Karen Renaud and Lewis Mackenzie (2013)

SimPass: Quantifying the Impact of Password Behaviours and Policy Directives on an Organisation's Systems

Journal of Artificial Societies and Social Simulation 16 (3) 3
<http://jasss.soc.surrey.ac.uk/16/3/3.html>

Received: 13-Feb-2012 Accepted: 28-Dec-2012 Published: 30-Jun-2013

Abstract

Users are often considered the weakest link in the security chain because of their natural propensity for choosing convenience over safe practice. One area with a vast amount of evidence related to poor user behaviour is that of password management. For example, when hackers gain unauthorised access to public websites, subsequent analysis generally confirms that compromised passwords are to blame. We have a pretty good idea of the extent to which careless behaviour impacts on the individual user's personal security. However, we don't fully understand the impact on the organisation as a whole when such laxity is aggregated across a large number of employees, nor do we know how best to intervene so as to improve the level of protection of critical systems. Current wisdom mandates the use of increasingly draconian policies to curb insecure behaviours but it is clear that this approach has limited effectiveness. Unfortunately, no one really understands how the individual directives contained in these policies impact on the security of the systems in an organisation. Sometimes a mandated tightening of policy can have unexpected side-effects which are not easily anticipated and may indeed prove entirely counterproductive. It would be very difficult to investigate these issues in a real-life environment so here we describe a simulation model, which seeks to replicate a typical organisation, with employee agents using a number of systems over an extended period. The model is configurable, allowing adjustment of particular input parameters in order to reflect different policy dictats so as to determine their impact on the security of the simulated organisation's IT infrastructure. This tool will support security specialists developing policies within their organisations by quantifying the longitudinal impacts of particular rules

Keywords:
Passwords, Policies, Organisation, Security, Authentication

Introduction

1.1 "Good Practice" in information security states that at least the following password rules must be included in information security policies, and enforced within organisations FIPS (1985).

- Do not recycle passwords, use a different password on each system.
- Use strong passwords.
- Do not write passwords down.
- Do not share passwords: never tell anyone your password.

1.2 The thinking behind these rules is depicted in Figure 1. The term "weak password" in the figure refers to so-called *common passwords* (See Section 4.4): e.g. a password which is a variant of a user's own name (Brown et al. 2004) or the system name (Bishop & Klein 1995) or a variation of a previous password (reuse) (Riley 2006) etc. A very common practice is *recycling* (Inglesant & Sasse, 2010), the use of the same password on more than one system.

1.3 The arrows in the diagram indicate a *conventionally assumed* causal relationship. So, for example, as more passwords are written down, so more will leak (become known to others), and this will reduce overall system security. The potential for increased security incidents increases, thus escalating the vulnerability of the systems. The dashed line indicates a more tenuous link: this causative will only occur if passwords leak outside the organisation. The certain danger is internal since most recorded passwords will be easily accessed by people within the trusted interior. The four causatives are on the left of the diagram and one

can see the attraction of attempting to tighten security by forbidding them. The assumption is clearly that removal of these triggers will eliminate those factors that lead to poorer system security.

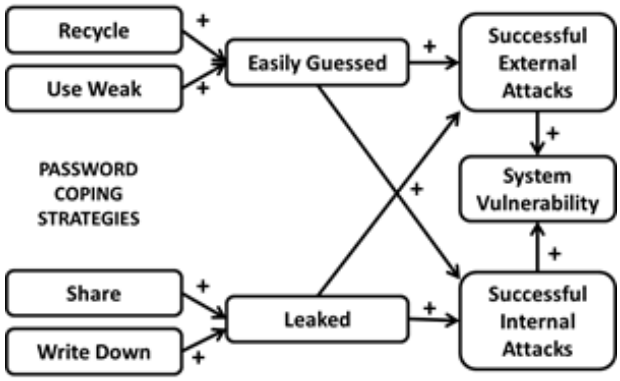

Figure 1. Commonly Deployed Coping Tactics to cope with Multiple Passwords

1.4 Unfortunately, the prevalence of these triggers shows that the practices in question will not be easy to eradicate. There is evidence that users engage in these potentially damaging user behaviours as *coping tactics* (Adams & Sasse, 1999), an inevitable result of people being unrealistically overloaded with passwords while having only limited human capability to cope with the memorial load.

1.5 When a prominent system such as Sony, is breached, researchers invariably report on the large percentage of "common" passwords chosen and the limited number of strong ones in use (See Section 4.4). This confirms that a large percentage of users choose weak passwords, even though they are probably aware that their accounts could easily be compromised as a consequence.

1.6 Some user behaviours have a wider impact than others. For example, a user may use the same password on all their systems at work and, if this password becomes known to another employee, there is an opportunity for much more damage than if no such recycling has been practised. Of course, if a user shares his or her credentials and another user logs in using these, there is no evidence that this masquerading has occurred. An audit might well conclude that a particular organisation's security is satisfactory without realising that people are using each other's credentials. Since non-repudiation is such a core concept of information security this user behaviour must be seen as constituting a threat of a fundamental nature.

1.7 It is inherently difficult to measure the true impact of password coping tactics on the security of the systems of any particular organisation. Password policies must be evaluated within the context of the entire organisational structure and not based on the behaviour of a few individuals. Moreover, it is clear that the view depicted in Figure 1 is rather naïve because it does not consider *why* people are tempted to use these coping tactics. There is an implication that undesirable password practices can be attributed to innate human weakness whereas, in fact, the system within which the human functions clearly plays a key role in inducing these user behaviours; in consequence, merely focusing on the symptoms and trying to eliminate them without identifying underlying causes is bound to fail. Figure 2 expands one part of systems diagram slightly, showing the interaction of a few more factors that common sense suggests could play a role in leading to leaked passwords.

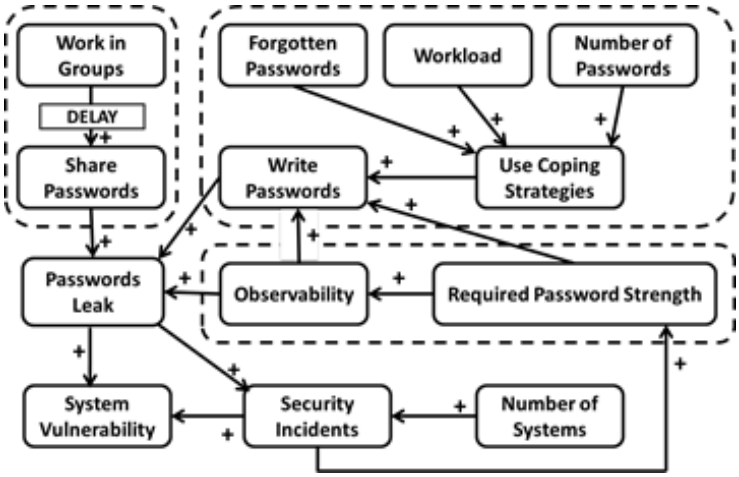

Figure 2. System Causatives and their Role in Leading to Undesirable Password Practices

1.8 For example, the response to a security breach is often a strengthening of password requirements (link from "security incident" to "required password strength" in the diagram). Tari et al. (2006) have shown that the more complex a password, the more easily it can be observed by another user (link from "required password strength" to "observability"). Complex passwords are also more easily forgotten, so users are probably more likely to write them down. Hence this effort to strengthen passwords may actually lead to more passwords being leaked.

1.9 Users do not operate in isolation: a number of factors may encourage them to behave in a particular way, and they often feel they have no option but to break rules which are very difficult or too constricting to obey. Hence great care needs to be taken to ensure that policy rules are indeed possible to follow, do not present users with an ethical dilemma and do not require too much effort (Inglesant & Sasse 2010).

1.10 For example, we know that when people work together in groups they will start to trust one another and share information. Sharing passwords is a natural extension in many scenarios and insisting that colleagues do not do so may present them with an ethical dilemma where the group sees itself as working together towards a common purpose. Denying a colleague the use of your password when he or she needs to make a contribution to this common purpose may be seen as unhelpful and so incur significant peer pressure (Renaud 2012).

1.11 Given the complex nature of the psychological and social factors at play, the typical degree of heterogeneity of the systems involved and the infeasibility of conducting live field studies in a real organisational environment, it is hardly ever feasible to gauge the impact of user password behaviours on the security of an organisation's systems by experimental means alone. A viable alternative is the use of computer, a well-established approach (Simon 1969) whereby a software model is abstracted from knowledge garnered from a set of observed real systems and then run with a range of input parameters of interest. It must always be borne in mind that observation of a real system is the only sure way to establish the level of accuracy of simulation predictions and thus *validate* the model in question. However, as we cannot, in general, test predictions across the whole parameter space, we extrapolate that a validated model will be able to make correct predictions across a generalised subset of the parameter space where conditions are similar to the validation points. With such reservations in mind, simulations are helpful in two ways: they can "explain" (in the sense of identifying a unifying model) retrospectively what has already been observed; more importantly, they can give insight into the functioning of systems of the modelled type, in particular, predicting user behaviour in previously unexplored regions of the parameter space.

1.12 It must be acknowledged, at the outset, that a simulation is only as good as the assumptions that are built into it and in what follows an effort has been made to ensure that the model rules and default input parameters are grounded in the literature wherever suitable studies exist. It is reasonable to assume that such a simulation can provide understanding and insight which is simply impossible to gain in a real-life setting. It can also help us to understand the wider effects of variations in individual human behaviours integrated across organisations, something almost impossible to gauge experimentally in the real world. As a result, it can assist us in understanding the often unexpected effects of particular policy directives. So, for example, if the organisation's auditors require password changes more frequently than previously, this requirement can be "plugged into" the simulation, and the net effect can be charted.

