2007

Once IS Enough: Single Sign-On

Peter Yacano
Monash University, yak83@bigpond.net.au

Kathy Lynch
University of the Sunshine Coast, Maroochydore, Kathy.lynch@usc.edu.au

Once IS Enough: Single Sign-On

Peter Yacano
Caulfield School of Information Technology
Monash University
Melbourne, Australia
Email: yak83@bigpond.net.au

Kathy Lynch
University of the Sunshine Coast
Maroochydore, Australia
Email: Kathy.lynch@usc.edu.au

Abstract

For eons, passwords have been the gatekeepers to information and data located that is behind a 'locked door' or stored in a secret location. It is no different today, as passwords are a key to secrets, however, what is different today is the number of passwords that one needs to construct, recall and keep safe. This multiplicity has created a memory overload for the user, less secure passwords, and often, a strain on computer help-desk staff.

Password technologies that reduce the need for multiple passwords are evolving; their developers claim that the technologies lessen the security risk to a system due to a reduction in the number of passwords required to get through the day-to-day work of a 21st century citizen. Smart cards, biometric devices, and Single Sign-On (SSO) systems are the most promoted alternatives. Specifically, Single Sign-On password systems are of interest to the study presented here. Single Sign-On allows end users to access multiple services and systems with a single username and password, therefore reducing the cognitive load on the end user and thus supposedly, reducing end user frustration which is turn reduces password-related security risks.

This paper presents the results of a study conducted within two businesses that explored the influence SSO password systems have on system security.

Keywords

Single Sign-On passwords, IS security

Introduction

Information systems have been designed, networked and distributed across locations around the globe bringing forth a greater reliance on passwords to access information these systems hold and safe guard. End users of these information systems usually have to recall a set of credentials (user name and password) in order to be identified within a network and gain access to the systems or resources within that network. With the ever increasing reliance on multiple information systems, end users commonly have to recall multiple sets of credentials to access the information they require.

There has been widespread research highlighting many of the negative aspects associated with password security, including the repercussions that face end users when dealing with memorising and recalling multiple user credentials. While some organisations are conscious of the issues that face information systems that utilise this data control mechanism, few organisations seem to be aware of the various security alternatives that are available to minimise security risks, and improve user experience and productivity.

An alternative to the traditional password procedures of typing user credentials for every system one needs to access, is a new breed of control mechanisms allowing end users to be identified and managed from credentials that do not need to be memorised; namely, what a user has (i.e. smart card) or what a user is (i.e. biometrics). However, the adoption of these technologies are still limited across the broad spectrum of organizations for password access to their information systems. A secure alternative to the smart card and biometrics systems is the SSO password system, and it is these systems that are of primary interest to the research presented.

Password Systems

Security specialists have found that writing passwords down is a common technique that end users adopt in dealing with recalling passwords. Users either record their credentials as a soft copy on a computer's hard disk

or email system, or physically write them down. It is not uncommon to see passwords recorded on 'post-it' notes that have been fixed to the computer screen; this practice is extremely insecure and is similar to a person leaving their keys in the front door and encouraging would-be hackers and others to steal credentials, identities, and their associated authority and assets.

Notwithstanding end users employing short cuts to aid password recall, experts unanimously believe that most passwords are eventually forgotten by end users (Thaddeus, 2001). This situation is exacerbated as users are required to use more secure passwords; for example, passwords that are longer, case sensitive, and are a combination of numbers, letters and symbols. Santos (2004) claims that end users "often have so many passwords that they invariable forget them and have to call the helpdesk to either retrieve or reset them" (p1). Bigler (2004) reports that 15 to 45 percent of helpdesk support calls are related to forgotten or expired passwords. These figures are rather staggering, and ultimately results in a drop in overall productivity, decreased security, and creating unnecessary overloads for the organisation. Helpdesk staff are commonly engaging in reactive support by dealing with password resets, rather than being proactive and dealing with problems before they impact on performance or security.

Accessing multiple information systems that require the input of user credentials to access the data, have traditionally required separate credentials to each systems. The alternative system that is reported on in this paper are systems that have one set of credentials to access multiple systems, SSO systems. A simplified comparison of the login procedure for each of these models is presented in Figure 1.

