Pers Ubiquit Comput (2005) 9: 357–367
DOI 10.1007/s00779-005-0347-6

ORIGINAL ARTICLE

Jakob E. Bardram

The trouble with login: on usability and computer security in ubiquitous computing

Received: 15 April 2004 / Accepted: 8 March 2005 / Published online: 23 July 2005

Abstract Logging in by typing usernames and passwords is by far the most common way to access modern computer systems. However, such contemporary user authentication mechanisms are inappropriate in a ubiquitous computing environment, where users constantly are accessing a wide range of different devices. This paper introduces new concepts for user authentication in ubiquitous computing, such as the notion of *proximity-based user authentication* and *silent login*. The design of these new mechanisms is part of the design of a ubiquitous computing infrastructure for hospitals, which is grounded in field studies of medical work in hospitals. The paper reports from field studies of clinicians using an electronic patient record (EPR) and describes severe usability problems associated with its login procedures. The EPR's login mechanisms do not recognize the nature of medical work as being nomadic, interrupted, and cooperative around sharing common material. The consequence is that login is circumvented and security is jeopardized.

Keywords Login · User authentication · Ubiquitous computing · Computer-supported cooperative work (CSCW) · Activity-based computing (ABC) · Electronic patient record (EPR) · Healthcare · Hospitals

1 Introduction

The title of this paper paraphrases the title of Donald Norman's old paper on "The Trouble with UNIX" [17]. In his paper Norman analyses some of the basic commands in the UNIX operating systems and points to some of the fundamental usability problems associated with these commands. For example, it is in no way obvious why the command *cat* is used to print out a text file on the screen.

In this paper, we would like to draw the attention to another fundamental usability problem associated with the use of practically every computer in the world, namely the trouble of logging in and out of a computer. This 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. This paper demonstrates that the classic login and logout design pattern causes fundamental usability problems. And because the login design pattern is used in practically every computer systems on the globe, this usability problem is already of enormous scope.

But with the advent of pervasive computing the problem is increasing. Pervasive or ubiquitous computing [23] envision a future where computers are available in huge numbers that they are mostly embedded in everyday artifacts, like furniture, cars, buildings, etc., and they cooperate via a basic communication infrastructure. We are entering a period where instead of every user having a personal computer, a user would be able to use a vast number of more or less public computers. Now, imagine that a user would need to type in his username and password on all these computers before he could start using them. Clearly, if the design pattern of login and logout is not considered a usability problem today, it will most certainly become one in the years to come.

The aim of this paper is twofold. First, it presents findings from a field study of clinicians using an electronic patient record (EPR) with special emphasis on issues related to user authentication and user session management. Even though this EPR cannot be characterized as an ubiquitous computing environment at all, the study provides an important insight into the challenges in designing proper user authentication mechanisms for an ubiquitous computing environment supporting the highly nomadic, dynamic, interrupted, and cooperative work in hospitals. Second, the paper presents new concepts for user authentication mechanisms for ubiquitous computing environments,

J. E. Bardram
Centre for Pervasive Healthcare, Department of Computer Science, University of Aarhus, Aabogade 34, 8200 Aarhus N, Denmark
E-mail: bardram@daimi.au.dk

which are grounded in the field studies. These mechanisms have been implemented and evaluated as part of a larger ubiquitous computing environment for hospitals, called the *ABC Framework*.

The paper starts by introducing some historical background and related research on user authentication and usability. Section 2 introduces the field study and Sect. 3 discusses the findings from this study. Section 4 presents the new concepts for user authentication in ubiquitous computing and Sect. 5 concludes the paper with a discussion of tradeoffs between usability and security.

1.1 Background: identification and user authentication

User authentication is a basic theme in computer security and covers establishing who the user is (*identification*), verifying this identity (*verification* or *authentication*), and providing proper access to the resource that the user is allowed to use (*authorization*). User authentication became important when multi-user computers and operating systems were introduced. The later mainframe batch and timesharing systems were the first to introduce the login by typing username and password. Early minicomputers (e.g. PDP-1 and PDP-8) did not have a login procedure; neither did the Apple II or the original IBM PC. But with the spread of UNIX on the PDP-11 minicomputer and the networked PCs, login again became needed [22].

Even though the traditional login by typing username and password has developed technically over the years it has not changed since the 1960s seen from a usability point of view. This tendency is also reflected in the research done around user authentication where most work has been done within the fields of computer communication and computer security, and very little has been done from a usability point of view.

A few 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. However, 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. Zurko and Simon [24] and later Flechais et al. [11] call for doing *user-centered security* to create security models, mechanisms, systems, and software that have usability as a primary motivation or goal. This paper is an example of doing this kind of 'user-centered security' design.

There is, however, a commercial pressure on handling the process of login in a more convenient manner. We thus witness the design of hardware as well as software system for easier login. For example, one of the prominent usage scenarios for the smart card is user authentication [8]. The SunRay system from SUN utilizes smart card technology as a way of logging in a user on an X Windows terminal and to restore the user session. Likewise, software systems are devised to help user authentication across different domains and systems. For example the lightweight directory access protocol (LDAP) can be used as a central repository for usernames and passwords enabling single signon. Similarly, Microsoft Passport.net aims at solving the increasing problem of typing in usernames and passwords on numerous web sites by creating a centralized authorization mechanism.

