The impact of authentication on health digital resources

Anne Adams
UCLIC
Remax House, 31 – 32 Alfred Place
London. WC1E 7DP
+44 (0)20 7679 5288
a.adams@cs.ucl.ac.uk

ABSTRACT

Security is a major issue within the health domain. It is important to ensure that sensitive personalised data is protected from misuse. However, there is also a need for efficient medical systems that don't impede clinicians work practices. This paper will briefly detail some of the authentication issues that have been highlighted within two comparative hospital studies in the health domain. 93 clinicians' perceptions towards clinical information resources were analysed whereby security and authentication issues were highlighted as a critical issue. This paper details how those issues related to organisational structures and discusses how authentication and security must be designed around communities of practice.

Categories and Subject Descriptors

H.1.2 [**User/Machine Systems**] *Human factors*; H.5.2 [**User Interfaces**] *Ergonomics, Evaluation/methodology, User-centered design*.

General Terms

Design, Experimentation, Human Factors.

Keywords

Patient Health Information, Digital Libraries, User Studies

1. INTRODUCTION

With the growing use of online and mobile systems in the clinical domain there is an increased importance of security issues. The culture of the security domain determines the type of security problems identified and the approach to potential solutions. Historically, the security discipline has focused on malicious intruders and technological solutions rather than users' perceptions, usability issues or the organisational role. This focus produced technical solutions that were both unusable and inappropriate.

Technological developments are increasingly focusing on the importance of directing design towards the work practices and communities they support [7]. Supporting communities of practice can assist the development of effective ways to share knowledge across organizational boundaries, thus promoting collaboration and coordination while also increasing productivity and organizational performance [9]. This is of particular relevance to the development of digital library resources that support and develop communities. Within the clinical domain, in particular, social structures and informal community practices are paramount to the smooth-flowing of clinical systems [12]. Security systems however often clash with the concept of communities as audit tracking and individually identifiable actions take precedence.

Authentication, in particular is an important security mechanisms especially with regard to clinical digital libraries [2]. However, there are different drives behind these mechanisms within the educational and clinical domains. Within the educational domain digital library authentication is driven by economic needs to pay for resources developed. However, within the clinical domain authentication is driven by issues of confidentiality and integrity of data sources. Within hospitals these two domains frequently meet through ongoing training, education and evidence based medicine. This paper highlights how within two comparative hospitals security processes (primarily authentication mechanisms) caused usability and cultural clashes through hospital communities of practice.

2. BACKGROUND

Security, in general terms, is often taken to mean *protection from danger*. With regard to computer security, that danger relates to malicious or accidental misuse [11]. Computer security, therefore, tends to concentrate on human misuse rather than computer malfunctions. Two important aspects of security are *confidentiality* and *integrity*. Confidentiality is concerned with the protection of information from unauthorised access, while integrity refers to maintaining the unimpaired condition of both the system and the data used. Both confidentiality and integrity closely relate to the endeavour of making sure that misuse does not impact on computer reliability. Ultimately, security seeks to ensure that learning resources are available, unimpaired, to all authorised users when they are needed. To maintain the commercial viability of digital libraries it is therefore vital to ensure that the people who pay for services have access while other non-authorised users are excluded. To retain this access to unimpaired data it is necessary to deal with issues of authentication and ownership. It is essential that the appropriate people have access to information with the correct data manipulation rights.

2.1 Authentication

With sensitive information, such as patient data, it is crucial that security procedures are in place. Authentication is pivotal to the concept of confidentiality but it also relates to integrity. To maintain appropriate access to information, and yet protect it from unsanctioned manipulation, it is crucial to accurately authenticate users.

Authentication procedures are usually divided into two stages. The first *user identification* (User ID) stage identifies the user interacting with the system. As it is merely a means of specifying who the user is, this ID does not have to be secured. Once the user is identified the second *user authentication* stage verifies them as the legitimate user of that ID. The means of authentication, therefore, must remain secret.

There are three different ways to authenticate a user [8]:

1. Knowledge-based authentication: The user *tells* the computer something only they know. (e.g. password).
2. Token-based authentication: The user *shows* the computer something only they possess (e.g. a key card).
3. Biometrics: The user themselves is *measured* by the computer (e.g. fingerprint).

