Secure Mobile Ad-hoc Interactions: Reasoning About Out-Of-Band (OOB) Channels

Ronald Kainda, Ivan Flechais, A.W. Roscoe
Oxford University Computing Laboratory
Wolfson Building, OX1 3QD, Oxford
{ronald.kainda, ivan.flechais, bill.roscoe}@comlab.ox.ac.uk

ABSTRACT

Previous research has proposed Human-Interactive Security Protocols (HISP) for bootstrapping security in *ad hoc* mobile device interactions. These protocols rely on low bandwidth Out-Of-Band (OOB) channels—that are suitable for transferring limited information (e.g. fingerprints of public keys) but unsuitable for transmitting cryptographic keys due to bandwidth constraints—and high bandwidth channels such as Bluetooth and WiFi. In this paper, we argue that factors that are crucial to designing OOB channels that are both usable and secure have not been understood and analysed, and propose a framework for reasoning about them in order to design OOB channels that suit human and contextual needs to achieve usable and acceptable effective security.

Categories and Subject Descriptors

H.1.2 [**Models and Principles**]: User/Machine Systems—*Human Factors*

General Terms

Security, Human Factors

Keywords

Framework, Usability, Device Association, OOB Channels

1. INTRODUCTION

Secure exchange of cryptographic keys in *ad hoc* wireless networks is challenging. This is due to lack of a Public Key Infrastructure (PKI) or trusted third party that is practical or sufficiently universal to cover all scenarios of mobile interactions [18]. To bootstrap security in *ad hoc* interactions, using a low bandwidth Out-Of-Band (OOB) channel, in addition to a high bandwidth (normal) channel has been proposed.

In this proposal, associating devices exchange public information, such as public keys, over the normal channel. Devices then independently compute a cryptographic fingerprint of all information received and sent. These fingerprints are transferred between devices via an unspoofable OOB channel to verify the authenticity of the public key(s). The security requirement on the OOB channel is integrity rather than secrecy [17]—as the property of secrecy is difficult to achieve.

Proposed protocols (e.g. [12, 17]) rely on users to transfer (or compare) fingerprints between participating devices. We call these protocols *Human-Interactive Security Protocols* (HISP). The length of the fingerprint depends on the level of theoretical security required. These protocols, however, are actively constrained by the fact that the level of security offered may depend on the amount of human effort expended. Users are expected to compare or transfer fingerprints accurately but this can be problematic given known problems of user attentiveness and motivation.

Attempts to minimise human effort in HISP tend to focus on user interfaces even though this alone does not improve overall usability [27]. They also focus on devices of similar capabilities such as devices with very limited input and output interfaces (e.g. single button devices [25]), or devices with reasonable input/output interfaces such as camera phones [16]. There are many scenarios where devices of differing capabilities need secure association, and these may in fact be the common ones. Examples include a Bluetooth hands free set and mobile phone, a PDA and printer or external storage media etc.

While attempts to improve usability of OOB channels cover a limited range of scenarios, they tend to take the position of finding a universal solution that covers *all* use scenarios. Focusing on a universal solution is likely to overshadow crucial factors that may only be uncovered when a specific scenario is considered before generalising to other scenarios. For example, factors such as motivation may come into play for certain scenarios and not for others. One may be motivated not to share a credit card PIN with anyone else while at the same time willing to share the password to a company computer with a colleague. Scenarios such as this, in the context of OOB channels, provide insights that may be crucial to designing usable and secure OOB channels that apply to a wide range of scenarios.

We are of the view the failure to take crucial factors into consideration is due to lack of a framework that identifies those factors and puts them into context. In this paper we propose such a framework to help both researchers and system designers in reasoning about the various factors that have an effect on the usability, security, and applicability of OOB channels. The paper is organised as follows; in Section 2 we present the framework and discuss its application in Section 3. We conclude and discuss future work in Section 4.