The use of biometric systems is receiving an increasing attention currently. Biometric identification is a common term for using a person's biological traits as a way of identifying him. There are basically eight biometric types that are used in systems at the moment: face geometry, fingerprint, hand geometry, iris pattern, retinal pattern, signature, voice print, and facial thermogram [12]. Even though it is also being 'marketed' as a new user-friendly user authentication mechanism, there is little research so far into the usability of these systems. Most work and research on biometric systems focus on security and accuracy.

Login using usernames and passwords are designed for, and often used in an office situation, characterized as being individuals working while sitting down at a desk using the same personal computer for a long period of time—typically a whole working day. It is the aim of this paper to demonstrate how this traditional login schema completely disrupts a smooth flow of work in settings characterized by workers being mobile, often interrupted, cooperating and using many different computers during a working day. We want to argue that the design of ubiquitous computer systems for these kind of working environments needs to accomodate such challenges, rather than unconsciously adopt existing user authentication mechanisms.

2 The study

Our field study can be characterized as an ethnomethodologically oriented investigation [13]. We have made participant observation and interviews of a mixed group of nurses and doctors at a Cardio-Thoracic surgical department, called department T, at a large Danish hospital.

2.1 The site: department T

Department T specializes in surgical procedures relating to the heart, lungs and stomach—for example bypass operations and replacing heart valves. The department performs approximately 15 heart surgeries every week.

Department T consists of a ward where the patients are initially admitted before surgery and transferred back to post-op treatment after having spent an average of 24–48 h at the intensive care unit immediately after surgery. The ward can carry 30 pre and post-op patients and department T treats approximately 1,300 patients a year. The ward occupies the sixth floor in the main hospital building, whereas the surgeons' and head nurse's offices are located on the second floor in a separate building, which also holds the offices of the perfusionists and some of the secretaries. Overall, the department employs roughly 20 surgeons, 50 nurses, 8 perfusionists and 6 secretaries. The ground plan for the ward is illustrated in Fig. 1.

The number of doctors and nurses present at the ward changes depending on the time of day. In a day shift, 13–15 nurses are working at the ward while 8–10 surgeons do the morning round before proceeding to operating theatres, whereas during the night shift, the ward is 'guarded' by 3–5 nurses with 2 doctors on call.

The EPR system installed at department T is a classic client-server solution with a centralized database server located in the hospital's IT department and 'thick' clients running on Windows NT PCs. When installing the EPR system, the ward's office (A + B in Fig. 1) was completely refurnished with new computer desks arranged in a way so that users would sit besides one another facing the PC (see Fig. 2). There were eight PCs installed in the office, two PCs in the conference room (D), and one PC in the medicine room (C). The PCs in the medicine room and in the conference rooms were not used. The one in the medicine room was too small and the ones in the conference room were too far away from where the work took place. Department T has been using the EPR system for 2 years and is one of the departments in Denmark with the most experience in using EPR systems.

2.2 Data collection and analysis

Three researchers made 80 person-hours of participant observations of the clinical staff, i.e. followed a person around for the duration of their shift and during that time observed the work and asked questions to broaden our understanding of the work routines, general work practice and the use of the computer system [18]. We did site observations of a particular room. For example, we stayed in the ward's office during day and night shifts, looking at movement patterns in the room and the usage of the computers [13]. We observed staff meetings, like the surgeons' X-ray conferences with the radiology department, meetings about newly operated patients with the intensive care unit, and the frequent information meetings at the ward about the patients' health-wise progress. Such meetings took place both between the nurses as they 'handed over' their patients to the next shift, and between the nurse in charge of a patient and a surgeon in preparation of one of the two daily ward rounds. Our observations covered different work tasks (e.g. preliminary patient examinations, different staff meetings, ward rounds, medicine dispensing and a by-pass operation), and different time slots (day, evening and night watch, week-days and weekends). Field notes were taken continuously and pictures were taken. The observations were followed by seven interviews lasting ca. 45 minutes each, and four future workshops [14], which were video recorded. The theme for the interviews and workshops were to reflect on some of the observations, and to let the clinicians articulate their problems experienced with the current computer support in their daily work and to discuss visions for the design of new types of computer support for clinical work. A part of these interviews and workshop dealt with the problems surrounding login and logout of the EPR system.

The field notes and the interviews were transcribed and analyzed for recurrent patterns of usability problems and design challenges. This paper reports on one such pattern, namely the design pattern of login and logout of the EPR.

3 Findings

The introduction of the EPR introduced the need for identification and authentication of users when accessing the EPR system. This is such a fundamental and legal aspect of using an EPR that it never received much attention during the implementation of the system.

