Personal and Ubiquitous Computing preprint
DOI: 10.1007/s00779-015-0840-5

Only Play in Your Comfort Zone: Interaction Methods for Improving Security Awareness on Mobile Devices

Peter Riedl, Rene Mayrhofer, Andreas Möller, Matthias Kranz [1], Florian Lettner, Clemens Holzmann, Marion Koelle

Part of this work has been carried out within the scope of *u'smile*, the Josef Ressel Center for User-Friendly Secure Mobile Environments. We gratefully acknowledge funding and support by the Christian Doppler Gesellschaft, A1 Telekom Austria AG, Drei-Banken-EDV GmbH, LG Nexera Business Solutions AG, and NXP Semiconductors Austria GmbH.
Part of this work has been carried out within the project "AUToMAte – Automatic Usability Testing of Mobile Applications" funded by the Austrian Research Promotion Agency (FFG) under contract number 839094.

P. Riedl
JRC u'smile, University of Applied Sciences Upper Austria,
Softwarepark 11, 4232 Hagenberg, Austria
E-mail: peter.riedl@fh-hagenberg.at

R. Mayrhofer
JRC u'smile and Institute of Networks and Security, Johannes Kepler Universität,
Altenbergerstraße 69 A-4040 Linz, Austria
Tel.: +43-732-2468-4121
Fax: +43-732-2468-4125
E-mail: rene.mayrhofer@jku.at

M. Kranz, M. Koelle
Institute for Embedded Systems, Universität Passau, Innstraße 43, 94032 Passau, Germany
Tel.: +49-851-509-3080
Fax: +49-851-509-3082
E-mail: matthias.kranz@uni-passau.de,E-mail: marion.koelle@uni-passau.de
[1]corresponding author

F. Lettner, C. Holzmann
Department of Mobile Computing, University of Applied Sciences Upper Austria,
Softwarepark 11, 4232 Hagenberg, Austria
E-mail: clemens.holzmann@fh-hagenberg.at

A. Möller
Metaio GmbH, Hackerbrücke 6, 80335 Munich, Germany
Tel.: +49-89-5480-198-0
Fax: +49-89-5480-198-99
E-mail: andreas.moeller@metaio.com

Abstract In this paper, we study the concept of *security zones* as an intermediate layer of compartmentalization on mobile devices.

Each of these security zones is isolated against the other zones and holds a different set of applications and associated user data and may apply different security policies. From a user point of view, they represent different contexts of use for the device, e.g. to distinguish between gaming (private context), payment transactions (secure context), and company-related email (enterprise context).

We propose multiple visualization methods for conveying the current security zone information to the user, and interaction methods for switching between zones. Based on an online and a laboratory user study, we evaluated these concepts from a usability point of view.

One important result is that in the tension field between security and usability, additional hardware can support the user's awareness towards their zone context.

Keywords Mobile Security · Security Zones · Sandboxing · Separation · Compartmentalization

1 Introduction

Current mobile devices are becoming the primary means of accessing information services for a significant part of the world population[1], and many of the services are or will become security-critical. In addition to mobile payment, ticketing, and physical access control applications, we expect virtual identity documents (passports, driving licenses, etc.), personal medical data processing, and industrial control to move towards integration into mobile devices such as smartphones or smart wrist watches. There are two direct implications of these trends for future mobile device usage: 1. Many users will use their mobile phone as their only device for performing security-relevant tasks without any form of prior training or exposure to more traditional computing systems, and the services and applications will therefore need to be *intuitively usable*. 2. At the same time, these application scenarios will require *higher security* than currently available on mobile device platforms. Besides, the trade-off between usability and security is aggravated because of the highly different requirements between applications running on the same device and the intrinsic context dependency: using a device within one's own office requires a different trade-off than using it while crossing a busy road. Current approaches of using application-level compartmentalization and permissions for access control do not seem to provide a reasonable trade-off because of their low granularity of compartmentalizing a mobile device [15].

We hence suggest to add an intermediate layer between the physical device platform on the lower and applications on the upper end of the stack to

[1] By the end of 2013, the number of mobile-connected devices is expected to exceed the number of people on earth [9].

Fig. 1: Security zone visualizations from left to right: hardware visualization (HWV), colored border visualization (CBV), colored notification bar visualization (CNV), colored text visualization (CTV). [best viewed in color]

provide users with a small number of well-defined and understandable *security zones*. Each zone holds a different set of applications and associated user data, and can apply different – potentially context-aware – security policies (such as authentication or networking restrictions). As motivating examples for applications with different security/usability requirements, we use mobile banking, accessing sensitive company email, and mobile gaming. These scenarios also cover the typical issue of bring-your-own-device (BYOD) initiatives, which describes the problem of using a personal device (untrusted from the organization point of view) for company purposes (e.g. reading email), and the sharing of otherwise personal devices with friends or family [20] (mostly in the gaming/entertainment context). Our approach addresses the "malicious app" threat, opposed to the "malicious user" threat, which is not scope of this work.

This concept of security zones raises research questions in terms of secure implementation [25] and concerning usability. From a user point of view, interacting with such zones requires both that users are aware of which zone they are interacting with at any time – a *visualization method* of the active zone – and to actively change between zones – a *switching mechanism*. Even though recent research [30] suggests that automatic, context-based switching would be desirable, we claim that the user should also have a way to manually override the automatically chosen zone (e.g. if users want to check business emails while they are not at their workplace). Therefore our concept of proactive security zone switching can complement context-based approaches. In this paper, we focus only on usability and compare multiple visualization and interaction mechanisms in terms of zone distinguishability, error rate, cognitive overhead, satisfaction, and time spent in the context of our motivating examples. We implemented four different visualization methods (three in software, one with additional hardware) and four different interaction methods (two different gesture-based approaches, selection via lock screen, and hardware switch) and present the results of three iterative user studies. Under the assumption that the concept of security zones is improving the security/usability tradeoff (backed by products such as Blackberry Balance and Samsung Knox), our

main contribution is to present an approach for interacting with such zones that is intuitive, exhibits a low error rate, and seems preferable to end users.

2 Related Work

Smartphones are often shared devices. Karlson et al. [20] found that when users share their phones with family, friends, and colleagues, different permission levels are applied. Voicemail, text messages and notes were seen more critical than sharing the device for e.g. watching a video or making a call. Interviewees highly welcomed security models that restrict device access, backing our assumption that users care about security and privacy as long as it does not cause additional burden.

To increase security awareness, different visualizations have been proposed. *Dynamic Security Skins* [12] try to prevent phishing attacks by dynamically skinning secure UI elements which are hard to predict by attackers (i.e., the approach is a sort of visual hash). *Sesame* [32] is an extension of the desktop metaphor, where the desktop can be rotated to view security-related information "behind the scenes". This should inform security decisions of the user, e.g. whether to allow an application to access the Internet.

However, with current state of the art in mobile platforms, we have to assume all devices to be insecure: even if sandboxing techniques are used to compartmentalize applications from each other and protect the operating systems from applications (cf. [8] for proposed improvements to the standard Android sandbox), the overall complexity of the whole stack leads to security-relevant issues, either in the form of exploitable bugs [17, 10] or conceptual problems in the sandbox restrictions [14]. Egners et al. [13] provide a classification of threats to mobile services into owner threats, platform threats, threats to other users, and mobile network operator threats. As an example for current threats to mobile device users and their installed applications, the lack of awareness for security updates has been identified as problematic in large scale app store-based studies [26, 21]. In our focus on visualization and interaction, we are mostly concerned with owner threats, and suggest to use the notion of security zones [28] as one way to reduce their impact.

