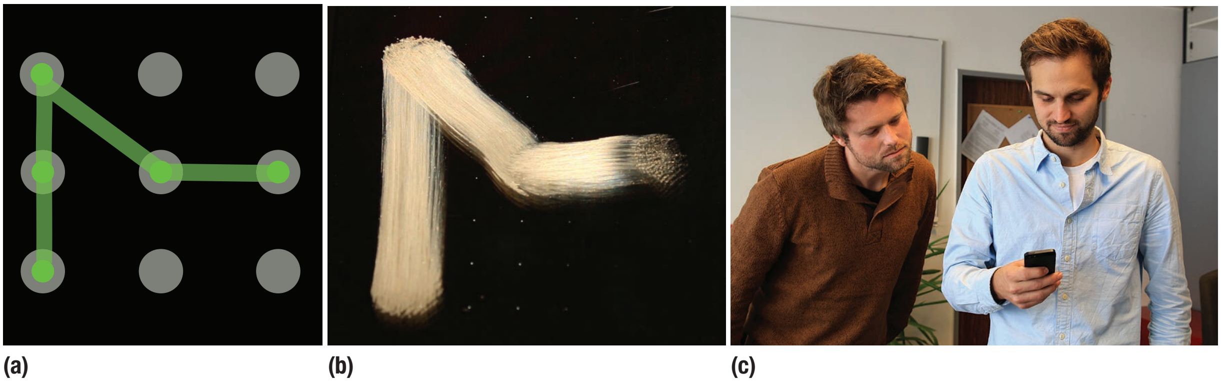

Figure 1. Android pattern lock authentication system. (a) Users swipe a finger across a specific sequence of dots to unlock the device. Although fun and easy to use, the system is vulnerable to (b) smudge attacks and (c) shoulder surfing. (Photo: Doris Hausen)

practical password space is limited[2] and the system is susceptible to both smudge attacks and shoulder surfing.[3]

The challenge faced by system designers is to make smartphone authentication both secure *and* usable. Authentication could easily be made much more secure than it is now by ignoring user needs, but given that the average user unlocks his or her phone 50 times per day,[4] au thentication must be fast and convenient or most users will disable it.

In recent years, researchers have spent considerable effort exploring alternative smartphone authentication methods. The diversity of use cases precludes a universal solution—for example, a mobile banking app would probably prioritize security over execution time. However, three well-known general approaches, alone or in combination, appear promising for many scenarios: "something you are," "something you know," and "something you have."

BIOMETRIC AUTHENTICATION

Many computing systems use biometric authentication, including fingerprint, iris, face, and voice recognition. Smartphones have likewise begun to incorporate such "something you are" systems, but these systems present numerous challenges.

Fingerprint authentication

Fingerprint scanners are commonly used in industry, such as to clock in and out of work or access restricted areas, and are now appearing in theme parks, such as Walt Disney World in Florida, and other commercial venues. Fingerprint scanners have also been developed for a growing number of consumer devices ranging from laptops to personal safes to cars.

Many smartphones include fingerprint sensors to simplify unlocking. Apple's Touch ID technology, offered in selected iPhones (and iPads), is the most notable and has motivated other companies including Samsung to incorporate similar technologies in their devices (http://webcusp.com/list-of-all-fingerprint-scanner-enabled-smartphones). Some online services also support phone-based fingerprint authentication. For example, two UK banks recently announced that customers with iPhones could access their accounts using Touch ID.[5]

Despite its ease of use and relatively low implementation cost, fingerprint authentication has some major drawbacks. First, injuries such as cuts and burns, as well as environmental factors like moisture, sunscreen, ink, and dust, can interfere with readers. In addition, fingerprints can't be changed once they're compromised and yet are highly exposed to theft because government agencies around the world, as well as many companies, collect and store them. Furthermore, after Touch ID's launch, researchers were quick to expose the technology's vulnerability to spoofing by photographing a latent print on the device and using this to create a fake finger.[6] Another disadvantage of using fingerprints for authentication is that it could imperil users' personal safety: a committed attacker might well remove your finger if that's the easiest way to access your bank account.