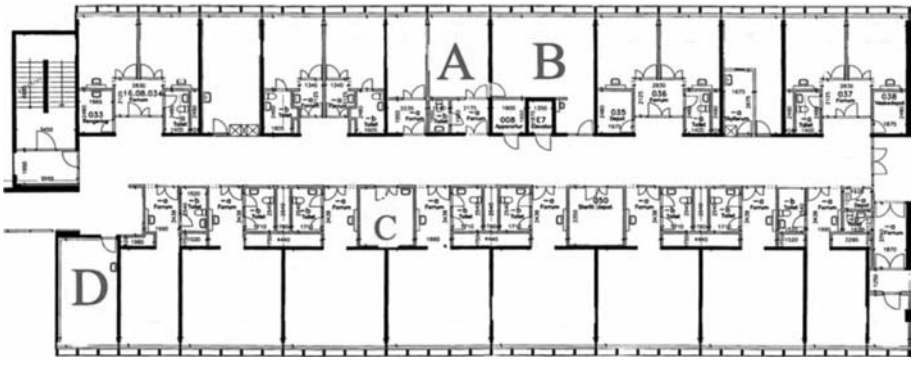

Fig. 1 Ground plan of the ward at department T. Important locations are: the ward office (A + B), the medicine room (C), and the conference room (D)

Fig. 2 The ward office equipped with PCs lined up in one row, forcing the clinicians to work one-to-one with the EPR. This picture is taken in location A in Fig. 1

However, this seemingly truism was the root of many usability problems at the department.

Our analysis has identified some basic aspects of medical work, which we shall present in this chapter and discuss how the login procedure of the EPR system contradicts the way medical work is being accomplished in practice.

3.1 Clinical work happens in a fast pace while login causes focus shift

A striking feature of medical work in a modern hospital is that it is happening in a fast pace—for an outsider it might even seem chaotic. Much work takes place ad hoc in the hallway, during lunch, in the door openings, and while moving from one location to another. Furthermore, a clinician is often engaged in several tasks in parallel and is often having a conversation going on with several people simultaneously. Clinicians also seldom sit down—most work is accomplished either standing up or walking around.

Take the ward round as an example. The ward round is performed by the ward round team—a physician and one or two nurses. A typical ward round at department T consists of a tour round the ward, where the physician and nurses visit the patients admitted here. The usual pattern is to alternate between three sub-tasks. First, the clinicians would *prepare* themselves for the visit. This includes browsing through the medical record, looking up if there are new answers to e.g. blood tests, and discussing how well the patient is doing in his or her overall treatment and care. This task involves very different information from the medical records, both paper-based and electronic. The main outcome of this task is a plan for what the next step in the patient's treatment and care would be. For example, a prescription of a drug or the need for a blood test. The second subtask involves *visiting* the patient at the bedside. This task involves a discussion of how the clinicians view the progress in treatment and care, as well a the patient's view on it. During this subtask, it is common to consult the medical record for looking up details in e.g. medication or to see what another physician might have written in the records yesterday. The third subtask involves *closing* the case for today, which involves making relevant drug prescriptions, ordering blood tests, requesting X-ray images taken, etc. It also involves making the relevant documentation in the medical records as to what has been decided and done.

Before the EPR system was introduced these three subtasks were typically done in close connection, the first one taking place in the hallway, the second one obviously at the patient's bedside, and the third one at the bedside or in the hallway again. In this way, the ward round team would walk from one patient to the next, finishing each patient at that time. The introduction of the EPR system, however, required the clinicians to use the PCs in subtask one and three, and they lost the connection to the medical record in subtask two. To avoid running back and forth between the patients' bedside and the PCs in the ward office, this caused the clinicians to stop walking around the ward, but instead forced them to stay in the ward office to prepare all the patients first, i.e. to carry out subtask one for all patients simultaneously. Then they would take the ward round, while making detailed notes on print-outs and notepads, and subsequently enter the ward office again to carry out subtask three for all patients. The physician would dictate an entry to the record to be transcribed later the same day by a secretary, and the nurse would need to type her information into the EPR system directly. It was a general complaint during our interviews and at the workshop to address this issue – as one of the nurses put it:

> *Before we got the EPR, I would have finished the task I was doing before I left the patient's room. Now I have to remember a lot in order to enter it into the system later.*

The introduction of the EPR system running on desktop PCs fits very poorly with this fast paced medical work. Today, in order to get access to the EPR system the user was forced to enter the ward office, sit down at a computer desk, log in and find the relevant data. This moves the clinician away from the hallway, the door opening, etc. where the job had happened before. A simple thing like having to sit down on an office chair all the time fitted poorly into the work.

Taking a closer look at the usage of the EPR system, one of the first and most obvious observatione at the ward was that logging in to a computer is, for many nurses and doctors, a tedious and highly awkward thing to do. Remembering usernames and passwords is just plain difficult even for experienced computer users and

typing them in, created a breakdown in the interaction with the computer, forcing the user to focus on the computer instead of his or her task at hand. The whole idea of using a normal desktop PC and arranging it for individual usage in the office seemed to fit very poorly with the way clinicians were working.

These problems are often worsened by the need for several different usernames and passwords for different computer systems. The problem of having numerous accounts to different computer systems, operating systems, web sites, etc. is well known to most computer users. At the hospital, the installation of the EPR system on Windows NT PCs created a double level of login; first level was the NT login and the second level was the login to the EPR system. Because the EPR system could not synchronize with the NT domain controller, the users had different logins for these two levels and had to type them in both places.

3.2 Medical work is nomadic while login is fixed to one computer

The ward round example above also illustrates how medical work is inherently mobile [4]. Clinicians of all kind are constantly moving around within their 'action-range'. For example, the nurses move around within the ward or the outpatient clinic, and the doctors within the whole hospital. The EPR system does not in any way support this mobile and nomadic nature of medical work and especially the login and logout procedures for the system caused a lot of inconveniences for the users when moving around. The login and hence the user session is always tied to a certain computer, which is located in a specific place and it is thus impossible to continue the work as the clinician moves around in the hospital or within the ward.

