# Short Paper: Smartphones: Not Smart Enough?

Ian Fischer
University of California, Berkeley
ian.fischer@berkeley.edu

Cynthia Kuo
Nokia Research Center, Palo Alto
cynthia.kuo@nokia.com

Ling Huang
Intel Labs, Berkeley
ling.huang@intel.com

Mario Frank
University of California, Berkeley
mfrank@berkeley.edu

## ABSTRACT

Today's mobile devices are packed with sensors that are capable of gathering rich contextual information, such as location, wireless device signatures, ambient noise, and photographs. This paper exhorts the security community to re-design authentication mechanisms for users on mobile devices. Instead of relying on one simplistic, worst-case threat model, we should use contextual information to develop more nuanced models that assess the risk level of the user's current environment. This would allow us to decrease or eliminate the level of user interaction required to authenticate in some situations, improving usability without any effective impact on security. Ideally, authentication mechanisms will scale up or down to match users' own mental threat models of their environments. We sketch out several scenarios demonstrating how contextual information can be used to assess risks and adapt authentication mechanisms. This is a research-rich area, and we outline future research directions for developing and evaluating dynamic security mechanisms using contextual information.

## Categories and Subject Descriptors

H.1 [**Models and Principles**]: User/Machine Systems

## General Terms

Human Factors, Security

## Keywords

Mobile Security, Usability, Context, Presence

## 1. INTRODUCTION

Chances are that you carry a smartphone. Smartphones now account for half of all mobile phones in the U.S. [21]. Among U.S. users aged 25–34, smartphones account for almost two-thirds of mobile phones [20]. Smartphones are so useful that one-quarter of users say that they mainly use their smartphone to go online [16].

The unique property and usage pattern make mobile devices subject to specific threats that are different from desktop machines.

First, mobile devices often store and access many types of sensitive data and services, including personal photos, email, text messages, GPS traces, social media feeds, bank accounts, and corporate infrastructure. Always-on access to services makes it easy for attackers to leverage one account to gain access to another; for example, an attacker that gains physical possession of a device can request a password reset for one service, which sends a reset message to an email account on the device. Second, users carry and use mobile devices everywhere. These small devices are easily lost, forgotten, or stolen. In many major U.S. cities, over 40% of users have lost their cell phones or been victims of cell phone theft [10].

However, industry surveys estimate that between 38% and 70% of smartphone users do not even lock their phones with passwords or PINs [13, 11, 17]. Why do users prefer insecure access on devices that are both sensitive and prone to theft? One explanation is that entering passwords and PINs on virtual keyboards is time-consuming, cumbersome, and error-prone. Another explanation is that users do not believe that extra passwords or PINs are needed.

Users' reluctance to use authentication on their devices may be rational. Herley points out that user effort is not free, and users may be estimating their risks better than security professionals. In fact, ignoring today's security advice may be perfectly reasonable in light of the actual harm wrought by weak passwords [6]. Wimberly and Liebrock show that users implicitly assess their level of risk and adjust their actions accordingly [22]. Both studies suggest that users intuitively create their own subjective threat models. For example, someone who keeps his phone on his person at all times could rationally decide that a screenlock is generally unnecessary. However, he may also recognize that in some situations he would prefer to have stronger authentication. Modern authentication mechanisms do not support dynamic scaling of security, so users may default to the simpler option.

Below, we highlight three major shifts in technology that should change the way we think about mobile device security: mobility, sensors, and constant connectivity.

**Mobility.** Mobility creates uncertainty about the environmental conditions surrounding a mobile device. Devices may


*SPSM'12,* October 19, 2012, Raleigh, North Carolina, USA.

be used in secure environments, such as homes or offices, or in public spaces, such as airports and coffee shops. The variety of environments exposes mobile devices to a large pool of potential attackers: everyone from friends and family members to total strangers. Traditionally, security mechanisms have been designed to resist attacks in a one-size-fits-all, worst case scenario. Unfortunately, strong passwords and their equivalents impair the usability of mobile devices and apps. Users need a flexible solution that adapts to their current situation.

