A Sense of Security in Pervasive Computing
- is the light on when the refrigerator door is closed?

Jakob Illeborg Pagter[1] and Marianne Graves Petersen[2]

Abstract. In this paper, we investigate how existing theoretical contributions on usable security can serve to guide the design of a specific system. We illustrate how going through this theoretically informed, concrete design process, also provides the basis for complementing existing theoretical contributions.
The system we have designed is a system taking advantage of pervasive computing technology to offer hotel guests access to their personal, digital materials while in a hotel room. The design is based on two ideas novel to usable security, namely falsification and the singleton invariant..

1 Introduction

New infrastructures and interaction technologies potentially provide new means for accessing and integrating personal, digital materials in everyday life. While on a business trip, you may access your personal music, film and movie collection stored on a home-server from anywhere in the world. This opens up for new opportunities, at the same time as it raises a need for dealing with security in a way, which makes it feel safe to exploit these new opportunities. We are particularly interested in investigating new contexts and situations where secure access to personal, digital materials can contribute to the growing experience economy (Pine and Gilmore [25]). At the same time, we wish to explore such situations in order to contribute to the emerging area of usable security.

Recently, there has been a growing activity in the area of usable security – or HCI-SEC [7], and we take this as our starting point. In line with others, our starting point is that systems need to be designed in a way which integrates qualities and that neither usability nor security can successfully be designed in isolation or as an add-on ([26], [21]). Different strategies for such integration have been presented. One of the key ideas is to seamlessly integrate security and user goals and let user goals be what drives the interaction and making the security state somehow visible to the user [26]. We take this approach as our starting point, but we also illustrate how it is sometimes beneficial to make security aspects more visible. This idea is inspired by recent trends in usability research, e.g. designing visible and remarkable computing [24].

[1] Centre for IT Security, The Alexandra Institute Ltd., Denmark. jakob.i.pagter@alexandra.dk. Supported in part by ISIS Katrinebjerg Software.
[2] Dept. of Computer Science, University of Aarhus, Denmark. mgraves@daimi.au.dk. Supported in part by ISIS Katrinebjerg Software (www.isis.alexandra.dk/software).

We also share the starting point of Grinter and Smetters [16] that "security cannot be considered in the abstract, separate from a particular application and context of use". We have investigated how to design for secure access to personal digital materials in a hotel room. This setting is chosen as it exemplifies how pervasive computing can contribute new experiences in everyday life. Also, we find that the semi public nature of a hotel room is an interesting site for exploring the nature of usable security in everyday life. Inspired by Dourish et al. [13] we have learned from how people organize themselves around physical materials. We have used this as a basis for designing a system which allows secure access to personal materials in a hotel room.

2 Designing for usable security in a hotel room

The existing literature on HCI-SEC has concentrated on two main areas: A) studies of the usability of existing security systems (e.g. [2] [30]), and B) studies on how to design systems with usable security (e.g. [9], [13], [26]). We have focused on the latter area as our interest is to design usable security systems, but they are of course intertwined.

Based on [4,8,9,13,16,19,26,33,34] we identify the following overall principles for designing for usable security:

- Design for a specific context
- Establish coherence between "normal" actions and security actions
- Make security states visible
- Implicit infer security actions from user actions
- Use explicit security actions when users need to act in response to significant security risks

As investigated in the following, we hypothesise that explicit security actions can be used strategically to design for new engaging experiences, offering security as a major part of the experience. In the following, we investigate how this can be realised in a hotel room context.

Due to the private nature of life in hotel rooms, and therefore the challenges in studying this, we have embarked on a number of resources in understanding how costumers behave. We have used cultural probes materials [15], and in particular the untraditional, but highly relevant empirical material collected by the artist Sophie Calles [6]. Based on her observations and experiences as a maid during a three week stint at a hotel in Vienna, she carefully documented and reflected on how people live in hotel rooms. Further there is a potential in offering new experiences in a hotel room, exploiting pervasive computing technologies. In hotel rooms, people typically bring some personal technologies, but the hotel may offer enhanced experiences if a secure and easy transfer of personal media to other platforms, e.g. wide screen, high quality sound systems etc. is possible

Dourish et al. [13], have illustrated how it is important to learn from how people currently organize themselves in terms of physical arrangement of space and objects in designing future interactive systems for the same context. We interpret the observations of Calles [6]onto a set of characteristics of life in a hotel room in the following ways.