Consider the work at the ward, for example. Most activities involve walking between several locations—primarily the ward office (A + B), the medicine room (C) and the different patient rooms (E), but also the different rooms for clean and dirty equipment. It is no coincidence that the office and the medicine room are located in the centre of the ward (see Fig. 1). Take for example the nurse's task of handing out medicine. When a patient has been prescribed medicine, it is the duty of the nurse to ensure that the medicine is given to the right patient at the right time, in the proper way, and that the process is properly documented. This activity of handing out and documenting medication involves constant walking between the medicine room, where the nurse finds, prepares, and arranges the medicine and down to the patient's bedside, where the medicine is handed out. This task is repeated for practically all patients, four times a day and since the ward carries up to 30 patients, this task happens frequently; and several nurses carry out this task simultaneously.

The medicine schema for a patient is essential for performing this task of giving medicine. This schema contains the information of the medication, like the type of medicine, dose, frequency, and instruction for taking the medicine. The medicine schema is part of the EPR and thus 'located' in the computer. To access and use the medicine schema, the nurse would need to log in to a computer. And since the PC in the medicine room is too small for practical use, and because there is only one, she/he would necessarily have to use one of the computers in the office. Here she/he would find the patient, find his medicine schema and scroll to the relevant day and time and find the medicine and its details. She/he would log out, go to the medicine room, fetch the medicine, go to the patient's bedside, hand out the medicine and make some notes on a piece of paper. When finished at the patient, she/he would need to find a vacant computer in the office and transfer his or her documentation to the EPR system. Here the whole process of logging in and finding the patient and his medicine schema would be repeated in order for him or her to document the medication. Thus, the introduction of the EPR system has made the work of the nurse even more nomadic. Before, handing out of medicine involved walking between the medicine room and the patient room. Now, the route has become office – medicine room – patient room – office.

Clearly this is a rather cumbersome way of handing out medicine and taking the busy environment of a hospital into consideration, it is not surprising that the nurses have established a work-around to this tedious login and logout nightmare. Even though the EPR has been installed, they still use the 'old-fashioned' paper-based records. Now they just start every morning by printing out relevant data sheets from the EPR, especially the medicine schemas. These print-outs are used during the day as a mobile tool for the medication hand-out, including reading the prescriptions on the paper and documenting it directly, writing notes on the paper. Before leaving the ward in the afternoon, they now need to type in all the notes taken during the day.

3.3 Login contradicts the interrupted nature of medical work

The collaborative work among clinicians is often done in an ad hoc manner. There are, of course, scheduled medical conferences and operations; but a large part of medical work is established ad hoc as the situation calls for it. A typical situation is a patient calling the nurse because of pains, who then calls the physician on duty in order to have him prescribe some painkillers.

An unavoidable side-effect of the distributed and close collaboration among clinicians is that they often interrupt each other. In order for a clinician to establish a collaboration or communication she/he must often interrupt the other person in whatever she/he is doing. In the above example, the nurse interrupts the physician

who needs to suspend what he/she was doing when the phone rang, and to start a dialog with the nurse about the patient and his/her condition. Such a situation would often require the physician to look up the patient record or actually to go and visit the patient, distracting him or her even more from the original work activity.

Another classic example of interruption happens among nurses working in the medicine room (Fig. 3). They frequently cooperate by asking each other questions and by handing over the different medicine schemas. Hence, there is a high degree of interruption, but this is considered fruitful because it is a central part of a close cooperation.

Every time a user logs in to the EPR system, she/he gets the same start page—typically the list of patients admitted to the ward. Hence, when a user is interrupted, logs out and leaves the computer she/he has to start all over again upon return. To accommodate this problem, the EPR has a feature of locking the computer. However, only the user, who locked the computer, can unlock it again—leaving the computer literary unusable for anybody else. Because it was such a cumbersome task to log out and log in again, everybody would just lock 'their' computer. During the busy dayshift, this often created a huge bottleneck in availability of computer because the ratio was eight computers for 15 to 20 users. Furthermore, as described above, users tend to enter and leave the department constantly. Therefore, computers could stay locked by persons that no longer were at the department and it became a tedious and irritating job to locate these people and ask the person to come back to the department and unlock the computer. In its utmost consequence, the computer could be left locked and unusable for days, if the person using it had gone home. Furthermore, there is no support for the micro-mobility happening in the medicine room enabling the nurses to alternate between different user sessions. This is further discussed below.

Fig. 3 The Medicine Room – Nurses are preparing medicine for patients, while asking each other questions

3.4 Medical work is collaborative using shared material while login is intended for single user activities

Another fundamental aspect of the login concept is that it is personal. This is caused by the security need for traceability—the system should record (log) who is doing what. This personal login basically contradicts the fact that most medical work is collaborative-through the sharing of common material, like the patient's record.

