Enabling e-Learning 2.0 in Information Security Education : A Semantic Web Approach

by

Ryan Gavin Goss

Enabling e-Learning 2.0 in Information Security Education : A Semantic Web Approach

by

Ryan Gavin Goss

Dissertation

submitted in fulfillment
of the requirements
for the degree

Magister Technologiae

in

Information Technology

in the

Faculty of Engineering, The Built Environment and Information Technology

of the

Nelson Mandela Metropolitan University

Promoter: Johannes F. van Niekerk

January 2009

Contents

List of Figures

Chapter 1

Introduction

In order to prosper in today's modern society, people require skills that were not necessarily taught to them by their parents. For example, most children are taught how to avoid actions that could lead to personal harm from a very young age, yet very few adults today were taught how to protect themselves from harm whilst conducting themselves on public information networks by their parents. The rapid growth of computer and Internet use was so unexpected and so fast, that humans were simply not ready for it. This was due, in part, to the fact that parents had not experienced the technology so could not impart any knowledge on to their children.

Past technological advancements, such as the development and large-scale deployment of the motor vehicle took time to advance and enter into the daily lives of people. This gave people time to accept the introduction of this technology and the opportunity to better understand it. As people learnt more about the technology, so they passed on this information to their children, allowing an ingrained awareness of safe behaviour in and around motorized vehicles to be developed over time. This awareness involved many aspects, including the need for people to act securely around motor vehicles, in order to protect themselves from bodily harm and potential death. It further afforded people the opportunity to slowly develop a subconscious awareness of operating safely around motor vehicles. These concepts were passed down from generation to generation by parents educating their children in these and other security concepts. These concepts developed to include awareness surrounding all aspects of the motor vehicle, including the road on which they operate. Children were taught by their parents to look both ways before crossing the road, in order to protect themselves from harm by vehicles traversing the streets.

The development of computer systems did not afford people the same opportunity to slowly build up awareness as to the various threats they may face whilst operating them. Unlike that of the motor vehicle analogy, computer system development and introduction did not span multiple generations. In fact, the first personal computer systems were deployed in the 1980s by a company called IBM, which sought to target the home user with an affordable, number crunching machine. The popularity of such machines grew faster than could have been predicted and, therefore, the technologies that these systems were built on began to undergo further developments.

Public networks, more specifically the Internet, which was introduced in the mid 1990s, grew in popularity virtually over night. Some of the main drivers included organizations looking to interconnect and share information with their suppliers. With the cost of Internet connectivity slowly subsiding as it grew in popularity, more and more individual users began to sign up and "get online". The creation of a global, public network of users, which seemingly knew no geographic boundaries, opened up a whole host of risks to the information stores of both organizations and individuals. Virtually anyone connected to the Internet could gain access to them. This posed a potentially serious problem to organizations, which store company secrets and other confidential information in these systems. A disclosure of information to a person external to the organization could end up costing the organization in lost profits and slowed productivity. Furthermore, an interruption in access to information within an organization could lead to financial losses being incurred and the company losing money whilst the systems were being restored. Information systems should, therefore, be viewed as critical business assets to organizations and be protected.

Organizations, however, are not the only users of the Internet. Individuals, too, have information on their computer systems which needs to be protected from disclosure to the wrong people. Individuals, who conduct commerce with various organizations online, often provide sensitive information such as their credit-card information, their physical address, contact numbers, etc. If this information is leaked to a would-be attacker, the attacker could use it to exploit the user, stealing their identity and making purchases under their name.

The information contained within both organizational and individual information systems, therefore, is important and needs to be protected. Users of such computer systems are potentially one of the biggest threats to the information systems and the failure of such users to secure them may lead to the demise of an information security system as a whole. This is true for both organizational and individual computer systems. In order to mitigate the problem of users of the system being its biggest threats, **users need to know how to act securely** as users, for the most part, lack the knowledge required to act securely in their role within an information system (Van Niekerk & Von Solms, 2007).

One way to ensure that users act securely is to encourage a change in behaviour, both in the work place and in the home computer system environment. This change in behaviour is possible through the development of an information security culture. One of the keys to enabling such a culture is user education. All users of information systems require education to enable them to conduct their daily activities securely.

1.1 Motivation for this Study

All users of computer systems require education in order to act securely in the roles they play within an information system. Most current awareness/education programs are created by information security experts who are not necessarily educationalists. The single largest problem with current information systems, according to Puhakainen (2006), is their **lack of theoretically grounded and testable concrete guidance** to ensure that users are committed to fulfilling their information security mission. However, even if formal "traditional" education theory is used, they may still not be practical in educating users of computer systems world-wide. The **deliv-**

ery method of such methods are not completely feasible in the context of modern society, where the reach of the education system spans multiple continents. The **cost of learning** to both organizations and individuals would be excessive and the benefits of education would be hard pressed to outweigh them. In order to facilitate educating all users, all **scheduling conflicts would need to be resolved**, educating users at a time and date suitable to everyone: **a potentially impossible feat**. This is due to the **logistics of location**, as learners requiring education are from all round the world, having different languages and cultural backgrounds. These differences of learners mean they will also have **different learning styles**; therefore, the standard ”one-size-fits-all” analogy will not be well suited to educating them.

It is, therefore, apparent that in order to educate all users of computer systems world-wide in information security, **a new education system is required to address these and other requirements of learners**. With traditional delivery systems, such as classroom-based education systems, **this feat is nearly impossible to accomplish**. Educating all users in acting securely on computer systems has become a problem which society on a whole needs to address (Siponen, 2001). The discovery of a new method for the delivery of information security education content is thus required in order to accomplish this.

1.2 Problem Statement

The motivation for this study argued that current information security education systems are inadequate for educating all users of computer systems world wide in acting securely during their operations with information systems. **There is, therefore, a pervasive need for information security knowledge in all aspects of modern life**. E-Learning 2.0 could possibly contribute to solving this problem, however, **little or no knowledge currently exists regarding the suitability and practicality of using such systems to infer information security knowledge to learners**.

1.3 Thesis Statement

This dissertation's thesis statement is two-fold. Firstly, it **asserts that e-Learning 2.0 is very suitable for the implementation of an information security education system**, which will be suitable for educating users of computer systems world wide. Secondly, the use of **the Semantic Web to implement an e-Learning 2.0 environment** provides the means to build such a system.

1.4 Delineation

E-Learning 2.0 systems are only possible through the use of a standard set of ontologies. The creation of such ontologies is a major task and cannot feasibly be completed by a single person. As no such information security ontologies exist, the concept presented in this dissertation cannot be proved via a prototype. This study shall thus present a "proof of concept" in the form of a case study, supported by argument and where suitable, examples. Thus, the objective of this study will not be to show a fully working implementation of an information security education program using e-Learning 2.0, but rather to present an example which clearly demonstrates the feasibility of such an approach.

1.5 Research Objectives

1.5.1 Primary Objective

The primary objective of this study is to show, by means of argument and a comprehensive example, that the creation of collaborative information security education content and the education of users in information security, based on the principles of e-Learning 2.0 can become a possibility through the use of the Semantic Web as the primary content storage and retrieval mechanism.

1.5.2 Secondary Objectives

- To clearly demonstrate Web 2.0 and its benefits in overcoming the downfalls of current information security education systems in educating all users of computer systems, independent of their role within their computer system.
- To clearly demonstrate the Semantic Web and its benefits for enabling the development and deployment of such information security education.

1.6 Research Methodology

The methodology that was utilized for this research project comprised of the following:

- **Literature studies**: A literature study was performed in order to establish the current state of information security education in modern society. This information was analyzed and evaluated, leading to a second literature study conducted to review the various learning methods available for educators in general, in order to ascertain the best method to educate learners in information security. Following this, a third literature study was conducted in order to establish the viability of using the Web as a platform for developing an information security education system capable of reaching the intended audience. The information gathered was then analyzed and it was found that e-Learning 2.0 emerged as a potential solution to this problem. Finally, an investigation into e-Learning 2.0 revealed that when combined with the Semantic Web, e-Learning 2.0 produces the best results for educating users.
- **Argumentation**: The relevance of these findings was then extensively argued according to principles outlined in (Mason, 1996) which revealed the suitability of e-Learning 2.0 and Semantic Web implementations for information security education.

- **Case Study**: A case study was presented in order to demonstrate the relevance and possibility of implementing these findings, presented in accordance to the guidelines set out by Creswell (2007).

1.7 Layout of Dissertation

The dissertation consists of eight chapters, the layout of which is depicted in Figure 1.1.

1.7.1 Roadmap for this Dissertation

Chapter 1 presents the research subject and gives background information to define the problem area and the motivation for this study.

Chapter 2 argues that information contained in computer systems is important to both organizations and individuals. This information, therefore, needs protection and the characteristics of secure information are described. The chapter further discusses the various risks associated with information systems, stating there are risks from threats exploiting vulnerabilities in information security systems in order to harm the information they protect. The risk management process is then discussed in order to mitigate risk by introducing controls or safeguards. The chapter lastly identifies users of an information system as the greatest risk to it.

Chapter 3 highlights the users of information systems as the greatest risk to them in more detail. The chapter asserts the possibility of reduction of such risk, by changing the behaviour of the users through the development of information security culture. One of the keys that is identified to the development of such culture is education. The chapter follows by providing an in-depth view of the current state of information security education. It discovers that current education systems are inadequate for educating all users of computer systems world wide. It asserts, therefore, that a new system needs to be developed, addressing the new target audience. What users should be taught, and how these users should be educated, is discussed, with the Web being raised as a possible platform for the development of the system.

Chapter 4 starts from the grassroots of learning, with the intention to identify best learning method based for educating users in information security education. Web-based learning is then checked for suitability of implementation for such a learning method. E-Learning emerges as a possibility, with its adaptive and intelligent features. Finally, benefit from the latest trends in Web development, namely Web 2.0, are identified as possible enhancements to such systems.

Chapter 5 begins with a discussion on the progression of Web technologies, from Web 1.0 to Web 2.0. The trend in Web-based education is discovered to be toward e-Learning 2.0, enabled through the use of Web 2.0 technologies and methods. The guidelines for designing such systems are presented, with reference to information security education systems; thereafter, the advantages to both educators and learners are discussed. It is found that there are challenges in implementing such systems, which need to be addressed in order to ensure its success.

Chapter 6 describes the challenges mentioned in Chapter 5 in more detail. This chapter then presents the Semantic Web as a solution to many of these problems and provides an approach for the implementation of e-Learning 2.0 used in conjunction with the Semantic Web for information security education systems.

Chapter 7 provides an example case study of the implementation of such a system, showing that it is possible that e-Learning 2.0 and the Semantic Web can work together to build and effective information security education system.

Chapter 8 concludes the dissertation, summarizing the findings of the chapters throughout. It further provides future researchers with additional problems for investigation as time progresses and technologies advance and become more available. Lastly, the chapter asserts that it is possible that e-Learning 2.0, built on Semantic Web technologies, will successfully implement an information security education system, suitable for educating all users of computer systems world-wide.

1.8 Conclusion

This chapter aimed to provide background on the problem area addressed by this dissertation. The main objective for the study was identified and the way the dissertation aimed to address it presented. Following that, a layout of the dissertation was presented, showing the structure and flow of the chapters which comprise it.

The following chapter is an extension of this chapter and builds on the background, showing that **information is important to both organizations and individual users of computer systems and needs to be protected**.

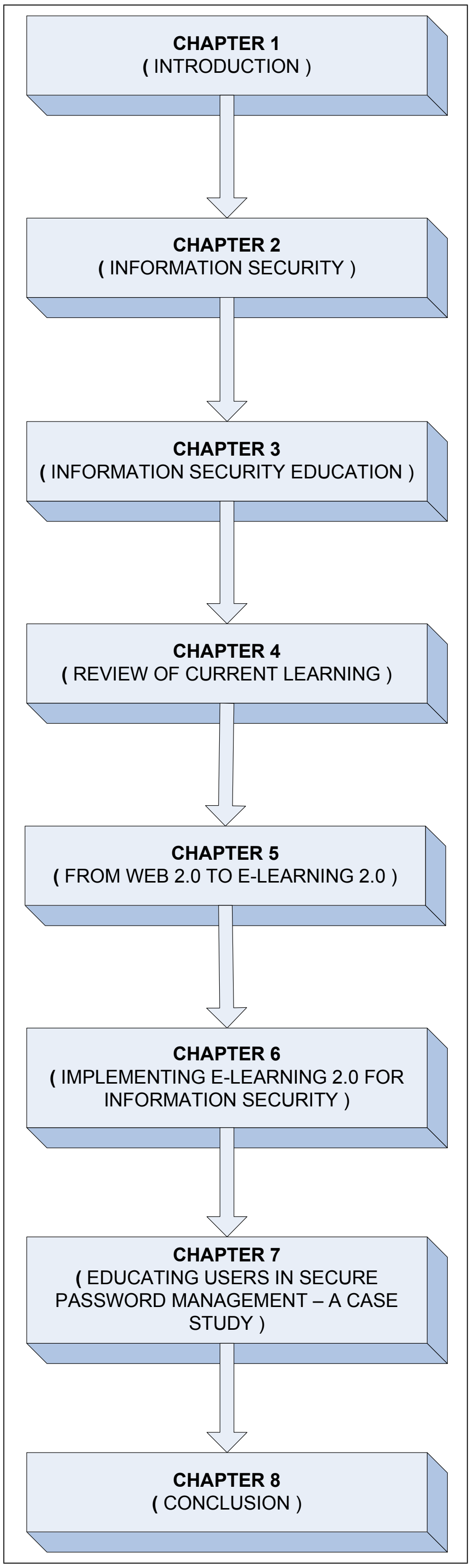

CHAPTER 1
(INTRODUCTION)
CHAPTER 2
(INFORMATION SECURITY)
CHAPTER 3
(INFORMATION SECURITY EDUCATION)
CHAPTER 4
(REVIEW OF CURRENT LEARNING)
CHAPTER 5
(FROM WEB 2.0 TO E-LEARNING 2.0)
CHAPTER 6
(IMPLEMENTING E-LEARNING 2.0 FOR INFORMATION SECURITY)
CHAPTER 7
(EDUCATING USERS IN SECURE PASSWORD MANAGEMENT – A CASE STUDY)
CHAPTER 8
(CONCLUSION)

Figure 1.1: Layout of dissertation

Chapter 2

Information Security

2.1 Introduction

In order to prosper in today's modern society, people require skills that were not necessarily taught to them by their parents. For example, most children are taught from a very young age how to avoid actions that could lead to personal harm, yet very few adults today are taught by their parents how to protect themselves from harm whilst conducting themselves on public information networks. The rapid growth of computer and Internet use has been so unexpected and so fast that humans were simply not ready for it. This was due to the fact that parents had not experienced the technology and thus could not impart any knowledge of it to their children.

Past technological advancements, such as the development and large scale deployment of the motor vehicle took time to advance and enter into the daily lives of people. This gave people time to accept the introduction of this technology and the opportunity to better understand it. As people learnt more about the technology, so they passed on this information to their children, allowing an ingrained awareness of safe behaviour in and around motorized vehicles to be developed over time. This awareness involved many aspects, including the need for people to act securely around motor vehicles in order to protect themselves from bodily harm and potential death. It further afforded people the opportunity to slowly develop a subconscious awareness of operating safely around motor vehicles. These concepts were passed down from generation to generation by parents educating their children in these and other security concepts. These concepts developed to include awareness surrounding all aspects of the motor vehicle, including the roads on which they operate, for example children were taught by their parents to look both ways before crossing the road.

The development of computer systems did not afford people the same opportunity to slowly build up awareness as to the various threats they could face whilst operating them. Unlike that of the motor vehicle analogy, computer systems development and their introduction did not span multiple generations. In fact, the first personal computer systems were deployed in the 1980s by a company called IBM, which sought to supply home users with affordable, number-crunching machines. The popularity of such machines grew faster than could have been predicted; therefore, the technologies that these systems were built on began to undergo further developments.

The personal computer system began to include forms of non-volatile storage for the information generated, allowing users of such systems to share information with other computer users, providing it to them on diskettes. The requirement for furthering technologies to enhance the communication process between users of different computer systems lead to the development of local area networks (LANs). For the first time, users of separate computer systems were able to connect to other personal computers, accessing their computer resources including the information which they had stored on them. Initially there was little or no concern regarding access to this information, as this depended on the remote computer system being connected directly to the host computer system using a physical cable. It was assumed that the users who were connected were trustworthy. This was adequate, until the introduction of public information networks such as the Internet.

Public networks, more specifically the Internet, grew in popularity virtually over night. Some of the main drivers included organizations looking to interconnect and share information with their suppliers. With the cost of Internet connectivity slowly subsiding as it grew in popularity, more and more individual users began to sign up and get online. The creation of a global, public network of users, which knew seemingly no geographic boundaries, opened up a whole host of risks to the information stores of both organizations and individuals. Virtually anyone connected to the Internet could gain access to them. This posed a potentially serious problem to organizations storing company secrets and other confidential information on these systems. A disclosure of information to a person external to an organization could end up costing it in lost profits and slowed productivity. Furthermore, an interruption in access to information within an organization could lead to financial losses being incurred and the company losing money whilst the systems are being restored. Information systems should therefore be viewed as critical business assets to organizations and be protected.

Organizations, as discussed, are not the only users of the Internet. Individuals also have information on their computer systems which needs to be protected from disclosure to the wrong people. Individuals who conduct commerce with various organizations online often provide sensitive information such as their credit card information, physical addresses, contact numbers, etc. If this information was leaked to a would be attacker, the attacker could use it to exploit the user, stealing their identity and making purchases under their name.

The information contained within both organizational and individual information systems, therefore, is important and needs to be protected. The process of protecting information within computer systems is known as information security, and will be the focus of the following chapter. In order to better understand information security, it is necessary to take one step back and discuss information and security as separate concepts.

2.2 Information

Information is a collection of related data or knowledge about a particular topic, processed and stored in a format that is understandable by its intended audience. Examples of information include printed bank statements or other filed documentation which provides knowledge pertinent to an organization or individual. This dissertation will focus on information that is stored within computers; however, the educational principles involved could apply to all information. The collection of such information within a computer system is known as an information system. The contents of an information system, as briefly outlined in the introduction to this chapter, are important to both organizations and individuals alike. The following sections elaborate on this point.

2.2.1 Importance of Information

To an organization

Any organization which suffers an interruption in critical services will suffer both financial and competitive losses (Goguen, Stoneburner, & Feringa, 2002). Critical services to organizations depend on the field in which they operate, but may include such services as electricity, licenses to operate and human resources. With the advent of computer systems, information systems have become one such **critical business asset** (Carr, 2003). Nagaraj (1999) describes the access to information as power and, for all practical purposes, information is control. Organizations of today need their information systems to support their decision-making processes and conduct their business. If this information system is interrupted or compromised, the organization may suffer great losses.

The interruption or compromise of information can take many forms, each with a different level of severity to consider. The incorrect data capture or accidental deletion of information is far less severe than the disclosure by an organization of its secrets to its competitors. Information, by nature, is highly replicable (Carr, 2003), making its disclosure a high risk for an organization. This replicated information can be transferred to an attacker via a multitude of media, including external storage media and public networks. These attackers are often individuals who test the vulnerability of these systems as part of a game, often gaining access via public networks: the same public networks installed to enhance an organization's business.

These and other individual computer system users have information stores which also need protection. Individuals are often the victims of attacks as they are easy prey for attackers. The following section will, therefore, assess the importance of information systems to individuals and why protecting them is important.

To the individual

Individuals are often the target of information system attacks which target information stored on a computer system or information in transit between the system and a secure remote host. Any breach in security of the remote host could also compromise the information it stores about its clients. When an online retailer is compromised, so is their customer data. The interception of information and remote access to stored information allows attackers access to confidential information, such as social security numbers, credit card details and other personal financial information. By compromising the confidentiality of this information, a critical aspect of information described in Section 2.4.1, attackers are able to exploit the individual, using credit card and other information they have intercepted.

In acknowledgement of the threats posed to individual computer systems and to the personal security of the individual through the disclosure of such information, individuals should act securely whilst conducting themselves within computer systems. By being made aware of the risks at large, individuals will be far better prepared to implement security features or modify their behaviour in order to mitigate the risks.

In this section, information was demonstrated as an important asset to both organizations and individuals. A loss of information may imply other kinds of losses, including money and even life, if a hospital's information security system was compromised (Siponen, 2001). The importance of information thus leads to the requirement for protection of these information systems. In order for security measures to be developed for protecting information, a general understanding of security needs to be discussed.

2.3 Security

As a general view, security is the quality or state of being secure, to be free from danger (Whitman & Mattord, 2003). Security is comprised of three basic elements: Assets, Vulnerabilities and Threats (Goguen et al., 2002) each of which are examined in more detail.

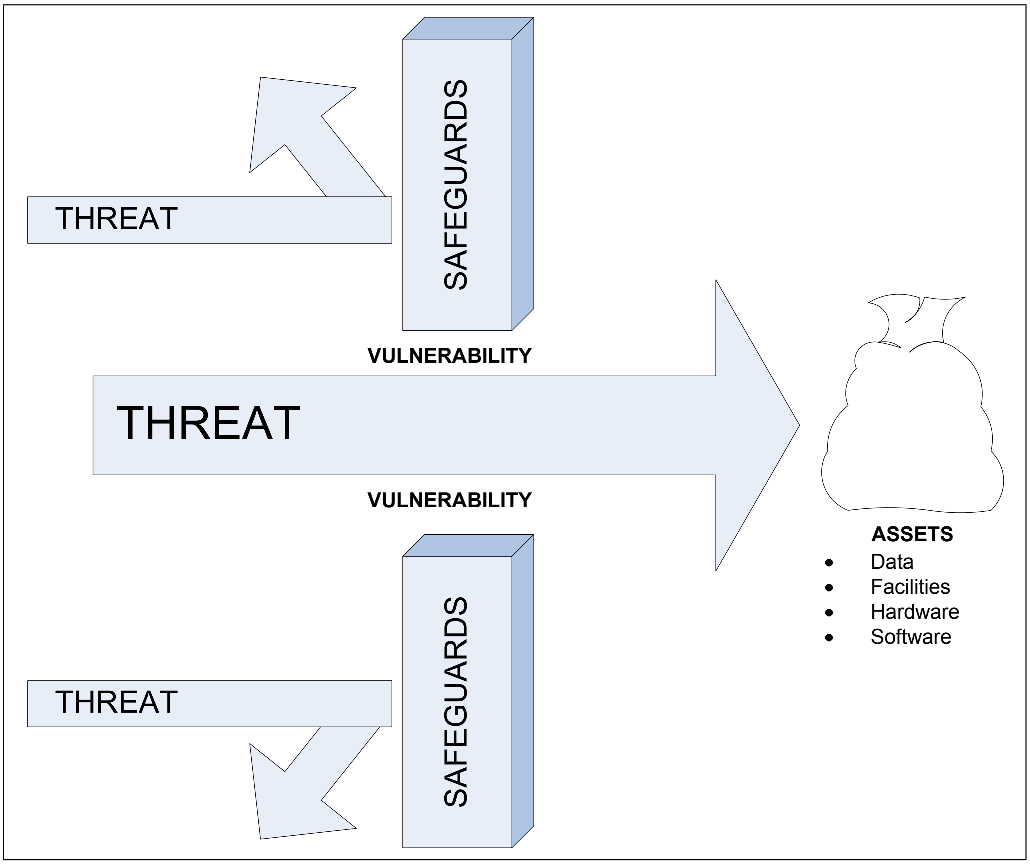


Figure 2.1: Assets, Vulnerabilities, Threats and Safeguards Adapted from Guttman and Roback (1995)

2.3.1 Elements of Security

Assets

An asset in general terms is something which exhibits a valuable or useful quality. For the purposes of information systems, an asset is the information contained within these systems which is of value to the organization or the individual. In the introduction to this chapter, it was discussed that parents educate their children in acting securely in order to protect themselves from bodily harm. In this light, the child's body is viewed as the asset. An asset, which may be a physical and tangible object or an organizational secret, is the object of a security system which must be protected from damage.