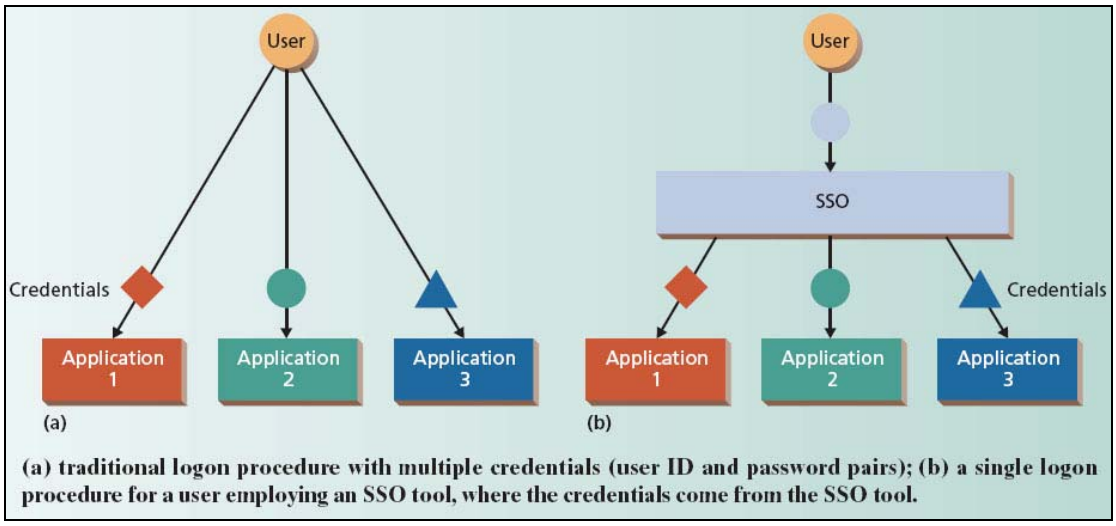

Figure 1: Traditional password systems versus SSO password systems (Volchkov 2001, p4)

Traditional Password Systems

Traditionally, passwords have been a *software* solution to user authorisation; the process of identifying and permitting a user onto a network. Passwords are simple by nature and require a user to type a string of numbers, letters or symbols into a dialogue box to gain access to a system.

The initial setup and training costs of information systems utilizing traditional passwords is usually low, as they can also be easily administered and maintained by general helpdesk staff. Correspondingly, end users are familiar with passwords as a form of authentication as they have become embedded into our society and every day living.

Some security experts would argue the main reason why traditional passwords mechanisms are considered such a popular option for system administrators is that the technology is an inexpensive way of providing security and authorisation (especially on smaller sized systems).

Two of the issues associated with traditional password access to secure information systems is an organisation's failure to see the long term costs associated with traditional passwords, in particular those costs associated with productivity and support (Santos, 2004). Furthermore, Gates (cited in Kotadio, 2004), claims that passwords "don't meet the challenge for anything you really want to secure" (p1).

Password selection methods ultimately affect password memorizability (Zviran, 1999). When a password is automatically generated, or assigned according to a formula, the end user is not involved in the selection process, therefore, there is an increased risk that the end user will forget his or her password as the password is

meaningless to the one who is required to use it. This suggests that randomly generated, system assigned passwords are more likely to be forgotten than self assigned passwords, and therefore, they are less secure.

Password security often deteriorates as users are forced to memorize more than one password across more than one system. Halderman (2005) believes that "typical users can be trained to select and remember a single secure password, but multiplying this dozens of times is sure to push the physiological limitations of human memory" (p1). Adams and Sasse (1999) add to this argument by suggesting that by "having a large number of passwords, it reduces memorability and increases insecure work practices, such as writing passwords down" (p3). Users often struggle to remember more than a handful of passwords; it's unrealistic to expect them to memorize every username and password combination for each unique system or service that they use.