Second International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU)
May 17, 2010, Helsinki, Finland

2. FRAMEWORK

The framework puts factors that are crucial to designing or proposing OOB channels into a wide context in which mobile devices may operate and, hence, provide a better understanding of the social and physical elements that may pose challenges to OOB channels. Designers may use the framework to reason about their system within the context in which the system may operate and help them select, among existing methods, an OOB channel that suits their application environment, while researchers may use it to understand and reason about the different factors in order to design OOB channels.

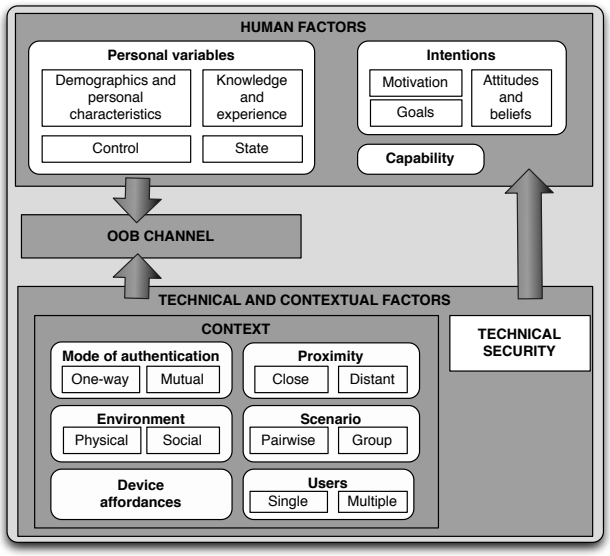

Figure 1: Framework

The framework is based on the work of Cranor [3]—*The human-in-the-loop security framework*. The human-in-the-loop framework was designed to help understand human behaviour in performing security-critical functions. While this framework provides insights into human behaviour in the wide context of security, our framework is a tool for reasoning about the different factors specific to *ad hoc* mobile device environments. It is aimed at helping in designing or choosing of OOB channels that suit both human and contextual needs without compromising security.

The framework also builds on the findings of various Human-Computer Interactions Security (HCISec) studies and a review of mobile device *ad hoc* interactions together with currently proposed OOB channels. HCISec research has revealed users' experience of varying levels of difficult when using secure systems. Specifically, studies on the usability of passwords, e.g. [20], have revealed human limitations such as attention, memory, and accuracy. While these limitations are fully understood in other contexts, significant other factors affect users in mobile environments.

The framework (Figure 1) consists of three elements: technical and contextual factors, human factors, and OOB channels. Technical and contextual factors have direct effects on OOB channels. For example, technical security (size of fingerprint) may dictate an OOB channel used. In addition, they affect users in relation to specific human factors. The type of input interface on a device, for example, is likely to affect human performance when entering text. Finally, human factors too affect what OOB channel is used. An OOB channel that requires touching devices simultaneously may be inappropriate if users are incapable of doing so because devices are distant, for example.

2.1 Technical and contextual factors

Secure systems are socio-technical—they operate in concert with other systems and are used by humans. Systems must, therefore, be secure at the technical as well as social level [8]. While computers can deal with complexity, humans face significant challenges (e.g. [21, 27] in dealing with complex systems. It is, therefore, necessary that secure systems are designed with simplicity as complexity may introduce vulnerabilities [28]. These vulnerabilities are due to either unintentional insecure user actions or difficulty-of-use which leads users to abandoning a secure system altogether and resorting to insecure methods [27].

In addition to the socio-technical elements, secure systems operate within social and environmental contexts. Context has positive and negative effects on both security and usability of a system [1]. Understanding how specific contexts affect usability and security of a system is crucial to designing systems that work in a usably secure manner across contexts.

2.1.1 Context

Secure systems, together with their users, operate within context. Context is the extension of a socio-technical system to consider factors outside the system. For example, an authentication system may operate in context with external objects such as Closed Circuit Television (CCTV) cameras, humans, computing devices etc. These external artefacts directly or indirectly affect how one evaluates a system's security or how users interact with the system [1].

