Computer Science Department,
The University of Auckland,
New Zealand

Exploring the 'Weakest Link': A Study of Personal Password Security

Gilbert Notoatmodjo

Submitted, 15 July 2007
Accepted for MSc (First Class Honours), 15 November 2007
Minor revisions, 06 December 2007

Supervisor: Clark Thomborson

A THESIS SUBMITTED IN FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN COMPUTER SCIENCE

Abstract

The security of most password authentication mechanisms hinges on the secrecy of only a single word – if an adversary obtains knowledge of a victim's password, the adversary will be able to impersonate the victim and gain access to the resources to which the victim is entitled. Although cryptographic means and protocols offer some degree of protection during the transmission and storage of passwords, users are often left unprotected by nothing but security policies and guidelines which are often neglected. Various literatures have shown that users are the 'weakest link' in any password authentication mechanism, due to their propensity to create weak passwords and reuse passwords on multiple accounts. While various identity management solutions have been developed to address the prevalence of users' insecure password practices, these solutions still suffer from their own problems and drawbacks.

Before we could work towards a more appropriate solution to users' insecure password practices, it would be necessary to study the underlying cause of these practices, which lies within users' perceptions of their accounts and passwords. In this thesis, we present the findings from our exploratory, survey-based study, which investigated how user's perceptions of their accounts and passwords influence their password selection. Our findings revealed that our participants mentally classified their accounts and passwords in several groups based on various perceived similarities. We also discovered that they tended to use passwords that they perceived to be stronger and did not reuse passwords as often in account groups which they considered important.

Acknowledgement

After countless sleepless nights accompanied by hundreds of cups of coffee and bars of chocolate, finally comes the time to write my acknowledgement page. I would like to first and foremost express my gratitude to my supervisor, Clark Thomborson, for providing his constructive advice, guidance, expertise and friendship during this whole year (*…and free luncheon, a spot in a 'corner' office…the list goes on!* ☺).

I would also like to thank ('*Lord Professor')* Stephen Drape ('*FRS')*, ('*Dr.')* Anirban Majumdar, David Leung, Jasvir Nagra and Jinho Lee at the Secure Systems Group (SSG) for their friendship and support during this project. Thanks to Robin Young and Anita Lai from the Computer Science Department for providing me with all the necessary help during the survey and allowing me to use (*read: drag and abuse*) the departmental shredder. I am also grateful to Shirley Gaw at Princeton University for sharing her survey instruments.

Special thanks go to both of my awesome parents for their love, emotional and financial support, and also for coping with me during my *5th Eriksonian stage*. I would also like to credit my dad for raising my interest in computer security and my mom for her tireless efforts. Special thanks also go to Angela Halim from the Physiology Department for providing editorial help, constant support and TLC.

Last but not least, I would like to thank all participants who took part in this study (*and also all subjects who were involved in my earlier, not-so-ethical security 'experiments')*. As much as I would like to mention your names, my signature on the ethics application

form which was scribbled at a gunpoint prohibits me from doing so – I can only hope that the compensation was well spent!

Thanks to everyone who helped make this possible.

Table of Contents

Table of Figures

Table of Tables

"There is nothing more difficult to take in hand, more perilous to conduct or more uncertain in its success than to take the lead in the introduction of a new order of things. " –Niccolo Machiavelli

1
Introduction

As most modern computer systems are intended to accommodate multiple users, the ability to authenticate different users becomes imperative. Up to the time of this writing, password authentication is the most commonly used authentication method in computer systems. In password authentication, the identity of an individual is verified based on his/her ability to present a previously agreed word. For this reason, the security of password authentication schemes hinges on the secrecy of only a single word – if an adversary obtains knowledge of a victim's password, the adversary will be able to impersonate the victim and gain access to the resources to which the victim is entitled. Although cryptographic means and protocols offer some degree of protection during the transmission and storage of passwords, users are often left unprotected by nothing but security policies and guidelines which are often neglected, making them the 'weakest link' of any password authentication mechanism.

Previous studies have shown that users have a propensity to create weak passwords and reuse passwords across multiple accounts. Password reuse was cited in various literatures

as being a bad practice, because if one of users' passwords is compromised, then all their accounts that share the same password will also be at risk. While human memory capacity is very unlikely to increase significantly over the next few years, the proliferation of internet based services which require password authentication will force most users to reuse their passwords.

Many service providers attempt to minimize the risk of password reuse by forcing users to change their passwords on a regular basis and prohibiting them to reuse their passwords on their other accounts. These strategies left much to be desired, as they tend to add more burdens on user's cognitive load, leading users to devise their own methods for the sake of convenience, which is likely to result in even riskier practices. Various identity management solutions have also been developed under the assumption that decreasing the amount of passwords and associations that have to be managed would reduce the prevalence of password reuse and other insecure password practices. However, these solutions are not free from their own problems and drawbacks.

Before we could review existing solutions, or work towards a more appropriate solution to users' insecure password practices, it would be necessary to study the underlying cause of these practices, which we believe lies in users' perceptions of their accounts and passwords. While earlier studies discovered users' tendency to choose weak passwords by analyzing large collections of passwords, later studies have shifted their focus on users' insecure password usage behavior and revealed that users in fact tend to use stronger passwords and avoid password reuse on accounts which are perceived as being of high importance. By conducting an exploratory survey, we investigated how people's perceptions of their accounts and passwords influence the way in which they classify and associate their accounts and passwords.

1.1. What Is Identity?

Before continuing further, we discuss the meaning of the word *identity* and the concepts of identity as defined by Leibniz and Erikson, which we believe would give our reader a

better understanding of the concept of identity in the context of modern computer systems.

The origin of the word *identity* is from the Latin word *idem* [1], which roughly translates to 'the same' [2]. According to The Oxford English Dictionary [3], the current definition of identity includes:

1. (a) The fact of being who or what a person or thing is.

   (b) The characteristics determining who or what a person or thing is.

   (c) [as modifier] (of an object) serving to establish who the holder, owner, or wearer is by bearing their name and often other details such as a signature or photograph.

2. A close similarity or affinity.

The 17th century philosopher Leibniz defined identity in terms of a set of property P of Boolean-valued attributes or properties which might distinguish an entity *a* from any other entity *b* chosen from a set U of similar entities [4-7]. His principle of the *identity of the indiscernibles* states that if two entities *a* and *b* have identical values on all their properties, then *a* is identical to *b*. This principle can be stated formally in predicate logic as follows:

$$(\forall\, a, b \in U) (\forall P \in P) [(Pa \leftrightarrow Pb) \rightarrow a = b]$$

Equation 1: Identity of indiscernibles expressed in predicate logic.

Conversely, Leibniz also defined that two entities can only be identical, if they have identical values on all their properties. This principle is known as the *indiscernibility of identicals,* and is formally expressed in predicate logic as:

$$(\forall\, a, b \in U) (\forall P \in P) [a = b \rightarrow (Pa \leftrightarrow Pb)]$$

Equation 2: Indiscernibility of identicals expressed in predicate logic.

Both of these principles are widely known as the Leibniz's Law, which forms the foundation of the concept of identity in classical philosophy.

On the other hand, Erikson, a German psychoanalyst defined identity as a subjective sense an individual has of their personal characteristics and uniqueness from other people, which constantly changes as the individual gains new experience through his/her interactions with others [8, 9]. In [9], Eriksson outlined his theory of the development of identity in eight-stage process, which extends from an individual's birth to his/her adulthood.

Stage	Age Range	Psychosocial Crises	Related Elements of Social Order	Radius of Significant Relations
Stage 1	Infant	Trust vs. Mistrust	Cosmic Order	Maternal Person
Stage 2	Toddler	Autonomy vs. Shame/Doubt	Law and Order	Parental Person
Stage 3	Preschooler	Initiative vs. Guilt	Ideal Prototypes	Basic Family
Stage 4	School-Age Child	Industry vs. Inferiority	Technological Elements	Neighbourhood, School
Stage 5	Adolescent	Identity vs. Role Confusion	Ideological Perspectives	Peer Groups, Model of Leadership
Stage 6	Young Adult	Intimacy vs. Isolation	Patterns of Cooperation and Competition	Partners in Friendship, Sex, Competition, Cooperation
Stage 7	Middle-Age Adult	Generativity vs. Stagnation	Currents of Education and Tradition	Divided Labour and Shared Household
Stage 8	Older Adult	Ego Integrity vs. Despair	Wisdom	Mankind

Table 1: Erikson's eight stages of identity formation (adapted from [9]).

It is obvious that Leibniz and Erikson looked at 'identity' from two distinct perspectives. Leibniz viewed identity as a neutral set of attributes that defines the uniqueness of an entity, whereas Erikson viewed identity as individuals' subjective perceptions of their own uniqueness, which are developed through a personal process. Both of these concepts are relevant to the concept of identity in modern computer systems, or often termed *digital identity*. In the next section we present some background information on digital identity, and discuss how digital identity is viewed from both system providers' and users' perspectives, which resemble Leibniz' and Erikson's concepts of identity respectively.

1.2. Digital Identity

In the context of modern computer systems, identity (or digital identity), can be defined as digital representation of entities, including both human and non-human, which consists of one or more attributes. In this thesis, we do not discuss the application of digital identity on non-human entities; instead, our primary focus in this thesis will be digital representation of human entities.

Some of these digital representations only exist as a result of storing information in digital format and are only used for recording purposes, whereas some others are used to satisfy the security objectives of a system. While every service provider has different security requirements, most of them can be generalized into three main headings (CIA, in short) [10, 11]:

1. **Confidentiality**
   This requirement ensures that resources can only be read by authorized individuals.

2. **Integrity**
   This requirement ensures that resources can only be modified by authorized individuals.

3. **Availability**
   This requirement ensures that all authorized individuals are always able to perform all operations and access all resources for which they have the rights to.

There are two steps involved before an individual is granted access to a resource by a service provider. The first step is the process of confirming the identity of an individual**,** which is known as *authentication*. This process is then followed by granting access privileges to the authenticated individual, which is known as *authorization.* To ensure that these procedures act in accordance with the security requirements, they are usually

supplemented by another procedure known as *audit*, which is the process of recording and examining the identity of individuals and resources involved in operations performed within the system [10, 11]. Together, authentication, authentication, and audit are known as 'the gold standard of computer security' [1] [11].

During the authentication process, an unknown individual *u* presents a claimed identity, $a \in U$ and a set of claimed properties $C_i a$. The system then attempts to verify this identity claim by comparing the claimed properties $C_i a$ to the set of previously recorded properties of *a*, $P_i a$. This procedure normally follows the aforementioned Leibniz Law, that is**,** if the claimed properties match, the system then authenticates *u* as *a*.

$$(\forall u, a \in U) (\forall P \in P) [(C_i a \leftrightarrow P_i a) \rightarrow u = a]$$

Equation 3: Authentication process expressed in predicate logic.

The assumption that has to be taken by service providers is that only the individual who presented or was assigned a particular set of attributes during the enrolment process would be able to present the same set of attributes in the authentication process.

Digital identity attributes are also used in a process called *identification*, which is defined in [12] as a process of recognizing an entity. Due to their similarity, the terms identification and authentication are often used interchangeably by practitioners, and as a result the distinction between them has become rather vague. However, there are still differences between these two processes. Contrary to authentication, in identification the system is given a set of properties $P_i u$ for some unknown individual *u*. The system then attempts to identify the individual, that is, to find a known entity *a* whose properties $P_i a$ match $P_i u$. Not all attributes which can be used for authentication are suitable for identification, and vice versa. Our main focus in this thesis will be the usage of digital identity attributes in authentication process rather than identification.

[1] 'Gold' here is a mnemonic which contains dual meanings. ***Au****thentication*, ***Au****thorization* and ***Au****dit* all begin with ***Au***, which is the chemical symbol for gold, from the Latin *Aurum.*

Based on the types of digital identity attributes used to verify identity claims, authentication can be classified into three main categories [10, 13-15]:

1. **Knowledge-based authentication (what the person knows)**

   In knowledge-based authentication, the identity of an individual is verified by his ability to demonstrate one or more pieces of information, which is assumed to only be known by that particular individual. O'Gorman [14] drew a distinction between 'secret' and 'obscure' (or 'secret from most people') information used in knowledge-based authentication.

   Some examples of 'obscure' knowledge-based attributes which are often used include grandmother's maiden name, prior names, date and place of birth, and so on. Regardless being relatively 'weak', this type of information are still used to authenticate individuals in various instances, an example being telephone banking in case of lost PIN. Examples of information which is considered more 'secret' include password and PIN (Personal Identification Number). Interestingly, it is not uncommon for people to use 'obscure' phrases and obvious number sequences, such as '1234' or 'password' as their passwords and PINs.

   The main issues with knowledge-based authentication are that that this type of information is often forgotten or disclosed to other people, either deliberately or as a result of deception or trickery [13, 16-18]. Knowledge based authenticators also tend to become less secret each time it is shared for authentication [14]. These issues could lead to discovery by others, which could potentially result in identity theft.

2. Token-based authentication (what the person has)

In token[2] based authentication, the identity of an individual is verified by means of one or more physical objects (or tokens) that the individual has in possession [13-15] . In most cases, these tokens are assigned by service providers.

A few examples token-based authenticators from pre-digital period, most of which are still used up to the time of this writing are written documents, such as birth certificates and driver's licenses. Examples from the digital era include smart cards, RFID (Radio-Frequency Identification) tags and so on.

The main issue with pure token-based authentication is that tokens are relatively easy to be lost or stolen and exploited by finders, since anyone who is holding a token would be recognized as a legitimate individual. However, one of the advantages of using physical tokens is that in the case of lost or stolen tokens, owners can quickly realize, and apply preventive measures accordingly. Depending on the complexity of tokens, duplication and forgery might also be an issue [13, 14].

3. Biometrics authentication (what the person is)

In biometrics authentication, physical and behavioural characteristics are used as means to verify the identity of individuals. These characteristics are often not 'secret', as most of them can be freely seen or observed by others. Jain [19] defined four requirements of physical characteristics which are suitable for biometrics authentication, which include *universality* (the characteristic can be found in all individuals within the authentication boundaries), *distinctiveness* (the same characteristic of any two persons should be sufficiently different to distinguish them), *permanence* (the characteristic should remain sufficiently unchanged over a period of time), and *collectability* (the characteristic can be

[2] Token in this context refers to hardware or physical token, or sometimes called 'metal keys', rather than software token or cryptographic keys.

quantitatively measured). Examples of biometric characteristics which are commonly used include face, fingerprints, hand geometry, iris, and voice.

a).  b).  c). 

Figure 1: Examples of biometric characteristics a). Fingerprint, b). Iris, c). Hand geometry.

Biometrics authentication provides somewhat greater degree of confidence than knowledge-based authentication and token-based authentication, because physical characteristics are reasonably difficult, though not impossible, to steal, change or forge [20]. However, unlike passwords and token-based authentication, matching users' biometric characteristics to previously enrolled samples is probabilistic due to the nature of the data, i.e. two samples of the same biometric characteristic from the same person will not be exactly the same at any two given occasions, which may result in false negative and false positive occurrences[19, 20].

Improperly designed biometrics authentication mechanisms and protocols which are prone to attacks [20, 21] could easily expose users' biometric characteristics to the attackers. This problem becomes rather serious in biometrics authentication; because once a biometric characteristic is compromised, it would be very difficult to revoke due to its permanence. Biometrics authentication typically requires considerably high infrastructure cost [14, 22], which is perhaps the main reason why biometrics authentication has not been widely adopted despite its promising potential.

There are occasions in which combinations of these attributes are used in authentication process, in order to provide a greater degree of confidence and assurance. This is known as *multi-factor authentication* [14]. One example of this is the combination of bank card

and PIN. If the card somehow falls into the hands of an adversary, PIN would provide a second layer of protection, such that it would prevent the adversary from performing any transaction without acquiring the PIN. Another example of multi-factor authentication is biometrics passports, which combines biometrics and token-based approaches.

Figure 2: New Zealand Biometric Passport. The new biometrics passports, marked with a small symbol on the front cover, contain small RFID chips which stores biometric details of the passport holders. These passports, which adopt both biometrics and token-based authentication approaches, are an example of multi-factor authenticators.

From users' standpoint, the way digital identity is viewed shows close resemblance to Erikson's view of identity (Section 1.2.). As humans become increasingly reliant on computers in their daily tasks, the number of services that require authentication also increases. At the time of this writing, it is not uncommon for a regular user to maintain several accounts which require different means of authentication with various attributes. For this reason, the management of digital identities has become a rather personal matter to users, in which their subjective perceptions play a significant role. These perceptions are very likely to change as they accumulate more accounts and gain more experience.

It has been proposed in various literatures that users adopt different usage profiles (or often termed *digital persona*) according to the context of their accounts and the type of relationships they form with other users. In the next section, we present some background information on *digital persona*, which we believe will help us to understand how people's perceptions influence the management of their digital identities.

1.3. Digital Persona

The word *persona* originates from a Latin word which translates into 'mask' [23]. The concept of different personae within an individual was first developed by C.G. Jung. Using 'mask' as an analogy, Jung in [24] defined 'persona' as the personality which is presented to the outside world. Individuals may adopt different personae (or change their 'masks', following the analogy) according to the current situation or other individuals they interact with.

In the computing field, the term *persona* has been used in various contexts. In a subfield known as Human Computer Interaction (HCI), the terminology *persona* is used to represent the description of user archetype which is used as an aid during interface design process [25-28]. In Artificial Intelligence (AI), the term *persona* has also been used to represent various intelligent agents [29-32].

In the context of digital identity, (digital) persona is often used to represent separation of information based on different usage profiles. Clarke [33] formally defined *digital persona* as: "A model of an individual's public personality based on data and maintained by transactions, and intended for use as a proxy for the individual."

The need for separation of information based on users' personae in modern computer systems has been discussed in various literatures. Li [34] in her thesis on fifth generation messaging systems, identified the need for accommodating such separation in the proposed messaging system for both privacy and convenience purposes. Li's work was later extended by Mutu-Grigg [35], who discussed possible implementations of Li's concepts, and Leung [36] who further developed the persona notion to propose an improvement to operating systems, by separating a user's workspace based on various usage profiles of the access privileges assigned to the user. Baier and Kunze [37] also highlighted the importance of persona separation in identity management systems.

Suler in [38] writes that internet users often adopt many digital personae, which can either be real-to-life, imaginary or hidden, depending on the nature of services offered by the service provider and people they interact with. He also suggests in [39] that users often seek to compartmentalize and disassociate their personae, especially when these personae are considered incompatible with each other, for example, the president of a large corporation may need to keep his participation in online dating services separate from his business personae.

As users attempt to compartmentalize and disassociate their digital personae, it is very likely that they will intuitively classify their accounts according to how their accounts are perceived to match their differing personae. We believe that the concept of digital personae will help us to investigate how users' perceptions influence the way in which they classify and associate their accounts and passwords. We will discuss how we use this concept as an organizing idea for our study in Chapter 3.

The rest of the thesis is structured in the following manner: Chapter 2 discusses password authentication in further details, along with current issues and solutions. Chapter 3 describes the motivation of our survey based study and reviews ten user studies which have been discussed in previous literatures. Chapter 4 describes our survey design along with our ethical concerns and considerations which influenced the design of our survey methodology. Chapter 5 presents our findings, while Chapter 6 discusses the implication of our results and concludes our thesis.

"When ideas fail, words come in very handy. " –Johann Wolfgang von Goethe

2

Password Authentication

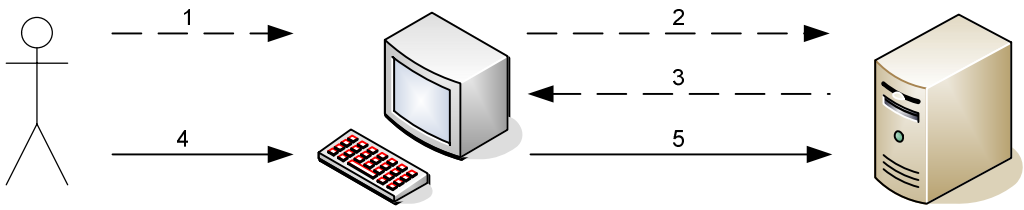
In this chapter, we present a general overview of password authentication and discuss various issues with password authentication, including known attacks and users' insecure password practices. We also describe and review various identity management solutions which are developed to address these insecure practices.

2.1. Overview of Password Authentication

The origin of password authentication could perhaps be traced back to the ancient secret societies, when secret phrases are used as one of the means of identification among their members [40]. Passwords have also been used throughout military history as a way to distinguish friends from enemies [10]. At the present time, a password is by far the most common authentication method used in modern computer systems.

The attractiveness of password based authentication does not lie in its strength or security, but in its simplicity and relatively inexpensive cost, not only in terms of financial cost, but also time and practicality. Lampson [11] argues that perfect security is not practically feasible; consequently, decisions regarding the choice of security mechanisms,

including authentication methods are usually made by balancing the tradeoffs between the cost of protection and the risk of loss. Although biometrics and multifactor authentication are known to provide a greater degree of confidence compared to password based authentication, until the time of this writing, they are normally associated with rather expensive infrastructure cost, which deter most service providers from adopting them [14, 22].

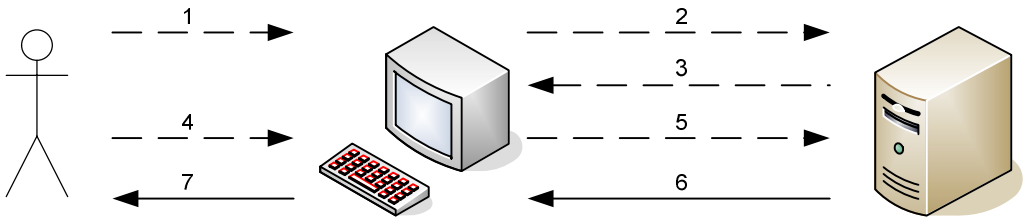


Legend

— — — Initial handshakes and request

——— Transmission and handling of password

a). Enrolment scenario 1: Service provider prompts user to create a password. 1, 2. A User makes an initial request an initial request to the service provider for the first time and forwards it through his client terminal. 3. The service provider prompts the user to create a password. 4. The user selects a password and keys in the password along with other required details (such as username, contact details, and so on) through his/her terminal. 5. The selected password is forwarded to the service provider, which then stores user's password and credentials for later authentication purposes.



Legend

— — — Initial handshakes and request

——— Transmission and handling of password

b). Enrolment scenario 2: Service provider creates and assigns password to the user. 1, 2. A user makes an initial request to the service provider for the first time and forwards it through his client terminal. 3. The service provider asks the user to provider his details (such as username, contacts, and so on). 4, 5. The user replies and forwards required details through his terminal. 6. The service provider generates a password, stores the password along with user's other details and forwards the password to the user via his terminal. 7. The user receives and keeps the password for later authentication purposes.

Figure 3 a, b: Typical enrolment procedures in password authentication mechanisms (simplified).

In a typical enrolment process, a user and a service provider establish a password, which would later be used to authenticate user's identity. Generally, the service provider asks the user to create his/her own password (Figure 3a), although sometimes format restrictions such as length of phrase and number of characters or digits apply. In some cases, the service provider may also generate and assign a secret phrase to the user (Figure 3b). The agreed password is then stored for later authentication purposes.

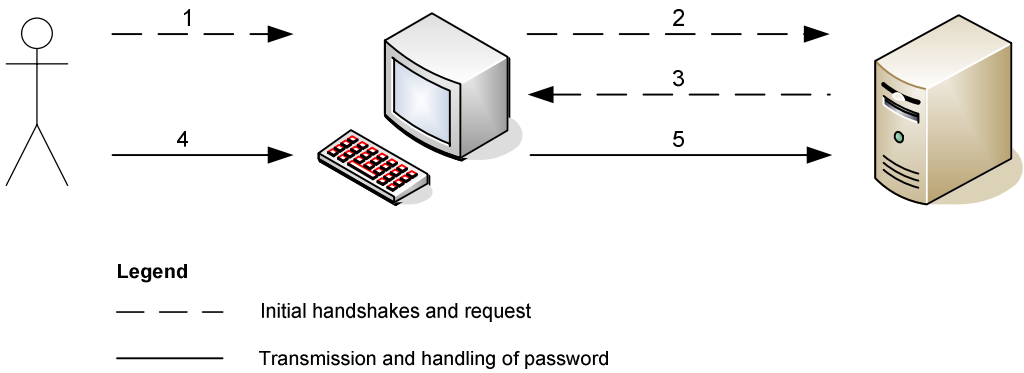


Figure 4: Password authentication process. 1,2. A user make a request for access to a resource or service to a service provider through his terminal 3. The service provider prompts the user for his password and other credentials (normally username). 4,5. The user presents his password and other required credentials. The service provider then compares the presented password to the previously enrolled password, and authenticates the user if they match.

In the authentication process, a user is asked to present his/her username and password, following his/her request for a resource or service. The service provider then compares the presented password against the previously stored password and authenticates user if they match. There are obviously slight differences in the procedures used by different service providers, but the common ground is that a user will be authenticated if he/she is able to present the same password which was agreed during the enrolment process. In the next section, we discuss current issues with password based authentication.

2.2. Issues with Password Authentication

The security of password based authentication mechanism hinges on the secrecy of a single word. If an attacker obtains knowledge of a victim's password, the attacker will be

able to impersonate the victim and gain access to the resources to which the victim is entitled.

In this section, we discuss various issues with password authentication. In Section 2.2.1, we describe three categories of attacks to password authentication based on the target of the attacks. In Section 2.2.2, we discuss users' insecure password practices and why users are considered to be the weakest link in password authentication mechanisms. In Section 2.2.3, we showed how password reuse can be exploited by an attacker in new-account scenario, known as *malicious server attack*. In Section 2.2.4, we discussed various identity management solutions which attempt to address password reuse and other insecure password practices.