**Sensors.** Today's mobile devices are equipped with a variety of sensors, including GPS, accelerometers, gyroscopes, magnetometers, proximity sensors, microphones, cameras, and radio (cellular, Bluetooth, Wi-Fi, RFID, NFC) antennas. These sensors fueled an explosion of new applications tailored for mobile devices.

Researchers are exploring the application of sensor data to security. Greenstadt and Beal advocate fusing multiple low-fidelity streams of sensor data to perform biometric recognition and to track user presence [3]. Jakobsson et al. implicitly authenticate users by comparing users' recent behavior to personalized models of past behaviors [7]. Smartphone accelerometers have been used for biometric gait authentication [2] and GPS for location-based authentication [19].

Most existing research focuses on user authentication, but sensor data is useful for more than binary authentication decisions. Contextual cues can be used to scale the security behavior of devices and applications. For example, Gupta et al. dynamically adapt the locking timeout and unlock mechanism for smartphone screenlocks based on location familiarity [4]. In concurrent, independent research with this paper, Qin et al. propose a progressive authentication system that combines multiple sensor signals to determine the confidence level in a user's authentication. The system uses this confidence level to decide when to request authentication and for which applications, thus reducing the number of times a user has to authenticate [12].

**Constant connectivity.** Mobile devices have constant access to the Internet and other devices. Constant connectivity allows devices to offload some security-relevant computations to remote servers or other machines. Aggregating sensor data across devices also enables the development of fine-grained contextual models [15, 9].

# 2. SENSING THE OPPORTUNITY

The accepted way to design a security system is to create a threat model and formulate a solution that addresses the prioritized threats in the model. Swiderski and Snyder outline a methodical process in their book [18]. Similarly, Gutmann proposes using problem-structuring methods (PSMs) to consider the social, environmental, and political aspects of computer security challenges [5].

However, intangible and physical world factors are difficult to model. As a result, a large body of academic work sidesteps the issue and often assumes the worst case. The usability of security suffers as a result, particularly on mobile devices.

Sensors enable us to gather information about the context surrounding mobile device use. With contextual information, we can form situation-dependent threat models. Transitioning from one static threat model to many contextual threat models allows us to dynamically adapt security mechanisms to the situation. Devices and apps could remove or reduce explicit authentication mechanisms in safer environments and increase them in riskier situations. The goal of such a dynamic authentication system is to improve usability with little effective reduction of security for mobile devices.

Since we are concerned with physical authentication mechanisms, threats related to malware, worms, phishing, and social engineering attacks are out-of-scope.

# 3. USING CONTEXT INFORMATION

Below, we illustrate how context information may be used to subtly alter authentication mechanisms in high and low risk environments. The scenarios are described at a high level; Section 4 discusses the technologies that can support these interactions.

## 3.1 High Risk Scenario

Alice is waiting for her flight. She pulls out her smartphone to pay a bill that is due during her trip. She enters her PIN to unlock her phone.

She then opens her mobile banking app, which takes her photo and asks her to enter her bank password. After login, the app displays a limited interface that allows her to check her balance, pay bills to existing payees, and find nearby banks and ATMs. Because the airport is a high risk environment, some transactions are disabled and a photo is required.

With time before her flight, Alice browses the stores in the terminal. She decides to buy an expensive gift using her e-wallet app. The app shows her the total and prompts her to enter her PIN. As an additional security measure, the app takes her photo, and the cashier's terminal displays Alice's profile photo from the e-wallet provider. The cashier acknowledges that the Alice standing in front of him is the same person as the Alice in the picture.

After boarding the plane, Alice uses her Amazon app to purchase an item that she forgot to pack. Alice enters her password and re-enters her credit card verification code before adding her hotel's address for shipping and completing the purchase.

## 3.2 Low Risk Scenario

Bob is shopping in his favorite clothing store. He pulls his smartphone out. As he moves the phone towards his face, it recognizes him and unlocks the screen.