1.13 This paper reports on an actual implementation of just such a simulator, SimPass, an engine which models user password usage within an organisation. In a SimPass organisation, users authenticate using usernames and passwords, on a variety of different systems. Over time they manifest the kinds of behaviours their real life counterparts engage in. The simulation also includes hacker agents and malicious agents, both attempting to breach user accounts. At the end of the simulation the engine provides summary data related to the security of the system after a period of time, reflecting the impact of particular agent behaviours.

1.14 The rest of the paper is structured as follows. Section 2 briefly describes the simulation model: the main entities abstracted from real-world scenarios for the purposes of the simulation model and the behaviour of the agents within the simulation. Section 3 explains how the engine was implemented. Section 4 explains how the system is configured in order to test the effects of different policy and overall system settings. Section 5 gives an example of how a particular policy change was tested using SimPass and Section 6 concludes.

Simulation Model

2.1 Employees usually have an assigned position within a hierarchical organisational structure, as shown in Figure 3. Employees often work closely with other people in their "branch" of the structure, with infrequent interactions with other branches. They build relationships with their branch colleagues, and work towards a common purpose. In carrying out their duties they make use of one or more computer systems which can be internal or external, with respect to visibility to the outside world. Systems can be attacked by outside hackers and by internal malicious employees but the security of the organisation is also at risk from the ill-advised actions of well-intentioned employees.

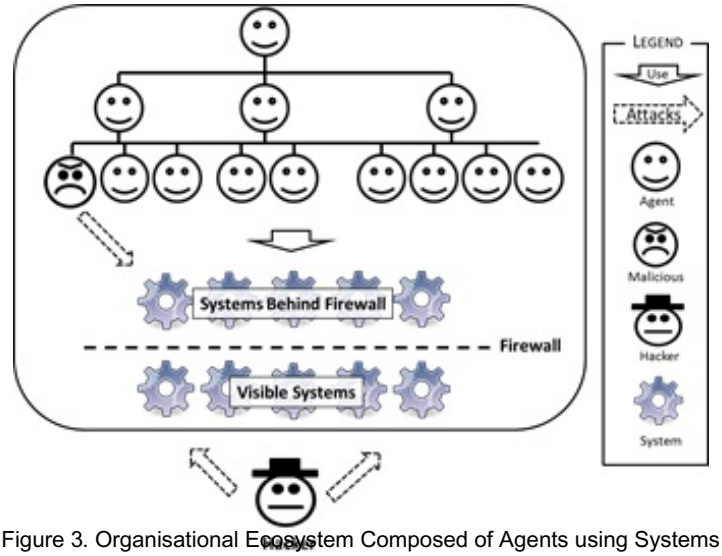

Figure 3. Organisational Ecosystem Composed of Agents using Systems

Model Entities

2.2 The key entities which SimPass abstracts are employees and systems. We begin by briefly examining the nature of each in turn.

Employees

2.3 Employees work within a particular environment, and are subject to the pressures of that environment: their position within the hierarchy, the tasks they are paid to undertake, their workload, the culture of the organisation and the quality of the relationship with their colleagues (Figure 4). They are also constrained by various information security policies.

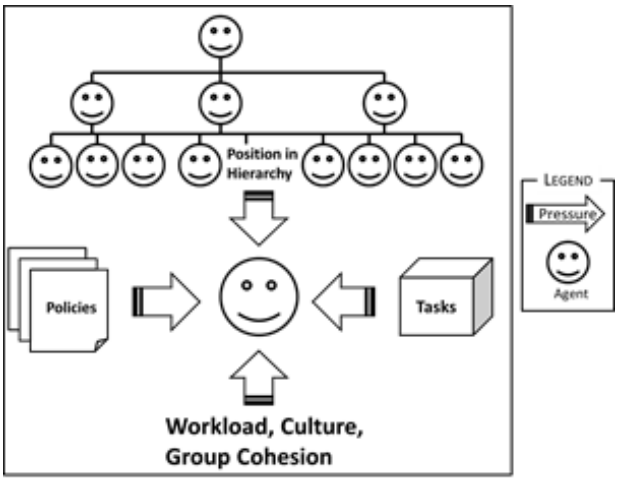

Figure 4. Pressures on Employees

2.4 Employees, as unique human beings with varying backgrounds and histories, come into the organisation with different approaches to life. They vary in numerous ways, but for the purposes of this discussion we are interested in a limited number of relevant characteristics which will impact on their password practices, as shown in Figure 5. For example, someone who is prepared to be dishonest might be tempted to steal a password from another employee. Some employees are willing to share passwords and others are not. Different individuals favour different password coping tactics : some use variants of their own names, while others use their telephone numbers, still others the names of pets etc. Sometimes employees become disenchanted and decide to do damage to the company, so they can be considered malicious.

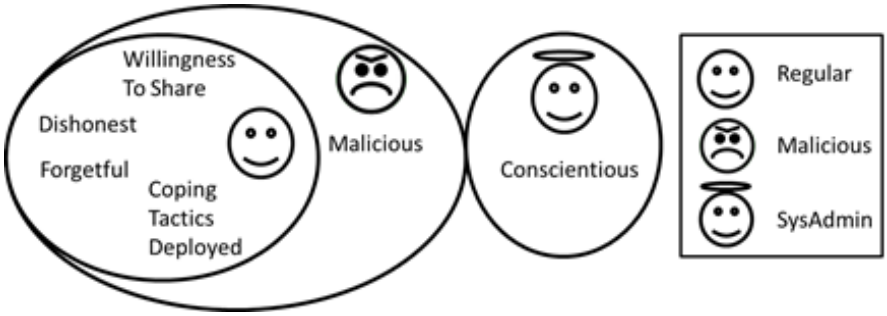

Figure 5. Employee Propensities

Systems

2.5 An organisation will typically have a number of software systems, executing on different hardware. Such systems are either visible to the outside world, or hidden behind a firewall. Some systems issue passwords while others allow employees to choose their own. Furthermore, systems can be configured to implement particular organisational rules, such as, for example password length, lockouts etc. SimPass's model of a system housed within the organisational context is shown in Figure 6.

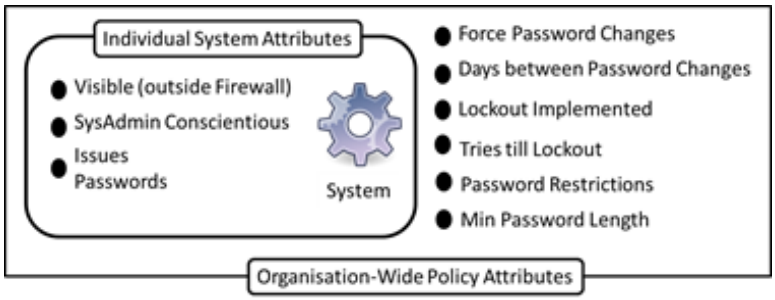

Figure 6. System Characteristics

Model Agent Behaviour

3.1 SimPass is a multi-agent system which simulates the organisational Ecosystem as described in the previous section. A SimPass agent is described as a 4-tuple:
$Agent=(Sit,Act,Dat,f_{Agent})$
where

- *Sit* is the set of situations the agent can be in,
- *Act* is the set of actions that the agent can perform,
- *Dat* is the set of possible value combinations of the agent's individual settings, and
- f_{Agent} is the agent's decision function, and can be expressed as follows:

f_{Agent}: $Dat \times Sit \rightarrow Act$.
There are four kinds of agents representing regular employees, system administrators, malicious employees and hackers (outsiders). These agents do not operate in isolation but interact with other agents regularly and in a variety of ways.

3.2 When the engine starts, systems and agents are created and configured with characteristics tailored as discussed in Section 4. The configuration settings are enumerated in the appendix. *Regular agents*, $Agent_{Regular}=(Sit, Act, Dat, f_{Regular})$ are simply trying to do their jobs by using the various systems they have credentials to access.

- *Sit* constraints are contextual, depicting the situation an agent is in. For example, an agent wants to log in, or needs to enrol for a new system.
- *Act* is the set of actions that the agent can perform in a situation. For example, if an agent forgets a password, it can be locked out, try to get a shared password, or try to steal a password.
- *Dat* is the set of possible value combinations of the agent's internal settings, as shown in Figure 5.

3.3 The other agents have more specific natures.

- *Malicious agents* $Agent_{Malicious}=(Sit, Act, Dat, f_{Malicious})$ will use their systems as usual, but sometimes they might try to try to use another agents' credentials perhaps because they have a grudge against their victims or because they wish to carry out fraudulent activity (attacks are randomly generated). If they decide to do this, they will use shared, stolen or guessed passwords to gain access to accounts with other employees' credentials. All such logins are termed "bad".
- *Hacker agents* $Agent_{Hacker}=(Sit, Act, Dat, f_{(Hacker)})$ try to attack the system from outside: trying to guess credentials without the ability to find written records, and only being able to access visible systems. Hackers can try to breach systems using well-known default system passwords, which might not have been reset by less conscientious system

administrators. They could also try to gain access to password files, which they can try usin brute force. Failing this, they can try a combination of user names and passwords to attempt to access the system. Successful hacker logins are also termed "bad".

- *Sysadmin agents* $Agent_{Sysadmin}=(Sit, Act, Dat, f_{Sysadmin})$ administer one or more of the systems in SimPass. These employees are generally considered to be honest: they do not engage in any of the harmful coping behaviours mentioned above. However a sysadmin may occasionally fail to attend to its duties by, for example, failing to patch a system for which it is responsible.

3.4 Agents are randomly assigned to an organisational management hierarchy thus ensuring that they work in groups, with a number of trusted "colleagues" whom they could on occasion ask to share passwords with them. Agents are initially given access to a limited number of systems. Each week thereafter a random number of agents will be required to enrol for additional systems, as is the case when one gains experience in a typical organisation.