Information assets are susceptible to various attacks, some of which damage the assets and others which simply replicate them, leaving the original intact. Although the original asset is intact, its confidentiality has been compromised and is, therefore, of less value to the organization. Organizational assets may include company secrets, employee payroll information or secure files. Individual information assets may include credit card information, personal medical histories and other confidential information.

Vulnerabilities

A vulnerability within a security system is a flaw or weakness in it which allows unauthorized access to the assets which it protects (Goguen et al., 2002). Examples of vulnerabilities include buffer overruns in software code being exploited, allowing the attacker direct access to the computer system, incorrectly configured firewalls and non-updated antivirus applications.

Threats

Threats are events, objects or even people which pose a risk to the safety of the assets protected within a security system (Goguen et al., 2002). For example, if the underlying source code of an application is vulnerable to attack, an attacker could attempt a buffer overrun to exploit it. Likewise, if a firewall is incorrectly configured, a hacker could exploit an open port and potentially gain unauthorized access to the system. In both cases, the threat of attack exists solely due to the existence of vulnerabilities.

Security involves the **protection of an asset**, from the **risk** of **threats** and **vulnerabilities** that can **impact** on it negatively. An asset is exposed in one or other way to various threats which exist in the world in which it resides. A **threat** exploits a **vulnerability** in order to gain **access** to the **asset**. The likelihood that a threat can exploit a vulnerability within a security system, causing an adverse reaction is known as **risk** (Goguen et al., 2002).

In order to protect an asset, the risk posed by a specific threat can be reduced through the introduction of controls. For example; to protect one's children from the risks posed by an automobile accident, one can educate them on how to safely cross a road. In this case the asset is the child's person, the threat is the possibility of being run over by a car, the risk is the likelihood of this happening and education is the control implemented to reduce the risk.

The definition of security for the purposes of this dissertation is thus: "The protection of an asset from a threat by introducing controls (or safeguards) which mitigate the risk that such a threat will exploit a vulnerability and, therefore, adversely effect the asset".

Information was viewed as an asset to organizations and individuals in the previous section and thus requires protection. Nagaraj (1999) states that the one problem with information technology (IT) is its misuse, but goes on to say that this is not IT's fault, but rather the fault of those who choose to misuse it. Information systems therefore need to be protected against those who choose to misuse them. The protection of the information and the systems and hardware that use, store and transmit that information is known as information security (Whitman & Mattord, 2003).

2.4 Information Security

Information is comprised of bits of data: ones and zeros. A duplicate copy of information can be created with little or no trace of the activity. Likewise, information can easily be modified by changing these data bits. Due to the nature of information, there is no method to guarantee its complete safety and security. Instead, information security should attempt to balance controls against risks, forming an equilibrium. It is very difficult to know exactly what controls are required in order to ensure a minimum level of information security within an information system (Van Niekerk & Von Solms, 2007).

The requirements of various information system protection differ, for example an individual's information system protection needs are different to those of an organization's.

In order to address the problem of which controls and safeguards to implement, security experts require ways of ensuring all basic information security requirements are met. To accomplish a baseline (a base for measurement of minimum safety) information security system, security experts make use of best practises and international standards which assist in the creation and deployment of information security controls in order to build an effective information security system (Van Niekerk & Von Solms, 2007). These international standards offer information security (IS) professionals a baseline configuration which covers the essential security risks which may present themselves as threats to information systems. In order to ascertain the effectiveness of an information security system and the severity of damage after an attack, the information should be tested against the characteristics of secure information (Goguen et al., 2002).

2.4.1 Characteristics of Secure Information

The characteristics of secure information describe certain elements which must be unharmed in order for information to be classified as secure (Goguen et al., 2002). These elements have been described for many years by information security experts as the CIA triangle. The CIA or Confidentiality, Integrity and Availability (also Accountability) has been considered the industry standard for computer security since the inception of the mainframe (Whitman & Mattord, 2003). The following section details each of the elements of the CIA triangle in order to determine the importance of them.

Confidentiality

The prevention of disclosure of information to a third party person or application refers to the confidentiality of the said information. Sensitive information, such as passwords, bank authentication details and company secrets need to remain confidential. Certain information, if disclosed to external

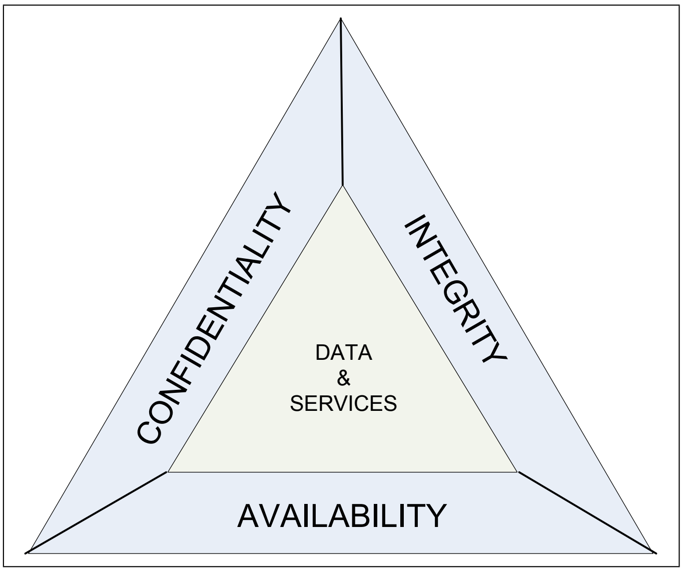


Figure 2.2: The CIA Triangle as Described by Whitman & Mattord (2003)

sources by unauthorized, unanticipated, or unintentional actions, could result in loss of public confidence, embarrassment, or legal action against the organization (Goguen et al., 2002). The unauthorized disclosure of sensitive information of both individuals and organizations could thus potentially cause certain harm to the entity, as the information is no longer known to only authorized users.

As an example, consider the following: Someone making use of social-networks (such as the Facebook) often falls victim to identity theft. This involves an attacker accessing confidential information from the target and then using it to pose as the target, making purchases under their name and often incurring significant debt from online purchases. By filling in various forms and information request pages on these social-network applications, users often open themselves and their identity (the asset) to identity theft (the threat) by submitting sensitive information to the application (the risk) in the hopes of winning competitions or other benefits. Controls can be imposed to mitigate these threats, such as the disallowing of hyper text transfer protocol (HTTP) cookies and maintaining up-to-date antivirus installations. Attacks which play on the ignorance of individuals are currently on the increase and attackers see these marks as soft targets. For example, the number of reported key logger cases has increased from 444 in the year

2002 to 6,191 in 2005 (Lenard & Britton, 2006) and continues to increase annually. Key loggers are software applications which bind hooks into the various input devices, normally the keyboard, and log all input passed by the user to the computer system, thereafter reporting this information to the attacker's server.

Integrity

The integrity of information relates to its quality or state of being whole or complete and uncorrupted, protected from improper modification (Goguen et al., 2002). If improperly modified information is served to users who have the sufficient access rights to view it, the information they receive is incorrect and could have resulting consequences on the organization or individual.
The integrity of information is threatened once it has been exposed or disclosed to an unauthorized person or system (Whitman & Mattord, 2003). In order to ascertain if the information received is properly modified information, a system needs to be developed to check its integrity. One method is to implement file hashing, as described by Whitman and Mattord (2003) in which a file is read through a particular hashing algorithm which computes a single hash value. This value can then be stored and compared to the file in future to ensure that no unauthorized changes have been made to it.

As an example, consider the following: Within an organization, a particular financial department staff member accidentally removes the recurring invoice batch from the accounting software. The accounting team has to rebuild the entire batch so that the invoices will successfully be dispatched at the end of the month. The asset in this case, is the completed accounting information stored on the computer system. The threat is the human accidentally manipulating the information store incorrectly and thus jeopardizing its integrity. The risk is that as the staff member works within the accounting system on a daily basis, the probability of something being accidentally deleted is quite high. By implementing controls such as a confirmation dialog box prompting the user "Are you sure you want to completely remove the batch?", the risk would be mitigated as the user would be made more aware of their actions and the consequences faced if they proceeded.

Availability

The availability element of information ensures that authorized users who are entitled to view, modify and save to the information, have access to it in the required format (Whitman & Mattord, 2003). A user who attempts to access a particular file on a shared drive, after authenticating to the system, should be able to access this file without any further interference or obstruction (Whitman & Mattord, 2003). If access to this information is denied and mission critical information is unavailable to its end users, the organization's mission may be affected (Goguen et al., 2002). Likewise, if an individual's important information such as financial records is unavailable, the task the individual is trying to accomplish will be hindered.

The CIA triangle model has been the industry standard for describing computer security for many years, but has, in recent times, needed to adapt to the ever-changing world of technology. Thus, it has expanded into a list of critical characteristics of information (Whitman & Mattord, 2003) including the addition of the following characteristics for describing the security of computer systems.

Accuracy of Information

Accuracy of information refers to the information being free from mistakes and the value presented to the user upon request being that which the user expects (Whitman & Mattord, 2003)

Authenticity of Information

Authenticity of information refers to the quality or state of being genuine and original, rather than a reproduction or fabrication (Whitman & Mattord, 2003).Carr (2003) stressed that IT is highly replicable and that indeed it would be hard to imagine a commodity more perfect for replication than a byte of data, which can be replicated perfectly with little cost.

Utility of Information

The purpose of the information is referred to its utility. Information represented in an unreadable format is meaningless and, therefore, not fit for a particular purpose (Whitman & Mattord, 2003).

Possession of Information

The quality or state of having ownership or control of information is referred to as possession of the information. Whilst a breach in confidentiality always results in a breach of possession of information, a breach in the possession of information does not necessarily result in a breach of confidentiality (Whitman & Mattord, 2003). Encrypted information can be possessed by an external source: however, if they lack the ability to decrypt this information, although the possession characteristic has been compromised, the confidentiality of the information has not.

This section provided the critical characteristics of information which ensure its security. These characteristics are constantly at risk from various threats, which seek to exploit vulnerabilities in order to affect the characteristics described above. In order to understand the process of information security, the relationship between risks and threats and how they act on the characteristics of information systems need to be discussed.

2.5 Risks and Threats to Information Systems

Risk, generally speaking, is the probability that something one does not want happening, happens (Whitman & Mattord, 2003). Risk from an information security viewpoint is the probability of a threat to the system, the probability that a vulnerability within the system will be discovered or the probability of equipment, hardware or software, failure (Whitman & Mattord, 2003). It has already been argued that information is important: therefore, the risks and management thereof to information systems need to be discussed. The management of risk to information systems is described by Goguen et al. (2002) as encompassing three processes.

2.5.1 Risk Management

Risk management was noted previously as an important aspect to consider when securing information systems. Many risks exist to information systems and originate from a number of threat sources, including natural disasters (flooding, earthquakes, tornadoes, etc.), human threats (unintentional acts, deliberate attacks, etc.) and environmental attacks (long-term electricity outages, pollution, liquid leakages, etc.) (Goguen et al., 2002). According to Goguen et al. (2002), the process of risk management covers three distinct sections: risk assessment, risk mitigation and evaluation and assessment. These are described below.

Risk Assessment

The risk assessment process involves the classification of risks which pose a threat to an information system and is the first process of risk management (Goguen et al., 2002). Much like human beings assess the risk of crossing the road by first looking left to right, so too should information security experts assess the risks which pose a threat to their information systems. The resulting discoveries from a risk assessment process assist in the identification of various controls used to eliminate or reduce the risk in the risk mitigation process (Goguen et al., 2002), discussed in the following section. These discoveries and the new controls implemented due to them should be analyzed in conjunction with potential vulnerabilities and existing controls within the IT system (Goguen et al., 2002). If new controls are not implemented to combat these potential risks, the impact of such an attack on the system could be significantly higher than if a control was in place. The impact of such an attack refers to the amount of harm imposed on the system due to a threat exploiting a vulnerability (Goguen et al., 2002). Risk, therefore, needs to be mitigated in order to lesson the harm imposed on the system by an attack. The risk mitigation process, therefore, plays an important role in ensuring the security of information within information systems and is discussed in the following section.

Risk Mitigation

Risk mitigation involves the prioritization, evaluation and implementation of controls which are set in place to protect information against risk (Goguen et al., 2002). For example, the crossing of roads at pedestrian crossings mitigates the risk of being run over by a car whilst crossing the road. The selection and implementation of information security controls should be prioritized, and higher priority given to the threat and vulnerability pairs that have the potential to cause significant impact to information systems (Goguen et al., 2002). These controls are discussed further in Section 2.6.

Evaluation and Assessment

In organizational and individual computer systems, network resources, software installations and other expansions take place (Goguen et al., 2002). These changes bring about new risks to the information system and sometimes old, previously mitigated threats will resurface and once more pose a threat to security (Goguen et al., 2002). Due to the fact that change is accepted and will always take place, the controls and policies information security professionals put in place need to evolve (Goguen et al., 2002) and constantly be updated to handle these changes. The evaluation and assessment of risk management systems, therefore, emphasize good practice and need for an ongoing risk evaluation throughout the risk management process (Goguen et al., 2002). Risk management is, therefore, a repetitive task, involving the assessment of risk, implementation of controls, policies and procedures to mitigate risk, evaluate the outcome of these implementations and make further changes where necessary.

The risk management process is a tool to assist information security professionals in the identification and mitigation of risks within an information system. The process involves the identification and classification of potential risks, the mitigation of these risks by way of implementing controls and procedures and finally, the evaluation and assessment of these risks on a recurring basis. The following section gives more insight into the controls which may be deployed by IT professionals in order to mitigate risks to an information system.

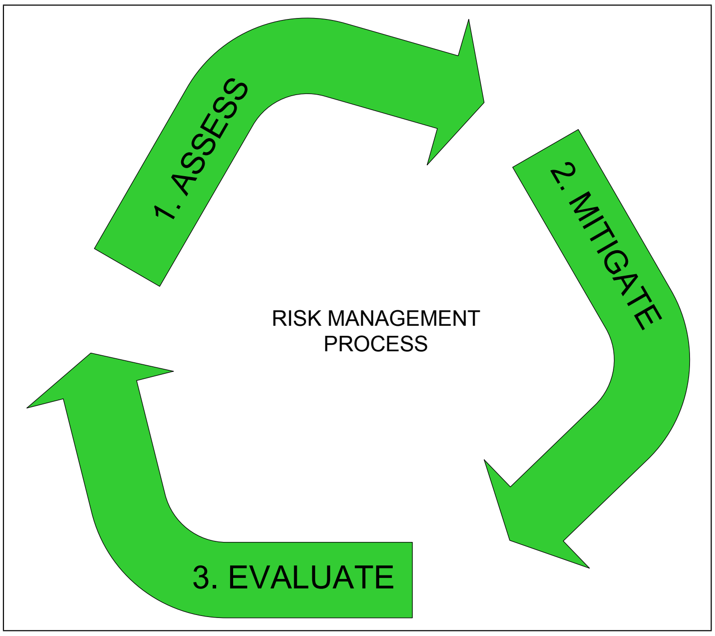


Figure 2.3: Information Security Risk Management Process as Described by Goguen et al (2002)

2.6 Information Security Controls

Information security, as described in the previous section, is a process of balancing controls against risk in order to protect information assets of both individuals and organizations. The following section presents the controls which can be implemented in order to mitigate risk and ensure that the characteristics of secure information are upheld. These controls form part of the safeguards, as depicted in Figure 2.1.

The controls, described as safeguards and countermeasures, can be classified from an organizational viewpoint into three categories (Van Niekerk & Von Solms, 2007)(Goguen et al., 2002): Physical, technical and operational Controls. These are discussed in the following sections.

2.6.1 Physical Controls

Physical controls in information security are controls implemented to protect the physical or tangible assets within an information system, such as laptop computers, file servers and data lines. The mitigation of risks by way of physical controls include security check points, electric fencing, gates and concrete ceilings for server rooms. These controls prevent access to information physically, having a physical appearance and warning to would be attackers. Physical controls are the first line of defence against an external attack on information, supporting the two remaining classes, technical and operational, in the information security process.

2.6.2 Technical Controls

A technical control is implemented through the use of technology like a piece of software or hardware device. An example of such a control would be requiring a username and password combination for accessing a particular computer system and gaining access to its resources. As technical controls deal with advanced software and hardware requirements, out of access to the ordinary end-user, they are often implemented by IT professionals who have had extensive training in them. This training involves the conveyance of knowledge of the product to the IT professional. A firewall, for example, is a technical control which is not easily modified by untrained operators. This control assists in filtering unwanted or malicious traffic on both public and private networks.

2.6.3 Operational Controls

Lastly, and arguably most importantly (Mitnick & Simon, 2002), the operational controls are those which deal with the user of an information system. An operational control is a control which governs the way users act within an organization, such as rules and requirements of secure password usage. Users choose a password unique to them, which they need in order to gain access through the technical control of logging into a particular computer system. The chosen password should follow selection methods as set out by the policies implemented by the operational controls governing password usage, such as minimum length and discovery of reasonably ”weak” passwords.

Users who choose weak passwords are likely to cause a vulnerability within the system, making it easier for an attacker to break through the technical controls by posing as a valid user. This attack would be a form of identity attack and leave the organization accusing the employee for the breach in security. If the user had provided a secure password in the first place, there would have been no vulnerability created and the information system would remain safe from attack.

For this reason, the physical and technical controls of an information security system rely heavily on the correct operation by the users within the information system (Van Niekerk & Von Solms, 2007). A door left ajar by an end user renders the physical control of the door useless. Such a user may write down their password for all to see or choose a blank password for pure convenience, rendering the technical control of requiring a password in order to gain access to a computer system ineffective in mitigating the risk of attack. Arguably, therefore, the greatest threats to information security are the users of the system (Mitnick & Simon, 2002) and for this reason, the human factor of information security needs to be addressed as a vital element in the information security process.

2.7 Conclusion

This chapter showed that information is important, not only to organizations, but also to individuals. Information was shown to be an asset, with various threats imposing risks upon it. The various risks and the mitigation of such risks were discussed, clearly demonstrating the need for protection. The protection of information and the systems which contain information is known as information security. Information security is implemented by means of controls, also known as safeguards. These deal with each aspect of security. Physical controls, such as a lock on a door, protect tangible assets associated with information systems, such as a user's laptop. Technical controls were shown to prevent unauthorized access to information systems by would-be attackers. Example implementations of such controls include firewalls, antivirus and intrusion detection systems. The operational controls dealt with the human aspect of information security, **potentially the weakest link in the protection process**.

The following chapter will discuss the human factor in information security in more detail and provide an analysis of how it is currently addressed.

Chapter 3

Information Security Education

3.1 Introduction

The previous chapter introduced the users of computer systems as one of the biggest threats to the information system within which they operate. If these users do not have the knowledge of and fail to co-operate with the protection of information assets, failure of the information security system, as a whole, is guaranteed. This fact is true for both operators within an organization as well as individuals on their own personal computer systems.

In order for humans to successfully play out their roles within an information security system, it was discussed that the users need to act securely. In order for them to act securely, they need to be educated in information security principles and act on their education during their daily operations within the computer system. Users, for the most part lack the knowledge required to act securely in their role within an information system (Van Niekerk & Von Solms, 2007).

This chapter firstly examines the role(s) humans play in the information security process(es), and shows the importance of education as an enabling factor for humans to successfully fulfil these role(s). It then discusses the current state of such education systems and why there is a need for change.

3.2 The Human Factor

It has been established that humans play a vital role in the successful deployment and operation of an information security system, both for individual computer systems and those of organizations, as they support all of the three categories of risk mitigation controls, namely physical, technical and operational controls either directly or indirectly. As they play a vital role, the question remains of how an organization or individual information system can ensure that the humans involved act securely. To act securely, the users within an information system should have sufficient knowledge of how to do so. These users should then use this knowledge daily during their interactions with the information system. Siponen (2001) agrees in saying that any user making use of computer systems, especially those connected to public networks, should be well versed in information security and have a firm understanding and awareness of the risks associated with it. Without such an understanding, they will quite likely be the weakest link in the information security system (Mitnick & Simon, 2002).

All users, whether employees within an organization or operators of individual computer systems should, therefore, be educated in order to support the information security system implemented on their computer systems. Each user within an information system plays a specific role in the system. The education system should thus cater to the needs of the user for securely fulfilling the requirements of their role in the system.

The various roles of users within an organization were outlined by Thomson and Von Solms (1998) as three main categories: Top Management, IT Personnel and the End-User.

3.2.1 Roles within an Information System

Users of information systems play different roles in their interactions with such systems; thus the content delivered by the education system should be customized to the needs of those specific roles. In so doing, users will be able to relate to the content and understand why they need to learn certain concepts. By allowing the users to draw logical links between the content taught and the job at hand, the task of learning will be less frustrating and confusing to them. In order to ascertain what to teach each user, the requirements of each of the three categories described by Thomson and Von Solms (1998) need to be evaluated.

