Duress Unlock: Using Covert Signals to Restrict Access to Mobile Devices

Diogo Marques
LaSIGE, University of Lisbon
Ed. C6, Piso 3, Campo Grande
1749-026 Lisbon, Portugal
dmarques@di.fc.ul.pt

Luís Carriço
LaSIGE, University of Lisbon
Ed. C6, Piso 3, Campo Grande
1749-026 Lisbon, Portugal
lmc@di.fc.ul.pt

Tiago Guerreiro
LaSIGE, University of Lisbon
Ed. C6, Piso 3, Campo Grande
1749-026 Lisbon, Portugal
tjvg@di.fc.ul.pt

CHI 2014 Workshop on Inconspicuous Interaction, April 26, 2014, Toronto, ON, Canada.

Abstract
An unlocked mobile device can be a treasure trove of private information. Adversaries that are socially close to the user are in a particularly favorable position to explore it: they have access, can observe the victim's authentication code and can even be handed the device for a legitimate task. To address this threat, we propose a new authentication concept that assumes that, by default, a user is authenticating under duress. An inconspicuous side-channel interaction with the device at authentication time dictates whether it grants regular access or enters a secure mode. This paper explores how systems based on this concept can help coping with shoulder-surfing while also allowing for impromptu device sharing.

Author Keywords
Security; Mobile; Authentication; Access Control

ACM Classification Keywords
H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

Introduction
Personal mobile devices, like smartphones and tablets, employ unlock authentication has a security mechanism against adversaries with physical access. But these adversaries are not all created equal. While unlock

authentication may work as an effective deterrent when a device is lost or stolen, it is hardly a match for socially close adversaries intent on snooping.

Consider the following example: Alice and Eve are roommates. Alice does not like living with Eve and is thinking of moving*, but can't tell her before she* finds a new roommate. Eve gets suspicious and decides to find out more by looking through *Alice's* PIN-locked smartphone. She can find out the PIN easily by observing when Alice distractedly enters it. Or she can ask for the device to take a picture of the cat; Alice would never say no.

Access control through knowledge-based authentication (e.g. passwords, graphical codes), however common, is largely ineffective against adversaries like Eve. Her objective is to snoop through personal communication, which is conveniently centralized in a device she has easy access to. Furthermore, she does not need any technical knowledge to conduct an attack.

Recent work suggests that Eve's behavior is not a corner case. A survey of crowdworkers found that 9% admitted to snooping through someone else's device [8]. Our own data suggests that this number can be as high as 60% among young adult smartphone users [7]. Personal mobile devices store a great deal of information that is considered sensitive, including passwords, files, contacts, emails, text messages, call logs, location traces, schedules, pictures and videos [2, 8]. Exposure of this information is particularly harmful, since it can damage social relationships [5,6].

The authentication moment is at the crux of this vulnerability. Inserting a secret code in the presence of others is potentially dangerous, but understandable. Either for convenience or as not to signal distrust, it must be expected to happen, in a context where mobile devices permeate our social lives [6].

Authentication methods that assume that a user is under threat when entering the code are a possible solution. Panic passwords are used in some security systems, including commercial home alarms. Users can purposefully fail to enter the correct code, and instead enter one that apparently deactivates it, but actually triggers security measures (e.g. calling the police). This concept, however, does not translate directly to securing mobile devices against socially close adversaries. After repeatedly seeing Alice authenticate with the correct code, Eve would be able to tell if she used a different code before sharing the device. The more general concept of duress codes, where the distress is signaled covertly, can be applied. In the TV show "24", fictional counter-terrorism agent Jack Bauer inconspicuously includes the phrase "flank two" when communicating with HQ to indicate that he's compromised. This duress signal, although explicit, is covertly included in the interaction, and is thus undetectable by an unknowing third-party.

We propose a new authentication concept for mobile devices combining features of duress codes (covert signaling) and panic passwords (engaging security measures).

Concept

Here we define the main flow of operation and discuss different alternatives for the specific mechanics. The concept is based upon the user resorting to a side-channel to inconspicuously indicate if, upon entering

the correct secret code, the system should grant regular access or otherwise trigger security mechanisms. These mechanisms must be such that the third-party does not realize they are in place. We further propose that the security measures are triggered by default. That is, when the covert behavior is not detected, but the correct authentication secret is inserted, the adversary is given some access, although controlled. This concept addresses both a) the handling of attempted unauthorized access and b) impromptu device sharing. Returning to the example:

- If Eve tries to snoop though the device while Alice is sleeping, she can authenticate with the correct secret code. But since she doesn't know about the covert action, security measures will be triggered, unbeknownst to her.

- If Alice hands the phone to Eve for her to take a picture of the cat, she authenticates with the correct code, but purposefully fails to perform the side-channel action correctly, defaulting to the secure mode.

- If Alice's phone is lost or stolen, a third party will still not be able to authenticate, lacking knowledge of the secret code.