2.2.1. Attacks on Password Authentication Mechanisms

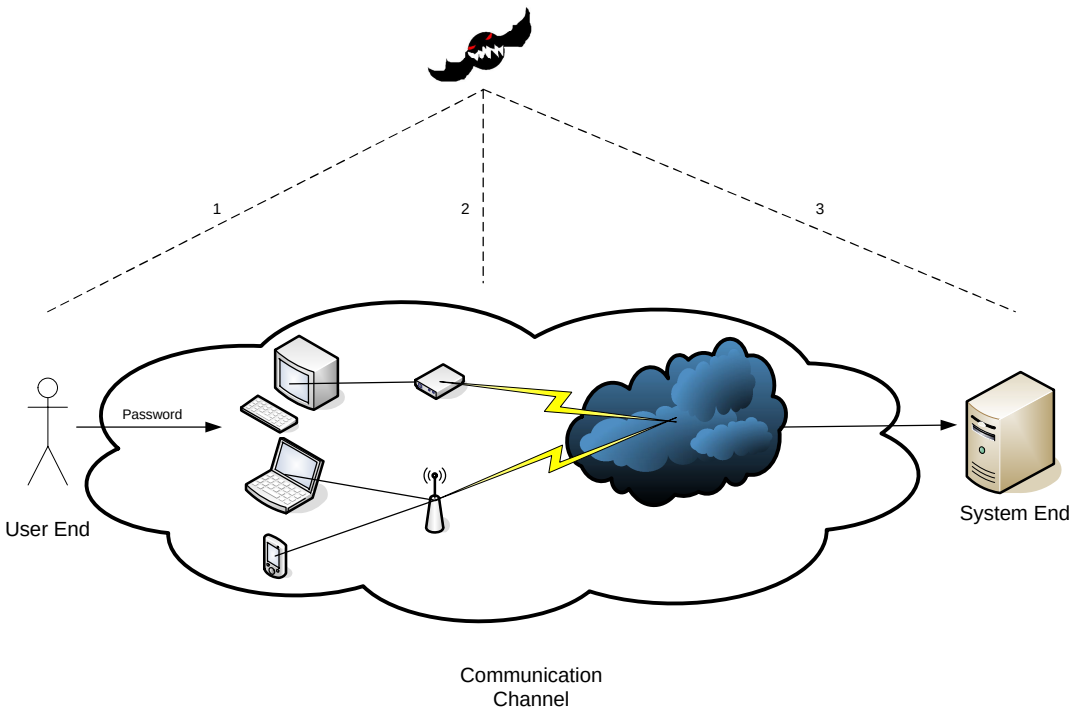


Figure 5: Classification of attacks on password authentication mechanisms based on the targets of the attacks: 1. Attacks on the user end 2. Attacks on the communication channel 3. Attacks on the system end.

There are various kinds of attacks which can be attempted by an attacker in order to obtain a victim's password. We classify attacks to password based authentication into three main categories based on the target of the attacks. We discuss our classifications in the following order: attacks to the system end, attacks to the communication channel, and finally attacks to the user end.

1. **Attacks on the system end**

   This classification covers attacks which are targeted to the system end, where passwords are stored. There are many known techniques and exploits which benefit from software flaws at the system end which may enable attackers to gain complete or partial control of the system and subvert the authentication mechanism, such as *SQL injection*, *code injection*, *backdoors*, and so on. These attacks can normally be prevented by appropriately validating user input, managing access control carefully, and frequently using virus scanners to detect and remove backdoors.

   We discuss another example of attacks to the system end, namely *password guessing attack* in more details. Password guessing attack can be further divided to *online guessing attack* and *offline guessing attack* [41-43]. *Online guessing attack* is an attack whereby the attacker tries different possible passwords to gain entry to the system, normally with the help of an automated program.

   In *offline guessing attack,* the attacker can check various possible passwords without requiring any feedback from the service provider end. In order to accomplish this, the attacker normally has to gain access to the password list stored at the system end, or a portion of it. In both cases, the attacker can either attempt to try possible combinations of characters and numerals in a set, known as *brute-force* approach, or use a precompiled dictionary of commonly used passwords, known as *dictionary* approach. These approaches can also be combined together, create a 'hybrid' approach which works by concatenating different combinations of additional characters to dictionary words. The

possibility of these approaches was first mentioned by Morris and Thompson in 1979 [44].

Nowadays, password cracking tools can be easily obtained from the internet. Examples include *RainbowCrack* [45] and *ophrack* [46], which are open source implementations of Oechslin's time-memory tradeoff technique [47]. *John the Ripper* [48] is multi-platform password cracker tool which can operate in both brute force and dictionary modes. Crack [49] is a password cracking tool which offers a network distributed feature, allowing computers connected by a shared file system to be used in a collective password cracking effort.

System administrators usually try to prevent online guessing attacks by limiting the number of login attempts [41-43], introducing delay between multiple login attempts [43], using verification image containing distorted letters or numbers which are readable to human but not to most automated programs [50-52]. Offline guessing attack is normally prevented by, limiting the access to and encrypting stored passwords [43, 44, 53].

2. Attacks on the communication channel

This classification covers attacks targeted to the communication channel. Our definition of communication channel includes all devices, mediums and protocols which connect user and the system end. Examples of this type of attack are *replay*, *eavesdropping*, and *man-in-the-middle* attacks.

Replay attack is an attack whereby the attacker captures old messages which were sent by user to service provider and re-sends to the service provider to access gain access to the resources entitled to the user. Stealing cookies and sessions from user's browser [54-56] is an common example of replay attack. This is can be done by exploiting cross site scripting (XSS) vulnerabilities in many browsers[57].

In *eavesdropping* attack, the attacker passively listens to the line of communication between user and service provider [15, 42, 58]. By doing this, the attacker can capture user's passwords and other credentials. Network sniffers, such as *Ethereal* [59] and *Tcpdump* [60] are ideal tools for mounting this type of attack if the attacker is connected to the same network as the victim, as these tools can be used to capture and log packets in Ethernet, making it possible for the attacker to gather credentials transmitted through the network [58, 61].

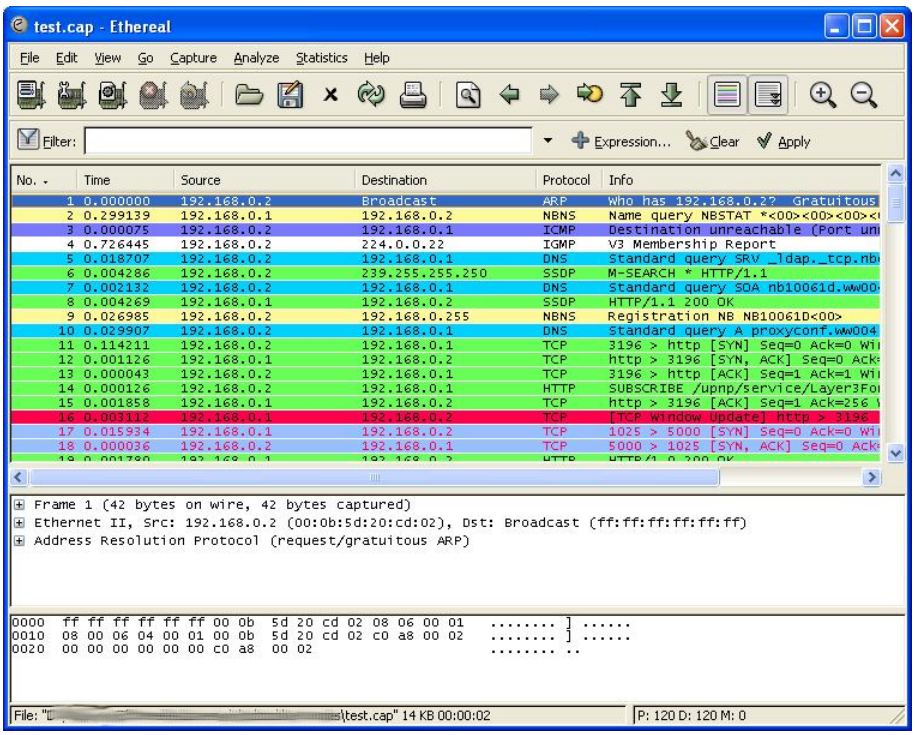


Figure 6: Ethereal in action [62].

Man-in-the-middle refers to a type of attack whereby the attacker intercepts communication between user and the system. Sometimes the attacker relays the messages between user and system end, so as to make the communication seem normal. However, during the process the attacker is able to manipulate the content of the messages, which differentiates man-in-the-middle from replay and eavesdropping attacks. Tools such as *arpspoof* and *dnsspoof* are ideal for launching man-in-the-middle attack if the attacker is connected to the same network as the victim [63]. Both *arpspoof* and *dnsspoof* work by sending spoofed responses to the victim, tricking the victim to forward his communication to the attacker instead

of the server. Another tool, *webmitm*, can be used in conjunction with *dnsspoof* to relay intercepted HTTP and HTTPS traffic to the server, and present the victim with a self-signed SSL certificate which may fool even advanced users [63]. In the wireless (Wi-Fi) realm, man-in-the-middle attacks can be done with the aid of rogue access point tools such as *airsnarf* [64].

Preventive measures to these attacks include careful management of sessions and cookies [15, 43, 55], using secure protocols, such as SSL [65] or its successor, TLS [66] appropriately and encrypting communication with well-proven cryptographic algorithms [15, 55].

3. Attacks on the user end

This classification covers attacks which are directly targeted to the user end. Most attacks which are directed to users fall into *social engineering* and *reconnaissance* categories. Social engineering attacks use social interactions to trick victim into divulging his passwords or other confidential information to the attacker, the types of social interaction vary from phony phone calls to face-to-face encounters [15, 67, 68]. Reconnaissance, on the other hand, refers to the practice of gathering discrete pieces information, and putting them back together like a puzzle [15]. These attacks are known to have relatively large chance of success, despite the relatively minimum level of technical knowledge required [15, 67-69]. We discuss three examples of to the user end, namely *shoulder surfing*, *dumpster diving*, and *phishing*.

Shoulder surfing refers to the act of visually observing individuals as they key in their PINs or passwords through input devices [15, 67]. The most basic form of shoulder surfing does not require any technical expertise to perform, and is particularly effective in public places such as Automatic Teller Machines (ATM), internet café, library and airport internet kiosks. With vision enhancing devices being readily available at relatively inexpensive prices, shoulder surfers are

increasingly incorporating devices such as miniature closed-circuit television cameras into their practices [70, 71].

Dumpster diving is a well proven technique for stealing credentials and other confidential information, which involves looking through victim's waste, searching for discarded items which contain confidential information [15, 67, 72]. One of the most famous example was perhaps performed by Jerry Schneider, who obtained documentation and manuals from Pacific Telephone & Telegraph Company, and abused the company's procedures to swindle hundreds of thousands of dollars worth of telephone equipment in late 1960s [73, 74]. Used hard drives which are not properly sanitized are also ripe of personal and confidential information [72, 75].

Phishing is a form of social engineering attacks whereby the attacker attempts to obtain user information such as passwords and credit card details by masquerading as a legitimate party, usually through e-mail communication[76-78]. The word 'phishing' is a derivative of 'fishing'[3]. The naming, which is based on the analogy that internet scammers are using e-mail bait to "fish" for passwords in the sea of Internet users was first mentioned in the alt.2600 hacker newsgroup in January 1996 [79].

Phishing is sometimes used in conjunction with URL obfuscation and graphical tricks to mislead unsuspecting victims to a bogus websites, which often look very similar to their legitimate counterparts [17, 18, 80]. JavaScript can also be used to construct more sophisticated redirection techniques, which can fool not only advanced users, but also static analysis techniques [81].

[3] Replacing 'f' with 'ph' is a fairly common practice in the 'hacker' community. Other examples include '*ph*reaking', which refers to manipulating phone switches using specific tones through a phone line, and '*ph*arming', which is also discussed in this section.

Despite being relatively simple to perform, phishing poses a real threat to customers and business worldwide that use internet as a medium for financial transactions. Based on a survey conducted in 2006, Gartner Research estimated that 3.5 million Americans had given sensitive or financial information to phishers, resulting in estimated $2.8 billion of financial losses [82]. The Anti-Phishing Working Group reported 55,643 phishing sites in April 2007, a massive increase of 35,000 websites from March [83]. Berghel, et al. [84] also claims that organized crimes in the United States and Eastern Europe have also adopted phishing to steal identities and cash from unsuspecting internet users.

Below is an example of phishing e-mail that we received on 27 September 2006. The phisher pretends to be a security advisor from *Westpac Bank* asking customers to confirm their online banking details by supplying 'necessary information' to a website whose URL string appears to be legitimate, but is actually linked to a bogus website. The result of our *whois* query indicates that the real website address is registered to a resident of Zürich, Switzerland via a hosting company located in Friedersdorf, Germany. Further observation of the e-mail headers revealed that the message might have originated from a mail server which is also located in Germany.

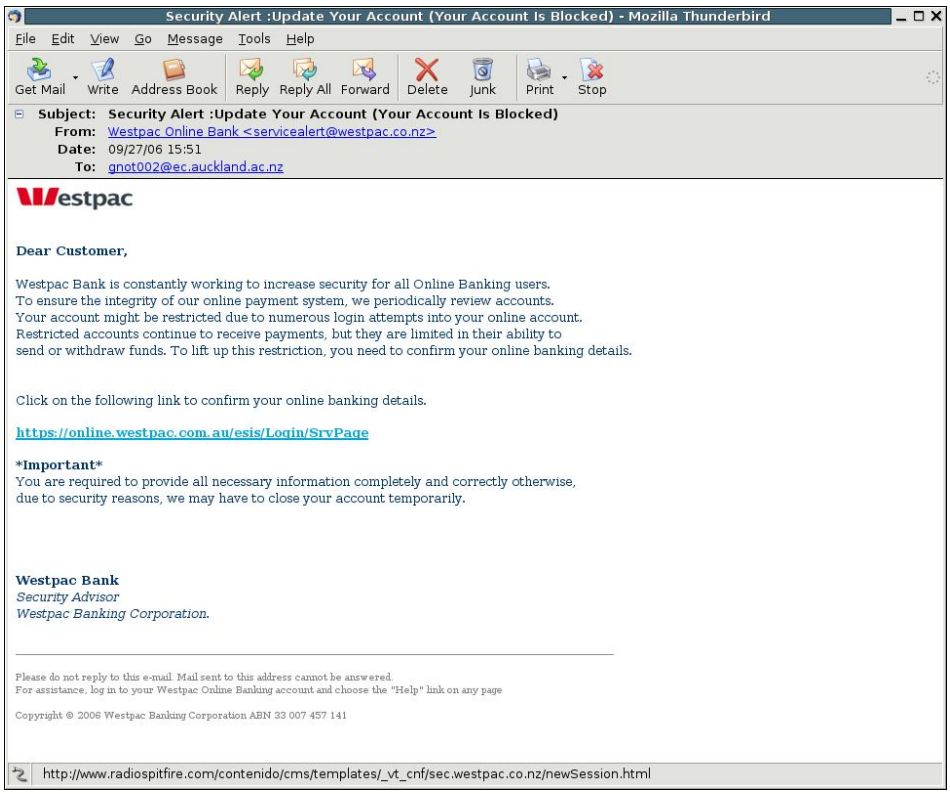


Figure 7: Phishing e-mail targeted to Westpac Bank customers, received by the author on 27 September 2006.

In some cases the attacker may also attempt to compromise a password authentication mechanism by targeting more than one component of the mechanism. These combination attacks normally operate by exploiting the vulnerabilities of a component of the password authentication mechanism to make other component(s) more susceptible to attack. These combinations usually result in more effective approach with higher success probability. Examples of this form of attacks are *pharming* and *keylogging*.

Similar to phishing, *pharming* is an attack which uses bogus websites to trick users into divulging their credentials to the attacker. However, rather than using e-mails or other social engineering methods, in pharming the attacker firstly exploits the communication channel by exploiting a victim's Domain Name Server (DNS) in order to redirect user to a fraudulent website each time user goes to a particular URL [17, 85]. Recent discovery has shown that DNS settings of consumer grade broadband routers can also be compromised by simply luring the victim to access a website loaded with malicious JavaScript and JavaApplet [86, 87], this can easily be done as most home users do not

change their broadband router passwords. Pharming is considered to be somewhat more powerful than phishing, as victims will almost certainly be redirected to attacker's site.

Keylogger, a form of spyware which logs keystrokes and records screenshots, is also a potent eavesdropping tool that can be used to collect passwords and other sensitive information [56, 88]. In order to launch this attack successfully, the attacker has to install the keylogger on victim's machine. This is usually done by deceiving the victim using various tricks, such as *drive-by-download*, whereby the attacker lures unsuspecting victims to open a compromised webpage which then installs a keylogger via *Active-X,* or by bundling keylogger together with other benign application installers to mislead unsuspecting victims to install the keylogger themselves.

2.2.2. Human Factor and Insecure Password Practices

We have discussed various forms of attacks to password authentication mechanism. Among the three categories, attacks to user end are perhaps the most alarming, as these attacks only require minimal level of technical or specialist knowledge to perform, and yet have relatively large chance of success. Furthermore, although cryptographic means and protocols offer a degree of protection at the system end and communication channel, users are often left unprotected by nothing but security policies and guidelines which are often neglected, making them even more vulnerable to attacks.

Indeed, users are the 'weakest link' of any password authentication mechanism. Most users have been noted as having low awareness of what attackers are capable of and the scope of damage that can be inflicted if their passwords are compromised [16, 89, 90]. Kevin Mitnick, the infamous hacker, in his testimonial before the US Congress stated that he obtained more passwords by exploiting users than by using technical means. *"I was so successful in the line of attack that I rarely had to resort to a technical attack...Companies can spend millions of dollars toward technological protections and that's wasted if somebody can basically call someone on the telephone and either convince them to do*

something on the computer that lowers the computer's defenses or reveals the information they were seeking. [91]*"*

Pfleeger and Pfleeger also made a similar remark in their book 'Security in Computing' [15], *"Guessing passwords and breaking encryption can be tedious or daunting. But there is a simple way to obtain a password: Get it directly from the user! People often tape a password to the side of a terminal, or write it on a card just inside the top desk drawer."*

Previous discoveries have corroborated that users often write their passwords down and post them in obvious locations [16, 92-94]. Adams and Sasse [16] in their survey-based study discovered that 50% of their participants wrote their password down in one form or another, while the other 50% refused to answer the question. Similarly, Dhamija and Perrig [93] discovered that the vast majority of their participants wrote their passwords down, regardless of whether they are novices or experts who have been trained in password security. Furthermore, many studies have also discovered that users often create 'weak' passwords based on obvious dictionary words or personal information, which can be guessed by people who know enough about them; these may include birth dates, personal names, nicknames, names of partners or favorite celebrities, and even the word 'password' [15, 95-98]. We will discuss these studies in greater details in Section 3.2.

The stories of insecure password practices do not just end there. Password sharing between friends and work colleagues has been noted as a common practice. Many users do this because of convenience and practical reasons [16] or as a result of 'social pressure'. In a study conducted by Weirich and Sasse [90], it was discovered that password disclosure is often perceived as a sign of trust between colleagues, and consequently, refusal to disclose passwords is seen as a sign of lack of trust. In teamwork settings, people who refuse to share passwords to their other team members is often viewed as unsociable, or get the image of not being good team players. Furthermore, Weirich and Sasse also found a number of situations that lead to voluntary password disclosure, such as when it is necessary for work, following higher orders, asking for help with computers, and so on.

This suggests that an attacker can easily obtain victim's password by pretending to be victim's work colleague, superior, or even IT support staff.

2.2.3. The Danger of Password Reuse

Another common practice which is often considered risky and insecure is password reuse. The reason for this is that if an account is compromised, all other accounts which share the same password would also be at risk. However, unlike other careless practices that we discussed, such as posting passwords on the screen and disclosing passwords to colleagues or strangers, password reuse is not something that can be easily avoided, especially with the proliferation of e-commerce and other services requiring password authentication. While human memory capacity is very unlikely to increase significantly over the next few years, the rising number of online services will force most users to reuse their passwords. A recent study [89] discovered that password reuse ratio tend to increase as people accumulate more accounts.

To show how password reuse could be exploited by an attacker, we discuss *malicious server attack*, which is mentioned in [99, 100] as a hypothetical, user targeted attack which benefit from careless password reuse. Madsen, et al [85] also mentioned a similar attack, but called it *password attack*. In order to launch this attack, the attacker sets up a 'legitimate' service with a malicious intent. Unlike phishing or pharming, the attacker does not need to impersonate any existing service. The attacker then lures the victim to register in order to gather the victim's passwords and other credentials. If the victim uses the same password on their other, more valuable accounts, the attacker will be able to impersonate the victim with ease and gain access those accounts. The attacker could also attempt to gather as much information as possible from the victim by asking the victim to provide personal details during the registration process. As if these were not enough, the attacker could also disable victim's access after a period of time, leading the victim to reveal his other passwords and usernames upon login failures. We believe that it would be very logical for the attacker to combine this attack with a dictionary based attack, by constructing a dictionary from the captured passwords.

Although our review of the literature revealed no statistics on the damage caused by malicious server attacks, we believe that this attack is highly plausible and would be very logical to attempt by someone motivated by financial gains. The success probability of this attack will only increase as people reuse their passwords on more accounts. Ives, et al. [101] has also highlighted that password reuse also has the potential to add 'domino effect' to successful attacks of any kind, which can in turn compromise even an entire organization. Given that many attacks are relatively simple to perform and a lot of careless users are literally giving their passwords away, password reuse would certainly put attackers in a tremendously advantageous position.

On the other hand, Karp in [102] argued that not reusing passwords would be equally dangerous, as the more passwords that people have to remember, the more memorable and guessable their passwords become. Adams and Sasse [16] also discovered that having a large number of passwords reduces their memorability, which in turn would increase insecure password practices. It is clear that password reuse has become a non-trivial problem which will only worsen overtime if a practical solution is not devised.

2.2.4. Current Solutions: One Password, Many Accounts

Currently, some service providers attempt to minimize the risk of password reuse by forcing users to change their passwords regularly, or prohibiting them to reuse their passwords on other accounts [15, 16, 67, 103, 104]. These strategies left much to be desired, as they have been found to place more burdens on user's cognitive load, leading users to devise their own methods for the sake of convenience, which tend to result in even riskier practices [15, 16, 90, 98].

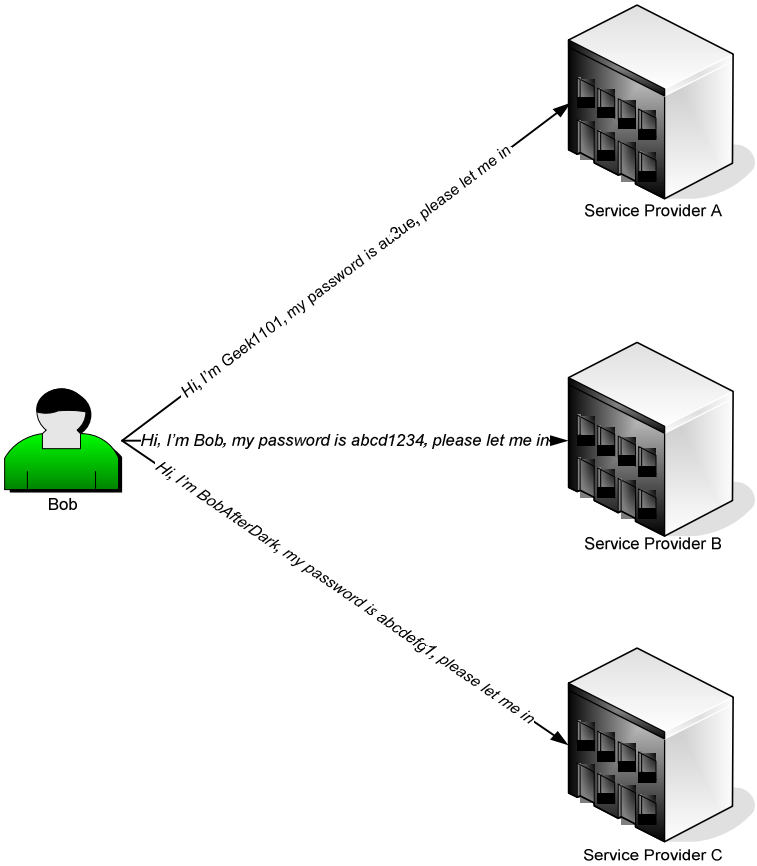


Figure 8: A simplified illustration of the current password authentication scenario (also termed *isolated identity model* [105, 106]), where a different password is required for each service provider.

Various identity management solutions have been developed under the assumption that decreasing the amount of passwords and associations that have to be managed would reduce users' memory strain, leading to a decrease in the prevalence of password reuse and other aforementioned insecure practices (Section 2.2.2). Most of these solutions work by allowing users' password and other credentials to be portably used across several service providers. Interestingly, this can in fact be viewed as 'controlled' password reuse. Current approaches to identity management solution can be classified into *provider-centric* and *user-centric* [105-108].

2.2.4.1. **Provider centric approach**

In a provider centric approach, service providers enforce and manage the scope of users' identities. Users themselves usually have no to minimal privileges to exercise their preferences regarding which identity should be associated with which services. Provider

centric approaches can be further classified into two categories based on their architectures [106, 108]:

1. **Centralized identity model**

   The centralized identity model has a single 'trusted' *identity provider*, which authenticates user and brokers user identities to other service providers. Service providers normally rely on a third party identity provider for authentication information of a user before granting access privileges. Examples of this approach include *Windows Live ID* [109] (formerly *Microsoft Passport*) and *Kerberos* based authentication.