Top Management

Top managements are concerned mostly with security policies, ensuring all IT policies are formulated and adhered to by users within their organizations. This category of user is not (usually) involved with the implementation of technical or physical controls, but is rather an overseer who ensure that these controls do exist and are, in fact, operational.

IT Personnel

IT personnel are concerned with the implementation of technical controls and other hands-on issues related to information security. They are the professionals in the industry and are the users who implement the technology: both the information systems and the controls which protect them.

The End-User

The end-user group are those users who are concerned with day-to-day operations within an organization. These are the users of the system who capture and manipulate information on a daily basis and include users within organizational information systems as well as individual computer systems. The daily operations within information systems pose a high risk to the information system; therefore, these users are where most of the education needs to be directed.

A typical end-user's education would, at the very least, contain information related to password management, selection of secure passwords as well as information related to computer viruses, risks associated with information systems and the safe usage of e-mail (Van Niekerk & Von Solms, 2007), a service over 91% percent of all online adults make use of (Lenard & Britton, 2006).

A top management user's education would involve much the same as the basic end-user training, but also extensive coverage of the organization's corporate information security policies (Van Niekerk & Von Solms, 2007).

The IT personnel should be educated more in the lines of technical controls, which neither of the other two categories would require (Van Niekerk & Von Solms, 2007). This education would include firewall implementations, intrusion detection mechanisms, early warning systems and other system design and implementation solutions to most effectively protect the information system they work with.

Having been sufficiently educated in information security and having various information security policies and controls in place are simply not sufficient. In order to support these policies and controls and to achieve some form of success, their actions should be visible in order to assess their effectiveness. In order to make the actions of such implementations visible, information security needs to become second nature for the users within an information system.

Making information security second nature is a difficult task to accomplish as most humans settle for an illusion of security, without caring about it too much more (Mitnick & Simon, 2002). In order to solve this problem and combat the "my own users are my biggest enemy" concern, organizations should cultivate an information security culture throughout the the organization (Von Solms, 2000) and amongst the users of individual computer systems.
Within organizations, it is necessary to develop an organizational-wide information security culture which will support the information security policies, procedures, methods and responsibilities of the company in such a way that information security becomes a natural aspect of the day-to-day activities of all employees of the organization (Von Solms, 2000).

3.2.2 Establishment of Information Security Culture

Information security cultures within organizations are designed to support the various information security policies and procedures put in place. This culture should be supported by an organizational-wide information security measurement system (Von Solms, 2000) providing managers with up-to-date information, allowing them to properly manage information security moment by moment.

By following a baseline code of practice (minimum measurement of guidelines and regulations), an organization can be assured that most of the security aspects that need attending to will be addressed. Implementing and following such a code of practice, ensures that an organization has the assurance that they are on par with international best practices (Von Solms, 2000) and, therefore, have peace of mind with regard to the risks associated with information systems.

No one can be 100% guaranteed of being secure and should, therefore, strive for a balance between risks and controls (Whitman & Mattord, 2003). Anyone who thinks that security products alone offer true security is settling for the illusion of security (Mitnick & Simon, 2002).

While information security culture is recognized as an essential aspect of any information security system, further research into this topic falls beyond the scope of this dissertation. Instead, **this dissertation will focus on one of the key elements for the establishment of such a culture between users of information systems, which is education.**

Information security was previously defined as a process. This was confirmed by Mitnick and Simon (2002) who quote well-known security consultant, Bruce Schneier, as saying, "Security is not a product, it's a process". In keeping up with the process, users of computer systems should be constantly made aware of the risks and challenges in securely operating within them. Constant reminders should be visible, indirectly and subconsciously triggering users to act securely in their daily operations.

3.2.3 Information Security Awareness

The art of acting securely can best be explained to people through education. In order to get the users to make use of this education, they need to understand why they need to act securely, in a way that makes sense to them in their role either as an employee within an organization or an individual user of a computer system.

Without an adequate level of user co-operation and knowledge, many security techniques are liable to be misused or misinterpreted by users (Van Niekerk & Von Solms, 2006), potentially resulting in an adequate security mechanism becoming inadequate (Siponen, 2001). When implementing their information security solutions, organizations typically focus on the technical and procedural security controls (Puhakainen, 2006), failing to appreciate the end user as their biggest threat.

From an information systems point of view, this is not enough: an effective organizational information security system requires that users are aware of and use the available security measures as described in their organizations' information security policies and instructions (Puhakainen, 2006).

As a result of the proliferation of office and home computers, applications such as antivirus and firewalls have been migrated into the realm of the everyday user, who is not necessarily a security expert (Johnston, Eloff, & Labuschagne, 2003). These users will install technical controls, such as a firewall or antivirus application, yet fail to use it properly and, therefore, render it useless.

They may be aware that they need to install them; however, they are not aware of why they need to do so or what risks they are mitigating by installing them. If they are aware of what types of websites to avoid, they will be less likely to browse these websites and, therefore, better support the technical controls of the information security system.

People as a whole need to understand that the information contained in information systems is just as important as other forms of information they consider valuable, such as that relating to their financial security. It is possible to teach and *convince* them through education; however, if users do not understand *why* they need this education, the concepts and skills learnt will more often than not be disregarded by them.

Mitnick and Simon (2002) argue that ongoing information security awareness training programmes are essential to resist and mitigate the occurrence of social engineering attacks. These attacks are specifically focused on the user not being properly educated and lacking knowledge with regard to the severity of security breaches. A caller pretending to be an IT professional within an organization can, more often than not, convince an uneducated user to provide them with their username and password; however, an educated user would be less susceptible and less likely to hand over those credentials to someone they did not know personally. Likewise, if a user knew that the disclosure of their password credentials within an organization could result in potential data losses, setting the company and themselves back many days of work, they would be far more co-operative when asked to choose secure passwords.

Awareness simply reminds the user to act securely; education is said to be an enabler to teach the users how to act securely. By way of awareness, users are constantly reminded to act securely and thus, when provided with education, are able to use this education to better the security of the information system. The problem with current information security education is that it does not focus on all users of computer systems, but rather those of organizational information systems. The rapid growth of the Internet has introduced many new vulnerabilities and threats to computer systems connected to it; therefore, current education systems may not be able to successfully educate and, hence, not prepare all users to act securely. For this reason, current approaches to information security education need to be evaluated to ascertain their value in the education of all users of computer systems world-wide.

3.3 Current Approaches to Information Security Education

Most current approaches to information security education use a continuum outlined by NIST 800-16 (1998) (see Van Niekerk and Von Solms (2007) and

Siponen (2000)). NIST 800-16 (1998) describes learning as a continuum, based on three levels of learning: awareness, training and education. The learning process in this context starts with awareness, builds to training, and evolves into education (NIST 800-16, 1998).

3.3.1 Awareness Aspect

Awareness is not training, but rather an attempt to focus the user's attention on security (NIST 800-16, 1998). This focus is generated by awareness campaigns, which include the publishing and display of posters in prominent areas, displaying thought-provoking security awareness statements such as "Are your passwords secure? You could be the victim of the next security attack!". These statements and attention-getting posters have the sole purpose of making users of computer systems aware of the risks they face on a daily basis whilst interacting with them. Any one of these users, as discussed previously, could jeopardise the critical characteristics of the information system they make use of; therefore, the promotion of awareness to security and the risks faced promotes better overall security and facilitates the creation of the all-important information security culture between users of computer systems. Once the awareness to risk of information systems has been established, the training aspect can occur, enabling users and providing them the necessary skills required in order to act securely on computer systems.

3.3.2 Training Aspect

Training is more formal than awareness, having a global goal to build knowledge and skills to facilitate job performance (NIST 800-16, 1998). The skills developed and training level provided are involved with the integration of all the security skills and competencies of the various functional specialities of information security, incorporating it into a common body of knowledge, striving to produce IT security specialists and professionals capable of vision and pro-active response (NIST 800-16, 1998). The IT security specialists trained during this process will be the users within the computer system, who implement and manage the technical controls, described in Section 2.6. These technical controls include those previously described, such as firewall or antivirus support, which mitigate various risks arising from the use of computer systems. Although users may be aware of the security risks and know how to implement controls to mitigate this risk, people still tend to brush off security as they fail to understand why information is so important to individuals and to organizations. In order to provide users with answers to why information security is so vitally important, the NIST learning continuum provides the third and final level of learning, the education level.

3.3.3 Education

The education level is concerned with answering why information security is such an important aspect in information systems. By answering the questions users may have and providing scenarios depicting data compromise and loss in a way users can relate to, these users will, over time, become convinced that information is important and once users are convinced, their buy-in to the education system will be established. By ensuring user buy-in, the learner will be able to gain the most of the education process (Van Niekerk & Von Solms, 2004) and, therefore, the education process on a whole will be significantly more successful than if the users had fought against it.

The NIST continuum, although arguably the most popular, has become somewhat dated in design. The design of the NIST learning continuum described in NIST 800-16 (1998) intends education solely to IT professionals within an organization. New developments such as the Internet and digital economy have brought new challenges in information security education as the target audiences have shifted from organization only to include all users of computer systems. The following section outlines these reasons for change more elaborately.

3.4 Reasons for Change

Users of computer systems in the past were, traditionally, adults operating within organizational computer systems. The rapid development and technical advancement of the personal computer, introducing accelerated graphics, gaming, multimedia and communication to users at home, spurred the growth of individual computer systems. These users also have information systems which need to be protected from risks, most of which prevailing from communication on public networks, such as the Internet. Researchers in the past have recognized the organizational need for information security awareness; however, have failed to see its other dimensions, such as the general public (individual computer users) (Siponen, 2001). Information security awareness should thus, in addition to organizational awareness, constitute an integral part of the general knowledge of citizens within the information society (Siponen, 2001). Individuals and organizations view information as an asset in some way and, thus, should be made aware of the various threats related to it (Siponen, 2001). These threats are more prevalent now, with the introduction of large-scale public networks such as the Internet.

The Internet provides organizations better ways to conduct their business with their business partners and suppliers, as well as providing them better connectivity and reach to their consumer base. Consumers benefit from the Internet providing easy, more convenient access to their favourite stores at better prices. The protection of organizational information systems, as well as those individual computer systems, created a change in the target audience for information security education systems.

3.4.1 Changing Target Audience

The NIST learning continuum is concerned with the educating of users primarily within an organizational context. Even so, it intends to educate only IT professionals and provide awareness to everyone else. Organizational information security awareness is no longer enough to satisfy the concerns of security; thus, additional dimensions of security need to be investigated (Siponen, 2001). These additional dimensions are based on the belief that all users of computer systems, either directly or indirectly, view information security awareness as an issue which needs to be addressed (Siponen, 2001).

It has already been argued that all users of computer systems required education in order to protect their sensitive information stores, not solely organizational users. This is based on the argument that there are at least some central information security issues that every citizen using IT services should be made aware of (Siponen, 2001). Van Niekerk and Von Solms (2004) say the target audience for current information security education systems, including those based on the NIST continuum, are adults as adults are traditionally the users of organizational information systems. These adults have well-established, not formative, values, beliefs and opinions (NIST 800-16, 1998) making them very difficult to educate using a generic ”one-size fits all” approach such as objectivist-based classroom education, which enforces set constructs of knowledge upon the learners.

In modern times, **adults are not the only users of computer systems**, but as computer graphics and interaction facilities, including communication improve, users of all ages are making use of computer systems. These users, although not necessarily operating in organizational information systems, also require education as their information is also important. The elements of information security these users require are potentially different to those required by organizational users and even then, the roles of users within an organization govern the requirements each individual within the organization needs pertaining to information security. NIST's learning continuum is, therefore, **not suitable for educating all users** of computer systems as it does not cater for the requirements of educating these users world-wide, but more often rather focuses on IT professionals within organizations.

As the requirements of information security have changed from traditionally securing organizational information systems to the inclusion of individual computer systems, so, too, must the education system used to educate users of these systems. The introduction of the Internet and the connecting of these computer systems on a shared public access facility further stresses the need for education. Without proper education, users connected to the Internet will not be ready for the risks that this new connectivity brings. With the risks, the Internet has brought about many significant advantages, such as the ability to conduct business from anywhere. This commerce which slowly evolved and, in recent years, exploded, is known as the digital economy.

3.4.2 The Digital Economy

The digital economy can be thought of as an online market place, which knows no geographic bounds or time constraints for commerce. This breaking of geographic boundaries for commerce required a large, cost-effective public network be utilized in order to act as a platform for the operation. The development of the Internet in the mid 1990s provided an answer to this problem and paved the way for the development of the digital economy.

Ironically, even as the Internet provided a suitable platform for the operations of the digital economy, it opened once individually secured networks to a host of new risks associated with public, accessible wide-area networks (WAN). By connecting their isolated computer systems to the Internet, organizations and individuals expose themselves to a world without rules and consequences for malicious activities. Even as public networks provided so many new risks, the attraction to both consumers and organizations looking to market their products online was far greater. The revolution of conducting commerce over the Internet was spurred on by organizations wanting bigger and better access to information and their customers. The growth of the digital economy showed a major impact on the United States economic performance, increasing to an annual rate of 4% in 1995-2000 from an annual rate of 2.37% at the start of the decade (Lenard & Britton, 2006).

From a consumer's point of view, it has become expected that all organizations have an online presence and are able to conduct their business there. Whilst some organizations deemed the current state of the Internet insecure and refrained from doing business online, many others followed the trend of electronic commerce with or without knowledge of the potential risks it posed to their business (Siponen, 2001). These organizations redesigned their marketing approaches to include an Internet presence and marketing budget.

The consumers also opened themselves up to risks associated with conducting commerce on the Internet. By divulging sensitive information to third parties, whose trustworthiness may not be known to them, these consumers become vulnerable to various risks, including identity theft, and may suffer losses relating to personal finance if an attacker manages to read their credit-card information. It is therefore true **that all users** of the Internet and those who pursue activities relating to the digital economy, **are at risk and need protection**.

The requirements for information security education have changed in recent years; therefore, it is paramount that the education systems which assist users in acting securely need to adapt to this change. Information security has become **more of a social responsibility** (Siponen, 2001) and information security education systems should cater for this by allowing contributions of information by the learners within the system.

Information security education has previously been based on adults operating within organizational computer systems. Times have, however, changed and the entry age of computer users has dropped significantly, with children starting to use computers around the time they start to read and write. The significant change in age of users is not the only change needing to be addressed by education systems. As computers and technology, in general, are becoming more available, so, too, is the diversity of people using these systems and connecting with the Internet. These **users have varying cultural backgrounds, specific language needs** and understandings of security and computer systems.In addition to the diversity of users, the single largest problem with current information systems, according to Puhakainen (2006), is the lack of theoretically grounded and testable concrete guidance to ensure that users are committed to fulfilling their information security mission. Mitnick and Simon (2002) outline that the goal of information security awareness training programmes is to influence people to change their behaviour and attitudes by motivating employees to protect the information assets of the company. For these reasons, a new education system needs to be developed, in order to accommodate these and other problems. This new system should be considered from the ground up, starting by analyzing the requirements for education for each user.

3.5 What Should be Taught

It has already been established that every user within a computer system has individual needs for information security education, based on the role played in such a system. There should be a classification of what is relevant and what is irrelevant pertaining to content taught to each of these target groups of users (Siponen, 2001). To define a common education curriculum, which would be applicable for all users with any role, would be near impossible. It is, however, possible and recommended to look to standards and best practices, which exist in order to help identify the essential content for an effective information security management system. Such standards include the ISO/IEC 17799 standards as the preferred approach in introducing information security to an organization (Van Niekerk & Von Solms, 2007) and, therefore, provide study content pertinent to the controls and procedures it brings with it.

For general end-users, including users of individual computer systems, the concern should not be related to the technical implementation of controls, but rather the awareness of its existence and the role they play in supporting it. The increasing number of home Internet users and organizational end-users with little knowledge of information security concepts may cause damage through careless use, such as the accidental distribution of computer viruses (Siponen, 2001). These users should be made aware of these problems as well as simple compromises of information, such as dumpster-diving, which describes the process whereby attackers will dive in dumpsters and trash in order to gain access to certain potentially sensitive printed information, which has been discarded. If employees were aware of these practices, they may be more inclined to support the procedure of shredding such information prior to throwing it out.

In order to effectively relay this knowledge to users, it is important to establish the best possible methods for educating them in information security concepts. The following section discusses this process in more detail.

3.6 How Users Should be Taught

The way users are taught **should be guided by educational theory** (Soloway et al., 1996). Soloway et al. (1996) describe the dominant educational paradigm as currently being "didactic instruction", where learning is viewed as an information transmission process. This process is described as teachers having the information and students lacking it. The teachers' lectures serve to move information they have into the heads of students (Soloway et al., 1996). In contrast to this educational paradigm, new educational reform movements are advocating for students to be actively engaged in the learning process, facilitating informal learning by allowing learners to construct their own understanding and meanings of information, not simply just receiving it (Soloway et al., 1996). Soloway et al. (1996) describes three unique needs of learners which must be catered for in the education environment: growth, diversity and motivation.

3.6.1 Unique Needs of Learners

Growth

The primary objective of educational systems is described by Soloway et al. (1996) as the promotion of the development of expertise of the learner. This means that rather than simply allowing the learner to perform tasks which may have no means of imparting knowledge to the learning, the system should support "learning while doing" (Soloway et al., 1996) ensuring the learner gets the most out of the educational experience.

Diversity

It was discussed that users of computer systems have different roles to play in computer systems, have developmental and cultural differences and prior knowledge of certain concepts. These differences amongst users play a major role in the suitability of materials for learners (Soloway et al., 1996); therefore, these differences should be addressed by the system in order to ensure its effectiveness.

Motivation

IT professionals partake in educational programmes in order to expand their technical knowledge and understanding of information systems. In contrast to the IT professional education, with learners such as end-users and individuals, initial interest and continuing engagement cannot be taken for granted (Soloway et al., 1996). Motivation of such individuals plays a large part in ensuring their support of information security education, which to them may not seem necessary or top of the agenda. By changing their perception of information security, these individuals will become motivated and view information security as a serious matter, the way it should be viewed.

The basic requirements for learning have been discussed. The following section describes the requirements specific to an information security education system.

3.6.2 Information Security Education Requirements

In order to establish a successful information security education system, certain requirements must be met. One such requirement is that **all learners should be able to pass the course** (Van Niekerk & Von Solms, 2004). Van Niekerk and Von Solms (2004) assert that in traditional education systems, there is usually a percentage of learners who fail to meet the assessment criteria and, therefore, fail the course. This is not acceptable for information security systems as a single user, who does not act securely in their role within the information system, may jeopardize the entire security system. For this reason, the **learning material presented to the learner should be customized** in a way which best meets their own personal learning requirements, thereby enhancing their chance of successfully completing the course. In order to assist the learner in finding areas of poor understanding, the system should **provide the learner with feedback** on a continual basis, assisting learners in gauging their competency within various aspects (Van Niekerk & Von Solms, 2004). The system should be able to track this progress with each learner and, therefore, **hold them accountable for their studies**, **making them responsible for their own education** (Van Niekerk & Von Solms, 2004).

In the current corporate world, it would be difficult to present information security education in classrooms. One could thus argue that one other major requirement for information security education systems is their **accessibility at anytime, from anyplace**. One of the major problems with existing education systems is they require learners to access them at a particular date and time, often causing an interruption in the learner's work or home environment. An education system which is to succeed in educating all users of computer systems should be accessible at anytime and anyplace to ensure that everyone's schedule is accommodated; therefore, allowing the learner access to the learning content at times which best suit them.

3.7 Conclusion

This chapter reiterated that people are the weakest link in the information security process within organizational and individual computer systems. In order to address this issue, it was discussed that the behaviour of users needed to change; this is possible through the development of information security culture. One of the keys to empowering users to develop such a culture is education.

Many current information security education systems are based on a learning continuum as set out by NIST. This type of system is not suitable for future information security learners as the changing target audience is steering away from solely adults to incorporating all users of computer systems. These include children, who have just began to read and write, surfing the Web at home. The introduction of individual or home computer systems to the information security requirement poses additional problems as the growth of the digital economy encourages more users to connect to the Internet.

Thus, information security education systems need to be revamped in order to sufficiently educate all users of computer systems world-wide. Learners have various requirements for learning which were discussed, citing motivation as a key factor for success. The requirements of information security education systems were discussed, promoting the trend from traditional classroom education, controlled by educators, to learner-centric education environments, where the learner drives the education process.

The Web was identified as a possible solution to the problems associated with current information security systems. The development of Web-based learning systems has increased significantly in recent years and should thus be investigated for suitability for information security education.

The following chapter first describes various learning methodologies in order to ascertain which is most suitable for information security education, if it is to move away from classroom-based education. Following this, the Web is discussed as a solution to the implementation of the new information security education system.

Chapter 4

Review of Current Learning

4.1 Introduction

The previous chapter identified the people within an information system as its greatest threat. For this reason, it was established that these users should be educated to change their behaviour in order to develop a culture. Traditional information security education systems were found to be inadequate for educating the current market of computer users, as these are based on adults within organizations and the target audience has changed to users of all ages, not only in organizations but at home.

Thus, this chapter attempts to set out the basis for a new information security education system, suitable for educating all users of computer systems world wide. It does so by first examining traditional learning methods, in order to determine how best to educate learners. The evaluation of Web-based technologies as suitable candidates as a platform for building such an education system follows closely after.

4.2 Traditional Learning Methods

Education is nothing new to the world, with even the earliest of human beings passing on knowledge from generation to generation in some form or another, albeit by the spoken word or drawings on cave walls. Education has come a long way since then, and many learning methods have been discovered which assist in providing a methodology as to how learning should occur, leaving the implementation of such methods up to course developers.Khalifa and Lam (2002) identified the main learning methods as objectivism, constructivism, collaboratism, cognitive information processing and socio-culturalism. The most popular of these learning methods are described in the following section, the result of which assisting in the identification of learning methods which will most effectively educate users in information security.

4.2.1 Objectivism

Objectivism is the first of the learning methods described and is arguably the most popular to date, dominating the field of education for several years (Vrasidas, 2000). The majority of traditional approaches to education, based on behavioristic and cognitive theories, share philosophical assumptions that are fundamentals within objectivism learning theory (Vrasidas, 2000). These traditional educational methods typically focus on teachers instructing and learners complying. The teacher is often a knowledgable expert in the field of study, who conveys knowledge to a classroom full of less-knowledgeable students and believes there is only one true and correct understanding of any topic (Vrasidas, 2000). The teacher is, therefore, the most active during the learning process, with students having little or no communication amongst themselves during the process. The teacher is responsible for the course design and is, therefore, tasked with what the learner needs to know, designing the course to effectively transfer objective knowledge into the learner's head (Vrasidas, 2000). This knowledge, or study content, is then broken into various modules, increasing in difficulty as the course progresses.