Many users will work around the multiple password syndrome by using the same or 'master' password for every passworded system (Stuhimuller, 2000, p1). This inturn creates a weak point in security by allowing a would-be hacker to potentially acquire the 'master' password, which then can be used to gain access to multiple systems or resources. Some users will overcome the use of a master password by employing passwords that are easier to recall. For example, the use of 'password' as the password is common, and carries with it, a very high security risk (Adams and Sasse, 1999). Other examples could include using common names (for example, mother's maiden name) or using a smaller sized password. Naturally, these passwords are far easier to recall by legitimate users, however, they are also far easier to be guessed or hacked by unauthorised users.

Passwords can supposedly made more secure by the system requesting frequent changes to the password (Franklin, 2005), and making the password more complex through the use of passwords that are longer, are case sensitive, numbers, symbols, and banning words found in "common dictionaries" (Franklin, 2005, p38). A complex password string, with a greater mix of numbers, symbols and alphabetical characters yields a stronger, more secure password. This is due to the fact that there are infinitely more alternatives or combinations in a password that is made up with a larger character set.

Morris and Thompson (1979) suggest "if we want to check all passwords of length, *n*, that consists entirely of lower-case letters, the number of passwords is 26^n" (p3). Table 1 presents password cracking times for various password lengths carried out by a PDP-11/70 mainframe computer with a 22-bit processor, and 4megabtyes of memory.

Table 1: Password cracking matrix (Morris & Thompson, 1979 p3)

Password length	26 lower case letters	36 lower case letters and digits	62 alphanumeric characters
1	30 milliseconds	40 milliseconds	80 milliseconds
2	800 milliseconds	2 seconds	5 seconds
3	22 seconds	58 seconds	5 minutes
4	10 minutes	35 minutes	5 hours
5	4 hours	21 hours	318 hours
6	107 hours	n/a	n/a

A similar study conducted by Yan (2001) addressed the same issue as Morris and Thompson's 1979 experiment, however, they used a faster computer (Pentium 333) and greater password combinations and lengths (Table 2).

Table 2: Password cracking matrix (Yan 2001, p4)

Composition	No. Possible Solutions	Cracking time
7 characters; 5 alpha, 2 numeric	24,950,889,600	32.57 Hours
7 characters; 4 alpha, 3 numeric	15,994,160,000	20.88 Hours
7 characters; 3 alpha, 4 numeric	6,151,600,000	8.03 Hours
5 characters, 5 alpha	11,881,376	55.83 Seconds

Yan's work demonstrates that a password containing a higher ratio of alpha characters to numeric characters ultimately results in a stronger and more secure password.

Randomly generated, system assigned passwords are often a common mechanism employed by system administrators to bolster security when a randomly generated password is produced; often this password is created from a set of rules or guidelines. These rules or guidelines might enforce a set length for the password or that the password should be made up of a certain amount of alphabetical or numerical characters.

Emerging Password Systems

To overcome many of the weaknesses associated with dealing with traditional password systems, specifically, multiple passwords across multiple information systems, various technologies have emerged; for example:

- Password vaults, where a user can set a single, secure master password to gain access to other, less frequently used passwords (Lindstrom, 2005).
- One-time passwords, where a user needs to use a different password every time to authenticate themselves; the change of password is authenticated using an electronic key (Halevi & Krawczyk, 1999).
- Password synchronisation, the user is required to enter the same username and password to multiple systems or services within the organisation (Volchkov, 2001).
- Single Sign-On (SSO), where a user accesses multiple services and systems once using a single set of credentials (username and password).

As previously stated, it is SSO that is of greatest interest to this study, and is further discussed in the following section.

Single Sign-on Password Systems

SSO passwords are designed to allow users to use a single encrypted 'key' to access all authorised systems with just one password and one ID" (Bigler, 2004, p2). Lodha and Sarma (2006) suggest that true SSO systems should "intercept login prompts by secondary applications, and automatically fill in fields such as login ID or password" (p2). Under this schema, there is usually a centralised server that is used to authenticate end users. This centralised server has a backend database that is used to store credentials, such as user access levels and details concerning applications and services within the system. After a user is successfully identified and authorized, the central SSO server allocates a session ID (or token) that "enables transparent validation while transversing various systems or servers" (Bigler, 2004, p2). Commonly, this style of infrastructure is also referred to as Enterprise SSO (ESSO), as this method delivers SSO in a heterogeneous environment, including web, client/server and legacy applications (Lindstrom, 2003).

