Physical Intrusion Detection and Prevention for Android Smartphones

Joana Velho, Diogo Marques, Tiago Guerreiro, and Luís Carriço

Faculty of Sciences of the University of Lisbon
jvelho@lasige.di.fc.ul.pt, {dmarques, tjvg, lmc}@di.fc.ul.pt

Abstract. Authentication mechanisms are useful when a device is lost or stolen, but ineffective when it comes to preventing friends and family from snooping through contents. Most unlock authentication methods are vulnerable to observation attacks than can easily be performed by those in a close social circle. Moreover, unlock authentication does not address the common use case of device sharing. Intrusion Detection and Prevention Systems (IDPS) are based on the assumption that a system will eventually be attacked, and are widely used in network systems as an additional security measure that works around authentication flaws. In this paper, we present and evaluate the adequacy of an inconspicuous IDPS for Android smartphones, intended to dissuade socially-close adversaries from snooping through device contents. This system runs on the background and attempts to determine, through face recognition, if the device is being operated by the owner. If it is not, it starts recording user actions, which can later be reviewed by the owner. We conducted a laboratory study (n=12) to examine users concerns over other people looking through their data, and to present the system to participants. We also conducted a field study (n=10), where participants used the system for an extended period of time, in order to understand how they adopted it. Results indicate that the IDPS approach addresses previously unmet needs, namely by offering a security measure that does not require users to expend effort in every interaction with the device.

Keywords: IDPS, Inconspicuous, Mobile Devices, Adoption

1 Introduction

Mobile devices, such as smartphones and tablets, have become ubiquitous, and keep data on many aspects of users' lives. For that reason, many users set up unlock authentication to inhibit others from accessing device contents. Modern mobile devices offer a variety of authentication mechanisms, including some based on secrets, such as PIN, password and pattern, and some based on biometrics, such as face recognition. Unlock authentication is useful when a device is lost or stolen. However, recent studies suggest that unlock authentication is ineffective in protecting mobile contents from close adversaries [13]. On one hand, the most popular unlock authentication methods that are based on secrets are vulnerable to simple physical attacks, that can easily be performed by those in a

close social circle. On the other hand, some users quit or never configure unlock authentication because they consider inconvenient to enter a code every time they use their devices. Furthermore, unlock authentication does not address the common use case of device sharing.

In order to prevent family and friends from snooping through device contents, and to address the device sharing case, we designed and developed and intrusion detection and prevention system (IDPS) for Android smartphones. This software recognizes the owner through face recognition, and starts recording user actions when someone else uses the device. Later, the device owner can review the recordings. We designed our proposed IDPS to be inconspicuous, by running on the background and not disrupting the normal use of the device.

In this paper, we present the concept and architecture of our proposed system, as well as implementation details. We then present the results of a study consisting of semi-structured interviews with twelve smartphone users. The study was conducted in order to explore motivations for device sharing, and to identify defenses and emerging concerns. In this study, we also presented a prototype to participants, in order gather their perceptions on how such a system could be put to use. Finally, we present the results of a field study that was conducted to better understand how participants really adopt this system in their social context. Ten participants were recruited for this study, and used an instrumented version of our software for nine days. We assessed the usefulness of this approach and whether it addresses user requirements. We also used this study to find remaining usability problems. Overall, the IDPS approach was found to be useful, and to cater to user's desire to have security without having to incur in constant effort and vigilance.

2 Related Work

Smartphones and tablets are used for a many purposes, including to play games, access social networks, make phone calls, send text messages and shop online. With the emerging *Bring Your Own Device* trend, where employees are encouraged to use their devices to access enterprise data and systems, mobile devices also now commonly store sensitive work products [10].

Users are aware of the sensitivity of the data stored on their devices, and are concerned about security threats [5]. Recent studies indicate that unauthorized access by socially-close adversaries is not only not an uncommon occurrence, but may have a particular negative impact on users. In a survey of internet users, 14% of participants reported that their mobile devices were used by someone else without permission, and 9% admitted that they have used someone else's device without permission [13]. In another recent study, 70% of participants indicated a preference for preventing socially-close individuals from accessing some functionality on their phone [9], when confronted with a tool that provided that ability. Among the reasons invoked to use unlock authentication, users often cite physical threats, like the risk of loss or theft, or the desire to avoid family and

friends from snooping through contents or past unauthorized access experiences [7].