Face and voice authentication

Face and voice authentication, which are available on some Android and Samsung Galaxy phones, are emerging alternatives, but existing implementations are unreliable—critics claim they can be fooled by showing a digital image, or playing recorded voice commands, of the authorized user. Apple and Google, among other companies, are striving to make these technologies

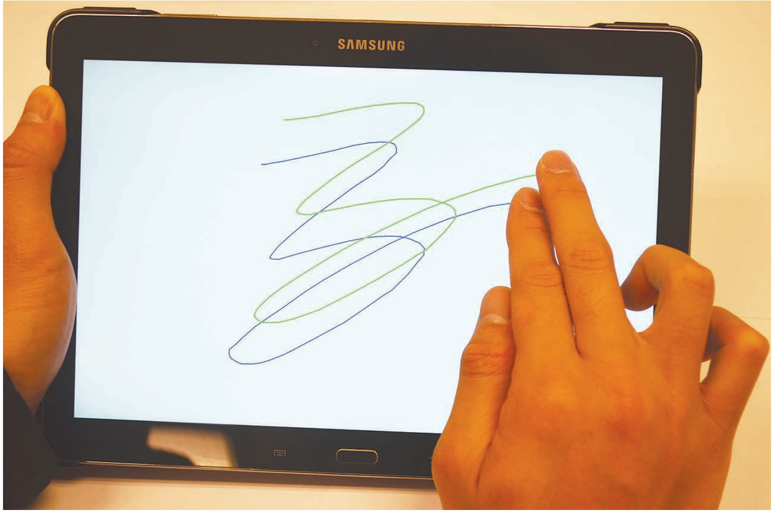

Figure 2. Example of a user-generated, free-form multitouch gesture. Unlike the Android pattern lock system and graphical passwords, gesture-based authentication lets users create both complex and simple, easily repeatable secrets without the need for visual cues.

more robust—in the case of face recognition, by adding facial gestures such as smiling—but physiological traits alone might never provide sufficient security for some scenarios.

Behavioral biometrics

To address the above challenges, researchers are exploring the possibility of incorporating behavioral biometrics—the unique ways users perform actions such as entering keystrokes or touching the screen—into smartphone authentication. For example, the system could determine whether the rightful user entered a PIN based on tapping behavior.[7] Alternatively, the system could monitor smartphone usage and, if it detects anomalous activity, lock the device.[8] Whether the specific action that serves as the basis for authentication is instantaneous or continuous, *implicitness* is a critical usability property: ideally, users shouldn't have to think about what they're doing.

Not a panacea

Compared to traditional smartphone authentication techniques, biometric authentication offers the possibility of faster, easier access, which in turn should motivate more users to activate the system.[9] However, in contrast to PINs and passwords, which are deterministic, behavioral biometrics are heuristic and thus can have high false rejection rates. Incorrectly denying access is extremely annoying and can quickly lead to user opt-out. Furthermore, many people have privacy concerns when it comes to providing biometric data. Given these limitations, biometric solutions will likely need to be backed up by another authentication system.

GESTURE YOUR PASSWORD

Gesture-based smartphone authentication relies on user-generated, free-form doodles or swipes instead of typing an (alpha)numeric secret.[10] Figure 2 shows an example gesture consisting of two squiggly lines created with two fingers.

This "something you know" approach has several advantages. First, gestures let users create both complex and simple, easily repeatable secrets without the need for visual cues such as those required by Android's pattern lock system. Second, for some users, employing motor memory can make a secret easier to recall. Third, gestures can be captured by the device's camera as well as the touchscreen.[11] Finally, the playfulness of gesture-based authentication enhances its likeability.

Researchers are also exploring the integration of gestures with physiological and behavioral biometrics: to help compare user-generated gestures, the system uses machine learning to assess unique individual characteristics such as hand size, the pressure applied by the user, and the speed with which the user creates the gestures.[11]

IS A PICTURE WORTH A THOUSAND PASSWORDS?