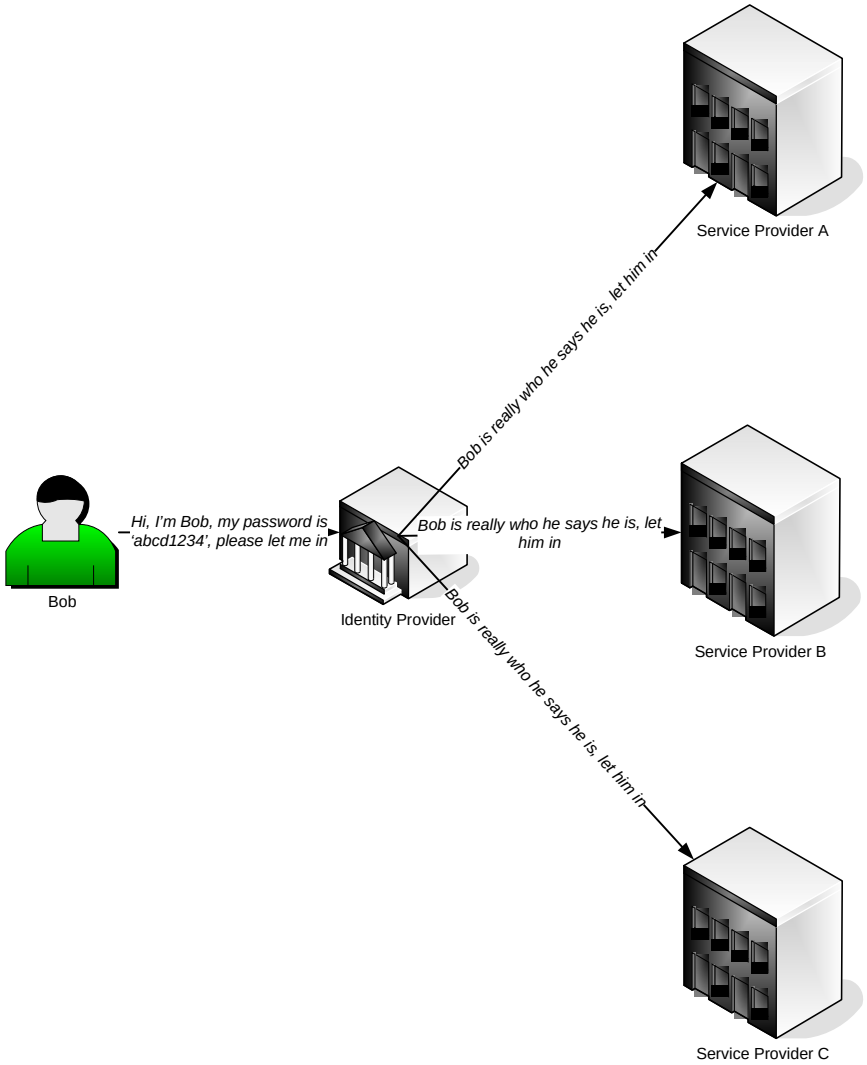


Figure 9: A simplified illustration of the centralized identity model.

This approach has been criticized as having a 'single-point of failure [108, 110]. Furthermore, although this approach is well suited for closed network where service providers are essentially managed by the same organization, trust and privacy issues may arise in environments where service providers are run by different organizations, since this architecture would allow the organization which acts as the identity provider to control and abuse users information [105, 106, 108].

2. Federated identity model

Federated identity model avoids the single point of failure drawback in centralized model by distributing the responsibility of identity provider to service providers within the federation. Federation is essentially a group of service providers which establish a mutual agreement to accept user identities vouched for by other members, which is passed in the form of security assertion [105, 108, 111].

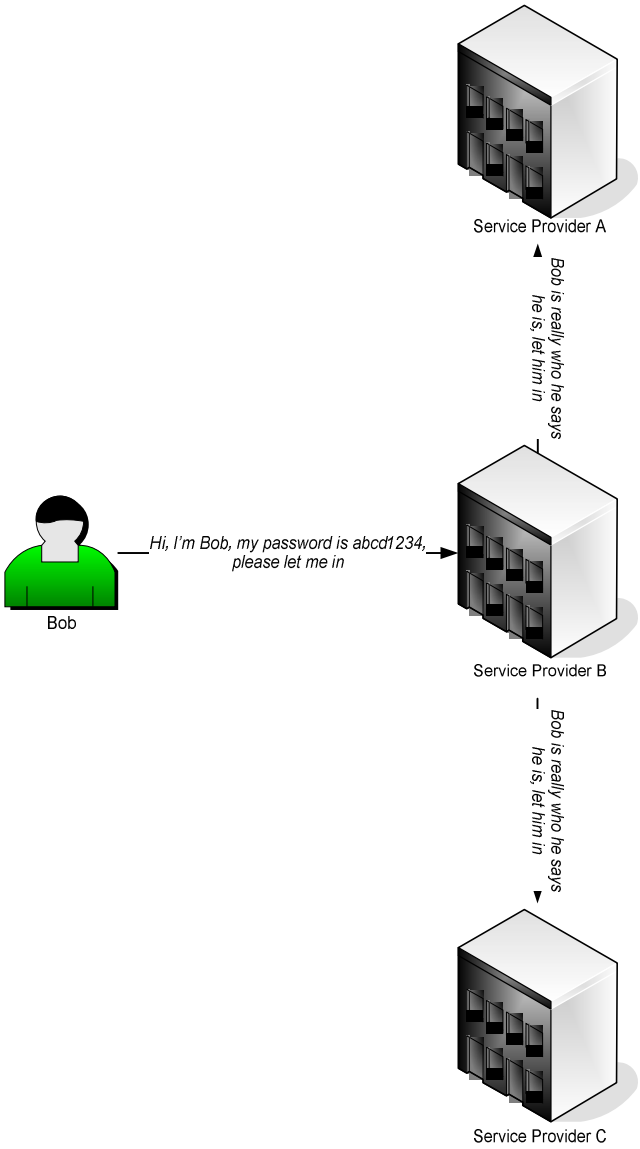


Figure 10: A simplified illustration of the federated identity model.

Although single point of failure drawback can be avoided in the federated model, this approach brings underlying technical complexities, for example, since service providers have different security level, it becomes difficult to regulate the information flow across service providers [107], it is also reasonably difficult for service providers to distinguish a security assertion originating from a genuine user's request from one that comes from a compromised service provider [105]. Examples of this architecture include *Liberty Alliance Project* [112], *Shibboleth* [113], and *AthensDA* [114].

There are currently varying opinion regarding provider centric identity management solutions. On one side, these approaches allow users to manage fewer passwords, promoting more secure practices and better awareness [85]. On the other side, provider-centric identity management approaches have been generally criticized as having:

Problem 1: Cascading implications of successful attacks

Similar to password reuse, a successful attack on user's password would almost ensure that other accounts within the authentication scope are compromised. This even put the attacker in an even more advantageous situation, as the attacker now knows for certain which accounts share the same passwords. Current approaches are still unsafe from most if not all aforementioned attack techniques. A report published in 2001 [115] has shown how an attacker could obtain credit card details from *MSN Wallet*, by stealing sessions from *Hotmail*, Microsoft's free e-mail service which also uses Microsoft Passport single-sign-on mechanism.

Problem 2: Lack of user control

In most of these systems, users are largely dependent on identity or service providers to manage their identities [108]. Most of the times, users are forced to use the same password and credentials across many services which are of different natures and would normally call for different passwords, for example a free e-mail account and an e-commerce account which stores credit card numbers. Depending on the implementation, sharing of user information among different service providers this could potentially raise privacy concerns [105, 111].

Problem 3: Poor scalability

Although this approach could potentially reduce the number of passwords which have to be maintained to some extent, they tend not to scale well [105, 106, 111]. Due to the existence of various architectures and implementation standards, in addition to conflict of interests, competition and other issues between service providers, it is very likely that users would still have to deal with numerous authentication domains, and we are back to square one.

2.2.4.2. **User centric approach**

Lack of user control (Problem 2) in provider centric approach has caused user centric identity management paradigm to emerge. This paradigm attempts to return the control of identities back to users. Interestingly, the traditional isolated approach may actually be considered to have good user control, however, as we have discussed, this became more of a burden than a benefit. Hence, user centric identity management approaches usually aim to achieve a balance between user control, security and usability [105, 107, 108, 114]. We further classify user-centric approach into:

1. **Non-autonomous**

   A non-autonomous approach attempts to address lack of user control in provider-centric approach, by increasing user involvement in the authentication process. Using this approach, users are now able to select appropriate credentials for different services; however, users' passwords and credentials are still controlled and handled by identity providers. Not unlike provider-centric approach, this approach still suffers from poor scalability (Problem 3), as it generally requires service providers to adopt certain standards. An example of this approach is *OpenID* [116].

2. **Autonomous**

   An autonomous approach enables users to fully manage their own passwords and credentials, regardless of the architecture and implementation standard adopted by service providers, while at the same time reducing user's memory burden. Autonomous approach does not require any change on the service provider end. This is usually done by storing or generating a number of passwords, and protecting access to these passwords with a 'master' password.

   Examples of hardware based solutions include 'wallet' applications for smart phones which allow users to store their important information in encrypted form, such as *CodeWallet Pro* (for Windows Pocket PC) [117], *eWallet* (for Windows

Pocket PC and Palm OS) [118] , *Password Manager for Symbian* (for Symbian OS) [119].

Some software implementations, such as browser integrated password databases in modern browsers such as *Firefox*, *Internet Explorer*, *Safari*, and *Opera*, work by maintaining stored password on users' computers in encrypted form. While these are sufficient for users who only use a single computer for a long period of time, this solution is undesirable for people who often change computers or use different computers at different places. Hashing based implementations eliminate the need of storage by generating passwords on-the-fly using hashing functions based on a user specified master password and some additional information (normally website name). Examples of hashing based password management applications are Lucent *Personalized Web Assistant* [120], HP *Site Password* [121], Halderman et al.'s *Password Multiplier* [122], and Yee et al.'s *Passpet* [123].

Although autonomous approach generally does not suffer from Problems 1, 2, and 3 above, they still have some drawbacks. Software applications are usually not portable, i.e. users would normally be required to download and install the application again if they were to log in to their accounts from another computer, which could be troublesome in public or shared places such as offices and internet cafes, where users do not have the rights to install applications. Although there are applications which can be can be installed on and run directly from USB disks, such as *KeyPass* [124] and *Password Manager XP* [125], they are usually platform specific, which makes it rather unusable for users who often switch or use different platforms. It is also very likely that many organizations will strictly control or restrict user access to removable disks in the near future due to potential espionage related activities [126]. Hardware based solutions offer greater portability, but like token based authenticators (see our discussion about token based authenticators in Section 1.2), they normally suffer from physical threats (can be lost or stolen) and is prone to shoulder surfing attacks (see Section 2.2.1

for more detailed discussion on this attack), as users would normally have to read from a device while typing their passwords.

2.2.5. Summary

We have discussed various issues with password authentication. In Section 2.2.1, we began by describing a variety of known attacks, which we classify into three categories: attacks to the system end, attacks to the communication channel and attacks to the user. Among these three categories, attacks to the user are the most alarming, as they commonly require minimal level of technical knowledge to perform, and yet have a relatively large chance of success. Furthermore, while attacks to the system end and the communication channel can be prevented by careful implementation and cryptographic protocols, users are often left unprotected by nothing but security policies and guidelines which are often neglected, making them the 'weakest link' of any password authentication mechanism.

In Section 2.2.2, we discussed users' tendency to adopt insecure password practices which have been discussed in various literatures, which include writing passwords down in obvious locations, creating extremely weak passwords, sharing passwords with their colleagues, and reusing passwords on multiple accounts. Password reuse is generally considered a bad practice, because if one of users' passwords is compromised, then all their accounts that share the same password will also be at risk. In Section 2.2.3, we showed how password reuse can be exploited by an attacker in new-account scenario, known as *malicious server attack*. However, while human memory capacity is very unlikely to increase significantly over the next few years, the proliferation of internet based services which require password authentication will force most users to reuse their passwords.

In Section 2.2.4, we discussed various identity management solutions which attempt to address password reuse. These solutions are developed under the assumption that decreasing the amount of passwords and associations that have to be managed would reduce users' memory strain, leading to a decrease in the prevalence of password reuse

and other insecure practices. Nevertheless, these solutions are not are not free from their own problems and drawbacks. In the next chapter, we describe the motivation and organizing idea of our survey based study along with ten previous user studies on password authentication.

"Study without desire spoils the memory, and it retains nothing that it takes in." –Leonardo da Vinci

3
Our Study

In this chapter, we describe the motivation of our study. We also review ten previous user studies on password authentication, and discuss how we use the concept of digital persona as an organizing idea for our survey based study.

3.1. Motivation

We have described the issues with password reuse and how it could potentially benefit attackers (Section 2.2.3). However, as we have also discussed, it is almost inevitable that most people reuse their passwords, due to the rapid increase in number of accounts which is not balanced by human memory capacity to recall passwords. Requiring users to create a completely unique password for each of their accounts would be unrealistic and this could in fact increase insecure practices, such as writing passwords in obvious locations and creating extremely weak passwords, which would also lead to password disclosure. While various identity management solutions have been developed to address password management problems, as we have discussed in Section 2.2.4, they are not free from their own problems and drawbacks.

We agree with Gaw and Felten [89], who wrote that many projects focus on developing new technology and solutions to improve poor password practices without studying what encourages these poor practices. In order to be able to objectively evaluate existing solutions, or work towards a more appropriate solution to password management problems, we believe that it would be necessary to investigate the root of the problem, that is, the factors which influence the way in which people's password usage behavior. This will be the primary objective of our research. We believe that conducting a survey-based study would be the most appropriate way to achieve this objective. In the next section, we discuss ten previous user studies on the subject of passwords and other identity management issues that have been published in literatures.

3.2. Previous User Studies on Password Authentication

In this section, we discuss ten previous survey-based studies on password authentication in chronological order (see Figure 11), starting from Morris and Thompson's study in 1979 [44], followed by studies by Riddle et al (1989) [97], Adams and Sasse (1999) [16], Dhamija and Perrig (2000) [93], Petrie (2001) [95, 127], Brown et al (2004) [96], Yan et al (2004) [128], Riley (2006) [129], Gaw and Felten (2006) [89], and finally Florencio and Herley (2007) [130].

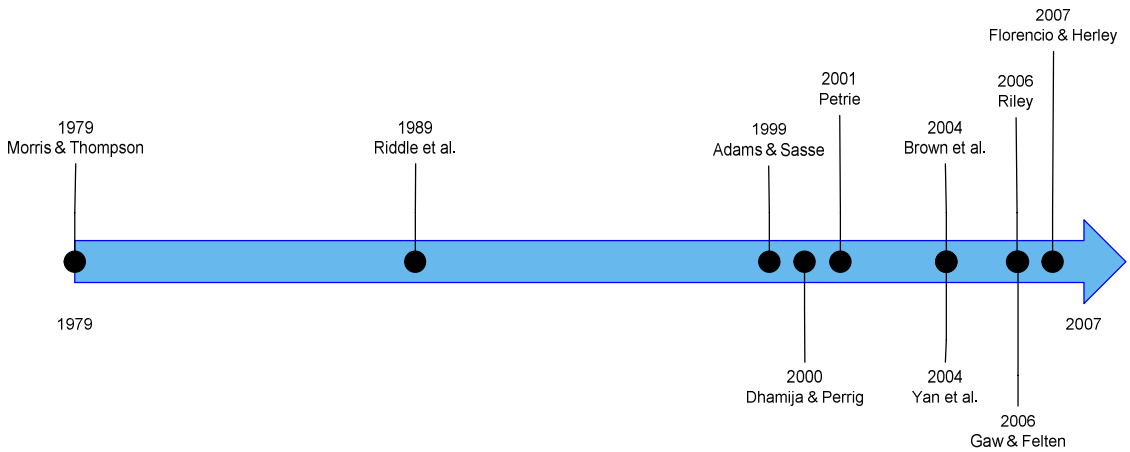


Figure 11: Chronologies of user studies on password authentication. The rising frequency of user studies conducted on passwords suggests an increasing level of interest in this subject.

3.2.1. Morris and Thompson (1979)

One of the earliest user studies was performed by Morris and Thompson in 1979. In their publication entitled "Password Security: A Case History" [44], Morris and Thompson discussed dictionary and brute force attacks on user generated passwords, and demonstrated the plausibility of this attack by analyzing real passwords.

Morris and Thompson collected a corpus of 3,289 passwords from many users over a long period of time to determine typical users' habits in the choice of passwords when no constraint is put on their choice and were appalled to find that 86% of these passwords were extremely weak. Many passwords were too short, composed of only lowercase or only uppercase letters. Moreover, a five minutes dictionary search produced about one third of their whole password corpus[4]. Based on these results, they concluded that users should be urged to use either longer passwords, or create passwords from a larger character set.

3.2.2. Riddle et al. (1989)

Riddle et al [97] analyzed 6226 user generated passwords from IBM CMS environment used by students and staff at Syracuse University in 1987. At that time, users were suggested to create passwords which were 3-8 characters in length (could be any uppercase letters, lowercase letters or numbers), and make their passwords hard to guess. Although these suggestions were well advertised, there were no formal rules on not creating passwords shorter than the maximum suggested length, or on not creating easily guessable passwords.

[4] Estimating how fast this search could be performed on today's machines would be rather difficult, as Morris and Thompson did not specify their exact experiment setup, e.g. specifications of machines that they used, their search algorithms, and so on. However, as a reference, one of the top performing microprocessors in 1979, *Motorola 68000* is capable of performing 1 MIPS (Million of Instructions Per Second) and is clocked at 8 MHz, while *Intel Core 2 Extreme QX6700*, one of the top performing consumer grade microprocessors at the time of this writing, is clocked at 2.66 GHz and is able to achieve ~50000 MIPS [132, 133]. Note that MIPS and clock speed are **not** direct indicators of microprocessor performance. For more discussion on microprocessor performance, see [134] and [135].

Their findings were similar to Morris and Thompson's study from ten years prior. Many passwords were discovered to be extremely short, with 88% of the passwords being only 4 characters long or less. Excluding two or three character passwords, 44% of the passwords were true English words. Furthermore, among passwords which are 5 characters or longer, 27% were persons' names. Riddle et al. concluded that unless constraints are enforced, most people would resort on the weakest possible password for convenience reasons.

3.2.3. Adams and Sasse (1999)

Adams and Sasse [16] conducted a study on password related user behaviors, including password construction, frequency of use, password recall and work practices. They received a total of 139 responses from their web based questionnaire, which was followed by semi structured, in-depth interviews involving 30 employees of two business organizations.

50 % of their participants admitted to writing passwords down in one form or another, while the other 50 refused to answer the question. Many participants blame their insecure password practices (such as writing passwords down), and poor password choices (such as choosing "password" as the password) on the need to maintain multiple passwords for different accounts and security regulations (such as periodical password changes) which according to them accomplish nothing but increase their memory burden. Some participants tried to alleviate memory strain from having multiple passwords by using related passwords, such as by varying elements in linked passwords (name1, name2, name3, and so forth). Choosing passwords which are both secure and memorable is found to be a difficult task for many participants.

Adams and Sasse further stated that their participants' knowledge of password security was inadequate. Participants often pictured attackers as complete strangers who try to guess their passwords by hand, and do not understand how password cracking works. Finally, they concluded that their participants lack security motivation and understanding of password policies, and tend to circumvent password restrictions for the

sake of convenience (notice the similarity with Riddle et al.'s findings in Section 3.2.2. above).

While prior studies only inferred users' password selection behavior by analyzing large databases of passwords, Adams and Sasse went further by investigating users' perceptions and reasons behind their practices. Nevertheless, their results suggest that users' awareness of security had not improved much since Morris and Thompson's study in 1979 (Section 3.2.1).

3.2.4. Dhamija and Perrig (2000)

Dhamija and Perrig [93] performed a user study to compare their prototype image authentication system to traditional password authentication. Interview results from 30 participants were reported in a qualitative manner. Although demographic information of their sample population was not described in details, Dhamija and Perrig claimed their sample population to be 'representative of the general population of computer users'. The results of their study confirm most of Adams and Sasse's results (Section 3.2.3).

Participants reported that they maintained 10-50 accounts which require passwords, while only having 1-7 unique passwords, many of which are based on variations of each other to enhance memorability. Most of their participants admitted to writing their passwords down.

They further discovered that participants often use things which are meaningful to them, such as their own names, names of their family members and favorite movies as inspirations for creating passwords. They also found that participants tend to find 'workarounds' to circumvent system restrictions, which often result in insecure password practices, for example, one of their participants admitted that she likes to maintain only one password, so when she is required to change any password, she would change all of her passwords to be the same. Moreover, they discovered that level of security training does not appear to have any impact on participants' password practices – even trained

participants often view secure password practices as being too cumbersome and impractical.

Following the interview, the participants were asked to create a password that they had not used before and believed to be secure. After only one week, the recall level was unimpressive – only 70% of the participants were able to recall their passwords.

3.2.5. Petrie (2001)

Petrie [95, 127] analyzed responses from 1200 participants throughout the United Kingdom in a survey sponsored by CentralNic, a London based internet domain name registry. The result of this analysis revealed 4 categories of participants based on the inspirations from which they created their passwords:

1. Family oriented (48%)

   This group of participants created passwords that symbolize people or events with emotional value. These people based on own name or nickname, name of their children, partners, pets and date of birth.

2. Fans (32%)

   These participants used the names famous celebrities (athletes, singers, movie stars), fictional characters (such as Homer Simpson), and sports teams. Petrie said that this category mostly consists of young people who want to associate themselves with the lifestyle represented by a celebrity.

3. Fantasists (11%)

   Participants in this category created passwords based on references to sexual characteristics, such as “sexy”, “slapper”, “bitch”, ”goddess” and “stud”. The majority of people in this category are male, with only 37% identified themselves as female.

4. Cryptic (10%)

This category consists of security conscious participants who created passwords consisting of a mixture of upper case letters, numbers, and punctuation.

These results confirm earlier findings from earlier studies by Morris and Thompson (Section 3.2.1), Riddle et al (Section 3.2.2) and Dhamija and Perrig (3.2.4), that most people use names and true English words as their passwords.

3.2.6. Brown et al. (2004)

Brown et al. [96] conducted a survey involving 218 college students in Introductory Psychology course at Southern Methodist University to evaluate their password generation and usage behavior. Participants were asked to describe their accounts which require passwords, and indicate what type of information they used as an inspiration to generate password for each application.

On average, their Participants maintain 8.18 accounts which require a password (S.D. = 2.81, Range = 3 to 20), while only having 4.45 passwords (S.D. = 1.63, Range = 1 to 11). These numbers are not considerably different from Dhamija and Perrig's study three years earlier, which reported a range of 10-50 accounts and 1-7 unique passwords. The majority of participants (92.9%) reused their passwords on at least one account (37.4% reused on only one account, 29.7% reused on two accounts, 20.9% reused on three accounts, while 5.9% reused on five or more accounts).

Similar to Dhamija and Perrig's (Section 3.2.4) and Petrie's (Section 3.2.5) findings, most of their participants drew heavily upon themselves and others close to them as inspirations for creating passwords. 66.5% of the passwords were created with reference to 'self', followed by 'relative' which contributes 7% to the whole passwords collection. The rest of the passwords were created using references to animal, lover, location, celebrity, and so on. Only 5.7% of the passwords were described as being created using 'random' information.

It is remarkable how users' methods for creating passwords did not seem to change much since Morris and Thompson's study 25 years prior (Section 3.2.1). Brown et al. discovered that the overwhelming majority of the passwords (75%) were constructed using intact (full) information, 13.5% were created using only part information, while only 10% were formed by transformations (abbreviation, backwards, or combinations).

Brown et al. further discovered that 31.1% of their participants have forgotten at least one password, while 25.5% have experienced at least one password mix up. Furthermore, 54.1% of their participants admitted that they keep a written record of their passwords, which confirms findings from earlier studies by Adams and Sasse (Section 3.2.3) and Dhamija and Perrig (Section 3.2.4).

3.2.7. Yan et al. (2004)

Yan et al. [128] performed a study on password memorability and security, involving 288 first year students at the University of Cambridge's School of Natural Sciences, which includes physics, chemistry, geology and materials science majors.

Unlike prior studies by Morris and Thompson (Section 3.2.1) , Riddle et al (Section 3.2.2), Petrie et al (Section 3.2.5), and Brown et al (Section 3.2.6), which evaluated users' passwords using retrospective approach, Yan et al. took a prospective approach by asking user to generate passwords and analysing them. During the experiment, Yan et al. divided the participants into three groups:

- Group A: one third of the participants were instructed to create a password containing at least 7 characters with at least one being non-letter.

- Group B: one third of the participants were instructed to create passwords by randomly picking eight characters from a sheet of paper with A-Z and 1-9 printed repeatedly with their eyes closed.

- Group C: one third of the participants were instructed to create passwords based on mnemonic phrases, for example *"I's12&Iah"* from *"It's 12 noon I am hungry"*.

Yan et al. then attempted to crack the passwords using brute force, dictionary, and combination approach. They successfully cracked significantly higher proportion of passwords in the naively selected password group (Group A) than in either the random character or mnemonic groups (Group B and C). To assess the memorability of each type of passwords, participants were asked to rate the difficulty of remembering the passwords using a five points Likert scale in a few months following the experiment. As a result, random passwords (Group B) were found to be the hardest to recall), while mnemonic and naively selected passwords were found to be as easy to remember as the other.

They further discovered that 35% of users in group A selected poor passwords, while both group B and C still suffered from a non-compliance rate of about 10%, including passwords which are too short and password created contrary to their instructions. This to some extent extends previous findings of Riddle et al (Section 3.2.2) and Dhamija and Perrig (Section 3.2.4) that despite the suggestions and instructions given, it is inevitable that some users would still create weak passwords.

3.2.8. Riley (2006)

Riley conducted a survey to investigate password generation practices and usage behavior involving 315 undergraduate and graduate students, with ages ranged from 18 to 58 years old. Participants were instructed to complete a self-report questionnaire.

On the topic of password generation, Riley reported that 85.7% of the participants use lowercase letters in high frequency. 54.9% indicated that they used personally meaningful words such as names of children, pets or street names as inspirations for create passwords. The reported length of passwords is on average 6.84 (S.D. = 1.79) characters, which seem to have improved since Morris and Thompson's study in 1979 (Section 3.2.1). In using passwords, 54.6% of participants reported using the same exact password for multiple

accounts “very frequently” or “always”, while 33% used variations of the same password for multiple accounts.

Another interesting finding from Riley’s survey is that when asked, the majority of the participants were able to identify most of the recommended password practices, such as, not using personally meaningful words or numbers as passwords, using special characters in their passwords, using passwords with seven or more characters, and changing passwords frequently. However, as Dhamija and Perrig (Section 3.2.4) and Yan et al (Section 3.2.7) discovered earlier, knowledge of secure practices does not always translate into real practices and behaviors - most of the participants in Riley’s study, even the ones who successfully identified recommended practices admitted to do things differently from what they believe they should do.