Unlock authentication mechanisms are intended to protect mobile devices in the event of theft or loss, but they are not appropriate to avoid friends and family from snooping through contents. Most unlock authentication methods are vulnerable to observation attacks than can easily be performed by those in a close social circle. The most popular unlock authentication mechanisms, which are based on secret codes, are susceptible to shoulder-surfing attacks, where someone could find out the access code just by looking when it is being entered [15]. Unlock authentication mechanisms, specially patterns, are also vulnerable to smudge attacks [2]. Interactions with the touch screen leave oily residues from the fingers; an attacker can observe the marks and often infer the secret code. Such observation attacks can easily be performed by those in a close social circle, for instance friends and family. Furthermore, many users choose not to lock their devices or give up on unlock authentication. In a recent large-scale study of smartphone users, 42% indicated that they didn't lock their devices. The most cited reason was that locking was too much of a hassle. [7]

Mobile devices users often share their devices with others for specific tasks, such as making phone calls, sending text messages and playing games [12]. As a result, sometimes the owners cannot control what others are doing on their devices, even if momentarily. Unlock authentication does not address this common use case. It will not avoid others from snooping through contents, since it is an all-or-nothing access control mechanism. Protecting contents from those in a close social circle should start with and understanding of how people commonly use their devices, and what actually worries them.

A proposal similar to ours is *continuous authentication*, in which the operator's identity is continuously monitored during the interaction with the device. Crawford *et al.* proposed a continuous and transparent authentication framework for mobile devices based on keystroke dynamics and speaker verification [6]. This framework associates identity confidence levels to tasks. The confidence value is re-calculated from biometric data acquired while devices are being used. Itus [11], is a related approach, and provides implicit authentication by continuously authenticating the device owner based on biometric behavior using accelerometer, touch and keystroke dynamics. The intrusion detection aspect of our approach is similar to these proposals, in the sense that it also captures biometric data to continually identify the operator.

FaceProfiles is another concept similar to our proposal, which associates different access permissions to groups of contacts, and when a new user is detected, through face recognition, permissions are recalculated and the user interface adapts accordingly by showing only applications allowed [8]. Our approach is similar, in the sense that it is also uses facial recognition to identify users, and that it targets sharing among socially-close adversaries, but differs in that the reaction is not multi-user support, but logging.

3 A user-facing IDPS

3.1 Concept

Intrusion detection and prevention systems are based on the assumption that a system *will* be attacked. Their main purpose is to detect intrusions and prevent damages. The intrusion detection model may be suitable for mobile devices as a defense against physical attacks performed by socially-close adversaries.

Drawing on this model, we designed and developed an inconspicuous physical IDPS for Android smartphones. It can prevent, detect and react to intrusions. It is capable of identifying if the device is being operated by the owner, and if not, reacts by recording user actions. The recordings are made available for later review. It offers the device owner the opportunity to know who used his device and for what purpose.

Intrusion detection. We propose detecting if the device is being used by its owner or by someone else, by continuously authenticating the operator. Continuous authentication using biometric characteristics does not require the user to perform any specific action. We specifically propose using facial recognition to identify the device's owner. While the user is interacting with the device, the system is, periodically and inconspicuously, taking pictures using the front-facing camera. This way the user can operate the device normally while intrusion detection runs on the background.

Intrusion reaction. Intrusion reaction is a set of actions performed by the system when it detects an intrusion [14]. This system's reaction to intrusions is to record users actions, in such a way that those recordings can be later audited by the owner.

Intrusion prevention. Surveillance cameras protect people, places and objects by constantly monitoring physical spaces. It is well know that just the awareness of their existence inhibits misbehavior. Mirroring this concept, we propose making the device display a permanent warning (as a notification), informing the operator that pictures will be taken and actions on the device will be recorded. In a close social context, even if the attacker hides his/her identity to the camera, it is likely that the owner is able to perform the identification given other context (e.g., time and even the details of the attack). Our system does not place any barriers that prevent an adversary from accessing the device. Yet it supports a password lock to access this mobile application.