Security research has tended to concentrate on technical mechanisms for authentication (e.g. iris-scanning, smart-cards). However, although these technologies have potential in future applications, passwords and Personal Identification Numbers (PINs) are currently the most widely used form of authentication. Even where the other forms of authentication (i.e. token-based or biometrics) are used, they are invariably reinforced by the use of a PIN or password. Knowledge-based authentication has the advantage of being both simple and economical. These two factors probably account for their universal appeal and ensure their use for many systems and years to come.

One of the problems with popular knowledge-based authentication mechanisms, such as passwords and PINs, are their poor usability. Current mechanisms rely on users to recall data to be input rather than recognising the correct authorisation information. To counteract these problems there are a wide variety of knowledge-based authentication mechanisms that claim to be more usable and yet secure:

- Passphrases (a phrase required instead of a word);
- Cognitive passwords (question-and-answer session of personal details);
- Associative passwords (a series of words and associations) and
- Passfaces (user selection of faces)

However, the take-up of these mechanisms has, to-date, been limited [14]. One-word passwords and PINs are still the easiest and cheapest to apply and thus most often implemented.

2.2 Clinical social structures & DLs

The effectiveness of security policies and applications have been noted as strongly intertwined with an organisations social structures [5]. Communities of practice and social structures within organisations can have a strong impact on the day to day working practices of work-based communities [18]. Within the clinical domain, communities of practice exert a strong influence on both formal and informal work practices [3]. The clinical domain also presents interesting security issues (e.g. highly sensitive data) because of rapid technological developments that are designed to support effective clinical decision making (e.g. telemedicine, electronic healthcare records). However, the hospital setting, in particular, is very hierarchical in nature, and many users have negative perceptions of technology, poor IT skills, little flexible time, and poor access to technology and support [4].

The diverse organisational culture of hospital structures, made up of many different professions with their own specific social identifiers, can often produce conflicts between those professions [10; 13; 17]. Symon *et al* [16] found conflicts within a clinical setting relating to social status and information practices. For example, higher status professionals were found to be more concerned with keeping their social status as an expert within the organization than adhering to formal organisational norms. How social and organisational structures impact upon security systems is a poorly researched area which this paper seeks to rectify.

3. METHOD

The focus of this paper is on how security and communities of practice relate to findings from the clinical domain, and, in particular, from studies conducted in two large teaching hospitals. The organizational structure of both hospitals studied is complex, hierarchical and undergoing dramatic change. Funding restrictions mean facilities are limited and under-resourced. Technology provision varies greatly; however, the majority of clinicians do have access to a computer, even if that computer is shared. Most end-users have limited computer skills, although abilities vary quite dramatically. Many clinicians are resistant to change, particularly technological change; this resistance is due largely to a poor understanding of how applications can support, rather than hinder, current working patterns.

The qualitative data collected through in-depth interviews, focus groups and observations were analysed using a grounded theory approach [15]

	Job	**Status & Role**	**No**	**Web-based information resources used**
Provincial Hospital	Clinicians, Nurses etc.	Nurses, Consultants, Managers, Library, IT & Security staff	20	Medline, the Cochrane library and the UK National electronic Library of Health (NeLH), Specialist web-sites, Department of Health web-site, GOOGLE to search the web.
Inner City Hospital	Nurses	Pre-Registration & Registered	36	
	Clinicians etc.	Doctors, Consultants, Surgeons, AHPs, IT & managers	37	

Table 1. Participant descriptive data

3.1 Hospital study 1

Study one was conducted in a provincial teaching hospital. In this hospital, most of the computers were in offices and the library, and allowed access to the web. There were still some dumb terminals on the wards that provided access to specific administrative applications. Security was not only initiated by national directives but also by local issues, and implementation was driven by the privacy officer and security team. 20 in-depth interviews were used to gather data from clinicians (i.e. nurses, consultants etc.) management, library and IT staff (see table 1).

3.2 Hospital study 2

The second study was based in a London teaching hospital. In this hospital, computers have been placed on the wards, with web-accessible digital libraries. Security was directed by national directives. However, community specific issues were not identified and security and privacy issues were low on the local agenda. Focus groups and in-depth interviews were used to gather data from 73 hospital clinicians. Approximately 50% of the respondents were nurses while the other 50% were junior doctors, consultants, surgeons, Allied Health Professionals (AHPs; e.g. occupational therapists), managers, and library and IT department members (see table 1).

