Privacy Implications for Single Sign-on Authentication In a Hospital Environment

Rosa R. Heckle
UMBC
1000 Hilltop Circle
Baltimore, MD
heckler1@umbc.edu

Wayne G. Lutters
UMBC
1000 Hilltop Circle
Baltimore, MD
lutters@umbc.edu

ABSTRACT
Healthcare providers and their IT staff, working in an effort to balance appropriate accessibility with stricter security mandates, are considering the use of a single network sign-on approach for authentication and password management. There is an inherent tension between an authentication mechanism's security strength and the privacy implications of using that authentication technology. This is particularly true with single sign-on authentication. While single sign-on does facilitate authentication, our on-going field work in a regional hospital reveals several unanticipated privacy implications.

1. INTRODUCTION
HIPAA is forcing the health care industry to review and improve security practices. The HIPAA Security Rule spells out strict guidelines on data security: passwords and user IDs can no longer be shared. Each user accessing patient-identifiable data must be identified and authenticated. Audit trails must be kept of who accesses what types of patient information. In their attempts to address the HIPAA Security and Privacy rules, CIOs are caught in a conundrum. They must find a way to increase data security while at the same time ensuring that clinicians can access clinical data quickly and easily. In this effort, IT managers are exploring alternative forms of authentication, including biometrics and proximity cards (active badges). However, the single sign-on (SSO) approach to authentication is emerging as the most practical current solution. SSO is the ability of a computer user to log in to a network once and then be able to navigate the myriad of applications seamlessly without the need to enter authentication credentials for each application.

There are many tradeoffs in the design of authentication systems. The primary reason for authentication is for security; however, security and privacy are contentious. While authentication systems are mechanisms specifically designed to protect sensitive data, how they are designed and implemented could actually undermine privacy interests of the user. Research has shown that a higher level of assurance (stronger security measures) threatens privacy [1] and impacts usability.

There is an abundance of research on the inherent tradeoff between usability and security [1] as well as the inherent tradeoff between security and the privacy invasiveness of the authentication method for the user [2]. Research work on single sign-on technology usage however, is scant. The work available finds that single sign-on capability has multifold benefits for its users; however, if not implemented properly may actually introduce new security holes. The issue of trust between the SSO user and the organization implementing it has been cited as being critical for a successful adoption [3].

Understanding only the underlying technologies is insufficient for appreciating the ramifications of authentications systems. It is important to know how the systems will work in context to determine their security and privacy implications. This is particularly important for a hospital environment which has many complexities and idiosyncrasies. While some research has looked at SSO technology in general, little empirical research has been done on SSO adoptions in health care. This paper reports preliminary results from an on-going field study of one hospital's design and adoption of a SSO solution. Our intent is to identify the usability and privacy implications of SSO technology for the users of the technology, and determine what if any effect it has on the eventual successful adoption.

Symposium On Usable Privacy and Security (SOUPS) 2007, July 18-20, 2007, Pittsburgh, PA, USA..

2. STUDY DESIGN

2.1 Study Site
This single sign-on pilot is unfolding in an organization which we will call General Hospital from this point forward. General is a suburban hospital with 292 acute-care beds, handling nearly 22,000 inpatient admissions annually. It employs approximately 2,600 full time individuals, with 1,200 of them being physicians, who handle 60,000 emergency room visits and perform 40,000 surgeries annually.

Every medical organization is a unique configuration of fairly routine roles, routines, and requirements. The lessons learned about the SSO implementation at General should have a high degree of transferability to other organizations with similar configurations

2.2 Methodology
The goal of this study is to gain a deeper understanding of the factors affecting an implementation of single sign-on. At its current stage the study is largely descriptive, aiming to discern both the process and factors impacting both the adoption of SSO technology. The primary data collection techniques used are ethnographically informed – observation, contextual interviews, and document review of what if any affect it has on the eventual successful adoption.

The observations for this study began with the first author observing the SSO Implementation Committee meetings. This group consisted of the representatives from the IT Department, the development team, and intended user groups (i.e., nurses, physicians, radiologists, billing, admitting). The group met five

times. Observations are continuing to this day of the Management Information Systems (MIS) group and select user group representatives, as the project goes through the design phase. These meetings were audio digitally recorded, which were later transcribed and augmented with field notes. Individual committee member notes taken during the meeting were also collected and digitized (for the benefit of both the team and our research).