Security zones are an established concept. Stajano et al. [31] suggest a multi-user operating system with multiple sessions, allowing individual rights for each user, plus one public session with applications and content non-critical for privacy. From both a usability and implementation point of view, Feske and Helmuth [16] present an extension to the X windowing system to indicate which security context an application window belongs to. However, mobile devices require different approaches to visualization because window managers and the resulting window decorations are rarely available, and running applications often use full screen modes. *TreasurePhone* [30] emphasizes the dynamic character of privacy by multiple spheres, which represent privacy requirements in a specific context, and which can overlap. Spheres can e.g. represent home

or work contexts, but also location. From a technical implementation point of view, security zones can be implemented by virtualization [19,7,28].

For explicitly switching between zones, e.g. gestures can be used. Bragdon et al. [6] analyzed touchscreen gesture designs under different conditions. According to them, gestures do not perform worse than soft buttons, even "on the go". However, free-form gestures resulted in a worse performance than simpler bezel gestures. Research suggests that also the device hardware itself can be integrated in the interaction. Wolf et al. [34] investigated on-device gestures and found that e.g. drag and lift gestures can easily be executed one-handed when using the phone. De Luca et al. [11] suggested back-of-device interaction for authentication patterns as unlock alternative less prone to shoulder-surfing attacks.

3 Conceptual Background and Context

3.1 Security Concepts

3.1.1 Motivation for Employing Security Concepts

As Becher et al. [3] state, "with increased processing power and memory, increased data transmission capabilities of the mobile phone networks, and with open and third-party extensible operating systems, phones become an interesting target for attackers". Security is, to many users, a rather abstract and vague conceptual entity. Huang et al. [18] note that in this context, "people seldom question the benefits of using computers and Internet for communication and doing business". Among many categories of threats identified in their study, they name especially "deliberate software attacks" by viruses, worms, or Trojan horses. We explicitly try to raise awareness in users to recognize (not to prevent) this attack type. Given the developments and spread of mobile systems and their ubiquitous use, it is very important to investigate usable concepts that help to ensure information security, that is the protection of information and the systems and hardware that use, store and transmit that information [27]. Despite that, so far, there has not been any major attack with large-scale implications for a large number of mobile device users, we feel the need to raise both awareness of the users on security issues and, at the same time, aim at providing a usable and effective solution in everyday contexts.

Increasing the users' responsibility in ensuring information security demands not only knowledge on and awareness towards security issues, but requires to increase the value of the role of the user. This requires, according to Albrechtsen et al. [2], motivational aspects to account for security and a security solution that is functional and does not demand large additional efforts. This is especially important in situations where the user's primary goal of achieving a task conflicts with security. This means, e.g., that the user's desire to acquire information, such as bank account balance, might lead her

to not check if the server certificate is trustworthy. We explicitly try keeping the needed mental load as low as possible.

We provide a selective discussion on security concepts limited to personal mobile devices, who are mainly used by a single user. We explicitly do not consider multi-user device usage, e.g. as recently introduced in the Android operating system. For these scenarios, our approach would be implemented for every user. Related concepts, such as safety and privacy, are not investigated within this work, as our primary focus is on visualization and interaction concepts.

3.1.2 Zones

The concept of zones, as we use it in this work, is that of disjunct spheres of concerns. The zones are intended to allow for and provide a clear separation between things (applications, data, ...) that should be kept distinct. One implementation in a mobile enterprise context, for two zones, is the so-called "BlackBerry Balance", enabling users to keep both personal data and business data separated from each other. This e.g. ensures that business emails are always accessed only from the business mail application. This concept has also been pursued in a high-security governmental context, but also only limited to the two zones 'open' and 'secure'[2]. While this distinction is sufficient from a corporate point of view, it is not for an individual. Being in their private zone, users might still have different security demands, e.g. for mobile banking or playing a web-based game.

Strictly separating the zones implies that apps might exist multiple times – one time for each zone. An example for this multiplicity would be an email application. The same app will be present in each of the zones, but always use different data, not allowing to access business data in a private context.

During initial discussions with end users and by evaluating existing concepts, we identified three distinctive *types* of zones that can be used as a basis to separate concerns on single-user mobile devices. Our concept allows for the introduction of additional zones, depending on the personal context of the mobile user (e.g., multiple business zones instead of one if the user had multiple jobs). A limiting factor will be though the interaction concepts used for switching between them. We will elaborate on this in the section on the potential mechanisms for changing from one zone to another. The three most important types of zones, to us, are:

- **Open Zone:** This zone is unrestricted (full network access, all apps can be installed and started at any time). This zone could e.g. be used when playing games, such as "Angry Birds". The purpose of this zone is to provide all functionalities and freedom users are currently used to. Therefore it also faces the same security concerns (e.g. malware infection by third party application stores).

[2] `http://www.telekom.com/media/enterprise-solutions/200664`, last visited 09/09/2013

- **Secure Zone:** This zone is partially restricted, that is, only secure apps can be installed and executed that do fulfill certain criteria, e.g. certain trusted applications that come with a valid issuer certificate. This zone could be used for applications with a higher security demand, e.g. when confidential personal data or payment information is involved, such as mobile banking. This zone is fully controlled by the user, in contrast to the remotely "managed zone".
- **Managed Zone:** This zone is managed by an enterprise, meaning that the users cannot control themselves which apps can be installed or which networks the device connects to when being in this zone. The remote administration contributes both to a high level of security and comfort for the user. An example would be corporate Intranet access or corporate email.

3.1.3 Security on Platform Level (Software and Hardware)

Common software-level concepts for security include access control, e.g. on application level (only a certain user might execute apps) or on file system or user level (only a certain user might have access). These concepts are too limited in several ways. It would, e.g., require the user to have a dedicated app for each email context. This, we argue, will result in confusion (due to an additional cognitive load upon the user to memorize which context an email app belongs to) and maybe in a threat towards the security goals.

3.2 Interaction and Visualization Concepts

We have chosen Google's Android mobile OS as basis for our implementation, as Android allowed us more modifications at a lower system level, e.g. to substitute the lock screen, define additional gestures, or include external hardware. While other mobile platforms have different overall user interface concepts, most individual interaction concepts, such as device unlocking or touch gestures, resemble each other. We hence argue that an adoption and implementation of the concepts with the iOS platform would have yielded comparable results.

3.2.1 Interaction Concepts for Switching Zones

Given the rich sensing and input modalities offered by current mobile devices, different interactions for zone switching are possible. Below we discuss the concepts on a general level. The specific details (including figures) are described together with the prototype. All switching mechanisms are, from an interaction point of view, known to the user (e.g. swiping). Thus, familiarity and thereby educated feedback from the users should be possible, despite the novel security context.

As discussed, usability of security is a key factor for user acceptance. Therefore, the switching methods have to be simple to perform, easy to memorize,

quickly accessible, but at the same time do not have to interfere with existing input actions.

We have presented examples discussing the usability of both touchscreen- and hardware-based mobile interaction in the *Related Work* section [6,34, 11]. We have chosen to investigate two touchscreen-based switching mechanisms (swiping, gestures), a combination of touchscreen-based and physical input (lock screen) and hardware-based switching mechanism (using a physical switch on the added casing of the device).