Lodha and Sarma (2006) claim that a true SSO infrastructure typically consists of the following major components:

- User authentication
- User authorisation
- A portable user profile
- A trusted, globally accessible user token
- A centralised user store

(Lodha & Sarma, 2006 p3)

User authentication and authorisation are typically found in almost all security mechanisms today. The authentication stage deals with identifying the individual behind the login attempt, while the authorisation stage examines if the user should be granted access to the system.

In most cases, the authentication stage is carried out under a single factor authentication scheme; for example, only identifying the user through the use of passwords (Bigler, 2004). Security at this stage can be bolstered with the use of a second authentication method, for example, the use of smartcards or other hardware based systems.

Once a user has been identified, the system must determine what level of access the user possesses within the system boundaries. This authorisation phase is assisted by cross referencing the user against the centralised user store; normally in an encrypted database. The centralised user store accumulates information such as user credentials, login history, and details specific to services or applications within the SSO framework.

Additionally, once the user has been identified, permission granted and have been allocated their access level, the system generates a globally accessible user token which is recognised across the whole SSO network and associated services or applications. This token is used for the duration of the user's visit and can be easily transported from one application to the next. This token ensures the system continues to recognise and grant access to the authorised user across various applications and services for the full duration of their login.

One of the key benefits of implementing SSO in an organisation is that SSO reduces the number of passwords end users have to remember in a day at work. In most cases, end users would only have to remember one master password following a SSO rollout, therefore, eliminating the need for the user to recall multiple credentials.

In direct relation to users only requiring one set of credentials to access multiple systems within the organisation, password guidelines can also be tightened to ensure maximum security levels within an organization: passwords can be longer in length and contain a greater variety of characters or symbols. Sonnenberg (2003) argues that "by relieving users of the need to memorize multiple passwords, SSO solutions

make it easier for organisations to implement and enjoy the increase protection afforded by strong passwords" (p8). Anchan *et al* (2004) supports the reduction of password numbers by suggesting that after a SSO rollout, "the chances of a user committing blunders such as storing passwords in written form out of concern of forgetting them is reduced, which increases security" (p2). Puljala *et al* (2000) also support password number reduction by denoting, "users will not have to create and maintain multiple accounts and passwords, reducing the need to physically store passwords and thus reducing security risks" (p2).

Lindstrom (2003) suggests that "if an SSO solution doesn't provide single sign-on to all desired applications, then it doesn't fulfil its intended mission" (p8). He continues his argument and suggests that true SSO systems often "support multiple application platforms within an enterprise" (p8). Puljala *et al* (2000) support this claim and propose that "the central authentication and authorisation [of SSO] must provide a flexible and standardised framework to accommodate the wide range and diverse nature of end user applications" (p2). This increased support, standardisation and coverage across different hardware and software platforms are typically appealing factors when implementing a SSO based security solution. A summary of the benefits associated with SSO are presented in Table 3.

Table 3: SSO Benefits – Summary Table (adapted from Lindstrom, 2003; and Puljal et al, 2000)

1.	Increased, standardised security due to simplicity for the end user (transparent security)
2.	Reduction of recalling multiple passwords for end users
3.	Users no longer the weak link - mental strain vastly reduced on end users
4.	Improved workflow and usability throughout entire system for end users
5.	Vastly reduced helpdesk costs
6.	Enforcement of global security and password policies
7.	Increased, standardised and automatic auditing and monitoring due to centralised administration
8.	Heterogeneous support for all types of hardware and software environments

The Study

Generally, there has been low adoption of SSO password systems for information systems within an orgnaisation, and little research has been undertaken in the effects of single sign-on within a business or educational environment. This study was designed to explore some of the impacts that single sign-on has in regards to enhancing security and improving productivity for the end user. Therefore, the main research questions for this study are,

Does SSO password systems enhance password security in information systems?
Does SSO password systems improve password usability for end users within information systems?

