Security in Context – Lessons Learned from Security Studies in Hospitals

Jakob E. Bardram
IT University of Copenhagen
Rued Langgaards Vej 7, DK-2300 Copenhagen S., Denmark
bardram@itu.dk

ABSTRACT
In this position paper I discuss methods for analyzing, designing, and evaluation usable security systems. The discussion is rooted in a long-term engagement in the study and design of usable user authentication technologies in hospitals. Based on this empirical background, I discuss lessons learned and some of the challenges I see in this area. These discussions are intentionally open-ended in order to foster discussion at the workshop.

1. INTRODUCTION

Logging in and out of a computer system is a mundane and yet fundamental aspect of using a computer and it therefore seldom receives much attention during the design and implementation of new computer systems. Often standard, build-in mechanisms in the underlying operating system or middleware is used in the creation of new applications.

Some studies have pointed to usability problems with the use of passwords and the organizational policies surrounding it. Adams and Sasse [1] note that mechanisms and policies for increasing security, like frequent change of passwords, had the opposite effect because users then made easy-to-remember passwords and wrote them down, thereby lowering security. Hence, security mechanisms incompatible with work practices may be circumvented by users and thereby undermine system security overall. Adams and Sasse's investigations also demonstrate that users are certainly motivated to support the security of the system, but often unable to determine the security implications of their actions. I have previously studies the security surround the use of computers in a hospital setting [3]. These studies show, amongst other things, that conventional login procedures caused considerable usability problems. Many of these problems arise because technology designed and developed for the office environment is transferred without modification to the hospital setting. For example, the Electronic Patient Record (EPR) system used normal username/password authentication which added much overhead to the frequent access to the medical record. Generally speaking, I have argued that the traditional login procedure does not in any sense recognize the nature of medical work as being nomadic, often interrupted, cooperative, and involving sharing of common material. Hence, I strongly agree with Zurko and Simon [6] and later Flechais et al. [5], who call for doing *user-centered security* in order to create security models, mechanisms, systems, and software that have usability as a primary motivation or goal.

It is, however, still a very open question how we actually *do* such user-centered security; how do we identify the challenges; how do we do design together with users who would often rather prefer being without any security hazzle; how can we implement security mechanisms which are *sufficiently* secure while being usable; and how do we evaluate such technologies.

In this short position paper I would like to discuss some of these issues in an open ended fashion in order to provide input for further discussion at the workshop. I will base my discussion on empirical experience in the study of usability problems related to security, the design of usable security mechanisms, and the attempts to evaluate such technologies. Most of my work has been within user authentication and the present discussion will hence deal with this aspect of security.

2. THE SECURITY / USABILITY TRADEOFF

There is a general tendency to view security as a tradeoff against usability – the more secure you want a system to be, the more hard to use is it. For example, strict password requirements – like long, no-sense passwords which are often changed – are clearly putting an additional usability burden on the users. Similarly, the use of smart cards can be combined with a PIN code – this is more secure in the case of theft, but is less easy to use that just swiping the card through a reader.

However, as argues by Adams and Sasse [1] technically increasing the security by adding strict requirements on the behavior of the users can often lead to less *de-facto* security since people compensate in non-secure ways. We found, for example, in our studies at the hospital ward that the use of cryptic passwords made users write the passwords on the computer displays (as shown in figure 1); the requirement of constantly changing passwords made users alternate between passwords like '12345' and '67890'; and because login was rather time-consuming, they often just left terminal without logging off (which is also evident in figure 1).

Hence, as I have previously argued [4], the core challenge is not only to make theoretically secure system, but system

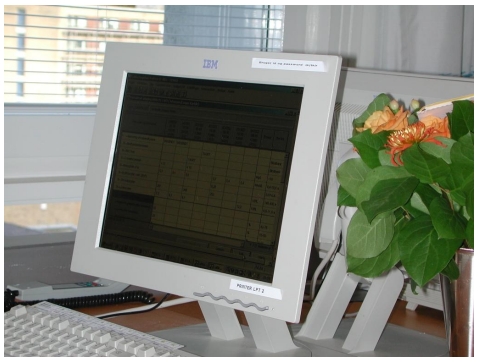

Figure 1: A terminal left on a hospital ward. Note that the user id and password are written on the top right and that the terminal has been left logged into a medical record.

Figure 3: An elderly woman trying to use a tablet PC, including using the finger print scanner for user authentication.

which are *sufficiently secure* from a practical/usability point of view. Furthermore, I do not completely accept the security/usability tradeoff argument. This tradeoff is apparent with most of the security technologies available today, but a core design goal must be to design security technologies which makes such technologies secure *as well as* usable.

In the following I will present how we have been working with these matters, focusing on a discussion of the methods used.

3. ANALYZING SECURITY ISSUES

We have been analyzing security issues in different hospitals using ethnography; i.e. participative field studies, interviews, observation, artifact studies, etc. In this case, artifacts include more technical artifacts related to computer security, like user directories (e.g. LDAP servers), log files, security policies, etc. In general, our experiences are that many security issues can be revealed using such ethnographic methods. Especially combining observations of how users actually *behave* as compare to what the *say* during interviews. Users may often think they behave in a secure way, while trained security eyes will often reveal that there are numerous security holes in their behavior. For example, leaving the terminal without logging off or writing down passwords.