3.2.2 Visualization Concepts for Zone Awareness

In this part, we discuss the selected concepts for making the user aware of the current security zone. Besides simply using the zone names for identifying zones, colors can be a means for unobtrusive and easily perceptible awareness of which zone the user is currently in.

The idea of visualizing the security status of a web site by the use of colored browser themes has e.g. been used by Maurer et al. [24]. They change the color of the whole browser theme to indicate the validity of a server's SSL certificate and thereby the information security of the user's data on this page. They used a greenish theme for an extended validation of the certificate, blue for a standard SSL certificate and a reddish color for unencrypted page content.

Colors for coding information have, besides many advantages, also significant shortcomings. There are cultural differences in the interpretation and perception of colors [5,29], though there are also indications that some associations seem to be common in their perception [1]. In addition, there exist different types of color blindness [33]. We, though, have chosen to use color-based information mediation of the current security zone as we feel that the potential individual shortcomings can all be addressed and thus counterbalanced. The display of the current zone with the associated color might give an attacker some information, but we feel that shoulder surfing for gaining personal data is a bigger risk towards information security than displaying the zone information [23]. The possibility of personalization is important regarding acceptance of services and systems. The lack thereof might give the user a feeling of lack of control. By adding the option to personalize the color scheme, including color values, hue and saturation, towards one own's preferences we would not only support the normal user, but also allow a color-blind person to select distinguishable colors. We are aware that using colors for indicating the security zones might lead to scalability issues: on the one hand, memorizing a larger number of color-zone associations would put a mental load on the user; on the other hand, the number of easily distinctive colors is limited.

In our implementation, we have chosen red, green, and blue as colors for visualizing the zones. While the colors were mainly chosen with focus on distinctiveness, we opted against yellow, as it could have implied a "middle secure/dangerous" zone (incorrect association with traffic lights).

The association between colors and zones was, for our cultural context, chosen as follows:

- **Red:** standard/open zone; red implying potential risks
- **Green:** private/secure zone; green implying safety
- **Blue:** business/managed zone; blue as distinctive 3rd color

The color scheme can be combined with different visualization elements as described in the following.

We, in the following, only used the coloring as described below. It can be assumed that repeating the individual color in other user interface elements will additionally contribute to the user's awareness. This is, though, not part of the current work.

3.3 Motivation for Software and Hardware Prototypes

While several alternatives could potentially be investigated with a pure questionnaire approach or using a Wizard-of-Oz approach with relation to the implementation, there exists the possibility to miss a "good" combination of visualization and switching mechanism due to this study setup. To be able to investigate the potential of the different visualization and switching approaches, we designed a three-step study setup. By this process, described in detail below, we aimed at reducing the number of options (number of visualizations $\times$ number of switching mechanisms) to an amount that can be handled in a hands-on laboratory study.

4 Visualizations

In this section we describe our proposed visualizations for the currently active security zone and elaborate on advantages and disadvantages thereof. A summary of advantages and disadvantages of all visualizations is given in Table 1.

4.1 Colored Border Visualization (CBV)

The *CBV* (see Figure 1) consists of a colored border around the entire visible screen. The intent of this visualization is to constantly inform the user about the currently active zone unobtrusively. Neither the notification bar nor the displayed soft buttons are enclosed within this border. The reason for this is that depending on the hardware (mobile device) the soft buttons may be visible or not. The notification bar is also not visible all the time, so in order to keep a consistent user experience we decided to exclude this area. One advantage of this approach is that regardless of the running application, the user is continuously aware of the currently active security zone. A disadvantage of this visualization is that the border inevitably reduces the display space available for applications to a certain extent, depending on the pixel width of the border.

4.2 Colored Notification Bar Visualization (CNV)

The *CNV* (see Figure 1) uses the notification bar to visualize the currently active security zone. The background color of the notification bar is set to the color of the active zone according to the color scheme. The advantage of this visualization is that the user is informed about the currently active security zone in an ambient manner whenever the notification bar is visible. This is also a disadvantage of this approach: whenever the notification bar is not visible (e.g. when using full-screen applications), the user is not reminded about the security zone. Another potential problem are customized operating system themes which could interfere with a colored notification bar.

4.3 Colored Text Visualization (CTV)

The *CTV* (see Figure 1), like *CNV*, uses the notification bar to visualize the currently active zone. This is done by displaying the name of the currently active zone in its respective color according to the color scheme presented in the *Concept* section. One clear advantage of this visualization is the low cognitive load for the user – even if users do not remember the color scheme, they can simply read the name of the zone. One disadvantage is that it is not easily possible to inform the user about the currently active zone in an ambient manner. Users explicitly have to shift attention, away from their current task, to the notification bar in order to read the name of the zone. Besides this fact, it suffers from the same disadvantages as *CNV* when the notification bar is not visible or when custom themes are used.

4.4 Hardware Visualization (HWV)

Unlike all previously mentioned visualizations, the *HWV* (see Figure 1) combines software and hardware to visualize the currently active zone. We used transparent resin to cast a case for the device which enables us to place a microprocessor board in the case and multi color light emitting diodes (LEDs) around the device. The LEDs are used to illuminate the case in the color of the respective zone according to the color scheme. An advantage of this visualization is that – regardless of the displayed information on the device (e.g. home screen, full-screen application, etc.) – the security zone is conveyed to the user. A disadvantage of this solution is the need for additional hardware that is as of now not available on off-the-shelf mobile devices.

5 Switching Mechanisms

In this section, we explain all proposed switching mechanisms and their respective advantages and disadvantages. A summary thereof is given in Table 2.

Table 1: Advantages and disadvantages of the presented visualizations.

Visualization	**Advantages**	**Disadvantages**
CBV	continuity	reduced screen size
CNV	ambient	incontinuity, theme interference
CTV	low cognitive load	attention shift, incontinuity, theme interference, space requirements
HWV	continuity	additional hardware

5.1 Gesture Switching Mechanism (GSM)

The *GSM* (see Figure 2) leverages gestures to switch between the different security zones. The gesture to switch to the desired zone is the first letter of the zone name according to the one stroke alphabet [4]. This alphabet uses gestures that closely resemble well-known Arabic letters that can still be drawn in a single stroke. We chose this approach to minimize the learning effort and cognitive load for the user. An advantage of *GSM* is that the desired zone can be directly accessed, which could reduce the task time for experienced users. Disadvantages are that the user has to remember all zone names and that recognition – especially of more complex gestures – is error-prone.

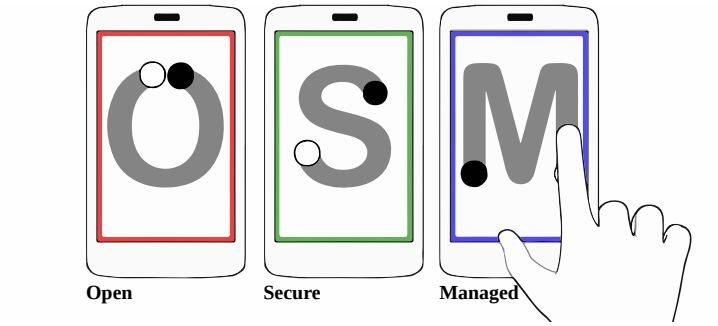


Fig. 2: The gesture switching mechanism (GSM) allows to directly switch to the desired zone by drawing the starting letter of the zone name. Note: The border color indicates the zone that will be switched to after the gesture. [best viewed in color]

5.2 Lock Screen Switching Mechanism (LSM)

The LSM enhances the lock screen with the functionality to switch between security zones. In contrast to all other switching mechanisms presented here, *LSM* requires switching to the lock screen to perform a zone change. The full

description of the switching process is depicted in Figure 3. With *LSM* the user can directly access the desired zone without having to navigate through other zones. To perform a switch with *LSM*, the user has to perform more actions than with the other switching mechanisms. Because the names of all available zones are displayed on the lock screen, there is no need to remember the order of zones (as e.g. necessary for *SSM*), or which zones are available. Another advantage of *LSM* is the increased awareness about the zone switch.