3.2.9. Gaw and Felten (2006)

Gaw and Felten [89] conducted a survey to investigate how users manage passwords for their online accounts, measured the extent of password reuse and users’ justification of this practice, and investigated user’s knowledge of attackers and their capabilities. Their survey involves 49 participants, most of which were undergraduate students at Princeton University.

In order to quantify how many web accounts each participants have, they first created a list of 139 websites which use login authentication and asked the participants to identify which websites they have accounts with. Participants were then given 90 seconds to login to the websites that they had identified, and were told to record the passwords for successful logins. Participants were also asked to recall other accounts that they use, but were not included on the list. Participants were reported to have 7.86 accounts (S.D. = 4.96, Range = 1 to 24) on average.

Gaw and Felten anticipated the possibility that users reused passwords with some transformations, and thus instructed users to group passwords which were created using the following transformations into ‘families’ [136]:

- Repeating a previously used phrase (nothing changes), such as "*Princeton*" and "*Princeton*"

- Changing the capitalization of letters within a phrase, such as "*Princeton*", "*princeton*", "*prINcEtoN*"

- Adding numbers or characters to a phrase, such as "*Princeton9*","*A-Princetonian*", "*PrincetonPrinceton*", "*AP~rinceton3*"

- Removing numbers or characters from a phrase, such as "*Pton*", "*Printon*", "*Prince*"

- Combining some of the previous methods

Unlike earlier studies by Dhamija and Perrig (3.3.4 above) and Brown (3.3.8 above), Gaw and Felten considered the number of unique passwords as number of families, thus passwords within the same 'family' (which were created by applying aforementioned transformations to the same base phrase) were not considered as unique passwords, even though they are semantically different.

On average, their participants had 3.31 password families (S.D. = 1.76, range = 1 to 10). Furthermore, they discovered that number of accounts increased by years in school, and concluded that people accumulate more online accounts as they get older. Number of unique passwords, however, was found not to increase by years of study. Gaw and Felten further quantified password reuse as the ratio of number of online accounts per unique passwords, and discovered that this ratio was positively correlated with the number of accounts (see Figure 12).

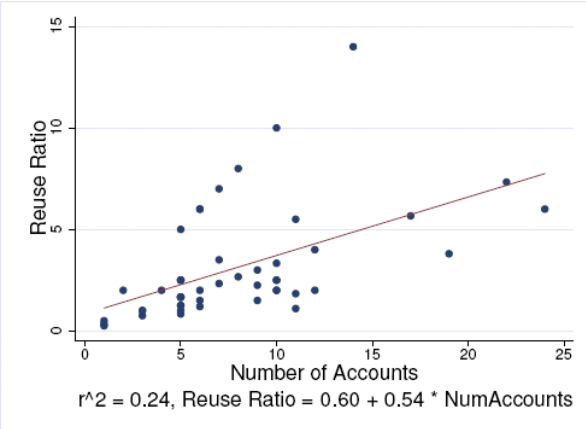


Figure 12: Plot of reuse ratio vs. number of accounts from Gaw and Felten's findings. Notice that reuse ratio increases as number of account increases. This shows that participants in Gaw and Felten's study tend to reuse more passwords as they accumulate more accounts.

Participants were then asked to justify their password reuse practices. "Ease to remember" was found to be the most popular reason cited for reusing passwords, while "security" and "protecting private information" were cited as the most frequent reasons for not reusing passwords. Moreover, responses from their participants seem to agree that they partition their accounts depending on their level of importance, and passwords based on their perceived security level, for example, "I don't use my 'less secure' password for accounts that contain credit card information, etc." Similarly, "for less important accounts, I use an easy password for simplicity."

Similar to Adams and Sasse's earlier findings (Section 3.2.3), Gaw and Felten also discovered that in general, most of their participants still conceptualized attacks as human adversaries who try to guess their passwords by hand, and majority do not understand how password cracking works.

3.2.10. Florencio and Herley (2007)

Florencio and Herley [130] from Microsoft Research conducted a large scale study of password usage and reuse practices which involved half a million participants. Data was collected by means of client software, which was shipped as a component of Windows Live Toolbar. The participation in this study was optional, as users were presented with an opt-in agreement.

This client software captured users' passwords, receiving URL and bitstrength of the passwords, and reported the gathered statistics to the server, only when user reuses his passwords on a different site, in order to capture every reuse event. However, the passwords and any other identifying information were not sent to the server. Passwords less than 20 bitstrength were excluded from this study; Florencio & Herley admitted this omission as a source of error. Participants were reported to have on average 25 accounts which require passwords, and 6.5 passwords (each of which is shared across 3.9 different sites).

Password bitstrength was calculated as:

$$log_2((alphabetsize)^{length})$$

where alphabet size is the sum of the sizes of different types of characters, i.e. lowercase (26), uppercase (26), digits (10) and special characters (22). Florencio and Herley compared the bitstrength of passwords used on 3 different sites, namely New York Times (an online newspaper subscription), PayPal (online payment service), Fidelity (financial related account), with passwords used on Microsoft OWA, an internal account for Microsoft employees for accessing their email and calendar information, which is governed by strong password creation and usage policy. Among these Microsoft OWA has the highest average password bitstrength (51.36), followed by PayPal and Fidelity (42.04 and 39.92 respectively), while New York Times was reported to have the lowest average password bitstrength (37.86).

Florencio and Herley noted that high average password bitstrength on Microsoft OWA was clearly a result of Microsoft's enforced password policy. Interestingly, participants seem to assign passwords of different strength based on the value of information related to the accounts – there is a considerable difference in bitstrength between passwords used to protect a newspaper (New York Times) and passwords used to protect financial related accounts (PayPal and Fidelity). Moreover, Florencio and Herley also discovered that

weaker passwords tend to be shared at more sites, while stronger ones at fewer. This agrees with Gaw and Felten's earlier findings (Section 3.2.9) which indicates that users do vary the complexity of their passwords depending on the account's importance and reuse less passwords on accounts which they consider to contain private and valuable information.

In general, although length of passwords seems to have vastly improved since Morris and Thompson's study in 1979 due to imposed password length requirements (a minimum of 6 characters is common at the time of this study), a large fraction of passwords were still found to only contain lowercase letters. Even for passwords which are 13 characters long, lowercase only passwords still account for 78% of the cases.

With 544,000 participants, this study is by far the largest study on passwords that has been done so far. Florencio and Herley's approach was rather different from other password studies we have discussed, as they were able to observe what people actually do over a period of time, rather than imposing users practices based on self reported information. However, Florencio and Herley stated their data was collected and analyzed under the assumption that each user only used one machine and one machine was only used by one user, and thus the results of their study might not be accurate if a lot of participants in fact had used more than one machine to access their accounts, or conversely, the machines had been used by multiple users.

3.3. Discussion

The earliest studies of password usage were analyses of large collections of passwords. Through these studies it was discovered that users tend to choose weak passwords. Later studies were based on surveys of users, resulting in better understanding of users' password practices. However, these studies came to an unsurprising conclusion: left to their own devices, most users tend to resort in insecure password practices and circumvent security measures in favour of convenience and practicality. While insecure passwords have been found to be extremely common, Dhamija and Perrig (Section

3.2.4), Riley (Section 3.2.8) and Yan et al (Section 3.2.7) have discovered that these insecure practices were not motivated by users' lack of security knowledge.

We believe that the underlying problem lies in users' perception of their accounts and passwords. Results from previous studies conducted by Gaw and Felten (Section 3.2.9) and Florencio and Herley (Section 3.2.10) have demonstrated that users do in fact use stronger passwords and avoid password reuse on accounts which are considered of high importance. Drawing from these findings and the concept of digital persona that we have discussed earlier in Section 1.3, we hypothesize that users manage their passwords and accounts by mentally classifying their accounts and passwords based on differing perceived similarities between their accounts and passwords. Below, we present two fictional examples of such classification. Example 1 (Figure 13) represents a user who groups his accounts based on their importance, and his passwords by their perceived security level. Example 2 (Figure 14) shows a user who groups his accounts by the type of service, and group his passwords based on inspirations used to create them.

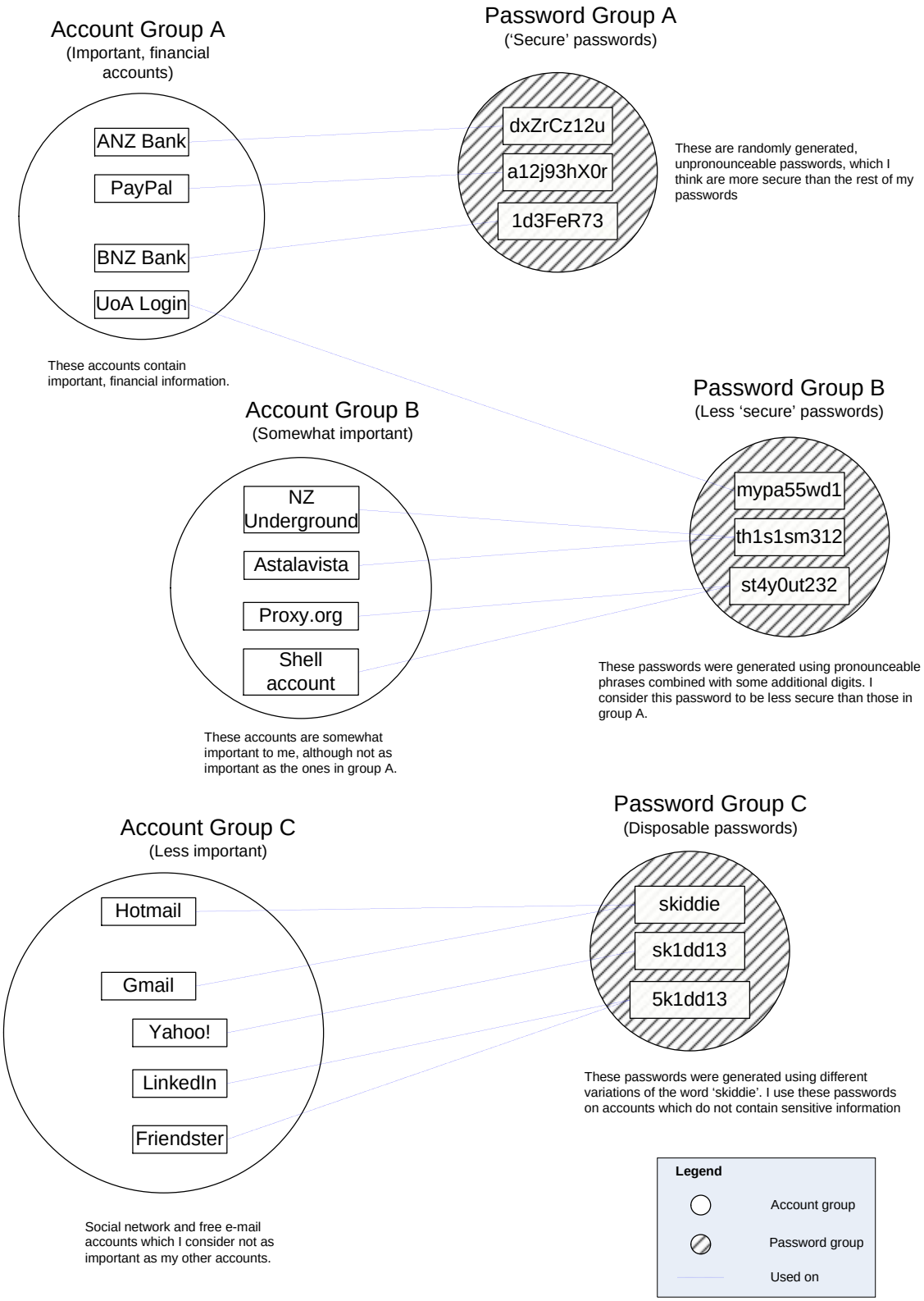


Figure 13: Example of account and password groupings. This example shows a user who groups his accounts based on their importance, and his passwords by their perceived security level

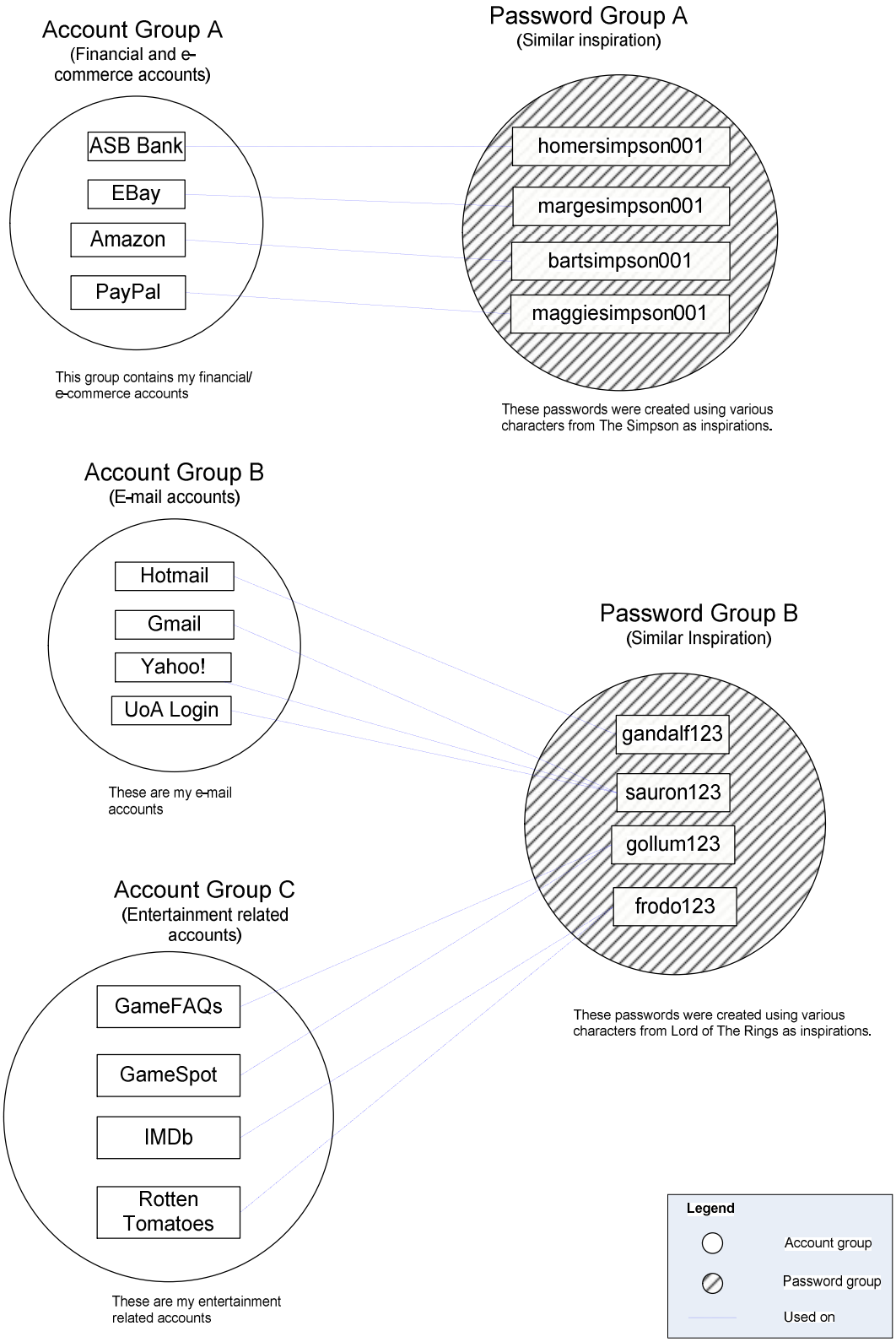


Figure 14: Example of account and password groupings. This example shows a user who groups his accounts by the nature of service, and group his passwords based on inspirations used to create them

This hypothesis would be the main organizing idea of our exploratory survey. In the next chapter, we discuss our ethical concerns and considerations which later influenced our survey design, and describe our survey procedures in details.

"Design can be art. Design can be aesthetics. Design is so simple, that's why it is so complicated." –Paul Rand

4

Survey Design

The University of Auckland regulations [137] requires its staff and students to obtain an approval from the Human Participants Ethics Committee for any studies involving human participations. During the application process, we realized that there are many ethical issues that need to be considered. In Section 4.1, we discuss our views and ethical concerns and how they affected our survey design, which is further described in Section 4.2.

4.1. Ethical Issues and Considerations

There is a belief in the society which considers science to be ethically neutral. This argument is likely to be based around Hume's classical proposition that no 'ought' can be correctly inferred from 'is', implying that no moral proposition can be derived from non-moral propositions [138]. Many believe that since ethics is primarily related to moral judgments, it has no relation to science, which is often perceived to only deal with rare facts. In contrary to this common belief, Bronowski [139] stated, "*Those who think science is ethically neutral confuse the findings of science, which are, with the activity of science, which*

is not". According to his view, science is affected by human views and interpretations, and thus is subject to moral judgments.

Despite these arguments, we realized that in any study that involves human participation, there are often tradeoffs and ethical considerations that have to be made concerning the amount of information that could be gathered without violating the rights or endangering the safety and well being of the participants. In 1966, an unethical experiment at National Women's Hospital in Auckland resulted in severe physical consequences to a significant proportion of individuals involved [131]. Although our study imposes almost no risk of physical injury, it involves rather sensitive information, which if exposed, could result in privacy or even financial loss to the participants.

The University of Auckland Human Participants Ethics Committee Guidelines [140] defines 8 ethical principles which govern research involving human participants, which are:

1. Informed and voluntary consent.

2. Respect for the privacy rights of participants.

3. Social and cultural sensitivity.

4. Acknowledgement of the Treaty of Waitangi.

5. Soundness of research methodology.

6. Transparency and the avoidance of conflict of interest.

7. Minimization of harm.

8. Principles relating to human remains, tissue, and body fluids.

We consider principles 3, 4, and 8 to be irrelevant to our study, because our study involves neither socio-culturally sensitive materials nor human remains. Among the rest, there are two principles that had a significant impact on our survey design.

The second principle – "Respect for the privacy rights of participants" implies that we have to respect the privacy rights of research participants. In order to achieve our research objectives by investigating how people manage their passwords, ideally, we would need to gather and analyze real passwords and accounts from our survey participants. However, asking participants to disclose such materials would be impossible without putting our participants' privacy rights at risk.

The seventh principle – "Minimization of harm" requires us to ensure that the risk of the participants being harmed is minimized. In our study, the most likely cause of harm is financial damage caused by the leakage of participants' passwords and accounts information. If we decided to collect real passwords and accounts from participants, we still could arrive at a difficult position if participants' accounts were compromised by other means completely unrelated to our study, even though we tried our best to minimize this risk.

We could also learn from a recent study conducted by Jagatic et al [141] on a closely related subject, phishing (for more details on phishing see our discussion in Section 2.2.1). Jagatic et al evaluated the viability of extending phishing attack using victim's social connections gathered from social networking websites, such as *Friendster*, *MySpace*, *Orkut* and *LinkedIn*, by mounting real attack to students at Indiana University, who had not been previously informed. The study, which was approved by Indiana University Human Subject Committee, revealed astonishing results – 349 (72%) of the 472 targeted individuals divulged their passwords in this experimental phishing attack.

This attracted a massive amount of complaints from both involved individuals and external observers [142, 143], accusing the study as unethical. While Jagatic et al claimed that passwords and other sensitive information were not stored, some subjects still felt angry and disappointed: "*Some subjects called the experiment unethical, inappropriate, illegal, unprofessional, fraudulent, self-serving, and/or useless. They called for the researchers conducting the study to be fired, prosecuted, expelled, or otherwise reprimanded*." [141]

Although there was no actual privacy or financial loss occurred as a result of this study, it is clear that the individuals involved suffered from emotional consequences. We avoid the debate regarding the ethicality of Jagatic et al's study; nevertheless, this incident has taught us that passwords are indeed sensitive information, whose disclosure could result in not only privacy and financial loss, but also emotional consequences.

This is a complicated situation. On one side we need to collect information about password and accounts from the participants in order to obtain accurate results and achieve our research objective. On the other side, after considering the ethical issues and potential harms, it seems that asking participants to entrust their actual passwords and accounts to us would be prohibitive. Thus, a tradeoff has to be made between the amount of information we could gather and the potential risks exposed to participants. Upon consideration, we decided to collect descriptions about participants' passwords and accounts without asking them to disclose their actual passwords and accounts. This decision influenced our survey methods, which is further discussed in the next section.

4.2. Survey Methods

4.2.1. Preparation

We submitted our application to The University of Auckland Human Participants Ethics Committee on 22 September 2006, and received an approval on 16 October 2006. Our application to the committee can be found in Appendix A.

Considering the time constraints of this project, we decided to take our sample population from the student body of our university. A consequence of this decision is that our results might not be the best representation of the general user population. We advertised our survey by means of posters which were posted on notice boards within various departments in both the City campus and Tamaki campus, as we intended to obtain sample data which is representative of our university's student population with diverse majors and degrees. A copy of our poster can be found in Appendix A.

Figure 15: Our posters in various locations within The University of Auckland.

We provided our e-mail address on the posters as a first point of contact for potential participants. Upon receiving expressions of interest from potential participants, we replied with a detailed description of our survey and our availability.

Participation in our survey was entirely voluntary. As a compensation for their time and effort, participants were rewarded $20 NZD after completing the survey. The survey was conducted from 28 September 2006 until 31 October 2006 (during second semester study break and examination period).

4.2.2. Survey Procedures

To solve the aforementioned problem (Section 4.1 above), we decided to use a coding scheme to allow participants to describe their passwords, accounts and associations between them without revealing their actual passwords and accounts. A potential weakness of this approach is that the procedure would be mentally exhaustive as participants would have to describe their passwords and accounts without writing them down. To avoid this, we decided to allow participants to write down their passwords and accounts on a sheet of paper as an aid for completing our survey, and instruct them to destroy the sheet using a provided commercial grade strip-cut paper shredder at the end of the procedure. We also advised participants to bring any passwords or accounts remembering aids, if they felt necessary.

The survey was conducted on one-to-one basis in a tutorial room within the Computer Science department. We anticipated the possibilities that the participants might accidentally or mistakenly attempt to reveal the sheets containing their accounts and passwords, or any remembering aids to us during the survey procedure. To minimize the likelihood of this incident, the seating positions were arranged as follows:

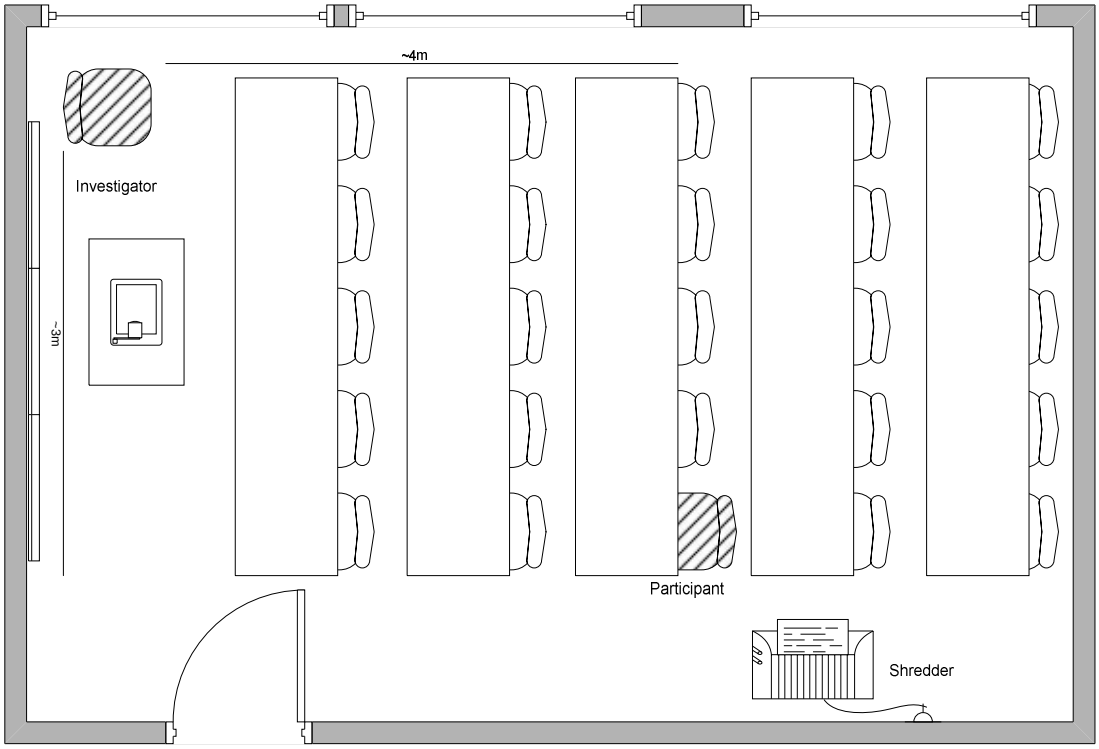


Figure 16: Seating arrangements during our survey.

This arrangement would prevent the participants from mistakenly showing any sensitive information to the investigator, while still allowing them to be guided throughout the entire survey procedures. Direct access to a commercial grade strip-cut paper shredder ensures that participants are able to destroy the sheet containing their actual accounts and passwords immediately after the survey procedures are completed.

Before the survey started, we presented the Participant Information Sheet, which outlines the terms and conditions of taking part in our research, to our participants and asked them to sign the Participant Consent Form. These forms can be found in Appendix A.

Our survey consists of two main parts. In the first part, the participants were asked a few general questions about their background information (degree pursued, major of study, number of years spent at the university), and experience with computers and the internet.

The second part consists of a guided exercise, which was performed using the worksheets that we provided. The exercise procedures comprise of five steps:

1. Participants were asked to write all their passwords in a piece of paper. This was done to help participants in the next procedure.

2. After given thorough explanation about the hypothesis regarding how people organize their passwords by mentally grouping them, participants were then asked to complete a table by assigning numbers and codes to their passwords according to the way they group their passwords based on their perceived similarities (see Table 2.). We also instructed the participants to describe the similarities that they use as a basis for grouping their passwords together. In cases where participants did not use any grouping to help them organize their password, they were instructed to use a different group for each password, and leave the 'similarities' column blank.