In answering these questions, the study explored the effect SSO password systems had on the end user, in particular password composition, methods of recalling passwords, re-use of passwords across multiple systems, the number of times a user is required to enter a password, and the impact password complications had on productivity. The findings reported here are focused on the two main issues directly related to SSO password systems; that is, the number of times passwords need to be entered to access information within an organisation, and the use of multiple credentials.

The Study Design

Surveys were used throughout the research to capture participant responses to primarily quantitative questions. Work conducted by Zviran (1999) and Campbell (2004) into password security underpinned the survey questions. The survey was online, anonymous, distributed to a large number of potential participants, and was convenient for the participants to complete. A high response rate was expected, therefore yielding valid results. Neuman (2000) suggests that the total response rate is typically found to be high (80 to 90 percent) in directly administered questionnaires (p239); for example a survey that is directly handed out to participants in a physical location. The survey used in this research, though not directly distributed to the participants, was distributed via a web link embedded in an email message sent to employees by the IT Manager in the two participating organisations.

Data Collection Instrument

A combination of quantitative and qualitative data was captured from the survey using a yes/no response, selection of given options, or a qualitative response. The quantitative questions provided statistical data, the qualitative questions allowed for an insight to individual end users' experiences.

The survey was accessed online from a commercial data capturing site, SurveyMonkey.com : SurveyMonkey™ is an organisation that specialises in web surveys. SurveyMonkey.com uses 128bit encryption to ensure maximum security levels and highest level of data integrity, and it is listed on the United States Department of Commerce 'Safe Harbour List'. (Privacy and data integrity information can be found at http://www.surveymonkey.com/help/Privacy.asp).

Participants

Participants were from one of two organisations, and were recruited using a global email sent from the organisation's IT Manager. Embedded within the email was a secure link to SurveyMonkey.com for the data collection. The managers stressed in their email that participation was completely voluntary, and contributing to this study would have no effect on their job status.

> Organisation A was a large city council located in Australia. This organisation was used as the control group during this research as the organisation employs information systems that require end users to utilise tradition password systems to access various applications and services.
>
> Organisation B was a medium to large insurance company located in the same region in Australia. This organisation was surveyed twice over the period of a few months. The first survey was the same as that distributed to Organisation A, the second survey was modified to reflect specific issues relating to the organisation's recent implementation of SSO.

Data Analysis

The quantitative data was analysed using the statistical package Statistical Package of the Social Sciences (SPSS). The mean was calculated to indicate the average result within each question; the standard deviation was used to reveal the distribution of variation to the mean. Percentages were calculated for nominal data.

The small amount of qualitative data gathered during the Round 2 of the data collection was used to support the quantitative analysis.

The results were grouped according to the following themes; however, it is only the last theme that is reported here:

- Password composition: composition of passwords, and selection method.
- Password reuse: using identical or similar passwords over multiple systems.
- Password recall: methods used for recall of passwords, and forgetting passwords.
- Password entry: the number of passwords to be remembered, and the number of times each day a password is entered.

Results and Findings

Two small to medium organisations were involved throughout the duration of the study; Organisation A, a city council located within Melbourne's suburban boundaries and Organisation B, an insurance company located in Melbourne CBD.

- Organisation A participants were surveyed on one occasion; this yielded 126 responses (98% response rate).
- Organisation B participants were surveyed twice over the period of a few months. Fifty-eight participants returned results in the Round 1 of the data collection (100% response rate); and 52 participated (90% response rate) in Round 2.

Password Entry

The two issues reported here relate to the one of the most common frustrations that a user has with respect to passwords, and are often the reason behind the user push for SSO systems;

- the number of different passwords a user is required to remember in any one work day, and

- the number of times a user is required to enter their credentials in any one work day.

Number of Different Passwords Used in a Work Day

In traditional password models, passwords are unique to a system; however, the user may decide to use the same password for multiple systems. More often than not, an employee in their everyday work is required to use a number of information systems, and traditionally, each require a password to be entered. Organisation A requires its employees to enter new credentials for every system. Organisation B also required this (Round 1) until they introduced a SSO system (Round 2). The users where asked the number of passwords they were required to remember in any single work day, the results are presented in Table 4.