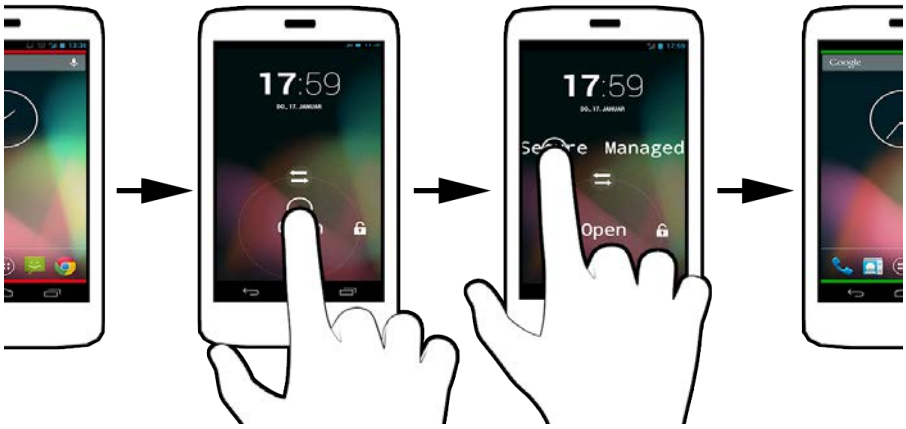


Fig. 3: The lock screen switching mechanism (LSM) allows to change zones on the lock screen. For the depicted switching method, the colored border visualization (*CBV*) has been used in this example. [best viewed in color]

5.3 Swipe Switching Mechanism (SSM)

The *SSM* (see Figure 4) utilizes a horizontal three-finger swipe gesture to switch between security zones. One common application for that interaction method is e.g. browsing through a picture gallery. We adopted this technique to browse through security zones in a circular manner. This means, consecutive swipes in the same direction (left or right) will switch through all available zones until the initial zone is reached again eventually. One advantage of this approach is simplicity.

This might include the potential for unintentional zone changes. A disadvantage of *SSM* is that the desired zone can not be accessed directly – it may happen that the user has to swipe through several zones to reach the desired one.

Fig. 4: The swipe switching mechanism allows to switch between zones with a three-finger swipe gesture. [best viewed in color]

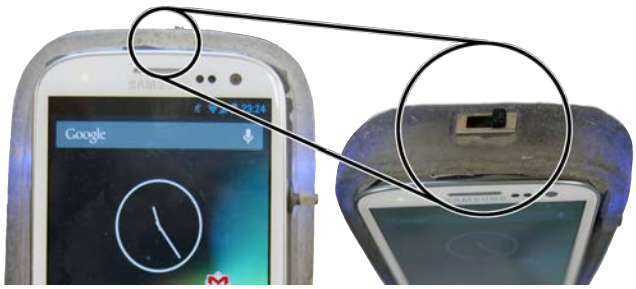


Fig. 5: The hardware switching mechanism utilizes the sliding switch mounted on the custom-built case to switch between zones. [best viewed in color]

5.4 Hardware Switching Mechanism (HSM)

In order to switch between zones using the *HSM* (see Figure 5) we again leverage the custom-built transparent resin case. Besides LEDs we mounted a three-state (left, center, right) slide switch on the top of the case. The state of the switch directly determines the selected security zone. We intentionally did not place the switch on the sides of the case to avoid accidental zone switches and to enforce explicit user interaction to raise awareness about the currently active security zone.

One disadvantage of of this approach is the need for additional hardware. Another disadvantage is if the current zone is the one associated with the left position and users want to switch to the zone associated with the right position, they inevitably have to go through the zone at the center position. The *HSM* also limits the number of security zones to the number of available states.

Table 2: Comparative discussion of the four switching mechanisms in terms of selected properties.

Switching	**Advantages**	**Disadvantages**
GSM	direct access	cognitive load, error-prone
LSM	direct access, awareness	multiple steps, time-consuming
SSM	simple, well-known	error-prone, no direct access, in-app gesture interference
HSM	simple, awareness, haptic feedback	no direct access, additional hardware, limited num. of zones

6 Evaluation

6.1 Scenarios

The scenario the participants were presented was inspired by a typical work day. The daily routine of getting up, performing tasks at work and relaxing in the evening was imitated. The story associated with the scenario started with the user getting up in the morning and checking the private bank account. This is a typical example for the use of the *Secure* zone. The second task was to check business emails – in the *Managed* zone. Finally, after the workday, the task was to relax playing a game, to be performed in the *Open* zone.

6.2 Questionnaire

To gain user feedback on the zone visualizations and switching mechanisms, we used a questionnaire both in the online and the lab study. Subjects rated the look and effectiveness of visualizations, and the memorability and simplicity of switching mechanisms. While the ratings were based on video demonstrations in the online study, they were based on a real prototype in the lab study.

In addition, we collected in the online study, in a second part of the questionnaire, information on mobile device usage. These questions covered in particular the number and purpose of used devices, their operating systems, separation between work and private devices and tasks associated with these devices. Goal of these questions was to obtain an impression of current device usage and awareness for potential security risks associated with this usage behavior.

If not stated otherwise, questionnaire items were answered on a 5-step Likert scale, where 1 corresponds to “strongly disagree” and 5 to “strongly agree”. When reporting the results, we use α for significance levels and σ for standard deviations.

6.3 Pilot Study

We conducted a pilot study to test the questionnaire, the implementations of the prototype and the logging mechanism, and to identify potential problems. The pilot was run with 30 participants (4 female, 26 male, avg. age 29, σ = 4.3) who answered the questionnaire and evaluated the visualizations and switching mechanisms. The pilot revealed some interesting findings on what could be improved for the next iteration of the prototype. The initial zone names *Standard*, *Private* and *Business* were changed to *Open*, *Secure* and *Managed*, since especially *Private* was frequently misconceived as the leisure zone, instead of the privacy-preserving zone. Further, we improved the gesture recognition, as some participants had problems drawing the zone name in the *GSM* method. Likewise, some wordings in the questionnaire were improved.

6.4 Online Study

6.4.1 Participants

150 participants took part in the survey (36 female, 114 male); the average age was 27 years (σ = 5.8). They were recruited via social network cross-posting (second-tier network context) so that the initiator was unknown, which suggests unbiasedness in participation. Most subjects originated from Central Europe and the UK, but also from Asia and India.

6.4.2 Task and Measurements

Participants answered an online questionnaire consisting of two parts. In the first part, we asked about the usage behavior of mobile devices, especially with relation to multiple devices and security-related aspects. We hoped to gather indicators on potential security problems, motivating our zone concept.