The way the coursework is presented **provides little room for deviation in terms of presentation, but rather the content is presented in a generic format**, not catering to learners and their individual learning styles. An analogy of the way computers operate relates, in that all computers transfer information amongst themselves in the same format. In order to gauge the effectiveness of the learning process on the individual, the teacher will run a series of tests at various stages of the course, showing which learners are grasping the concepts taught and which are not.

4.2.2 Constructivism

From a philosophical perspective, constructivism can be seen as a counterpoint to objectivism, on the opposite end of the continuum (Vrasidas, 2000). Constructivism allows the **learner to build their own internal representation of knowledge, based on his or her own experiences** (Ashcraft, Treadwell, & Kumar, 2008). This knowledge is open for change on a constant basis, with the knowledge base changing as the learner acquires further knowledge during their experiences within the subject domain. As new knowledge is acquired, its linkages and structure change to accommodate the new information being stored.

This custom structure of knowledge building provides insight into another belief of Constructivism, that there is not only a single correct answer, but rather multiple truths and realities (Vrasidas, 2000) and that education should be encouraging multiple perspectives. The real world sets boundaries, between which these truths and realities are built (Vrasidas, 2000), allowing for the negotiation and construction of multiple perspectives of concepts.

The fact that constructivism does not necessarily follow structured learning methods, such as in objectivist theory, does not mean it should not be confused with other "unguided", pure discovery educational methodologies argues Ashcraft et al. (2008), who say that these claims are made by those who misunderstand the theory: constructivist teachers do not expect learners to reinvent science, but rather guide them in drawing knowledge from themselves. This process of allowing the learner to develop their own knowledge makes constructivism, unlike objectivism, a learner-centric methodology. This learner centric methodology allows learners to construct their own knowledge of the world through assimilation and accommodation (Liaw, 2001). The teacher within a constructivist learning environment should structure the learning process so that he or she becomes a "co-constructor" of the knowledge being constructed by the learner, thus forming a partnership between both the student and the teacher (Cook, 2006).

As learners construct their own knowledge, it should be apparent that certain learners have more insight into various concepts than others. Vrasidas

(2000) states that as a characteristic of the constructivist pedagogy, the teachers do not assume that all learners need to learn the same material and, therefore, steer away from the traditional teacher role, into more of a facilitator role, ensuring the students have everything they need in order to complete their studies.

4.2.3 Collaborativism

Collaborativism is a learning methodology which promotes the collaboration amongst peers within the education process. Constructivism and collaborativism are two closely related learning methods, both being learner-centric (Hardless & Nulden, 1999), allowing learners to construct their own knowledge, rather than have a generic understanding enforced upon them.

Constructivism allows users to take in knowledge from their own experiences and store it in a way which best suits them as individuals. The collaborativist model differs from constructivism by **focusing on learning as a result of group interactions amongst peers**, rather than solely individualized understandings. Having peers to discuss information related to the subject matter is argued by the promoters of this learning method as an essential asset to learners. By communicating their thoughts within the group, learners create a shared understanding (Hardless & Nulden, 1999), all the while improving their listening and communication skills. This communication forms the base of Collaborativism which promotes active participation within the group (Hardless & Nulden, 1999).

Not all learners, however, exhibit characteristics which would make them active in a group; certain learners may feel the need to remain passive. Passive learners will not benefit from such interactions as much as active learners; therefore, all learners should be motivated and engaged, having the instructors support, rather than control, the learning process. This engagement and support by instructors affords learners the opportunity to discuss their views of the subject with their peers, receiving immediate feedback on their thoughts and viewpoints. This discussion and feedback process assists learners in the assimilation of the knowledge they construct and strengthens their standpoint as they often have a better understanding of the subject after explaining it to someone else.

4.2.4 Socio-Culturalism

Soloway et al. (1996) describe socio-culturalism as a central notion that learning is enculturation, the process by which learners become collaborative meaning-makers among a group defined by common practices, language, use of tools, values, beliefs, and so on. The educational process is, therefore, not only within the minds of the learners, but also in their bodies and in their surroundings. Aspects such as the culture of the learner, their immediate surroundings and, to some degree, the language they speak help to shape the knowledge they construct. These knowledge constructs are developed and stored in settings of joint activity; therefore, socio-culturalism closely relates to the collaborativist learner method. The use of peers and surroundings in education is encouraged in order for learners to construct their own opinion and understanding of the subject domain.

The construction of knowledge using socio-culturalism leads to a new method of educating learners, known as socio-constructivism (Soloway et al., 1996). Socio-constructivism, therefore, allows for the provision of guidelines for the design of learning environments and the scaffolding (Soloway et al., 1996) that support both the socio-culturist, collaborativist and constructivist learning theories.

4.2.5 Evaluation of Learning Methods

It could be argued, based on the information provided in this section, that objectivism as a learning method for information security education systems will not work efficiently as it does not solve many of the problems already associated with current education systems. One such problem, identified in the previous chapter, is that users of computer systems have different roles to play; thus, the knowledge taught to the learner should be pertinent to their field of operation. Using the objectivist approach, a generic knowledge construct would be taught to all users, even those who do necessarily need to know it. If humans cannot relate the knowledge they are being taught to their own experiences, they will become annoyed and act against the education, rather than support it. Objectivism has another problem; for objectivism to occur, classes need to be scheduled in order for teachers to present the courses they designed. These classes will not be able to fit into the schedules of all users of computer systems; therefore, many users will miss out on the education. The audience for a world-wide information security education system was shown to be of all ages; therefore, making it very difficult if not impossible, to produce a single syllabus of generic construct, catering to the individual needs of each user of computer systems.

The constructivist approach, being learner-centric, is far more accommodating to the differing age groups, learning speeds of individuals and the roles the users play within computer systems. Learners are able to pace themselves and their learning, forming their own constructs and building their own understandings and perceptions around information security concepts.

The collaborativist approach too has many advantages as a learning method for information security education systems. These advantages include allowing discussions of various security-related issues amongst peers who have different view points. These discussions promote the social aspects of learning, which are important to the successful education of learners (Mejias, 2008). Siponen (2001) says that information security researchers are likely to be helpful in providing information concerning security issues which other learners of information security can use. The sharing of information between information security people has so far been ineffective, however, in spite of that fact that such sharing promotes possibilities for synergism (such as shared goals) (Siponen, 2001).

The socio-culturalism learning method provides a means for learners to look past the text books and into their own experiences and backgrounds for knowledge construction. This process has the benefit of applying real-world scenarios and experiences to the learning environment, allowing the learner to grasp the contents of the educational programme far more efficiently, as they are able to relate various concepts to their own experiences.

Thus, the socio-constructivist learning method proves to be the most appropriate learning method to implement in an information security education programme, as it includes the best elements of constructivism and collaborativism all the while considering socio-culturalist aspects of education. The socio-culturalist and collaborativist methods of learning are important as they promote informal methods for learning. Such informal methods are important as 80% to 90% of all learning has been attributed to learning occurring informally outside of the classroom (Schlenker, 2008). Objectivist courses, such as traditional classroom environments, follow formal methodologies for course design, missing out on the important informal aspects. Many existing information security education systems are based on objectivist learning theory and fail to pay attention to the informal aspects of learning. The following section presents a discussion of existing information security education systems, their benefits, downfalls and areas which require improvement.

4.3 Web-Based Education Systems

A basic understanding of learning has been laid out in the previous sections, showing models and methods which have been tried and tested within the educational sector over past years. These models and methods have been shown to be quite dated in terms of information security education, which has since grown to include a need to be extended to all users of computer systems, world-wide. This need for world wide education has encouraged developers of educational system to make use of the Internet as a viable platform for the delivery of educational facilities to users, independent of their location in the world. The Web-based delivery of educational facilities has long been a viable alternative to traditional education and is, therefore, by no means in its infancy as an instructional delivery platform. The electronic learning environment, or e-Learning, is an alternative concept to the traditional tutoring system (Gladun, Rogushina, Garcia-Sanchez, Martinez-Bejar, & Fernandez-Breis, 2009), which allows learners to free themselves from the stereotypical classroom environment, allowing them the opportunity to learn when they want and what they want. The standardization of initiatives for learning technologies by the Learning Technology Standards Committee (LTSC) has caused the growth of these e-Learning systems to become more widespread and accepted methods of educating learners (Gladun et al., 2009). Previously, e-Learning systems consisted of static information captured by the teacher and presented to the learners in one or more formats. These systems, often based on objectivist learning theory, presented little or no way to customize the learning experience, based on the learner's socio-cultural background. These systems were also very disconnected and distributed in nature, making it hard for learners to follow the course and find references to other related information.

The disjointedness of the educational systems on the Web has been addressed by the introduction of "hypermedia", a concept which offers a multimedia information environment, supports non-linear access to information, and provides a means of interaction with the user, all the while integrating the various information formats into a common display (Liaw, 2001; Donnelly, 2008). Hypermedia is described by Donnelly (2008) as a development which took hypertext's simple, established concept of linking from one text page on the Internet to related pages and extended it beyond the passive exercise of reading words on the digital page. This new linking and enhanced interface design, by the inclusion of multimedia and other attention-getting features, promoted the rapid migration of educational systems to hypermedia-based applications (Liaw, 2001).

These new educational systems' advancements have continued to grow, all the while improving the quality and standards of e-Learning systems. The following section shows the progression of Web-based education systems in more detail.

4.4 Progression of Web-Based Education

Technology and schools have not always been the best of friends, with many failed attempts to introduce technology in the past through innovative technology (Clarke, 2002) causing more harm than good. Technology has, however, since become more visible in today's educational institutions with the latest in developments helping to overcome many boundaries experienced by existing education systems. These developments of e-Learning are depicted by Clarke (2002) on a basic time-line.

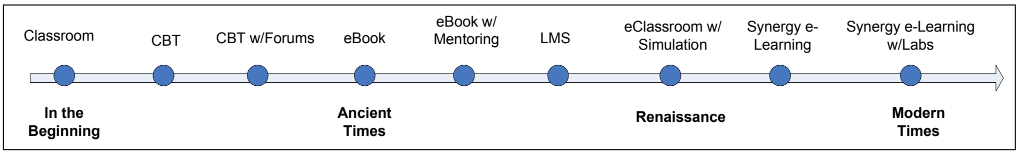


Figure 4.1: The e-Learning Timeline as Depicted by Clarke (2002)

4.4.1 Computer-Based Training

Computer Based Training (CBT) has been in existence for over ten years Clarke (2002) (see Apple Computers ”Hypercard” learning system introduced to schools in 1987 (Donnelly, 2008)); however, it is only listed on the timeline at the time it became Internet aware. This system consists of a one-dimensional study guide on CD-ROM disk with access to instructors and other students via Internet forums (Clarke, 2002). This form of early e-Learning was also referred to as ”Blended learning”, which describes the use of both Web-based and classroom instruction to study a particular subject (Donnelly, 2008).

4.4.2 e-Book (Online CBT)

The rapid growth of the Internet and the development of the World Wide Web (WWW) sparked CBT companies to race to stream their Electronic Books (e-Books) over the Internet (Clarke, 2002). The actual content of such training material did not improve (Clarke, 2002); however, the material became more accessible for all learners to access than traditional CBT learning material. Since the e-Books are downloaded and often read by individuals outside of a group learning environment, people using these environments often feel isolated and remote (Wahlstedt, Samuli, & Marketta, 2008), consequently their learning experience is hindered. In order to combat this problem, it became apparent that a learning system offers some form of social interaction amongst the learners and instructors.

4.4.3 e-Book with Mentoring

A few pioneering e-Learning providers decided to add network-based interactivity and coaching - ”mentoring” to their standard e-Book learning platforms (Clarke, 2002). This mentoring solved some of the basic problems identified with e-Book learning methods, becoming a critical aspect for any successful e-Learning program, due to it providing otherwise isolated online students with a chance to interact with each other in real time (Clarke, 2002).

4.4.4 Learning Management Systems (LMS)

The development of e-Learning systems has, in the past, been hindered by the high cost of developing the systems and building the content for them (Clarke, 2002). This problem was solved a few years back when a few ex-Oracle employees developed an Enterprise Resource Planning (ERP) system for learning (Clarke, 2002). This system was the first off-the-shelf e-Learning software platform, which could be purchased, installed and propagated with content related to various subject domains. These systems allowed learners to register, track their skills and report back on their progress (Clarke, 2002), an important aspect for any learning system (Van Niekerk & Von Solms, 2004).

4.4.5 e-Classroom with Simulation

Traditional classroom environments, as outlined previously, have served their purpose for many years as the standard for educating learners (see section 4.2). While many companies spent their time developing LMS software solutions, some began to develop systems to bridge the learning chasm between traditional classroom environment and web-based learning - the ”e-Classroom” was born (Clarke, 2002). e-Classrooms today provide the sceptic e-Learning adopters with the comfort of a traditional classroom environment via the Web (Clarke, 2002). These classrooms do, however, violate one of the most important aspects of e-Learning, the anytime, anywhere concept (Clarke, 2002), as they are scheduled training sessions presented online by an instructor to a virtual classroom of online learners.

4.4.6 Synergy e-Learning with Live Labs

It can be argued that this form of e-Learning is the most advanced learning technology to date (Clarke, 2002). The success of this e-Learning environment can be attributed to the combination of three key elements which Clarke (2002) describes as necessary for successful e-Learning programs. These include **prescriptive assessment**, the personalization of the lesson plans, enabling each learner to work at their own pace and only cover knowledge that they need to know (Clarke, 2002). The **provision of hands-on tasks** and activities (Live Labs), enabling a performance-based approach to learning is integrated, allowing learners to demonstrate their understanding of the knowledge (Clarke, 2002).

Motivation was found to be an essential element in successful learning systems; therefore, the use of **multi-sensory learning tools** help keep the learner engaged in the education process, thereby improving retention of information taught to them (Clarke, 2002). The use of such multi-sensory tools in order to retain focus and attention on the education experience is expressed by NIST 800-16 (1998) as one of the requirements for successful learning programs.

The Synergy e-Learning approach is learner-centric (Clarke, 2002), allowing the learner to build their own knowledge. By allowing the learner to practice assimilation of the knowledge constructs in their own way is far more effective in education than teacher-centric approaches, inspired by objectivist learning methods (Khalifa & Lam, 2002).

In order for these e-Learning systems to be structured around the learner, it is necessary for both the content and the interface to dynamically adapt to the learner. Current trends in Web development have also recently focused on the customization of Web pages to the individual user, who is further enticed to view the site if they gain a sense of customization. Educational systems addressed this need by incorporating adaptive and intelligent features into their design, providing a new form of e-Learning - Adaptive and Intelligent e-Learning.

4.5 Adaptive and Intelligent Web-Based Educational Systems

In order for Web-based education to support constructivist learning methods, it needs to implement features to promote such learning paradigms, such as the adaption of the system to the learner. Gladun et al. (2009) further promote this element saying that e-learning systems should emphasize engaging students in the learning process by adapting to the individual learner. Adaptive and intelligent features attempt to make Web applications more customized to the user by building a model of the goals, preferences and knowledge of each individual learner and using this model throughout the interaction with them in order to facilitate their specific needs (Brusilovsky & Peylo, 2003). By considering and implementing such features, the e-Learning system solves the problem of adapting content and presentation aspects of the learning environment to the learner. Systems which exhibit such functionality are more intelligent than other forms of e-Learning systems, by performing activities traditionally executed by a human instructor, such as coaching learners and diagnosing their misconceptions (Brusilovsky & Peylo, 2003). Although adaptive and intelligent features operate well together, they can also exist as stand-alone systems, existing as adaptive Web-based educational systems and intelligent Web-based educational systems respectively (Brusilovsky & Peylo, 2003).

4.5.1 Adaptive Features

Adaptivity within e-Learning systems usually begins with the user attempting to externalize their views on a particular concept or subject domain, however tentative these may be (Hay, 2008). These cognitions are then represented in a student model, which stores preferences for learning and current knowledge the learner has regarding the context of education. The current knowledge and learner preferences serve as the starting point for the system in content selection and interface presentation techniques (Brusilovsky & Peylo, 2003). While the system interacts with the learner, the student model is currently updated as the learner gains further knowledge and more about the learner's individual learning style is understood. By taking into account these preferences the learner has for learning, the system is able to offer an adaptive presentation of the content, displaying it in a format best conducive for learning for the particular learner (Brusilovsky & Peylo, 2003). As the student continues to learn, the student model is updated with the new knowledge so that the system will present new knowledge, based on goals and the current knowledge the learner has within the subject context (Brusilovsky & Peylo, 2003).

The modelling process is, thus, an important aspect (Froschl, 2005), in that it accommodates learners who have certain learning styles, multiple intelligences, culture, prior knowledge, media preferences and differing social contexts (Sims, 2008).Hay (2008) describes the modelling process as the facilitation and recording of the outcomes of cognitive processes that underpin personal understanding. In analyzing the student model, the system is able to provide links to other related information which may be of interest to the learner. This process, known as adaptive navigation, assists the learner in hyperspace orientation and navigation by changing the appearance of visible links, making it easier to know where to go next (Brusilovsky & Peylo, 2003).

The driving force to the development of these systems is spurred on by an interest to provide distance education over the Web (Brusilovsky & Peylo, 2003)

4.5.2 Intelligent Features

Intelligent features' support allow systems to apply techniques from the field of Artificial Intelligence (AI) to provide broader and better support for the learners in Web-based educational systems (Brusilovsky & Peylo, 2003). These features include curriculum sequencing, intelligent-solution analysis and problem-solving support. These features and the roles they play in e-Learning systems are discussed in the following section.

Intelligent Curriculum Sequencing

Intelligent curriculum sequencing attempts to guide students in the right direction of their studies, helping them to find the optimal path (Brusilovsky

& Peylo, 2003) through the learning material. By making use of adaptive navigation support, described in Section 4.5, learners are guided through the learning process in the direction best matching their goals as described in the student model.

Intelligent-Solution Analysis

Intelligent-solution analysis deals with the learner's solution to a problem (Brusilovsky & Peylo, 2003), more specifically, it acts as an intelligent analyzer for the solution. This analyzer, unlike non-intelligent checkers, which more often than not can only tell right or wrong, provides the learner with extensive error feedback and automatically updates the student model with new information (Brusilovsky & Peylo, 2003). This feature allows the system to show the in-depth workings of students on problems which usually could not be shown. By providing insight into the problem-solving ability of students, the educators are able to spot and quickly correct any problems in the way of thinking utilized by the student.

Problem-Solving Support

Interactive problem-solving support simply offers the learner intelligent help on each step of the problem-solving process, by providing hints and/or executing the next step in the process for the learner (Brusilovsky & Peylo, 2003). This facility does not aim to solve the problem for the learner, but rather act as a co-constructor of knowledge in that it provides the learner with a point of reference when stumped.

4.6 Evaluation of Web-Based Education

4.6.1 Potential Problems

Although much work has gone into e-Learning systems, some problems still exist. Some of the issues relating to Web-based education are described in the following section.

Content is Dumbed Down

It has been argued by some that e-Learning systems ”dumb down” certain vital text-based content with an exorbitant amount of attention-getting features provided by hypermedia (Donnelly, 2008), in favour of keeping the learner’s attention. This provision of an overly rich presentation factor may infact impair the learning experience as many of the vital points are potentially masked from the learner’s view, thereby creating a counter-productive learning environment.

Accessibility anytime, anywhere

One of the advantages of e-Learning systems is their ability to be deployed on environments, such as the Internet, which allow easy access for learners. These systems, for maximum efficiency and effectiveness, should be accessible anytime, anywhere. Many e-Learning systems deployed do not cater to this need, as the systems are stashed on a highly firewalled company intranet and not exposed to public networks. This means learners are only able to access the educational content when they are at work or connected via Virtual Private Networks (VPN), which are not always available.

Lack of social interaction amongst learners

The social interaction with other learners, such as is available within a traditional classroom environment, has been noted as important for learning; therefore, e-Learning systems should be perceived as a place where social interaction is supported (Wahlstedt et al., 2008). Currently, very few e-Learning systems support this kind of social interaction amongst learners in a way which supports collaborative education.

Timely and accurate creation of content model

The time spent by teachers and moderators in e-Learning courses is critical and costly in resources (Gladun et al., 2009). Care should be taken to ensure that the e-Learning platforms chosen by the developers are based on constructivist learning theory, allowing the learner to drive the education process. In order to build an information security education system, based on socio-constructivist learning theory with adaptive and intelligent features, an extensive and accurate knowledge base is required, containing various principles and concepts from within the subject domain. It is from this knowledge base that content models are built, to which the student model is compared for learner evaluation purposes. The development, storage and transport of the knowledge base needs to be addressed as a critical factor in any successful educational system. This is not true for most current e-Learning systems which exhibit generic, centralized knowledge stores in a proprietary format, not suitable for sharing. This limits the creation of additional content by external sources, which could add to the value of the stored knowledge.

Do not address the lack of motivation for study

On a whole, general hypermedia e-Learning systems do not motivate the learner to study, but simply present the content in an eye-catching format. Although the presentation aspect of e-Learning systems is important, motivation has been found to be an essential element for the educating of learners. In ensuring motivation, the system often gets the learner to buy-in to the program, further ensuring its success.

An e-Learning-based information security education system will need to address these and other potential problems if it is to be truly successful in educating all users of computer systems around the world. This system will also need to draw from and leverage the benefits associated with Web-based education, discussed in the following section.

4.6.2 Benefits

E-Learning, although having potential problems, solves many of the drawbacks identified in traditional classroom environments. Its advantages are that:

- Allows the learner to structure their learning approach
- Allows learners to pursue cross-references
- Remembers various aspects of the learning session
- Saves company time and money on training

- Allows access to the environment anytime, anywhere
- Encourages a higher quality of participant interactions
- Allows a view into a student's learning process.

Allow the Learner to Structure their Learning Approach and Pursue Cross References

Using technologies described in Sections 4.5 and 4.5.1, e-Learning systems allow the learner to structure their learning approach and to decide the path to follow in their educational process. This supporting, rather than dictating, direction to the learner falls in line with the requirements for a learner-centric education system. This learner-centric environment provides learners the opportunity to construct their own knowledge of the subject. This assimilation process by the learner ensures that the knowledge is stored in a way which best benefits the learner and falls in line with their own ontological beliefs. See Liaw (2001) for more information.