For example, doctors and nurses would often engage in a conversation about the treatment of a patient just before the ward round. This conversation is accompanied by a collaborative browsing, reading and editing of the paper-based record. A nurse would, for example, describe a medication problem of a patient and the doctors would suggest that the patient is prescribed some other medicine. This frequently occurring interaction is easily supported by paper where the nurse would hand over the medicine schema and the doctor would just add the prescription and sign it by affixing his initials. Such kind of *micro-mobility* of paper-based material is common in medical work [15], because the physical properties of paper as being thin, light, flexible, opaque, and writable afford the human actions of grasping, carrying, folding, writing, and so on [20]. Figure 4a depicts a typical work situation where nurses and physicians discuss, share, and edit common paper-based material including the medical record.

In the computer-based record, however, this little task of handing over the medicine schema for additional prescription becomes highly awkward. Imagine that the nurse is using the computer having a patient's medicine schema shown. Because a nurse is not authorized to prescribe medicine she/he would need to log out and the doctor would need to log in, leading them away from the patient in question and back to the login start page of the EPR. Thus, before the doctor could initiate a prescription, she/he would now need to find the patient again, and navigate to the medicine schema, and scroll to the medicine in question. Now, if the nurse wants to use the computer again, she would need to start all over once more. A feature of the EPR system did, however, accomodate this work practice by enabling the nurse to prescribe medicine in the name of a doctor, who later could log in and approve this prescription. But this feature was primarily designed and used for situations where the physician was not present at the ward.

The real challenge arises when nurses and physicians are preparing for the ward round together in the ward office. In order to establish a shared workspace like the table in Fig. 4, they would use two or more computers as shown in Fig. 5. Here one of the nurses is logged in to the computer on the right-hand side of the picture, while the physician is logged into the computer on the left-hand side. This creates a rather awkward working situation, where the clinicians instead of facing a shared workspace (the papers on the table) now are turned away from each other. One might argue that this can be

Fig. 4 Medical cooperation between nurses and physicians sharing and editing various paper-based material

Fig. 5 Medical cooperation between two nurses and a physician using two computers in order to view different parts of the EPR

solved by simply arranging the monitors side-by-side, which some of them also are (see Fig. 2). The point here, however, is that the nurse and the physician are not working together on the shared material, which is handed over and edited by all involved persons. There is still no way a physician in the EPR system can do what corresponds to taking a pen and writing a prescription on the medicine schema that is currently on the nurse's monitor.

3.5 Login is being circumvented

The consequence of this tedious login schema is that it is being circumvented at department T. First, the NT login was circumvented by having one universal login used by everybody and the username and password for this login was written directly on all monitors on the ward. Second, it was widespread practice to 'borrow' a login from somebody by just handing over the keyboard and mouse to somebody to do a minor task without logout and login. This of course implies that the traceability is jeopardized. Third, usernames and passwords were frequently written in notebooks, on pieces of paper, and even directly on the monitors. And finally, passwords were often made easy to remember—a common strategy was to alternate between "123" and "456" as passwords whenever the system asked for renewal of passwords. These are well-known security problems [21], which are enlarged by the trouble of login to the EPR.

4 User authentication in ubiquitous computing

So far we have argued how a typical user authentication mechanism as a simple software component leads to considerable usability problems in the daily work at a hospital ward. The usability problems can clearly not be credited to the login mechanism alone. It is just a minor part of a complex computer system, and the usability problems discussed above have linkage into other aspects of such a typical client–server system design. Our aim here is, however, to put special focus on the design and usability of user authentication mechanisms, which is an often overlooked feature of a computer system.

Basically, a high level of security is necessary in the healthcare domain. The security parameters of identity, authentication, and traceability are fundamental

requirements to any computer system within healthcare. Being able to see who has entered what data—a prescription for example—is also of high importance usability-wise. Hence, the challenge is to design a computing infrastructure that fulfills this requirement.

Based on these observations, we have concluded that the conventional computer equipment seems more appropriate for office use rather than for medical work in hospitals. We argue that the concepts, designs, and technologies within ubiquitous, pervasive, and mobile computing can significantly improve computer support for clinical work, including the close cooperation taking place in e.g. a hospital. Another important part of our research is therefore to constructively design, implement and evaluate new types of pervasive computing support for healthcare [9]. However, just as pervasive computing technologies might offer some new opportunities, it introduces at the same time new design challenges—including challenges for new kind of computer security. Because security in general, and user authentication in particular, is fundamental to healthcare systems, we have to consider this 'login challenge' within our design.

In our design of new user authentication mechanisms, we have put special emphasis on four things: (1) to support *proximity-based user authentication*, where users are logged in by just approaching a display, (2) to support *silent login* where users can seamlessly alternate between being logged in, (3) supporting *migrating user sessions*, enabling users to carry with them their work on the move, and (4) to support *suspendable user sessions*. Our current research into the design of a basic pervasive computing infrastructure for hospitals (and other settings) pivots around our activity-based computing (ABC) infrastructure. See [3,9] for details.

The ABC framework has been emerging during a two year period. It has been developed in close cooperation with clinicians (physicians and nurses) having their daily work in hospitals. We have conducted 11 design and evaluation workshops, each lasting a whole day, where clinicians were asked to co-design, use, evaluate, and test the framework. A common method in our design workshops was to let the clinicians role play a number of clinical scenarios, while using and EPR build on top of the ABC Framework. In addition, we conducted four whole-day evaluation workshops with clinicians who never had seen the ABC Framework before nor had been introduced to the concepts of activity-based computing. The pictures in Figs. 6 and 7 were taken at these workshops. User authentication was a recurrent theme at all the workshops, and the following sections describe the current design in the ABC Framework.