In user centred design [19], context is one of the four factors that must be considered, and Dey [6] defined context as

> *"...any information that can be used to characterise the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves."*

Dourish et al. [7] argued that for most users the central problem of security is to match the settings in which they find themselves to an immediate set of needs and practical concerns. This problem is even greater in systems considered here as [3] contends that security solutions must be designed such that they transfer across contexts.

In *ad hoc* mobile device associations, context can be characterised in terms of both physical and social environments, association scenarios, device proximity, number of users, and

mode of authentication. Usability and security of OOB channels may vary significantly between different contexts.

Environment Device associations are bound to occur in varying social and physical environmental contexts. Physical contexts may include light intensity and background noise. For example, a payment and ticketing system based on mobile device interactions can occur in contexts ranging from streets, bars, airports etc. Each of these example environment has characteristics that may have negative consequences on the usability and security of OOB channels.

People are governed by social norms and tend to conform to socially acceptable (informally) set of behaviours [9]. These norms and acceptable behaviours virtually govern how humans interact with various artefacts in different environments. The presence or absence of people not participating in a secure device association may be considered a social variable as users may behave differently in either case [11].

In thinking about OOB channels, there is need to think about how different physical and social contexts affect their usability and security. Specific questions at this stage must address concerns of user acceptance of a method and a method's adaptability to changing social and physical contexts.

Association scenario Scenarios may be pairwise or group (3 or more devices). The distinction between pairwise and group association scenarios allows us to reason about the scalability of a particular OOB channel. Dourish et al. [7] noted that security is a mutual achievement of multiple parties. In mobile device associations, all devices have to "behave securely" in order to achieve security. There is, therefore, need to think about how an OOB channel may adapt to group scenarios in terms of both security and usability.

As group size dictates acceptable actions for users [14], the major concern about association scenarios is whether a proposed OOB channel can be used securely in group scenarios. Specific concerns on group size revolve around whether an OOB channel is usable with a single human user associating multiple devices simultaneously or multiple human users are able to sufficiently share the tasks to avoid letting a single user do all the work.

Device proximity Associating devices may be in close proximity, a few centimetres apart for example. In this scenario, users have access to all devices involved or at least each is able to see all devices or their human users. However, secure device associations may also occur between devices that are physically far apart and communicate, say, using Internet. In this scenario, human participants have no physical direct access to one another or devices. Access is only through the OOB channel which the intruder is unable (or at least finds difficult) to forge.

An OOB channel must be human-verifiable by providing visual cues [7] or otherwise, to give assurances to users that the devices they wish to associate are the only ones being associated. This is consistent with recent calls to make security relevant actions visible to users [7, 8] rather than hiding them.

Specific concerns such as the effect of close as well distant devices on OOB channels, and how cues are presented to users for verifying that their devices have achieved required security need to be addressed.

Number of human users The number of users involved in a device association may affect security and usability of OOB channels. An association can either be single-user, where an individual controls all the devices involved, or multi-user, where each device has its own user. In a multi-user scenario, a well designed OOB channel may consider distributing work among users and, as such, it may give an opportunity for using fingerprints of sufficient size (for theoretical security) as opposed to where a single user is expected to do all the work.

The number of nodes where security may fail increases with each additional device or device/user pair as correct behaviour of every user is necessary to achieve desired security [7]. In HISP, users achieve *global* security—by sharing a common cryptographic key, for example—among them only when they all behave correctly. OOB channels, therefore, can only achieve security when they make desirable user actions easier to do than undesirable ones within the context in which they are used.

The concerns to be addressed here are: how can we design or propose OOB channels that allow for work distribution among participants? How can a single user securely associate multiple devices with acceptable mental and physical effort? How does increasing the number of devices or device/user pair affect usability and security of an OOB channel?

Mode of authentication Authentication can be either one-way (asymmetric) or mutual (symmetric). In one-way authentication, one device authenticates one or more participating devices. For example, an Access Point (AP) authenticating mobile devices wanting to access the Internet through it. In this scenario, a user may identify the AP by name or by other means. In short, the user conducts a *weaker* authentication of the AP. The AP on the other hand requires a stronger authentication in which it may require the user to transfer some information to verify that the owner of the device is within the vicinity and hence (presumably) has access rights to it.