The challenging part is to make users talk freely about these security matters. Often you will need to ensure them that any non-compliance to the hospital's security policy found during the study will *not* be held against them. Hence, making such security/usability studies will need the hospital management's guarantee on such a conduct. Our experience is, that once you gain trust amongst the clinicians, they quite freely talk about security issues in the daily work – especially because it often adds considerable stress to the use of computers in a otherwise hectic working environment.

But the most important part of the analysis of security problems is to discover usability problems that are rooted in security aspects of a computer system. In the hospital, for example, we found that the whole notion of 'user authentication' was actually contradictionary to the way work was done in a hospital ward. As illustrated in left side of figure 2 much work around the patient record is done in a co-located collaborative fashion enabling all users to view and annotate the record. When using the electronic patient record (EPR) – as shown in the right side of figure 2 – this work setup is difficult to achieve because user authentication on a computer is *personal*. Users at the hospital ward complained that it was nearly impossible to work together 'around' the medical record after it had been digitalized. There are several challenges in creating true multi-user co-located collaboration technologies, but one of them is to enable users to 'share' a login, i.e. enabling some kind of collective user authentication. This notion clearly contradicts the personal user authentication evident is all types of user authentication technologies available today. In order to capture such more fundamental issues, we would argue that field studies of security issues should look beyond the issues that you would normally consider to be related to security.

In another study pertaining to the design of home monitoring devices for elders, user authentication again surfaces as an area causing many usability problems for the users. The monitoring setup consisted of two parts; one part was the set of monitoring devices, including a scale and a blood pressure monitor; the other part was a web-based portal where the elders and their caregivers and relatives could read the monitoring data as well as related data like prescribed medicine. The monitoring devices communicated wirelessly to a hub in the home, which relayed the data to a server. The web-portal was accessed using a tablet PC situated in the home.

In the design of these technologies, little care was devoted to the usability of the security mechanisms of the system. User authentication to the tablet PC was based on Windows login and access to the web portal was done using username and password. We were using a tablet PC with a build-in finger print scanner which – in theory – was supposed to help users logon to Windows. However, when inviting a group of elders to help us design and evaluate the technology in a workshop, it became evident that this kind of technology was very difficult for these persons to use. As illustrated in figure 3 an elderly lady has severe problems of using the tablet PC and she did not succeed in actually authenticating herself to the system using the finger print scanner. And she

Figure 2: Co-located collaboration around the medical record. Left – paper-based record; Right – using the EPR.

never came to understand the whole notion of usernames and passwords.

Now, one may argue that his person was simply too old and needed to be in an assisted living facility. The point is, however, that she actually *was* living in an assisted living facility – one which were trying out these new technologies! And more generally speaking; if pervasive healthcare technologies are going to help us deal with the growing elderly population, then we seriously needs to address how this technology is designed to work – including the security mechanisms.

4. DESIGNING AND EVALUATING SECURITY TECHNOLOGIES

Performing user-centered design of security technology seems not to be the most obvious this to do. However, it is our experience that this can actually be done. In several design sessions we have been discussing and experimenting with different user authentication technologies. For example, the use of biometric technologies was discussed and some of them were tried out. However, the clinicians were generally not satisfied with these technologies. Finger print scanners were deemed unsuitable for a hospital environment because clinicians often wear latex gloves. Furthermore, finger print scanners were viewed as a potential hygiene risk if many people were touching them constantly.

In the design of the proximity-based user authentication mechanism [4], users were involved in the design and evaluation. The overall goal with this proximity-based user authentication technology was to log in the user when he or she approached a computer, like a large public display. This design is illustrated in figure 4 which is a scene form a video prototype created to illustrate various design ideas for pervasive computing in a hospital setting [2]. This video prototype was used as a design tool and was presented to a group of clinicians, and the user authentication was subsequently discussed. Later in the design process, the idea was implemented as part of a prototype and the user could experiment with the proximity-based authentication technology.

From this design process we learned a lot of things that improved the system. First of all, after a while the users pointed out that the idea of logging in a person by approaching a display may not work in a real hospital. Often during a hectic

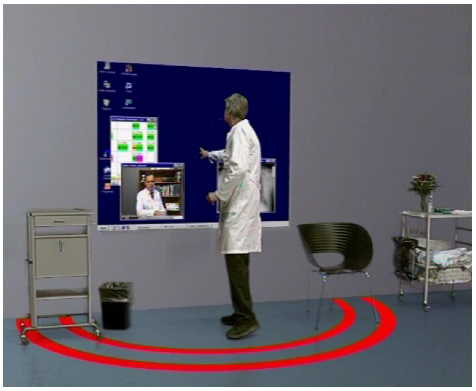

Figure 4: An illustration of the proximity-based user authentication mechanism [4]. The scene is take from the video prototype presented in [2]

.

working day, many users would be located next to a display, without the need for using it. Hence, the authentication needs to be triggered by some deliberate gesture from the user wanting to log in. Another issue that came up was the need for ensuring fast switching between users – in hospitals you would often have situation where one clinician is taking over from another. Hence, there was a need for supporting a 'shift user' command in a graphical environment which would change from one user to another, but leaving the entire screen as is, displaying the current patient with related medical data. Strictly speaking, one could argue that this 'shift user' mechanism had very little to do with user authentication. But again, this is a good example of how a user-centered design process of security technologies reveals some more fundamental issues that contains potentials for improving more basic aspects of the underlying execution platform. It is often when security technologies are viewed in a context that usability issues arise.