In the second part, the zone concept presented above was introduced to subjects. After a textual description of the concept, videos of three zone visualizations and three switching mechanisms were shown and subsequently evaluated by the subjects. The presented visualizations of the current zone were *CNV*, *CBV*, and *CTV* (cf. Section 4). The presented switching mechanisms were *SSM*, *GSM*, and *LSM*. The order of the presentation of visualization and switching mechanisms in the questionnaire was randomized between participants to avoid learning effects.

6.5 Online Study Results

6.5.1 Device Usage

61% of subjects own more than one mobile device; 10% have even four or more. The most common device type were phones, followed by tablets, and,

significantly less, media consumption devices (music players, ebook readers) and sports devices (fitness trackers, etc.). The most common platforms in our sample were Android (57%) and iOS (19%).

If subjects have multiple devices, they are also using them regularly. 41% use their primary device every day. For secondary devices daily usage was reported by 57% of subjects, for tertiary devices by 71%, and for quaternary devices by even 87%. At first sight, this looks as if primary devices are used less frequently than non-primary devices. However, the rising quotas for secondary to quaternary devices reflect the fact that the percentage values for the n-th device include subjects that only have n devices in total.

This means the more devices people have, the more they tend to use all of them – potentially in different environments.

In particular, we were interested in *what* those devices are used for (e.g., shared work and private usage on one device), which would justify the proposed zone concept. The amount of business-related usage rises from primary to quaternary devices, probably because non-primary devices are often dedicated work phones or tablets. While 20% use their primary device for business purposes, the amount of work usage is 33% for the secondary, 31% for tertiary and 67% for quaternary devices. However, we found that work usage is not exclusive: 17% use their primary device, 29% the secondary, 28% the tertiary and 53% the quaternary device for both private and work applications. Only 66% of subjects indicated to separate devices by task (e.g., using their work device only for office tasks and their private device only for private tasks). Even less (28%) separate by location (e.g., using their work device only in the secure enterprise network). This implicitly tells about the security awareness of subjects.For example, some subjects stated to read business mails on private devices (or the other way round), to use their business phones to do payments (e.g. banking) and to use social network apps.

6.5.2 Zone Visualizations

Subjects rated the look (*"The look of the visualization was appealing"*) and effectiveness (*"The different zones were distinguishable with the visualization"*) of each of the three visualizations. Friedman rank sum tests revealed a significant effect of visualizations on look ($\chi^2 = 47.92$, $p < 0.001$) and effectiveness ($\chi^2 = 9.11$, $p = 0.01$). Post-hoc Wilcoxon tests with Bonferroni correction showed that the look of *CNV* was rated significantly better than of the other visualizations ($p < 0.001$), and that the effectiveness of *CNV* was significantly better than of *CBV* ($p = 0.008$). There were no significant differences in look or effectiveness between *CBV* and *CTV*. The results are visualized in Figure 6a.

Subjects presumably found the color in the notification bar easier to perceive than at the screen border. Additionally, some criticized the loss of screen real estate with the border visualization. In the free text comments in the questionnaires, participants mentioned general drawbacks both for text and color representations. Color (both for *CNV* and *CBV*) requires the memorization of

the mapping to the respective zones, which is not a problem of *CTV*. However, *CTV* takes up precious space in the notification bar. Another raised issue is the usage of color-only representation for colorblind users. However, in Section 3, we presented an idea on how to resolve this by custom color schemes.

6.5.3 Switching Mechanisms

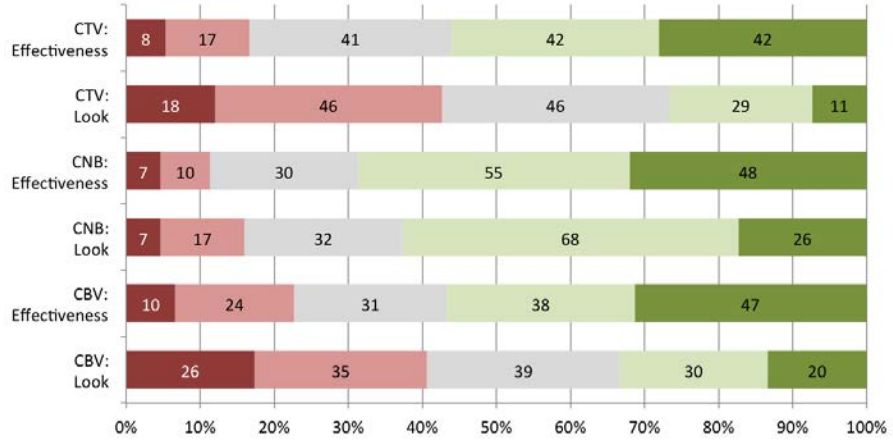
Subjects rated each switching mechanism in the dimensions memorability (*"The switching mechanism can easily be memorized"*), and simplicity of execution (*"The switching mechanism can be applied easily"*). In all dimensions, *LSM* was evaluated best; second-best was *SSM*, followed by *GSM*. Friedman rank sum tests showed a significant effect of switching mechanisms on understandability ($\chi^2 = 28.65$, $p < 0.001$), memorability ($\chi^2 = 84.38$, $p < 0.001$) and simplicity ($\chi^2 = 88.79$, $p < 0.001$). Post-hoc Bonferroni-corrected Wilcoxon tests showed differences between all mechanisms to be significant, with $p < 0.002$ for understandability and $p < 0.001$ for memorability and simplicity. The results are shown in Figure 6b.

Results suggest that *GSM* was seen as too complicated, which was confirmed by free-text answers in the questionnaire. It requires, firstly, a high cognitive effort to remember the first letter of the desired zone, and secondly, the drawing skill to fulfill the gesture. *SSM* was easier to understand and perform, but has a higher risk of accidental switches and of a confusion with multi-finger swipes that are mapped to other functions within applications. Likewise, the "position" of each zone must be memorized to know whether to swipe left or right. *LSM* does not require to remember a mapping between the desired zone, and it is unlikely to be performed erroneously. However, in its present form, it is applicable only for a limited number of zones (fitting around the unlock circle). In order to scale for significantly more zones, a recursive pie selection mechanism could be applied, similar to e.g. the contextual menu in Android 4.3's stock camera app.

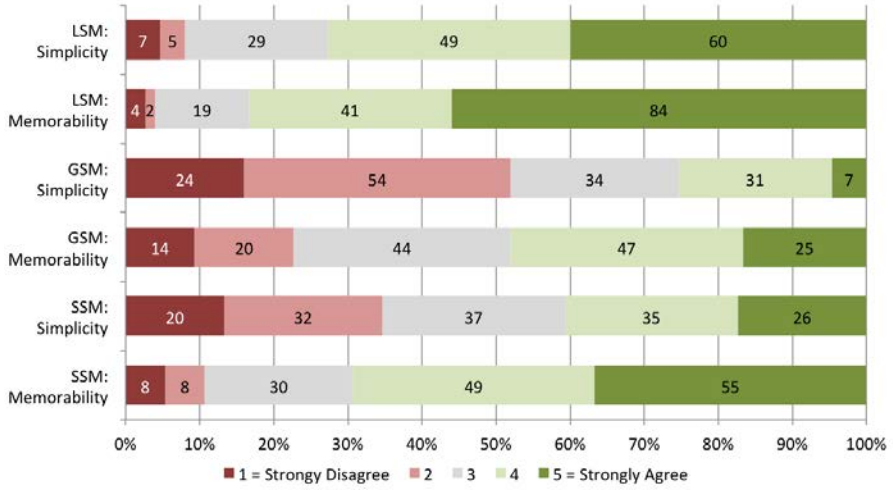
6.6 Lab Study

6.6.1 Motivation

With the online study we gained first usability results of our initial choice of visualizations and switching mechanisms. It helped us to define a manageable subset for a lab study, in which the methods could now be evaluated based on hands-on experiments. We excluded *GSM*, as this was the significantly worst rated switching mechanism. Instead, we introduced *HSM* as new condition (which was not part of the previous study since it would have been difficult to evaluate online). For visualizations, we added *HWV* and instead dropped *CBV*. First, *CBV* received a rather poor rating and, second, *HWV* shares the idea of continuity (going around the whole screen) with *CBV*, so that we



(a) Online Study: Evaluation of Zone Visualizations



(b) Online Study: Evaluation of Switching Mechanisms

Fig. 6: Evaluations of zone visualizations and switching mechanisms in the online study. [best viewed in color]

considered *HWV* as improved replacement of *CBV*, using the feedback from the pilot study.