4.1 Proximity-based user authentication

Looking back at the findings at Department T, there are numerous occasions where the login procedure caused focus shifts or breakdowns in the use of the EPR. There are some basic problems in typing and remembering usernames and passwords. Various solutions to this 'problem' exist. The use of smartcards can be used as a combined identification and authentication token. Most smart cards can log in the user (identify and authorize) when the card is inserted in the reader. However, as a physical token smart cards are subject to be lost or stolen. Hence, when smart cards are used in hospitals, users are still required to type a password when inserting the card.

The use of biometric systems is an appealing solution to the trouble of typing usernames and passwords. By using biometric systems people can be identified by something they *are* instead of something they *have* (e.g. a smart card) or *know* (e.g. their password). Several commercial biometric solutions already exist, including ones that combine a smart card with a fingerprint reader. A common way of testing a biometric system is to measure the tradeoff between the *false-acceptance rate* (FAR) (the percentage of imposters incorrectly matched to a valid user's biometric) and the *false-rejection rate* (FRR) (the percentage of incorrectly rejected valid users). This tradeoff is still rather high for most systems, leaving us to choose whether we want a highly secure system, that rejects a lot of valid users, or a more useful system that potentially can allow incorrect access to imposters (see e.g. the test report from the British CESG authorities [16]).

In the design of the ABC Framework, our original vision was to log in users as they approach the computer [2] without forcing the user to find and insert a smartcard into a reader, or having the user to place a finger somewhere or look into an iris-scanner for biometric identification. In a hospital setting this is appealing for hygiene reasons eliminating the need for potential dirty smartcards or having a surgeon all dressed up to remove his gloves to place a thump on a fingerprint reader (which by the way would be subject to distributing many bacteria). We call this principle *proximity-based user authentication*. In our current implementation [5] we have, however, introduced a physical token. During our design workshops and working with the design, we discovered that it was preferable that users made an active gesture in order for them to log in, and not log in a user just because she/he was standing next to a monitor. Hence, we designed a *Personal Pen* that a clinician would carry around, and use as a pen on the displays scattered around the hospital. Embedded in this pen is a Java Card, which work as an encryption engine for user authentication. We use contactless smart card readers to access this embedded Java Card and the user thus does not need to insert anything into a reader of any kind. A nurse using a personal pen during one of our design workshop is shown in Fig. 6.

Instead of asking the user to verify his or her ownership of the pen by typing in a password or pin code, we use a context-awareness system to verify the user's location. Hence, by tracking the location of users in the hospital we have separated the user authentication into

Fig. 6 A physician is using a wall-based display in a conference situation. In her hand she is holding a *Personal Pen*, which is used to authenticate her to the computer. An active badge woven into her white coat (not visible) is revealing her location to a context-awareness system

two independent mechanisms, thereby maintaining a high level of security. A detailed security analysis can be found in [5].

4.2 Silent login: support for co-located cooperation

Another central aspect of medical work that needs to be addressed in design of a pervasive healthcare system is the cooperative character of most work at a hospital. Looking specifically at the login problems described above, we observed that a fundamental problem with the conventional login schema is its personal nature. Hence, when nurses and doctors hand over paper and medicine schemas to one another to read and annotate, this micro-mobility is not supported by the EPR system. From a usage point of view we would like to have a kind of 'shared login' where several people, like the doctor and the nurse discussing medication, can be logged into the same computer at the same time. However, this would jeopardize the fundamental requirement of traceability—it is very important that the activities of each individual are logged for later retrieval. For example, looking up the name of the doctor who made a prescription.

To solve this apparent conflict between wanting a shared, but still personal login we can return to the paper-based world for inspiration. How was this task accomplished when using the paper-based medical record? In this case the doctor and nurse would spread out all the paper on a table and if a person would move, remove, add, or relocate a piece of paper, this was obvious for everybody participating. And they would have an ongoing conversation while manipulating the documents. If something needed to be added to a piece of paper, a prescription on the medicine schema for example, the doctor would take the paper and use a pen to add the information and sign it with his initials. This signature was recognizable for most parties involved.

In our current design, we imitate this process in the computer system. The user sessions introduced above have been created in a way so that several persons can participate. All participants would have access to this shared user session and can manipulate whatever the session is displaying.

When clinicians are gathered around the same computer—which is often the case in clinical conferences—there is a need for them to participate in the work activity in turn. In this situation we use the Personal Pen described above, but we do not log out one user and log in another. We simply keep the users' session running and 'silently' tell all applications involved in the session that there has been a change of user. The users seldom see any fundamental changes at the display, depending on the specific application. For example, in the EPR system, the only visible change when shifting from a physician to a nurse is that the 'ordinate medicine' button is disabled. We call this mechanism *Silent Login* and can be conceived as a windows-based parallel to the Unix command 'su <username>'. Figure 7 is a picture from one of our evaluation workshops. It illustrates how a group of clinicians are gathered around an interactive conference table participating in a shared user session. They can each 'silently' log in to the session and participate. For example, the physicians can prescribe medicine and add notes to the medical record, whereas the nurses can document the hand-out of medicine, or add comments to the nursing record.