- People creatively inhabit the room with personal materials they have brought from home as well as new materials they acquire on the visit.
- Guests exercise different levels of control of access to the room, using available means, i.e. do not disturb sign on door and lock on suitcase
- A feeling of control over access to private situations and materials is crucial to shaping a sense of home in a hotel room

Pervasive computing technology may potentially provide new means for "making home" in a hotel room. In Calles' examples, people brought physical photos and placed them in the room in order to make home. Using available technology, it is possible for guests to access and organize themselves with all their personal digital materials while in a hotel room. But according to the above observations, we propose that this is only an interesting opportunity, if the users, in an understandable way, are able to delicately control the access to these materials.

Above, we identified a number of principles for designing for usable security. Interpreting these in the hotel context, we see how the principle of designing for visible security states is important in this context too. E.g. the do not disturb sign is very visible both to the person placing it on the door and to the maid responding to it. In particular, also placing the sign on the door is a very explicit action, which is not something happening implicitly as part of a naturally occurring action. Thus this is somewhat conflicting with the principle of designing implicit security actions. This context suggests that explicit security actions must be designed for strategically, with respect to the aspects that the user is most concerned with. In this case including: A) controlling who enters and leave the room and when, and B) controlling access to private materials in one's presence and absence from the room. In the following we discuss how to design for B) when exploiting the possibilities for making home with digital materials in a hotel room.

3 Designing for Usable security in a hotel room

The basic technical setup is that the user has a cell phone either containing or providing access to a variety of digital objects. Further we have a hotel, where each room has a comptatible net-enabled entertainment system.

Based on the above requirements for establishing a sense of security we propose a singleton invariant solution. The overall idea is that at any point in time, contents or activity the user engages in, is only accessible from a single device, i.e. either from the user's cell phone or from the system in the hotel room. We call this the *singleton-invariant* and it is directly inspired from the properties of physical objects which can only be at one place at a time.

A customer/user in a hotel will experience the following sequence of actions: 1) The customer checks into the hotel at night and his cell phone is associated to the hotel room. 2) Upon entering the hotel room she can transfer objects from the cell phone to the hotel room system. For instance the user might place photos on the walls and open a conversation with her family at home for the purpose of, participate in saying goodnight to her kids. 3) The next morning the user leaves the hotel room, goes to a meeting and all personal objects are *automatically transferred back to her cell phone*.

In the cab on the way to the meeting venue, she might continue last night's conversation with the family at home. 4) When later that day she returns to the hotel room, the room is again automatically setup as when she left it in the morning. 5) The next morning she checks out from the hotel, and her cell phone is disassociated from the hotel room system. We see that as specified by the singleton invariant, any digital object is (logically) always either on the phone or on the hotel room system.

From a security point of view, the two primary weak spots are 1) trusting the hotel and its personel, and 2) protecting your cell phone. The first is a necessary assumption. Conversely it could be argued that if we trust the hotel and its personel *fully,* there is also no need for a security solution. We address the middle road where we may believe the hotel as an organization, but might not trust hotel personnel or others who might enter the room when the guest is not there.

As for the cell phone, the immediate solution is of course the built-in authentication mechanism based on PIN-codes. But as shown by Dourish et al. [13] this mode of access control on cell phones is rarely adopted by users; also the PIN only protects the SIM-card, not all data on the phone. An alternative solution could be to use the physical fact that cell phones are typically in the immediate proximity of their owner. One could for instance build a solution based on Bluetooth enabled watches[3] that when paired to another device will provide a warning when this device is out-of-range.

As for usability, we believe that the above solution is indeed designed according to the five guidelines identified above.

4 A sense of security?

A central topic in establishing a sense of security is how to convey the basic security properties to the user, in particular the singleton-invariant. According to Dourish et al. [13], this property must be highly visible and available for *inspection and examination*. The problem is of course, that in the above solution, when a guest leaves the room, his private documents are automatically removed and when he re-enters they are automatically displayed again. How can he know what is displayed in the hotel room when he is outside the room? Is the light on when the refrigerator is closed? Dourish et al. emphasize that security should not be transparent but that it should be "*highly visible* – available for inspection and examination". The point is that visibility does not imply availability for inspection and examination, but that these exact properties may be of high importance in some cases.

It is a well-known and wide-spread scientific principle that any hypothesis must be falsifiable, i.e. it must be possible to construct an experiment which potentially disproves the hypothesis. Experiments which fail to falsify the hypothesis, increase your trust in the hypothesis. We propose to use falsifiability as an instrument in realising inspection and examination. Falsifiable security makes a non-visible security property (i.e. a part of the security state which is not directly invisible, but not observed by the user) visible through an *explicit* action of the user. A good everyday example is locking the door when you leave your home to go for work; it is reassuring to check that the door is indeed locked.