In mutual authentication, each participating device authenticates all other devices. In the AP example, the user or her personal device may require more than just a name of the AP. The device may require the AP to compute something which the user can verify.

Either of these scenarios poses different usability and security challenges. In one-way authentication, an authenticating device's acceptance of an association request is good enough for the authenticated device. For example, once a connection to a named AP is established, that is good enough for the device. In practice, the AP may require the user to transfer some information from the AP to the device and no further action from the user.

In mutual authentication, a user(s) may be required to take

extra steps. An AP may be required to indicate to the user acceptance or refusal of the association request and indicate to the device appropriately. The amount of effort expended in mutual authentication may be double that expended in one-way authentication. For example, using a 2D barcode method (as in [16]), the barcode may have to be captured $n-1$ times for one-way authentication and $n(n-1)$ times for mutual authentication where n is the number of devices involved. Understanding this difference in human effort between the two scenarios may be invaluable to designing usable OOB channels.

The extra step in mutual authentication may also be a potential source of security failures. For example, a user misinterpreting a refusal by an AP as an acceptance of the association may result in pairing a device to an unintended AP or interpret a message on an AP correctly but fail to indicate accordingly on the device. These usability and security challenges that one-way and mutual authentication pose to OOB channels must be addressed.

Device affordances Affordances are the means through which a user can input information or instruction to and receive feedback from a device [2]. For example, a mobile phone may have a keypad, a camera—as a means through which a user can pass information or commands to it—a display, and a speaker—through which the user gets feedback from it.

In the literature on OOB channels (e.g. [25, 22]), assumptions on device affordances, though realistic, are too restrictive. They consider only devices of similar affordances but such interactions may not be very practical. Common interactions involve devices of differing affordances. Examples include mobile device and a printer, mobile device and vending machine, mobile device and AP, laptop and mobile phone. This does not imply looking at all possible devices (and their affordances) as it is impractical for a simple reason that devices (and affordances) are continually being invented. We may, however, categorise devices into groups such as mobile, stationary, keypad and display, keypad only, and so on, to help assess and analyse the impact that associations of devices from different groups may have on usability and security of OOB channels.

2.1.2 Technical security

Technical solutions to security problems operate in social settings and secure systems do not only face technical attackers but also social engineers. For example, users find complex passwords difficult to remember and write them down or reveal passwords to someone who claims to be a member of their support team [26]. This is not a human problem [26]) but a result of an attempt to secure a system with technical solutions without considering users. While threats from technical attackers are real, threats from social engineers and unintentional user actions are real too.

Security requirements are also situational—they depend on circumstances [7]. Technical solutions are usually rigid and may require one with technical expertise to be reconfigured. Unlike in organisational settings, such expertise is likely to be unavailable in both home and mobile *ad hoc* interactions. In HISP, technical security requirements determine fingerprint size that users should transfer or compare over an OOB channel. Technical security can be set to fit security requirements at hand.

The challenge on technical security is ensuring that technical solutions are used correctly in the context within which they are deployed. The design and implementation of an OOB channel that facilitates secure human interaction with the system is crucial. An OOB channel must be able to adapt to changes in technical security with little or no effect on the usability of the system.

2.2 Human factors

Users are stakeholders and have personal requirements such as privacy, usefulness of system and easy-of-use [5] on the systems they use. They are aware of their security needs [7], but are unmotivated [8, 27] because doing security is usually not their primary task.

Humans are constantly making security decisions [8]; conscious or unconscious. Different people may make different security decisions under similar circumstances. Naturally risk averse people take less risks in the digital world compared to those who are not. Similarly, those who have been exposed to certain risks tend to be risk-averse towards such risks [24].