Regular Agents

3.5 To support the information security principles of non-repudiation and authorisation, agents are given their own credentials, username and password for each of the systems to which they have access, and for a given individual the number of such systems tends to increase the longer he or she is employed. Each agent thus "owns" a set of credentials for each system which they use. Passwords are selected based on the characteristics of both the agent and the system involved, as shown in Figure 7. For example, if an agent sometimes recycles it might well use one of its existing passwords rather than choosing a new one. New passwords are chosen from a representative password repository (as described in Section 4.4).

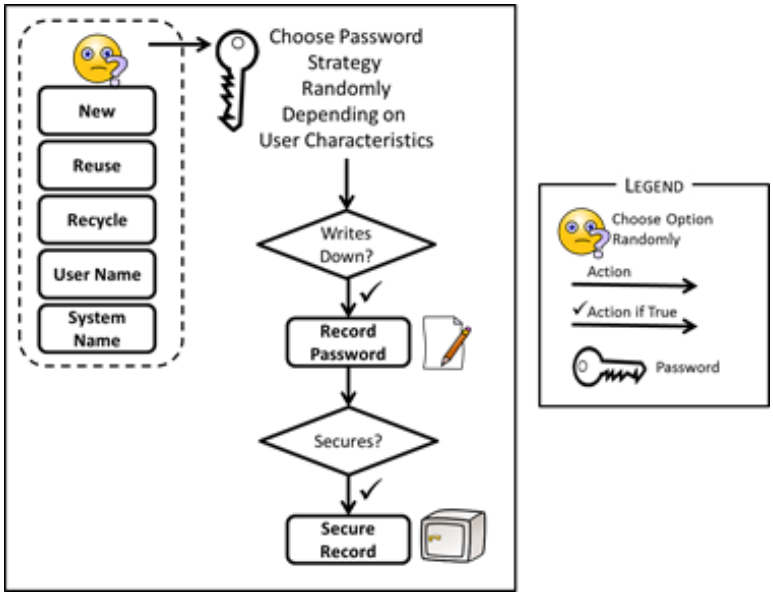

Figure 7. Actions For a Regular Agent Enroling for a New System

3.6 For each of the agent's systems a "next usage" is randomly chosen to be one of the following number of days: 1,2,3,7,14,30, 60, or 90, reflecting daily, frequent, weekly, bi-weekly, monthly and three-monthly usage. The choice is weighted to favour frequent accesses more than infrequent ones. This is achieved by selecting one of the appropriate time intervals from a list according to probabilities determined by associated weights as follows: 10,9,9,10,10,5,1,1. Thus daily usage will appear 10 times more often than 3 monthly usage.

3.7 As shown in Figure 8, agent A, when prompted to use its systems, will attempt to log in. If the password is remembered it will do so without incident. If not, a number of actions can result. It can accept that it is locked out, which means that it cannot complete its tasks for the day and must wait for a replacement password. If the work is urgent it could try to obtain credentials from another agent, B, either because the latter has willingly shared them, or because A has managed to obtain them dishonestly. The systems being logged into will never uncover this kind of activity, since it appears to be legitimate use by agent B and so the principle of non-repudiation is broken.

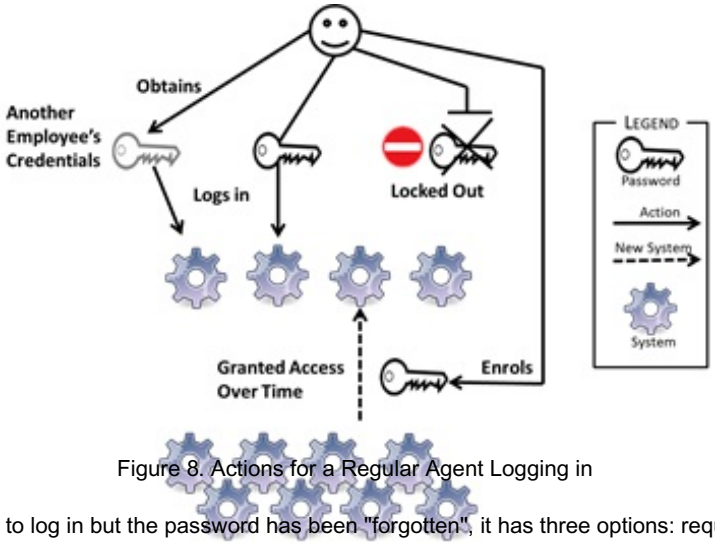

Figure 8. Actions for a Regular Agent Logging in

3.8 In summary, if an agent tries to log in but the password has been "forgotten", it has three options: request a new password and be locked out of the system; ask a fellow agent to share its password;, or try to steal one. The tactic is chosen randomly but with probabilities depending on the agent's propensities. For example, only dishonest agents will steal passwords. See Figure 9.

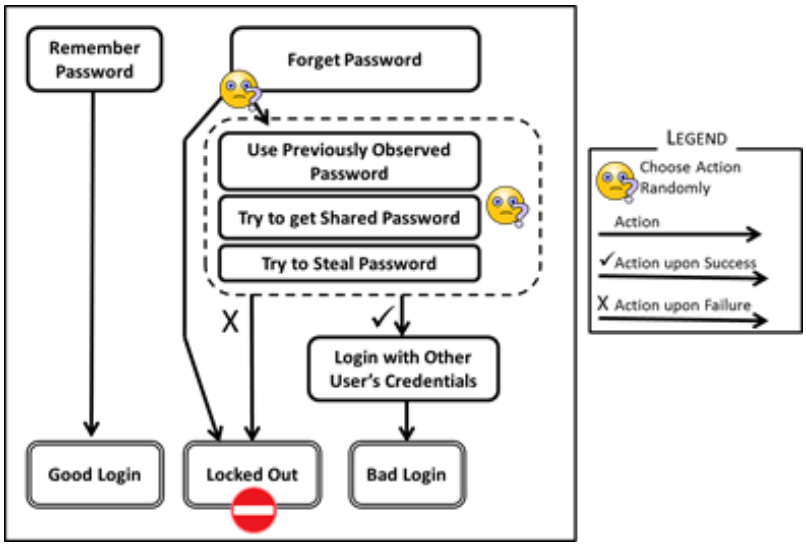

Figure 9. Actions for a Regular Agent Trying to Login

3.9 If an agent shares or steals a password and logs into the system using it, that is termed a "bad" login. An agent who logs into the system using its own credentials executes a "good" login.

Malicious Agents

3.10 A Malicious agent is an otherwise regular agent who, for whatever reason (e.g. revenge, fraud), tries masquerade as another agent credentials to gain access to systems. The attacking agent will use the following tactics to log into the target's account on some system:

1. Check whether the target agent has, some time in the past, shared a password with the attacker. The agent will test to see whether it is still valid.
2. Check whether the target has recorded its password, and not secured it. Try to access the system using this password.
3. Opportunistically try the following strategies:
    a. a randomly chosen common alphanumeric password string from a list maintained by SimPass. Examples are *123456*, *password1*, or *qwerty*;
    b. a variation of the username, eg *John1*; or
    c. a variation of the system name eg *Amazon1*.

3.11 If the malicious agent manages to breach the target's account, it will try to use the same password on other systems, in the hope that the target agent recycles passwords. It might also choose to change the target agent's password, thus locking the victim out, and disrupting its ability to do its job (see Figure 10).

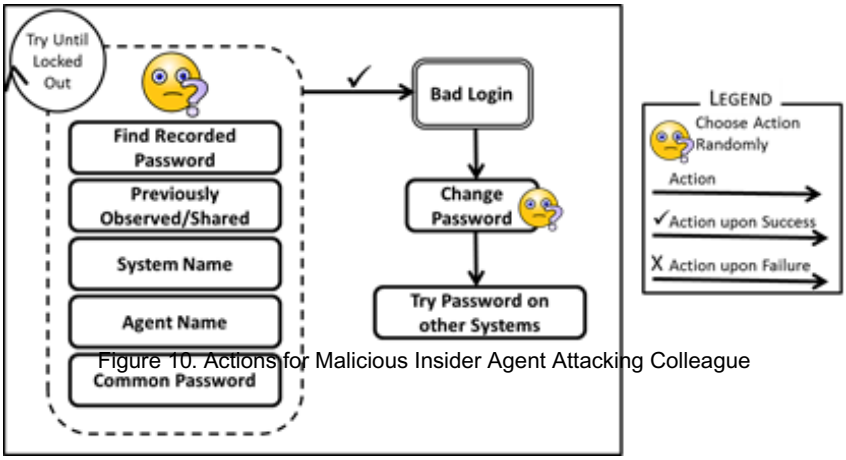

Figure 10. Actions for Malicious Insider Agent Attacking Colleague

Hacker Agents

3.12 Hackers often target specific organisations, for different reasons. Newspaper stories of their exploits are easy to find (BBC 2011). Hackers will first try the default password of all visible systems (van Doorn 1992) in the hope that the system administrator will not have reset these (Workman 2008). Hackers will also try to get hold of the password file if it this is not secured properly. With access to this file, a brute force attack will be carried out to try to determine the passwords for the listed agent names. Correctly guessed combinations will be used to break into systems. Their tactics are depicted in Figure 11.

3.13 The next step will be to try username-password combinations. Since these attacks are usually conducted without personal knowledge of system users, a targeted approach, where the hacker guesses a password for a specific user based on personal knowledge, is not usually feasible. SimPass hacker agents use a generic approach, simply trying various username and password combinations to see whether they can gain access:

- a randomly chosen common password from a list maintained by SimPass. Examples are 123456, password1, or qwerty;
- a variation of the username, eg *John1*;
- a variation of the system name, eg *Amazon1*

3.14 If the hacker agent breaches an account it might also change the victim's password, thus locking it out, and disrupting its ability to carry out its tasks.