[3] Such as the Bluetooth Watch MBW-100 introduced recently by Sony Ericsson.

In this light, the hotel solution presented above in section 4 is in fact *too* automatic in inferring security actions from the user's actions. Even though the inferred actions are correct, they inhibit the user from attempting to falsify the hypothesis that the singleton-invariant actually works. One way to achieve falsifiability is to change the solution so that objects are no longer automatically moved from the cell phone to the hotel room system as the user enters. Instead we reserve some special command or gesture for moving all objects back to the hotel room system. Note that we might instead have disabled the automatic disengage or both. We do not disable both because disabling one is sufficient and we aim for maximal implicitness and strategically chosen explicit security actions. We choose to disable disengage rather than engage because security is more critical when the user leaves than when he re-enters.

When the user leaves the hotel room he can not only see that objects are moved back to his cell phone, he may also physically go back into the room and verify that all objects have been removed. In this way, falsifiability is ensured.

The change in the interaction is small and subtle, but we are convinced that using the concept of falsifiability in this "strategic" manner can significantly increase the user's sense of security.

5 Conclusions and Future work

The hotel case illustrates in a concrete situation how security is not just a "necessary evil" which needs to be dealt with in one way or another. On the contrary, using falsifiable security, security can in fact become a visible, enabling factor; it can be a significant part of the experience which is sold to people.

Realised in this way, it can give people true control over their most sensitive documents. Our main contributions include falsifiable security as an extension of existing work on how to design systems that are secure and usable. Further we have demonstrated how it is possible to work with these theoretical ideas in the practical design of a system based on the singleton invariant principle. A minor contribution is that our work emphasizes the fact that usable security for commercial applications is a domain far wider than home banking and similar web-based solutions.

To further mature and test our theoretical and practical concept, we plan to implement aspects of the system in the future and to conduct an evaluation of this implementation. Future work also includes addressing the common scenario of multiple guests in the same hotel room.

In the present work we have articulated how falsifiable security can be implemented in a pervasive computing system, which has strong physical aspects, however, falsifiable security can be further matured through investigating how this can be designed for in contexts with less physical aspects, e.g. can it contribute to prevent phishing.

6 References

[1] G. D. Abowd, and E. D. Mynatt, 2000. *Charting past, present, and future research in ubiquitous computing.* ACM Trans. Comput.-Hum. Interact. 7, 1 (Mar. 2000), 29-58.

[2] A. Adams and M.A. Sasse. *Users Are Not The Enemy.* Communications of the ACM, vol 42(12), 1999.

[3] D. Balfanz, D.K. Smetters, P. Stewart and H.C. Wong. *Talking to strangers: Authentication in Ad-Hoc Wireless Networks.* Proceedings of Network and Distributed System Security Symposium 2002 (NDSS'02), 2002.

[4] J. E. Bardram, R.E. Kjær, and M.Ø. Pedersen: *Context-Aware User Authentication – Supporting Proximity-Based Login in Pervasive Computing.* UbiComp 2003, 2003.

[5] J. E. Bardram. *Activity-Based Computing: Support for Mobility and Collaboration in Ubiquitous Computing.* Personal and Ubiquitous Computing, 9(5), p. 312-322, 2005

[6] S. Calles. *Double Game.* Violette Editions. 2000.

[7] L. F. Cranor and S. Garfinkel. *Secure or Usable?* . IEEE Security and Privacy, vol. 2(5), 2004.

[8] R. de Paula, X. Ding, P. Dourish, K. Nies, B. Pillet, D. Redmiles, Jie Ren, J. Rode, and R.S. Filho. *In the Eye of the Beholder: A Visualization-based Approach to Information Systems Security.* International Journal of Human Computer Studies Special Issue on HCI Research in Privacy and Security, 2005.

[9] R. de Paula, X. Ding, P. Dourish, K. Nies, B. Pillet, D. Redmiles, Jie Ren, J. Rode, and R.S. Filho. *Two Experiences Designing for Effective Security.* Symposium on Usable Privacy and Security (SOUPS), 2005.

[10] A.J. DeWitt and J. Kuljis. *Aligning Usability and Security: A Usability Study of Polaris.* Symposium on Usable Privacy and Security (SOUPS), 2006.