Group	Code	Password	Reason/types of similarities used for grouping
1	A	abcd	Similar length (4-5 characters)
	B	pass	
	C	itsme	
	D	pswd	
	E		
2	A	do182ad9	Similar length, combination of alphabetical/numerical characters
	B	4uckld012	
3	A	u1a2c3u#3	*(ungrouped password)*
…	…	…	…

Table 2. An example of the table used in Step 2.

The sheet containing this table would be used to as a reference for completing the next step, the reason for this is because, as we mentioned earlier, asking participants to describe their passwords and groupings without writing their passwords down would be mentally exhaustive. The participants were also instructed not to show this sheet to anyone else including us.

3. Participants were instructed to describe each of their passwords by completing the following columns:

- **Length**

  The total number of characters in each password.

- **Perceived security level**

  Measured using a 5 point Likert scale based on the participants' perceptions of how secure each of their passwords is, with 1 being the least secure and 5 being the most secure.

- **Difficulty of recall**

  Measured on a 5 point Likert scale based on the participants' perceptions of how difficult it is to recall each of their passwords, with one being the least and 5 being the most difficult.

Group	Code	Length	Perceived security level (1-5)	Ease of recall (1-5)	Reason/types of similarities used for grouping
1	A	4	1	5	Similar length, short passwords (4-5 characters)
	B	4	1	5	
	C	5	1	5	
	D	4	1	5	
2	A	8	4	2	Similar length, combination
	B	9	4	3	of alphabetical/numerical
					characters
3	A	9	5	1	
…	…	…	…	…	…..

Table 3: An example of the table used in Step 3.

Participants were asked to replicate the numbering scheme and reasons for grouping which they had completed in the previous step using the previous worksheet as a reference. However, this time, they were instructed not to write

down their actual passwords, as they would be asked to hand in the sheet containing this table at the end of the survey.

4. Similar to Step 2, participants were told to list their accounts in a table and assign numbers and codes to them, following the manner in which they organize their accounts using mental groups according to their similarities as perceived by the participants themselves.

Group	Code	Account	Reason/types of similarities used for grouping
1.	A	Hotmail	Free web based e-mail
	B	Gmail	
2.	A	Online banking	Valuable/very important information
	B	Personal health record	
3.	A	Trademe	Online auction/trading account
	B	E-bay	
…	…	….	…..

Table 4: An example of the table used in Step 4.

The sheet containing the above table would only be used as an aid to complete the next step, and participants were instructed not to show this sheet to anyone else including us.

5. Finally, participants were asked to collate all the previous information together by completing the following columns for each of their accounts

Account group	Code	Reason/types of similarities used for grouping accounts	Value of information	Frequency of use	Password (group number and code only)	Is password reused (Y/N)	Reason why password is reused/not reused
1	A	Free web based e-mail	2	4	1A	Y	7
	B		2	4	1A	Y	7
2	A	Valuable/very important material	5	2	2A	N	2
	B		5	2	3A	N	2
3	A	Online auction/trading account	4	3	2B	Y	4
	B		4	3	2B	Y	4
…	…	…	…	…	…	…	…

Table 5. An example of the table used in Step 5.

- **Account group**

  Corresponding account group number from the previous step.

- **Code**

  Corresponding account code from the previous step.

- **Value of information**

  Measured using a 5 point Likert scale based on the participants' perceptions of the value of information associated with the account, with 1 being the least valuable and 5 being the most valuable.

- **Frequency of use**

  Measured using a 5 point Likert scale based on the frequency of usage of the account, with 1 being the least frequent and 5 being the most frequent.

- **Password (Number and code only)**

  Password assigned to the account. We instruct the participants to not to write their actual password, but only the number and code they previously assigned to their passwords in Step 2.

- **Password reuse (Y/N)**

  Participants were asked to choose 'Y' if the password which is used on this particular account is also used on at least one other account or 'N' if the password used on this particular account is unique, or has not been used on any other account.

- **Reason why password is reused/not reused**

  Justification as to why participants decided to reuse or not to reuse passwords on a particular account. As a starting point, we provided the participants with two lists of statements, and instructed them to select one which they think

would be the best representative of their reasoning. Alternatively, participants were also allowed to choose "other" and describe their own reasons.

Below are the statements that we provided. We asked our participants to choose a statement from these if they reused password for an account:

1. This account belongs to the same category as the other account(s) which use the same password.

2. This account belongs to the same domain (leisure/work/family) as the other account(s) which use the same password.

3. I use this account in the same frequency as the other account(s) which use the same password.

4. The information that is stored under this account is of similar value/importance to the information stored under the other account(s) which use the same password.

5. I only have one password and I use it for all my accounts.

6. I have several passwords and I randomly assigned them to my accounts.

7. I reuse password for this account because it is easy to remember.

8. Other (please describe).

In cases where they chose not to reuse their password for a particular account, we asked them to choose a statement from the list below:

1. The account provider has password format restrictions, so I had to change my password to meet their restrictions.

2. The information stored under this account is of high value/importance.

3. I created a random password for this account.

4. I created a unique password to avoid confusion with my other account(s).

5. The password was assigned by the account provider.

6. I try to avoid password reuse because I believe it is not secure.

7. Other (please describe)

After all the procedures were completed, participants were instructed to separate and destroy the sheets containing their actual passwords and accounts from step 1, 2, and 4, using a provided commercial grade strip-cut paper shredder. The rest of the sheets were collected by us.

"Results! Why, man, I have gotten a lot of results. I know several thousand things that won't work." –Thomas A. Edison

5
Results

In this chapter we present the results of our survey. All statistical tests in this chapter were performed using SPSS version 14 for Windows, unless otherwise stated. We organized our analysis based on the following questions:

Question1: Do majors of study and gender have any effect to the number of accounts, number of passwords, number of account groups and number of password groups maintained by our participants?

Question 2: Do our participants perceive longer passwords to be more secure?

Question 3: Do our participants perceive longer passwords to be more difficult to recall?

Question 4: Do our participants perceive more secure passwords to be more difficult to recall?

Question 5: Does number of account increase as our participants gain more computing or internet experience?

Question 6: Does number of passwords increase as our participants gain more computing or internet experience?

Question 7: Do our participants reuse more passwords as they accumulate more accounts?

Question 8: Why do our participants reuse their passwords?

Question 9: Do our participants classify their accounts and passwords according to our hypothesis in Section 3.3.? If so, what similarities do they use to classify their accounts and passwords?

Question 10: Do our participants manage their account groups they consider as having more importance differently from their other account groups?

Question 11: What percentage of our participants reused their university passwords on their other accounts?

5.1. Data Description

5.1.1. Descriptive Statistics

During our pilot run, we successfully collected data from 26 participants; all were students at the University of Auckland at the time of the survey. Among the participants, 14 were male and 12 were female. Our participants came from various faculties and departments across the university and were pursuing different degrees and majors. Below are plots showing the distribution of participants by degree pursued and majors.

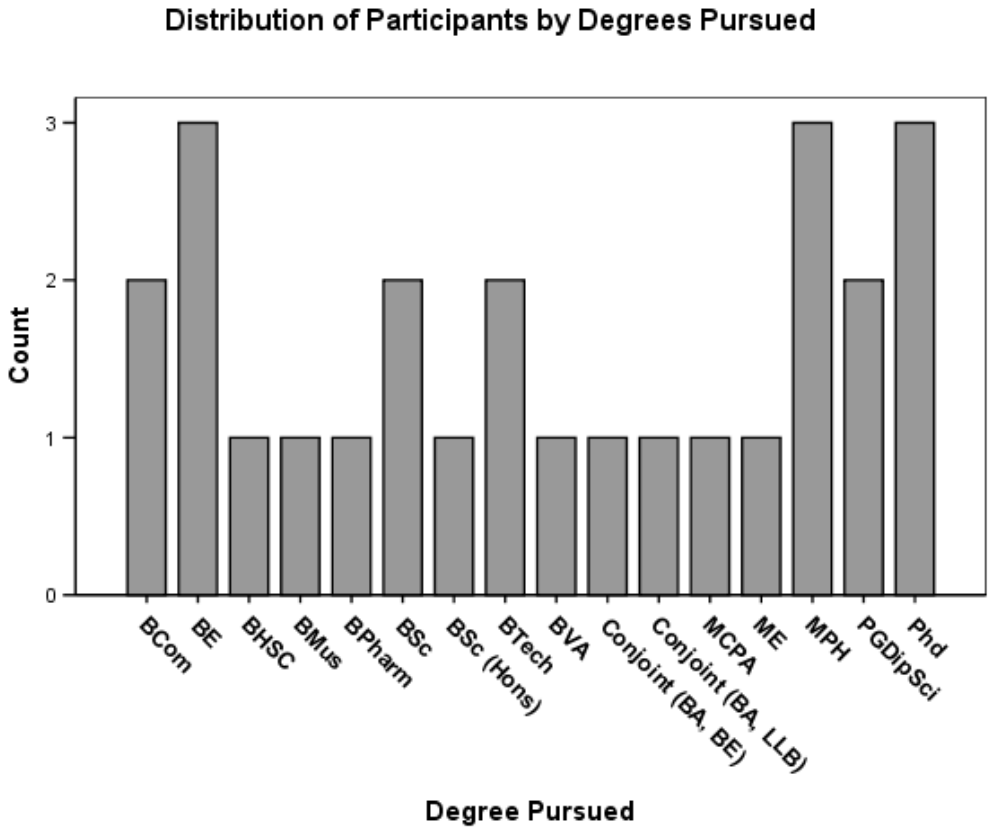
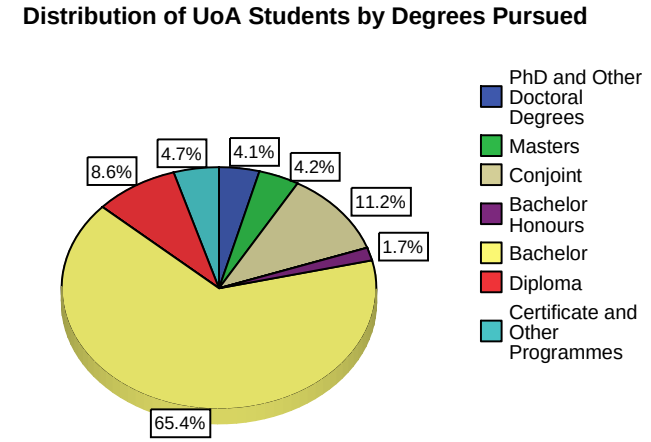
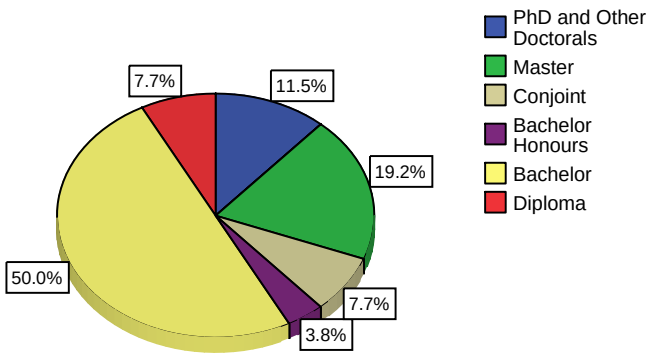


Figure 17: A bar plot showing the distribution of the participants by degrees pursued. The highest number of participants was studying for Bachelor of Engineering (3), Master in Public Health (3), and PhD (3), closely followed by Bachelor of Commerce (2), Bachelor of Science (2), Bachelor of Technology (2) and Postgraduate Diploma in Science (2). Each of the other degrees only contributed one participant to our final count.



a). Distribution of students at the University of Auckland by degrees pursued



b). Distribution of our respondents by degrees pursued

Figure 18 a, b: A comparison of the distribution of degrees pursued between the overall student population at The University of Auckland [144] (a) and our survey participants (b).

Although we received responses from almost all levels of degree offered at The University of Auckland, our sample population does not give a precise representation of the whole student population at the university. This is due to the relatively high proportion of Doctoral and Master students in our sample population, and somewhat lower proportion of undergraduates compared to the overall student population (see Figure 18). We suspect that this might be caused by the timing of our survey, which was conducted during the second semester study break and examination period. At our university, most

students at Doctoral and Master level are not required to sit any examinations, whereas undergraduates were mostly occupied by exam preparation during that time.

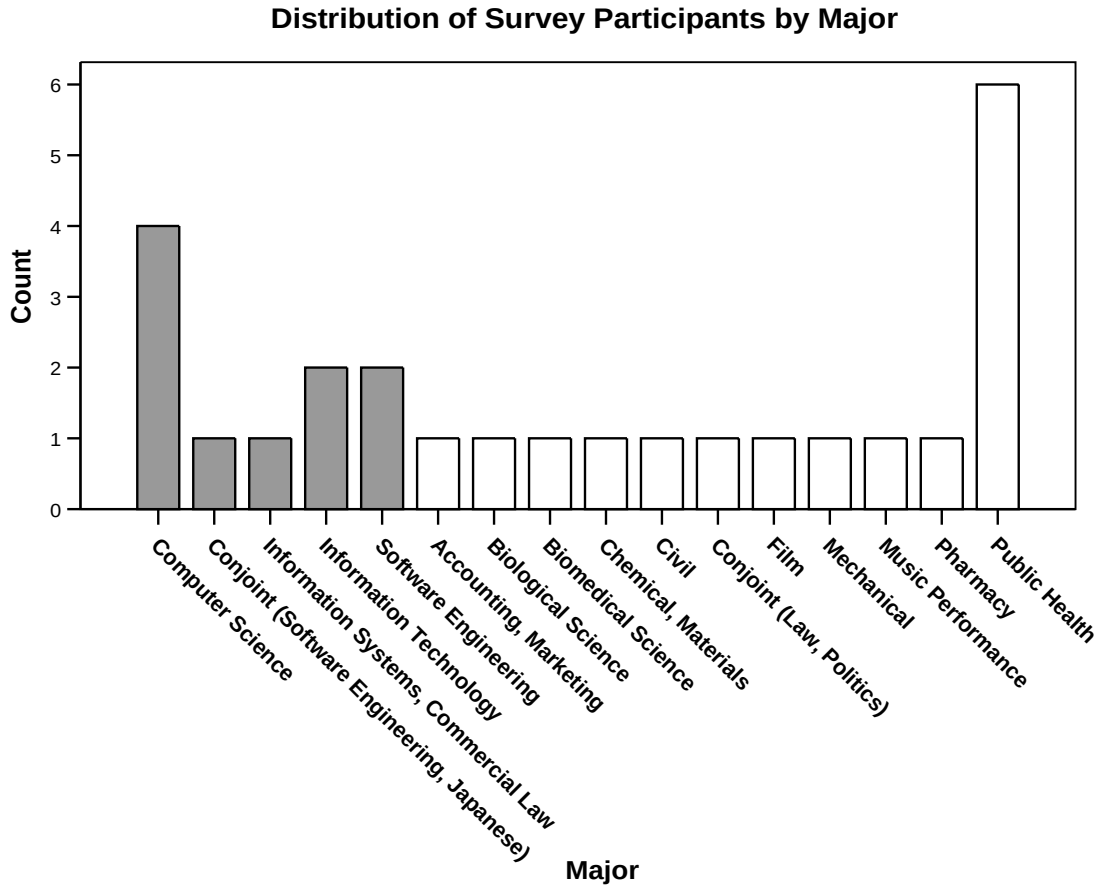


Figure 19: A bar plot showing the distribution of the participants by majors of study. Grey boxes represent all IT related majors, white boxes represent non-IT related majors.

It can be seen from the bar plot above that the highest number of our participants (6) chose Public Health as their major of study, followed by Computer Science (4), and Information Technology (2). Each of the other majors only contributed one participant to our final count. 10 participants (38.5%) were studying for IT related qualifications (Computer Science, Information Technology, Information Systems, and Software Engineering), or incorporated IT related majors to their study, while 16 other (61.5%) were studying for non IT related qualifications. Although we were unable to find the actual distribution of the student population at University of Auckland by their majors, we still suspect that our sample population might not be the best representation of the overall student population; therefore, our results must be interpreted with extreme care.

We measured 4 variables from each response that we collected:

- **Number of Passwords** (NOP), measured by counting the number of passwords from each response.
- **Number of Accounts** (NOA), measured by counting the number of accounts from each response.
- **Number of Password Groups** (NOPG), measured by counting the number of password groups from each response
- **Number of Account Groups** (NOAG), measured by counting the number of account groups from each response.

Below are the histograms and descriptive statistics of each of these variables:

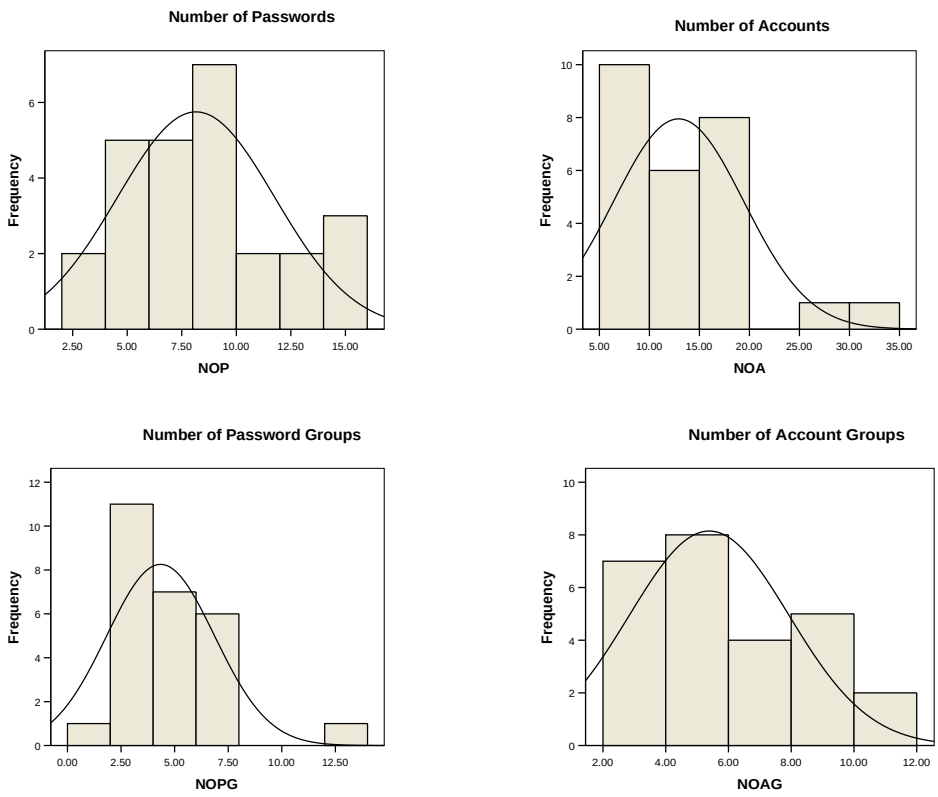


Figure 20: Histograms showing the distribution of number of passwords (NOP), number of accounts (NOA), number of password groups (NOPG) and number of account groups (NOAG)

Descriptive Statistics

Variables	N	Minimum	Maximum	Median	Mean	Std. Deviation	Skewness	
							Statistic	Std. Error
NOP	26	3.00	16.00	8.00	8.1538	3.60768	.596	.456
NOA	26	6.00	34.00	10.00	12.9231	6.52333	1.548	.456
NOPG	26	1.00	14.00	4.00	4.3462	2.51304	2.375	.456
NOAG	26	2.00	12.00	5.00	5.3846	2.54679	.838	.456

Table 6: Descriptive statistics of number of passwords (NOP), number of accounts (NOA), number of password groups (NOPG) and number of account groups (NOAG).

On average, each of our participants declared 12.9 accounts and 8.1 passwords. All distributions appear to be positively skewed to some extent, which seem to be more evident in Number of Accounts (NOA) and Number of Password Groups (NOPG), although not so obvious in Number of Passwords (NOP) and Number of Account Groups (NOAG). Skewness indicates departure from normality, and since many statistical tests are based on the assumption that the data being tested is normally distributed, the reliability of these tests may be severely affected. However, Kolmogorov-Smirnov test provided no significant evidence against the underlying distribution of our data being normal (NOP: P-value = 0.705; NOA: P-value = 0. 196; NOPG: P-value = 0.084; NOAG: P-Value = 0.454).

In addition to these, we also asked our participants about the number of years of internet and computing experience that they had. We recorded these in two separate variables called **Years of Internet Experience (YOIE)** and **Years of Computing Experience (YOCE).**

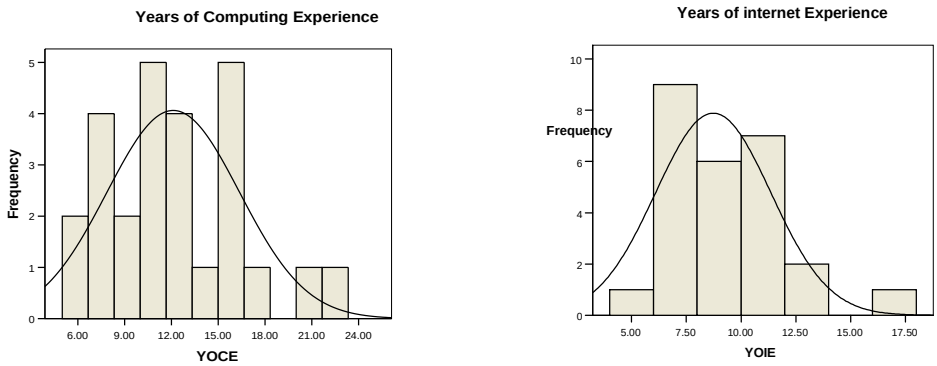


Figure 21: Histograms showing the distribution of Years of Computing Experience (YOCE) and Years of Internet Experience (YOIE).

Descriptive Statistics

Variables	N	Minimum	Maximum	Median	Mean	Std. Deviation	Skewness	
							Statistic	Std. Error
YOCE	26	6.00	22.00	11.50	12.1154	4.25513	.558	.456
YOIE	26	4.00	17.00	8	8.7308	2.63147	1.116	.456

Table 7: Descriptive statistics of Years of Computing Experience (YOCE) and Years of Internet Experience (YOIE).

Years of Internet Experience appears to have a smaller range and less variability than Years of Computer Experience. This is probably due to the fact that the internet itself has only been widely available for a relatively shorter period of time compared to computers. Both of these variables are somewhat positively skewed, however, Kolmogorov-Smirnov test provided no evidence against the underlying distribution of these variables being normal (YOCE: P-value = 0.585, YOIE: P-value = 0.621).

5.1.2. Effects of Gender and Qualifications

Before we proceed, we would like to assess the effects of gender and qualifications on the numbers of passwords, accounts, passwords groups and account groups. The questions of interest here concern the potential effects of the factors gender and qualifications on the aforementioned variables (Question 1). The results of this analysis will also determine

whether further steps, such as clustering would have to be taken to ensure that effect of gender and qualifications do not bias our end results. We hypothesized that:

Hypothesis 1: Both gender and qualifications studied would have some effect to numbers of passwords, accounts, passwords groups and account groups.

The reason for this is that participants who were studying for computer science, software engineering, and other IT related qualifications, would have had more exposure to computers and online services compared to participants who were studying for non-IT related subjects, thus they are very likely to have more accounts and passwords. They are also very likely to be more aware of the safety of their online identities. While it might seem rather speculative to suspect that gender has an effect to these variables, there are some existing literatures which suggest that there are differences between male and female users in their computer usage behaviors and perceptions towards technology [145], ability to detect deceptions in computer based media [146], and capability of performing various operations and utilizing features of a computer software [147]. Thus, we believe that there is no reason not to anticipate that there would be differences between male and female participants in the way they treat and manage their online identities.

We used Two-Way ANOVA (Analysis of Variance) to assess the effects of gender and qualification on number of passwords, number of password groups, number of accounts, and number of account groups. Since it would be impractical to evaluate all qualifications separately, we decided to partition the qualifications into two major groups, IT related and non-IT related qualifications. 10 participants who were studying for Computer Science, Information Systems, Software Engineering, Information Systems and Information Technology were placed under 'IT related qualification' category, while 16 participants who were studying for other qualifications were placed under 'non-IT related qualification' category.

a). Tests of Between-Subjects Effects (Number of Passwords)

Dependent Variable: NO_OF_PASSWORDS

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Model	1733.397(a)	4	433.349	29.737	.000
GENDER	.933	1	.933	.064	.803
QUALIFICATIONS	1.691	1	1.691	.116	.737
GENDER * QUALIFICATIONS	1.082	1	1.082	.074	.788
Error	320.603	22	14.573		
Total	2054.000	26			

a R Squared = .844 (Adjusted R Squared = .816)

b). Tests of Between-Subjects Effects (Number of Password Groups)

Dependent Variable: NO_OF_PASSWORD_GROUPS

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Model	499.825(a)	4	124.956	18.428	.000
GENDER	2.493	1	2.493	.368	.550
QUALIFICATIONS	2.154	1	2.154	.318	.579
GENDER * QUALIFICATIONS	1.284	1	1.284	.189	.668
Error	149.175	22	6.781		
Total	649.000	26			

a R Squared = .770 (Adjusted R Squared = .728)

c). Tests of Between-Subjects Effects (Number of Accounts)

Dependent Variable: NO_OF_ACCOUNTS

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Model	4400.254(a)	4	1100.063	24.063	.000
GENDER	1.082	1	1.082	.024	.879
QUALIFICATIONS	40.834	1	40.834	.893	.355
GENDER * QUALIFICATIONS	3.877	1	3.877	.085	.774
Error	1005.746	22	45.716		
Total	5406.000	26			

a R Squared = .814 (Adjusted R Squared = .780)

d). Tests of Between-Subjects Effects (Number of Account Groups)

Dependent Variable: NO_OF_ACCOUNT_GROUPS

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Model	759.619(a)	4	189.905	26.716	.000
GENDER	.199	1	.199	.028	.869
QUALIFICATIONS	5.478	1	5.478	.771	.389
GENDER * QUALIFICATIONS	.000	1	.000	.000	1.000
Error	156.381	22	7.108		
Total	916.000	26			

a R Squared = .829 (Adjusted R Squared = .798)

Table 8 a, b, c, d: Results of Two-way ANOVA assessing the effects of gender and qualifications to Number of Passwords (NOP), Number of Password Groups (NOPG), Number of Accounts (NOA), and Number of Account Groups (NOAG).

