Usable Security and Privacy for Spontaneous Interactions and Data Sharing Systems

Iulia Ion

ETH Zurich
Institute for Pervasive Computing
Haldeneggsteig 4, 8092 Zurich, Switzerland
Email: iulia.ion@inf.ethz.ch

Abstract. A core property of pervasive computing is smooth data flow with continuous availability across heterogeneous devices. In this context, the multitude of devices, the spontaneous nature of interactions, together with user mobility and frequent disconnections, pose novel challenges to designing secure systems. Furthermore, security related tasks such as setting up secure connections and access control lists, traditionally carried out by trained system administrators, must now be regularly performed by ordinary users. System designers should, therefore, pay special attention to the human factor. This doctoral research aims at defining usable security mechanisms that enable users to securely share information by easily establishing connections between devices and granting access rights to other parties. In this research, we apply usability principles to enable users to bootstrap secure ad-hoc connectivity and manage cross-device, fine-grained access control.

1 Problem Statement and Research Questions

The novel, pervasive computational model is fundamentally different from the static, predictable, desktop- and server-based one, which practically relied on fixed infrastructure. One of the main distinguishing factors is user mobility, which causes mobility of data and devices. The frequently changing, unpredictable nature of the context (which comprises the computing platform and its surrounding environment) affects the landscape of existing security threats. Previously, threat isolation was ensured by providing physical protection (e.g. secured data-cables, locked server rooms), and by setting up and relying on trusted environments (e.g. private networks protected by firewalls). Secure perimeters were created to prevent data leakage and defend against outside threats.

With mobility playing such an important role, however, the traditional criteria of distinguishing between outside (untrusted) and inside (secure) environments are no longer applicable. Furthermore, as the number of devices explodes, system complexity increases and security faces even greater challenges. For example, nowadays ordinary people possess a plethora of devices and use them frequently during the day, e.g. smart phone, iPod, photo camera, PDA, laptop, home computer, work computer, back-up hard disk. Most of these wireless devices never see a professional administrator and must be self managed. Following the vision of ubiquitous computing, devices should be easily accessible and interconnectable in order to facilitate data flow and enable availability of data, such as personal files, documents, emails, contacts and business reports, to authorized parties anytime, anywhere (and from any device).

However, due to the wireless nature of communications and the lack of a secure perimeter, ad-hoc connections between arbitrary devices are vulnerable to man-in-the-middle attacks. For this reason, authentication is required to secure spontaneous device interactions and it represents a key building block for any future distributed applications. No longer relying on wired connections and fixed infrastructures nor on the feasibility of trusted third parties due to the global scale of the problem, conducting spontaneous authentication is however not a trivial problem: With potentially tens of different wireless networks and hundreds of unknown devices in these networks, even selecting the intended communication partner is a major challenge for users. Nevertheless, to enable ubiquitous computing, at the outset, users should be able to easily and securely access new devices, possibly to configure and to add them to personal networks. To solve this problem, in this doctoral research, we address the following research question:

Question 1: *How can we enable users to easily and securely connect devices in spontaneous, temporary or permanent settings, in homes, offices or in public environments, in order to support and facilitate information flow and service sharing?*

In pervasive computing, device disconnection poses a main challenge and often requires data replication to realize permanent data availability and smooth data flow. Despite the increased storage capacity, file management and availability across several potentially disconnected devices constitute a problem for most users. The large amounts of data, and the discrepancy between application symbolic file view (e.g. iPhotos, iTunes library) and the hierarchical file system structure make file management, in general, and access control, in particular, a challenging task. Usable, fine-grained access control mechanisms should cope with the mobility and disconnection of devices to provide people with intuitive and easy means of sharing data with other parties. This problem raises the second research question we want to address:

Question 2: *How can we enable users to make informed security decisions in order to manage data across devices and grant fine-grained data access permissions to other parties?*

Usability is a key concept in this doctoral research and it shall have a strong influence in all design stages: from requirements definition, to system design and development and to the post-release phase. Usable security is a relatively young research field with many unresolved challenges. Still, there is growing recognition that technology alone will not provide all of the solutions needed to solve current security and privacy challenges. As human factors play an important role in these areas, it is critical for security and privacy experts to have a good understanding of how people will interact with the systems they develop. When implementing data protection mechanisms, we will pay special attention to the human-in-the-loop, the so-called *weakest link*, and aim to provide users with adequate conceptional models of the system. Consequently, user studies will play a key role in the design and evaluation stages. Further challenges are raised by the fact that most of the times mobile applications are characterized by short interactions, must have fast response time, cope with small displays, and limited input modes.