6.6.2 Participants

30 volunteers took part in the study. 9 were female, 21 male; the average age was 33 years ($\sigma = 10.3$). All participants except one were right-handed.

A multitude of professions was covered by the participants (e.g. gardener, researcher...). However, the minority of them was familiar with compartmentalization concepts like BlackBerry Zone (1/30) or Android multi-user functionality (3/30). This also accounts for unbiasedness towards the presented experiment.

6.6.3 Task and Measurements

Subjects performed a task according to the scenario described in the beginning of the *Evaluation* section. The task consisted in launching three applications, each in a different zone (the business email app in the *Managed* zone, the home banking app in the *Secure* zone, and a game in the *Open* zone). It was up to participants to decide which was the right zone for each task. Each participant performed the task three times, each time with a different of the following switching mechanisms: Swiping with three fingers (*SSM*), using a hardware switch (*HSM*), and selecting the zone from the unlock mechanism on the lock screen (*LSM*). The order of switching mechanisms was randomized to avoid learning effects.

The zone visualizations were varied in a between-subjects design. Each group used one of the following visualizations for all tasks: *CNV*, *CTV*, or *HWV*. After each task, subjects evaluated their experience in a questionnaire.

All interactions (touch events, the currently visible screen, etc.) on the device were logged with the methodology as described by Lettner et al. [22]. This did not only allow us to capture the exact time needed to complete the task, but also to detect whether subjects made errors (every deviation from the optimal path to navigate to the desired zone was considered an error).

6.7 Lab Study Results

6.7.1 Zone Visualizations

Similar to the online study, the three visualizations were rated by the dimensions look and effectiveness. A Friedman test showed a significant effect of visualizations on look ($\chi^2 = 9.92$, $p = 0.007$) and on effectiveness ($\chi^2 = 7.19$, $p = 0.03$). Post-hoc Wilcoxon tests with Bonferroni correction showed that the look of *CNV* was rated significantly better than of the other visualizations ($p < 0.05$); there was no significant difference between *HWV* and *CTV*. Further, *CNV* was significantly more effective than *CTV* ($p < 0.005$). The results are visualized in Figure 7(a).

CNV and *HWV* can thus be both considered as best options with relation to "effectiveness". However, *HWV* performs worse in the "appeal of look" category, which may have two reasons. First, the case is in early prototypic state and does not yet look as smooth as a final product. Second, some participants noted that they do not want nearby persons to see in which zone they currently are. This privacy problem could be addressed by a customizable matching of

colors and zones. A certain color would then only have a meaning to the owner of the device and not provide any information to others.

6.7.2 Switching Mechanisms

Subjects rated each switching mechanism in the dimensions memorability and simplicity of execution. There was a significant effect of switching mechanisms on memorability ($\chi^2 = 14.56$, $p < 0.001$) and simplicity ($\chi^2 = 10.05$, $p < 0.007$). Post-hoc Wilcoxon tests with Bonferroni correction showed that *HSM* was easier to memorize and simpler to perform than *LSM* ($p < 0.05$). There were no significant differences between the other methods. All answers can be seen in Figure 7(b).

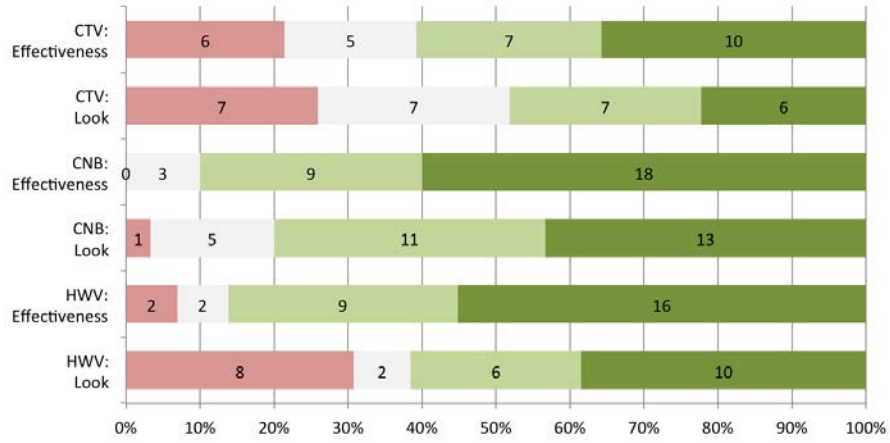
Interestingly, this result differs from the online study, where *LSM* was evaluated to be significantly simpler. This could be due to the drawback of *LSM* that the user must switch off and on the device to change zones. This additional step was probably less noticeable in the online study. The higher number of steps presumably were responsible for the fact that *LSM* received an even weaker memorability rating than *SSM*, although *SSM* requires actually more memorization (of each zone's position), which *LSM* does not.

6.7.3 Zone Switching Performance

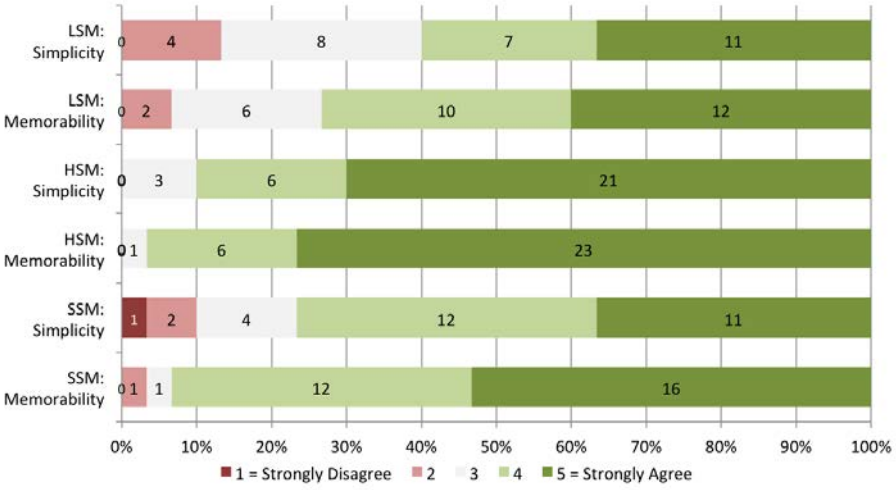
Subjects performed the zone switching task with *HSM* in averagely 38.27 s ($\sigma = 16.87$ s). The average time needed with *SSM* was 44.30 s ($\sigma = 23.88$ s), and with *LSM* it was 53.87 s ($\sigma = 29.18$ s). With one-way repeated-measure ANOVA, we found a significant effect of the switching mechanism on task time ($F(2,58) = 5.123$, $p < 0.01$, partial $\eta^2 = 0.07$). Post-hoc t-tests (with Bonferroni correction) revealed the significant difference between *HSM* and *LSM* ($p < 0.05$). The results are visualized in Figure 8a.