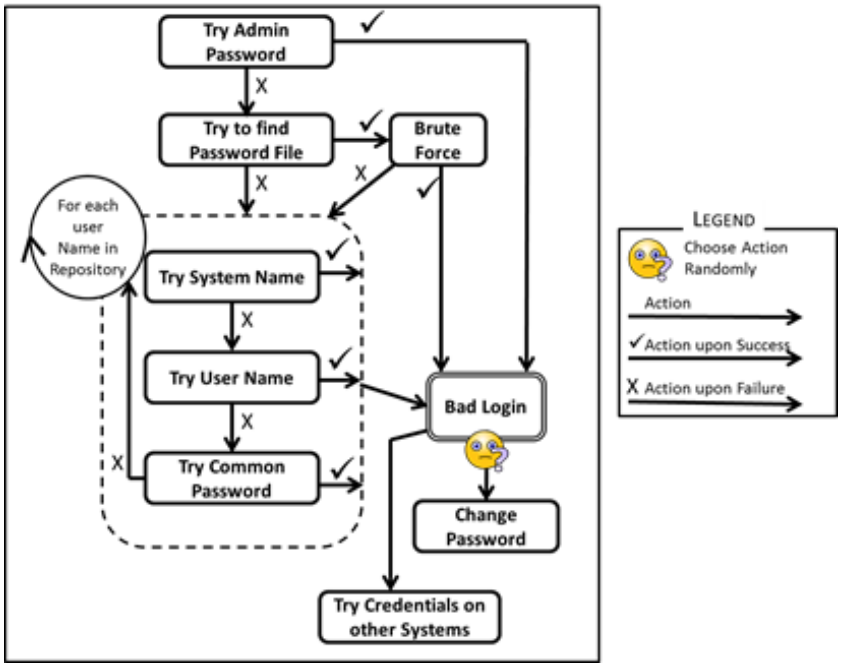

Figure 11. Actions for a Hacker Agent Attacking System

Systems Admin Agents

3.15 Systems admin agents are responsible for one or more systems into which they will randomly log in. If they are trained, they will change their systems' admin passwords, and keep the systems patched and the password files secured. Untrained systems administrators might well neglect these responsibilities and make it more likely that a hacker can breach the systems.

Summary

3.16 Table 1 summarises the internal settings of the different agents (*Dat*)

Table 1: Agent Internal Configurations

	Dishonest	Malicious	Forgetful	Sharing
Regular	Yes/No	No	Yes	Yes/No
Malicious	Yes	Yes	Yes	Yes/No
System Administrators	No	No	No	No
Hackers	Yes	Yes	No	No

The following section explains how the engine has been implemented.

Simulation Engine

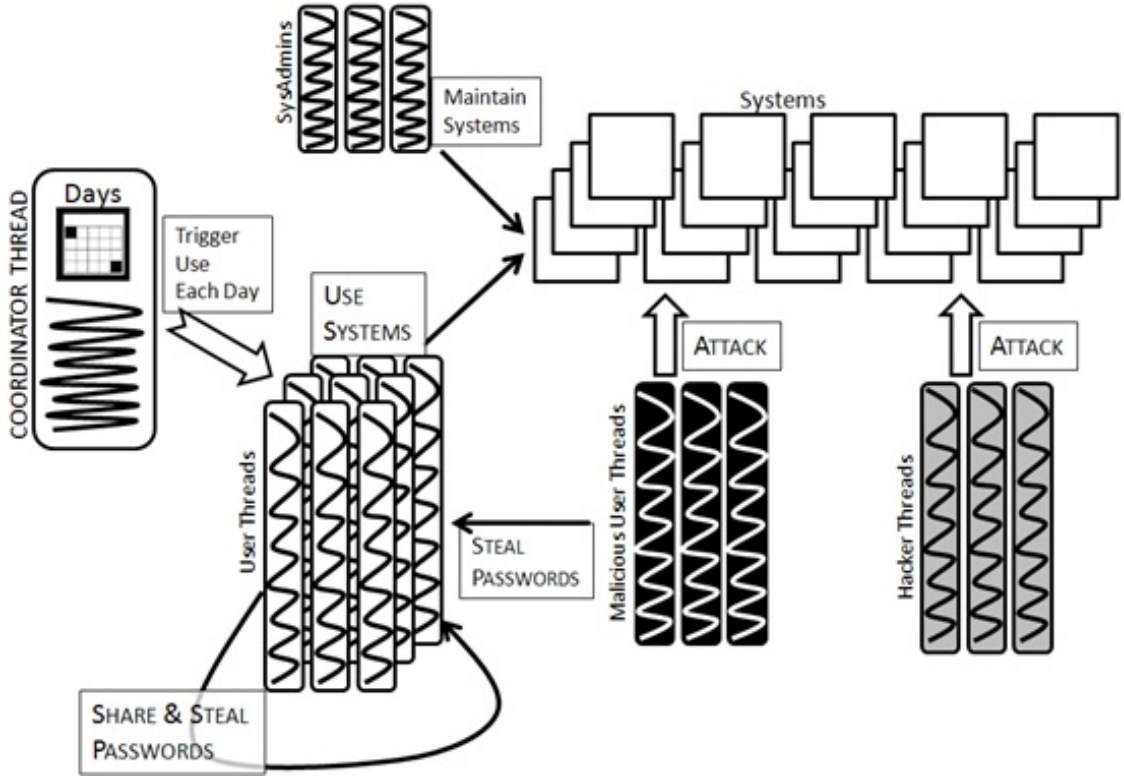

Figure 12. SimPass Architecture

4.1 SimPass is implemented in Java, as a multi-threaded application which generates discrete events at regular intervals, as shown in Figure 12. On startup it will read a configuration file, and initialise the simulation as follows:

1. An object is created to represent each agent and a thread launched for each (regular, malicious, sysadmin and hacker)
2. A system object is created for each "system" in the simulation.
3. A time manager object ensures that the simulation runs for as many days as specified. As each "day" starts, the time manager prompts each agent to log into those systems scheduled for use on that day. The time manager advances the day counter when all agents have concluded their day's tasks.
    a. Every time the agent logs in, the system randomly generates a "next use" until the simulation ends. When the "next use" day is chosen the system will decide whether the agent will forget the password or not, based on the literature on memorability (Section 4.1.1).
    b. The same mechanism applies to malicious and hacker agents who will, at random intervals, carry out attacks.
4. Agents interact with one another as they carry out their daily tasks.
    a. Sharing passwords with colleagues.
    b. Trying to find other agents' recorded passwords ie. stealing them.
    c. Observing each other typing in passwords. Whereas theft is goal-directed and will happen as a result of an agent's either having lost their own password or maliciously wanting to breach someone's account, observation can happen casually. Agents will not always "remember" an observed password: this, too, is randomised.
5. Agents and systems log all their activities to individual log files. At the end of the simulation a summary of all activity is printed to a summary log file to support further analysis.
6. SimPass keeps a tally of particular events in the system to support quantification of overall system security, as shown in Table 2.

Table 2: Events of Interest in the Simulation

Good login	A login where the agent uses his own credentials
Bad login	A login where the agent uses someone else's credentials (shared, observed, guessed or stolen)
Lockout	When a user has had to request a password reset
Stolen Password	A password which has been observed, and recorded, by another agent or where a written record of a password is discovered by another agent.
Shared Password	A password which the agent has willingly allowed someone else to use

Simulation Model Settings

Agent Characteristics

5.1 Various coping tactics are commonly used by people working with IT systems (Figure 13) and agents are designed to reflect these user behaviours. Each agent will deploy some, all or none of these mechanisms and will be subject to limitations reflecting those of average humans. Agent characteristics and how they help select default values for the input parameters to SimPass are discussed in the following subsections. Needless to say, each parameter can be varied from the selected default if desired, in order to explore the corresponding dimension of the input space.

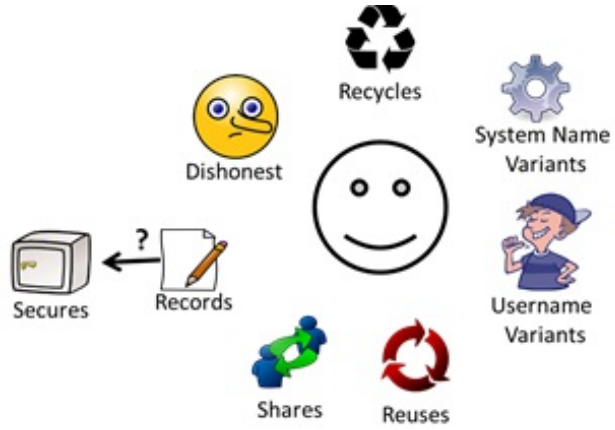

Figure 13. Agent Characteristics: *Dat(Regular/Malicious)*

Forgetting

5.2 A number of researchers have investigated forgetting rates. Florencio & Herley (2007) reported that 4.28% of regularly used passwords are forgotten. Bunnell (1997) reports on 27% forgetting rates after 2 weeks. Zviran and Haga (1993) reported on a 75% forgetting rate after 3 months. This was confirmed by Beedenbender (1990) who reported 72.8% forgetting after 3 months.

5.3 Some surveys have asked users to report on how many passwords forgotten after a month (Brown 2004), (Tamil et al. 2007; Elcomsoft Proactive Software 2009; Campbell & Bryant 2004). If the numbers of respondents are tallied, it becomes clear that 30% of passwords are forgotten after a month of non use. This is confirmed by the study carried out by Theusinger and Huber (2000) and by Brown et al. (2004), who found that 32% and 31% of passwords were forgotten by system users within a month.

5.4 As discussed in the psychological literature Ebbinghaus (1885), these figures are a good fit to a parabola with the formula:
$y=(-0.002)x^2+0.96x+3.04$
The forgetting rates used in SimPass, shown in Table 3, reflect this relationship.

Table 3: Forgetting Rates

Intervals	1	2	3	7	14	30	60	90
Forgetting %	4	5	6	10	16	30	53	73

5.5 In SimPass these forgetting rates will be tailored depending on how many times a specific password has been used in the past. A

frequently used password is less likely to be forgotten than an infrequently used password so the system will factor in previous use when deciding whether or not a password will be forgotten. Figure 14 shows the forgetting rates in a typical simulation run. The upper line depicts the values given in the above table, and the line below those generated by SimPass itself.