Summing up, this doctoral research aims to create usable security mechanisms to enable information sharing, smooth data flow and continuous availability across heterogeneous devices. To accomplish this, we design a system that enables secure, spontaneous interactions and provides users with usable mechanisms to configure their desired privacy and security levels in order to grant other users permanent or temporary access rights to personal files and devices.

2 Approach and Methodology

On the one hand, system security is usually complex, difficult to understand and evaluate for normal users. Consequently, system designers have tried to make security actions transparent, to hide system complexity and automate security decisions. On the other hand, users are reluctant to using systems or features they cannot understand. Applications that hide too much of this underlying complexity do not gain user's trust and if users do not trust the system and do not consider it secure, they will simply not use it or will bypass its security mechanisms. This leads to a sort of design paradox, which can only be solved through a carefully chosen trade-off between simplicity and visibility. While secure systems must hide unnecessary complexity, they should, nevertheless, still provide the user with visibility into the underlying actions and policies.

Research steps

To conduct this research, we will take the following main steps:

1. Conduct an exploratory user study to identify real problems, user needs and expectations regarding distributed data sharing.
2. Design a system meeting the defined requirements, placing special emphasis on the human factor.
3. Implement a proof-of-concept system that deals with access control and spontaneous interactions.
4. Conduct user studies to evaluate the perceived security level, user trust in the system, efficiency and usability as well as psychological acceptability of the security mechanism.

Theoretical considerations

To improve usability we should create clear, understandable systems by abstracting out the mechanisms meaningfully to users and maximizing the use of physical analogies in a user-centric design. In this research, we will follow the general usability principles outlined by Donald Norman in his seminal book *The Design of Everyday Things* [14]. In particular, we will:

- pay special care to providing users with an appropriate conceptual model of the system that properly reflects system functionality,
- provide visibility into system's actions through immediate feedback, to allow users to easily verify task execution,
- create natural mappings through analogies with the physical world. (Here, in particular, the auxiliary authentication channels in device pairing methods can provide an innovative solution to assign permissions to other devices.)

Furthermore, to effectively balance system automation and visibility, we will make use of a proposed framework for reasoning about the human-in-the-loop [5], which should serve to provide a systematic way for system designers to rationalize when actions should be seamless, transparent to the user and when the user should be prompted for a decision or input.

Proof of concept

As a second step in this dissertation, we will build upon the results from the previous step and follow usability guidelines and theoretical considerations to work towards aspects of spontaneous device interaction, file migration and access control granting and implement a proof-of-concept system. The access control design should be applicable to proposed data management systems in different environments. Furthermore, it should incorporate user profiles, policy definition and conflict resolution.

For example, the following systems represent a good context and potential building frameworks for this research.

Digital home storage: The goal is to control access to personal files and share these files with other users and devices. Although several systems support file replication and synchronization (e.g. Perspective [16], Unison [15]), usable access control has not been sufficiently explored. Such systems, however, offer a valuable framework to investigate access control mechanisms and place special emphasis on spontaneous interactions.

Office environment: The goal is to share files during a meeting securely with intended business partners. Courier, a collaborative phone-based file exchange system, enables information sharing. Till now, privacy concerns have not been investigated. Studies on the system show that the lack of usable privacy mechanisms reduce user trust in the system and, consequently, system acceptability [9].

Entertainment centers: The goal is to share files with friends permanently or during temporary get-togethers such as through the intermediation of entertainment centers (e.g. play your mobile phone music during parties). Currently, such systems allow users to make personal data accessible on the play center and to browse it on the stations' display, but do not offer fine-grained access control mechanisms.

We recognize the broad scope of this research problem and plan to further investigate the research area in order to identify more specific key aspects of the system and potential contributions.

Evaluation of research results

Through this work we hope to increase information fluidity and data sharing and connect devices and services. In order to validate the claims and answer the proposed research questions, our proof-of-concept system must effectively support real world users. We will have succeeded if we determine how to best design device pairing methods and usable access control mechanisms to support spontaneous, cross-device information sharing in pervasive computing environments. To evaluate the implemented system, we will (1) measure usability through user studies, and compare the system to existing approaches such as Windows access control, and (2) validate against theoretical risk management guidelines [7]. We will conduct quantitative analysis to estimate user efficiency in task completion and adopt a qualitative approach to examine affective aspects of the interaction design. In particular, we aim to evaluate the following system properties:

Effectiveness: the degree to which the system fulfills its intended purpose and supports users by enabling accurate and complete task performance.