4. RESULTS

Within both the studies many of the clinicians proposed that digital libraries were a key element in enabling them to develop effective information management strategies. Previous hard copy management strategies required the user to frequently identify their current, imminent and future information needs for each journal they subscribed to. This meant frequent reading and re-reading of journals, sorting, cutting out and filing of relevant sources. Electronic libraries enable these users to dramatically simplify this process by speeding up the search, selection and filing procedures. For example:

> *"... then you want to look back and of course in looking back you've always lost the paper copy so then you mean to go across to the library and you don't get across to the library. Whereas electronically it's easy."* **(Doctor)**

4.1 Authentication and social structures

The use of passwords to access online resources anywhere and at any time can increasing the potential of digital libraries in supporting evidence based medicine. However, the practicalities of implementing password systems have serious usability problems. Initially there are issues of awareness and education around password distribution

> *"But I must say that if it's on the computer if you have not been educated in how to use the computer like a study day how to access the computer, which number to use, and your password and everything. You can't access the computer. Maybe its there but you don't know how to access it."* **(Nurse)**

Awareness about obtaining and using passwords was identified as a major barrier to information access for some authorized users.

> *"They work on the wards but they don't know the passwords on the wards so it's something to do with access which is something of an issue."* **(Allied Health Professional)**

Within the Inner London hospital (study 2) studied most senior clinical staff were unaware of these problems and saw authentication as a clear benefit to protecting information access to increase possible usages:

> *"...so you could say I work for the ******** hospital here is my password I want to know what the hospital thinks about bleeding or what-ever..."* **(Surgeon)**

The IT department, within this hospital, were eager to increase computer accessibility, and had negotiated Internet access for all users within the organisation. A national directive had, at the same time, dictated that everyone from a janitor to a consultant should be given access to email accounts. However, the practicalities of implementing password systems entailed problems.

> *"At the moment we don't have a way of individually passwording our Internet access which is available easily. So its completely free access and the non-exec managers board we're quite happy for that to happen on the basis that it would increase usage."* **(IT Department member)**

However, when clinicians (other than senior doctors) were interviewed, their understanding of when and how they could access the Internet was poor. Senior clinicians were noted as using this poor authentication awareness and social structures as a barrier, for more junior clinicians, to accessing medical knowledge. For example, one nursing manager detailed a long procedure that she had be told by senior staff to go through to be granted a password for Internet access.

> *"I have access because I'm studying for a further PhD anyway and I think this job is where I actually need that information so I have access but it had to be granted by the director ... As things stand at the moment 4 pieces of paper had to be signed before I could actually get it."* **(Nursing Manager)**

Once she had a computer and Internet access, she was then not aware that this access was unlimited, and consequently restricted her usage to out of office hours

One contributing factor could be this hospital's current information hierarchy (i.e. information only for those of a higher status). This was found to limit perceptions of who should be using the technology, what it is used for and general computer awareness. The approach by some senior staff of information hoarding was identified as being associated with that of technology hoarding. Nurses' and AHPs' (i.e. Allied health professional e.g. physiotherapist, nutitionists) access to current technology within the hospital was limited by either physical or social restrictions (e.g. passwords, computer locks, location of computers).

> *"... But they put a block down on that because they've said 'well if one student nurse gets to use it then all the student nurses will want to use it'."* **(pre-registration nurse).**

A clear problem identified within this hospital (study 2), was one of poor communication between the IT department and end-users on the multitude of different authentication procedures required. Poor awareness was compounded by different procedures for different systems. The Internet was freely available from specific computers (with registered IP addresses), the library systems were authenticated through external bodies with passwords (There were several required for different systems) obtained and supported by the library services, the email system required 2 passwords and was administered and maintained by the IT department. Department specific systems would often have associated passwords specific to that system.

> *"The new ***** email actually has to have a 2nd password as well as the first."* **(IT Department member)**

Users noted solutions such as single sign-on.

> *"Maybe we could use our own passwords that we have already to access. You know just have it sort of tagged on somehow – tagged onto the code"* **(Nursing Manager)**

However, the practicalities of these mechanisms are associated with those of inter-operability and a multitude of systems in the health service that simply do not talk to each other.