In contrary to Hypothesis 1, the tests that we performed showed no evidence that gender and qualification interact on the number of passwords (P-value = 0.788, refer to Table 8a), number of password groups (P-value = 0.668, refer to Table 8b), number of accounts (P-value = 0.774, refer to Table 8c), number of account groups (P-value=1.0, refer to Table 8d).That is, if we change gender the effect on these variables is the same for those who are studying for IT related qualifications and those who are studying for non IT related qualifications and vice versa.

There is no evidence that the gender of the participant alone has any effect on number of passwords (P-value = 0.803, refer to Table 8a), number of password groups (P-value = 0.550, refer to Table 8b), number of accounts (P-value = 0.879, refer to Table 8c), number of account groups (P-value = 0.869, refer to Table 8d). Furthermore, we also have no evidence that qualification pursued by the participant alone has any effect on the number of passwords (P-value = 0.737, refer to Table 8a), number of password groups (P-value = 0.579, refer to Table 8b), number of accounts (P-value = 0.355, refer to Table 8c), number of account groups (P-value = 0.389, refer to Table 8d).

Further analysis also suggests that there is no significant difference between participants who were studying at undergraduate level and postgraduate level, in number of passwords (P-value = 0.476), number of password groups (P-value = 0. 943), number of accounts (P-value = 0. 775), number of account groups (P-value = 0. 777).

5.2. Password Properties: What Do People Think of Their Passwords?

We asked our participants to describe their passwords by completing 3 columns on the worksheets that we provided (refer to Section 4.2.2. above). As a result, we obtained 3 variables for each of their passwords:

- **Length**, measured by counting the number of characters in each password.

- **Perceived security level**, measured on 5 point scale (Likert) based on the participants' perceptions of how secure each of their passwords is, with 1 being the least secure and 5 being the most secure

- **Difficulty of recall**, also measured on a 5 point scale (Likert) based on the participants' perceptions of how difficult it is to recall each of their passwords, with one being the least and 5 being the most difficult.

We are interested to investigate whether there are any correlations between these variables to answer questions 2, 3 and 4. Our initial hypotheses were as follow:

Hypothesis 2: Longer passwords are perceived to be more secure.

Consequently, we suspect that there would be a positive correlation between length and perceived security level of the passwords, because it is quite common for people to assume that longer passwords are more secure and vice versa.

Hypothesis 3: Longer passwords are more difficult to recall.

We anticipated that our data would show a positive correlation between length and difficulty of recall, because we believe that shorter passwords are usually easier to recall, and that the longer a password is, the more likely it becomes difficult to recall.

Hypothesis 4: Secure passwords are more difficult to recall.

We also suspect that there would be a positive correlation between perceived security level and difficulty of recall. It is a common perception that 'random' passwords are more secure (at least against dictionary or guessing attacks), and random passwords are usually harder to recall. During our survey, there were two participants who asked for a QWERTY keyboard as an aid to remember some of their passwords, because according to them, some of their 'secure' passwords are extremely random and unpronounceable that it becomes difficult to mentally recall them without relying on their finger movements.

The easiest way to analyze our data would be to pool passwords from all participants together into a single table and pretend as though all passwords came from different individuals; however, we believe that this would not be appropriate, since the variability between subjects is more likely to bias the result as each of the participants did not have the same amount of passwords. Pooling multiple observations from a single subject has also been noted to be likely to generate type I error [148, 149]. Taking these into consideration, we decided to collapse multiple observations from each participant by calculating the arithmetic mean of each variable from each participant, and use the results in our analysis, as suggested in [150]

One-sample Kolmogorov-Smirnov test of all three variables showed no evidence against the hypothesis that our data could have come from a normal distribution. (Length: K-S Z = 0.608, P-value = 0.854; Perceived Security Level: K-S Z = 0.731, P-value = 0.659; Difficulty of Recall: K-S Z = 0.703, P-value = 0.706).

We tested Hypotheses 2, 3 and 4 using non-parametric tests, Kendall's Tau and Spearman's Rho, instead of the renowned Pearson's correlation. Pearson's correlation test requires all variables to be on interval scale, while two of our variables were measured on a 5 point Likert scale, which is not an interval scale.

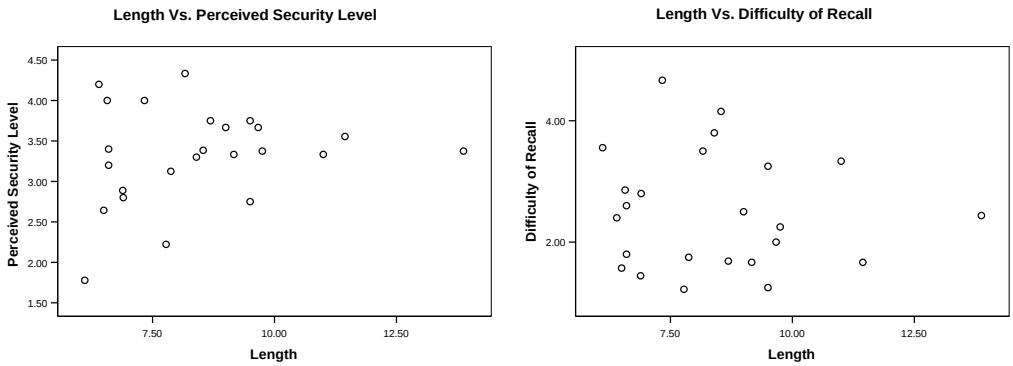


Figure 22: Scatter plot showing the relationship between length of passwords and perceived security level, and length of passwords and difficulty of recall. In contrary to our hypotheses (Hypotheses 2 and 3 above), there appears to be no positive correlation between these variables.

Our test indicated that there was no evidence that there is a significant correlation between length and perceived security level of the passwords (Kendall's Tau = 0.106, P-value = 0.471; Spearman's Rho = 0.165, P-value = 0.442). There was also no evidence of a significant correlation between length and difficulty of recall. (Kendall's Tau = -0.062, P-value = 0.673; Spearman's Rho = -0.089, P-value = 0.680).

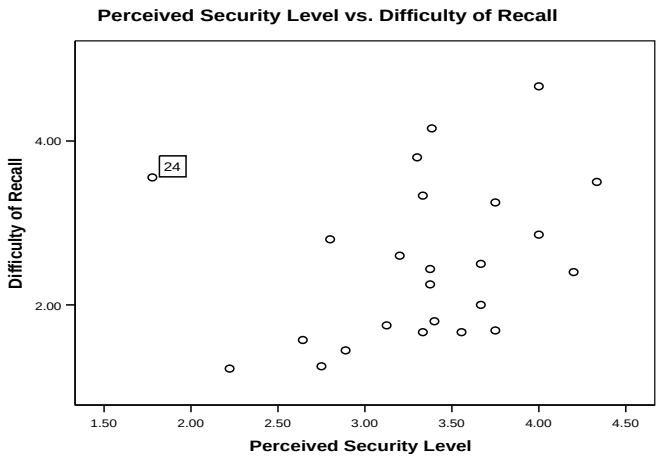


Figure 23: Scatter plot showing a positive relationship between perceived security level and difficulty of recall. There is an indication of a positive linear trend between these variables. In accordance to our hypothesis (Hypothesis 4 above), our participants seem to think that higher security passwords as being harder to recall, and vice versa.

There is, however, some evidence that there is a significant correlation between perceived security level and difficulty of recall (Kendall's Tau = 0.278, P-value = 0.059; Spearman's Rho = 0.359, P-value = 0.085). Visual observation of the scatter plot (refer to Figure 23 above) has also shown that there is an indication of a positive trend between these two variables, although there one possible outlier (participant 24). Further investigation suggests that most of this participant's passwords (6 out of 9 passwords declared), were 13 to 14 characters long, which are reasonably lengthy compared average length of passwords declared by our participants, which is only 8.6 characters. Excluding participant 24 from our analysis resulted in highly significant evidence of a correlation between perceived security level and difficulty of recall (Kendall's Tau = 0.372, P-value = 0.014; Spearman's Rho = 0.503, P-value = 0.014).

Our data provided no supporting evidences for hypothesis 2 and 3, that longer passwords would be perceived to be more secure and harder to recall. Nevertheless, we obtained some evidence in favor of hypothesis 4, that according to our participants' perceptions, the more secure a password is perceived to be, the more difficult it becomes to recall and vice versa.

5.3. Password Reuse Statistics

5.3.1. The growth of accounts and passwords

We are interested to investigate whether number of accounts and passwords increase as people gain more computing and internet experience (Questions 5 and 6). Our initial hypothesis was as follows:

Hypothesis 5: Number of accounts increases overtime, as people gain more computing and internet experience.

Hypothesis 6: Number of passwords increases overtime, as people gain more computing and internet experience.

Due to the increase of the number of online services requiring password based authentication from time to time, we would expect the number of accounts and passwords of computer users to correlate with the amount of computing and internet experience, i.e. longer exposure to computers or the internet would translate into more accounts.

In order to answer this question and verify our hypotheses, we built a regression model using the data that we collected. There were two potential predictors for our model, Years of Computing Experience (YOCE) and Years of Internet Experience (YOIE) (refer to 5.1.1. for more explanation of these variables). Further investigation suggests that YOCE and YOIE are in fact highly correlated ($r = 0.642$, P-value < 0.001). Using both variables in our model would result in *multicollinearity* problem, which could potentially bias our parameter estimation. Thus, we decided to choose only the most suitable predictor in our model and discard the other variable.

After considering all possible regressions as suggested in [151] using R^2 as our selection criterion, Years of Computing Experience (YOCE) was found to be of no further assistance

in explaining the number of online accounts, this could be due to the fact that during pre-internet era there were not many services which require accounts compared to the period after the internet became widely popular. Thus we decided to only use Years of Internet Experience (YOIE) in our final model (F = 7.696, R^2 = 0.243, Adj. R^2 = 0.211, P-value = 0.011).

Coefficients(a)

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	2.258	4.009		.563	.578	-6.015	10.532
	YOIE	1.222	.440	.493	2.774	.011	.313	2.130

a Dependent Variable: NOA

Table 9: Summary of the coefficients in our regression model using Years of Internet Experience (YOIE) as a predictor for Number of Accounts (NOA).

Our model explains 24% of the variation in the number of online accounts and therefore is not suitable for prediction. Nevertheless, we obtained very strong evidence for Hypothesis 5, that years of internet experience is related to the number of online accounts. We estimate, holding everything else constant, that for each year increase in the number of years of internet experience, the number of online accounts maintained by our participants changes by on average 1.2 accounts.

In contrast to Hypothesis 6, number of passwords does not seem to correlate with both Years of Internet Experience (YOIE) and Years of Computing Experience (YOCE). We were unable to build a significant regression model using our time variables to predict number of passwords.

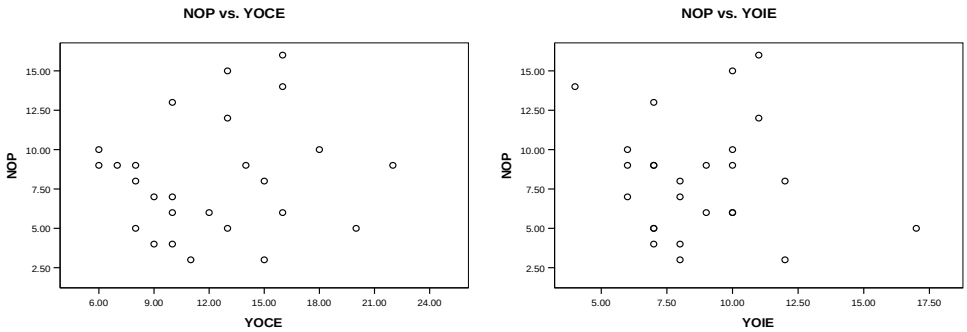


Figure 24: Two scatter plots showing the relationships between Number of Passwords and Years of Computing Experience (YOCE) and Number of Passwords and Years of Internet Experience (YOIE).

Regression	Adjusted R sq.	F	P-value
YOIE	-0.027	0.337	0.567
YOCE	-0.024	0.407	0.53
YOCE, YOIE	0.006	1.07	0.359

Table 10: Summary of all possible linear regression models using Years of Internet Experience (YOIE) and Years of Computing Experience (YOCE) as predictors for Number of Passwords (NOP)

Although we found no evidence that the variation in the number of passwords is related to differences in computing and internet experience, we are still convinced that these experience does affect the growth of passwords to a certain extent, for example there would obviously be a difference in the amount of passwords between someone who has only used computers for a day and someone who has 5 years of computing experience, and so forth. However, there might be other factors which are more influential to the variation in the number of passwords other than time, such as human memory limitations, convenience and so on. There is also a possibility that people would stop creating new passwords at some point and just keep reusing their existing passwords from then onwards. Furthermore, since all of our participants had more than 5 years of computing experience, we were unable to investigate further what happened during their earlier years of experience, which we suspect is vital to the development of their passwords.

5.3.2. Occurrences of Password Reuse

In the previous section we discussed that number of accounts tends to grow as our participants gain more internet experience, and with the rising number of online services which require password authentication, the rate at which the number of accounts grow per year is very likely to increase. We are interested to investigate whether our participants reuse more passwords as they accumulate more accounts (Question 7).

Regardless of any factors which might influence the growth of passwords, it is certain that if the number of passwords does not keep up with the increase in the number of accounts, people would have to reuse their passwords. Thus, we hypothesized that:

Hypothesis 7: People reuse more passwords as they accumulate more accounts.

We measured the number of password reuse occurrences, i.e. the number of accounts on which our participants reused their passwords, from each participant's data, and plotted our result against the total number of accounts. It is evident in the scatter plot below that our participants reused more as they accumulate more accounts.

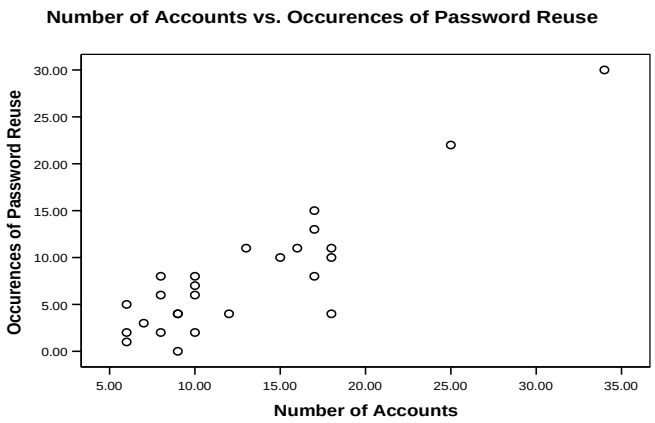


Figure 25. A scatter plot showing the relationship between number of accounts and number of password reuse occurrences. It can be seen that there is a positive linear trend between number of accounts and occurrences of password reuse.

We then constructed a linear regression model, using number of accounts as a predictor for number of password reuse occurrences. The summary of our model is presented in Table 11 below.

Linear Regression Model Coefficients(a)

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.	95% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	-4.101	1.466		-2.797	.010	-7.142	-1.061
	NOA	.926	.099	.894	9.352	.000	.721	1.132

a Dependent Variable: REUSED_ACCOUNTS

Table 11 : Summary of our linear regression model, which uses Number of Accounts (NOA) as a predictor for the number of password reuse occurrences. Reuse Occurrences = -4.101 + 0.926 x Number of Accounts

Our regression model explains 80% of the variation in the number password reuse occurrences and therefore would be reasonably suitable for prediction ($F = 87.465$, $R^2 = 0.799$, Adj. $R^2 = 0.790$, P-Value < 0.001). We obtained very strong evidence for Hypothesis 7, that is, the increase in number of password reuse occurrences is related to the increase in the number of accounts. We believe that the significant constant variable reflects that there is on average 4.1 accounts on which our participants did not reuse their passwords, whereas, the highly significant NOA coefficient suggests that apart from those accounts, our participants would reuse their passwords on almost all their other accounts. Since our participants only have from 6 to 34 accounts, we cannot make any inference outside of this range.

Participant	Number of Accounts	Number of Passwords	Number of Password Reuse Occurrences	Number of Unassociated Passwords
1	6	3	5	0
2	18	15	4	0
3	25	5	22	0
4	10	6	6	1
5	8	3	8	0
6	8	9	2	2
7	9	10	0	1
8	8	7	6	?
9	9	4	4	?
10	6	6	2	1
11	34	8	30	0
12	12	12	4	0
13	17	14	8	3
14	17	6	15	0
15	18	13	10	1
16	13	5	11	0
17	17	8	13	0
18	10	4	8	1
19	7	9	3	2
20	15	9	10	0
21	9	7	4	0
22	10	5	7	0
23	18	16	11	3
24	10	9	2	0
25	16	10	11	1
26	6	9	1	3

Table 12: Password reuse statistics. Participant 8 and 9 failed to accurately describe their password and account associations; consequently we were unable to present some of their information. Notice that although some of our participants had unassociated passwords, they still reused their passwords!

We were interested to find whether an insufficient number of passwords to cover increasingly large number of accounts was the only reason why our participants reused their passwords. From the total of 26 participants, 20 participants declared fewer numbers of passwords than accounts, 2 participants declared that they have the same number of accounts and passwords, while 4 indicated that they have more passwords than accounts. Interestingly, after analyzing our participants' data, we found that there are 11 participants who had unassociated passwords. Although there is a possibility that our participants might have not reported all of their accounts, this indicates that there are other reasons which influence their decisions whether to reuse passwords or not, rather than just an insufficient number of passwords.

5.3.3. Why Do People Reuse Passwords?

We now have a clear idea that most of our participants reused their passwords, although as we have discussed earlier, there are accounts on which our participants did not reuse their passwords. We are interested to investigate the reasons which influenced their decision to reuse their passwords for some accounts but not for other accounts (Question 8).

We asked our participants to choose a statement from a list of statements that we provided, which best represents the reason for their password usage practices (whether they reuse password or not) for each of their accounts (refer to section 4.2.2 for more details).

There were 336 accounts in total. 132 accounts were assigned unique passwords, while 204 were assigned reused passwords. Despite our instruction to only select the most suitable statement, there were 3 cases where multiple statements were selected, which contributed to the slight difference between our final count and total number of accounts. The frequency of how many times each statement selected by our participants is presented in Table 13 and Table 14 below.

Reasons cited for not reusing passwords	Frequency	Percentage
The information stored under this account is of high value/importance	38	28.4%
I try to avoid password reuse because I believe it is not secure	21	15.7%
The password was assigned by the account provider	18	13.4%
The account provider has password format restrictions, so I had to change my password to meet their restrictions	18	13.4%
I created a unique password to avoid confusion with my other account(s)	18	13.4%
Other (see appendix)	11	8.2%
I created a random password for this account	10	7.5%
Total	134	

Table 13: Reasons cited for not reusing passwords (sorted by frequency).

Reasons cited for reusing passwords	Frequency	Percentage
I reuse password for this account because it is easy to remember	72	35.1%
The information that is stored under this account is of similar value/importance to the information stored under the other account(s) which use the same password.	39	19%
This account belongs to the same category as the other account(s) which use the same password	38	18.5%
This account belongs to the same domain (leisure/work/family) as other account(s) which use the same password	27	13.2%
I use this account in the same frequency as the other account(s) which use the same password	16	7.8%
I have several passwords and I randomly assigned them to my accounts.	7	3.4%
I only have one password and I use it for all my accounts	3	1.5%
Other (see appendix)	3	1.5%
Total	205	

Table 14: Reasons cited for reusing passwords (sorted by frequency).

We found that there is no single reason to explain why people reused passwords on some accounts and not for the others, however, our results have shown that the highest proportion (28.4%) of the reasons cited for not reusing password is the value or importance of the accounts, followed by "I try to avoid password reuse because I believe it is not secure" (15.7%). This shows that our participants are aware that password reuse is not a secure practice which can put their valuable accounts at risk. Despite that, creating a new password for every single account would not be feasible for most people. This is most probably due to human memory limitations, as "I reuse password for this account because it is easy to remember" was the most popular reason cited (35.1%) to justify password reuse.

5.4. Account and Password Groupings

5.4.1. Similarities Used For Grouping

As we have discussed in Section 3.3., our main hypothesis was that people manage their accounts and passwords by mentally separating their accounts and passwords into several groups based on differing perceived similarities between their accounts and passwords. After thoroughly explaining our concepts of password and account grouping practices, we instructed our participants to complete a table to describe their password and account

groupings, and asked our participants to describe the reasons for grouping their accounts or passwords together for each password and account group that they created (refer to Section 4.2.2. for more details regarding our survey procedures). The results that we obtained indicated that all participants used some form of similarities to group their accounts, whereas all participants except one (Participant 5) grouped their passwords using some form of similarities. Further investigation indicates that Participant 5 only had 3 passwords, which is the smallest amount of passwords among all our participants

Most of our participants provided low level, and colloquial descriptions of the similarities used to group several accounts together, such as 'school stuff', 'e-mail accounts', 'online banking' and so on. We performed a bottom up analysis and classified these reasons into high level categories. During our analysis, we had to rely on our subjective interpretation at times, because we found some of the descriptions to be rather vague. Below are the classifications resulting from our analysis:

1. **Type of service (72%)**

   Grouping based on the types of service or usage associated with accounts, e.g. financial, communication, education, and so on.

2. **Risk (18.6 %)**

   Grouping based on the level of importance and risk of the information stored under the accounts, as well as the level of security measures assigned to the accounts.

3. **Frequency (5.2%)**

   Grouping based on frequency of usage of the accounts, where accounts with the same frequency of usage are grouped together.

4. **Alias (2.5%)**

   Grouping based on alias or login names associated with the accounts.

5. **Sharing (1.7%)**

   Grouping based on parties with which the account usage and credentials are shared, such as friends, work colleagues and family members.

There are 118 account groups for which explanations were provided by our participants. 85 (72%) account groups were based on similar 'Type of service', followed by 'Risk' contributed 22 account groups (18.6%). 6 account groups (5.2%), were created based on the similarity in the frequency of usage of the accounts, while 3 account groups (2.5%) were created based on the similarity of the login names (alias) used. One participant declared 2 account groups (1.7%) which were created based on different parties with which the accounts were shared. Table 15 below represents the distribution of each grouping classification as described by our participants.

Notice that all of our participants only used between 1 and 3 types of similarity, and in most cases there is one type of grouping which is used more frequently than the others, with the most popular (used by 8 participants out of 26) combination consisting of a large proportion of groups based on 'Type of Service' and a few groups based on 'Risk'.

Participant	Frequency	Alias	Risk	Type of Service	Sharing	Total
1		1		3		4
2			4			4
3				6		6
4			2	3		5
5				5		5
6			1	2		3
7						0
8				4		4
9	1					1
10		2				2
11			1	7		8
12			2	1		3
13	1			3		4
14			1	6		7
15				8		8
16			3	1		4
17			1	3	2	6
18	1		1	3		5
19				3		3
20	2			2		4
21			1	3		4
22				3		3
23			2	10		12
24			3			3
25				8		8
26	1			1		2
Total	**6**	**3**	**22**	**85**	**2**	**118**

Table 15: Distribution of types of similarity used for grouping accounts.

We repeated the same procedures as used for the account groupings, by performing bottom up analysis on the low level descriptions given by our participants. We faced the same problem during this procedure as with the account groups, that is, we had to rely on our subjective interpretation as most of the descriptions given are rather vague. Based on our findings, we created 6 categories to cover all the descriptions given by our participants.

1. **Semantic (44.4%)**

   Grouping based on similarities in semantic properties of the passwords, such as length, number of letters, number of words, permutation around similar phrases, pronunciation and so on.

2. **Perception of Security (12.5%)**

   Grouping based on users' perception of how secure the passwords are, where passwords that are considered to provide similar security levels are grouped together.

3. **Inspiration (15.3%)**

   Grouping based on the inspiration used to create passwords.

4. **Accounts (15.3%)**

   Grouping based on types or categories of accounts for which the passwords are used.

5. **Creation (6.9%)**

   Grouping based on who created the passwords, when and how the passwords were created, e.g. assigned by service providers during registration, created by own, and so on.

6. **Recallability (5.5%)**

   Grouping based on the ease of recall of passwords

Participant	Perception of Security	Semantic	Creation	Inspiration	Accounts	Recallability	Total
1		1			1		2
2		4					4
3		2	1				3
4		1		2			3
5							0
6		1	1	1			3
7						1	1
8				3	1		4
9				1	1	1	3
10				2			2
11	3				3		6
12	1				2		3
13		4					4
14						1	1
15		6					6
16		3					3
17		2					2
18				1			1
19		2				1	3
20		2					2
21		3					3
22							0
23	1						1
24			1		2		3
25	2	1	2				5
26	2			1	1		4
Total	**9**	**32**	**5**	**11**	**11**	**4**	**72**

Table 16: Distribution of types of similarity used for grouping passwords.

There are 72 account groups for which explanations were provided by our participants. We found that the most commonly used similarity used for grouping passwords is their semantic similarities, such as length, composition of numbers, symbols and letters, which contributed 32 password groups (44.4%) to our final count. 'Accounts' and 'Inspiration', contributed 11 password groups (15.3%) each to our final count. 5 password groups (17%) which fall under the 'Creation' category. 'Perception of Security' and 'Recallability' were among the least common similarities used, with only 9 groups (12.5%) and 4 groups (5.5%) respectively.

As we have discussed, these classifications of the similarities used to create account and password groups were formed based on our subjective assessment of the descriptions given by our participants. These results are thus inconclusive, as we believe that if the same analysis

was to be performed by others, the results would have been different. However, our findings have confirmed that our participants mentally classified their accounts and passwords in groups, based on the perceived similarities between their passwords and accounts.

5.4.2. Association between Account Groups and Password Groups

We have discussed different types of similarity on which our participants based their account and password groupings. We are interested to further investigate whether there is any association between the accounts and password groups. Non association would mean that the distribution of passwords from each password group would be more or less similar across every account group for each participant. This could only happen if our participants assigned their passwords to their accounts randomly without considering how they grouped their accounts and passwords.