3.2 Implementation

Our system is composed by a service module, an intrusion detection module, a recording module, a data repository and a user interface (Fig. 1).

When our application is running, the service module is responsible for coordinating the intrusion detection and recording modules. When the device is unlocked after a period of inactivity, the service module starts the intrusion detection module and stops it when the device is again locked. The intrusion

detection module is responsible for taking pictures inconspicuously and periodically, for processing face recognition analysis, and for then reporting the results to the service module. The service module stores the captured pictures and reacts depending on the face recognition result, by instructing the recording module to start or stop. The recording module is responsible for capturing users actions on the device.

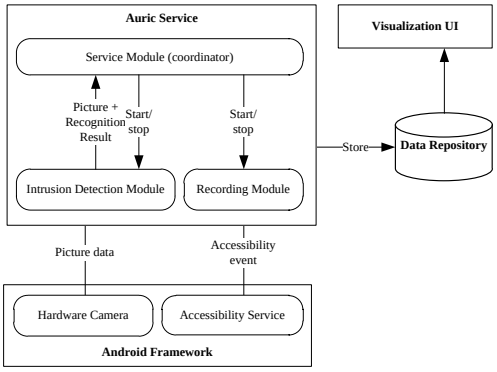


Fig. 1. Overview of the system's Android implementation.

3.3 Service Module

This module is responsible to start and stop recordings and for the intrusion detector. It has a receiver which listens to three types of Android system events and is notified when those events occur. It listens to "screen on" events, that are sent when the device wakes up and becomes interactive; "user present" events, that are sent when the user is present after the device wakes up, for instance after unlock; and "screen off" events, that are sent when the device becomes non-interactive. When a user starts to interact with the device, the background service is notified and starts the intrusion detector and waits for the face recognition result. If the device owner was not recognized, the background service will prompt the recording module to activate. If the owner is recognized by the intrusion detector, the background service will prompt the recording task to stop.

The service module acts as a coordinator of intrusion detection and user action recording. This way, the intrusion detection and recording modules are independent from each other. This module is also responsible for launching a notification informing the user that a intrusion was detected.

3.4 Intrusion Detection Module

This module is responsible for capturing pictures, processing face recognition analysis, and deciding the device is under a possible intrusion or not. Specifically, this module includes a task that awakes periodically and takes pictures

inconspicuously, using the front-facing camera. After that, the task performs face preprocessing, face detection and then face recognition. If the face recognition analysis indicates that the picture taken matches the owner's face with a configurable level of confidence, a possible intrusion is considered to be underway. Finally this module reports the result to the coordinator, which is the background service task.

We implement face recognition procedures, for instance face preprocessing, detection and recognition, using the OpenCV Library[3] and JavaCV[1]. OpenCV is an open source computer vision and machine learning software library that offers optimized algorithms to detect and recognize faces and also offers a SDK for Android. JavaCV is a Java interface to OpenCV which allow us to implement some features in Java instead of C++.

3.5 Recording Module

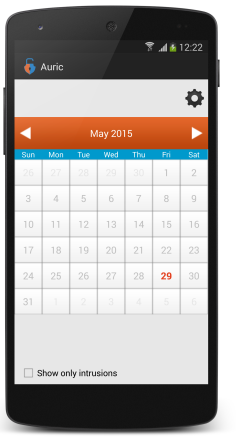
This module is responsible of recording users actions. It gathers data and processes it to a representation that is suitable for auditing. It supports two different methods of recording users interactions: *screen recording* and *event-based recording*.

The screen recording method produces a video of user activity on the device. Each frame of the video is like a screenshot taken while using the device.

