# Picking a (Smart)Lock: Locking Relationships on Mobile Devices

Elizabeth Stobert and David Barrera
ETH Zurich
Switzerland

## 1. INTRODUCTION

The last decade has seen an explosion of mobile device deployment and adoption. As these devices take on a more central role in users' everyday lives, the security of these devices becomes paramount. In addition to providing access to data stored elsewhere, smartphones and tablets often store considerable personal data locally, increasing the importance of only allowing legitimate access to the device. Local authentication to the device is thus of central importance in a user's security management tasks.

The environmental requirements of mobile users fundamentally change the threat model and design requirements for device authentication from the traditional "desktop" paradigm. Mobile devices are used in a variety of physical environments, and are thus not protected by the physical security measures that protect desktop computers. Mobile devices are exposed to a wider variety of potential attackers, and do not benefit from the predictable environments enjoyed by home and office computers. This portability, combined with increased exposure to people and unknown environments, leads to higher susceptibility to theft and loss.

The use patterns of mobile devices are also different from that of PCs. Mobile devices are used in short bursts, frequently throughout the day, and typically locked between uses to preserve battery power [2]. This means that device authentication takes place much more frequently than on traditional computers, and users spend a comparatively high percentage of their time on authentication tasks [5].

For all of these reasons, mobile device vendors and developers have innovated widely and rapidly in the space of device authentication. The predominant (and often default) form of authentication for modern desktop systems is text passwords, and in most contexts no alternatives are offered. In contrast, mobile operating systems offer a range of authentication options. Along with text passwords and PINs, iOS and Android offer graphical passwords, biometric options, and location-based authentication [1, 4]. The vertical integration between hardware and software allows vendors to not only rapidly deploy new authentication techniques, but also to market them as competitive advantages.


*Symposium on Usable Privacy and Security (SOUPS)* 2016, June 22–24, 2016, Denver, Colorado.

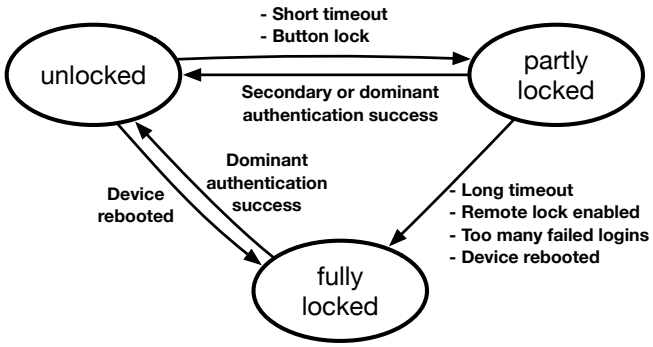


**Figure 1: State diagram showing the possible states of locking for mobile devices, as well as the transitions between states.**

In this position paper, we examine the relationship between the different types of locks available on current smartphones. We discuss the implications of these relationships and suggest future research directions based on our observations.

## 2. MULTIPLE AUTHENTICATION FACTORS

An innovation in smartphone authentication is the use of multiple methods of authentication to access a system. This relationship is novel and departs from existing two-factor authentication systems and fallback authentication systems (such as challenge questions) because both (or several) authentication mechanisms are meant to be used in conjunction with each other.

In the context of smartphone unlocking, the relationship between two (or more) authentication mechanisms is usually set up differently than in online authentication. One factor (usually a PIN), is set up as the *dominant* authentication. This mechanism can always be used to unlock the phone, and in specific (security-critical) situations, the OS insists that this authentication be used to unlock the phone. On the iPhone, the passcode (either a PIN or password) functions as the dominant authentication factor. The user can always use the passcode to unlock the phone. If the user has TouchID configured, the passcode dominates the fingerprint authentication. In ordinary situations, the user can choose freely whether to unlock the phone with TouchID or with the passcode. But if the user fails five login attempts with TouchID, they must use the passcode to unlock the phone. Similarly, they are obliged to use the passcode if the phone has been rebooted, if the phone has not been unlocked in 48 hours, or if the phone has been remotely locked [1].

If the PIN is the dominant authentication factor, then the other authentication factor(s) become(s) a *secondary* authentication factor. On Android, the user can use a PIN, password, or pattern unlock as the dominant unlock method, but they are free to configure any of the available "smart locking" techniques (Face Unlock, NFC, location-based unlocking, etc.) as the secondary authentication. The PIN /password/pattern has to be used if the phone has not been unlocked for four hours, or if the phone has been restarted [4].