Now, one could argue that silent login is still turn-taking just in a more quite way. We partly agree, and a design vision is to support several users each having their own pen, using it to write simultaneously. In order to support this scenario, we are struggling with the basic

Fig. 7 A group of clinicians is gathered around an interactive conference table for a team conference. They all participate in the session running on the table and can hence 'silently' be logged in and edit medical data according to their credentials in the EPR system

limitation of having just one pointing device per computer, one event queue, and singular focus in e.g. text fields, scrollbars, etc. Solutions to this is, however, being researched [7, 10].

4.3 Migrating user sessions: support for mobility

As can been seen from the descriptions above, a core aspect of medical work is its nomadic nature. Hence, the overall trouble with login is not as such to type in a username and password, as inconvenient that might be, but the fact that the user session needs to be reestablished whenever a user moves between locations and hence computers. Strictly speaking, these problems are not part of the user authentication mechanisms, but more an issue of user session management. However, these problems were conceived by the clinicians as part of the 'trouble with login' because they needed to reestablish their user session every time the logged into a new computer. Hence, we want to address these issues of user session management for mobile and nomadic users as part of the user authentication mechanisms in ubiquitous computing.

Basically, there are two solutions to this problem—either equip the hospital staff with mobile computers, like PDAs or Tablet PCs, or equip the hospital with computers located in relevant places and create a computing infrastructure that enables the user to move around while preserving their user session. We have experimented with both solutions. The mobile solution can alleviate some of the problems by providing specific support for isolated tasks, like documentation of medicine at the bedside. However, in many situations, a small device as regards to display size and computing power like the PDA is simply not sufficient to display and process the large amount of data involved in an electronic patient record. It is, for example, very difficult to have an overview of the result of a blood test or to look at an X-ray image on a PDA. Tablet PCs were considered too large and bulky, not fitting into a pocket in a white coat. Clinicians need to have their hands free for e.g. examination of patients and for handling medicine.

Therefore, we have also designed what we have termed *public computers*, which are scattered around the hospital for hospital staff to use as convenient. Public computers range from small PDA type of devices, workstations, computers built into the bed and into conference tables (Fig. 7), to large wall-size displays in conference rooms (Fig. 6). A user's session can be stored in the basic infrastructure and it follows the user around in the hospital being restored as the user logs in. Central to our design is what we have termed *application roaming* where a user's session, including the application the user is engaged in, can be 'roamed' between various public computers [3]. One concrete implementation is to transfer an ongoing session from a PDA to a desktop PC by using the PDA's barcode scanner and scan a barcode on the PC (see [6] for details).

4.4 Suspendable user sessions: support for interruptions

A final aspect of medical work, which puts up implication for the design of login systems, is the way that clinicians are constantly interrupted and need to alternate between many different tasks and activities.

In line with the idea of having a user session stored and hence distributed centrally, an infrastructure can allow the user to have multiple user sessions going on at the same time. These user sessions can be suspended and resumed on the same computer, on a different computer, or they can take place simultaneously on several computers. In clinical situations, when the user is interrupted, she/he can suspend the current user session, create a new one for the new task and when done, restore the last one. Furthermore, the user can carry on with his or her task on other devices (cf. the mobility aspect above).

5 Conclusion

The paper has discussed the relationship between clinical cooperation, usability and computer security.

From a usability point of view, we have described how the conventional login procedures caused considerable usability problems. From our field study of the EPR system at department T, we have seen how a range of usability problems can be associated with the system's login mechanism. We argue that many of these problems arise because technology designed and developed for the office environment is transferred without modification to the hospital setting. This is reflected in the design of the system, for example by using conventional username and passwords for login and the feature of individual locking of PCs, as well as in the arrangement of desktop PCs for individual use in the ward office (c.f. Fig. 2). We have demonstrated 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.

From a security point of view, we argue that our empirical case has demonstrated that usability cannot be ignored when addressing computer security. A highly secure system from a technical point of view can be made insecure if the authentication mechanisms are difficult or tedious to use [1, 19]. The result is that users find ways to circumvent and shortcut the security system, which leads to vulnerable systems.

We have introduced our design and current implementation of new ways of handling user authentication in our activity-based computing infrastructure. Here emphasis was put on enabling (1) proximity-based login, allowing a user to be authorized to the system by just approaching a display, (2) silent login, where several users can seamlessly alternate in using a display built-into, e.g. a table, (3) migrating user session, which could support the mobile work at a hospital, and (4) suspendable user session, allowing users to alternate

between several tasks, when interrupted. We have implemented these principles in our ABC infrastructure and these have been subject to user evaluation during a number of workshops in our lab at the university.

The findings from our studies of medical work and the design of new user authentication mechanisms presented in this paper have concentrated on our research within healthcare. We would, however, argue that the aspects of mobility, cooperation, interruption, and sharing of material are core aspects of much real-world work as also demonstrated by numerous studies in the CSCW literature. Such aspects play an increasing role these years as we are turning to ubiquitous computing with its overall concept of creating computer support that enables the user to move away from the office with its desktop computer. We cannot avoid addressing the fundamental usability challenges in login and authentication of users, if this vision is to become viable.

Acknowledgments The field study of department T was done together with Christina Nielsen and Thomas K. Kjær. We are grateful to the clinicians at department T for participation in this work. The Danish Center of Information Technology (CIT) funded this research.