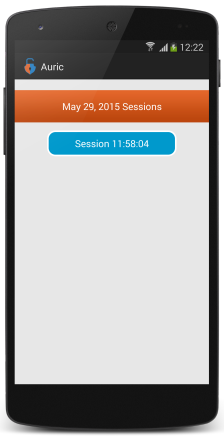
The event-based recording method produces a list of applications accessed and details about users interaction in each application. This method relies on events provided by Android's accessibility API. Accessibility events are messages about user interactions with visual interface components in an application. Those events help to produce a detailed log of users interactions with the device. This module communicates with an accessibility service that listens to specific accessibility events, such as text changing, view clicked, view selected, view scrolled and others. When one of those events occur, the accessibility service is notified and sends that information to this module to be processed and stored.

3.6 Visualization

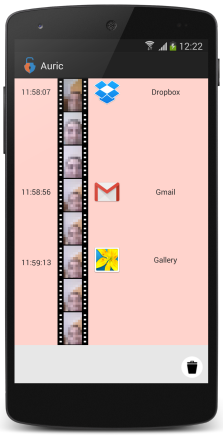
We designed an interface that allows the owner to easily access the recordings of intrusions detected (Fig. 2). We designed a calendar view showing the current month with the current day in bold; days where there were suspected intrusions are selectable and marked in red (Fig. 2(a)). By clicking on one of those days, a list of intrusion sessions will appear (Fig. 2(b)). Upon selecting a session, the recording of intruder's actions is shown. The way in which sessions are shown depends on recording method selected. If the screen recording method was used, a video capture of what happened on the screen is played, with the pictures taken with the front-facing camera rolling in the upper left corner. If instead the recording was event-based, a time-line of apps that were opened is shown, alongside a camera roll of pictures taken with the front-facing camera (Fig. 2(c)). Upon selecting an item on the list, all actions that were performed while using that app are shown (Fig. 2(d)).



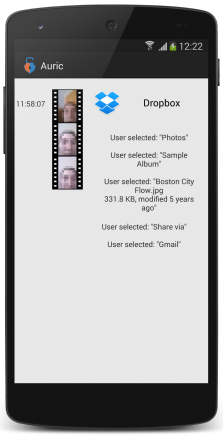
(a) Calendar View: the days when suspected intrusions occurred are marked in red.



(b) List of sessions from a day



(c) Time-line of apps used in a session, decorated with photos taken with the front-facing camera



(d) Details View: shows user actions within an app

Fig. 2. Visualization of logged activity on an Android smartphone.

4 Laboratory Study

We conducted a laboratory study in order to (1) learn about precautions that users have with mobile devices, to (2) explore concerns they have about people looking through their data, (3) to explore motivations for device sharing, and finally to (4) present the system to participants and understand how they would adopt it.

In this study, as well as in the next, we opted for a version of the system that only uses event-based logs. The screen recording method required devices to be rooted, and hence, we reasoned, would not realistically be adopted by many users.

4.1 Procedure

We conducted in-depth semi-structured interviews with twelve participants that use mobile devices, such as smartphones and tablets, on a daily basis. The study started with a set of questions about precautions that users have with mobile devices and their concerns over physical attacks. We then introduced our system's purpose and features. Next, we prompted participants to enroll in the system, and conducted a dramatization of two possible situations where our system can be useful, as follows:

Use case 1

1. The device is left unattended in a room for a few moments.
2. An attacker unlocks it and checks e-mail and text messages.
3. Before the device owner returns, the attacker leaves it where it was.
4. The device owner checks if someone used his device in his absence.

Use case 2

1. The owner searches for a photo in the device.
2. The owner hands the phone to another person to show that picture.
3. When unsupervised, that person sends it via e-mail.
4. The device is returned to its owner.
5. The device owner checks if the device was only used to view that photo.

After the dramatization, where participants acted as the owner, we conducted an exit interview, where we started by asking participants for general comments, and then probed specifically about our system's usefulness, and how they would adopt it, if at all.