On smartphones, the dominant and secondary authentication factors are linked by a disjunctive relationship (where one *or* the other may be used) in ordinary circumstances, but in security-critical situations the dominant authentication factor becomes the only way to log in. We model these two types of authentication and the relationships between locking states in iOS and Android in Figure 1.

A distinction that becomes clear when modelling the relationship between dominant and secondary authentication is that there exist multiple states of locking on modern smartphones. There is a fully locked state, in which almost no functionality is available (incoming and emergency calls are always available, but telephony seems to be becoming an increasingly unused corner case for smartphones). The phone is put into a fully locked state by being rebooted, by being remotely locked, or by failing a set number of login attempts. From fully locked, the phone can only be unlocked by using the dominant authentication method.

Once the phone has been unlocked using the dominant authentication (and its state has thus transitioned from fully locked to unlocked), the phone usually moves between the unlocked and partially locked states. In the partially locked state, slightly more functionality is available (on iOS the camera becomes available, and notifications appear on the screen), but the significant difference is that the secondary authentication method can be used to unlock the phone.

The relationship between the dominant and secondary authentication systems for smartphone unlocking is unlike that seen in web authentication. Two-factor authentication uses multiple factors, but the user has to successfully complete both challenges (e.g., enter a password and copy in a one-time password sent via SMS) before access to the system is granted. The purpose of two-factor authentication is to improve security, not to facilitate the ease of logging in. Fallback authentication systems, such as password resets and challenge questions use the same disjunction as we see in mobile device authentication, but these systems are clearly not meant for regular use. Login times are very slow, and systems often force a password change when they are used.

# 3. FUTURE RESEARCH DIRECTIONS

Our observations about the configuration of authentication systems for mobile devices suggest a number of future research directions.

### *Layering Security Mechanisms*

A security issue arising from having multiple authentication schemes available is how users will combine security mechanisms and the security implications of those combinations. Does adding smartlocks improve the overall security of the device? Are there security vulnerabilities that result from combining particular schemes? Although termed "locks", secondary authentication mechanisms are more like keys that open usable doors to the device. The inequality in security between dominant and secondary authentication factors is usually handled via lockout policies. Limiting the number of incorrect password entry attempts minimizes the damage that can be done from a guessing attack on the secondary authentication mechanism. However, how should lockout policies be configured to most effectively maintain the tradeoff between usability and security?

### *A Choice of Authentication Schemes*

Dominant and secondary authentication essentially offer the user a choice about how they'd like to log in. While the idea of offering authentication choices to users has been explored in academic literature [3], there have not been many examples of it in practice. A variety of academic research has found that users are not very good at reasoning about threats and appropriate defences [8], but little existing research has investigated how users set up and use the multitude of available smart locks. Especially in the Android ecosystem, where a variety of smart lock options are available, users are being asked to reason about their own preferences and the threats that are relevant to their lives.

### *Future Authentication Strategies*

The current state of partial unlocking is reminiscent of the proposals for "continuous" [2], "implicit" [6], or "progressive" [7] authentication. It also somewhat resembles Unix's "sudo" mechanism to execute binaries with administrator privileges. Biometric authentication is becoming commonplace on smartphones through the introduction of fingerprint scanners, and it seems likely that aspects of continuous authentication may be introduced into existing mobile operating systems. This creates opportunities to design new authentication strategies that leverage this new paradigm, and to propose improvements to traditional desktop authentication. One idea could be to make the security state available system-wide, and to let applications reveal a subset of their functionality depending on the lock state of the device.

# 4. REFERENCES


[1] Apple Inc. iOS Security. Technical report, June 2015.

[2] H. Crawford, K. Renaud, and T. Storer. A framework for continuous, transparent mobile device authentication. *Computers & Security*, 39:127–136, Nov. 2013.

[3] A. Forget, S. Chiasson, and R. Biddle. Choose Your Own Authentication. In *NSPW '15*, 2015.

[4] Google. Set up your device for automatic unlock - Nexus Help, 2015.

[5] M. Harbach, A. de Luca, and S. Egelman. The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens. In *CHI 2016*, 2016.

[6] M. Jakobsson, E. Shi, P. Golle, and R. Chow. Implicit authentication for mobile devices. In *USENIX HotSec*, 2009.

[7] O. Riva, C. Qin, K. Strauss, and D. Lymberopoulos. Progressive Authentication: Deciding When to Authenticate on Mobile Phones. In *USENIX Security Symposium*, 2012.

[8] E. Stobert and R. Biddle. The Password Life Cycle: User Behaviour in Managing Passwords. In *SOUPS*, 2014.