To Remember Various Aspects of the Learning Session

By developing student models for individual learners and groups of learners, the system is able to adapt to the preferences of the group or the particular learner. These models are able to be stored, thereby remembering the preferences for further education courses or gauging the development progress of the learner at a later date.

Saves Company Time and Money on Training - Anytime, Anywhere

One of the largest selling points of Web-based education is its ability to be undertaken anytime and at anyplace. This feature means companies need no longer have their employees physically leave work in order to be educated. Instead, with advances in communication such as the Internet, employees and individuals are able to access these education facilities at their own discretion and in their own time.

Encourages a Higher Quality of Participant Interactions

The use of hypermedia stimulates the senses of the learner more than a traditional textbook did in the past. By appealing to more senses simultaneously, it promises a richer intellectual experience through a deeper engagement with technology and the experience it can deliver (Donnelly, 2008). This increased stimulation aids in the motivation of the learner to learn and, therefore, increases the effectiveness of the education process as a whole. The motivation of learners within an education system is important, as described by the National Institute of Standards and Technology (NIST) IT Security Training requirement's document, which requires that security awareness and training presentations should be designed with the recognition that learners practice acclimation, or a tendency to tune-out if the stimulus or "attention-getter" is used repeatedly (NIST 800-16, 1998). The presentation aspect of Web-based education systems should, therefore, be ongoing, creative and motivational with the focus on the learner to consciously start incorporating new knowledge into their existing behavioural pattern by way of assimilation (NIST 800-16, 1998).

Furthermore, by allowing the learners of the system of all levels of understanding access to build the content on the educational system, one of the fundamental problems with e-Learning systems is solved - the creation of content and course work. A single individual or even a team of individuals employed on a full-time basis to create course work will never come close to creating content as quickly and accurately as the combination of the millions of IT professionals, end users and experts who would potentially participate in a shared education environment. Rather than compete with their own individual educational products, organizations would be hard pressed not to find it fit to collaborate in a shared educational environment, which will be far less budget intensive and offer a far greater level of experience and thinking than their own, limited content system.

Allows View into a Students Learning Process

Hay (2008) mentions another benefit is it allows teachers to look into a student's learning process. This facility promotes the use of intelligent solution analyzers, such as those described in Section 4.5.1. Much the same way, learners are encouraged to show their workings in mathematical sciences, now all learners' understanding of any subject can be broken down to "show the workings", previously not possible in traditional classroom-based education. This benefit further allows the system to automatically assist and correct the learner during the problem-solving phase, rather than simply giving a "wrong" answer.

These are just some of the benefits of Web-based education. The consequent applications of all multimedia and simulation technologies, computer-mediated communication and communities and Internet-based support for individual and distance learning have the potential for revolutionary improvements in education (Gladun et al., 2009). The growth of the e-Learning industry on a whole has been increasing substantially over the past few years and is foreseen to continue to rise. In order for Web-based educational systems to successfully fulfil the role of the information security education system of the future, it should be shown as an emergent technology, gaining more acceptance and development as time goes on, rather than showing signs of rapid decline. The following section describes findings within various surveys which illustrate the growth of these systems in more detail.

4.6.3 Growth of Application and Acceptance

E-Learning is currently gaining acceptance in the world as a suitable education platform, with 75% of respondents to a recent survey performed by the e-Learning Guild believing the term "e-Learning" serves a purpose and is here to stay for the foreseeable future (Guild, 2006). The number of online courses available on the Internet is growing rapidly, making e-Learning a growing business (Gladun et al., 2009). The report by Guild (2006) saw an increase in focus on both content quality and rapid development, as well as the development of the resources that make better, faster e-Learning possible (Guild, 2006) than the report by Massy (2002), which stated 61% of all respondents rated the overall quality of e-Learning negatively - as "fair" or "poor". 19% of the respondents in the first survey agreed that the term e-Learning has decreasing relevance and will begin to disappear in the year ahead, while in the most recent survey, this number dropped to 16% (Guild, 2006). Between

the surveys conducted however, Guild (2006) reported that the number of respondents stayed consistent with their beliefs that ”e-Learning” has a place in the vocabulary of the community. One of the questions posed to the respondents in the Guild (2006) survey was with regard to which e-Learning objectives will be the highest priority for the respondents' organizations in 2006. The improving of the quality of e-Learning content was first, with 33%, followed closely by the extending the global reach of the e-Learning content with 21% (Guild, 2006).
It can therefore be stated that e-Learning systems need work in the quality of their content and in their global reach. If e-learning is found to be a suitable platform for the development of an information security system, it will need to address the issues found in these and other surveys. For more information, see Guild (2006) and Massy (2002).

It has been shown that e-Learning systems are gaining momentum as the future delivery platforms for educational activities. These e-Learning approaches should be evaluated in order to ascertain their usefulness in information security education.

4.7 e-Learning-Based Information Security Education Systems

The use of hypermedia encourages user participation in education by breaking through the boundaries of text, audio and video by appealing to more of the senses, whilst all the while offering a richer intellectual experience through deeper engagement with technology and the experience it can deliver (Donnelly, 2008). By using hypermedia in combination with the Internet, learners are able to tap into a global community, a world-wide web of teachers and learners to expand their educational horizons (Donnelly, 2008). The access to this global community is on the increase, according to statistics compiled by Watson and Ryan (2006) as cited by Donnelly (2008), it continues to grow rapidly and benefits learners by removing the constraints of time and place. In order for e-Learning systems to be properly evaluated for use within an information security education context, they should be checked against and their benefits married to the requirements of an information security education system.

4.7.1 Suitability of Hypermedia-Based Education Systems for Information Security Education

The requirements of a successful information security education system need to be compared against the features of a hypermedia-based education system to justify its use as a suitable education system. Van Niekerk and Von Solms (2004) described the following points:

- All learners should be able to pass the course
- All learners should understand why
- Learning materials should be customized
- Learners should be responsible for their own learning
- Learners should be accountable for their studies
- Learners should receive feedback

This section discusses these headings in more detail in order to ascertain the effectiveness of Web-based education for information security education.

All Learners Should be Able to Pass the Course

It has been argued that all learners in an information security education system should be able to pass the course. As e-Learning course assessment is ongoing, rather than a final exam at the end, the system is able to revisit various problem areas for users who battle to grasp a concept. These concepts can be replayed to the user, over and over, in a variety of formats and displays. This will continue until the system determines that the knowledge of the learner matches that which they should know. Learning control needs the comparison between the learner's knowledge base (learner model), which is modified as the learning process evolves, with the course-domain knowledge base (content model) (Gladun et al., 2009).

All Learners Should Understand Why

An e-Learning system, unlike its human counterparts, is not impatient. The knowledge being conveyed to the learner by the system can be explained in detail, with the system drawing inference from the learner's own experiences in order to best explain the concept. This socio-cultural approach to learning assists the learner in developing metaphoric analogies for information security principles with their current understandings. The learner is able to interact with the system, ask questions and get answers. The learning process proposed for application in information security education should be based on the constructivist approach to learning, in that the whole learning experience is learner centric. This, as described in Section 4.2.1, allows the user to build their own understanding regarding a particular subject area as opposed to having the information taught to them parrot fashion. Understanding is a key aspect in assisting learners ascertain why certain principles and controls exist and how they aid in the protection of computer systems.

Learning Materials Should be Customized

With the advent of adaptive e-Learning technologies, the e-Learning system builds models of the learner, mapping their existing knowledge against a model of what they are supposed to know. The system constantly interrogates both models, student and content, to ensure the learner is learning. The student model is compared against this knowledge base or "domain model", and it is from this comparison that similarities are drawn and progress of the learner is quantified. The material conveyed to the learner will be that which they have not seen before or have little understanding of. Content selection is one part of the customization of the system, the second part being interface customization. It was discussed that every learner has their own method of learning, a typical "one-size-fits-all" is not suitable for education, especially so in an environment where age, cultural diversity and current knowledge differ so greatly. The system, therefore, builds into the student model the learner's preferences for learning, which it continues to change as the system learns more about the learner during the education process.

Learners Should be Responsible for their Own Learning

E-Learning (excluding e-Classroom) environments are available anytime, anyplace. In saying that, learners are treated to a more "distance learning"-based correspondence course, with the addition of social interaction. Using these facilities, the learner is responsible for ensuring their own education. The system will report back to the learner what they know and what they do not. The onus is on the learner to revisit areas the system says need work.

Learners Should be Accountable for their Studies

E-Learning systems track the progress of their learners, therefore managers and teachers are able to login at any stage and view the assessment details for the learners they have enrolled. Intelligent solution analysis agents allow for the working of the learner to be shown and reviewed by both the learner and the overseer, displaying an in-depth view of the understanding the learner has for every section within the knowledge base.

Learners Should Receive Feedback

E-Learning systems continually produce meaningful feedback to the learner in real-time during the course (Gladun et al., 2009). The learner need not wait for feedback at the end of courses, but rather receives feedback on problematic areas during training so that they can resolve the matter timeously. The system is able to guide the learner using features such as intelligent problem-solving support to assist them when required.

This section showed that Web-based systems are able to address the needs of information security education and are, therefore, suitable for use within such a system.

4.8 Conclusion

This chapter aimed to set the stage for the identification of both learning methods and platforms for the development of an information security education system of the future. The various traditional learning methods were evaluated and it was determined that a socio-constructivist approach to learning is best for information security education. A discussion on the history of Web-based education followed, showing promise that it could potentially aid in the solution to the problem of educating users world wide in information security concepts.

Adaptive and intelligent features pushed Web-based e-Learning into the forefront as a platform for the delivery of information security education to the world. The growth of acceptance of such technologies determined the same thing, with a significant annual increase in support being shown over the past few years. Hypermedia-based education was lastly evaluated for suitability for implementing an information security education system. The findings were that e-Learning is suitable for the implementation of such a system, however there were certain aspects that could be improved upon in order to ensure the effectiveness of such systems.

The Web is changing on a daily basis with new technologies and methods coming to fruition daily. Web 2.0 is the latest version of the Web and adds significantly to the quality of the information produced on it, allowing all users the opportunity to contribute to the online content stores. Web 2.0 in e-Learning is currently being evaluated by many institutions around the world. The following chapter thus examines Web 2.0 and its effect on e-Learning systems.

Chapter 5

From Web 2.0 to e-Learning 2.0

5.1 Introduction

Leading Web sites of many years standing have recently started to fall away in favour of new and more preferred ones. Some of these sites that have lost momentum include those like Geocities (http://www.geocities.com), who offered (amongst other things) free Web hosting accounts, where users could sign up and upload their contribution to the Internet, a personal home page, etc. These lost out to popularity Web sites such as Facebook (http://facebook.com) which provide the platform for users to post their content, making the creation of content easier and available to far more people. Sites like this also offer social networking facilities, allowing the development of virtual social communities of people with the same interest, promoting interaction and social discussions. This new trend shifted the focus from connecting information to connecting people and was dubbed, Web version 2 or Web 2.0.

The participatory, collaborative, and dynamic online approach of Web 2.0 is where most serious efforts at Web-based development are currently heading; therefore, it follows that online learning communities would naturally transform to use a similar approach (Rogers, Liddle, Chan, Doxey, & Isom, 2007). By following the trends of Internet users and the operation of the digital economy, these new learning environments prepare the learner for operating in the world. While it is true that some aspects and characteristics of the current educational system will most likely prove resilient as the preferred method for learning certain topics (Rogers et al., 2007), it is very likely that Web 2.0 trends will penetrate more of the educational system than one can now imagine.

Web 2.0 provides the learning environment with the tools necessary to enable learners to build their own knowledge constructs and not conform to the generic constructs of information that, for example, traditional education imposes on them. By allowing learners to construct their own knowledge and storing it in a way that is most efficient and effective for their own learning style, educators ensure the best possible outcome to the learning experience.

Downs (2006) describes sculptors who say, "The sculpture was already in the rock; I just found it". Quite literally, it would make no sense to say that the sculpture was not in the rock. The idea of "shaping the mind" could arguably be seen in the same light; it is a revealing of the potential that is latent in the mind, the pre-existing capacity to learn not only language but even sets of concepts and universal truths (Downs, 2006). For this reason, educators require methodologies which enable shaping the minds of the learners and allowing these learners to develop,concrete and map cognitions of information pertinent to their studies in a way which bests suits their own personality, ontologies and learning styles. Web 2.0 provides the tools for customizing the presentation aspect of these systems, allowing them to match the individual learning style of a particular learner.

The purpose of this chapter is to firstly discuss the progression of Web-based technologies, with specific focus on the underlying philosophies of Web 2.0. It will then further the discussion on Web-based learning by showing how the trend from connecting people to connecting knowledge by giving information developed through user contributions more meaning prevents the apparent problem of "information overload" for users browsing these Web sites. This provides machine users with the ability to understand content, allowing them to return more effective search results and move toward the kind of Web Tim Berners-Lee first envisioned as a network where computers adapt to humans, rather than the other way around.

5.2 Progression of Web-Based Technologies

5.2.1 Web 1.0

The development and large-scale deployment of the Internet sparked a need for the development of a mechanism for sharing information graphically. Hypertext Markup Language (HTML) was designed to address this and provided a scripting language, suitable for coding graphical representations of information which remote browsers could download and view. The early versions of HTML allowed for static information to be displayed to the remote client with hyper-links providing a means of simplified navigation between the various pages. This earlier version of HTML and the way the websites interacted with their browsers was dubbed Web 1.0 or Web version 1.0. This form of development included static, non-interactive Web pages offering limited or non-existent forms of contribution from users. Typically, these included personal Web sites: single-authored, content-based ones with updates based on non-interactive processes exhibiting design elements including framesets, HTML form email controls, online guest books and certain proprietary HTML tags such as <blink> and <marquee>, which have since been made redundant. These sufficiently served their users over the years; however, of late the trend has been for users who want to contribute to the content of various Web sites, by organizing a social gathering of users in a collaborative effort to develop their content. Web 1.0 was not suitable for this, so new ways of thinking needed to be developed and this led to the introduction of Web 2.0.

5.2.2 Web 2.0

Web 2.0 is described by Flew (2008) as the movement from personal, single-authoured Web pages to Web sites with blogs (described in the following table) or using blog integration, from publishing by an author to active participation by users of the site and from large, time and money-intensive content development to interactive, ongoing updates by site users. Flew (2008) further describes the change from content management Web sites, where content is listed under a particular category, to social tagging, where any one element can have multiple tags associated with it (folksonomy) allowing more

enhanced classification of subject matter than previously available in Web 1.0.
Web 2.0, also referred to as "the new Web" (Schlenker, 2008), is not about technology, but rather about the **human element**, making it work. Without user generated content, this new Web would be an empty shell of fancy technologies (Schlenker, 2008). Web 2.0 facilitates connectivity with other people, promoting conversation and supporting collaboration of content generation on a global scale (Schlenker, 2008). Such collaborations and conversations are spontaneous, informal and occur in realtime amongst Web users from all over the world (Schlenker, 2008).

Web 2.0 has a set of various tools which hace surfaced over the past few years and grown in popularity as social collaboration tools. Some of these are detailed in the following table.

TOOL	**DESCRIPTION**
Blog	A blog, or Web log, is a shared online personal journal whose entries usually follow in chronological order. Using a blog, a user can post his or her thoughts, experiences or interests for others to view and comment on. Blogs are easy to use, very popular and are arguably the most familiar Web 2.0 tool currently available (Virkus, 2008), having doubled every five months for the past two years and continuing to expand rapidly. Blogs are already gaining momentum as ways from which technical people learn about new technologies and discuss them amongst themselves online. An advantage of blogs is their ability to change on a daily basis, which enables readers to keep up with the rapid changes in technology.
Wiki	A wiki is a collaborative Web site, allowing anyone who accesses it the ability to modify and contribute to the content on it. Providing a simple markup language, wiki users are able to manipulate the display of the site to his or her liking. Wikis are relatively easy to use after some basic training; however, they are less familiar and not as well understood as blogs. Their uses include the replacement of cluttered shared drives, allowing access control to files stored in an ordered, manageable format as well as general-knowledge sharing and public service systems. An example of a large-scale wiki would be that of wikipedia (http://www.wikipedia.com/) which is a free, multilingual, open-content encyclopedia project run by a community of users instead of a single entity. Content on the wiki is read by millions of users world wide and constructed by just about anyone. The ability for anyone to add to the wiki makes it a far more extensive source of knowledge than traditional encyclopedias whose content is limited to that which was written at the time of publishing. The primary advantage of wikis is that it combines the experience of many people in the field; however, this also makes it difficult to ensure the validity of the information.

Social Networking	Social networking Web sites, such as Facebook and MySpace, allow users to connect with their friends, share photos, engage in instant messaging, file sharing and other forms of interaction amongst people with similar interests, friends or activities. These social network sites often exhibit open Application Programmer Interfaces (API) to which external, 3rd party software can draw inference from and harness the knowledge collected on the Web site for its own purposes. These sites also often allow for external applications, such as advertisements, to run on the page whilst the user browsers through the content of the Web site. For example, while a user browsers through family photographs, a particular camera retailer's advertisement may be displayed to the user, enticing them to make a purchase online. These advertisers pay the costs of operating the social network site as they offer the service free of charge to the users. The more users that come on board, the more exposure the advertisers will have and thus the more they are willing to pay for adverts.
Instant Messaging	Instant messaging and chat have been around since the start of the Web, however with the development of Web 2.0, it has become revolutionized as an integrated technology within Web 2.0 applications.

Table 5.1: Overview of Web 2.0 tools

Some information security education courses assign student scribes responsible for taking concise notes during a lecture. These notes are then uploaded to Web sites providing a Web-accessible lecture for other students and the instructor to follow (Yurcik & Doss, 2001). By making use of Web 2.0 technologies, each learner in the classroom is potentially a scribe and can assist in the contribution of content. Using a blog or wiki infrastructure allow the content creation to be more structured, making it easier to contribute than if the students had to build a lot of seemingly disconnected Web pages. Web 2.0, in combination with the tools it provides, also provides facilities which better promote the sharing and collaboration of content creation and dissemination. These facilities enable the classification of information in new ways, making it easier to index and search for information.

Tagging, not classifying

Heath and Motta (2007) describes a method of tagging Web 2.0 data, instead of requiring the user to link the new knowledge under a particular heading or category. This ensures ease of contribution by the user, since the information supplied no longer needs to be fixed within the confines of a particular category. Knowledge which may not easily be classified is now easily tagged and stored in the database (Heath & Motta, 2007). Each knowledge element is able to be tagged numerous times, thereby allowing Web searches more accuracy whilst querying the knowledge store. Having tags also allows for related information to be displayed to the user whilst they browse the site and provides a logical progression to related information.

Similar to tagging, many other Web 2.0 tools and methods exist. Some of these might be of use to help address the human factor in information security by improving the facilities provided by e-Learning systems to learners. The following section compares Web 1.0 to Web 2.0 in order to illustrate the major advancements provided by Web 2.0 in Web-based application development.

5.2.3 Web 1.0 vs Web 2.0

Whilst many existing e-Learning systems continue to be based on Web 1.0 approaches, Web 2.0 has many advantages over these seemingly archaic ways of thinking. Web 1.0 interactions with the user are predominantly about reading, whilst Web 2.0 is more about writing and the joint authoring of content. Web 1.0 was concerned with the client-server architecture for deployment, whilst Web 2.0 leans towards Peer to Peer or distributed networking. Web 1.0 was concerned with users having a homepage, Web 2.0 emphasizes the creation of blogs, which are far more interactive and easier to update and follow. These advancements are changing the way the Web is developed and promoted. Web 2.0 implementation within an e-Learning system will allow it to lean toward a more suitable asynchronous conversation with learners (constructivism), rather than that which is possible with current e-Learning environments, often implementing objectivist methods of learning.

Web 2.0 is all about the user, introducing blogs, wikis, social tagging and connecting people. Web 1.0 was all about connecting information and getting it on the Internet. Web 2.0 applications offer rich user experiences where the process of knowing is a community-based, collaborative endeavour (Virkus, 2008), an important aspect for learning (Wahlstedt et al., 2008). When average computer users begin to feel comfortable, they often begin to extend their browsing experience beyond the basic querying of search engines and start to consume, create and collaborate online (Schlenker, 2008). E-Learning has acknowledged this process as a powerful educational and learning tool accessible to every computer user and to the mainstream population at large (Schlenker, 2008). By combining Web 2.0 concepts and ways of thinking with existing e-Learning solutions, a new concept comes to light, dubbed e-Learning 2.0.

5.3 E-Learning 2.0

E-Learning has been suggested as a tool which could make education and lifelong learning more effective and efficient. The content driving such systems, however, is often static in nature and many of the e-Learning systems fail in that they simply imitate previous educational paradigms (Geser, 2007). This is also true of many IT-based fields as IT itself changes so rapidly with new technological advancements being introduced on a nearly daily basis. Growth of social software on the Internet and the **movement towards open educational content** has had researchers rethink previous models of e-Learning. Downes (2005) coined the term "E-Learning 2.0" to describe e-Learning systems, built on social networking software (Web 2.0) and published online. This e-Learning system is a new style of learning deeply rooted within the social constructivist paradigm (Servitium, 2008), described by Downes (2005) as a revolution, converting the Web as a medium, as it is widely known and accepted, into a platform for delivery of data. **Content is no longer only delivered, but also authored**. Web 2.0 in the educational environment is considered by several authors as progressive and the driver of educational change which offers new perspectives and challenges to education at all levels.

Some of the features which make Web 2.0 so favourable to the educational sector are its **ease of publication**, **sharing of ideas** and **re-use of study content**. Commentaries and links to relevant resources in information environments that are managed by the teachers and learners themselves also make Web 2.0 favourable in the eyes of educators (Geser, 2007). The idea of allowing learners the ability to manage and contribute to their learning environment is in contrast to previous education systems, where developers of the system employed creators of study content, who were tasked with building a generic knowledge base from which learners were educated. Forcing all learners to learn in the same way from such a knowledge store is not the most effective learning approach; therefore, Web 2.0 systems might have more success. Therefore, certain guidelines for the successful development of such systems are now discussed.