> *"single sign-on will reduce the number of passwords and identity and is something we would like to get to but the practicality of getting there is rather difficult."* **(IT Department member)**

4.2 Authentication and clinical resources

As noted above authentication can be seized by different communities as a means of restricting access to user groups who, although authorised users, are outside of the accepted hierarchical structures. Easy access to digital libraries for authorised users is essential if evidence based medicine is to be achieved. Awareness, as these studies have identified, is a serious barrier to usage. One solution to problems of local awareness is to increased perceived ownership for resources with local champions who will advocate and promote usage within their hospital. However, who they promote usage to is an interesting question as the opposite side of community ownership is exclusion for non-members of that community. Within the Inner city hospital there is an example of how community ownership can produce exclusivity when designing systems.

In study two the hospital was developing its intranet to allow access to local information and to provide a portal to the Internet and online resources. Politically, there was an established 'pecking order' of what information could appear on high-level pages within the intranet. It was discovered that one top-page link presented the name 'OVID' without any explanation of what it was. OVID is a digital library authentication mechanism used to verifying access to hospital employees rather than the public in general. The link had been championed by a top-ranking clinician who liked the service, as did his colleagues. The link took the end-user through to an authentication page used to restrict access to hospital personnel regardless of whether they were accessing the site from the hospital or home. However, the authentication page provided no feedback on what the resource was for or how to get support for the authentication process (e.g. where to obtain passwords from, or explaining the difference between user ID and password). Screen real-estate restrictions on the top-page stopped IT services from providing more information for the link. Background information and support links could be provided on the authentication pages (which was the resulting compromise). However, potential users who did not know what OVID stood for were unlikely to access this link in the first place. It was suggested that contextualizing the link within the library service pages would support users' understanding of it (e.g. what the service is likely to be, who is likely to support it and provide passwords). The library, however, was considered of too low a standing to be represented on the top page of the intranet. The usability of the OVID authentication (security) feature was compromised by the tension between the status of the sponsoring clinicians and that of the library within the organizational structure. Those championing the service saw it as a resource for their status equivalent peers and promoted it as such. This is an example of how necessary security mechanisms can be misused in order to maintain differences in power between individuals with differing status. Increasing authentication usability may be easier in theory, out of context, than within organizational settings.

Poor ownership of access rights to sensitive data can cause problems with the acceptability of those processes. Within study one restricted access produced a violent clash between one community of practice (in this case, clinicians as users of patient data) and another (the security team). Users within other domains might have circumvented procedures they felt were inappropriate, but these clinicians often expressed their dissatisfaction directly and actively. One incident, described by the privacy officer, concerned a computer room that contained very sensitive data. The room was only accessed by clinicians but it was at the end of a corridor occasionally accessed by the public. The IT department decided that as this data was particularly sensitive there was a need for increased security for this room. The security for the door to the room was therefore increase to be one that automatically closed and locked. All the relevant clinicians were provided with keys and informed of the reason for this new procedure being put in place. Some clinicians, however, felt this change in practice was 'paranoid' and uncalled for and argued against it. Subsequently the locked office door was found kicked down.

> *"...I had a problem with the clinician stamping their feet, kicking the door in, swearing at me"* **(Privacy Officer).**

Although the vandal(s) were not identified, consultations between the IT department and clinicians resulted in the computer room and its security (i.e. locked door) being reinstated. Poor consultation and a perceived 'high handed' approach was identified as the main problem. New processes (e.g. committees, email debates) to communicate between the hospital and IT staff was a direct result of this episode.

5. DISCUSSION

This paper details the findings from two studies within comparative hospitals. Although those studies aimed to uncover issues related to digital resources and organisational structures there were some noteworthy security issues uncovered. In this paper I have reviewed authentication issues within two hospitals and their relationship to communities of practice. The results revealed that poor communication practices and social structures can reduce awareness of authentication and access procedures. This can results in some user groups being excluded from resources as senior clinicians use security mechanisms in a socially divisive way.

As highlighted in the introduction communities of practice are important within any organisation [9, 18]. Within the clinical domain, social structures and informal work-practices have been widely recognised as being central to effective operation. Reddy and Dourish [12] identify one of the limitations of information technology in this domain is the way they take tasks out of context. Similarly, security mechanisms often ignore important contextual factors. Multiple clinical systems with authentication mechanisms and frequent change regimes increase the users' mental workload when it may be dangerous to do so. Single sign-on is reviewed as a solution, by different user groups, but the poor interoperability of clinical systems restricts the practicality of this option. Adams and Sasse [5] also highlight the difficulties created by people having individual passwords in a group working context. This study has highlighted the need to understand users' work practices and the relevance of these within the context of communities of practice.