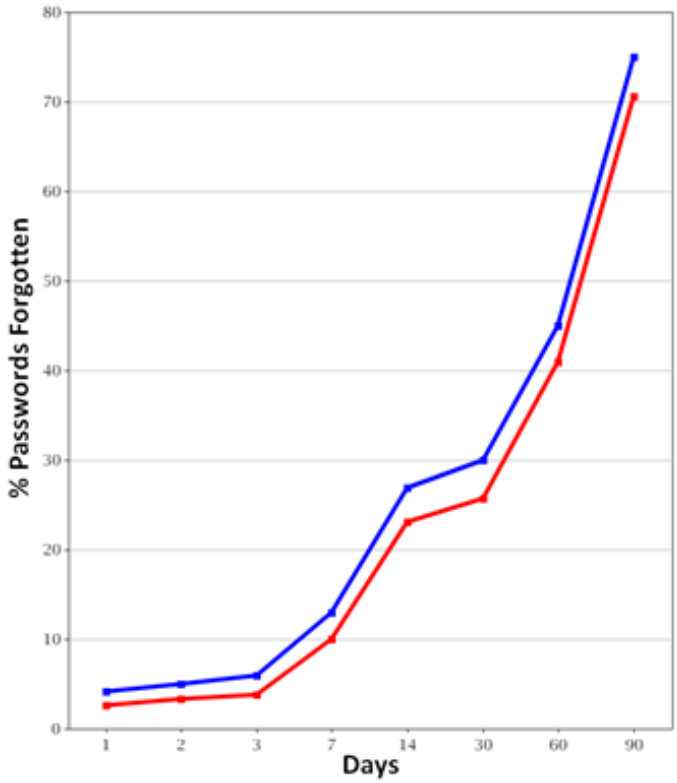

Figure 14. Forgetting Rates in a Typical Simulation (lower line=Simulation, upper-line based on forgetting rates)

Sharing of Passwords

5.6 Password sharing is strictly forbidden by most organisations yet the reality is that it is widely practiced. A number of password use surveys report on the prevalence of sharing (or at least reports on those who will admit to sharing). Martinson (2005) reports 38.1%, Bryant & Campbell (2006) reports 42%, Stanton et al. (2005) reports 34%, Tamil et al. (2007) reports 33.9% and Campbell and Bryant (2004) report 40%. However, Hoonakker, Bornoe and Carayon (2009) report that only 5% of respondents admitted to sharing passwords. It is possible that sharing is organisation-specific, but there may be other unreported factors at play here.

5.7 Since the majority of surveys report that close to a third of respondents share, and since most organisations find it difficult to accept any sharing at all, the default sharing percentage will be set to 33% but, as with all these values, this can be overriden in any SimPass simulation to explore the effect of different scenarios.

Stealing of Passwords

5.8 Using a stolen password is undeniably dishonest. How likely is it that an employee will do this? A quick look at dishonest behaviour in other settings is enlightening. Karstedt and Farrall (2006) found that 65% of people, given sufficient motivation, would behave dishonestly. Von Lohman (2004) reports on studies of P2P music sharing. Whereas 88% of the respondents in the study believed that this sharing was wrong, 56% still admitted downloading music illegally. Wilkes (1978) carried out a study into dishonest customer behaviour and found that for some offences between 70 and 80 percent of customers would offend. This study admittedly reports on customer behaviour, whereas SimPass is modelling employee behaviour. How honest can we expect employees to be? Wilson (2009) reports on a study by CyberArk, who surveyed 600 workers in New York and London. A surprising 48% said that they would steal their company's data if they were fired. Perhaps being fired constitutes sufficient motivation, but what about everyday behaviour? Wilkes (1978) cites a study by Tathum (1974) which reports that 50% of employees had admitted to stealing from their employers. Boye and Jones (1997) presented details of a study of restaurant employees which showed that 60% of respondents had stolen from their employers. There is some agreement that some organisations have more of a culture of dishonesty than others (Kidwell & Kochanowski 2005; Johnson & Philips 2003) and hence the dishonesty prevalence can be configured. The default prevalence of dishonesty in SimPass is 65%, taken from Karstedt and Farrall (2006).

5.9 Given the fact that someone is dishonest, does that necessarily mean that he/she will engage in stealing passwords? According to Cressey (1973), three elements must be present for a person to engage in dishonest behaviour: *motivation, rationalisation and*

opportunity. The latter could occur if someone sees another person entering their password, or if he/she finds a password that has been written down. *Rationalisation* can be assumed if a person is inclined to be dishonest: to varying degrees it or she will find an excuse for the dishonest behaviour. *Motivation* could be a function of the urgency of the task the agent is trying to engage in. A forgotten password that interferes with his need to use the system does not necessarily provide sufficient motivation since the use of that system might not be urgent. SimPass will randomly generate an *urgency* for each action, and this urgency will have to exceed a particular threshold level before sufficient motivation can be assumed. SimPass thus reflects the interaction of these three antecedents. SimPass will randomly choose a number between 0 and 9 to reflect urgency. If the number is greater than the threshold, default setting of 5, that is considered sufficient pressure to lead to dishonesty.

5.10 Certainly there is evidence that people do indeed steal passwords (Kidwell & Kochanowski 2005; Forbath 2005). but there is no hard evidence in the literature which quantifies the extent of the problem. In the absence of evidence we argue that, human nature being what it is, the literature mentioned in the previous paragraphs is a reasonable predictor of whether people will rationalise dishonest behaviour or not, in this case stealing and using someone else's password.

5.11 Reflecting their human counterparts, SimPass agents are also categorised as "dishonest" or "honest"; the latter will never steal a password, the former, given sufficient motivation, will rationalise the use of another's password. Agents can steal passwords that other agents have written down or recorded in some other unsecured way (the prevalence of this is discussed in Section 4.1.8). The former may, in addition to deliberately stealing a password, observe another agent entering a password and record it for later use. The observation rate for a simple password is set at 1% and for a complex password it is set to 2%. Moreover, an agent will only observe and record a password if it has sufficient motivation. The motivation in this case is that an agent has previously forgotten a password or passwords and therefore has a reason to want to guard against this eventuality in the future.

Username Variants

5.12 Brown et al. (2004) reported that 45% of users used a variant of their own name as their password. This was confirmed by Harada and Kuroki (1996) who found a prevalence of 42%. SimPass uses a default of 45%.

System Name Variants

5.13 Some people try to link their password to the system it is being used on, so as to increase their chances of remembering it. So, for example, they could use Amazon1 as their password for the Amazon website. Bishop and Klein (1995) reported that 11% of users employed of this tactic. Interestingly, however, Schneier[1] carried out an analysis of MySpace passwords and found the corresponding figure to be only 0.11%, which suggests that this prevalence varies across user populations. SimPass uses a default of 11% for this setting.

Recycling

5.14 Many users remember a few passwords and then use them across a number of systems. This coping tactic is probably the most common. Being able to predict the true prevalence of this coping technique is difficult, due to the different percentages reported by different studies. In order to use a realistic percentage a tally was made of all respondents who admitted to this practice from the studies reported by: (Hoonakker et al. 2009; Campbell & Bruyant 2004; Riley 2006; Zviran & Haga 1993; Tamil et al. 2007; Martinson 2005; Brown et al. 2004). 1592 of the total of 2966 respondents admitted to recycling passwords comprising 54% of those surveyed. Adams and Sasse (1999) reported a 50% prevalence and Summers and Bosworth (2004) report 55%. An analysis of actual leaked passwords from multiple systems show a recycling prevalence of 92% (Hunt 2011), and a survey reported by SecurityWeek (2010) reports that 75% of people recycled passwords. This suggests that many fewer people are prepared to admit to this practice than actually engage in it. SimPass uses a default of 54% based on the above composite tally.

5.15 Florencio and Herley (2007) found that users tended to maintain an average of 6.5 passwords, so SimPass agents do the same, the system ensuring that they have a maximum of 6 distinct passwords if they do indeed recycle their passwords.

Reuse

5.16 Some users will, when required to provide a new password for a system, simply vary the previous one: here this is referred to as reuse. Two studies have reported on the prevalence of this practice (Riley 2006; Hoonakker et al. 2009). 672 respondents out of a total or 1164 admitted to this practice (58%), which is used as the SimPass default.

Writing Down Passwords

5.17 Users often resort to writing down their passwords, or recording them in some other fashion. The following studies were consulted: (Zviran & Haga 1993; Brown et al. 2004; Martinson 2005; Hoonakker et al. 2009; Bryant & Campbell 2006; Stanton et al. 2005; Tamil et al. 2007; Riley 2006). Out of a total of 3386 respondents, 1309 admitted to writing their passwords down (39%). Only Hoonakker asked whether they also secured this password record and 18% said they did this. These values are used as the SimPass deafult settings.

Password Strength

5.18 There is some evidence that users, when forced to change their passwords, will choose a weaker password (Martinson 2005). A default of 68% was chosen based on this study.

System Admin Conscienciousness

5.19 We will assume that 77% of system administrators will patch systems and change passwords, with 23% leaving their systems unprotected. This is based on a study published by Microsoft (Forbath et al. 2005) which stated that only 77% of systems were patched, on average.

Threats

5.20 Threats are classified as internal or external depending on whether they are initiated by agents of, respectively, the malicious or hacker types. In SimPass, if a malicious (insider) agent or a hacker gains access to an agent's account it can decide to leave things as they are, or to change the agent's password. In the former case, details are always retained for later use so that if the hacked agent does not discover the hacker's activity the door is left open for later access. If the hacker decides to change the victim's password then the latter is prevented from accessing its account and will have the same choices as it has when it forgets its password.

5.21 If an attacker of either of the above types succeeds in breaching one account, it will try to get into the owner's other accounts using the same password, in the knowledge that many users recycle.