The error rate was lowest with *LSM* with averagely 0.77 errors ($\sigma = 1.10$), followed by *HSM* with averagely 1.10 errors ($\sigma = 0.99$), and by *SSM* with averagely 2.07 errors ($\sigma = 1.91$). A one-way repeated-measure ANOVA showed a significant effect of the switching mechanism on errors ($F(2,58) = 3.194$, $p < 0.01$, partial $\eta^2 = 0.14$). Post-hoc t-tests (with Bonferroni correction) revealed that the error number was significantly higher in *SSM* than in *HSM* ($p < 0.05$) and *LSM* ($p < 0.001$). The results are shown in Figure 8b.

The measurements show a clear advantage for *HSM*, in comparison to software-based methods regarding the switching time. While *LSM* showed similarly little errors compared to *HSM*, it was clearly the slowest method, as the display always had to be switched off and on again to get into the lock screen. The greatest drawback of *SSM* was its high error rate, which supports our proposition that a hardware-based solution is the best alternative both in terms of speed and errors.



(a) Laboratory Study: Evaluation of Zone Visualizations

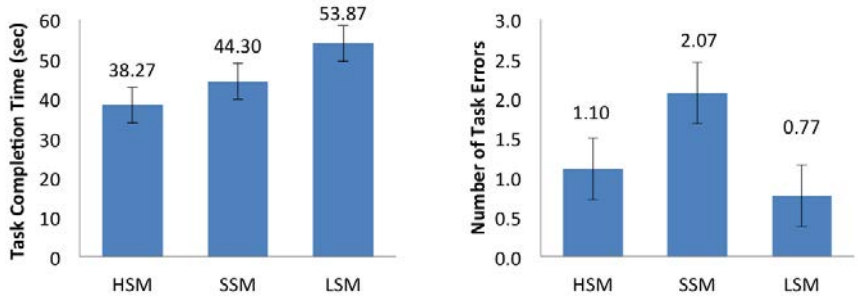


(b) Laboratory Study: Evaluation of Switching Mechanisms

Fig. 7: Evaluations of zone visualizations and switching mechanisms in the lab study. [best viewed in color]

7 Discussion

Objective and subjective measurements showed that different visualizations and switching mechanisms yield significant usability differences. In line with our argumentation that security concepts must be usable to be accepted and applied by users, we intend to give recommendations towards achieving this goal with our findings. In the following, we summarize and discuss the most significant lessons learned.



(a) Task completion times (b) Task errors

Fig. 8: Measurements of task completion time and errors for the zone switching task, Comparing Hardware (*HSM*), Swipe (*SSM*) and Lock screen (*LSM*) switching mechanisms. The error bars indicate the standard error. [best viewed in color]

Color (*CTV* and *HWV*) was more popular than text (*CTV*) to visualize the current zone, suggesting that the attention shift required for *CTV* was problematic. Thus, we suggest to use (at least an additional) color-coding for visualizing the zone. A hardware solution has, in addition, the advantage that it is harder to manipulate and also visible for full-screen apps.

For switching between zones, complex gestures (*GSM*) turned out to be too complicated. While multi-finger swiping (*SSM*) was easier, the risk of interference with other gestures was still given. The lock screen mechanism (*LSM*) was an all-discipline "winner" in theory (i.e., in the online study), but turned out as the slowest method in the lab study. A clear favourite was the hardware switch (*HSM*), which was both intuitive and fast. It is, however, only applicable for a small number of zones. While we argued that for most cases such a small number will suffice, this could still be a drawback for more complex scenarios. The software-based switching mechanisms support (through adaptation) more zones.

For multi-user device sharing, a future challenge will be how to switch between user accounts and zones (e.g., the question whether selecting the user or the zone first). A possible solution could be to implement user switching via the lock screen (as, e.g., in current Android versions) and combine this with a hardware switch for the zones.

8 Conclusion

The presented work discusses the concept of security zones in terms of zone visualization and inter-zone switching. Security zones allow to introduce an intermediate layer of compartmentalization to mobile interaction which allows the user to act within distinct semantic contexts in order to account for different security and privacy needs. As two key requirements we identify the

induction of the users' awareness of which zone they are currently acting in, and the provision of a mechanism that enables to actively switch amongst zones.

We presented an evaluation of four visualization types and four switching mechanisms staged into pilot, online and lab study. Our results imply that additional hardware can provide usable zone awareness and switching, and is thus a promising candidate for further investigations.

Future work could include refinements of the presented concepts above, and adapting them to more scenarios. One challenge is the integration of security zones with multiple user accounts and a thorough investigation of related questions (e.g., if then several open zones would exist). Furthermore, as we have argued for the benefits of hardware modifications, we plan to combine the presented hardware-based switching mechanisms and visualizations with hardware-level security (e.g. TPM). We will also investigate the effectiveness of zone visualizations with relation to attacks, i.e., how well users can detect when frauds try to mislead them by mimicking a different zone.

References

1. Adams, F.M., Osgood, C.E.: A Cross-Cultural Study of the Affective Meanings of Color. Cross-Cultural Psychology pp. 135–156 (1973). DOI 10.1177/002202217300400201. URL http://jcc.sagepub.com/content/4/2/135.abstract
2. Albrechtsen, E.: A Qualitative Study of Users' View on Information Security. Comput Secur pp. 276–289 (2007). DOI 10.1016/j.cose.2006.11.004. URL http://www.sciencedirect.com/science/article/pii/S0167404806002033
3. Becher, M., Freiling, F., Hoffmann, J., Holz, T., Uellenbeck, S., Wolf, C.: Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices. In: IEEE Symp. on Security and Privacy, pp. 96–111 (2011). DOI 10.1109/SP.2011.29
4. Blickenstorfer, C.H.: Graffiti: Wow! Pen Computing Magazine **1**, 30–31 (1995)
5. Bornstein, M.H.: Color Vision and Color Naming: A Psychophysiological Hypothesis of Cultural Difference. Psychol. Bull. pp. 257–85 (1973). URL http://www.biomedsearch.com/nih/Color-vision-color-naming-psychophysiological/4742311.html
6. Bragdon, A., Nelson, E., Li, Y., Hinckley, K.: Experimental Analysis of Touch-Screen Gesture Designs in Mobile Environments. In: Proc. CHI, pp. 403–412. ACM (2011). DOI 10.1145/1978942.1979000. URL http://doi.acm.org/10.1145/1978942.1979000
7. Brakensiek, J., Dröge, A., Botteck, M., Härtig, H., Lackorzynski, A.: Virtualization as an Enabler for Security in Mobile Devices. In: Proc. IIES, pp. 17–22. ACM (2008). DOI 10.1145/1435458.1435462. URL http://doi.acm.org/10.1145/1435458.1435462
8. Bugiel, S., Davi, L., Dmitrienko, A., Heuser, S., Sadeghi, A.R., Shastry, B.: Practical and Lightweight Domain Isolation on Android. In: Proc. SPSM'11, pp. 51–62. ACM (2011). DOI 10.1145/2046614.2046624. URL http://doi.acm.org/10.1145/2046614.2046624
9. Cisco: Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012–2017. Tech. rep. (2013)
10. Davi, L., Dmitrienko, A., Sadeghi, A.R., Winandy, M.: Privilege Escalation Attacks on Android. In: Proc. ICS, pp. 346–360. Springer (2011). URL http://dl.acm.org/citation.cfm?id=1949317.1949356
11. De Luca, A., von Zezschwitz, E., Nguyen, N.D.H., Maurer, M.E., Rubegni, E., Scipioni, M.P., Langheinrich, M.: Back-of-Device Authentication on Smartphones. In: Proc. CHI, pp. 2389–2398. ACM (2013). DOI 10.1145/2470654.2481330. URL http://doi.acm.org/10.1145/2470654.2481330
12. Dhamija, R., Tygar, J.D.: The Battle Against Phishing: Dynamic Security Skins. In: Proc. SOUPS, pp. 77–88. ACM (2005). DOI 10.1145/1073001.1073009. URL http://doi.acm.org/10.1145/1073001.1073009