Bob opens his mobile shopping app and uses it to take a picture of a barcode on a jacket that caught his eye. The app informs him that the same jacket is available online in a variety of colors for less. He selects the color and size he wants and purchases it using his default credit card and shipping address. The store is a common destination for him, so Bob's password is not required to check out. Instead, he answers a multiple choice question about his last purchase at the store; answering the question is a breeze compared to entering his password.

Before leaving the store, he notices a scarf that he would like to wear that evening. He brings the scarf to the counter and moves his phone towards the payment point. His phone displays the total amount, and he clicks the "Purchase" button to complete the transaction. Bob's PIN is not required because the relatively low amount is transferred to a known store.

At home, Bob pulls out his tablet, which automatically recognizes him and unlocks the screen. He opens his mobile banking app and selects "Add a New Payee." The app takes his photo and compares the photo and his location to his existing profile. A moment later, Bob is able to add his cable provider to his list of payees without entering his long bank password.

# 4. APPLICATIONS OF CONTEXT

In the previous section, we described how device context enables the dynamic scaling of security requirements. Below, we examine the four examples in more depth.

## 4.1 Device Unlock

Screenlocks are a ubiquitous feature on every PC, tablet, and smartphone in the market today. A screenlock hides what the user was last viewing and prevents the device from responding to input. It activates after a predetermined amount of idle time, or when a user engages it.

We assume that a user needs to gain physical access to unlock a mobile device. After unlocking, she can immediately access some information, such as personal contacts, calendar, emails, and text messages, and some functionality, such as making phone calls and sending email. However, she may not have access to critical applications that are protected by additional layers of security, such as password input.

On smartphones, screenlocks are often deactivated using numeric PINs, secret gestures, or dots that need to be connected into a pattern. Contextual information can be leveraged to adapt unlock mechanisms for the user's current situation, scaling authentication requirements between high risk and low risk scenarios.

**High risk.** In Section 3.1, when the accelerometer detects that Alice is moving the phone towards her face [1], the camera captures a series of images and performs facial recognition to determine whether she is the authorized user on this device. At the same time, the Wi-Fi radio checks to see if it recognizes any nearby wireless access points, and the Bluetooth radio checks to see if it recognizes any nearby devices. Visible Wi-Fi networks and Bluetooth beacons can be used to determine the user's location, map the location to public spaces or the user's personal points of interest, and assess the level of foot traffic in the vicinity. Microphone information can also be used to identify crowded public spaces.

Public, crowded, or unknown spaces may be classified as risky. In risky situations, Alice's smartphone authenticates her with both her PIN and a biometric identifier. Identifiers could include her face, patterns of movement, or the manner in which she interacts with the screen. In this scenario, the smartphone performs face recognition automatically using the front-facing camera, without explicit action from Alice.

**Low risk.** If Bob is in a known and familiar location, or Bob's mobile device has tracked his constant presence (through cameras and other sensors) since entering a PIN, it unlocks by simply recognizing Bob's face when he makes a motion of intent. If someone else attempts to unlock Bob's device, the front-facing camera takes a photo and alerts Bob the next time he picks up the device.

[1]We consider Alice moving the phone towards her face to be a *motion of intent*. Discriminating motions of intent from incidental motions should be a straightforward classification task.

**Discussion.** The numeric PIN commonly used today on smartphones is the worst of both worlds: too weak to resist attackers when the user loses control of the device, and too strong for convenient use in daily routines.

For many mobile device users, a combination of facial recognition, presence tracking, and an audit trail of unlock photos will restrain acquaintances. Scaling down unlock to forgo PIN entry can still provide sufficient protection against data exposure or device tampering while increasing ease of use.

In contrast, high risk spaces require more assurances. Combining a PIN with face recognition or another biometric identification increases the level of security.

## 4.2 Mobile Shopping Application

For consumers accustomed to comparing prices and perusing online reviews, shopping on mobile devices is a natural extension. Anecdotally, mobile online shoppers fall into one or more of the following categories.