Insider (Malicious)Threats

5.22 Malicious insiders can cause a great deal of damage (Probst et al. 2010). Predd, Hunker and Bulford (2008) cite a survey by the Computer Security Institute which reported that the organisations that responded to their survey had attributed 40% of their losses to insider activities. It is much harder to predict the incidence of malicious insiders since many are undetected. Price Waterhouse Cooper's 2010 Information Security Survey found that 19% of large organisations and 5% of small organisations had reported staff using their systems for theft or fraud.

5.23 A 2008 Forrester Research report[2] proposed that 30% of security breaches were caused by malicious insider activity. PriceWaterhouse (2010) reports that organisations experienced an average of 45 incidents last year, suggesting that an average of 13 per organisation were caused by insiders. This argument cannot, however, be used to arrive at an estimation of the number of malicious insiders since multiple incidents could be caused by the same person. As Calder argues, it is difficult to arrive at a reliable estimate of the average incidence of malicious employees in organisations (Calder 1987).

5.24 What is interesting is evidence that, for whatever reason, incidents of this type are increasing year on year (PriceWaterhouse 2010). In 1969 Robin (1969) reported on malicious user behaviour in three companies. The number of employees apprehended was 0.48% per annum. However, Choo and Tan (2007) refer to research at the University of California at Berkeley which reported a 115% increase student dishonesty cases between 1995 and 2000. The former increase could well be attributed to increasing use of computer systems but the latter is less easy to explain.

5.25 Here, it was decided that the incidence of malicious employees would be set at 1%, in order to depict a relatively optimistic scenario but, of course,the figure can be set by the simulation user. Malicious agents may decide target specific individuals at random intervals, attempting to breach their accounts in order to do damage to them, or to use the account to carry out nefarious activities.

Outsider (Hacker) Threats

5.26 The number of hackers that will target a particular company's systems over a period of interest may vary widely. Here, a default of 3 hackers has been chosen, but this number is configurable. Hackers will attack at randomly assigned intervals, and will target a maximum of 10 agent accounts on any system before retreating to try again another day. This technique is deployed by many hackers, who do not wish their activity to be too easily spotted by vigilant systems administrators.

System Characteristics

5.27 Many aspects of systems can be configured (see Figure 6). The default values are grounded in the research literature, as with agent characteristics. When such research is unavailable, the simulation owner may provide settings to explore different scenarios. The following configuration aspects have default values but can be varied to explore the parameter space.

- *System Visibility*: Some systems are visible from outside the organisation, others reside behind the firewall and cannot be accessed. Visible systems are susceptible to outsider attacks. In SimPass, 50% of the systems are visible by default.
- *System-Issued vs Self-Chosen Passwords*: Some systems issue passwords and others allow agents to choose their own. Since there is no published evidence of the distribution, an arbitrary proportion of 10% of systems will do the former

and the rest will allow agents to choose their own passwords.

Some system characteristics are specified by the organisation, to align with their policy directives. Examples of these follow.

- *Password Changes*: This determines whether agents are required to change their passwords and, if so, the number of days between mandatory changes. The default setting is that changes are required and that 30 days will lapse between password changes. It is assumed that agents cannot re-use a previously used password but they can add a numeral to the end, as is commonly the case.
- *Lockout*: This value measures whether authentication attempts are limited. Since many systems apply the practice of three times lockout, this will be applied in SimPass.
- *Password Requirements*: Organisations often impose a minimum password length and complexity on their employees, regardless of what individual systems require. The most common of these is that a password must have a minimum number of characters, that it should contain a numeral, upper case characters and/or a special character.

Password Corpus

5.28 SimPass agents choose passwords for their systems, and a realistic password corpus is required. Various sites have had their passwords leaked and "post mortem" analyses have sunsequently been carried out. For example: Schneier (2006) analysed 34 000 passwords; Calin (2009) reported on an analysis of 9843 Hotmail passwords; Hunt (2011) analysed 77 million Sony passwords; and phished phpBB passwords were analysed by Graham (2009). A summary is given in Table 4.

Table 4: Stolen Password Analysis

	MySpace	Hotmail	Sony	phpBB
Common Passwords	2.7%		2.5%	> 10%
Numbers Only	1.3%	19%		
Lowercase Only	9.6%	42 %	45%	
Dictionary Word			64%	65%
Alphanumeric	81%	30%		
Alphanumeric & Special Char	8.3%	6%	4%	
Average Length	8	8	8	6

5.29 Disturbingly, 4% of phpBB passwords were variations of the word "password". When a number is used, in 45% of cases it is the number 1, and when a special character is used, it is most often "! ", followed by the ".". What these surveys show is that while the passwords used by a particular population vary significantly, users will often choose simpler and weaker options when given the option to do so. In SimPass the password corpus will include realistic percentages of representative categories of most major identified password types.

5.30 The password collection used by SimPass uses the percentages of passwords in each of the following categories as shown in Table 5. Note that a "people name" category has been included, despite having no evidence from the above analyses to support it. However, Medlin et al. (2005) found that 19.3% of the people in their study chose passwords which reflected family names. Such a significant number was thus worth including.

Table 5: SimPass Passwords

Common Passwords	10%
Numbers only	5%
One Word	30%
Movie Names	10%
People names	10%
A word followed by a number	20%
Two words	5%
Two words separated by a number	5%
Alphanumeric and a special char	5%

5.31 The list of common passwords was obtained from Whats My Pass (2008) and the words were mined from an online dictionary. The password corpus holds 100 000 passwords altogether. The minimum length of such passwords is 6 characters and the length extends to as many characters as specified by the simulation user.

6.1 To demonstrate the potential of SimPass here the issue of writing down passwords will be addressed to assess its impact in a scenario using mostly the deafult settings established above. Most organisations officially forbid the recording of passwords in this way but, despite this, many users do so anyway so that they will not forget their passwords. The perceived risk is that other people will find such records and exploit that knowledge, as depicted in Figure 15.

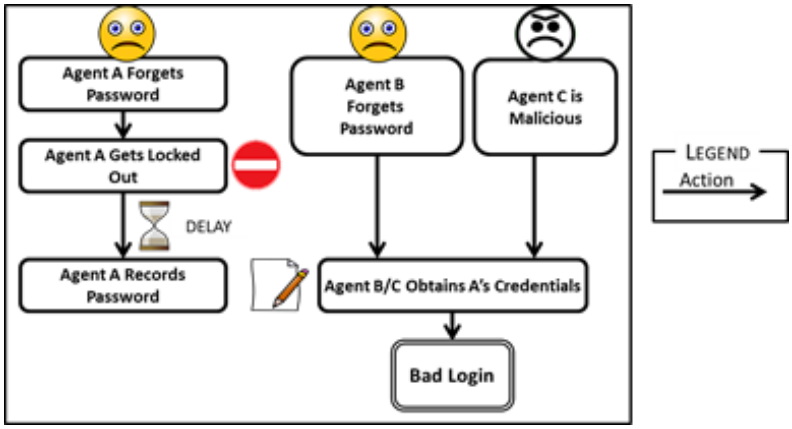

Figure 15. Writing Passwords Down

6.2 Whereas most current information security policies forbid the recording of passwords, an alternative approach might be to focus on reducing the incidence of forgotten passwords thus removing much of the motivation for passwords to be stolen. The expected downside would be an increase in vulnerability, if insecure recording methods were to make it easier for malicious employees to steal passwords should they still wish to do so.

6.3 To test the effect of writing down passwords on the security of the system, two simulations were executed, spanning 100 days with 100 agents using up to 27 systems simultaneously. One malicious and three hacker agents were introduced to attempt to breach visible systems at random intervals. The two simulations varied as follows.

- 39% of agents recording their passwords, either insecurely (in a spreadsheet, for example), or securely (using a password management application).
- 100% of agents recording their passwords, again securely or insecurely.
- The simulation was executed 100 times, and the resulting values for the following were averaged across all 100 simulations.
- Good and bad logins.
- % shared and % stolen passwords.
- Number of lockout events.
- Number of malicious logins and number of hacker logins during the 100 days.

In order to confirm the choice of running the simulation 100 times we calculated the 95% confidence intervals (t-distribution) for 50 and 100 runs as shown in Table 6.

Table 6: 95% confidence Intervals for Number of Simulations

		Confidence Intervals	
	% Recording Passwords	Number of Lockout Events	Number of Bad Logins
50 Simulations	39%	16.71% ± 0.48%	232.02 ± 6.01
	100%	1.42% ± 0.31%	19.06 ± 4.83
100 Simulations	39%	16.78% ± 0.35%	233.03 ± 6.30
	100%	1.63% ± 0.23%	22.59 ± 3.35

6.4 These figures show that the extra 50 samples do not really improve the confidence (already very high) that the difference between the 39% and 100% cases is a genuine effect and not just a sampling artefact. We were thus satisfied that 100 samples was sufficient to demonstrate differences due to configuration settings.

6.5 Figure 16 shows that the number of bad logins shrinks from 14.35% to 1.6% when agents record their passwords. The number of lockout events, as shown in Figure 17, shows a 90% decrease. This is a large effect from a relatively small adjustment to the system.