4.2 Analysis

We recorded audio of the interviews and then a researcher transcribed it for analysis. The analysis of the interviews was done using thematic coding inductively. [4]. Two researchers used the first four interview transcripts for code discovery and then independently developed code books. Then, they met and agreed on a preliminary set of codes. Afterwards, the same two researchers re-coded four

interviews and compared the results, and by consensus, agreed on an extended set of codes. The two researchers then coded all the remaining interviews. Reliability was measured in the end and found to be acceptable (Cohen's $\kappa = .92$). The reported results are the marginal frequencies found by one of the coders.

4.3 Results

Current Usage All recruited participants, except one, considered their devices to be private, because they contain private or personal data.

A quarter of participants indicated that someone used their devices without authorization or to access unauthorized content.

> "There was a time that I lent the phone for someone else to play, and I ended up discovering that he was not playing. Suddenly I peeked and I saw that person was reading my text messages." (P1)

Device Sharing All participants reported that they have shared their devices with someone else to perform specific tasks: to show something (10/12), to make phone calls (5/12), to send text messages (4/12), to play games (2/12), to surf the internet (2/12), and for other purposes (3/12), such as using camera or operating the music player.

We identified some defenses used by the participants, including not handing the device to share contents, instead just showing it on their hand (5/12); keeping the mobile device in close proximity at all times (5/12); taking precautions with the accounts on the device, for instance, logging out (4/12), keeping close supervision when someone else is using the device (4/12) and sharing the device with the target application already open (1/12). The large majority of participants (10/12) commented on how trust affects attitudes towards the use by others.

> "I only give the device to someone I trust." (P8)

Adoption We tried to understand how participants planned to use the technology, if it was available to them. Responses indicate it often depends on the specific situation and on the nature of relationships with others. Half the participants intended to adopt the technology for deterrence. They foresaw using the application in such a way as to inhibit others to misbehave, for instance by informing them that the application was installed or by having it show notifications.

> "To be a deterrent method. Don't touch or I will know." (P12)

Almost all participants (11/12) intended to use our system for passive discovery of intrusions. They suggested using the application to discover misbehavior by others, but without any explicit intention to change their own behavior in order to catch intruders. A significant portion (4/12), however, indicated that they would use our system for entrapment, intending to actively create situations where others might be caught misbehaving.

"Maybe I would leave the phone on the table on purpose." (P5)

Only one participant intended to inform everybody that our system was installed. Three indicated that they wouldn't inform anyone. The majority (8/12), however, said they would inform some people but not others. Similarly, when asked if they would set up notifications, only one participant wanted to always show them. The majority (8/12) didn't want to show notifications at all, and 3/12 wanted to show them depending on the situation. Two participants indicated that they wouldn't tell anyone or show notifications because it would be embarrassing if others knew they were being recorded. Four participants commented on how anonymity affects behavior, indicating that if they were to let others know, they might act differently.

> "They do not know what they are doing is being monitored and it is more likely that people will do something, that maybe would not with the user's supervision." (P3)

A quarter of participants expected to catch people using their devices without permission if they were using our application; half did not, and the remaining were unsure.

Suggestions Prompted to give suggestions of ways to react to another person using the device, 3/12 participants suggested locking the device, 2/12 suggested to restrict access to certain contents, 2/12 to lock only if there was a high risk (e.g. when the other user does something that is considered sensitive). Some participants (3/12) also suggested that a notification to an external service could be sent, for instance via e-mail.

Advantages We asked participants if they saw any advantages of this approach in comparison to the security they already have in place. Two participants indicated that our application would be useful to control damages, by informing what contents were accessed.

> "To anticipate damage, if it is something secret, such as documents. People can have a contingency if they know what happened." (P3)

Half the participants indicated that our system could be used as an additional security measure; for instance, that it could be used along with unlock authentication.

The vast majority of participants, however, saw as the main advantage the ability to regulate social relations, for instance, using our system to "know who your friends are".

> "If I had this application, it would be easy to see who to trust and who could not be trusted" (P10)

> "I think we should just live surrounded by the people that we trust and they would not do this to us [snoop]. This app would help me identifying those people and have control over who you consider as a friend." (P5)

We also asked participants if they would like to leave with our application installed on their devices. Most did (10/12), but still some didn't (2/12). In those cases, technical difficulties were cited, e.g. not having a front-facing camera.