- Users adopting mobile devices as PC replacements at home or in the office. These users gravitate towards the native apps (e.g., Amazon or Zappos) to read reviews and purchase items.
- Users comparing the online price of an in-store item.
- Users using online reviews to make a purchasing decision at the store.
- Users completing "errands" on the mobile device while on the go.

With such a wide array of uses, mobile shopping applications could easily benefit from contextual information. Below, we assume that any shopping application will ask users to authorize purchases with their login passwords or context-supported mechanisms.

**High risk.** A high risk shopping transaction is characterized by novelty: a new shipping address, an usually expensive purchase, or a new location. Making purchases in a new location or sending purchases to a new address could be an indicator of device theft, so the app requires stronger authentication. Defaulting to the established checkout procedure for web applications, such as entering an alphanumeric password and credit card verification code, makes sense to both Alice and the online shop.

**Low risk.** As Bob peruses his favorite local shop, the mobile application tries to match his current location with his location history of previous transactions, or with his existing shipping or billing addresses. The app also performs face recognition using images from the front-facing camera. These activities can take place in the background, establishing a high probability that the shopper is indeed Bob.

In addition to probabilistically identifying Bob, the app considers his purchase data; for example, the item is shipped to Bob's existing shipping address, is below a price threshold, and fits his purchase history profile. This combination of factors categorizes the purchase as low risk. For low risk transactions, the app could ask a simple multiple-choice question based on Bob's purchase history, such as, "Last month, did you buy the (a) Hunger Games Trilogy, (b) Kindle Fire, or (c) Panasonic DMC-FH25K 16.1MP Digital Camera?"

**Discussion.** Using context data, the online store streamlines its purchase flow—requiring only one touch instead of a long alphanumeric password—without risking a significant increase in fraudulent activity.

## 4.3 E-Wallet

In many parts of the world, merchants and individuals are using and accepting mobile phones to exchange currency. In particular, phones can be used:

- As a debit card or credit card. A service such as Google Wallet enables customers to transfer money to their Google Wallet accounts or to associate credit cards with their accounts. The user can then pay at supporting merchants.
- As a mobile bank account. Service providers such as M-PESA [14] and Celpay [1] enable users to deposit money into their accounts and transfer money out.

This turns mobile phones into sophisticated wallets and, similar to old-fashioned wallets, attractive targets for fraud. Google Wallet requires that the user, in addition to unlocking the phone, enter a dedicated PIN and tap the phone on a reader to enable reading the payment information from a dedicated chip in the phone. Similarly, money transfer services require a password to carry out transactions. Cashing money from a mobile bank account requires a valid ID that is checked at the service point.

**High risk.** High risk transactions may involve large amounts of money, historically anomalous purchases, or money transfers to new recipients. In high risk situations, the mobile device can take a picture during a credit/debit transaction and compare it with a photo taken during account enrollment. This implements an additional verification step that is completely transparent to the user. Alternatively, if a camera is unavailable on the mobile device or the photo is unusable, a human comparison is effective. The remote server can send Alice's photo to the other party in the transaction and ask the other party to confirm her identity.

As e-wallet users tend to send money to the same receivers—most transactions are directed home to family members—the service provider can establish a social network in which nodes are connected whenever money is sent between them. If Alice sends money to an unknown receiver, the device could request that the receiver take a picture of his face, which the system sends back to Alice.

**Low risk.** Reducing security requirements for low risk transactions requires a strict set of security policies. For example, when Bob attempts to make a purchase at a payment point, the system queries a server to determine the level of authentication required for the account holder at that particular payment point. If Bob has made a number of purchases at that location, has logged into his phone recently, was matched to his profile photo in the background, and his current purchase is less than a predetermined threshold, a lower level of authentication is required. Bob can complete his purchase without his PIN.

**Discussion.** Careful risk modeling using the contextual data provided by mobile devices can allow e-wallet providers to improve the usability of their service, which may increase adoption. Since e-wallet technology often relies on trusted hardware to store keying material, cryptographic protocols will need to be developed that allow re-keying using contextual data. This may include using an identifier stored in the merchant's e-wallet reader, for example.