	Account Group 1	**Account Group 2**	**Account Group 3**
Password Group 1	*A*	*B*	*C*
Password Group 2	*D*	*E*	*F*

Table 17: Illustration of the distribution of passwords and accounts distribution groups. The proportions of cells A-F would be more or less similar if our participants assigned their passwords to their accounts randomly without considering their account and password groupings.

We hypothesized that there would be an association between account and password groups, which we suspect to influence our participants' decision which determines which password should be assigned to which account(s).

In order to verify our hypothesis (H-9), we used Fisher-Freeman-Halton test (an extension of Fisher test for tables larger than 2x2) to test each participant's data. This test was chosen as an alternative of Chi-Square test, as our data does not meet the expected cell frequency and number of cases for Chi-Square test. We used StatXact version 4 to perform this analysis,

since Fisher-Freeman-Halton test was not available in SPSS version 14 that we used, unless an extension module is purchased.

Two participants (Participant 8 and 9 – consult Appendix C for more details) failed to describe the associations between their passwords and accounts according to our instructions, and consequently we were unable to extract the information needed to perform this analysis. One participant (Participant 18 – consult Appendix C for more details) only had one password group, which is unsuitable for Fisher-Freeman-Halton test, and thus was excluded from this analysis.

From the total of 23 cases, we obtained 15 (65%) statistically significant results (P-value ≤ 0.05) against the proportion of password groups being independent across different account groups. This outcome suggests that there is an association between account groups and password groups which affects the way in which our participants assign their passwords to their accounts.

5.4.3. High Importance Account Groups

In the previous section we discussed how our participants used groupings to manage their online accounts. We believe that most of our participants have at least one account group that is somehow considered of higher importance or more valuable than their other account groups. We are interested to investigate whether these account groups are managed differently from other account groups which are considered of less importance (Question 10).

Before any further investigation could be done, we first needed to separate the high importance account groups from the other, less important account groups. In our survey, we asked the participants to assign a 'value of importance' score to each of their accounts using 5 point Likert scale, with 1 being the least valuable and 5 being the most valuable, which

should give an indication of how valuable or important each account is according to our participants.

These scores were used to distinguish groups which are considered of high importance. From each participant, we selected the account group which has the highest average (arithmetic mean) of 'value of importance' scores among all their account groups. In cases where there are several groups having the same highest average score, all these groups were selected. Two participants (numbers 8 and 9 – consult appendix for more details) failed to describe the associations between their passwords and accounts according our instructions, making it impossible to extract the information needed to perform this analysis. Consequently, we decided not to include their responses in this analysis. As the result of our selection process, 37 account groups were selected as high importance account groups, while 93 unselected account groups were classified as low importance account groups.

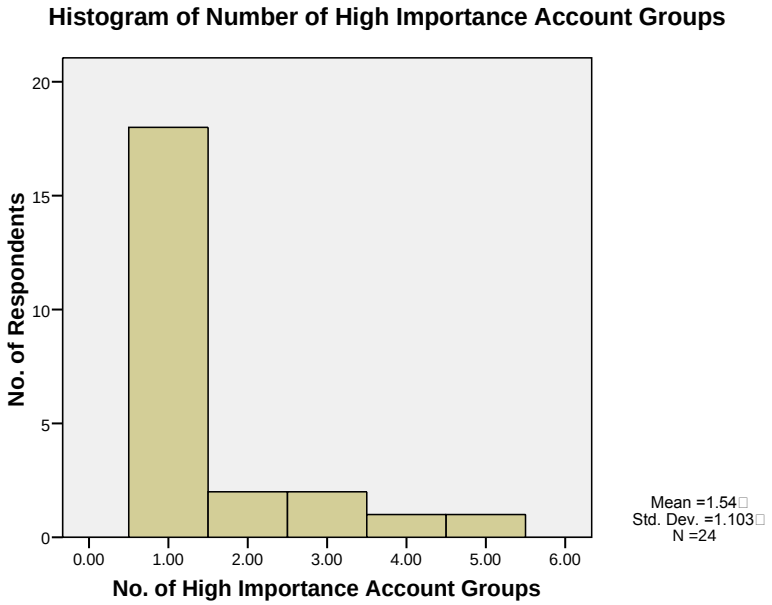


Figure 26: A histogram showing the distribution of high importance account groups per participant. Most of our participants only have one high importance account group, although there are some who have 2, 3, 4 and even 5 groups. On average, each person has 1.54 high importance account groups (N= 24, SD = 1.102)

The main differences that we found between high importance account groups and low importance account groups are:

1. **Size**

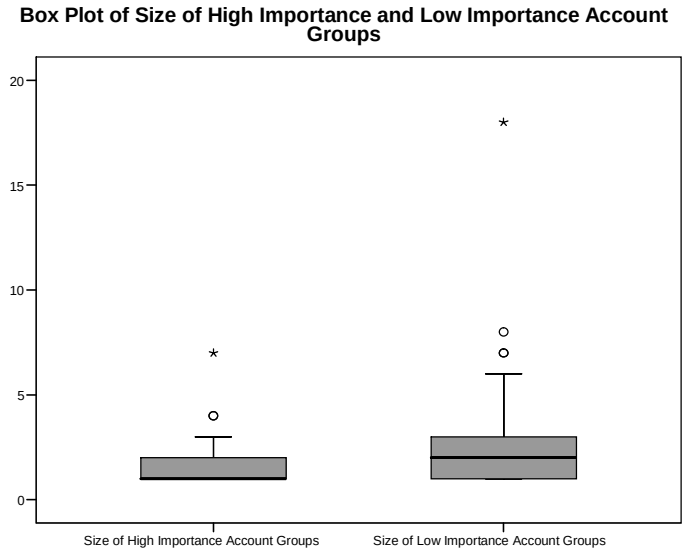


Figure 27: Box plot showing the differences in size of high importance account groups and low importance account groups.

We found high importance account groups to be of smaller size (in terms of number of accounts per group) on average (Mean = 1.84, SD = 1.28), compared to low importance account groups (Mean = 2.78, SD = 2.21).

2. **Password reuse behavior**

In total there are 68 accounts in our high importance account groups, 43 accounts were assigned passwords which have not been used for any other accounts, where 25 accounts were assigned passwords which have been used for other accounts. In contrast, there are total of 253 accounts in the low importance account groups, among which 171 were given passwords which have been used for other accounts, and only 82 were assigned unique passwords which have not been used for any other accounts.

Only 11 out of 24 participants (45%) reused their passwords on at least one account in their high importance account groups, whereas 23 out of 24 participants (96%) reused their passwords on at least one account in their low importance account groups.

Our analysis provided significant evidence that participants who reused their passwords on at least one account in their high importance account groups have on average larger number of accounts compared to participants who did not reuse passwords on their high importance account groups (P-value = 0.020). We estimated the difference to be somewhere between 1.07 and 11.28 accounts. We also have significant evidence that participants who reused passwords on at least one account in their high importance account groups have on average longer internet experience than participants who did not reuse passwords in their high importance account groups (P-value = 0.028). We estimated the difference to be somewhere between 0.28 and 4.4 years.

3. Perceptions of passwords used

Our findings indicated that 17 of 24 (70%) of our participants have passwords that are exclusively used for accounts in high importance groups, and each participant has on average 2.9 of these passwords (S.D. = 1.9).

Using Student's t-test, we obtained significant evidence that passwords which are used exclusively on important account groups were considered to have significantly higher perceived security level (P-value = 0.017) and ranked as more difficult to recall (P-value = 0.02) compared to passwords which are used on less important account groups. Details on how perceived security level and difficulty of recall are measured have been discussed in Section 5.2.

We collected the descriptions that were given by our participants to describe their high importance account groups. It came as no surprise that the highest number of high importance account groups were described as financially related. The descriptions along with their respective frequencies are presented in the table below:

Descriptions	Frequency
Financial, banking, online trading accounts.	8
No reason or ambiguous description given.	7
Indicated that the accounts were of high value, importance or security level, but did not specify the actual type of information.	5
University related.	4
E-mail accounts.	3
Sites that require special passwords.	3
Computer login accounts.	2
Accounts which are shared with friends or family members.	1
Health related accounts.	1
Digital signing/encryption.	1
Accounts that are grouped based on a login name.	1
Accounts that are used on a daily basis.	1

Table 18: Descriptions of account groups which are considered of high importance.

Our findings have shown that our participants have account groups which are considered more important than the others, and are managed differently. Compared to the other, less important account groups, these account groups tend to have reasonably less number of accounts. We also found that password reuse occurrences are significantly less in these groups. Furthermore, passwords which are used on accounts in these groups are perceived to be more secure and harder to recall.

5.5. Compliance with University of Auckland Regulations

Every student and staff member at The University of Auckland has a password which is used to access university ICT facilities, such as e-mail, library services, online enrolment system, computer login within the university network, and so on. At the time of this writing, the authentication system at our university uses a *Single Sign-On* mechanism, which allows the same password to be used across different university services (see provider centric identity

management approach in Section 2.2.4). The usage of this system is governed by University of Auckland's Account and Password Management Policy [103]. This well-advertised policy forbids students and staff to divulge and reuse their university passwords.

During our data analysis, we found that several participants described some of their account groups as being "university related". These findings raised our interest to further investigate what percentage of these participants complied with the university IT policy which prohibits password reuse (Question 11).

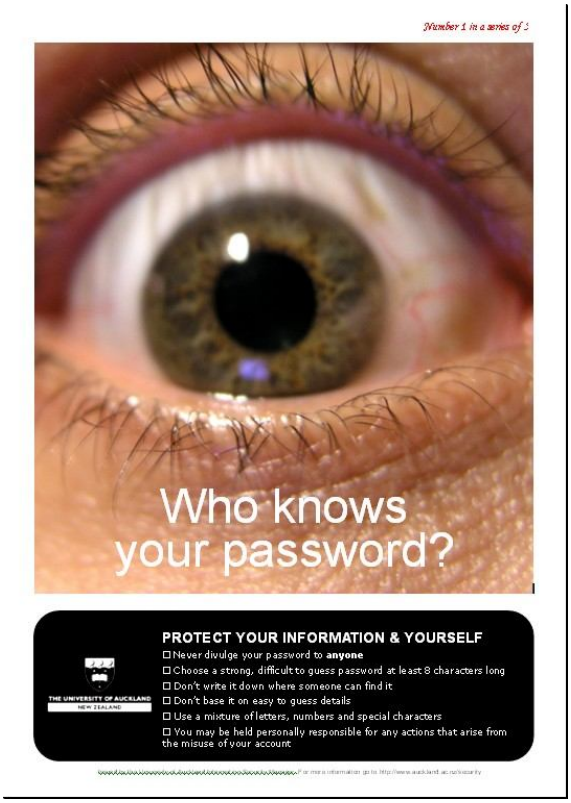


Figure 28: Who knows your password? Part of a series of posters published by The University of Auckland Information Security Management Team to promote safe IT practices in 2006.

Among 8 participants who described one of their account groups as being university related, 5 participants (62%) did not comply with the university policy, i.e. they reused their university password on at least one other accounts, while only 3 participants (38%) complied

with the regulations. We discovered that in the most extreme case, a participant indicated that he reused his university password on 23 other accounts.

We were unable to present further reliable statistics on this subject from the data we obtained, because our survey was initially designed with no intention to collect any information regarding university password usage. Nevertheless, this outcome indicates that regardless of strong warning and publication efforts the compliance rate may well be low.

In the next chapter, we summarize and compare our findings to the findings from previous user studies on password authentication that we have discussed in Section 3.2. We also discuss the implications of our findings, and suggest future directions.

"A conclusion is the place where you got tired of thinking." –Harold Fricklestein

6
Conclusion

In this thesis, we investigated how people's perceptions of their accounts and passwords influence their password selection. In Chapter 1, we outlined the concept of identity and authentication process in modern computer systems. We discussed the way digital identity is viewed from both service providers' and users' perspectives which resemble Leibniz' and Erikson's identity concepts respectively. We also outlined the concept of digital persona, which helped us to organize our investigation.

In Chapter 2, we discussed various issues with password authentication. We started by describing a variety of known attacks, which we classify into three categories: attacks to the system end, attacks to the communication channel and attacks to the user. Among these three categories, attacks to the user are the most alarming, as they commonly require minimal level of technical knowledge to perform, and yet have a relatively large chance of success. We discussed users' tendency to adopt insecure password practices which have been cited in various literatures, such as writing passwords down in obvious locations, creating

extremely weak passwords and reusing passwords on multiple accounts. Reusing password across multiple accounts is generally considered a bad practice, because if one of users' passwords is compromised, then all their accounts that share the same password will also be at risk. We showed how password reuse can be exploited by an attacker in new-account scenario, known as *malicious server attack*.

We discussed various identity management solutions which attempt to address users' insecure practices. These solutions are commonly developed under the assumption that decreasing the amount of passwords and associations that have to be managed would reduce users' memory strain, leading to a decrease in the prevalence of password reuse and other insecure practices. Nevertheless, as we discussed in Section 2.2.4, these solutions are not are not free from their own problems and drawbacks.

In Chapter 3, we described the motivation of our study. We believe that before we could review existing solutions, or work towards a more appropriate solution to address password reuse and other insecure password practices, it would be necessary to study the underlying cause of these insecure practices, which we believe lies within users' perceptions of their accounts and passwords. We reviewed ten user studies that have been published in literatures. We also described how we used the concept of digital persona as an organizing idea for our survey based study.

In Chapter 4, we discussed our ethical concerns and considerations which influenced the design of our survey methodology. We also described our survey procedures in details. In Chapter 5, we presented our data analysis which led to our findings.

The remainder of this chapter is divided into three sections. Section 6.1 summarizes and compares our findings with the findings from previous user studies on password

authentication that we have discussed in Section 3.2. Section 6.2 discusses the implications of our findings, while Section 6.3 suggests future directions beyond this thesis.

6.1. Summary and Comparison of Our Findings

Before we proceed further, we would like to remind our readers that our results must be interpreted with extreme care. As we have described in Section 4.2 and Section 5.1, our participants were all university students, hence our results might not be the best representation of the general user population.

We found no difference in the numbers of passwords, accounts, account groups and password groups between participants who were studying IT related qualifications and those who were studying for non IT related qualifications, despite the likelihood that participants who were studying for IT related qualifications would have had more exposure to computers and knowledge of computer security issues (Section 5.1.2). This to some extent supports earlier findings from Dhamija and Perrig (Section 3.2.4) and Riley et al (Section 3.2.8) that level of security knowledge does not have any impact on password practices. We also discovered that gender does not have any effect on these variables.

Unlike previous studies conducted by Morris and Thompson (Section 3.2.1), Riddle et al (Section 3.2.2), Brown et al (Section 3.2.6), Florencio and Herley (Section 3.2.10) which analyzed the strength of users' passwords by measuring their entropy, we took a different approach by investigating users' perspectives of their own passwords. Our findings suggest that according to our participant's perceptions, the more secure a password is, the more difficult to recall it becomes, and vice versa (Section 5.2).

We discovered that number of accounts maintained by our participants seems to increase as they gain more internet experience, while number of passwords does not (Section 5.3.1). We also found that our participants seem to reuse more passwords as they accumulate more

accounts (Section 5.3.2). These findings corroborate Gaw and Felten's (Section 3.2.9) earlier findings. However, unlike Gaw and Felten who quantified password reuse as a ratio of number of online accounts per unique passwords, we measured password reuse occurrences as explicitly reported by our participants.

The most frequent reason cited by our participants to justify password reuse is "I reuse password for this account because it is easy to remember" (35.1%) (Section 5.3.3). This confirms earlier findings from Adams and Sasse's (Section 3.2.3) and Gaw and Felten's (Section 3.2.9) earlier studies, that human memory limitations were the main reason why people reuse their passwords. This is followed "The information that is stored under this account is of similar value/importance to the information stored under the other account(s) which use the same password", which was cited 18.5% of the time – this shows that our participants took their account classifications into consideration when reusing passwords. The most frequent reason cited for not reusing passwords is "The information stored under this account is of high value/importance" (28.4%), followed by "I try to avoid password reuse because I believe it is not secure" (15.7%), which also agrees with Gaw and Felten's and Florencio and Herley's() findings that we have discussed earlier in Sections 3.2.9 and 3.2.10 respectively.

In accordance to our hypothesis in Section 3.3, our findings show that all our participants used some form of similarity for grouping their accounts (Section 5.4.1). We categorized the similarities used by our participants to classify their accounts into the following:

1. **Type of service (72%)**
   Grouping based on the types of service or usage associated with accounts, e.g. financial, communication, education, and so on.

2. **Risk (18.6 %)**

   Grouping based on the level of importance and risk of the information stored under the accounts, as well as the level of security measures assigned to the accounts.

3. **Frequency (5.2%)**

   Grouping based on frequency of usage of the accounts, where accounts with the same frequency of usage are grouped together.

4. **Alias (2.5%)**

   Grouping based on alias or login names associated with the accounts.

5. **Sharing (1.7%)**

   Grouping based on parties with which the account usage and credentials are shared, such as friends, work colleagues and family members.

All of our participants except one also indicated that they classify their passwords based on various similarities. We categorized the similarities used by our participants to classify their accounts into the following:

1. **Semantic (44.4%)**

   Grouping based on similarities in semantic properties of the passwords, such as length, number of letters, number of words, permutation around similar phrases, pronunciation and so on.

2. **Perception of Security (12.5%)**

   Grouping based on users' perception of how secure the passwords are, where passwords that are considered to provide similar security levels are grouped together.

3. **Inspiration (15.3%)**

   Grouping based on the inspiration used to create passwords.

4. **Accounts (15.3%)**

   Grouping based on types or categories of accounts for which the passwords are used.

5. **Creation (6.9%)**

   Grouping based on who created the passwords, when and how the passwords were created, e.g. assigned by service providers during registration, created by own, and so on.

6. **Recallability (5.5%)**

   Grouping based on the ease of recall of passwords.

We further discovered that our participants have account groups which are considered more important than the others, and are managed differently.differently from their other account groups which are considered of less importance (Section 5.4.3). Compared to the other, less important account groups, these account groups tend to have less number of accounts. We also found that our participants do not reuse their passwords as often on the accounts in their important groups. Furthermore, passwords which are used on accounts in these groups are perceived to be more secure and harder to recall. This, again, supports the findings from earlier studies by Gaw and Felten and Florencio and Herley that we have discussed in Sections 3.2.9 and 3.2.10 respectively.

Among 8 participants who described one of their account groups as being 'university related', 5 participants (62%) did not comply with the well-advertised university policy, which prohibits students and staff to reuse their university passwords on any other accounts. while only 3 participants (38%) complied with the regulations. We discovered that in the most extreme case, a participant indicated that he reused his university password on 23 other

accounts. These findings corroborate Riddle et al.'s findings (Section 3.2.2) that despite well advertised suggestions for creating strong passwords, weak passwords were still prevalent at their university's computer system and Yan et al's findings (Section 3.2.7) which still indicated non-compliance among their participants, regardless of the explicit instructions given.

6.2. Implications of Our Findings

The concept of digital persona is clearly manifested in the way our participants classified their accounts and passwords using differing perceived similarities between their accounts and passwords. Using this concept as an organizing idea for our exploratory study allowed us to view password management problems from users' perspectives and learn how our participants' perceptions of their passwords and accounts influence the way in which they assign passwords to their accounts.

We discovered that regardless of various similarities they use to classify their accounts, our participants tend to use passwords which they perceive to be stronger and did not reuse passwords as often in account groups which they considered more important than their other account groups. In real world scenario, people often put their valuable possessions in safe, inconvenient places, such as in safety deposit boxes. They are willing to go through the inconvenience because they understand the value of the possessions that they are trying to protect, and are aware of the risks associated with leaving their valuable possessions in easily accessible, obvious places. Our findings suggest that our participants have the same sense of security awareness, and understand that reusing passwords or using weak passwords on their important accounts could put their important information at risk. We believe that the underlying reason for users' insecure password practices is their failure to identify the importance of their accounts, and that any projects which attempt to solve poor password practices should focus on educating users to identify the importance of their accounts accordingly.

Can users be prevented from reusing passwords? Or more appropriately, do users need to be prevented from reusing passwords? Given the rapid increase in the number of online services which require authorization, it is very unlikely that password reuse can be prevented in foreseeable future. Drawing from our findings, we would like to propose a rather provocative suggestion: reusing passwords on unimportant accounts which contain no sensitive information should not be discouraged, as it will only increase users' memory burden. Expecting users to create unique, strong passwords for all their accounts is just as unreasonable as expecting someone to place all his/her possessions in a safe deposit box. Instead, users should be educated to identify which accounts they should not reuse passwords on.

By using passwords which they perceived to be more 'secure' on accounts that they considered important, our participants demonstrated their awareness of the importance of using strong passwords to protect their valuable information. As we did not measure the entropy strength of our participant's passwords, we are unable to make any assessment on the actual strength of their passwords. However, previous studies by Adams and Sasse (Section 3.2.3) and Gaw and Felten (Section 3.2.9) have shown that most users lack the knowledge of what attackers are capable of – they tend to picture attacks as human adversaries who try to guess their passwords by hand, and still think of password cracking and other attacks as 'myths'. Thus 'secure' passwords are often viewed as passwords which are not easily guessable or commonly used by humans. We believe that users still need to be educated about how various attacks on password authentication work to promote better knowledge and understanding of what comprises strong password contents.

Rather than enforcing blind instructions to avoid password reuse and create strong passwords, it would be more appropriate for service providers (particularly whose services deal with sensitive information, or in situations where a user's negligence can jeopardize

other users) to remind their users about the importance of the information stored on their accounts and how reusing passwords or using weak passwords on these accounts can put their important information at risk. Users also need to be informed about the potential damages and consequences which may result if their accounts are compromised. This way, users can be encouraged to adopt appropriate practices out of their own motivation, rather than mere obligation.

6.3. Future Directions

Due to time and resource constraints, we decided to limit our sample population to the student body within the University of Auckland. A possible avenue for future research is to verify the findings from our exploratory study by extending the sample population to include participants from a wider range of background. With further investigation and analysis, we also foresee that it would be possible to organize the development of an individual's digital identity into several stages similar to Erikson's identity development theory (Section 1.1 and Table 1).

We found no evidence that the variation in the number of passwords is related to the differences in computing and internet experience (Section 5.3.1). We suspect that this result might be attributed to the fact all of our participants had four years or more of computing and internet experience. A possible future direction beyond this research is to investigate how people's earlier years of experience contribute to the development of their passwords.

Our survey design could also benefit from further refinements. For instance, a high proportion of our survey was deliberately left open ended, as we intended to explore how our participants would describe the similarities between their passwords and accounts. However, this resulted in colloquial and vague descriptions which we later found difficult to analyze (see Section 5.4.1). For future studies, our findings could be used to provide more concise and structured choices to obtain crisper analysis.

The belief that 'secure' passwords are difficult to memorize may be the main cause why people often resort to weak passwords to avoid memory strain. However, strong passwords do not necessarily have to be difficult to recall. Findings from Yan et al's study (Section 3.2.7), which is corroborated by a more recent study by Kuo et al [152] suggest that the usage of mnemonic sentences enables the creation of reasonably strong, yet memorable passwords. Recently, Topkara et al [153] suggested an extension to the promising potential of mnemonic sentences by proposing a password creation scheme which generates multiple memorable passwords from a given mnemonic sentence. However, our review of the literature suggests that this prospect has not yet been thoroughly explored, and still warrants future research.

It is possible to extend our findings to design intuitive and user friendly identity management solutions which allow people to classify their accounts and passwords based on various perceived similarities. We also believe that our findings could be of assistance to system administrators and policy makers alike, who are seeking to refine their password usage policies and guidelines.

Lastly, we believe that the discussion regarding our ethical concerns and how they influenced the design of our survey methodology (See Section 4.1 and 4.2) could be of help to researchers who are considering to conduct human participation studies which involves sensitive and confidential information in the future.

THIS PAGE IS INTENTIONALLY LEFT BLANK

References

[1] T. F. Hoad, "The Concise Oxford Dictionary of English Etymology ", Oxford University Press, 1986.

[2] C. T. Lewis, *A Latin Dictionary for Schools*, London: Oxford University Press, 1889.

[3] C. Soanes, and A. Stevenson, "identity noun," *The Oxford Dictionary of English (revised edition)*, Oxford University Press, 2005.

[4] P. Forrest, "The Identity of Indiscernibles," *The Stanford Encyclopedia of Philosophy.* The Metaphysics Research Lab, Center for the Study of Language and Information, Stanford University, 1996. [Online]. Available: http://plato.stanford.edu/entries/identity-indiscernible/. [Accessed July 10, 2007].

[5] G. W. F. v. Leibniz, *The Monadology and Other Philosophical Writings; translated with introduction and notes by Robert Latta.*, 2 ed., London: Oxford University Press, 1925.

[6] A. Savile, *Routledge Philosophy Guidebook to Leibniz and the Monadology*, London: Routledge, 2000.

[7] C. Thomborson, "Personal e-mail communication," Jun 24, 2007.

[8] E. H. Erikson, *Identity: Youth and Crisis*, New York: W.W. Norton & Company, 1968.

[9] E. H. Erikson, *Identity and the Life Cycle*, New York: Norton, 1980.

[10] National Research Council, *Computers at Risk: Safe Computing in the Information Age*, National Academies Press, 1990. [Online]. Available: http://site.ebrary.com.ezproxy.auckland.ac.nz/lib/auckland/Top?id=10056738&layout=document. [Accessed July 10, 2007].

[11] B. W. Lampson, “Computer Security in the Real World,” *IEEE Computer,* vol. 37, no. 6, pp. 37 - 46 June 2004.

[12] Committee on National Security Systems, "National Information Assurance Glossary," *CNSS Instruction No. 4009.* [Online]. Available: www.cnss.gov/Assets/pdf/cnssi_4009.pdf. [Accessed June, 2006].

[13] R. Clarke, “Human Identification in Information Systems:Management Challenges and Public Policy Issues,” *Information Technology & People,* vol. 7, no. 4, pp. 6-37, December 1994.

[14] L. O'Gorman, “Comparing Passwords, Tokens, and Biometrics for User Authentication,” *Proceedings of the IEEE* vol. 91 no. 12, pp. 2019 - 2020, Dec 2003.