Communication and online feedback of authentication procedures is highlighted as an important factor in increasing security usability [5]. One approach to increasing digital resource awareness and communication within clinical setting is to have local champions. However, this study highlights that community based DL champions often have their own agendas working against open access for all clinicians. It is clear, though, that poor communication about security policy changes can lead to clashes with communities and their informal working practices (e.g. locks on doors to sensitive data computer rooms, see results section). A reasoned account of this user reaction can be found in the 'control and feedback' privacy approach [6]. This highlights that there is a need for further research in this area as the balance between individual privacy and community sharing become a key issues in online security [1]. The clinical domain, in particular, requires immediate solutions as security and online sharing increase in importance.

6. Acknowledgements

Part of this work is funded by ESRC grant RES-335-25-0032. I am also grateful for the help and support of all the participants who took part in this study within both the hospitals.

7. References

[1] Ackerman, M. S., Darrell, T. and Weitzner, D., (2001) Privacy in Context. Human Computer Interaction. 16.2/4. 167-176.

[2] Adams, A. & Blandford, A (2005) "Bridging the Gap between Organizational and User Perspectives of Security in the Clinical Domain" *International Journal of Human–Computer Studies*. 63. 175 - 202.

[3] Adams, A., Blandford, A & Lunt, P. (2005) "Social empowerment and exclusion: a case study on digital libraries" *ACM Transactions on Computer–Human Interaction*. ACM Press. 12.2. 174-200

[4] Adams, A. & Blandford, A. (2004) 'The unseen and unacceptable face of digital libraries.' International Journal of Digital Libraries. Springer-Vrelag, Heidelberg. 4 (2) 71-81

[5] Adams, A. & Sasse, M. A (1999) "The user is not the enemy" in Communications of ACM. ACM Press Vol. 42 (12) pp. 40 – 46 (Dec. 1999) Republished [2005] by O'Reilly books 'Designing Security systems that people can use' (ed. Cranor, L. & Garfinkel, S.) as a 'Seminal paper' in the field of HCI and Security

[6] Bellotti, V. and Sellen, A., (1993) Designing of privacy in Ubiquitous computing environments, in proceedings of ECSCW'93, the 3rd European Conference on Computer-Supported Co-operative Work", Kluwer (Academic Press), 77-92.

[7] Covi, L. and Kling, R. (1997). Organisational dimensions of effective digital library use: Closed rational and open natural systems model. In Kiesler, S (Ed.) *Culture of the Internet*. Lawrence Erlbaum Associates, New Jersey. 343-360

[8] Garfinkel, S. & Spafford, G. (1996): Practical Unix and Internet Security. 2nd Edition. O'Reilly and Associates.

[9] Millen, D. R., Fontaine, M. A and Muller M. J. (2002) Understanding the benefit and costs of communities of practice. In Communications of the ACM. Vol. 45 (4), 69-73

[10] Morgan, G.,(1991). Images of organization. London: Sage

[11] Neumann, P. G (1995) Computer related risks. Addison-Wesley, New York

[12] Reddy, M. and Dourish, P., (2002). A finger on the Pulse: Temporal Rhythms and information seeking in medical work. In Proceedings of ACM CSCW'02. ACM Press. 344-353

[13] Richman, J. (1987). *Medicine and Health*. London: Longman

[14] Sasse, M. A. Brostoff, S.& Weirich D. (2001): Transforming the "weakest link": a human-computer interaction approach to usable and effective security. BT Technology Journal, Vol 19 (3) July 2001, pp. 122-131

[15] Strauss, A. and Corbin, J., (1990) Basics of qualitative research: grounded theory procedures and techniques. Sage, Newbury Park.

[16] Symon, G., Long, K. and Ellis, J., (1996) The Coordination of work activities: co-operation and conflict in a hospital context. Computer supported cooperative work, 5,1. 1-3.

[17] Turner, B.(1987). Medical Power and Social Knowledge. London: Sage.

[18] Wenger, E., (1999) Communities of practice: Learning, meaning and identity. Cambridge: Cambridge University Press