PINs and passwords have the disadvantage of being vulnerable to shoulder surfing by others in the user's vicinity. One way to address this problem without changing the smartphone hardware is to employ graphical passwords.[12] With this approach, the interface itself reveals little if any of the authentication process.

SmudgeSafe is a novel "something you know" system that uses geometric transformations of background images to secure a graphical password against shoulder surfing as well as smudge attacks.[3] As Figure 3a shows, to authenticate, a user must draw a shape between different locations in the image known only to the user. In addition, as Figure 3b shows, the system randomly rotates the image between specific values to minimize the risk of smudge attacks.

A major problem with graphical password systems is greater input complexity, which increases mental demand and reduces authentication speed. Such systems are inappropriate for mobile contexts that require much user attention.

HARDWARE-BASED AUTHENTICATION

Standard two-factor authentication systems demonstrate that adding hardware to the process can significantly strengthen its security. A promising new approach leverages the capacitive touchscreens used by mobile devices to relay signals to the system software.[13] The touchscreen is typically tuned to the capacitance of a human finger, but researchers have demonstrated that it can also be stimulated by carefully crafted electronic pulses. Thus, easy authentication could be achieved via an external device such as a smartwatch or smartcard-embedded ring.

It's unclear, however, whether users, if given the choice, would generally accept this "something you have" approach. Having to carry additional and potentially expensive hardware is burdensome, and would have to be seamlessly incorporated into users' daily routines. The increasing popularity of wearable technologies is a major step toward minimizing this burden.

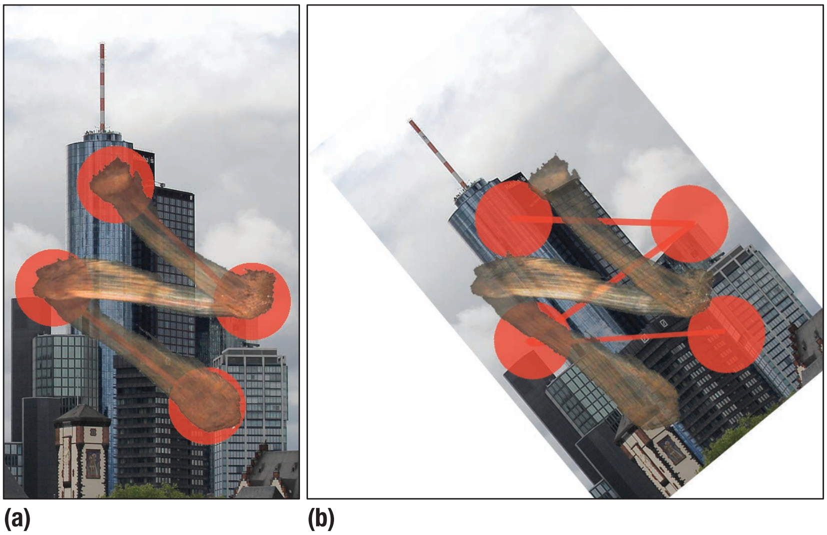

Figure 3. The SmudgeSafe graphical authentication system is designed to minimize vulnerability to both smudge attacks and shoulder surfing. (a) To authenticate, a user must draw a shape between different locations in the image known only to the user. (b) The system then randomly rotates the image between specific values.

Although researchers have studied user authentication for decades, the advent of mobile devices has significantly shifted the design goals. For people on the go who are continually activating their phone to access various types of services, an authentication system must not only be secure but also convenient and easy to use for it to be widely accepted.

Experience shows that a single authentication solution is impractical across multiple platforms and contexts. This presents a particular challenge in the case of smartphones, which have become a nearly universal tool for a wide range of social and transactional purposes. Authentication must be adapted to individual devices' capabilities and form factor. Likewise, it must be suitable for the task at hand: fallback authentication—gaining access to your device after locking yourself out—is totally different from logging into a social network.

Fortunately, hardware and software innovations are enabling novel ways to make smartphones more secure as well as to improve the user experience. Who would have believed 10 years ago that voice, fingerprint, and face recognition would be available in a pocket-size device, or that users could authenticate with a finger ring or through gestures?