[15] C. P. Pfleeger, and S. L. Pfleeger, *Security in Computing*, New Jersey: Prentice Hall Professional Technical Reference, 2003.

[16] A. Adams, and M. A. Sasse, “Users are not the enemy,” *Communications of the ACM,* vol. 42, no. 12, pp. 40-46, December 1999.

[17] H. Berghel, “ Phishing mongers and posers ” *Communications of the ACM,* vol. 49 no. 4, pp. 21-25, 2006.

[18] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in *Proceedings of the SIGCHI conference on Human Factors in computing systems*, Montreal, Quebec, Canada, 2006, pp. 581-590.

[19] A. K. Jain, "Biometric recognition: how do I know who you are?," in *The IEEE 12th Signal Processing and Communications Applications Conference,* 2004.

[20] S. Prabakhar, S. Pankanti, and A. K. Jain, “Biometric Recognition: Security and Privacy Concerns,” *IEEE Security & Privacy Magazine,* vol. 1, no. 2, pp. 33 - 42, Mar-Apr 2003.

[21] A. Bhargav-Spantzel, A. Squicciarini, and E. Bertino, "Privacy preserving multi-factor authentication with biometrics," in *The second ACM workshop on Digital identity management* Alexandria, Virginia, USA 2006, pp. 63-72.

[22] M. Rejman-Greene, “Biometrics — Real Identities for a Virtual World,” *BT Technology Journal,* vol. 19, no. 3, July 2001.

[23] "persona n.," *The Concise Oxford English Dictionary, Eleventh edition revised*, C. Soanes and A. Stevenson, eds., Oxford University Press, 2006.

[24] C. G. Jung, *Two essays on analytical psychology / Translated by R.F.C. Hull*, London: Routledge & K. Paul, 1953.

[25] B. Plimmer, and R. Amor, "Peer teaching extends HCI learning," in Proceedings of the 11th annual SIGCSE conference on Innovation and technology in computer science education, Bologna, Italy, 2006.

[26] L. Shyba, and J. Tam, "Developing character personas and scenarios: vital steps in theatrical performance and HCI goal-directed design," in Proceedings of the 5th conference on Creativity \& cognition, London, United Kingdom, 2005.

[27] P. T. A. Junior, and L. V. L. Filgueiras, "User modeling with personas," in Proceedings of the 2005 Latin American conference on Human-computer interaction, Cuernavaca, Mexico, 2005.

[28] A. Dix, J. Finlay, G. Abowd *et al.*, *Human-computer interaction*: Prentice-Hall, Inc., 1997.

[29] E. Andre, J. Muller, and T. Rist, "The PPP persona: a multipurpose animated presentation agent," in Proceedings of the workshop on Advanced visual interfaces, Gubbio, Italy, 1996.

[30] J. C. Lester, S. A. Converse, S. E. Kahler *et al.*, "The persona effect: affective impact of animated pedagogical agents," in Proceedings of the SIGCHI conference on Human factors in computing systems, Atlanta, Georgia, United States, 1997.

[31] S. Erin, W. L. Johnson, and G. Rajaram, "Pedagogical agents on the Web," in Proceedings of the third annual conference on Autonomous Agents, Seattle, Washington, United States, 1999.

[32] A. Paiva, I. Machado, and R. Prada, "Heroes, villians, magicians, \…: dramatis personae in a virtual story creation environment," in Proceedings of the 6th international conference on Intelligent user interfaces, Santa Fe, New Mexico, United States, 2001.

[33] R. Clarke, "The Digital Persona and Its Application to Data Surveillance," *The Information Society,* vol. 10, no. 2, pp. 77-92, June 1994.

[34] J. Li, “A Fifth Generation Messaging System,” MSc Thesis, Computer Science Department, The University of Auckland, 2002.

[35] M. Mutu-Grigg, “Examining Fifth Generation Messaging Systems,” Project Report, Computer Science Department, The University of Auckland, 2003.

[36] D. Leung, “Persona Support and Management in Operating Systems,” Project Report, Faculty of Science, The University of Auckland, 2007.

[37] T. Baier, and C. P. Kunze, “Identity Management for Self-Portrayal,” *Information Security Management, Education and Privacy*, pp. 231-244, 2004.

[38] J. Suler, “Identity Management in Cyberspace,” *Journal of Applied Psychoanalytic Studies,* vol. 4, pp. 455-460, 2002.

[39] J. Suler, "Integrating Online and Offline Living," *The Psychology of Cyberspace* January 2000. [Online]. Available: http://www.rider.edu/~suler/psycyber/integrate.html. [Accessed July 10, 2007].

[40] Microsoft Corporation, "Secret Societies," *Microsoft® Encarta® Online Encyclopedia* [Online]. Available: http://uk.encarta.msn.com/. [Accessed December 02, 2006].

[41] Y. Ding, and P. Horster, “Undetectable on-line password guessing attacks ” *ACM SIGOPS Operating Systems Review* vol. 29, no. 4, pp. 77-86, 1995.

[42] S. Halevi, and H. Krawczyk, "Public-key cryptography and password protocols " in *Proceedings of the 5th ACM conference on Computer and communications security*, San Francisco, California, United States 1998 pp. 122-131

[43] B. Pinkas, and T. Sander, "Securing passwords against dictionary attacks " in *Proceedings of the 9th ACM conference on Computer and communications security* Washington, DC, USA 2002 pp. 161-170

[44] R. Morris, and K. Thompson, “Password security: a case history,” *Communications of the ACM,* vol. 22, no. 11, pp. 594-597, 1979.

[45] Z. Shuanglei, "Project RainbowCrack," October 26, 2005. [Online]. Available: http://www.antsight.com/zsl/rainbowcrack/. [Accessed July 10, 2007].

[46] Objectif Sécurité, "ophcrack," June 28, 2007. [Online]. Available: http://ophcrack.sourceforge.net/. [Accessed July 10, 2007].

[47] P. Oechslin, “Making a Faster Cryptanalytic Time-Memory Trade-Off,” *Advances in Cryptology - CRYPTO 2003,* vol. 2729, 2003.

[48] Openwall Project, "John the Ripper," undated. [Online]. Available: http://www.openwall.com/john/. [Accessed July 10, 2007].

[49] A. Muffett, "Crack Password Cracker FAQ," Feb 21, 2003. [Online]. Available: http://www.crypticide.com/users/alecm/security/c50-faq.html. [Accessed July 10, 2007].

[50] Google Inc., "Google Accounts," 2007. [Online]. Available: https://www.google.com/accounts/Login?continue=http://www.google.co.nz/&hl=en. [Accessed July 10, 2007].

[51] Yahoo! Inc., "Sign in to Yahoo! ," 2007. [Online]. Available: [Accessed July 10, 2007].

[52] Microsoft Corporation, "Sign in to MSN.com," undated. [Online]. Available: http://login.live.com/login.srf?wa=wsignin1.0&rpsnv=10&ct=1181631501&rver=4.0.1534.0&wp=LBI&wreply=http:%2F%2Fwww.msn.com%2F&lc=1033&id=1184. [Accessed July 10, 2007].

[53] L. Gong, M. A. Lomas, R. M. Needham *et al.*, “Protecting poorly chosen secrets from guessing attacks,” *IEEE Journal on Selected Areas in Communications,* vol. 11, no. 5, pp. 648-656, June 1993.

[54] H. Berghel, “Hijacking the Web,” *Communications of the ACM,* vol. 45, no. 4, pp. 23-27, April 2002.

[55] K. Fu, E. Sit, K. Smith *et al.*, "Dos and Don'ts of Client Authentication on the Web (2001) " in *The 10th USENIX Security Symposium*, Washington, D.C., 2001, pp. 251–268.

[56] D. Yu, A. Chander, N. Islam *et al.*, "JavaScript instrumentation for browser security " in *The 34th annual ACM SIGPLAN-SIGACT symposium on Principles of programming languages* Nice, France 2007 pp. 237-249

[57] G. A. D. Lucca, A. R. Fasolino, M. Mastoianni *et al.*, " Identifying cross site scripting vulnerabilities in Web applications," in *Sixth IEEE International Workshop on Web Site Evolution, 2004 (WSE 2004)*, 2004, pp. 71-80.

[58] H. Xia, "Hardening Web browsers against man-in-the-middle and eavesdropping attacks " in *Proceedings of the 14th international conference on World Wide Web* Chiba, Japan 2005 pp. 489-498.

[59] Ethereal, Inc., "Ethereal The world's most popular network protocol analyzer " March 01, 2007. [Online]. Available: http://www.ethereal.com/. [Accessed July 10, 2007].

[60] tcpdump, "TCPDUMP Public Repository," June 14, 2007. [Online]. Available: http://www.tcpdump.org/. [Accessed July 10, 2007].

[61] F. Fuentes, and D. C. Kar, "Ethereal vs. Tcpdump: a comparative study on packet sniffing tools for educational purpose " *Journal of Computing Sciences in Colleges* vol. 20, no. 4, pp. 169-176, 2005.

[62] U. Lamping, R. Sharpe, and E. Warnicke, "Ethereal User's Guide," 2005. [Online]. Available: http://www.ethereal.com/docs/eug_html/. [Accessed July 10, 2007].

[63] D. Song, "dsniff," undated. [Online]. Available: http://www.monkey.org/~dugsong/dsniff/. [Accessed July 10, 2007].

[64] The Shmoo Group, "Airsnarf - A rogue AP setup utility," undated. [Online]. Available: http://airsnarf.shmoo.com/. [Accessed July 10, 2007].

[65] A. O. Freier, P. Karlton, and P. C. Kocher, "The SSL Protocol Version 3.0," *Transport Layer Security Working Group.* November 18, 1996. [Online]. Available: http://wp.netscape.com/eng/ssl3/draft302.txt. [Accessed July 10, 2007].

[66] T. Dierks, and E. Rescorla, *RFC 4346: The Transport Layer Security (TLS) Protocol Version 1.1*, The Internet Society, 2006. [Online]. Available: http://tools.ietf.org/html/rfc4346. [Accessed July 10, 2007].

[67] K. D. Mitnick, and W. L. Simon, *The Art of Deception: Controlling the Human Element of Security*, New York: John Wiley & Sons, Inc, 2002.

[68] T. Thornburgh, "Social engineering: the "Dark Art"," in Proceedings of the 1st annual conference on Information security curriculum development, Kennesaw, Georgia, 2004.

[69] G. L. Orgill, G. W. Romney, M. G. Bailey *et al.*, "The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems,"

in Proceedings of the 5th conference on Information technology education, Salt Lake City, UT, USA, 2004.

[70] S. Wiedenbeck, J. Waters, L. Sobrado *et al.*, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in Proceedings of the working conference on Advanced visual interfaces, Venezia, Italy, 2006.

[71] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," in Proceedings of the 11th ACM conference on Computer and communications security, Washington DC, USA, 2004.

[72] S. L. Garfinkel, "Design Principles and Patterns for Computer Systems That Are Simultaneously Secure and Usable," PhD Thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA, 2005.

[73] J. Becker, "Computer crime career of the future?," *SIGCAS Comput. Soc.,* vol. 12, no. 1, pp. 12-15, 1982.

[74] M. Gregg, *Hack the Stack: Using Snort and Ethereal to Master the 8 Layers of an Insecure Network*: Syngress, 2006.

[75] T. Spring, "Hard Drives Exposed," *PC World.* April 03, 2003. [Online]. Available: http://www.pcworld.com/article/id,110012-page,1/article.html. [Accessed July 10, 2007].

[76] The Anti-Phishing Working Group, "What is Phishing and Pharming?," undated. [Online]. Available: http://www.antiphishing.org/. [Accessed June 12, 2007].

[77] H. Berghel, "Phishing mongers and posers " *Communications of the ACM,* vol. 49 no. 4, pp. 21-25, 2006.

[78] M. Jakobsson, "Modeling and Preventing Phishing Attacks," *Phishing Panel of Financial Cryptography*, 2005.

[79] The Anti-Phishing Working Group, "Origins of the Word 'Phishing'," undated. [Online]. Available: http://www.antiphishing.org/word_phish.html. [Accessed July 10, 2007].

[80] M. Jakobsson, and J. Ratkiewicz, "Designing ethical phishing experiments: a study of (ROT13) rOnl query features," in *Proceedings of the 15th international conference on World Wide Web* Edinburgh, Scotland 2006 pp. 513-522

[81] K. Chellapilla, and A. Maykov, “A taxonomy of JavaScript redirection spam,” in Proceedings of the 3rd international workshop on Adversarial information retrieval on the web, Banff, Alberta, Canada, 2007.

[82] Gartner, Inc., "Gartner Says Number of Phishing E-Mails Sent to U.S. Adults Nearly Doubles in Just Two Years," November 9, 2006. [Online]. Available: http://www.gartner.com/it/page.jsp?id=498245. [Accessed May 28, 2007].

[83] *Phishing Activity Trends Report for the Month of April, 2007*, Anti-Phishing Working Group, 2007.

[84] H. Berghel, J. Carpinter, and J.-Y. Jo, "Phish Phactors: Offensive and Defensive Strategies," 2006.

[85] P. Madsen, Y. Koga, and K. Takahashi, "Federated identity management for protecting users from ID theft " in *Proceedings of the 2005 workshop on Digital identity management* Fairfax, VA, USA 2005 pp. 77-83.

[86] S. Stamm, Z. Ramzan, and M. Jakobsson, "Technical Report TR641:Drive-By Pharming," Indiana University Department of Computer Science, 2006.

[87] A. Tsow, M. Jakobsson, L. Yang *et al.*, “Warkitting: The Drive-by Subversion of Wireless Home Routers,” *Journal of Digital Forensic Practice,* vol. 1, no. 3, pp. 179-192, 2006.

[88] K. McDowell, “Now that we are all so well-educated about spyware, can we put the bad guys out of business?,” in Proceedings of the 34th annual ACM SIGUCCS conference on User services, Edmonton, Alberta, Canada, 2006.

[89] S. Gaw, and E. W. Felten, "Password management strategies for online accounts " in *The second symposium on Usable privacy and security* Pittsburgh, Pennsylvania 2006, pp. 44-55.

[90] D. Weirich, and M. A. Sasse, “Pretty good persuasion: a first step towards effective password security in the real world,” in Proceedings of the 2001 workshop on New security paradigms, Cloudcroft, New Mexico, 2001.

[91] K. Poulsen, "Mitnick to Lawmakers: People, Phones are Weakest Links," March 2, 2000 [Online]. Available: http://seclists.org/politech/2000/Mar/0005.html. [Accessed July 10, 2007].

[92] B. F. Barton, and M. S. Barton, “User-friendly password methods for computer-mediated information systems,” *Computer Security,* vol. 3, no. 3, pp. 186-195, 1984.

[93] R. Dhamija, and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in *The 9th USENIX Security Symposium*, Denver, Colorado, 2000.

[94] A. Horowitz, "Top 10 Security Mistakes," *Computerworld.* July 09, 2001 [Online]. Available: http://www.computerworld.com/securitytopics/security/story/0,10801,61986,00.html. [Accessed June 13, 2007].

[95] CentralNic, "Password Clues," *The CentralNic Password Survey Report.* June 2001. [Online]. Available: http://www.centralnic.com/news/research. [Accessed December 5, 2006].

[96] A. S. Brown, E. Bracken, S. Zoccoli *et al.*, “Generating and Remembering Passwords,” *Applied Cognitive Psychology,* vol. 18, no. 6, pp. 641-651, September 2004.

[97] B. L. Riddle, M. S. Miron, and J. A. Semo, “Passwords in use in a university timesharing environment,” *Comput. Secur.,* vol. 8, no. 7, pp. 569-578, 1989.

[98] M. A. Sasse, S. Brostoff, and D. Weirich, “Transforming the 'Weakest Link' — a Human Computer Interaction Approach to Usable and Effective Security,” *BT Technology Journal,* vol. 19, no. 3, pp. 122-131, 2001.

[99] M. G. Gouda, A. X. Liu, L. M. Leung *et al.*, "Single Password, Multiple Accounts," in *3rd Applied Cryptography and Network Security Conference (industry track)*, New York City, New York, 2005.

[100] H. Luo, and P. Henry, "A common password method for protection of multiple accounts," in *14th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, 2003, pp. 2749 - 2754.

[101] B. Ives, K. R. Walsh, and H. Schneider, “The domino effect of password reuse,” *Commun. ACM,* vol. 47, no. 4, pp. 75-78, 2004.

[102] D. Crawford, “Forum,” *Commun. ACM,* vol. 47, no. 6, pp. 11-13, 2004.

[103] S. Taylor, *Account and Password Management Policy Version 1.6*, The University of Auckland, November 2006. [Online]. Available:

http://www.auckland.ac.nz/security/AccountAndPasswordManagementPolicy.htm. [Accessed July 10, 2007].

[104] W. C. Summers, and E. Bosworth, "Password Policy: The Good, The Bad, and The Ugly " in *Proceedings of The Winter International Symposium on Information and Communication Technologies* Cancun, Mexico 2004 pp. 1-6

[105] A. Jøsang, M. AlZomai, and S. Suriadi, "Usability and Privacy in Identity Management Architectures," in *The Australasian Information Security Workshop (AISW'07)*, Ballarat, 2007.

[106] A. Jøsang, and S. Pope, "User Centric Identity Management," in *AusCERT*, Gold Coast, 2005.

[107] J. Altmann, and R. Sampath, "UNIQuE: A User-Centric Framework for Network Identity Management," *10th IEEE/IFIP Network Operations and Management Symposium, NOMS 2006.* , pp. 495- 506, 2006.

[108] A. Bhargav-Spantzel, J. Camenisch, T. Gross *et al.*, "User centricity: a taxonomy and open issues," in Proceedings of the second ACM workshop on Digital identity management, Alexandria, Virginia, USA, 2006.

[109] Microsoft Corporation, "Windows Live ID," 2007. [Online]. Available: https://accountservices.passport.net/ppnetworkhome.srf?lc=1033. [Accessed July 10, 2007].

[110] G.-J. Ahn, and J. Lam, "Managing privacy preferences for federated identity management," in Proceedings of the 2005 workshop on Digital identity management, Fairfax, VA, USA, 2005.

[111] D. Shin, G.-J. Ahn, and P. Shenoy, "Ensuring Information Assurance in Federated Identity Management," in *the 23rd IEEE International Performance Computing and Communications Conference (IPCCC)*, Phoenix, Arizona, 2004., pp. 821-826.

[112] The Liberty Alliance, "Liberty Alliance Project," undated. [Online]. Available: http://www.projectliberty.org/. [Accessed July 10, 2007].

[113] Internet2, "Shibboleth Project," undated. [Online]. Available: http://shibboleth.internet2.edu/. [Accessed July 10, 2007].

[114] Eduserv, "AthensDA," undated. [Online]. Available: http://www.athensams.net/local_auth/athensda. [Accessed July 10, 2007].

[115] M. Slemko, "Microsoft Passport to Trouble," May 11, 2001. [Online]. Available: http://www.znep.com/~marcs/passport/. [Accessed July 10, 2007].

[116] OpenID, "OpenID: an actually distributed identity system," undated. [Online]. Available: http://openid.net/. [Accessed July 10, 2007].

[117] DeveloperOne, "CodeWallet Pro," 2007. [Online]. Available: http://www.developerone.com/codewalletpro/mobile.htm. [Accessed July 10, 2007].

[118] Ilium Software, "eWallet," undated. [Online]. Available: http://www.iliumsoft.com/site/ew/ewallet.htm. [Accessed July 10, 2007].

[119] Brighthand, "Password Manager for Symbian v4.0," undated. [Online]. Available: http://software.brighthand.com/product.asp?id=1720. [Accessed July 10, 2007].

[120] Lucent Technologies, "The Lucent Personalized Web Assistant," May 07, 1998. [Online]. Available: http://www.bell-labs.com/project/lpwa/. [Accessed July 10, 2007].

[121] A. Karp, "Site Password," *Hewlett-Packard Company.* undated. [Online]. Available: http://www.hpl.hp.com/personal/Alan_Karp/site_password/index.html. [Accessed July 10, 2007].

[122] J. A. Halderman, B. Waters, and E. W. Felten, "A convenient method for securely managing passwords," in Proceedings of the 14th international conference on World Wide Web, Chiba, Japan, 2005.

[123] K.-P. Yee, and K. Sitaker, "Passpet: convenient password management and phishing protection," in Proceedings of the second symposium on Usable privacy and security, Pittsburgh, Pennsylvania, 2006.

[124] Dobysoft, "KeyPass," 2007. [Online]. Available: http://www.dobysoft.com/products/keypass/index.html. [Accessed July 10, 2007].

[125] CP-Lab, "Password Manager XP," 2007. [Online]. Available: http://www.cp-lab.com/index.html. [Accessed July 10, 2007].

[126] B. Halpert, "Mobile device security," in Proceedings of the 1st annual conference on Information security curriculum development, Kennesaw, Georgia, 2004.

[127] L. W. Andrews, "Passwords Reveal Your Personality," *Psychology Today.* Jan/Feb 2002. [Online]. Available: http://psychologytoday.com/articles/pto-20020101-000006.html. [Accessed July 10, 2007].

[128] J. Yan, A. Blackwell, R. Anderson *et al.*, "Password Memorability and Security: Empirical Results," *IEEE Security and Privacy,* vol. 2, no. 5, pp. 25-31, 2004.

[129] S. Riley, "Password Security: What Users Know and What They Actually Do," *Usability News,* vol. 8, no. 1, February 24, 2006.

[130] D. Florencio, and C. Herley, "A large-scale study of web password habits," in Proceedings of the 16th international conference on World Wide Web, Banff, Alberta, Canada, 2007.

[131] R. G. Daniels, "A Participant's Perspective," *IEEE Micro,* vol. 16, no. 6, pp. 21-31, 1996.

[132] Intel Corp., "Intel® Core™2 Quad Processors Overview," 2007. [Online]. Available: http://www.intel.com/products/processor/core2quad/index.htm. [Accessed July 11, 2007].

[133] F. Voelkel, B. Toepelt, and P. Schmid, "Intel's Core 2 Quadro Kentsfield: Four Cores on a Rampage," *Tom's Hardware.* September 10, 2006. [Online]. Available: http://www.tomshardware.com/2006/09/10/four_cores_on_the_rampage/. [Accessed July 11, 2007].

[134] R. D. Silverman, "Exposing the Mythical MIPS Year," vol. 32, no. 8, pp. 22-26, 1999.

[135] R. Yung, "Evaluation of a Commercial Microprocessor," PhD Thesis, University of California, Berkeley, 1998.

[136] S. Gaw, "Construction kit for Password Management Strategies for Online Accounts," 2006.

[137] The University of Auckland, "Guiding Principles for Conducting Research with Human Participants at the University of Auckland," 2006. [Online]. Available: http://www.auckland.ac.nz/uoa/fms/default/uoa/about/research/ethics/docs/Guiding%20Principles%20for%20Research%20-%2022%20Nov%2006.doc. [Accessed July 10, 2007].

[138] R. Cohon, "Hume's Moral Philosophy," *The Stanford Encyclopedia of Philosophy.* The Metaphysics Research Lab, Center for the Study of Language and Information, Stanford University, 2004. [Online]. Available: http://plato.stanford.edu/entries/hume-moral/. [Accessed July 10, 2007].

[139] J. Bronowski, *Science and Human Values*, New York: Harper & Row, 1965.

[140] *Guiding Principles for Conducting Research with Human Participants at the University of Auckland*, The University of Auckland, 2006 [Online]. Available: http://www.auckland.ac.nz/uoa/fms/default/uoa/about/research/ethics/docs/Guiding%20Principles%20for%20Research%20-%2022%20Nov%2006.doc [Accessed July 07, 2007]

[141] T. Jagatic, N. Johnson, M. Jakobsson *et al.*, "Social Phishing " *Commun. ACM. To appear.* [Online]. Available: http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf. [Accessed July 07, 2007].

[142] Anonymous, "Phishing for Credit," *Slashdot.* April 2005. [Online]. Available: http://it.slashdot.org/article.pl?sid=05/04/26/1959256&tid=172. [Accessed July 10, 2007].

[143] C. Corley, "'Phishing' experiment attracts national adebate about ethics of study," *Indiana Daily Student News.* April 28, 2005. [Online]. Available: http://www.idsnews.com/news/story.aspx?id=29791. [Accessed July 10, 2007].

[144] *The University of Auckland 2006 Annual Report*, The University of Auckland, 2006.

[145] S. Cockcroft, and S. J. Cunningham, "Gender and Other Social Issues," in *Software Education Conference*, 1994, pp. 336-338.

[146] P. Tilley, J. F. George, and K. Marett, "Gender Differences in Deception and Its Detection Under Varying Electronic Media Conditions," in *Proceedings of the 38th Annual Hawaii International Conference on System Sciences, 2005. HICSS '05*, Hawaii, 2005, pp. 1-9.

[147] L. Beckwith, M. Burnett, V. Grigoreanu *et al.*, "Gender HCI: What About the Software?," *IEEE Computer,* vol. 39, no. 11, pp. 97-101, November 2006.

[148] S. H. Jenkins, "Data pooling and type I errors: a comment on Leger & Didrichson," *Animal Behaviour,* vol. 63, pp. F9-F11, 2002.

[149] D. Bryant, T. C. Havey, R. Roberts *et al.*, "How Many Patients? How Many Limbs? Analysis of Patients or Limbs in the Orthopaedic Literature: A Systematic Review," *The Journal of Bone and Joint Surgery,* vol. 88, pp. 41-45, 2006.

[150] A. Petrie, J. S. Bulman, and J. F. Osborn, "Further statistics in dentistry Part 7: Repeated measures," *British Dental Journal,* vol. 194, no. 1, pp. 17-21, 11 January 2003.

[151] J. Neter, W. Wasserman, and M. H. Kutner, *Applied linear statistical models*, Chicago: Irwin, 1996.

[152] C. Kuo, S. Romanosky, and L. F. Cranor, "Human selection of mnemonic phrase-based passwords," in Proceedings of the second symposium on Usable privacy and security, Pittsburgh, Pennsylvania, 2006.

[153] U. Topkara, M. J. Atallah, and M. Topkara, "Passwords decay, words endure: secure and re-usable multiple password mnemonics," in Proceedings of the 2007 ACM symposium on Applied computing, Seoul, Korea, 2007.