Table 4: How many different passwords would you have to remember in a day at work?

	Org A. Round 1	**Org. B Round 1**	**Org. B Round 2**
	% *(n=126)*	**%** *(n=58)*	**%** *(n=52)*
No password (1)	0.0 (n=0)	0.0 (n=0)	0.0 (n=0)
1 password	6.3 (n=8)	12.1 (n=7)	48.1 (n=25)
2 – 3 passwords	44.4 (n=56)	56.9 (n=33)	42.3 (n=22)
4 – 5 passwords	30.2 (n=38)	17.2 (n=10)	7.7 (n=4)
5 – 7 passwords	12.7 (n=16)	12.1 (n=7)	1.9 (n=1)
8 – 10 passwords	5.6 (n=7)	1.7 (n=1)	0.0 (n=0)
10 – 15 passwords	0.8 (n=1)	0.0 (n=0)	0.0 (n=0)
More than 15 passwords (8)	0.0 (n=0)	0.0 (n=0)	0.0 (n=0)

Forty-nine percent of Organisation A's participants are required to remember more than four password in any one day, with 6.4 % of these participants being required to remember more than 8 passwords in any one day. The Round 1 results for Organisation B are slightly less exhausting at 31%, with only 1.7% having 8-10 passwords to remember, and no participant recorded that they had to remember more than 10 passwords.

SSO was introduced into Organisation B shortly after Round 1 was conducted, therefore SSO was still in a bedding down stage, and not all systems had been included into the SSO password system roll-out. However, the results from Round 2 data collection show significant reduction in the number of passwords to be remembered in any one day. Only 9.6% of participants claim that they are required to remember four or more passwords in any one day. This is a significant drop from the 31% in Round 1. Minimising the re-use of passwords across multiple systems minimises the risk of passwords being uncovered or cracked. What is noteworthy is that 90.4% of participants, are now required to remember only three passwords or less. The qualitative data collected in Round 2 substantiates this reduction due to the SSO roll-out in Organisation B:

> *"I found different passwords to be a nuisance. I tended to reuse themes and words and was running out of 'easy to remember' options (i.e.: names of family/pets etc). Creating one new password only to have another lapse was a pain. I think it is great to sign on once and everything is ready to go, especially when your system locks frequently during the day."*

> *"It made no sense to me why we should have 2 different passwords for our operating systems. If one of the passwords fell into the wrong hands, what's to say the other one wouldn't either. The single sign on is great in my humble opinion."*

Number of Times Passwords are Entered in a Work Day

Associated with the number of passwords that need to be remembered in any one day (Table 4), another question was asked to capture how many times a user was required to enter a password in any one day of work. This question was specifically asked due to the premise that the repeated entering of passwords is a cause of frustration – and one of the prime reasons why SSO passwords are introduced into organisations. The responses to this question are presented in Table 5.

Table 5: How many times a day would you manually enter a password?

	Org A. Round 1	Org. B Round 1	Org. B Round 2
	% *(n=125)*	% *(n=58)*	% *(n=52)*
None (1)	0.0 (n=0)	0.0 (n=0)	0.0 (n=0)
Once a day	4.8 (n=6)	0.0 (n=0)	7.7 (n=4)
1 – 3 times a day	19.2 (n=24)	1.7 (n=1)	26.9 (n=14)
4 – 6 times a day	27.2 (n=34)	20.7 (n=12)	32.7 (n=17)
7 – 10 times a day	22.4 (n=28)	27.6 (n=16)	15.4 (n=8)
10 – 15 times a day	13.6 (n=17)	20.7 (n=12)	7.7 (n=4)
15 – 20 times a day	4.8 (n=6)	20.7 (n=12)	5.8 (n=3)
20 – 25 times a day	3.2 (n=4)	5.2 (n=3)	1.9 (n=1)
More than 25 times a day (9)	4.8 (n=6)	3.4 (n=1)	1.9 (n=1)

Organisation A appears to require end users to enter their password details less times per day than end users in Organisation B. The mean for Organisation A is 4.72; this figure falls in the range of four to six password entries per day – though closer to six than to four, with a spread of 1.67. Organisation B was a little worse off, with a mean of 5.67; equating to a password entry number in the range of seven to ten password entries per day – though closer to seven than to ten, with a spread of 1.38. In Round 1 data collection, overall Organisation B users where required to enter their passwords more frequently than those in Organisation A.