There's nothing wrong with having several authentication systems—even in a single device—as long as they're complementary and don't detract from the user experience. However, this requires extensive evaluation of which approaches are appropriate for different scenarios. For example, speed might be prioritized for device unlocking, security for mobile banking, and memorability for fallback authentication. Instead of a one-size-fits-all approach, researchers should focus on solving specific use cases and then integrating the resulting solutions.

ACKNOWLEDGMENTS

The work performed by Janne Lindqvist described in this article is supported by the National Science Foundation under grant numbers 1223977 and 1228777. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

1. E. von Zezschwitz, P. Dunphy, and A. De Luca, "Patterns in the Wild: A Field Study of the Usability of Pattern and PIN-Based Authentication on Mobile Devices," *Proc. 15th Int'l Conf. Human–Computer Interaction with Mobile Devices and Services* (MobileHCI 13), 2013, pp. 261–270.
2. S. Uellenbeck et al., "Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns," *Proc. ACM SIGSAC Conf. Computer and Communications Security* (CCS 13), 2013, pp. 161–172.
3. S. Schneegass et al., "SmudgeSafe: Geometric Image Transformations for Smudge-Resistant User Authentication," *Proc. ACM Int'l Joint Conf. Pervasive and Ubiquitous Computing* (UbiComp 14), 2014, pp. 775–786.
4. M. Harbach et al., "It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception," *Symp. Usable Privacy and Security* (SOUPS 14), 2014, pp. 213–230.
5. K. Rawlinson, "Banks to Allow Account Access Using Fingerprint Tech," *BBC News*, 18 Feb. 2015; www.bbc.com/news/echnology-31508932.

6. “Chaos Computer Club Breaks Apple Touch ID,” blog, 21 Sept. 2013; www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid.
7. N. Zheng et al., “You Are How You Touch: User Verification on Smartphones via Tapping Behaviors,” *Proc. IEEE 22nd Int’l Conference Network Protocols* (ICNP 14), 2014, pp. 221–232.
8. H. Khan, A. Atwater, and U. Hengartner, “A Comparative Evaluation of Implicit Authentication Schemes,” *Proc. 17th Int’l Symp. Research in Attacks, Intrusions and Defenses* (RAID 14), 2014, pp. 255–275.
9. A. De Luca et al., “I Feel Like I’m Taking Selfies All Day! Towards Understanding Biometric Authentication on Smartphones,” *Proc. 33rd SIGCHI Conf. Human Factors in Computing Systems* (CHI 15), 2015; http://dx.doi.org/10.1145/2702123/2702141.
10. M. Sherman et al., “User-Generated Free-Form Gestures for Authentication: Security and Memorability,” *Proc. 12th Ann. Int’l Conf. Mobile Systems, Applications, and Services* (MobiSys 14), 2014, pp. 176–189.
11. G.D. Clark and J. Lindqvist, “Engineering Gesture-Based Authentication Systems,” *IEEE Pervasive Computing*, vol. 14, no. 1, 2015, pp. 18–25.
12. F. Schaub et al., “Exploring the Design Space of Graphical Passwords on Smartphones,” *Proc. 9th Symp. Usable Privacy and Security* (SOUPS 13), 2013; https://cups.cs.cmu.edu/soups/2013/proceedings/a11_Schaub.pdf.
13. T. Vu et al., “Distinguishing Users with Capacitive Touch Communication,” *Proc. 18th Ann. Int’l Conf. Mobile Computing and Networking* (Mobicom 12), 2012, pp. 197–208.

ALEXANDER DE LUCA is a postdoctoral researcher at the Ludwig-Maximilians-Universität München, and recently joined Google in Zurich, Switzerland, as a user experience researcher. Contact him at alexander.de.luca@ifi.lmu.de.

JANNE LINDQVIST is an assistant professor in the Department of Electrical and Computer Engineering and a member of WINLAB at Rutgers University, where he directs the Rutgers Human–Computer Interaction group. Contact him at janne@winlab.rutgers.edu.