5.3.1 Guidelines for e-Learning 2.0 Development

Although there is no way to guarantee the success of an e-Learning 2.0 educational system, Schlenker (2008) describes the following set of key elements which assist in guiding developers of such systems in their thinking and understanding of e-Learning 2.0:

- Web 2.0 technologies should support and facilitate informal learning
- Users must be free to publish (Rip, Mix, Feed)
- Content should be easily manageable
- Organizational cultures must change

Web 2.0 Technologies Should Support and Facilitate Informal Learning

80% to 90% of all learning has been attributed to learning occurring informally outside of the classroom (Schlenker, 2008). Informal explanations dominate over formal mathematical proofs and examples of computer applications security were found by (Yurcik & Doss, 2001) to be especially well received by learners in information security education. Informal learning design is nothing new, but is something e-Learning designers have previously ignored (Schlenker, 2008). The statistics themselves should be enough to force e-Learning design practises to incorporate more informal learning techniques (Schlenker, 2008); however, nothing significant has to date been done about it. Informal learning occurs in many different instances, including the reading and writing of email messages and documents, chatting to colleagues and friends on the phone and spending time socializing in groups at lunch breaks. These are only a few examples of where informal learning occurs, e-Learning 2.0 allows educators to capture these activities and provide them online, allowing each participant to learn whilst performing these activities amongst peers within certain focus groups, around a particular subject domain on a global level. Many information security educators report significant security events (newspaper headlines) occurring during their courses, which presents both a positive relevance to students but may also be a challenge to the instructor if not previously covered in the course (Yurcik & Doss, 2001). In this case, the student and the instructor learn together (Yurcik & Doss, 2001). Web 2.0 tools and methods facilitate this socio-culturist learning process by allowing both the learners and the educators to share their views and opinions with one another. As information is put forward by one learner, another may read and add to it. This process is described as Rip, Mix and Feed.

Users Must be Free to Publish (Rip, Mix, Feed)

E-Learning 2.0 systems should allow the user to act as both a consumer and a producer, allowing them to ”Rip, Mix and Feed” (Schlenker, 2008). As Web 2.0 facilitates the consuming, creation and collaboration amongst peers, each learner is permitted to filter through copious amounts of information on which they are encouraged to add their own thoughts, style and creativity (Schlenker, 2008). This new information and representation is then shared with the others. This process, put simply, includes the borrowing from others (Rip), the insertion of the learner’s own contribution (Mix) and the publishing of the new work (Feed) (Schlenker, 2008). Rip, Mix, Feed is a constant cycle of content consumption, creation and publishing that empowers Web 2.0 technologies and is now driving the e-Learning 2.0 concept into enterprise and education worlds (Schlenker, 2008). By allowing the learner to Rip, Mix and Feed, the system promotes a sense of ownership to the content developed on the system and therefore captivates the learner, keeping their attention and keeping them motivated throughout the learning process.

Content Should be Easily Manageable

Enterprise systems must enable content via the five ”-ables”, namely: searchable, editable, linkable, feedable and taggable (Schlenker, 2008). These features promote one of the key elements of Web 2.0: the facilitation of easy created content and publishing of digital content on the Web, which is important for e-Learning 2.0 systems as well (Schlenker, 2008). Therefore, the digital content published, in order to be truly Web 2.0 ready, should have the afore mentioned characteristics in order to be useful. Schlenker (2008) describes an example, where a certain user publishes a Microsoft Powerpoint presentation to a shared file store. This document is seemingly useless, unless it is managed by a system such as a Web 2.0 system, which allows it to be searchable, editable, linkable, feedable and taggable. By implementing these features, other users can search for the file and comment on its contents or simply link back to the file for other users to reference whilst reading their content. The Powerpoint file could also have multiple tags associated to it, allowing the classification of the file amongst files with similar content for easy indexing.

Web sites such as Wikipedia (http://www.wikipedia.org) and Facebook (http://www.facebook.com/) have shown that Web 2.0 social networking is popular not only within an organizational environment, but increasingly so also for home users. Facebook users spend hours online, building their personal profile and disclosing much about their personal information. Users of Facebook are of varying computer literacy levels; however, each of these users are able to contribute to the content of the system by making use of the Web 2.0 tools provided. Users are able to link to their friends, join various interest groups and share information between one another. Users are able to choose what content of others they want to see, by joining such groups. For example, if a user was interested in viewing humourous photographs uploaded by others, they would join a group which does so.

One of the major challenges for information security educators is that of content selection, selecting topics from many important and interesting possibilities (Yurcik & Doss, 2001). E-Learning 2.0 allow the onus of content selection to be placed on learners, allowing them to follow various links to related information and exploring that which interests them. This moving from educators controlling the course to allowing the learner to do so means the mindsets of educators need to change and this will bring about a change to the culture of education.

Cultures Must Change

Social networking is another aspect of Web 2.0 which is incredibly popular these days (Schlenker, 2008). Web 2.0-enabled social networking tools make it very easy to connect with the right people, share information and collaborate toward a common goal. The most important element within a social network are users themselves (Schlenker, 2008), without whom no content would be available. Supporting the collaborative learning model, e-Learning 2.0 promotes social networking amongst learners, allowing group input into the learning process. The more the learner contributes and interacts within the learning system, the more powerful it becomes. **E-Learning 2.0 is about empowering the self-directed end-user** (Schlenker, 2008), allowing a constructivist learning approach to learning by allowing the individual learner to structure their learning experience around their own ontologies, perceptions, requirements and time constraints.

Some of the advantages of an e-Learning 2.0-enabled education environment have already been discussed in this section. There are many further advantages educators have over traditional learning and e-Learning environments when implementing Web 2.0 as well as challenges which need to be factored into the design of such systems. The advantages and challenges faced by e-Learning 2.0 developers are discussed in the following section.

5.3.2 Advantages of e-Learning 2.0

Web 2.0 has truly revolutionized the Web and the e-Learning education systems which operate on it. In order to grasp the sheer magnitude of these changes, the following section outlines some of the advantages e-Learning 2.0

systems exhibit when compared to more traditional approaches to learning.

One of the biggest selling points to implementing an e-Learning 2.0 system is the potential for **cost reduction** (Servitium, 2008). This takes place firstly as the onus of learning is distributed amongst all participants within the learning environment (Servitium, 2008); therefore, the need for a physical, instructor-led education system will subside. These contributors assist in the construction of the education content; therefore, further costs will be saved in the application of such user-generated, peer-reviewed content by replacing large parts of content creation teams, whether internal or vendor (Servitium, 2008).

By removing the "one-size-fits-all" scenario in learning, these systems exhibit far **more effectiveness** in education than traditional methods (Servitium, 2008). As learners within the system assist in the education of other learners, bringing them up to speed, so too, at the same time, will their learning styles be translated as they teach (Servitium, 2008). By providing insight into their learning styles, users are able to locate content which is presented in a way which is in tune with their own learning styles (Servitium, 2008). The advantages of efficiently locating content is two fold: firstly, it assists the learner in furthering their own personal knowledge on particular content and secondly, it assists in the development of a culture amongst the learners, creating an appetite for further education (Servitium, 2008).

In creating culture and an appetite for further learning, the learners within a system are **motivated** to continue their education and further themselves. This motivation stems from the system actively engaging the learner in the learning process, by requiring them to integrate and maintain the social software tools which allow the learning to happen (Mejias, 2008). The learner is able to act as the author of the academic content, contributing to the system as a whole, allowing others to build on their ideas, all the while developing their own ideas off those of others (Rip, Mix, Feed). This process allows the learner a **sense of ownership** of the content which they and others are constantly expanding.

The ability to **track learner contributions** is also a significant advantage e-Learning 2.0 has over traditional learning environments. This ability allows instructors or overseers to constantly evaluate the learner's progress by rating the contributions the learners have made to particular content areas and scoring their submissions. Organizations, for example, could use such rankings in order to separate more prominent employees from less prominent ones, or, in the context of information security, which users of the system pose the largest problem to the security of the information system based on their understanding of information security. Further to this example, the rankings of contributions can be used to **gauge the accuracy and validity** of the content within such a system. Content created and modified by a more credible user would be higher rated than that posted by an amateur learner. Learners who rip this information are thus made aware that the content is not necessarily reliable and is potentially not a valid resource.

This constant evolution of content allows for **co-operative learning** amongst the learners, facilitating the aggregation and organization of content all the while demonstrating the diversity of individualized research interests, enhancing learning for all (Mejias, 2008). Learners are able to enhance their understanding of the content by actively participating in peer discussions and **collaboration** with other learners. This collaboration leads to **collaborative filtering**, assisting the learner in locating pertinent learning material by querying information from a specific focus group, rather than the entire Web.

Tools which promote discussions and content sharing **increase communication efficiency and productivity** over "back-and-forth" exchanges such as email and discussion boards (Mckiernan, 2005). The collaboration with others and the ability to seek out their own direction in terms of the content which is most pertinent to their individualized learning requirements, assists the learner in **developing basic research skills** and **evolution of the thought process** (Mckiernan, 2005), which they will need in the real world when constructing and disseminating knowledge obtained from online information networks as a root source (Mejias, 2008).

Rogers et al. (2007) assert that implementing education software on Web

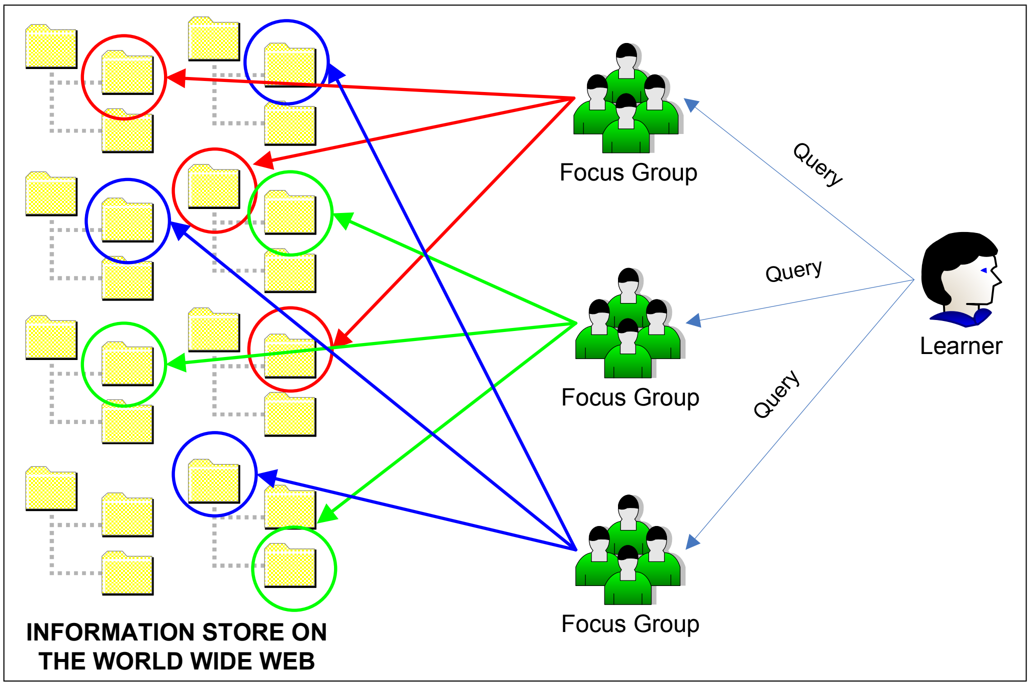


Figure 5.1: Collaborative Filtering in Web 2.0 as Described by Devedzic (2004)

2.0 based social networks, e-Learning 2.0, allows educators to **harness the power of collective intelligence** through collaboration and **social interaction amongst the learners**. Thus, the isolation problems faced by learners of typical e-Learning systems are reduced and content development is enhanced by allowing multiple authors of varying levels of understanding to contribute toward a common goal. Learners often have **differing backgrounds and cultures** and **different levels of understanding**, exposing other learners to content presented from a **variety of viewpoints**, rather than from the single viewpoint of a teacher. The provision for the allowance of individuals to express their views and ideas makes for a more creative environment and expanding knowledge base (Mckiernan, 2005) in which the learners are educated. Through the course of their studies, learners are able to take spare notes and thoughts which can be stored in a meandering collection of file formats (Mckiernan, 2005) for reference at a later date.

The advantages of e-Learning 2.0 systems are extensive and elaborate, allowing these systems to fast become viable options for replacing many of the traditional learning systems in production today. Even with the advantages of such revolutionary education technology challenges are faced which could hamper the development and success of such systems. Some of these challenges are discussed in the following section.

5.3.3 Challenges for e-Learning 2.0 System Designers

e-Learning 2.0 is a relatively new way of thinking about education, thus many educators will be hard pressed to be convinced that such change is necessary and that it will deliver the same (if not better) success that traditional learning methods do currently. Traditional classroom education methods of teaching currently dominate the information security education process (Yurcik & Doss, 2001), thus these educators, too, will be hard pressed to implement new ways of thinking such as e-Learning 2.0. This is one of the first challenges e-Learning 2.0 systems faces: the ability to **ensure buy in** from both the educators, learners and key stake holders (Servitium, 2008).

For those die hard learners who prefer traditional education systems, the e-Learning 2.0 environment should cater to them as well, thereby **supporting both traditional and new learning styles** (Servitium, 2008). The system should, therefore, exhibit the controls and infrastructure to support all learning styles.

This infrastructure is another challenge facing developers and maintainers of e-Learning 2.0 systems: the **ability to implement and maintain the required infrastructure** for such systems with regard to the technology and various processes which need to be put in place (Servitium, 2008). The development and deployment of such systems is, indeed, a challenge; however, the learning managers are perhaps the ones who have the biggest challenge with regard to e-Learning 2.0 systems.

Learning managers and educators need to be responsible for the **orchestration of learning**, rather than solely involved with the creation of the learning content itself (Servitium, 2008). These educators who are to act as co-constructors of knowledge need to move away from the mindset whereby they create content and present these constructs to learners in a generic fashion. Rather than this generic presentation, educators should change their way of teaching, allowing learners to construct their own knowledge pertaining to particular content and form their own knowledge constructs, stored in a way which best suits their own individual learning styles.

There are currently no clear cut methods for the implementation of e-Learning 2.0 systems; however, one can draw from previous experience of other such researchers who have attempted an implementation. The following section outlines a few case studies where e-Learning 2.0 systems were put to the test in order to ascertain their effectiveness in the field of education.

5.4 Conclusion

This chapter introduced Web 2.0 technologies and methods or enhancing the existing e-Learning systems, leading to e-Learning 2.0. E-Learning 2.0 was found to promote social interaction amongst learners by viewing each learner as a contributor to the system. This contribution was simplified by providing Web 2.0 tools such as blogs and wikis to facilitate the information-publishing procedure. The information published was then fed forward to others as fodder for other learners of the system to read and build further on, producing the Rip, Mix, Feed cycle of learning. By allowing learners to enhance content produced by other learners, the overall quality of the content produced was increased significantly as no single persons views and opinions were implied.

By involving the learner in all aspects of the education process, the learner becomes more motivated to contribute and learn from the system. This concept of motivation was noted in applications such as Facebook, where users of the system spent many hours contributing to content on their personal and group pages. This kind of motivation for contribution and participation in a learning environment is ideal for all kinds of educational environments, especially information security where all users need to have some level of understanding and awareness of potential risks whilst conducting themselves on public networks, such as the Internet.

Traditionally, information security education was found to be based primarily on traditional learning methods such as classroom based education. This process was found to be less effective than other forms of learning, such as informal learning, as the discussion of recent information security events in the world allow learners and educators to learn together. This allows for information security educator to act as a co-constructor of knowledge, rather than someone simply imparting generic information security knowledge to the learners, and supports the socio-constructivist learning method, which the previous chapter found to be the most likely candidate for information security education systems of the future.

It was argued that the success of information security depends on the development of culture within the organization or individual information system environments world wide. Education was found as a key to the development of such culture and e-Learning 2.0 provides a way to reach these users, making use of the Internet as a platform.

It is, therefore, the opinion of this researcher that e-Learning 2.0 is a suitable environment for the development of an information security education system, suitable for educating all users of computer systems, from organizational users to individual users at home. These e-Learning 2.0 systems are, however, not without their problems. The following chapter will discuss these problems in more detail and then introduce a number of additional tools and methods to solve such problems, providing a solution for information security education of the future.

Chapter 6

Implementing e-Learning 2.0 for Information Security

6.1 Introduction

E-Learning 2.0 is a suitable environment for the development of an information security education system of the future, as it allows all users of computer systems world-wide to have an understanding of the various threats facing their information systems and how to control them. This is important as the information contained in these systems is important to both organizations and individuals and needs to be protected.

Current information security education systems are inadequate for use globally as they are most often based on traditional classroom-based education. The schedules of all users of computer systems often do not allow for a time to be scheduled where everyone can be in the same classroom. For this reason, the Web and e-Learning 2.0 have emerged as solutions to educating these users. E-Learning 2.0, although with many advantages, also has a number of potential drawbacks which need to be addressed by any information security education system of the future.

This chapter firstly describes these problems in more detail and then investigates methods and technologies which could potentially be used to solve them and create an information security education system of the future. The chapter then demonstrates that the use of the Semantic Web as a knowledge storage and transport system can play a major enabling role in the implementation of information security education programs using e-Learning 2.0. Finally, a solution for an education system of the future, suitable for educating users of computer systems, world-wide over the Internet, at any date and time emerges, based on e-Learning 2.0 and the Semantic Web.

6.1.1 Problems with e-Learning 2.0 for Information Security

Developers of e-Learning 2.0 systems often encounter many problems and limitations whilst designing and constructing e-Learning 2.0 systems. This section will discuss these problems and potential solutions will be provided in order to show that e-Learning 2.0 is a suitable technology for future information security education.

The first issue to consider with regard to e-Learning 2.0 and the tools which it uses to educate learners, is its **complexity of use**. Information security concepts may already be confusing to non-professionals. The complexity of education tools would increase this confusion and the difficulty the learner experiences during the education process. The process of creating and modifying information on pages of certain tools, such as a wiki, is cumbersome for many individuals (Mckiernan, 2005). For these people, the way a wiki works is like nothing they have previously experienced so it does not make sense to them. This reaction often causes learners to reject the tools so they do not contribute and end up missing out on the whole experience, proving detrimental to their learning speed and effectiveness. These users may become frustrated and, therefore, fight against the system, rather than embracing the change and spending time learning how to use the system successfully (Mckiernan, 2005). Users of computer systems are of varying age and technical understanding. Information security education systems built on e-Learning 2.0 technologies and methods should consider this and accommodate the users in a way which best matches their technical abilities and their levels of understanding. Information security education systems of the past focused on adults in an organizational context; however, these days information security education systems need to address the changing target audience by adapting to their requirements and preferences as well. This is important as those learners who take the time to contribute to the content on the system will benefit by having peers and educators review their work and point out certain flaws in their beliefs and understandings of information security concepts. These contributions are important as it is from these that the content for other learners to pick up on is generated, making the content development process of e-Learning systems a social, community endeavour.

By allowing all users the ability to contribute to a learning environment's content base, the system allows both experts and amateurs to express their views on certain topics. End-users and individual users of computer systems can express their ideas and conceptions of information security and be corrected where necessary. The creation of such content, viewable by everyone, causes additional problems, in that the **credibility of authors** is not necessarily known or cannot be verified. Information security content is thus presented as unverified and learners may be reluctant to observe it as the truth or, perhaps, conversely believe the misconceptions of another learner on the system. Likewise, from an organizational view, the content of information security education needs to be correct so that the champions of such systems are reassured that the content their users are learning is true and correct. It is a well-known fact that the credibility of authors should be sound in order to act as references in academic work. The credibility of authors is usually very easy to determine by conducting research into the particular author, having a look at past papers and books written (Oberhelman, 2007) and analyzing which other authors have referenced their work. This is not as easy to do with content posted by learners on an e-Learning 2.0-style education system. The development of an information security education system based on e-Learning 2.0 should address the issue of author credibility in order to provide assurance of reference to sound content. One such method for performing author credibility checks is by allowing a **rating** to be allocated to each author, an idea which is currently not implemented in many e-Learning 2.0 systems. A particular author should be rated based on the credibility of their previous known work in the information security field or within verified topics on the system. The ability to track the contributions of various authors was already discussed as a feature in e-Learning 2.0; therefore, the contributions information security education learners make can be traced and verified by more experienced users of the system.

The credibility of authors is not the sole credibility problem visible in e-Learning 2.0. The contribution to a single information security topic by multiple authors presents an additional problem, that e-Learning 2.0 tools (such as the wiki) present the problem of hierarchy control and sense of lack of accountability (Mckiernan, 2005). As the content is created and edited by multiple authors, some more credible than others, it is very **difficult to determine the credibility of the work** as a whole. The credibility of each entry within a wiki, for example, would be very different to another on the same wiki, as the authors differ. The content of each entry is also subject to change on a daily basis, as are the authors of such entries. This change of authors and content is welcomed within an e-Learning 2.0 environment as it will, for the most part, aid in the learning process by promoting collaborative learning efforts and allow the changing dynamic of IT and information security to be reflected in the content. This trend is unlike traditional style Web sites where the author was known and his or her expertise in the field could be judged to make an intelligent assessment of the credibility and scholarly significance of a given site (Oberhelman, 2007). The proposed information security system should **provide a mechanism for measuring the credibility of each topic**. Much the same way a user is scored, so, too, should the content posted to a particular topic be scored, based on the ratings of the users who contributed to the content.

Oberhelman (2007) says one needs to learn how to cope with a certain degree of uncertainty and that just as people embraced Web 1.0 back in the 1990s, so too must they learn to embrace Web 2.0 and incorporate it into a new strategy of doing reference. This, however, is contradictory to the way academic scholars and librarians think with regard to research. Librarians are not comfortable with contingencies and unknowns; not being able to know the credentials of an author on a Web forum or a comments section may be positively disconcerting to many in the information security field. These concerns may hold some water, as the way e-Learning 2.0 structures its contributions, each entry in an information security e-Learning 2.0 tool such as a wiki or blog may be more complete or of better **quality/finality** than another document on the same site (Mckiernan, 2005). The reason for this is that multiple authors work on various entries; however, these authors are often not the same; therefore, the knowledge they impart would be of differing value to the system. **An information security concept created and maintained by IT professionals will be of higher quality than an entry created by an end-user trying to explain the same**. However, such a concept may be better understood by end-users if it were written by other end-users, rather than IT professionals. Learners reading through entries on the system should, therefore, not assume that the quality of one particular piece of work reflects the knowledge represented on the other pieces of work on the same system.