2.2.1 Personal variables

Cranor et al. [3] call for considering users of a secure system and their characteristics. This is the main basis of design methods such User Centred Design (UCD) [19] and AEGIS [10]. They emphasise on putting users at the centre of design and understanding their needs and characteristics. Users may broadly be grouped demographically in terms of age, gender, education, culture, occupation, and disability [3].

Users' security decision process may be influenced by their knowledge and experience of a system and the context in which a decision is made. Users misconceive risks they are exposed to [26]; they either underestimate the risk—in which case security decisions expose them to the risk— or overestimate the risk—in which case they feel there is nothing they can do to protect themselves.

Despite misconceiving risks, users are a social countermeasure for every dimension of security i.e. prevention, detection, deterrence, and reaction [9]. For them to be an effective social countermeasure, they need to attain some level of control in systems they use and protect. This calls for systems whose security status is visible to the user [8] rather than transparent. In addition to making security decisions based on knowledge and experience, users operate under different emotional states at different times, in different situations. Though the terms *emotion, feeling*, and *mood* are a source of argument in social science literature [23], the meaning here is not restricted to one or the other. In our case, examples of emotional states are excitement, stress, anxiety, concentration or lack of it, and tiredness. Emotional states may change as a result of peer pressure, time constraints, loss or gain of something etc. Users, even though presented with all the information they need and have the knowledge and experience to make the right security decision, may make an incorrect one because of emotional state in which they are.

Personal variables influence how one makes security decisions. A number of questions need to be addressed; what is the target population? Does it have the knowledge and experience to make correct security decisions? Are users empowered and in control to make the right decision? How do emotional states affect their security decision making? Can we design OOB channels that are secure and usable across personal variables?

2.2.2 *Intentions*

Intentions define an individual's willingness to carry out a particular behaviour [13]. They are, however, influenced by one's attitude towards that behaviour as well as the subjective norms (opinions of others and motivation to comply with those opinions) [13]. An individual's attitude towards security may have an effect on how she interacts with a secure system.

Whitten and Tygar [27] concluded that users display the unmotivated user property when security is orthogonal to the task at hand and [13] found that an individual's intention to show a particular behaviour is affected by his motivation to comply to subjective norms. Motivation, therefore, plays an important role in how users decide what action they can engage into. In addition to motivation, attitudes about a behaviour based on beliefs about and evaluations of that behaviour affect the intention to conduct the behaviour [13]. For example, [26] found that users' lack of compliance with security policies is because of beliefs and attitudes that the risk is not real and that their behaviour is insignificant even when the risk is real. Moreover, security-critical tasks must be aligned with user goals [8]. They should help and not deviate or hinder the user from accomplishing the goals at hand.

2.2.3 *Capability*

Before users adopt new technology, they must perceive it to be ease-to-use [5]. In other words, they must believe that they are capable of achieving a required behaviour in order to engage in that behaviour [13]. Doing security is no exception to this—users must have the capability to use the system in a secure manner without undue effort. Capability may be physical, mental or technological. Assessing whether the target population is capable of carrying out the security-critical task is an essential consideration in designing OOB channels. For example, the proposal to shake devices [15] in order to establish a secure association is only feasible if the devices in question are small enough for one to shake. These factors need to be put into perspective when designing OOB channels.

2.3 OOB Channels

An OOB channel must be evaluated against requirements derived from the technical and contextual and human factors. Typical questions must focus on security (is the method secure against human mistakes?), scalability (can the size of the digest be varied without significantly affecting the usability or security or both?), adaption (is the method capable of adapting to different physical and social contexts in which it will be applied?), and fit for purpose (does the method fit the tasks within the contexts in which they are carried out?).

The evaluation of methods against relevant requirements is crucial to ensure that the broad aspects of context, technical security and human factors are considered. System designers may focus on existing OOB channels while researchers may be interested in developing new ones. In either case, a specific OOB channel can be successful only upon critical consideration of all the factors that may affect its usability and security, and asking questions that are relevant to both (usability and secure) is important.