## 4.4 Mobile Banking

In Sections 3.1 and 3.2, the banking app on Alice's phone and Bob's tablet performs the same contextual queries. The app uses location cues from the mobile device, such as GPS, Wi-Fi networks, and Bluetooth devices, to determine if Alice and Bob are in familiar locations, such as known home addresses.

**High risk.** While Alice is in an airport, the app categorizes her environment as high risk and prompts her for both her banking password and a photo. Even with two-factor authentication, the app restricts what activities are available to Alice and how long she has to interact with the app before she has to reauthenticate. After all, Alice's phone could be stolen before its screenlock engages or Alice locks the device. If Alice wants to perform more sensitive operations, such as adding a new payee, she will need to move to a safer environment.

**Low risk.** The mobile banking app on Bob's tablet has high security requirements. The app will not query a remote location API to determine Bob's location and fetch a history of recent authentication attempts like the mobile shopping app. Instead, the bank app only uses the context information that is available directly from the device sensors. It reports Bob's approximate location and details of the Wi-Fi and Bluetooth environment to the bank's servers over a secure channel. The server incorporates that information into its risk profile. When Bob selects "Add a New Payee", the app explicitly photographs his face and informs him the photograph will be uploaded to the bank's servers as part of the transaction record. In addition to acting as a biometric authentication, the photograph reduces the risk of *friendly fraud* [8] and reassures Bob that the bank takes his security seriously.

Since the location matches his home address and the photo matches Bob's face, many banking actions are available without entering a password. However, a password or a secret spoken passphrase is still necessary to perform sensitive transactions, such as unusual or large money transfers.

**Discussion.** In general, all available contextual information could be sent to the bank during mobile banking transactions. This is feasible as mobile banking requires a network connection to be useful. Consequently, the device is able to offload the security computations to the bank's servers. That data can be fed into the bank's risk analysis engine, allowing the bank to have much more sophisticated models. This improved modeling also benefits the user, since she is less likely to be victimized. However, she may have valid privacy concerns about sharing such data with the bank.

# 5. PRIVACY

In our context-aware authentication paradigm, multiple sensors collect multifaceted data about the device, user, and environment. This data collection may concern some users. Careful system design can assuage most of these concerns.

**Device unlock.** For device unlock, all of the collected data is processed on the phone, and much of the data is transient. In the absence of malware, the only privacy concerns are due to physical compromise of the device. The device can encrypt sensitive data when it is stored. In order to use that data during the unlock procedure, the decryption key would need to be stored in memory. If the key can be generated from the user's normal passphrase, it can be deleted during any unlock procedure where the device thinks a new authentication is necessary.

The system can offer this authentication-secured storage as a service to other applications as well, so that any application with sensitive data, such as the applications we discuss

in this paper, can tie access to that data to the authenticated user. In this way, the user's privacy can be maintained under the threat of physical compromise.

**Mobile shopping.** The mobile shopping app can use services provided by the phone for all of its contextual authentication queries. For example, face recognition can be provided as a service, and does not require direct access to the camera, or even that the shopping app have a previous photo of the user. It only requires that the user registered with the device at some point, pairing the user's face with some internal identifier known to the shopping app and the device. Since the app does not have access to the user's photo, location, or other contextual data, it cannot compromise the user's privacy to the online store.

**E-wallet.** E-wallet transactions are similar to existing credit card transactions. They are sensitive and informative, and they require a set of central authorities to approve the transaction. These features mean that the e-wallet must expose more user data to third parties. However, the third-parties in question already collect much of the contextual information we propose using. For example, if a user were to purchase something with a credit card, the credit card company would immediately know the amount of the purchase, the location of the purchase, and the business name of the merchant. The only new set of data in use is the user's photo. Sending the photo to the merchant does not violate the user's privacy, since she is present with the merchant. Sending the photo to the e-wallet provider may be more sensitive. This topic deserves further user study.