Efficiency: the resources expended by users in achieving accurate and complete task performance.

User satisfaction: users perceived acceptability of the system. This includes user trust and perceived security as well as psychological acceptability.

The proof of concept system will also be compared to the state of the art in security systems. The user study will make a one-to-one comparison. The results of the evaluation will reinforce design guidelines that need to be fulfilled to effectively support file sharing in spontaneous interactions and personal networks.

3 Related Work

In this doctoral research, we build upon results from three different investigation areas: (1) usability theory, (2) secure device pairing methods and (3) access control for file sharing.

In performing tasks, security is almost never the final goal of the user. Traditionally, security has been seen as usability trade-off. Research on usable security and privacy for spontaneous interactions and data sharing has been rather limited so far. Cranor and Garfinkel compiled a book of essays on *Security and Usability* [4]. Only recently, security experts have started giving the user its deserved consideration when designing systems [3, 2] and argue against treating him as the enemy [1] and design frameworks for comparative usability testing of distributed applications [10].

To address the ubiquitous computing challenges in the problem of secure device pairing, a number of proposals have recently emerged, all of which somehow involve the user in the pairing process and partially rely on so-called *auxiliary* or *out-of-band* message channels. Examples of specific auxiliary channels are *video* by using mobile phone cameras and 2D barcodes [13], blinking patterns [18], or laser channels [12], *audio* by comparing spoken sentences [6] or MIDI tunes [19], *motion* by common movement [11], or synchronized button presses [20]. Several usability studies of secure device pairing methods have been proposed [22, 21].

Access control has been extensively investigated in security systems [17]. For its implementation, access control lists, capability lists, or policy-based mechanisms are often adopted. Role-Based Access Control (RBAC) is traditionally a centralized process in which an administrator assigns users to roles and sets access rules. Discretionary Access Control (DAC) deals with distributed, dynamic environments. Users set access rules for resources they own and can delegate access to others. To mitigate the usability problems of access control mechanisms in modern distributed systems, Cao and Iverson propose Intentional Access Management. User intentions (i.e. the descriptions of desired system outputs) are interpreted by an access mediator that either automatically or semi-automatically decides how to achieve the designated goals and provides enough feedback to the user.

To interconnect devices in personal and social networks, architectures like MyNet [8] have been proposed. The MyNet security framework assumes a social network of friends and pre-established trust relationships during an initial introduction process. Each MyNet host has a unique endpoint identifier, which is used to provide secure names for hosts and to encrypt communication. The framework provides authentication, authorization and fine-grained access control to protect the resources of a user's personal network. This doctoral research may build upon the MyNet results and place a further emphasis on spontaneous interactions, mobility and changing context.

In the management of data across potentially disconnected devices, Perspective [16] adopts an innovative construct to improve usability. Its semantic file system construct offers an intuitive, easy way for users to think about files and cope with replica management across devices. This simplifies the management of distributed data and improves the presentation of files in distributed home storage and can serve as a great basis for enabling access control decisions.

4 Preliminary Results

To enable secure communication between devices, we contributed towards the implementation of an open-source authentication toolkit. The goal is to bring together the most notable proposed device pairing methods on top of a common, underlying cryptographic protocol. The toolkit is designed to be easily extendable; the provided auxiliary channels are easily interchangeable. It already runs on a variety of mobile phones and desktop/laptop computers.

Currently, we are designing usability tests to compare existing device pairing methods. Of particular interest is the trade-off between security levels, speed and easiness of use in different scenarios (e.g. under time pressure, in the presence of an active attacker).

In the future, we would like to build on top of the device pairing framework to add file sharing and permission setting between devices.

5 Conclusions

Although a number of systems have been designed that address the problem of data sharing and data availability, people are reluctant to use them, mainly due to the lack appropriate usable access control, security and privacy mechanisms. The goals of this thesis is to enable users to easily and securely interconnect devices, share and access data across these devices, and give access control to friends, family, or business partners.

Results will consist in a set of guidelines for usable access control in data sharing pervasive systems, the design and architecture of the system, prototypical implementation to prove the concept and user studies to evaluate the obtained results and compare it to previous approaches.