3. APPLICATION OF FRAMEWORK

The application of the framework may differ depending on whether one is a researcher or system designer. A system designer may have a specific application from which she derives context, in which the application will be used, and technical security. By using the framework, she will identify human factors that may be crucial to the specific use context and identify candidate OOB channels that are likely to support those factors. Researchers, on the other hand, may want to reason about OOB channels and factors that affect them from a wider perspective in order to develop channels that are scalable, usable and secure across contexts. However, in order to develop such methods, it is crucial for the researcher to examine specific application scenarios and analyse how a proposed method may be affected by such scenarios.

Though the goal and approach in which the framework may be used by researchers and designers may differ, the process is similar in both cases; both researchers and designers need to have a target application in mind. For the designer, this may be specific while researchers are likely to have wider concerns than a single application. Having considered a specific application or domain, the framework may be used to design or choose an OOB channel.

In order to validate the proposed OOB channel, a usability study may be conducted. If the results of the study are acceptable i.e. they meet expectations, the method is accepted otherwise the framework may be used again. It is important to note that the framework may be used to propose OOB channels or reason about how a particular channel may be improved. As such, the framework may be used on methods whose usability study results do not meet expectations to improve on them rather than proposing a different one.

The framework fits into the User-Centred Design (UCD) process [4]. UCD is a 3-step process: Analysis, Design, and Evaluation. During the analysis phase, user, task, environmental, and comparative analyses are conducted [4]. It is during the analysis phase that our framework is proposed to be applied and, based on the outcome, an OOB channel proposed. The proposed OOB channel is then evaluated. The outcome of the evaluation is used as feedback that may be used to improve the proposed method, propose a different method or accept the method in its current state.

4. CONCLUSION AND FUTURE WORK

To help understand and reason about the different factors necessary for designing secure and usable OOB channels that work across contexts, we have proposed a framework. The framework can be used by both researchers and designers to reason about these factors and contextualise the target scenarios. Whilst this is an initial attempt at analysing

socio-technical and contextual factors for *ad hoc* device associations, it provides a basis upon which further analysis may be built. We are currently validating the framework by comparing its theoretical predictions and empirical results from usability studies.

5. REFERENCES

[1] A. Adams and M. A. Sasse. Users are not the enemy. *Commun. ACM*, 42(12):40–46, 1999.

[2] J. P. Chin, V. A. Diehl, and K. L. Norman. Development of an instrument measuring user satisfaction of the human-computer interface. In *CHI '88: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 213–218, New York, NY, USA, 1988. ACM.

[3] L. F. Cranor. A framework for reasoning about the human in the loop. In *UPSEC'08: Proceedings of the 1st Conference on Usability, Psychology, and Security*, pages 1–15, Berkeley, CA, USA, 2008. USENIX Association.

[4] K. Crisler, T. Turner, A. Aftelak, M. Visciola, A. Steinhage, M. Anneroth, M. Rantzer, B. von Niman, A. Sasse, M. Tscheligi, S. Kalliokulju, E. Dainesi, and A. Zucchella. Considering the user in the wireless world. *Communications Magazine, IEEE*, 42(9):56–62, Sept. 2004.

[5] F. D. Davis. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 12(Sept.):319–339, September 1989.

[6] A. K. Dey. Understanding and using context. *Personal Ubiquitous Comput.*, 5(1):4–7, 2001.

[7] P. DiGioia and P. Dourish. Social navigation as a model for usable security. In *SOUPS '05: Proceedings of the 2005 symposium on Usable privacy and security*, pages 101–108, New York, NY, USA, 2005. ACM.

[8] P. Dourish, E. Grinter, J. Delgado de la Flor, and M. Joseph. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal Ubiquitous Comput.*, 8(6):391–401, 2004.

[9] I. Flechais, J. Riegelsberger, and M. A. Sasse. Divide and conquer: the role of trust and assurance in the design of secure socio-technical systems. In *NSPW '05: Proceedings of the 2005 workshop on New security paradigms*, pages 33–41, New York, NY, USA, 2005. ACM.