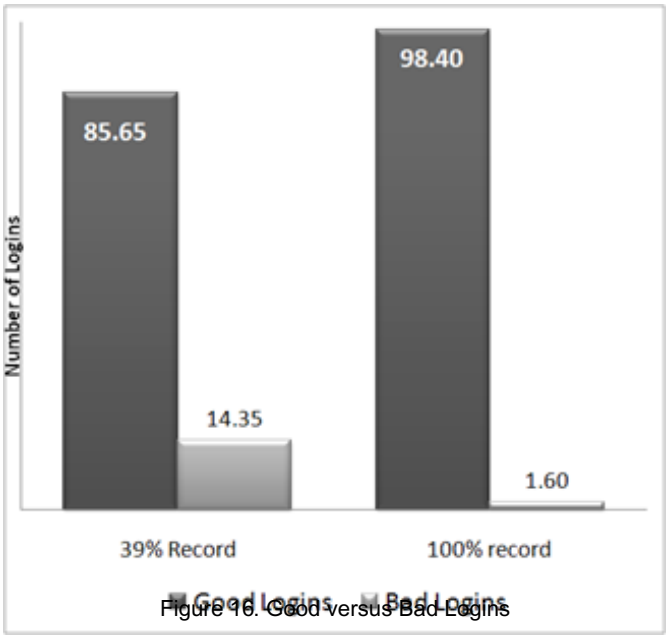

Figure 16. Good versus Bad Logins

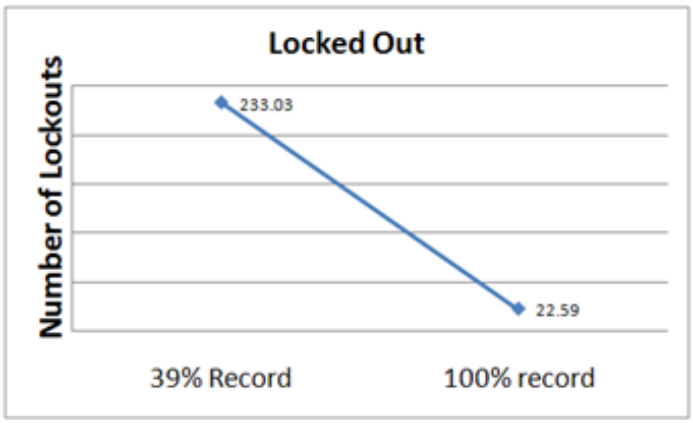

Figure 17. Lock Out Events

6.6 Has the security of the system been compromised to the same extent? As Figure 18 shows, the number of passwords either shared or stolen has been reduced, with the percentage of unleaked passwords increasing from 75.95% to 97.04%. This reflects the efforts of legitimate agents in the system. Figure 20 depicts the numbers of system breaches by malicious and hacker agents. There is indeed an increase in hacker successes. One possible explanation for this could be that forgotten passwords lead to password changes. SimPass systems do not permit use of previously-used passwords, so when passwords are frequently forgotten they change more often presenting hackers with a faster moving target. Even so, the increase in the number of attacks is relatively minor: from 15.34% to 17.95%. On the other hand, the number of malicious agent breaches decreases, the opposite of what is expected. This is due to the fact that malicious agents can and do make use of passwords that have been shared with them previously. That no longer happens since no one forgets passwords any more (the main causative behind sharing).

6.7 Table 5 shows the 95% confidence intervals for the malicious and hacker logins, which demonstrates that the differences are significant. Thus allowing people to write their passwords down does not lead to increased insider attacks - which is counter-intuitive. It is possible that we could mitigate the significant increase in hacker attacks by using other measures such as making passwords longer or more complex (and this will not impact on memorability since forgetting is no longer an issue).

Table 5: 95% confidence Intervals for Malicious and Hacker Logins

		Confidence Intervals	
	% Recording Passwords	Number of Lockout Events	Number of Bad Logins
50 Simulations	39%	16.71% ±0.48%	232.02 ±6.01
	100%	1.42% ±0.31%	19.06±4.83
100 Simulations	39%	16.78% ±0.35%	233.03 ±6.30
	100%	1.63% ±0.23%	22.59±3.35

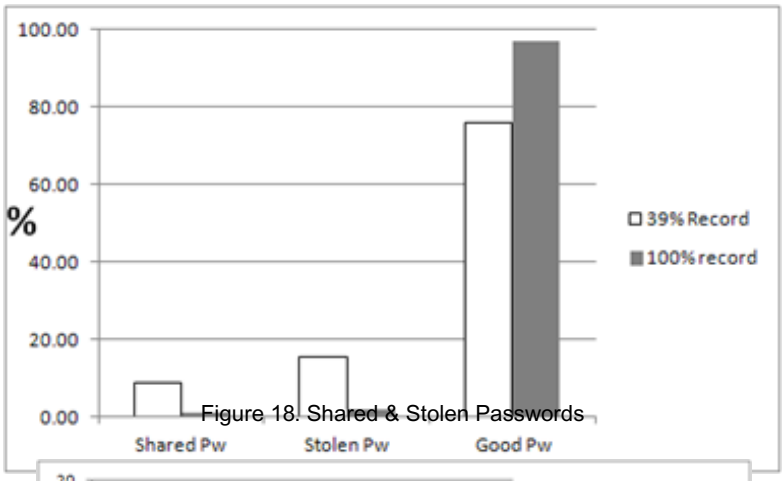

Figure 18. Shared & Stolen Passwords

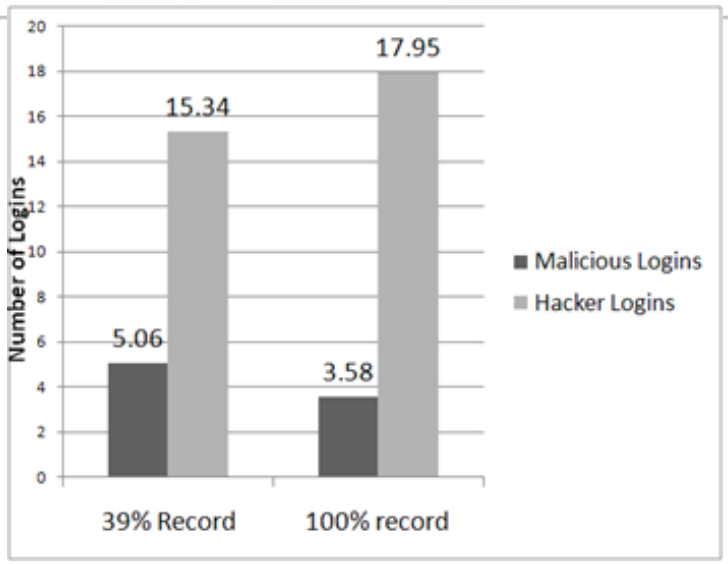

Figure 19. Malicious & Hacker Logins

6.8 What the simulations show is that, by removing the *need* for people to steal and share passwords, ie. eliminate forgetting, you can actually strengthen the system. If you remove the need of well-intentioned users to engage in these activities one is left with only the efforts of malicious employees and external hackers to compromise the security of the system. These threats are not controlled by security policies, but rather by auditing and other technical and management controls. Moreover, consider the significant reduction in the number of lockouts. Each lockout has an associated expense since the person will not be able to work while waiting for the password to be replaced. If a help desk has to be involved in the replacement the expense will be greater still. These results make it worth returning to Figure 1 and revising it, as shown in Figure 20. The apparently obvious causative link from people writing passwords down, to passwords leaking, and the systems' security being compromised, is not as clear cut as it appears to be. These findings should give system administrators pause, and make them think again before forbidding the writing down of passwords.

6.9 What these simulations show at a more abstract level is that one needs to tackle the cause of the problem rather than the symptoms to increase the overall security of an organisation.

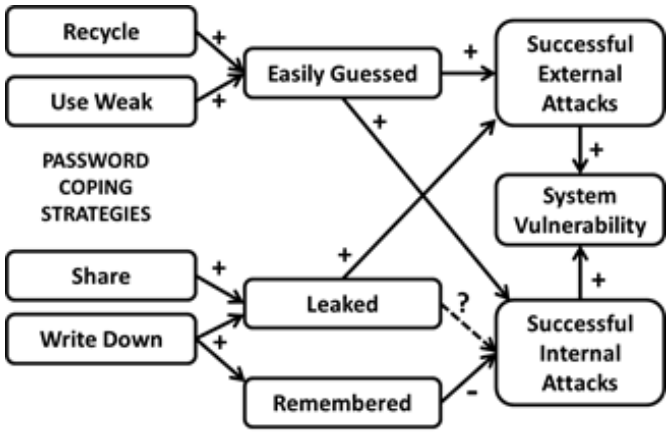

Figure 20. Revised Figure 1 (with a ? on the questionable link)

Conclusion

7.1 This paper has described the SimPass simulation model and engine, a first attempt to provide a mechanism for testing the effects of security policy directives. This tool simulates a number of different pressures and impacts on users and allows researchers to experiment with different settings in order to arrive at a particular set of policies which will deliver better security. It is necessary to abandon traditional thinking which mandates and forbids particular user behaviours, especially when such behaviours are effectively natural attempts to cope with the surfeit of passwords that is so characteristic of modern life. Using the tool we can come up with interventions and test such interventions once the simulation has been configured according to the specific organisation. In effect, it supports a systemic meta-approach to the problem of system security. The focus moves away from the user to the organisation and addresses the issue of what policy writers can do to achieve real security improvements.

7.2 In summary, SimPass is a flexible tool with many customisable input parameters. It makes it possible to test the effects on organisational security of varying one or more of these parameters, while holding others constant. It is ideally suited to allow IT managers to project the effect of suggested policy changes, including regulations and recommendations intended to change staff behaviour, on the overall ability of the organisation to resist attack.

Appendix

8.1 The following simulation settings are configurable in SimPass:

- The number of days the simulation should run
- The percentage of agents who write down passwords
- The percentage of agents who secure these records
- The percentage of agents who will share passwords
- Days between password changes
- Number of hackers
- Number of agents
- Initial number of systems to be assigned to agents
- Percentage malicious agents
- Percentage agents who have the potential to be dishonest
- Percentage of trained system administrators
- Percentage systems visible from outside
- Probability that agents choose weaker passwords after a change
- Number of tries before lockout
- Whether lockouts should be implemented or not
- Percentage of systems that enforce password changes
- Percentage of systems that issue passwords (as opposed to allowing agents to choose them)
- Minimum password length
- Whether passwords require numerals
- Whether passwords require uppercase letters
- Whether passwords require special characters
- Whether agents work in open plan offices or not (can password entry be observed?