**Mobile banking.** As with the e-wallet case, banks already collect much of the contextual data in question during traditional interactions, such as at an ATM or at home on a computer. Banks can mitigate privacy concerns by marketing the use of contextual data as a service to increase user's security. Of course, marketing is not sufficient to prove that the user's privacy has not been violated. Careful regulation of banks' privacy policies and data usage can mitigate the risk of abuse.

# 6. FUTURE RESEARCH AGENDA

Moving forward, a diverse mix of research topics need to be addressed for contextual threat modeling and the adaptation of security mechanisms to be successful. We highlight a few below.

**Understand how mobile device users construct a mental threat model in a variety of contexts.** Mobile device users will adopt contextual security mechanisms if they match users' expectations. The security community needs to understand users' own mental threat models through a mix of lab experiments and ethnographic study. For example, how do users' perceived threats change as they move from a trusted private space to a public space? Do users believe that unlock mechanisms or application-specific passwords are always necessary in private spaces?

**Incorporate physical world factors into contextual threat models.** We need methods for interpreting sensor data to create contextual threat models on mobile devices. Research is already moving in this direction [4] using location, but how else can the sensor data be used? New sensors, or new uses of existing sensors, may need to be developed. For example, an approach based on ultrasound sensors and machine learning techniques can be developed for detecting and differentiating humans within a small radius, which would enable a mobile device to model human traffic.

Also, context information can enable researchers to include physical security in system or application threat models. For example, if we can assess how a secure location reduces risk, we might consider a secure location and weak password equivalent to a strong password.

**Study the usability of adaptive security mechanisms.** One danger of dynamically adapting security mechanisms is that users may become confused. User studies will determine whether users accept different levels of security. Is inconsistency confusing to end users? Do problems arise because the system's behavior fails to match users' mental models, or because consistency—even if it entails more work for the user—lowers cognitive burden and is more acceptable?

**Address privacy concerns.** The collection and dissemination of sensor data raises serious privacy issues. Exposure may result from taking physical possession of the device, malware that steals information stored locally on the device, or organizations that gather and store sensitive, personally identifiable data. Researchers should carefully consider how to minimize data collection and aggregate any data that is stored.

**Optimize implementation for real-world use.** To facilitate adoption, adaptive security mechanisms must respond quickly to user interactions and minimally impact system resources. Environment sensing and context model construction, especially those involving sophisticated pattern recognition on high-data rate sensors such as a camera, or just using GPS, consume significant energy and can be slow. Mobile device users do not tolerate large reductions in battery life or delays in logging in. Selecting which sensors to collect data from and deciding where to do the context analysis (on-device vs. remote servers) to minimize energy consumption and latency while satisfying fidelity requirements are challenging research problems.

**Develop methods for evaluating the quality of contextual threat models and adaptive security mechanisms.** Like every research problem, an evaluation metric is necessary. How can a system judge the applicability of a contextual threat model to a person in a particular location at a given time? How do we assess whether a system scaled the security mechanisms appropriately for the environment? Answering these questions may require a mix of user studies and machine learning to incorporate user feedback.

**Develop cryptographic protocols to support dynamic keying.** Some current e-wallet apps use a Trusted Platform Module to store keys that decrypt data needed to complete a transaction. The keys themselves are encrypted using the user's PIN. In order to support purchases that do not require the PIN, we will need new protocols that allow the user to generate new keying material based off of contextual cues.

# 7. REFERENCES


[1] Celpay International BV. Celpay BV. `http://www.celpay.com/`.

[2] M. O. Derawi, C. Nickel, P. Bours, and C. Busch. Unobtrusive user-authentication on mobile phones using biometric gait recognition. In *Proceedings of the 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*,

IIH-MSP '10, pages 306–311, Washington, DC, USA, 2010. IEEE Computer Society.

[3] R. Greenstadt and J. Beal. Cognitive security for personal devices. In *Proceedings of the 1st ACM workshop on Workshop on AISec*, AISec '08, pages 27–30, New York, NY, USA, 2008. ACM.