[10] I. Flechais, M. A. Sasse, and S. M. V. Hailes. Bringing security home: a process for developing secure and usable systems. In *NSPW '03: Proceedings of the 2003 workshop on New security paradigms*, pages 49–57, New York, NY, USA, 2003. ACM.

[11] S. Gaw, E. W. Felten, and P. Fernandez-Kelly. Secrecy, flagging, and paranoia: adoption criteria in encrypted email. In *CHI '06: Proceedings of the SIGCHI conference on Human Factors in computing systems*, pages 591–600, New York, NY, USA, 2006. ACM.

[12] C. Gehrmann, C. J. Mitchell, and K. Nyberg. Manual authentication for wireless devices. In *RSA Cryptobytes*, volume 7(1), pages 29–37. RSA Security, Spring 2004.

[13] A. I. From intentions to actions: The theory of planned behavior. In J. Kuhl and J. Beckmann, editors, *Action Control: From Cognition to Behavior*, pages 11–39. Springer Verlag, New York, 1985.

[14] C. Kuo, A. Studer, and A. Perrig. Mind your manners: socially appropriate wireless key establishment for groups. In *WiSec '08: Proceedings of the first ACM conference on Wireless network security*, pages 125–130, New York, NY, USA, 2008. ACM.

[15] R. Mayrhofer and H. Gellersen. Shake well before use: Authentication based on accelerometer data. In *Proc. Pervasive 2007: 5th International Conference on Pervasive Computing*, volume 4480 of *LNCS*, pages 144–161. Springer-Verlag, May 2007.

[16] J. McCune, A. Perrig, and M. Reiter. Seeing-is-believing: using camera phones for human-verifiable authentication. In *Proc. IEEE Symposium on Security and Privacy*, pages 110–124, 8–11 May 2005.

[17] L. H. Nguyen and A. W. Roscoe. Efficient group authentication protocol based on human interaction. In *Proceedings of the Workshop on Foundation of Computer Security and Automated Reasoning Protocol Security Analysis (FCS-ARSPA)*, pages 9–33, 2006.

[18] A. W. Roscoe, S. J. Creese, M. H. Goldsmith, and M. Xiao. Bootstrapping multi-party ad-hoc security. In *Proceedings of SAC 2006*, 2006. to appear.

[19] J. Rubin. *Handbook of Usability Testing: How to Plan, Design, and Conduct Effective Tests*. John Wiley & Sons, Inc., New York, NY, USA, 1994.

[20] M. A. Sasse. Computer security: Anatomy of a usability disaster, and a plan for recovery. In *Proceedings of CHI2003 Workshop on Human-Computer Interaction and Security Systems*, 2003.

[21] M. A. Sasse. Red-eye blink, bendy shuffle, and the yuck factor: A user experience of biometric airport systems. *IEEE Security and Privacy*, 5(3):78–81, 2007.

[22] B. Saxena, Nitesh. Uddin and V. Jonathan. Universal device pairing using an auxiliary device. In *Symposium on Usable Privacy and Security (SOUPS)*, July 2008.

[23] K. R. Scherer. What are emotions? and how can they be measured? *Social Science Information*, 44(4):695–729, December 2005.

[24] B. Schneier. *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2003.

[25] C. Soriente, G. Tsudik, and E. Uzun. Beda: Button-enabled device association. In *In International Workshop on Security for Spontaneous Interaction (IWSSI)*, 2007.

[26] D. Weirich and M. A. Sasse. Pretty good persuasion: a first step towards effective password security in the real world. In *NSPW '01: Proceedings of the 2001 workshop on New security paradigms*, pages 137–143, New York, NY, USA, 2001. ACM.

[27] A. Whitten and J. Tygar. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *Proceedings of the 8th USENIX Security Symposium, August 1999, Washington*, pages 169–183, 1999.

[28] M. Zurko and M. Zurko. User-centered security: stepping up to the grand challenge. In *Proc. st Annual Computer Security Applications Conference*, pages 14 pp.–, 2005.