From this study, we conclude that users are interested in the possibility of auditing unauthorized access to contents. Users, the study suggests, could also use this technology to deter people in close social circles from even considering the possibility of snooping through device contents. Most of participants would adopt this technology as a way to regulate social relations, figuring out "who your friends are". In fact, it seems that many participants were more concerned with that than in keeping privacy.

5 Field Study

The main goals of field study were to perceive how participants would actually adopt this system, assess whether the concept is useful and whether it is appropriate to user requirements, and also to detect usability problems. For this study, we installed an instrumented version of our application on the participants own devices. The study lasted nine days, at end of which the application was removed. Data was gathered from three meetings with participants.

5.1 Apparatus

The participants used an alternative version of our system that did not take pictures; hence, it didn't detect intrusions, and simply recorded all interactions. In the field study version, participants also couldn't review logs on their own, only during the meetings with the researchers, which had a master password. We chose to prepare this special version because it would be unethical to record data from people that did not agree to participate, which would be the case of possible intruders.

5.2 Procedure

The study included three meetings with participants, on the first, second and ninth days, with the following structure:

Day 1

- **Step 1: Briefing** Participants were explained system's concept and functionality, the purpose of the study and the procedure, and asked for consent to proceed.
- **Step 2: Initial Interview** Semi-structured interviews to identify security measures used by participants and also their privacy concerns regarding mobile devices.
- **Step 3: Installation and Enrollment** Installation of our application in the participant's own device and initial set up. The enrollment was conducted to detect usability issues, since the version installed didn't perform face matching.

Day 2

Step 1: Interview Semi-structured interviews to identify changes in behavior, to assess if participants remembered their interactions, and their expectations regarding unauthorized access.

Step 2: Sessions Review The logs were reviewed by participants, and contrasted with their answers in the previous step.

Day 9

Step 1: Comments Participants were asked to offer general comments about the application concept and experience as a participant.

Step 2: Exit Interview Semi-structured interviews to summarize how participants adopted the system, and how they changed their behavior or perceptions, if at all.

5.3 Analysis

We recorded and then transcribed audio of the interviews. The analysis of the interviews was done using thematic coding inductively. [4]. The researcher who transcribed the interviews created an initial set of codes. That researcher and another coded two interviews each, compared the results, and agreed on an extended set of codes. The researchers then re-coded the interviews and measured reliability, which found to be acceptable (Cohen's $\kappa = .95$). One researcher coded the remaining interviews. The analysis is based on that researcher's coding.

5.4 Results

Use by third parties We again examined what motivated participants to share their mobile devices, their defenses to protect personal data and level of concern about a third-party using their device.

All participants reported that they have shared their devices with someone else to perform specific tasks: to show something (7/10) such as a photographs, to make a phone call (5/10), to play games (4/10), to send a text message (4/10), to surf the internet (3/10) and others (2/10).

Reported defenses included not handing over the device when showing contents (3/10); keeping supervision when someone is using their device (2/10); keeping the device around (8/10), trusting that friends and family will not snoop through device contents (6/10); and not storing very sensitive information on devices (4/10).

Regarding worries about having someone looking through their device data, 5/10 participants reported that it depended on the type of person or their trust relationship; and 2/10 that they were concerned over anyone using their devices. Only 1 participant wasn't concerned at all.

Bring your own device Two participants reported working in organizations that adopted BYOD policies. They use their own devices to handle professional e-mail and documents. Hence, their concerns were not only over personal data, but also sensitive work products.

> "This [device] has information about the two parts of my life, my personal and professional life." (P8)

Experiences of unauthorized use Two participants shared that someone used their devices without authorization, prior to the study. P9 reported a suspicion that a colleague snooped through her device after sharing it for a phone call. P6 reported that her tablet was accessed without permission to consult specific data.

Impact of participation As a result of participating in study, two participants reported an increased awareness of the threat, and plans to act on it. Before the field study, P9 did not use unlock authentication because it was inconvenient, but afterwards decided to set it up. P2 said that this study helped her realize the sensitive data stored on her device, and that she would now set unlock authentication also.

