Realities of Authentication Management In a Hospital Environment

Rosa R. Heckle
Department of Information Systems, UMBC
100 Hilltop Circle
Baltimore, MD 21250, USA
heckler1@umbc.edu

Wayne G. Lutters
Department of Information Systems, UMBC
100 Hilltop Circle
Baltimore, MD 21250, USA
lutters@umbc.edu

ABSTRACT

Healthcare providers and network administrators, already grappling with the tradeoff between the timely availability of electronic health records and patient confidentiality concerns, now have to consider the implications of complying with HIPAA mandates. In an effort to balance appropriate accessibility with HIPAA's stricter security mandates, many are considering the use of single network sign-on approach for authentication and password management. While this seems to be a simple and viable solution, our field work in a regional hospital revealed fundamental mis-matches with routine work practices that will significantly impact its effective adoption.

1. THE PROMISE OF SSO

Security administrators preach strong security – using long cryptic passwords, changing them every 60 days, and authenticating on all applications. However, they are responsible for providing users with access to what they need in a timely manner. Password administration has always been a burden for network administrators. As more applications require authentication, users are bombarded with a vast number of different system logins each day with most requiring a different username and password. Users are plagued not only with trying to create new and different passwords, but also with the difficulty of remembering all of them. As a result, network administrators spend more time assisting users with forgotten passwords.

Emerging as the leading technology solution for this password management crisis is the single sign-on (SSO) approach. SSO systems are designed to allow a user to log in to a network once and then be able to navigate the myriad of applications seamlessly without the need to enter unique authentication credentials for each application. There are many benefits to SSO technology. Single sign-on technology not only improves usability of authentication for multiple-system users, but it also increases compliance with the Health Insurance Portability and Accountability Act (HIPAA) (104-191 1996). Using single sign-on technology can simplify the deployment of stronger passwords and help enforce an effective password policy. Since users need only one password for single sign-on, users should be able to more easily comply with secure password policies that require a 'strong' password. Enforcement of the security policies is also centralized, making it easier to manage. For example, when a new employee is hired or when an employee leaves the firm the process of adding or removing their authorization rights to specific applications can be done centrally (Anchan and Pegah 2003).

Single sign-on has shown to be a successful paradigm in a network environment. However, the context within which this system is used could introduce usability issues to the users that ultimately make management of the SSO problematic and create new vulnerabilities. This is particularly true when an SSO is used within the context of a healthcare environment.

Seeking to deepen our understanding of the benefits and limitations of SSO approaches, we are carefully following a SSO pilot project at a community hospital.

2. CURRENT STUDY

A single sign-on pilot is unfolding in an organization which we will call General Hospital from this point forward. General is a community 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. General Hospital is undertaking a pilot with the use of single sign-on for password management and password provisioning.

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.

The password situation at General Hospital at this time is as follows: The average user has 4 to 6 applications on a daily basis, each requires user authentication. Each application has its own schedule for: password length, character mix, expiration, as well as limitations as to how often passwords may be recycled.

3. THE ISSUES WITH SSO

3.1 Policies and Their Affect on SSO

Healthcare providers and network administrators are working towards HIPAA compliance for the privacy and security of personal health information. HIPAA requires that a patient's record not be displayed where they can be viewed by those who should not have access to them. Personal computers are available throughout the hospital and many of them are in areas that are accessible by patients and their visitors. Therefore when a nurse walks away from their computer, the nurse should 'suspend' the application which would close the application, or logoff. For HIPAA compliance purposes, the hospital policy dictates that the application will automatically shut itself off (auto logoff) after a certain period of inactivity. After an auto logoff, the nurse must re-authenticate in order to return to their work. The policy on the timing of the auto logoff is important.