The contributions to certain information security topics by these authors may be abundant in certain parts and lacking in others. The reason for this is that authors may have knowledge in parts of the topic, which they impart by way of publication; however, in areas they lack knowledge, they are unlikely to contribute. The finality of the topic as a whole should be addressed by the proposed information security education system, to ensure that a learner is clearly shown the level of completeness of a particular entry in order for them to know firstly, where they are able to contribute and secondly, where the system lacks content.

As many authors contribute to the works of a particular information security topic, another problem arises: that of the ownership to the **copyright of information**. If each author retained their own copyright, the process of Rip, Mix, Feed would be hampered as access to the knowledge would be subject to obtaining sufficient rights before works could be furthered. For this reason, the proposed information security education system should **promote contributions which are published under the Creative Commons (or similar) license**,making the information available, free of charge, to all viewers and contributors (Geser, 2007), thus facilitating the evolution of knowledge into new knowledge, where required. In this way, all learners are encouraged to Rip, Mix and Feed from information security content, all the while developing their own understandings and constructing their own knowledge on various concepts. This new knowledge is then able to be shared with the rest of the community, allowing the learner to act as a producer of content and contributing to the education of others.

Although through the use of e-Learning 2.0, with adaptive e-Learning features, it is theoretically possible to **track a learner's contributions** and posts, it is a difficult to implement in practice. The contributions and posts a learner makes to an information security topic do not in themselves solve the problem as a whole, but rather contribute to a group solution or understanding. Rogers et al. (2007) could find no existing standards that would mark a participant's work as an "assignment", allowing learners to show what they have done, and to get comments back on that information. This is an issue as educators are **unable to accurately gauge the competency of each individual learner** in information security concepts, but rather only ascertain the fitness of the group as a whole. The proposed information security education system should thus **provide mechanisms for the establishment of the competency of learners around each topic** within the system.

The promotion of learner-assisted content publishing and creation allows an abundance of information on a number of information security topics to be generated. The generation of such volumes of traffic produces yet another potential problem for a system as big as the proposed information security education system. This is the move from the lack of sufficient information security content, to potential information overload (Ohler, 2008). One of the problems with traditional e-Learning systems was that it took a long time and a lot of financing in order to build a suitable knowledge base from which to educate learners. Developers of the coursework of information security education systems were typically experts in the field who were paid to develop content for the system. E-Learning 2.0 solved this problem by allowing the learners themselves to contribute and build up the learning material, building a system based on "folksonomy" or user-generated taxonomy. Although this provided many advantages, it also gave rise to potential for **information overload**. If learners are not limited to the scope of a contribution, certain information security topics may have a large amount of content associated with them, so when a learner searches for a particular topic, too much information is returned and the learner is unable to manage and sift through it to find specifics (Ohler, 2008). The proposed system **must allow the large amount of information posted to be managed in an effective way**, so that learner searches are optomized and only information pertinent to the search are returned.

This is difficult to accomplish on e-Learning 2.0 systems, as each typically provides their own proprietary knowledge storage facility, each differing in design from other such applications. This means that for one system to share content with another system, it would need to provide an API to its knowledge store and the receiving application would need to write specific code in order to interact with this API. This type of code would need to be written for all remote knowledge stores that the receiving application wishes to interact with, severely limiting the scope of applications which can interact with one another. Consider, for example, two of the largest social network applications of today, Facebook (http://www.facebook.com/) and MySpace (http://www.myspace.com/), each of which built on Web 2.0 technologies. A certain user who creates a profile and uploads photos to Facebook, will need to repeat the process on MySpace, as the two do not share an underlying knowledge storage and transport platform. Although, theoretically, MySpace could harness the power of the Facebook API, this would not solve the problem when additional social network websites become available. This is true also for information security education systems based on e-Learning 2.0. As new educational interfaces become available, they should be allowed to connect to the content produced by other e-Learning 2.0 systems in order to greatly enhance the content available to the learner. In order to accomplish this, the information security education system **should be built on a suitable knowledge storage and transport platform, which facilitates multiple, customized e-Learning 2.0 environments or systems interconnecting with it and sharing information with it**.

The problems of implementing e-Learning 2.0 systems for information security education can thus be summarized as follows:

- Complexity of use

- Credibility of authors
- Credibility of content
- Quality and finality of content
- Copyrights
- Tracking learner contributions
- Gauge competency of individual learners
- Information overload

Many of the problems presented are not only with e-Learning 2.0, but Web 2.0 as a whole. These problems relate mostly to the storage and sharing of information posted on Web 2.0 systems. The Semantic Web offers advances which aim to solve many of these problems and is evaluated in the following section.

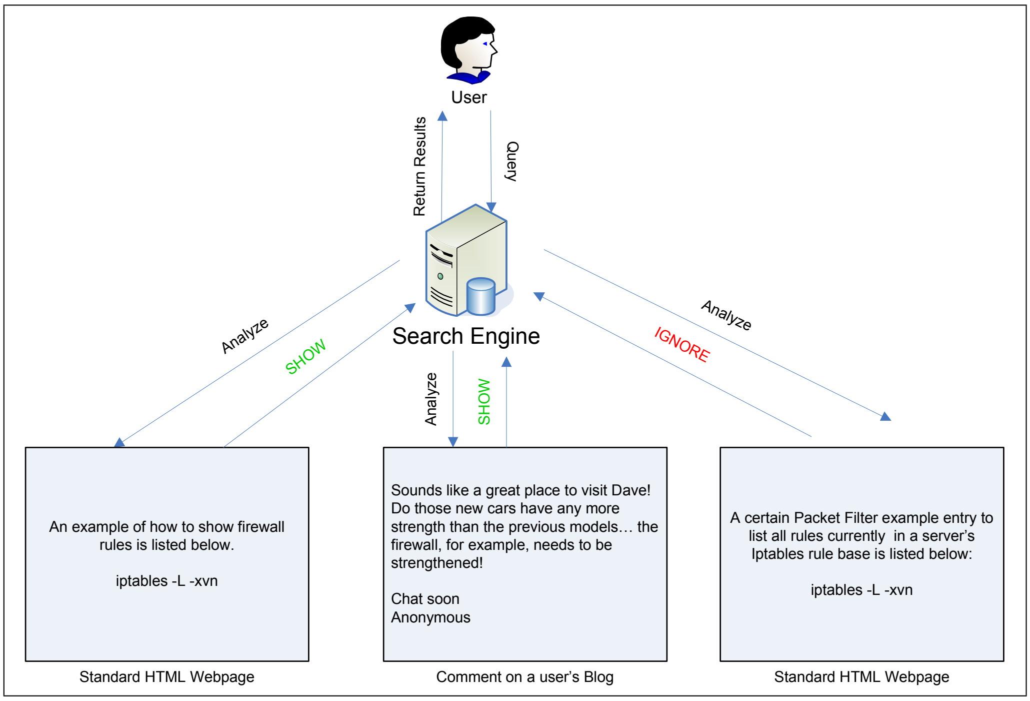
6.2 Semantic Web as a Possible Solution

Web 2.0 opened the Web and allowed contribution of information by the average computer user. This contribution facility, although solving the problem of content generation, introduced further problems which needed to be addressed in order to ensure the continued success of the Web and facilitate its large growth. One of the problems with allowing contribution from many sources, is that the information is posted and stored in a format suitable only to human readers, making it very difficult for machine users (or applications) to understand and draw inference from it. This meant that machine users and applications are unable to understand information security concepts and the contributions learners make on the system. **Although information security education concepts would be *machine readable*, they would not necessarily be *machine understandable*** (Devedzic, 2004). In order to facilitate searches which filtered through all of this information accurately and effectively, preventing information overload to the users of the system, machine users need to be able to parse the information and have an understanding of its contents.

Current trends in the evolution and design of the Web aims to address this. The Semantic Web can be thought of as a large relational database, joining tagged items and incorporating all topics and concepts (Ohler, 2008), from book chapters to cell phones to the price of laptop computers. By joining these topics in a way which computer applications can understand, the Semantic Web allows information generated by learners on an information security education system to be transformed from a "display only" form, only parsable by humans or software agents written specifically for the task, to a vast database of knowledge, which **computer applications can parse and understand** (Ohler, 2008). This knowledge **allows computers to more accurately search for specific criteria within the information security education system content base** and do much of the grunt work in information processing and filtering for searches performed by human users of the system. The Semantic Web further allows users to find relationships between tagged items, such as related information security topics (Ohler, 2008). This process is possible due to the Semantic Web's ability to use inference rules and data organizational tools known as "ontologies" (Ohler, 2008), which are domain theories, enabling a Web that provides a qualitatively new level of service (Devedzic, 2004).

Figure 6.1 depicts a simplistic view of a standard Web search, showing a user sending a query to a search engine. Supposing the query was "*Firewall Example*", the diagram shows how the search engine, a machine user (agent), would do its best to parse the human-readable information by matching the words "firewall" and "example" and then returning the pages with the best results to the user in the hopes that they were correct. The search engine had to parse the human readable text, as that is all it had to go on in order to gain an understanding of the information stored on the page.

As can be seen, the agent returned the first page result correctly; however, the second page, which was simply a comment on a blog of a social network user informally chatting to a friend was also returned. This information was not pertinent to the search; however, the search engine did not have anything to confirm or deny that, so did its best using its internal reasoning and decided to include the page in the search results. Likewise, the third Web page that was crawled, which did not have the same wording as the


User
Return Results
Query
Search Engine
Analyze
SHOW
Analyze
SHOW
Analyze
IGNORE
An example of how to show firewall rules is listed below.

iptables -L -xvn
Sounds like a great place to visit Dave! Do those new cars have any more strength than the previous models… the firewall, for example, needs to be strengthened!

Chat soon
Anonymous
A certain Packet Filter example entry to list all rules currently in a server's Iptables rule base is listed below:

iptables -L -xvn
Standard HTML Webpage
Comment on a user's Blog
Standard HTML Webpage

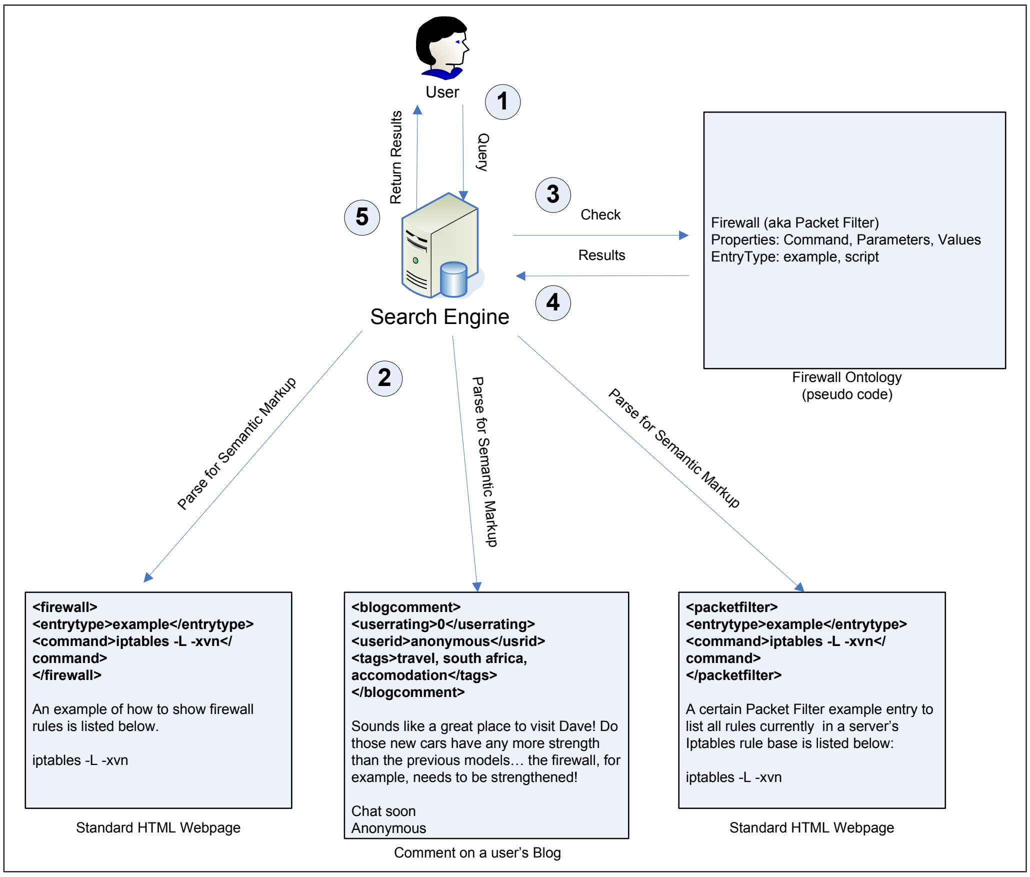
Figure 6.1: Standard Web Search - Potential to Return Undesirable Results

query, was skipped completely and not returned to the user as the search engine did not find any relationship between ”packet filter” and ”firewall”. The user was thus left with a heap of information to filter through manually, much of which were results not in the context of their search, making it a time-consuming process with much relevant information being discarded by the search engine before reaching the user.

Consider Figure 6.2, based on the description by Devedzic (2004), showing the same example executed within the Semantic Web.

The user enters a query at the search engine or agent and specifies that they are looking for ”firewall” information and, more specifically, an ”example” of such. The semantic agent checks for the existence of an ontology which best described the user's search criteria. It locates the ”Firewall” ontology and found that ”EntryType” was one of its attributes, which the user provided (the key word ”example”).

The agent begins to parse various Web sites in search of ones which are linked to the ”Firewall” ontology and then which have their EntryType set



Firewall (aka Packet Filter)
Properties: Command, Parameters, Values
EntryType: example, script

```
<firewall>
<entrytype>example</entrytype>
<command>iptables -L -xvn</
command>
</firewall>
```

An example of how to show firewall rules is listed below.

iptables -L -xvn

```
<blogcomment>
<userrating>0</userrating>
<userid>anonymous</usrid>
<tags>travel, south africa,
accomodation</tags>
</blogcomment>
```

Sounds like a great place to visit Dave! Do those new cars have any more strength than the previous models... the firewall, for example, needs to be strengthened!

Chat soon
Anonymous

```
<packetfilter>
<entrytype>example</entrytype>
<command>iptables -L -xvn</
command>
</packetfilter>
```

A certain Packet Filter example entry to list all rules currently in a server's Iptables rule base is listed below:

iptables -L -xvn

Figure 6.2: Semantic Web Search as Described by Devedzic (2004)

to ”example”. The agent locates the first page and, by reading the **semantic markup** in the page code, is able to determine that this page is linked to the firewall ontology and is of the correct entry type. The web agent, therefore, adds this page to the results to be returned to the user.

The agent then parses the second page, once more reading its semantic markup tags, which provide the machine readable components of the Web page, transparent to the normal human reader’s view. The semantic agent is able to determine that the contents of this page are not linked to the firewall ontology; therefore, the contents thereof are not pertinent to this particular search and the page is discarded from the search results.

Lastly, the third page is parsed. The agent is able to determine that the page contains information regarding ”packet filter”, which, according to the Firewall ontology, is synonymous with ”firewall” and is thus added as a result to return to the user as the EntryType attribute exists and is also a match.

As demonstrated, **the Semantic Web assists in the locating and linking of information on the Web, providing more accurate search results and connecting knowledge of information security concepts**. By making information on the Web (and thus e-Learning 2.0 systems) more understandable to machines, humans are able to turn to machines for processing and analyzing Web contents more precisely (Devedzic, 2004). This is a great benefit to humans, who themselves can only process a tiny fraction of information available on the Web. By having machines perform all the hard work and structuring results which most closely match the user's query, the Semantic Web truly brings more meaning to information on the Internet.

An example was provided in order to demonstrate the need for the Semantic Web as a way of further enhancing the Web. Before the pertinence of the Semantic Web in the education field can be demonstrated, a brief understanding as to the implementation of such technologies and design challenges for implementing an information security e-Learning 2.0 system needs to be discussed. Devedzic (2004) asserts that these challenges related to the Semantic Web can be roughly classified into four categories: Languages for the Semantic Web, Ontologies, Semantic markup of pages on the Semantic Web and Services that the Semantic Web should provide.

6.2.1 Languages

It is important, since the Semantic Web allows the interaction of multiple web applications or agents to share information, that the languages they communicate with are standardized. Designers and implementers of information security education systems using Semantic Web technologies should, therefore, agree upon the data's syntax and semantics before it is coded (Devedzic, 2004), thereby avoiding high costs incurred in changing systems at a later date. In order to facilitate the interpretability of data between Semantic Web applications, many languages have been developed and implemented, most of which are based on the eXtensible Markup Language (XML), XML Schemas, Resource Definition Framework (RDF), and RDF Schemas (Devedzic, 2004).

The languages described above form the basis for descriptive languages

LANGUAGE	**DESCRIPTION**
XML	XML languages are more structure-orientated than standard HTML pages, which are layout-orientated (Devedzic, 2004). Whilst HTML relies of fixed tags to present the information, XML benefits from allowing developers the ability to define their own tags and bear some semantic information themselves (Devedzic, 2004)
XML Schemas	Provide the necessary framework for creating XML documents by specifying the valid structure, constraints, the number of occurrences of specific elements, default values, and data types to be used in the corresponding XML documents (Devedzic, 2004)
RDF	A framework used to represent data about data and for modelling of date about resources located on the Web (Devedzic, 2004). RDF is typically stored in the form of a table, implemented as O-A-V triples (Object, Attribute, Value): each statement describes a particular value an object has for a certain attribute. These tabular triplets can be represented in a table form, a labelled graph or using XML-based encoding (Devedzic, 2004). An RDF model simply provides a domain-neutral mechanism to describe metadata, but does not define the semantics of any application domain in particular (Devedzic, 2004).
RDF Schemas	Much like XML schemas did for XML, RDF schemas define the ”vocabulary” of an RDF model (Devedzic, 2004). RDF schemas provide a mechanism to define domain-specific properties and classes of resources to which those properties can be applied, using a set of basic modelling primitives (class, subclass-of, property, subproperty-of, domain, range, type) (Devedzic, 2004). RDF schemas are typically represented using RDF style encoding, however, are quite simple and therefore, do not provide exact semantics of a domain.

Table 6.1: Overview of XML based languages. Adapted from Devedzic (2004)

on which the reference ontologies are built. These ontologies form the basic structure of the Semantic Web, providing initial points of comparison and agreement on shared-knowledge ideas and constructs. **Ontologies are used to describe content stored on multiple servers, containing information security education information to various machine users crawling them on behalf of learners.**

6.2.2 Ontologies

An ontology, according to Gruber 2003, as cited by Gladun et al. (2009), is a formal and explicit specification of a shared conceptualization. Formal, meaning it should be represented in a formal representation language and shared, indicating that the ontology describes knowledge accepted by a community (Gladun et al., 2009). A primary goal of ontologies is to facilitate knowledge sharing and reuse, providing a common understanding of various content that reaches across people and applications on the Semantic Web (Devedzic, 2004). From a technical perspective, an ontology is a text-based piece of reference-knowledge, formatted using syntax of an ontology representation language, most of which is built on XML and RDF, uploaded to the Web and used by agents who consult it when necessary. One such ontology representation, released by the World Wide Web Consortium (W3C), which is gaining in popularity as a Semantic Web representation language is OWL or Web Ontology Language. The widespread use of OWL has the possibility to make it the standard ontology representation language for the Semantic Web of the future (Devedzic, 2004) and thus the standard ontology representation language for information security education built on Semantic Web technologies.

From a practical perspective, ontologies provide structure and logic to information embedded within Web pages and as a result of this, the Semantic Web can know, learn and reason just like humans do. Ontology, in philosophy, is a theory about the nature of existence and, more particularly, what types of things exist; Ontology, as a discipline, studies such theories (Berners-Lee, Hendler, & Lassila, 2001). Ontologies have become the defacto-standard knowledge representation technology after the emergence of the Semantic Web, Semantic Web Services and the Semantic Grid;

for all of these new research branches, ontologies are the cornerstone technology (Gladun et al., 2009). In a Web context, ontologies provide a shared understanding of a domain. Such sharing is needed to avoid terminological differences between various concepts (Gladun et al., 2009). For example, in information security, the terms "awareness" and "education" are often used interchangeably to mean the same thing. This is, however, incorrect and by defining them in an ontology, such misconceptions and confusion can be removed.

The example presented earlier demonstrates another advantage of using ontologies - to **eliminate the problem of terminological differences**. The program should be provided with a method to relate various identifiers to one another for whatever database it encounters. In the example, "Firewall" and "Packet Filter" were found to be synonymous; this was inferred by the ontology which had a rule stating that the two names were synonymous. A program that wants to compare or combine results from two different databases requires a method to know that certain attributes, although having different identifiers, have the same meaning (Berners-Lee et al., 2001). This issue is addressed by the ontologies within the Semantic Web. The ambiguity of the human language, for example, is removed by allowing the system to query various ontologies and figure out that a particular name may exist as a book, a movie, or even the name of a river. By reading the knowledge in context, the program aims to delineate these ambiguities and improve Web searches on particular subject domains such as information security. When searching for information security culture, for example, many search engines would provide references to general social culture as well, which is not related to the search. By defining information security culture in an ontology, it will not be misunderstood as the social culture of certain people, but rather that of the behaviour of users within an information security system. In so doing, semantic search agents will be able to remove references to Web sites which are not related specifically to the queries that the user puts forward.

Each ontology has a number of attributes with identifiers, all interconnecting with one another, in order to describe pages which have the ontology as a reference. These attributes, or taxonomies, assist the various agents in the discovery of inter-relating information. Furthermore, these taxonomies allow the tools built on Semantic Web technologies to understand the relevance of the information retrieved and thus present the information textually or graphically in the form of graphs or 3D renderings, providing a more enticing interface to the user.

Taxonomy Within an Ontology

The taxonomy within ontologies defines classes of objects and the relations which exist among them (Berners-Lee et al., 2001). For example, a chapter may be defined to exist within a book. Pages may be defined to exist within chapters, and so on. Likewise, **in information security**, a certain rule such as all **passwords should be 7 characters long** is a requirement for secure password selection and **can be inferred by an ontology**. Classes, subclasses and the relations among entities are a very powerful tool for Web use (Berners-Lee et al., 2001), providing the ability to express a large number of relations among entities by the assignment of properties to various classes and then creating subclasses which inherit from these parent classes. **Ontologies, in conjunction with taxonomies, can be used to reason in order to arrive at various conclusions. This is possible through the use of an ontology's inference rules**.