References

1. Anne Adams and Martina Angela Sasse. Users are not the enemy. *Commun. ACM*, 42(12):40–46, 1999.
2. Dirk Balfanz, Glenn Durfee, Rebecca E. Grinter, and D. K. Smetters. In search of usable security: Five lessons from the field. *IEEE Security and Privacy*, 2(5):19–24, September 2004.
3. J. Cornwell, I. Fette, G. Hsieh, M. Prabaker, J. Rao, K. Tang, K. Vaniea, L. Bauer, L. Cranor, J. Hong, B. Mclaren, M. Reiter, and N. Sadeh. User-controllable security and privacy for pervasive computing. In *Eighth IEEE Workshop on Mobile Computing Systems and Applications, 2007. HotMobile 2007*, pages 14–19, 2007.
4. Lorrie Cranor and Simson Garfinkel. *Security and Usability.* O'Reilly Media, Inc., August 2005.
5. Lorrie Faith 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.
6. M. T. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, and E. Uzun. Loud and clear: Human verifiable authentication based on audio. In *Proc. ICDCS 2006*, page 10. IEEE CS Press, July 2006.
7. Audun Josang, Bander AlFayyadh, Tyrone Grandison, Mohammed AlZomai, and Judith McNamara. Security usability principles for vulnerability analysis and risk assessment. *Computer Security Applications Conference, Annual*, 0:269–278, 2007.
8. Dimitris N. Kalofonos, Zoe Antoniou, Franklin D. Reynolds, Max Van-Kleek, Jacob Strauss, and Paul Wisner. Mynet: A platform for secure P2P personal and social networking services. In *Proc. PerCom '08*, pages 135–146. IEEE CS Press, 2008.

9. Amy Karlson, Greg Smith, Brian Meyers, George Robertson, and Mary Czerwinski. Courier: A collaborative phone-based file exchange system. Technical Report MSR-TR-2008-05, Microsoft Research, 2008.
10. K. Kostiainen, E. Uzun, N. Asokan, and P. Ginzboorg. Framework for comparative usability of distributed applications. Technical Report NRC-TR-2007-005, Nokia Reserach Center, 2007. http://sconce.ics.uci.edu/CUF/ex_abs.pdf.
11. 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.
12. R. Mayrhofer and M. Welch. A human-verifiable authentication protocol using visible laser light. In *Proc. ARES 2007: 2nd International Conference on Availability, Reliability and Security*, pages 1143–1147. IEEE CS Press, April 2007. Track WAIS 2007: 1st International Workshop on Advances in Information Security.
13. J. M. McCune, A. Perrig, and M. K. Reiter. Seeing-is-believing: Using camera phones for human-verifiable authentication. In *Proc. IEEE Symp. on Security and Privacy*, pages 110–124. IEEE CS Press, May 2005.
14. Donald A. Norman. *The Design of Everyday Things.* Basic Books, September 2002.
15. Benjamin C. Pierce and Jérôme Vouillon. What's in Unison? A formal specification and reference implementation of a file synchronizer. Technical Report MS-CIS-03-36, Dept. of Computer and Information Science, University of Pennsylvania, 2004.
16. Brandon Salmon, Steven W. Schlosser, Lorrie Faith Cranor, and Gregory R. Ganger. Perspective: Semantic data management for the home. Technical Report CMU-PDL-08-105, Carnegie Mellon University Parallel Data Lab, May 2008.
17. R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman. Role-based access control models. *Computer*, 29(2):38–47, 1996.
18. N. Saxena, J.-E. Ekberg, K. Kostiainen, and N. Asokan. Secure device pairing based on a visual channel. Cryptology ePrint Archive, Report 2006/050, 2006.
19. C. Soriente, G. Tsudik, and E. Uzun. HAPADEP: Human asisted pure audio device pairing. Cryptology ePrint Archive, Report 2007/093, March 2007.
20. Claudio Soriente, Gene Tsudik, and Ersin Uzun. BEDA: Button-enabled device pairing. In *Proc. IWSSI 2007*, pages 443–449, September 2007.
21. J. Suomalainen, J. Valkonen, and N. Asokan. Security associations in personal networks: A comparative analysis. In *Proc. ESAS 2007: 4th European Workshop on Security and Privacy in Ad hoc and Sensor Networks*, pages 43–57. Springer-Verlag, 2007.
22. E. Uzun, K. Karvonen, and N. Asokan. Usability analysis of secure pairing methods. In *Proc. USEC 2007: Usable Security*, February 2007.