[11] R. Dhamija and J.D. Tygar. *The Battle Against Phishing: Dynamic Security Skins.* on Usable Privacy and Security (SOUPS), 2005.

[12] P. DiGioia and P. Dourish. *Social Navigation as a Model for Usable Security.* Symposium on Usable Privacy and Security (SOUPS), 2005.

[13] P. Dourish, R. E. Grinter, J. D. de la Flor, and M. Joseph. *Security in the wild: user strategies for managing security as an everyday, practical problem.* Personal and Ubiquitous Computing, vol. 8, 2004.

[14] I. Flechais, M.A. Sasse, and S.M.V. Hailes. *Bringing Security Home: A process for developing secure and usable systems.* New Security Paradigms Workshop 2003, ACM 2004.

[15] W. Gaver, T. Dunne, and E. Pacenti. *Cultural Probes*. Interactions, Vol. 6, issue 1, 1999. ACM Press, pp. 21-29.

[16] R. E. Grinter and D. K. Smetters. *Three Challenges for Embedding Security into Applications.* Proceedings of CHI 2003 Workshop on HCI and Security Systems, USA, 2003.

[17] S. Knap. *Fængslets hjemløshed (Homelessness of Prison).* Jordens Folk 2/2005. University of Aarhus, www.jordensfolk.dk, pp. 42-45.

[18] J.M. McCune, A. Perrig, and M.K. Reiter. *Seeing-is-believing: Using Camera Phones for Human-Verifiable Authentication.* Technical report, School of Computer Science, Carnegie Mellon University, CMU-CS-04-174, 2004.

[19] R. Newman, S. Gavette, L. Yonge, and R. Anderson. *Protecting Dometisc Powerline Communications.* Symposium on Usable Privacy and Security (SOUPS), 2006.

[20] J.I. Pagter and M.Ø. Pedersen. *The All-Or-Nothing Anti-Theft Policy – Theft Protection for Pervasive Computing.* In preparation, 2006.

[21] L. Palen and P. Dourish. *Unpacking "Privacy" for a Networked World*. Proceedings of the ACM Conference on Human Factors in Computing Systems CHI 2003 (Fort Lauderdale, FL), 129-136. New York: ACM, 2003.

[22] S.N. Patel, J.S. Pierce, and G.D. Abowd. *A Gesture-based Authentication Scheme for Untrusted Public Terminals.* UIST'04, 2004.

[23] M. G. Petersen, and K. Grønbæk, K. *Shaping the Ambience of Homes with Domestic Hypermedia.* In P. Markopoulos et al. (Eds.) Proceedings of European Symposium on Ambient Intelligence, Eindhoven, Netherlands, November 8-10, 2004 (EUSAI 2004), LNCS 3295, pp. 218–229, 2004. Springer-Verlag Berlin Heidelberg 2004.

[24] M. G. Petersen. *Remarkable Computing – the Challenge of Designing for the Home.* In Proceedings of CHI'2004, ACM Press, pp. 1445-1449.

[25] B. J. Pine and J. H. Gilmore. *The Experience Economy: Work Is Theater & Every Business a Stage*. Harvard Business School Press (April 1999).

[26] D. K. Smetters and R. E. Grinter. *Moving from the Design of Usable Security Technologies to the Design of Useful Secure Applications.* New Security Paradigms Workshop '02, USA, 2002.

[27] F. Stajano and R. Anderson. *The Resurrecting Duckling: Security Issued for Ad-hoc Wireless Networks.* 7th Internation Workshop on Security Protocols, 1999.

[28] ISO 9241-11

[29] R. West. *HCI and Security – A Contradiction in Terms?* Special issue of interactions May + June 2006, ACM Press.

[30] A. Whitten and J.D. Tygar. *Why Jonny Can't Encrypt: A Usability Evaluation of PGP 5.0.* Proceedings of the Ninth USENIX Security Symposium, 1999.

[31] I. Winther. *Hjemlighed. Kulturfænomenologiske studier (Sense of Home, Cultural Phenomenological Studies).* Danmarks pædagogiske universitets forlag, 2006.

[32] F.-L. Wong, Frank Stajano and Jolyon Clulow. *Reparing the Bluetooth pairing protocol.* Security Protocols 2005.

[33] M. Wu, R.C. Miller, and G. Little. *Web Wallet: Preventing Phishing Attacks by Revealing User Intentions.* Symposium on Usable Privacy and Security (SOUPS), 2006.

[34] K.-P. Yee. *Aligning Usability and Security.* IEEE Security and Privacy, vol. 2(5), 2004.