[4] A. Gupta, M. Miettinen, and N. Asokan. Intuitive security policy configuration in mobile devices using context profiling. Technical Report CERIAS 2011-13, Center for Education and Research Information Assurance and Security (CERIAS), Purdue University, 12 2011.

[5] P. Gutmann. Applying problem-structuring methods to problems in computer security. In *Proceedings of the 2011 Workshop on New Security Paradigms Workshop*, NSPW '11, pages 37–44, New York, NY, USA, 2011. ACM.

[6] C. Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 Workshop on New Security Paradigms Workshop*, NSPW '09, pages 133–144, New York, NY, USA, 2009. ACM.

[7] M. Jakobsson, E. Shi, P. Golle, and R. Chow. Implicit authentication for mobile devices. In *Proceedings of the 4th USENIX conference on Hot topics in security*, HotSec'09, pages 9–9, Berkeley, CA, USA, 2009. USENIX Association.

[8] M. Jakobsson and S. Taveau. The Case for Replacing Passwords with Biometrics. In *Mobile Security Technologies*, March 2012.

[9] A. Kapadia, S. Myers, X. Wang, and G. Fox. Secure cloud computing with brokered trusted sensor networks. In *Proceedings of The 2010 International Symposium on Collaborative Technologies and Systems (CTS 2010)*, 2010.

[10] Lookout Mobile Security's The Lookout Blog. Lost and found: The challenges of finding your lost or stolen phone. `http://blog.mylookout.com/blog/2011/07/12/`. Published July 12, 2011.

[11] Norton. Norton survey reveals one in three experience cell phone loss, theft. `http://www.symantec.com/about/news/release/article.jsp?prid=20110208_01`. Published Feb 08, 2011.

[12] C. Qin, O. Riva, K. Strauss, and D. Lymberopoulos. Progressive authentication: deciding when to authenticate on mobile phones. In *Proceedings of 21st USENIX Security Symposium*, 2012.

[13] Retrevo Blog. iPhones, backups and toilets, what's the connection? `http://www.retrevo.com/content/blog/2011/08/iphones-backups-and-toilets-connection`. Published Aug 02, 2011.

[14] Safaricom. M-PESA. `http://www.safaricom.co.ke/index.php?id=250`.

[15] M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies. The case for vm-based cloudlets in mobile computing. *IEEE Pervasive Computing*, 8(4), October 2009.

[16] A. Smith. Smartphone adoption and usage. http://pewinternet.org/Reports/2011/Smartphones.aspx. Published Jul 11, 2011.

[17] Sophos Naked Security blog. Survey says 70% don't password-protect mobiles: download free Mobile Toolkit. `http://nakedsecurity.sophos.com/2011/08/09/free-sophos-mobile-security-toolkit/`. Published Aug 9, 2011.

[18] F. Swiderski and W. Snyder. *Threat Modeling*. Microsoft Press, 2004.

[19] H. Takamizawa and N. Tanaka. Authentication system using location information on ipad or smartphone. *International Journal of Computer Theory and Engineering*, 4(2), 2012.

[20] The Nielsen Company. Generation app: 62% of mobile users 25-34 own smartphones. `http://blog.nielsen.com/nielsenwire/online_mobile/generation-app-62-of-mobile-users-25-34-own-smartphones/`. Published Nov 3, 2011.

[21] The Nielsen Company. Smartphones account for half of all mobile phones, dominate new phone purchases in the US. `http://blog.nielsen.com/nielsenwire/online_mobile/smartphones-account-for-half-of-all-mobile-phones-dominate-new-phone-purchases-in-the-us`. Published Mar 29, 2012.

[22] H. Wimberly and L. M. Liebrock. Using fingerprint authentication to reduce system security: An empirical study. In *Proceedings of the 2011 IEEE Symposium on Security and Privacy*, pages 32–46, Washington, DC, USA, 2011. IEEE Computer Society.