Furthermore, if we accumulate the scores across the categories, we can see a clearer picture. Within Organisation A, 26.4% of end users enter their credentials ten or more times a day. Increasing the spectrum to include seven or more password entries a day, this figure increases to 48.8% of end users. Focusing on Organisation B, 50.0% of end users manually enter their password ten or more times a day. Once again, increasing the range, a staggering 77.6% of end users are required to enter their password seven or more times a day.

The mean for the Round 2 results drops to 4.23, equating to four to six password entries per end user per day, though closer to four. Upon further examination of the figures, the trends are clearer with only 17.3% of end users manually entering a password ten or more times a day, compared to the 50% in the first round. Increasing the spectrum again and 32.7% of end users are now entering passwords seven or more times a day; this is compared to 77.6% of end users in the first round of results. The multiple entering of passwords in a SSO system could be explained through system time outs, computers crashing, and or incomplete integration of all systems into the SSO model. The incomplete integration was a comment made by several participants,

> *"There are other software applications I use as part of my daily work that are not standard across the company, and so single sign-on doesn't apply. There are also service provider websites we log into, and some have their own password format that is different from ours."*

However, in Round 2 (Organisation B), it can be seen that 7.7% of end user within Organisation B now only have to enter a password once in an average day at work; this is compared to zero percent of end users in the first round. Furthermore, 26.9% of end users now only have to manually enter their credentials between one and three times a day after the adoption of a SSO system within the organisation. This figure highlights the decrease in manual password entry subsequent to the SSO rollout, as a low 1.7% of end users had the luxury of entering their password one to three times a day in the first round. It is predicted that this positive affect will flow down to other areas concerning end users' password security and productivity issues.

Productivity

SSO password models supposedly improve use efficiency and productivity. This question was asked of participants from Organisation B were asked this question in Round 2 (No organisation in Round 1 had SSO implemented at the time of data collection). A simple yes or no question followed by an open ended response was used to elicit responses relating to the productivity perception of users as a result of SSO implementation. The qualitative responses are embedded in the discussion below to support the quantitative findings.
A staggering 82% of participants (n=49, Organisation B, Round 2) claimed that the implementation of SSO has streamlined the way they work. A number of the indicative comments are below:

> *"SSO has significantly reduced the amount of time spent typing passwords into the system and reduced the errors in signing in due to putting the wrong password into the different applications."*
>
> *"I don't have to think about signing on and I get straight to the programs I need. I also spent time coming up with new passwords for different access and I don't do that anymore either."*
>
> *"starting the day's work is immediate, rather than a drawn out exercise in bureaucracy."*

"There is less chance of password errors and locking myself out, which saves time"

"It's much easier to operate. Also less time consuming."

"Saves time. Saves data entry. Saves frustration."

Participants also commented that the benefits of SSO was not for the end user alone, but the company as a whole, for example:

"more than one sign-on often meant that my network password would differ from my i90 [the mainframe of the organisation] password, creating problems with locking myself out of the system. I would then have to wait up to two hours for my password to be reset by the helpdesk."

"A single sign-on system will be far more effective and efficient for end users and administrators alike."

"an excellent initiative, and will surely reduce the number of helpdesk calls received."

Conclusion and Future Work

With the reduction of passwords that a user is required to enter in any one day, come benefits, including increased productivity of the end user and the organisation as a whole. Findings from the study indicate that the benefits 1 to 5 of SSO as reported by Lindstrom (2003) and Puljal *et al* (2000) are still of great important today and are evident in organisations that adopt SSO password systems for their organisation's information systems. Benefits 6 to 8 were not explored in the study, and therefore should be explored in future SSO research.