These improvements of the idea came out of a concrete design process – it was during the hand-on experimentation with different prototype that the users started to understand what the technology was about, how it worked, and – most importantly – how it could be improved. It is our experience that once you get the users involved and introduced to secu-

rity issues, these things are not as difficult to relate to as you may suspect and it is possible to engage in a user-centered design process of security technologies.

5. LESSONS LEARNED

Instead of a conclusion, I will end the paper by summing up some of the lessons learned from my analysis and design of security technologies. This may add to the discussion at the workshop.

L1 Ethnographic field studies are very useful in understanding security problems, their origin, and consequences related to usability. One should, however, be aware that security usability problems may not be limited to just things related to security; some usability problems arise because of inadequate security mechanisms; but security problems also emerge from usability problems. Therefore, such security studies must apply a broad study of the work in a work setting.

L2 Design security technologies based on what users *do* rather than merely improving existing security technologies. For example, many new kinds of user authentication technologies have been designed over the years, like biometrics systems and smart cards. None of these technologies, however, break with the fundamental user authentication principle, i.e. that you authenticate *one* user based on some identification (e.g. the username) and some verification (e.g. the password). In a hospital setting, for example, this model is not sufficient because what you often would like to have is some notion of a 'shared login' supporting co-located collaboration.

L3 An important step in making security more usable is to realize that there is a need for many different kinds of security – one size does not fit all. There is a huge difference between ensuring confidential medical data on a public network as compared to user identification for the use of medical devices in the home. Because there seems to be a trade-off between usability and security (see however the section above on this), care should be take to deploy security measures which are *appropriate to the situation at hand.*

L4 Make security *visible and understandable*. Based on our studies we would strongly suggest that technologies for security are made more visible than they are today. In the hospitals, for example, most users expressed concerns for security – they would very much like to behave in a way that maintained secure use of medical data. Most of them, however, had limited knowledge of what to do. And when using the computers, they had no idea of how secure their behavior was. Making security visible is indeed not easy, and I have no concrete suggestions for how to do this in a general way. I do think, however, that having this in mind when designing security technologies would make security more usable.

In general, I would argue that it is important to put the design and evaluation of security technologies into a *realistic use context*. It is often when analyzing the use of security technologies in a context that the real benefits and drawbacks of the technology reveals itself. Often, security technologies which are proven secure in isolation may turn out to be difficult or even impossible to use in a real-world context, which again may lead to user applying the security improperly. I think it is important for the design of security technologies to incorporate the use situation to a larger degree in order to build technologies which are really secure.

About the Author

Jakob E. Bardram is a professor in computer science at the IT University of Copenhagen. His main research interests are software architectures and middleware for pervasive computing, with special focus on the challenges pertaining to healthcare, both in hospitals and in the home of the patients. Since healthcare deals with sensitive patient data, security is absolutely crucial in this domain. However, for pervasive healthcare technologies to be successful, they have to be easy to use. Especially taking into consideration that the users would typically include elderly and disables persons as well as people with physiological and metal health problems. Hence, making easy-to-use secure systems within pervasive healthcare is quite central – and challenging.

REFERENCES

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

[2] J. Bardram, C. Bossen, A. Lykke-Olesen, R. Nielsen, and K. H. Madsen. Virtual video prototyping of pervasive healthcare systems. In *Proceedings of the conference on Designing interactive systems*, pages 167–177. ACM Press, 2002.

[3] J. E. Bardram. The Trouble with Login - On Usability and Computer Security in Ubiquitous Computing. *Personal and Ubiquitous Computing*, 9(6):357–367, 2005.

[4] J. E. Bardram, R. E. Kjær, and M. . Pedersen. Context-Aware User Authentication - Supporting Proximity-Based Login in Pervasive Computing. In A. Dey, J. McCarthy, and A. Schmidt, editors, *Proceedings of UbiComp 2003*, volume 2864 of *Lecture Notes in Computer Science*, pages 107–123, Seattle, Washington, USA, Oct. 2003. Springer Verlag.

[5] I. Flechais, M. A. Sasse, and S. M. V. Hailes. Bringing Security Home: A process for developing secure and usable systems. In *Proceedings of the 2003 Workshop on New Security Paradigms*. ACM Press, 2003.

[6] M. E. Zurko and R. T. Simon. User-centered security. In *Proceedings of the 1996 workshop on New security paradigms*, pages 27–33. ACM Press, 1996.