Acknowledgements

We thank Joerg Denzinger for his very helpful comments on earlier drafts of this paper.

Notes

[1] http://www.schneier.com/blog/archives/2006/12/realworld_passw.html

[2] http://www.forrester.com/rb/Research/state_of_enterprise_it_security_2008_to/q/id/47857/t/2

References

ADAMS, A. and Sasse, M. A. (1999) Users are not the enemy: Why users compromise security mechanisms and how to take remedial measures. *Communications of the ACM*, 42(12), 40-46. [doi:10.1145/322796.322806]

BBC (2011) Sony faces legal action over attack on playstation network. BBC News, April. http://www.bbc.co.uk/news/technology-13192359.

BEEDENBENDER, M. G. (1990) *A comparison of password techniques*. Master's thesis, Naval Postgraduate School. Monterey CA.

BISHOP, M. and Klein, D. V. (1995) Improving system security via proactive password checking. *Computers & Security*, 14(3), 233-249. [doi:10.1016/0167-4048(95)00003-Q]

BOYE, M. and Jones, J. (1997) Organizational culture and employee counterproductivity. In R. A. Giacalone and J. Greenberg, editors, *Antisocial behavior in organizations*, pages 172-184. Thousand Oaks, CA: Sage.

BROWN, A. S., Bracken, E., Zoccoli, S. and Douglas, K. (2004) Generating and remembering passwords. *Applied Cognitive Psychology*, 18(6), 641 - 651. [doi:10.1002/acp.1014]

BRYANT, K. and Campbell, J. (2006) User behaviours associated with password security and management. *Australasian Journal of Information Systems*, 14(1). [doi:10.3127/ajis.v14i1.9]

BUNNELL, J., Podd, J., Henderson, R.,R. Napier, and Kennedy-Moffat, J. (1997) Cognitive, associative and conventional passwords: Recall and guessing rates. *Computers & Security*, 16(7), 629-641. [doi:10.1016/S0167-4048(97)00008-4]

CALDER, J. D. (1987) New corporate security: The autumn of crime control and the spring of fairness and due process. *Journal of Contemporary Criminal Justice*, 3(1), 1-34. [doi:10.1177/104398628700300402]

CALIN, B. (2009) Statistics from 10,000 leaked hotmail passwords, October. http://www.acunetix.com/blog/news/statistics-from-10000-leaked-hotmail-passwords//.

CAMPBELL, J. and K. Bryant. (2004) Password composition and security: An exploratory study of user practice. In S. Elliot, M.-A. Williams, S. Williams, and C. Pollard, editors, *Proceedings of the 15th Australasian Conference on Information Systems*. University of Tasmania, 2004.

CHOO, F and Tan, K. (2007) An "american dream" theory of corporate executive fraud. *Accounting Forum*, 31(2), 203-215. [doi:10.1016/j.accfor.2006.12.004]

CRESSEY, D. R. (1973) *Other people's money*. Patterson Smith, Montclair, 1973.

EBBINGHAUS, H. (1885) *Memory: A Contribution to Experimental Psychology*. Originally published in New York by Teachers College, Columbia University.

ELCOMSOFT PROACTIVE SOFTWARE. (2009) Password security survey 2009. http://www.siteglimpse.com/elcomsoft.com

FLORENCIO, D and Herley, C. (2007) A large-scale study of web password habits. In *WWW 2007*, Banff, BC. [doi:10.1145/1242572.1242661]

FIPS (1985) Federal Information Processing Standards Publication 112. Standard for Password Usage. http://www.itl.nist.gov/fipspubs/fip112.htm

FORBATH, T., Kalaher, P. and O'Grady, T. (2005) The total cost of security patch management, April 2005. Contact author on Theodore.forbath@wipro.com for copy.

GRAHAM, R. (2009) PhpBB password analysis, February 2009. http://www.darkreading.com/blog/227700652/.

HARADA, Y. and Kuroki, K. (1996) A study on the attitude and behaviour of computer network users regarding security administration. *Reports of National Research Institute of Police Science*, 37, 21-33.

HOONAKKER, P.,Bornoe, N. and Carayon, P. (2009) Password authentication from a human factors perspective: Results of a survey among end-users. In *Proceedings of the Human Factors and Ergonomics Society 53rd Annual Meeting*. [doi:10.1177/154193120905300605]

HUNT, T. (2011) A brief sony password analysis, 2011. http://www.troyhunt.com/2011/06/brief-sony-password-analysis.html.

INGLESANT, P. G. and Sasse, M. A. (2010) The true cost of unusable password policies: password use in the wild. In *Proceedings of the 28th international conference on Human factors in computing systems*, CHI '10, pages 383-392, New York, NY, USA. ACM. [doi:10.1145/1753326.1753384]

JOHNSON, L. and Philips, B. (2003) *Absolute Honesty - Building a Corporate Culture That Values Straight Talk and Rewards*

Integrity. Amacom, 2003.

KARSTEDT, S. and S. Farrall. (2006) The moral economy of everyday crime. *British Journal of Crimonology*, 46:1011-1036, 2006. [doi:10.1093/bjc/azl082]

MARTINSON, K. W.. (2005) Passwords: A survey on usage and policy. Master's thesis, Air Force Insititute of Technology. Department of the Air Force, Air University.

MEDLIN, B. D., Crazier, J. A. and Dave, D. S. (2005) Password selection by end users from an ecommerce site: An empirical study. In *Americas Conference on Information Systems (AMCIS)*, pages 3296-3305, Omaha, NE, USA, 11 - 14 August 2005.

PREDD, J., Hunker, J. and Buklford, C. (2008) Insiders behaving badly. *IEEE Security & Privacy*, 6(4), 66-70. [doi:10.1109/MSP.2008.87]

PRICEWATERHOUSE. (2010) Information security breaches survey 2010. http://www.pwc.co.uk/audit-assurance/publications/isbs-survey-2010.jhtml.

PROBST, C. W., Hunker, J., Gollmann, D. and Bishop, M. (2010) Aspects of insider threats. In C. W. Probst, J. Hunker, D. Gollmann, and M. Bishop, editors, *Insider Threats in Cyber Security. Advances in Information Security 49*. Springer, 2010. [doi:10.1007/978-1-4419-7133-3_1]

RENAUD, K.V. (2012) Blaming Non-Compliance is too Convenient: What really causes Information Breaches? *IEEE Security & Privacy*. 10(3), 57-63. [doi:10.1109/MSP.2011.157]

RILEY, S. (2006) Password security: what users know and what they actually do. *Usability News*, 8(1).

ROBIN, G. D. (1969) Employees as offenders. *Journal of Research in Crime and Delinquency*, 6, 17-33. [doi:10.1177/002242786900600103]

KIDWELL, J. Roland E. and Kochanowski, S. M. (2005) The morality of employee theft: Teaching about ethics and deviant behavior in the workplace. *Journal of Management Education*, 29,135. [doi:10.1177/1052562903261180]

SCHNEIER, B. (2006) Real-world passwords. http://www.schneier.com/blog/archives/2006/12/realworld_passw.html.

SECURITYWEEK. (2010) Study reveals 75 percent of individuals use same password for social networking and email, August 2010. http://www.securityweek.com/ study-reveals-75-percent- individuals-use-same-password- social-networking-and-email.

SIMON, H. A. (1969) *The Sciences of the Artificial*. MIT Press, 1969.

STANTON, J. M., Stam, K. R., Mastrangelo, P. and Jolton, J. (2005) Improving system security via proactive password checking. *Computers & Security*. 14(3), 124-133. [doi:10.1016/j.cose.2004.07.001]

SUMMERS, W. C. and Bosworth, E. (2004) Password policy: the good, the bad, and the ugly. In *Proceedings of the winter international synposium on Information and communication technologies*, WISICT '04, pages 1-6. Trinity College Dublin.

TAMIL, E. M., Othman, A. H., Abidin, S. A. Z., Idris, M. Y. I. and Zakaria, O. (2007) Password policies: A study on attitudes towards password usage amon undergraduate students in klang valley malaysia. *Journal for the Advancement of Science and Arts*. 3.

TARI, F., Ozok, A. A. and Holden, S. H. (2006) A comparison of perceived and real shoulder-surfing risks between alpahnumeric and graphical passwords. In *Proceedings of the second symposium on Usable security (SOUPS '06)*, pages 56-66, New York. [doi:10.1145/1143120.1143128]

TATHUM, R. L. (1974) Employees' views on theft in retailing. *Journal of Retailing*, 94,213-21.

THEUSINGER, C. and Huber, K.-P. (2000) Analyzing the footsteps of your customers - a case study by ask-net and sas institute gmbh. In *Proceedings WEBKDD*, Boston, August 2000.

VAN DOORN, L. (1992) Computer break-ins: A case study. In *Proc of the annual Unix User Group (NLUUG) Conference*, 143-151.

VON LOHMAN, F. (2004) Is suing your customers a good idea? September 29. Law.com. http://www.law.com/jsp/article.jsp?id=1095434496352

WHATS MY PASS? (2008) The top 500 worst passwords of all time, November 2008. http://www.whatsmypass.com/the-top-500-worst-passwords-of-all-time.

WILKES, R. E. (1978) Fraudulent behaviour by customers. *Journal of Marketing*, 42(4), 67-75. [doi:10.2307/1250088]

WILSON, T. (2009) Employees willing to steal data; companies on the alert, Nov 2009. http://www.darkreading.com.

WORKMAN, M., Bommer, W. H. and Straub, D. (2008) Security lapses and the omission of information security measures: A

threat control model and empirical test. *Computers in Human Behavior*, 24, 2799-2816. [doi:10.1016/j.chb.2008.04.005]

ZVIRAN, M. and Haga, W. J. (1993) A comparison of password techniques for multilevel authentication mechanisms. *The Computer Journal*, 36(3), 227-237. [doi:10.1093/comjnl/36.3.227]