Adoption Only one participant reported adopting our system as a deterrent. P9 indicated that she informed her family that this kind of application was installed on her device in a way to discourage them to use her phone. Eight participants used the application to discover misbehavior by others, but without any changing their own behavior. One participant used the application for entrapment, i.e. actively creating situations where others could be caught misbehaving.

Problems All but one participant had some kind of difficulty setting up the application, including problems with enrollment, or with connecting the accessibility service or runtime service. These were usability problems that can be easily overcome by creating a wizard to help users through the initial configurations steps.

Half the participants expressed concerns over negative impact on battery life.

Seven participants had some kind of difficulty in interpreting the logs collected by the application. Some participants initially didn't understand the meaning of some the applications that appeared on the logs, such as home, lock screen, and launcher, because these packages are not commonly seen as being apps. This usability problem was mitigated early, and users received an update where packages related with system activities were filtered out.

Four participants reported difficulties in determining if the logged activities were their own. This problem was expected in the instrumented version used in the field study, which doesn't capture pictures because of ethics concerns. Indeed, 9/10 participants reported that they would prefer seeing pictures taken with the front-facing camera along with the logs.

Four participants expressed difficulty in understanding some labels in the app, such as "session", which we meant as the period of time between the device waking up and being again turned off. The main reason why this happened was

because users do not represent their usage as a set of sessions, but as continuous. This issue warrants further evaluation of design alternatives, for instance presenting a condensed time-line, with expandable logs for whole days.

Advantages Four participants indicated having a stronger sense of security with our application.

> "I feel more secure because if someone uses it I will know." (P4)
> "The icon makes me feel more secure, since everybody can see that is being recorded." (P7)

Three participants indicated that the application could be used to monitor a child's activity.

> "I could use it to know what my son does on his tablet" (P6)

The majority of participants (8/10) manifested being pleased with having passive security, e.g. that the app does not require attention, or that it runs on the background.

> "I think it is a type of application that does not require attention. It is running and when you feel the need you see the recordings. I think that's positive." (P5)

> "It doesn't ask me for a PIN or a sketch to use my phone."(P7)

Eight participants were pleased that the application allows them to know *who* used the device without permission, thus confirming our observation in the first study, that users want to closely regulate their trust relationships.

Four participants were pleased that the application allows knowing *what* was done in the device by others, which indicates a type of adoption that focuses more on damage control, as do traditional intrusion detection systems.

6 Limitations

Face Recognition Accuracy One known limitation of face recognition is that it's accuracy strongly depends on light conditions, camera quality and framing of the pictures. In this system, the lack of accuracy can somewhat be mitigated by the fact that multiple pictures are taken. Furthermore, since a false positive will only produce an additional log, the recognition algorithm can be optimized to minimize false negatives. Since the objective of our studies was to assess the feasibility of mobile intrusion detection systems, and how they would be adopted, we leave further investigation into specific biometric techniques (face or otherwise) for future work.

Privacy Implications As much as device owners see the potential in our application to protect their privacy, their friends and family might see it as infringing on their own privacy. In fact, our software could be used as an offensive tool, and the owner might seek to share the device in order to see what other people do, which may include accessing their own accounts. The fact that 3 participants in the field study suggested that our system could be used to control children's activities is revealing of the possibility of misuse. However, we find that if someone's intent were to spy on others, there are several tools better suited for the job than our software, and there's nothing to stop someone from installing spyware on their own devices.

Performance Because we wanted to examine feasibility and adoption issues, we did not conduct a formal performance analysis, nor did we optimize the software, leaving that for future work. Given the possible impacts on battery and data storage, we conducted only a test in a heavy user's device during 8h, between 5pm and 1am. The device was a Wiko Getaway smartphone with Android 4.4. Our system was configured to take pictures every fifteen seconds, while the device was being used, and to record all interactions regardless of the recognition result. In that period, our system was responsible for 5% of battery consumption, and occupied 140MB of storage. The space occupied by the application is essentially due to the size and number of photographs taken during monitoring. The impact on storage is significant and it could be improved by compressing pictures and/or offloading them to the cloud. The impact of battery consumption was not significant but could still be improved.