References

1. Adams A, Sasse MA (1999) Users are not the enemy. Commun ACM 42(12):40–46
2. Bardram J, Bossen C, Lykke-Olesen A, Nielsen R, Madsen KH (2002) Virtual video prototyping of pervasive healthcare systems. In: Proceedings of the conference on Designing interactive systems. ACM Press, pp 167–177
3. Bardram JE (2004) Activity-based support for mobility and collaboration in ubiquitous Computing. In: Baresi L (ed) Proceedings of the 2nd international conference on ubiquitous mobile information and collaboration systems (UMICS 2004). Lecture Notes in Computer Science, Riga, Latvia, Sept. 2004. Springer-Verlag, pp 169–184
4. Bardram JE, Bossen C (2003) Moving to get aHead: local mobility and collaborative work. In: Kuutti K, Karsten EH, Fitzpatrick G, Dourish P, Schmidt K (eds) Proceedings of the Eighth European Conference on Computer Supported Cooperative Work. Helsinki, Finland, Sept. 2003. Kluwer Academic Publishers, pp 355–374
5. Bardram JE, Kjær RE, Pedersen MØ (2003) Context-Aware User Authentication—Supporting Proximity-Based Login in Pervasive Computing. In: Dey A, McCarthy J, Schmidt A, (eds) Proceedings of UbiComp 2003, volume 2864 of *Lecture Notes in Computer Science*. Seattle, Washington, USA, Oct. 2003. Springer Verlag, pp 107–123
6. Bardram JE, Kjær TK, Nielsen C (2003) Supporting Local Mobility in Healthcare by Application Roaming among Heterogeneous Devices. In: Chittaro L (ed) Proceedings of the Fifth International Conference on Human Computer Interaction with Mobile Devices and Services, volume 2795 of *Lecture Notes in Computer Science*. Udine, Italy, Sept. 2003. Springer Verlag, pp 161–176
7. Beaudouin-Lafon M, Lassen HM (2000) The architecture and implementation of CPN2000, a post-WIMP graphical application. In: Proceedings of the 13th annual ACM symposium on User interface software and technology. ACM Press, pp 181–190
8. Burkhardt J, Henn H, Hepper S, Rindtorff K, Schack T, Schaeck T (2002) Pervasive Computing: Technology and Architecture of Mobile Internet Applications. Addison-Wesley, 1st edn, 2002
9. Christensen HB, Bardram JE (2002) Supporting Human Activities – Exploring Activity-Centered Computing. In: Borriello G, Holmquist LE (eds) Proceedings of Ubicomp 2002: Ubiquitous Computing, volume 2498 of *Lecture Notes in Computer Science*. Göteborg, Sweden, Sept. 2002. Springer Verlag, pp 107–116
10. Dietz P, Leigh D (2001) DiamondTouch: a multi-user touch technology. In: Proceedings of the 14th annual ACM symposium on User interface software and technology. ACM Press, pp 219–226
11. Flechais I, Sasse MA, Hailes SMV (2003) Bringing Security Home: A process for developing secure and usable systems. In: Proceedings of the 2003 Workshop on New Security Paradigms. ACM Press
12. Jain A, Hong L, Pankanti S (2000) Biometric identification. Communications of the ACM 43(2):90–98
13. Jordan B (1996) Ethnographic Workplace Studies and CSCW. In: Shapiro D, Tauber M, Traunmüller R (eds) The Design of Computer Supported Cooperative Work and Groupware Systems. Elsevier
14. Kensing F, Halskov Madsen K (1991) Generating Visions: Future Workshops and Metaphorical Design. In: Greenbaum J, Kyng M (eds) Design at Work: Cooperative Design of Computer Systems. Lawrence Erlbaum Associates, Hillsdale, NJ, pp 155–168
15. Luff P, Heath C (1998) Mobility in collaboration. In: Poltrock S, Grudin J, (eds) Proceedings of the 1998 ACM conference on Computer Supported Cooperative Work. ACM Press, pp 305–314
16. Mansfield T, Kelly G, Chandler D, Kane J (2001) Biometric Product Testing. Final Report. Technical Report CESG contract X92A/4009309, CESG – The National Technical Authority for Information Assurance, Centre for Mathematics and Scientific Computing, National Physical Laboratory, UK, 2001. Available from http://www.cesg.gov.uk/
17. Norman D (1981) The Trouble with UNIX. Datamation, 27(7)
18. Patton MQ (1990) Qualitative Evaluation and Research Methods, 2nd edn. Sage Publications, London
19. Schneider B (2000) Secrets and Lies : Digital Security in a Networked World, 1st edn. John Wiley & Sons
20. Sellen AJ, Harper RHR (2001) The Myth of the Paperless Office, 1st edn. MIT Press
21. Sundhedsstyrelsen (2002) IT-sikkerhedsvejledning for sygehuse (IT Security Recommendations for Hospitals). Technical report, Sundhedsstyrelsen (The Danish Health Authorities), Copenhagen, Denmark, 2002. Available from http://www. sst.dk/
22. Tanenbaum AS (2001) Modern Operating Systems, 2nd edn. Prentice Hall
23. Weiser M (1991) The Computer for the 21st Century. Scientific American 265(3):66–75
24. Zurko ME, Simon RT (1996) User-centered security. In: Proceedings of the 1996 workshop on New security paradigms. ACM Press, pp 27–33