In a hospital setting, clinicians, particularly nurses, are always documenting on their systems continuously throughout the day. If they move away from the machine to care for a patient, then return to their computer to find that they had been automatically logged off, they will have to re-authenticate. Looking at this cumulatively, a continuous logon/logoff cycle for every request for every user may have an overall effect on the network response time depending on the time limit set by the policy. In a member-to-member survey of hospital CIO's (2006) regarding the adoption of SSO, revealed auto logouts to be a problem because it increased the need to re-authenticate (logon) once resuming work. Out of 52 respondents who were asked if the implemented SSO solution had met their expectations, 67 percent said that it had, while 33 percent said that it had not. Of the latter, 23 percent cited increased 'logon time' as a problem in the open responses including: "Duration to login and logout is too long." "Increases the logon time excessively." "A number of desktop issues can impact speed of sign-on." "Slow or failed logons." While this increase in login time may be acceptable in many organizations, in a hospital environment, an increase in login time is not tolerated as well.

Far more important than network delay is the disrupted work of care giving. Care giving is a nurse's priority and in an effort to do this, the nurse will always find a work around, which circumvents the security. While this auto logoff policy makes sense on paper it clashes with the actual practice of care giving where the users are not glued to a keyboard!

3.1 Integrating proprietary systems

Though integrating existing application's functions with the SSO can be problematic. For example, there is a major medical application that is used by all clinicians. This application allows the user to 'suspend' the application session so that they may leave the computer, and then continue working at the exact place they left off when they return. This 'suspend' functionality is part of the application interface, and the nurses have become accustomed to using this functionality when they want to temporarily logoff (suspend) the application. SSO also provides this same functionality; however, with SSO the entire workstation is locked not just the application. In an SSO environment, the problem occurs because once a user is signed on to the workstation, all of their applications are available. If the user applies the application 'suspend' rather than the SSO lock, they will only secure that particular application, leaving all of their other workstation applications open; thus creating a security breach

3.2 Controlling secondary usage of passwords

How will the SSO deal with passwords that have secondary uses and are not under SSO control? For example, nurses use their 'medical system application' id and password as a way to co-sign for insulin injections. This is done within the application itself. Will the medical application coordinate with the SSO system to use the same password? When the network password is changed, will the medical application recognize that change or will the nurse still have to remember the medical application password to co-sign for the insulin?

Passwords are used for many things other than accessing resources on the network. There is a proliferation of passwords required for many physical work tasks as well. Access to medical supplies cabinets, access to the narcotics room and dispensing system; all need passwords to gain access. Will these passwords be coordinated with the network password controlled by the SSO system?

If password management is not appropriately integrated or synchronized for ALL passwords used, the password management problem has not been fully addressed with the SSO adoption.

4. CONCLUSION

Technically the single sign-on approach seems like a viable solution to a simple password management problem, in reality the problem is much more complex. There are a multitude of forces exerting tensions on the implementation. These tensions stem from conflicting and oftentimes stringent requirements from the different stakeholders; the hospital wants quality patient care; HIPAA wants patient privacy preserved; clinicians need easy access in a timely manner to provide the quality care.

From a preliminary analysis of our on-going field study at a community hospital, there appears to be a number of mismatches between the SSO vision and the realities of routine work. While we cannot conclusively say if a SSO adoption will be effective in meeting its goals in a hospital environment, we do know that it will affect the work practice and that will make the management of the SSO system problematic.

We are keenly interested in how this implementation will play out. Our field work will continue through the roll out and an extended adoption period. Our focus is to identify all the forces that inhibit or influence the adoption of the technology, delineating the different tradeoffs to be made, and understanding the technology's affects and effects within the hospital environment. The ultimate goal is to not only inform this SSO effort, but other organizations wrestling with similar password management struggles.

5. REFERENCES

Adams, A., & Sasse, M. A. (1999). Users are not the (2006). Member-To-Member Survey: Single Sign-on Solutions

College of Healthcare Information Management Executives.

104-191, P. L. (1996). HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996, 104th Congress.

Anchan, D. and M. Pegah (2003). Regaining single sign-on taming the beast 31st annual ACM SIGUCCS conference on User services San Antonio, TX, USA