7 Conclusion

Our approach offers intrusion detection and response capabilities to end-users, specifically for the risk of physical intrusion by socially-close adversaries. Our system can act as a deterrent, and also as a tool for incident management.

In two user studies, we found that users are indeed concerned about third-parties looking through their mobile device data, and that those concerns are often dependent on trust relationships. Despite that, a large number of participants did not use unlock authentication because it is inconvenient or tedious. Our approach bridges this gap, catering to users' desire to protect the contents of their mobile devices, but without having to expend additional effort. Our system offers users the opportunity to know if their phone was attacked, to know who was the attacker, and what they did.

Future work on our implementation will target the usability issues that were identified, on improving performance, and on improving the accuracy of facial recognition by implementing an algorithm based on face and eye detection.

8 Acknowledgements

This work was supported by FCT through funding of the LaSIGE Research Unit (UID/CEC/00408/2013), and a PhD studentship (SFRH/BD/98527/2013).

References

1. S. Audet. JavaCV - Java interface to OpenCV and more. https://code.google.com/p/javacv/. 2009.
2. A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith. Smudge Attacks on Smartphone Touch Screens. In Proceedings of the 4th USENIX Conference on Offensive Technologies, WOOT'10, pages 1-7, Berkeley, CA, USA, 2010. USENIX Association.
3. G. Bradski. The OpenCV Library. Dr. Dobb's Journal of Software Tools, 2000.
4. K. Charmaz. Constructing grounded theory. Sage, 2014.
5. E. Chin, A. P. Felt, V. Sekar, and D. Wagner. Measuring user confidence in smartphone security and privacy. Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12, (1):1, July 2012.
6. H. Crawford, K. Renaud, and T. Storer.: A framework for continuous, transparent mobile device authentication. Computers & Security, 39, Part B(0):127-136, 2013.
7. S. Egelman, S. Jain, R. S. Portnoff, K. Liao, S. Consolvo, and D. Wagner. Are You Ready to Lock? Understanding User Motivations for Smartphone Locking Behaviors. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, CCS '14, pages 750-761, New York, NY, USA, 2014. ACM.
8. A. Hang, E. von Zezschwitz, Alexander De Luca, Heinrich Hussmann. FaceProfiles: Inconspicuous, Private and Secure Mobile Device Sharing Workshop on Inconspicuous Interaction at CHI 2014. Toronto, Canada, April 26- May 1 2014.
9. E. Hayashi, S. Das, S. Amini, J. Hong, and I. Oakley. CASA: Context-aware Scalable Authentication. In Proceedings of the Ninth Symposium on Usable Privacy and Security, SOUPS '13, pages 3:1-3:10, New York, NY, USA, 2013. ACM.
10. IBM BYOD - Bring Your Own Device - United States. http://www.ibm.com/mobilefirst/us/en/bring-your-own-device/byod.html. 2015. [Online; accessed 27-April-2015].
11. H. Khan, A. Atwater, and U. Hengartner. Itus: An Implicit Authentication Framework for Android. Proc. of 20th Annual International Conference on Mobile Computing and Networking (MobiCom 2014), Maui HI, September 2014.
12. A. K. Karlson, A.J. Bernheim Brush, and Stuart Schechter. Can I Borrow Your Phone? Understanding Concerns When Sharing Mobile Phones. In Proceedings of the 27th international conference on Human factors in computing systems - CHI'09, New York, New York, USA, April 2009. ACM Press.
13. I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, and K. Beznosov. Understanding users' requirements for data protection in smartphones. In Proceedings of the 2012 IEEE 28th International Conference on Data Engineering Workshops, ICDEW '12, pages 228–235, Washington, DC, USA, 2012. IEEE Computer Society.
14. M. E. Whitman and H. J. Mattord. Principles of Information Security. Course Technology Press, Boston, MA, United States, 4th edition, 2011.
15. 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 Smartphones. In Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services - MobileHCI '13, page 261, New York, New York, USA, 2013. ACM Press.