A preliminary review and analysis of all observations, transcripts, and documents has been performed. Based on this we have identified several unanticipated privacy implications with the SSO implementation which are described in the following section

3. FINDINGS

5.1 Concern with E-mail Application. An emergent theme among the user groups was a concern with their e-mail application being available through single sign-on. Users would comment "I don't think I like my e-mail being on single sign-on." Another comment made by the vendor during design, and referring to the users, "they may not care about their network password, but for them once their email password is guessable; they are going to be in a hurry to change their password. There are those users who feel very protective of their e-mail." This concern with e-mail can also be corroborated with observations that were made in the hospital units on workstations where doctors and clinicians would access their e-mail, as well as patient data. On these workstations, oftentimes multiple sessions of the medical application were open on a desktop (indicating someone had used the application, but did not close it). However, I had never observed the e-mail application left open on the desktop.

The concern with email stems from a usability issue created by the routine work practices of nurses. To explain this: there is a major medical application that is used by all clinicians. This application allows the user to lock the *application session* so the user may leave the computer and then resume when they return after re-authenticating. This is referred as 'suspending' the application. This functionality is part of the application user interface. SSO also provides this same functionality; however, with SSO the *workstation* is locked. The privacy issue occurs because once a user is signed on to the workstation, all of their applications are available – including e-mail. If the user uses the application locking function, rather than the SSO locking function, they will lock that particular application; however, all of their other applications remain open – including their e-mail application.

5.2 Moving from Attribute to Individual Authentication. Compliance requires that each individual accessing patient data needs to be identified and the details of access logged and auditable. While this may be necessary for compliance purposes, the need to identify a specific individual causes usability issues and has privacy implications for users in a hospital environment. For example, in some hospital units all clinicians use shared workstations. On these workstations a generic user id would be used to log onto the network. Then each individual clinician would log into whatever application they would need. In some cases, particularly emergencies, they would oftentimes simply use an application that another individual had already logged into.

With the adoption of single sign-on, generic user ids will be eliminated. Each computer will require a unique user id to log on to get access to the network, and then ultimately to the applications on the network. While this may be necessary for compliance purposes, individual authentication is more privacy invasive than attribute authentication. Also, in this particular environment, this need to identify a specific individual causes usability issues. A hospital is a very collaborative environment centered on roles rather than individuals, which makes individual identity problematic. This may create tension – individual identity is stressed, however, the work practices do not support individual identity.

5.3 Surveillance Ability. With single sign-on all of a user's movements on a system can be tracked – from application to application. If this data is collected and stored for a long period of time, it can be used to create dossiers of its users. The existence of dossiers or the ability to create them magnifies the privacy risks of the authentication system. In addition, another possible privacy risk with the use of an SSO is if the captured audit data is used for secondary purposes other than compliance. At this particular time policy has not been established as to what exact data will be retained or the retention period. However, this decision will have privacy implications for the users in this particularly environment, as there have been references made to trust, both implicitly and explicitly. For example, when conversing with a nurse on the unit during observations, the nurse asked why "they" - referring to the Hospital - chose this particular unit to observe. In a MIS meeting a reference was made to the feeling that the employees did not trust management when reporting compliance issues. In the same MIS meeting, but referring to a different event, was a comment made that employees would not participate in a reporting activity because they didn't trust management. While these statements did not directly relate to SSO, they do show that trust is an issue in the organization.

4. CONCLUSION

All authentication mechanisms are privacy invasive in one form or another, including SSO. While it is the intention of the hospital at this point to use the audit data for compliance purposes only, the fact that the data is available may lead to other problematic uses if not adequately protected. Privacy protection needs to be addressed in the design of the system, particularly when trust is essential for successful adoption of the technology.

5. REFERENCES

[1] Adams, A., & Sasse, M. A. (1999). Users are not the Enemy: Why Users Compromise Computer Security Mechanisms and how to take Remedial Measures. Communications of the ACM, 42(12), 41-46

[2] National Research Council. (2003). *Who Goes There? Authentication Through the Lens of Privacy*. Washington, DC: National Academy Press.

[3] Jøsang, A., et al. (2005), Trust Requirements in Identity Management. in Australasian Information Security Workshop. Newcastle, Australia..