13. Egners, A., Marschollek, B., Meyer, U.: Hackers in Your Pocket: A Survey of Smartphone Security Across Platforms. Tech. rep. (2012). URL http://itsec.rwth-aachen.de/publications/ae_hacker_in_your_pocket.pdf
14. Egners, A., Meyer, U., Marschollek, B.: Messing with Android's Permission Model. In: Proc. TrustCom, pp. 505–514. IEEE (2012). DOI 10.1109/TrustCom.2012.203. URL http://dx.doi.org/10.1109/TrustCom.2012.203
15. Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E., Wagner, D.: Android Permissions: User Attention, Comprehension, and Behavior. In: Proc. SOUPS, pp. 3:1–3:14. ACM (2012). DOI 10.1145/2335356.2335360. URL http://doi.acm.org/10.1145/2335356.2335360
16. Feske, N., Helmuth, C.: A Nitpicker's Guide to a Minimal-Complexity Secure GUI. In: Proc. ACSAC, pp. 85–94 (2005)
17. Höbarth, S., Mayrhofer, R.: A Framework for On-Device Privilege Escalation Exploit Execution on Android. In: Proc. IWSSI/SPMU, pp. 1–6 (2011)
18. Huang, D.L., Rau, P.L., Salvendy, G.: A Survey of Factors Influencing People's Perception of Information Security. In: Human-Computer Interaction: Applications and Services, LNCS, pp. 906–915. Springer (2007). DOI 10.1007/978-3-540-73111-5_100. URL http://dx.doi.org/10.1007/978-3-540-73111-5_100
19. Hwang, J.Y., Suh, S.B., Heo, S.K., Park, C.J., Ryu, J.M., Park, S.Y.: Xen on Arm: System Virtuali- zation Using Xen Hypervisor for ARM-based Secure Mobile Phones. In: Proc. CCNC, pp. 257–261. IEEE (2008). DOI 10.1109/ccnc08.2007.64
20. Karlson, A.K., Brush, A.B., Schechter, S.: Can I borrow your Phone?: Understanding Concerns when Sharing Mobile Phones. In: Proc. CHI, pp. 1647–1650. ACM (2009). DOI 10.1145/1518701.1518953. URL http://doi.acm.org/10.1145/1518701.1518953
21. Kranz, M., Murmann, L., Michahelles, F.: Research in the Large: Challenges for Large-Scale Mobile Application Research – A Case Study about NFC Adoption using Gamification via an App Store. IJMHCI **5**(1), 45–61 (2013). DOI 10.4018/jmhci.2013010103. URL http://www.igi-global.com/article/research-large-challenges-large-scale/76334
22. Lettner, F., Holzmann, C.: Automated and Unsupervised User Interaction Logging as Basis for Usability Evaluation of Mobile Applications. In: Proc. MOMM, pp. 118–127. ACM (2012). DOI 10.1145/2428955.2428983. URL http://doi.acm.org/10.1145/2428955.2428983
23. Luo, X.R., Brody, R., Seazzu, A.F., Burd, S.D.: Social engineering: The neglected human factor for information security management. IRMJ **24**(3), 1–8 (2011). DOI 10.4018/irmj.2011070101. URL http://dx.doi.org/10.4018/irmj.2011070101
24. Maurer, M.E., De Luca, A., Stockinger, T.: Shining Chrome: Using Web Browser Personas to Enhance SSL Certificate Visualization. In: Proc. INTERACT, LNCS, pp. 44–51. Springer (2011). DOI 10.1007/978-3-642-23768-3_4. URL http://dx.doi.org/10.1007/978-3-642-23768-3_4
25. Mayrhofer, R.: When Users Cannot Verify Digital Signatures: On the Difficulties of Securing Mobile Devices. In: Proc. TSP. IEEE (2013)
26. Möller, A., Michahelles, F., Diewald, S., Roalter, L., Kranz, M.: Update Behavior in App Markets and Security Implications: A Case Study in Google Play. In: B. Poppinga (ed.) Proceedings of the 3rd International Workshop on Research in the Large. Held in Conjunction with Mobile HCI, pp. 3–6 (2012)
27. Polla, M.L., Martinelli, F., Sgandurra, D.: A Survey on Security for Mobile Devices. IEEE Communications Surveys & Tutorials pp. 446–471 (2013). DOI 10.1109/SURV.2012.013012.00028
28. Riedl, P., Koller, P., Mayrhofer, R., Möller, A., Koelle, M., Kranz, M.: Visualizations and switching mechanisms for security zones. In: Proceedings of International Conference on Advances in Mobile Computing & Multimedia, MoMM '13, pp. 278:278–278:281. ACM, New York, NY, USA (2013). DOI 10.1145/2536853.2536948. URL http://doi.acm.org/10.1145/2536853.2536948
29. Segall, M.H., Campbell, D.T., Herskovits, M.J.: The Influence of Culture on Visual Perception. Bobbs- Merrill (1966)
30. Seifert, J., De Luca, A., Conradi, B., Hussmann, H.: TreasurePhone: Context-Sensitive User Data Protection on Mobile Phones. In: Proc. Pervasive, LNCS, pp. 130–137. Springer (2010). DOI 10.1007/978-3-642-12654-3_8

31. Stajano, F.: One User, Many Hats; and, Sometimes, No Hat: Towards a Secure yet Usable PDA. In: Proc. SP, pp. 51–64. Springer (2006). DOI 10.1007/11861386_6. URL http://dx.doi.org/10.1007/11861386_6
32. Stoll, J., Tashman, C.S., Edwards, W.K., Spafford, K.: Sesame: Informing User Security Decisions with System Visualization. In: Proc. CHI, pp. 1045–1054. ACM (2008). DOI 10.1145/1357054.1357217. URL http://doi.acm.org/10.1145/1357054.1357217
33. Wald, G., Brown, P.K.: Human Color Vision and Color Blindness. In: Cold Spring Harbor Symp. on Quantitative Biology, vol. 30, pp. 345–361 (1965)
34. Wolf, K., McGee-Lennon, M.R., Brewster, S.A.: A Study of On-Device Gestures. In: Proc. Mobile HCI (Companion), pp. 11–16 (2012). DOI 10.1145/2371664.2371669