Side-channel: explicit vs. implicit
The side-channel input can be explicit or implicit. An explicit input is a specific, purposeful action by the user. For instance, the user could enter a PIN by clicking all digits on the leftmost side of the button. Implicit input, on the other hand, is "based on actions users would carry out anyway" [4], i.e. the behavior while authenticating. For instance, while authenticating with Android's pattern unlock, the touch screen data can be used to distinguish the legitimate owner from others [3].

Reacting to the signal: bogus account vs. logging
Upon not detecting the covert input, the device enters in a secure mode. As much as possible, its activation should not be transparent the third-party. For instance, if Alice were to share her device using Android's restricted accounts [1] functionality, this would be visible to Eve, and therefore signal distrust. Instead, we propose two possible security mechanisms:

- Bogus account: this secure profile must be set-up by the user. In xShare [9], it is proposed that a sharing policy is defined for applications, file access, and system resources. This concept could be further extended to allow bogus access to some applications, e.g. opening the messaging app would only show a selection of meaningless exchanges.

- Logging: allow access to either the regular or the bogus account but track usage for later review. Tracking can include not only user interactions but also screen captures, location data, and even photos or video taken with the device's front camera.

Preliminary validation

To start assessing this proposal, we conceived of a simple authentication method, based on Android's pattern unlock, that includes an explicit covert action. Namely, after performing the last stroke, making a small movement against the natural flow is required for unlocking.

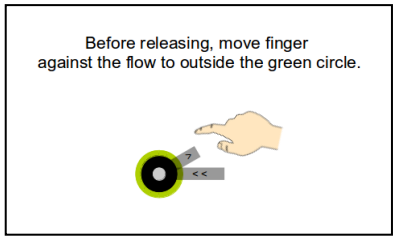

Figure 1 Instructions on how to perform the side-channel covert code as they were shown to user study participants.

User study

We recruited 8 students and asked them to perform two tasks. Task 1 involved observing, from a front angle, as the experimenter authenticated 3 times and, afterwards, trying to repeat it 10 times. Subjects were told that the objective was to see if they could rotate the pattern mentally. The unlock code would only be accepted if they performed the covert action. Task 2 started by explaining that they had been deceived, showing them the instructions on Figure 1, and having them try again 10 times.

For task 1, the mean success rate was .26 (SD=0.39). This larger-than-expected dispersion is largely explained by two subjects that perceived the pattern has having a returning stroke at the end. Although a full stroke was not necessary, it satisfied the criteria of the covert action. Of the remaining 6 users, only one was successful in one of the trials, by accident. This suggests that the covert action was difficult to observe and thus mostly successful as a side-channel code. For task 2, the mean success rate was .9 (SD=.16). Five users were successful on all attempts. This suggests that the explicit covert code is usable with no training.

Outlook

The authentication method that was evaluated could not be used in the real-world because wide knowledge would render it insecure. It is conceivable that a whole vocabulary of subtle gestures could be made available to the user, which would then be able to compose a personalized code. The evaluated method, nevertheless, speaks to the overall feasibility of using covert codes to cope with shoulder-surfing while supporting impromptu device sharing. Future work will focus on devising methods with large-enough dictionaries of explicit, covert side-channel actions, while still preserving usability. Furthermore, ways to give credibility to bogus accounts will also be investigated.

Acknowledgements

This work was supported by FCT (SFRH/BD/98527/2013, PTDC/EIA-EIA/117058/2010, PEst-OE/EEI/UI0408/2014).

References

[1] Restricted Profiles (retrieved 2014-01-17). http://support.google.com/nexus/answer/3175031

[2] Ben-Asher, N. et al. On the need for different security methods on mobile phones. In Proc. MobileHCI '11, ACM Press (2011), 465-473.

[3] De Luca, A. et al. Touch me once and i know it's you!: implicit authentication based on touch screen patterns. In Proc. CHI '12, ACM Press (2012), 987–996.

[4] Jakobsson, M. et al. Implicit authentication for mobile devices. In Proc. HotSec '09, USENIX Association (2009), 9.

[5] Johnson, M., Egelman, S., Bellovin, S. M. Facebook and privacy: it's complicated. In Proc. SOUPS '12, ACM Press (2012), 1-15.

[6] Karlson, A. K., Brush, A. J. B., Schechter, S. Can i borrow your phone?: understanding concerns when sharing mobile phones. In Proc. CHI '09, ACM Press (2009), 1647.

[7] Marques, D., Guerreiro, T., Carriço, L. Measuring Snooping Behavior with Surveys: It's How You Ask It. In CHI'14 EA, ACM Press (2014).

[8] Muslukhov, I. et al. Know your enemy: the risk of unauthorized access in smartphones by insiders. In Proc. MobileHCI '13, ACM Press (2013), 271-280.

[9] Liu, Y. et al. xShare: supporting impromptu sharing of mobile phones. In Proc. Mobisys '09, ACM Press (2009), 15.