1. Increased, standardised security due to simplicity for the end user (transparent security)
2. Reduction of recalling multiple passwords for end users
3. Users no longer the weak link - mental strain vastly reduced on end users
4. Improved workflow and usability throughout entire system for end users
5. Vastly reduced helpdesk costs
6. Enforcement of global security and password policies
7. Increased, standardised and automatic auditing and monitoring due to centralised administration
8. Heterogeneous support for all types of hardware and software environments

In answering the research question: *Does SSO password systems enhance password security in information systems?* The following can be established; SSO password systems

1. eliminate the negative characteristics associated with passwords, such as password reuse or recording/sharing user credentials;
2. simplify and strengthens security for the end user by allowing end users to recall fewer passwords. This simplification methodology aligns with Anchan et al (2004) comments, arguing that after the rollout of a SSO solution, "the chances of a user committing blunders such as storing passwords in written form out of concern of forgetting them is reduced, which increases security" (p2), minimising many of the security risks associated with password authentication, and therefore, increasing security, not only for the end user but also the organisation as a whole.

In answering the research question: *Does SSO improve password usability for end users within information systems?* The following can be established; SSO password systems

1. streamline work processes and encourages productivity;
2. minimise downtime due to password re-sets and password entry delays, therefore, increasing efficiency and reducing frustration.

The overall findings from the research show that SSO password systems enable a system to be more secure, users to be less frustrated with passwords, improve the user experience and productivity, and streamline work processes.

Although the study as a whole explored more areas than are published here, with the insight gained through the exploration of the number of passwords and the times they are used, the remaining of the data needs to be-analysed individually and holistically to enable a more comprehensive understanding of the benefits and disadvantages of SSO password systems. Furthermore, as SSO password systems mature and are more widely adopted, a more detailed study should be conducted. Further exploration should include a study of the

relationship between password use and workflow, password policy, and access rights. The authors plan to conduct further research to answer such questions with a focus on organisations that have a matured SSO implementation.

References

Adams, A. and M. Sasse (1999). “Users are not the enemy: Why users compromise security mechanism and how to take remedial measures.” Communications of the Association for Computing Machinery 42(12): pp 40-46.

Anchan, D. and M. Pegah (2003). "Regaining single sign-on taming the beast." Proceedings of the 31st annual ACM SIGUCCS conference on User services. San Antonio, TX USA pp 166-171.

Bigler, M. (2004). “Single sign-on”. Internal Auditor. 61: 4.

Franklin, C. (2005). "Strong authenication." Network Computing 16(2): 7.

Halderman, J. A., B. Waters, et al. (2005). “A convenient method for securely managing passwords” International World Wide Web Conference, Japan.

Halevi, S. and H. Krawczyk (1999). “Public-key cryptography and password protocols”. Association for Computing Machinery Conference on Computers and Communication Security, Nov 1998, San Francisco.

Lindstrom, P. (2003). “The evolution of single sign-on” Spire Security: 11.

Lindstrom, P. (2005). “Truth and fiction with single sign-on” Spire Security: 9.

Lodha, A. and R. Sarma (2006). “A Single Sign-On Approach” 1-12.

Morris, R. and K. Thompson (1979). "Password security: A case history." Communications of the Association for Computing Machinery (22), 11: pp 594--597

Neuman, W. L. (2000). “Social Research Methods: Qualitative and quantitative approaches.” Boston.

Puljala, R., R. Sadasivam, J. Robinson and J. Gemmill. (2000). “Middleware: Single sign-on authentication and authorisation for groups.” Computer and Information Sciences. Birmingham, University of Alabama: 6.

Santos, M. D. L. (2004). "The Marriage of Physical and Logical Access." Computer Technology Review 24(6): 2.

Sonnenberg, A. (2003). “SSO: Enabling an effective password policy” Imprivata: 9.

Stuhlmuller, R. (2000). "User identity: The key to safe authentication." Communications News 37(3): 1-3.

Thaddeus, J. (2001). “Need a password? Just call the helpdesk.” Computerworld. 35: 1.

Volchkov, A. (2001). “Revisiting single sign-on.” IT Pro: 39-45.

Yan, J. (2001). "A note on proactive password checking." Association for Computing Machinery.

Zviran, M. and W. J. Haga (1999). "Password security: An empirical study." Journal of Management Information Systems 15(4): 161-182.

Copyright