Inference Rules

Inference rules within ontologies provide them with even more power (Berners-Lee et al., 2001); For example, if a page forms part of a chapter and a chapter forms part of a book, the system is readily able to deduce that a certain character mentioned on a page of a particular book is, in fact, from that book. Although the system does not truly understand that this character exists within the story, it allows the system to more effectively manipulate the terms in ways more meaningful and useful to the human user (Berners-Lee et al., 2001). In the same way, if the act of a user selecting a secure password supports the technical controls, it can be inferred that users play an important role in supporting the technical controls or safeguards of an information security system. Inference rules assist the ontology in the provision of various services, driven by the users of the Semantic Web.

6.2.3 Service Provision

Devedzic (2004) advises that users of the Semantic Web are looking to it in order to receive intelligent, high-level services like information brokers, search agents, information filters, intelligent information integration, and knowledge management. Likewise, **in information security, users are looking to it to provide detailed information as to the protection of their information assets**. These may be in the form of an information security virtual expert, whose knowledge is based on content stored and created on the Semantic Web. These services are only possible through the development and large-scale deployment of ontologies, which will populate the Web with machine understandable information, thereby facilitating the semantic interoperation between such agents and applications (Devedzic, 2004), sharing terms between various information and providing an overall understanding of the information to the calling application such as the minimum length passwords should be in order to be deemed secure. The operation of such services is only possible through ontologies, which describe the services themselves, thereby providing machine-readable information as to what the service offers and how to make use of such a service (Devedzic, 2004). By providing machine-readable descriptions of the services and how to use them, the Semantic Web will expand by itself, incorporating new services as they become available, with little or no human intervention. If these services present their attributes, properties, capabilities, interfaces and effects in unambiguous machine-understandable forms, agents will be able to recognize them and invoke them automatically (Devedzic, 2004).

An example may be that of an intelligent Semantic Agent accessing a resource library on behalf of a user. The agent will need to know how to locate the library's information store, how to perform a search on the information and what results should be expected in return (full text or abstracts). The format of such results should also be known to the agent, in order for them to be correctly returned to the user. The agent should further be aware of the conditions implied when accessing the data, namely the cost of retrieval and which full texts are available only via subscription services (Devedzic, 2004). After the agent reasons with these conditions, if there are no internal conflicts with its own logic, it will eventually learn how to invoke these data stores by itself (Devedzic, 2004). As more information security education services become available, such as ones which educate users on verifying the integrity of secure Web sites, these should be automatically included as content for potential learners who may be interested or required to use them.

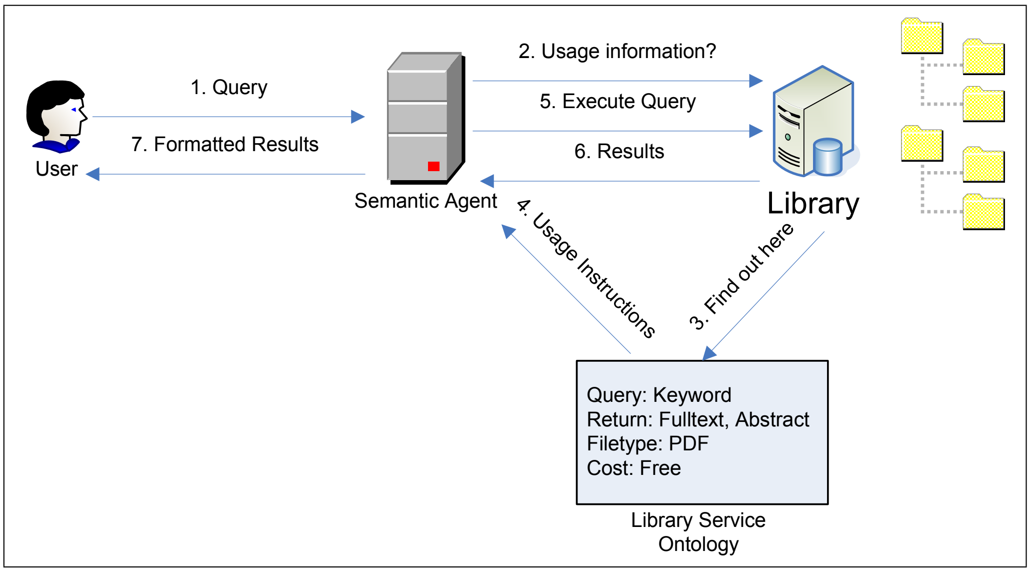


Figure 6.3: Semantic Web Service Discovery as Described by Devedzic (2004)

This situation is completely converse to the current operation of information retrieval, whereby the user needs to find the location of a particular library's Web site, invoke the search facility, wade through an exorbitant amount of information returned and perform their own filtering techniques in order to obtain the information they were looking for. This is particularly appropriate for information security education. Many learners do not view information security as necessarily important; therefore, information should be presented in a concise, accurate form to these users rather than as a collection of unordered (and not necessarily related) information. By providing concise content, the learners attention can be acquired for long enough to provide for an efficient education course, rather than a research intensive discovery course.

In the example above, the library service referred the agent to an ontology in order to understand how to access it. In order to ascertain which ontology the library service is described by, the agent had to look at the machine readable and understandable code on the library page, known as the **semantic markup**.

6.2.4 Semantic Markup

Providing ontologies on the Semantic Web is simply not enough to ensure its success. In order for an agent, information broker or human user to be able to link a particular Web page to an ontology, the Web page should exhibit some form of semantic markup code (Devedzic, 2004). This code is often written in an XML format and provides links to ontologies which further describe the information contained on the page. By linking to ontologies describing the contents of the page, these pages allow automated reasoning about the document and services, such as how to use them, the parameters to supply and what results will be returned (Devedzic, 2004).

By automatically inserting these markups in pages, ontology-aware authoring tools assist the publisher in creating these markup tags by providing a list of the various ontologies available and allowing them to select which ontologies to link the document with. In so doing, the markup can evolve over time, along with the document, accommodating any changes in vocabularies, conflict resolutions and growth of the content contained within the document (Devedzic, 2004). It is, therefore, important that the authoring tools provided by the proposed system facilitate the automated creation of semantic markup to annotate the content of each contribution by learners.

The use of the Semantic Web promotes the easy use and distribution of large amounts of information, keeps it available and easily understandable to both human and machine users. The following section provides a discussion of the combined use of e-Learning 2.0 and the Semantic Web in order to ascertain its usefulness in enhancing information security education of the future.

6.3 e-Learning 2.0 and Semantic Web in Information Security

Web 2.0 technologies were introduced as an enhancement to the basic e-Learning environment. The content generated on such a system was driven by the learners themselves, which assisted in fast, quality content being developed. The problem, however, surfaced that this content was predominantly suitable for human readers and the storage of content was in a way which was not easily understandable by machines. The Semantic Web changes that by allowing more meaning to be given to content generated on such systems for machine users. The provision of such technology **allows for machines to parse the content generated and assist learners in obtaining accurate, related information from underlying content models**. An information security education system will thus only return **information security content which is relevant** to the user.

Pedagogical agents are used to accomplish this task, by providing the necessary infrastructure for knowledge and information flow between the clients and the servers (Devedzic, 2004). These agents are autonomous in design and collaborate with other such agents in the context of the learning environment (Devedzic, 2004). **The main tasks of these pedagogical agents are to assist the learner in locating, browsing, selecting, arranging, integrating, and otherwise using educational material (pertinent to information security education) from different educational servers** (Devedzic, 2004), exhibiting collaborative filtering techniques amongst themselves. These agents are able to support both collaborative and individualized learning, all the while supporting the learner's own personal cognitive processes (Devedzic, 2004).

The agents are able to gain access to the information security educational content by way of Semantic Services which offer the content to the agents. The server, which hosts these services, builds a student model for each individual learner and possess enough intelligence to personalize the content that is returned to the agent for a particular learner (Devedzic, 2004). This means that **as learners begin to become more familiar with certain**

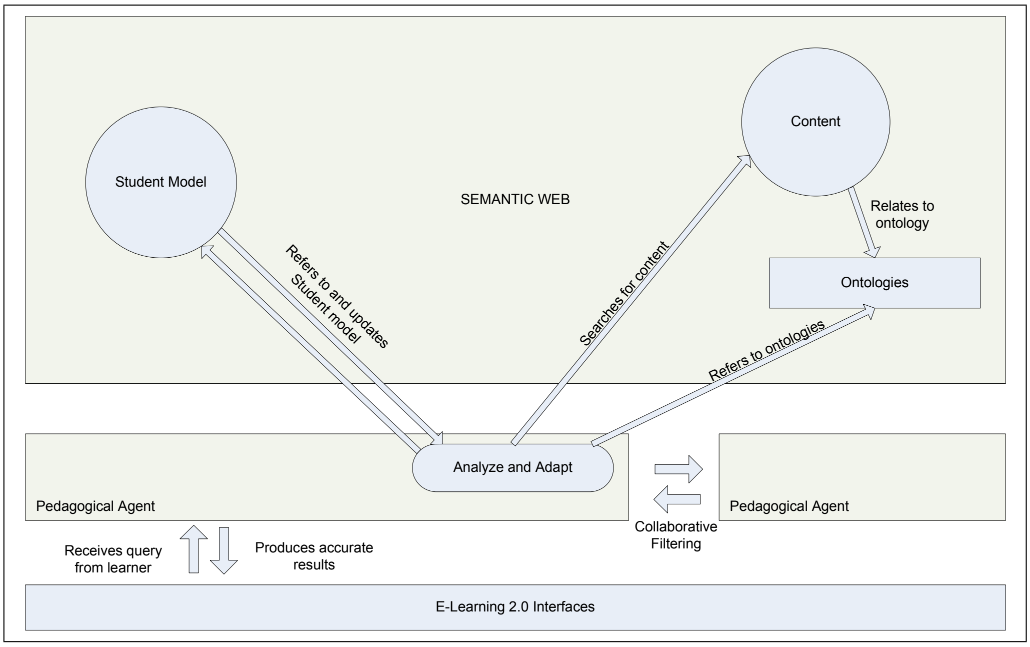


Figure 6.4: Semantic Pedagogical Agents as Described by Devedzic (2004)

information security concepts, the system will recognize this and move on to the next concept or increase the level of difficulty presented for that concept, depending on the role the users play within the computer system environment they are in (organizational or personal) or the prerequisites set out by their instructors.

From the learner's perspective, the server appears to act as an intelligent tutor, or information security expert, storing and formatting both domain and pedagogical knowledge in an effort to conduct a learning session (Devedzic, 2004) in the same way adaptive e-Learning systems of the past did. In order to conduct such a learning session, the system employs the use of a presentation planner, which aids in the selection, preparation and adaption of the information security domain content material to output to the learner. This content is selected based on the role the learner plays within the information system. For example, the system will present technical knowledge to IT professionals, whilst only basic knowledge to provoke awareness to end-users or individuals. During these interactions with the learner, their responses are continually analyzed and the student model is slowly created in order to track the learner's actions and learning process. **Whilst con-**

structing the student model, the system detects and corrects the learner's errors and misconceptions of information security, using intelligent features such as intelligent solution analysis and intelligent problem solving support and, if need be, redirects the session accordingly (Devedzic, 2004).

Learners within an e-Learning 2.0 system are encouraged to contribute to the creation of content for the system. In order to make the content generated by the learners more machine-processable and hence, agent ready, the system needs to provide semantic markup for each page of contributions, including pointers to shareable educational ontologies which explain the contents of the pages to machine users (Devedzic, 2004). The creation of such markup should be done automatically by the authoring tools of the system each time a learner contributes to the system. These authoring tools should therefore ensure that all content posted has semantic annotations and markups associated with it that ensure easy and automatic access by pedagogical agents (Devedzic, 2004). These markups should be transparent to the learner, as most learners of information security are not expected to be ontological experts (Devedzic, 2004), but rather average computer users.

The problems exhibited by e-Learning 2.0 education systems were laid out at the start of this chapter. In order for information security education to advance by incorporating e-Learning 2.0 and the Semantic Web, solutions to the problems with e-Learning 2.0 need to be found. The following section presents potential solutions to many of these problems, after which the following chapter will demonstrate by way of example how such a system will be implemented.

6.4 Solutions to e-Learning 2.0's Current Problems

The Semantic Web was noted as a potential solution to the underlying problem of content storage and retrieval on e-Learning 2.0 systems. The following section presents this solution in more detail, outlining how such a system would be built and what requirements there are in terms of technical specification and user access. There are many instances where user information needs to be stored with an information security education system. This includes the student model and methods to track the author, their contributions and their credibility. One such method for creating and linking user profiles on the Semantic Web, which is growing in acceptance, is the Friend of a Friend (FOAF) project.

6.4.1 Friend of a Friend

The Friend Of A Friend (FOAF) vocabulary is one of the largest projects on the Semantic Web and is a widely accepted standard for representing social networks, used by many social networking Web sites to create Semantic Web profiles of their users (Golbeck & Rothstein, 2008). FOAF is frequently used as an example of the success of the Semantic Web (Golbeck & Rothstein, 2008) and thus should be considered for use within the proposed information security education system.

It is common for users of social networks to have multiple social network profiles, such as profiles on Facebook and MySpace, as social networking Web sites often do not share profile-relating information with one another (Golbeck & Rothstein, 2008). The merging of these multiple profiles would be advantageous as a friend with multiple accounts would be represented as a single person (Golbeck & Rothstein, 2008).

FOAF is written in OWL and is a framework for representing information about people and their social connections (Golbeck & Rothstein, 2008). The full set of classes and properties available in FOAF are described in Table 6.4.1, adapted from (Golbeck & Rothstein, 2008).

By including FOAF into its design, the proposed information security education system has access to all user profiles published on the Semantic Web in FOAF format. Golbeck and Rothstein (2008) found only 11 of the 226 identified social network Web sites output FOAF files for their users, providing access to approximately 13,120,000 members. This number will increase over time as these social networks begin to move toward more suitable content management facilities, such as the Semantic Web. In order for FOAF objects to be linked between multiple social networks, a unique identifier is required so as to ascertain that the FOAF object read on one social network, for example, matches that of the same user on another.

For the purposes of this discussion, one of the most important semantic features of the FOAF is the *owl:InverseFunctionalProperty*. This inverse functional property connects an instance to a unique identifier (Golbeck & Rothstein, 2008) such as an identification number (ID Number) to a South African citizen. People within FOAF are described as an instance of the foaf:Person class, and thus **require a unique identifier**. Most FOAF social networking-enabled Web sites include at least one *foaf:mbox_sha1sum* for each user (Golbeck & Rothstein, 2008), which is a an SHA1 checksum generated based on the user's email address. The availability of such a key allows various semantic agents to merge profiles from different networks based on the Web, as depicted in Figure 6.5.

This facility enables pedagogical agents to learn more about the learner from their social network profiles and facilitates the development of the student model for the learner faster than can be done by manually by querying the learner. The preferences and past experiences with various aspects of information security are some of the concepts drawn from related FOAF objects. The education system will thus create its own FOAF instance for the user, built using the information merged from the social networks as

FOAF Basics	Personal Info	Online Accounts	Projects / Groups	Documents
Agent	weblog	OnlineAccount	Project	Document
Person	knows	OnlineChatAccount	Organization	Image
name	interest	OnlineEcommerceAccount	Group	PersonalProfileDocument
nick	currentProject	OnlineGamingAccount	member	topic (page)
title	pastProject	holdsAccount	membershipClass	primaryTopic
homepage	plan	accountServiceHomepage	fundedBy	tipjar
mbox	based_near	accountName	theme	sha1
mbox_sha1sum	workplaceHomepage	icqChatID		made (maker)
img	workInfoHomepage	msnChatID		thumbnail
depiction (depicts)	schoolHomepage	aimChatID		logo
surname	topic_interest	jabberID		
family_name	publications	yahooChatID		
givenname	geekcode			
firstName	myersBriggs			
	dnaChecksum			

Table 6.2: FOAF Classes and Properties Adapted from Golbeck & Rothstein (2008)

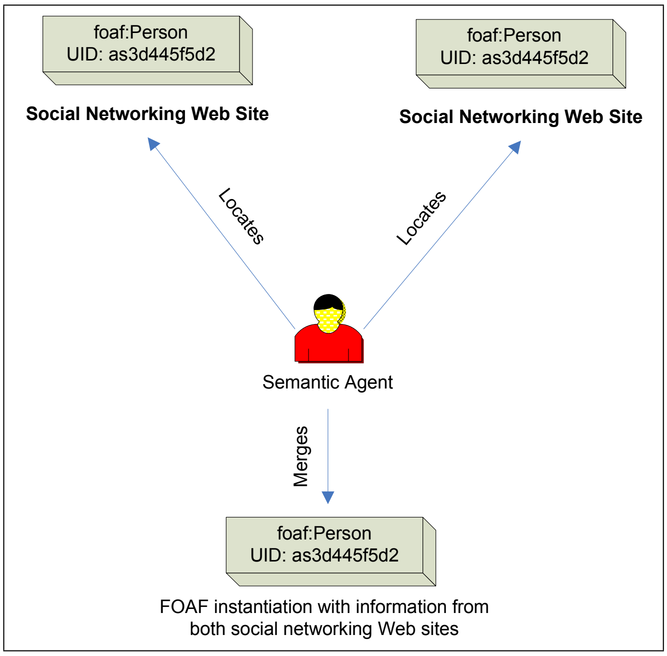

foaf:Person
UID: as3d445f5d2
Social Networking Web Site
foaf:Person
UID: as3d445f5d2
Social Networking Web Site
Locates
Locates
Semantic Agent
Merges
foaf:Person
UID: as3d445f5d2
FOAF instantiation with information from both social networking Web sites

Figure 6.5: Merging FOAF Profiles as Described by Golbeck & Rothstein (2008)

a starting point. This FOAF object will contain all information relating to the student model of the system, which is updated by the pedagogical agent as the learner progresses through the information security education course. **The FOAF object will thus provide a storage mechanism for remembering which information security concepts the learner has experience in and the extent of their knowledge therein**. Further to this, the FOAF instance is able to track the contributions the learner makes within the course, making use of the Documents attributes available within the object. The scores of such contributions will also be stored within the FOAF object and used in conjunction with other controls such as peer evaluations in order to determine and overall competency and credibility rating for the learner. **By querying the FOAF object of the information security education system, external applications are able to determine if the user meets the minimum information security awareness knowledge required** for accessing their Web site and if not, they are referred to the education system before allowing them access.

Another feature beneficial to information security education systems, which FOAF is able to address (Golbeck & Rothstein, 2008), is that of being a recommender. The system, based on the profiles of its learners, is able to perform recommendations as to which content the learner needs to read in order to be skilled in a particular concept. This feature is similar to intelligent curriculum sequencing exhibited by adaptive e-Learning systems; however, it gauges its recommendations based on a social aspect of the paths other learners have followed, rather than execute its own reasoning. User's FOAF profiles are used to determine their interests and find music which best matches their taste in some systems (Golbeck & Rothstein, 2008), so it stands to reason that the content required for educating learners can be ascertained the same way.

FOAF can also draw from its deep semantic pathways and reasoning to determine conflicts of interest within information security education systems (Golbeck & Rothstein, 2008). For example, when assigning reviewers to determine the skill level of a particular learner, the system is able to provide a list of reviewers who are best suited to the task. This review of work is required in order to solve the quality and credibility of works the learner produces on the system for others to view and draw knowledge from.

6.4.2 Assessing the Quality and Credibility of Works

The quality and credibility of works produced by users of e-Learning 2.0 systems was brought up as a problem with existing systems. The problem of quality was attributed to the fact that many authors work on various topics and, depending on the credibility of such authors, the quality may vary. This problem is solved by the system by attributing the credibility of authors to the quality of the work produced. Contributions by less credible authors are scored lower than those performed by highly credible authors. Furthermore, the system may request certain highly credible authors to review works as a whole and provide a score to them. These scores are then stored in Semantic Markup on the content and referenced by the ontology which describes information security topics. By performing a simple calculation on the credibility of authors (from their FOAF profile) and the score the topic was given by a credible author (from the semantic markup), the quality of the work is determined to a degree of certainty. The quality of work is required due to the fact that so much content will start to become available and learners searching for particular content should be presented with the most quality information available. The large-scale contribution by users of the system was discussed as another problem facing existing e-Learning 2.0 systems, a problem which the Semantic Web aims to solve.

6.4.3 Information Overload: Optimizing Searches

The Semantic Web was already shown as a more effective way of searching information stored on the Web. This is possible if such information is stored using semantic markup, linking it to various ontologies describing it. This feature would be extremely useful in an information security education system, as each information security concept and topic would be described by an ontology and thus the pedagogical agent could follow semantic pathways and retrieve information from multiple content servers, with all information pertinent to the query the learner put forward. In addition to this, pedagogical agents can communicate amongst one another, assisting each other using collaborative filtering techniques to further improve the efficiency of content location and retrieval.

One of the main benefits to learners and users of a Semantic Web-based system is that they are able to select the ontologies which define the search context of queries they execute (Devedzic, 2004). By doing this, pedagogical agents are able to filter the results of queries and only return content which is pertinent to the subject domain specified by the learner. The pedagogical agent does so by crawling the Web and finding documents whose semantic markup relates to the ontologies the learner selected when providing their search criteria. This facility promotes intelligent curriculum sequencing and thus allows the learner to drive the learning process, at their own pace.

In order for the agents to crawl pages and return significant results, semantic markup is required on pages which may be come across by a semantic web crawler. It is, therefore, important to discover which components should exhibit this markup.

6.4.4 What Should be Marked Up

One of the major decisions to be made in the development of an the proposed information security education system is deciding **what should be coded with semantic markup in order to be indexed by Semantic Web crawlers** . Devedzic (2004) suggests the following items which should be marked up in order to function successfully within such an environment:

- Educational Semantic Services
- User and Group Constraints and Preferences
- Agent Procedures.

Educational Semantic Services

Any service which is to be of service to pedagogical agents should exhibit semantic markup in order to describe themselves, their operation and the results which they produce. This is necessary as pedagogical agents will need to autonomously learn about a particular service from the service itself in order to understand its use and, therefore, make use of it when the need arises. For example, assuming the existence of a service which provides verification of secure passwords exists, this service should be marked up so that the pedagogical crawlers of an information security education system can locate and learn how to use it. This service will then be made available to learners within the system, educating them in secure password usage.

User and Group Constraints and Preferences

By modelling the learner and creating student models (using FOAF objects) for individual learners or groups of learners, the pedagogical agent is able to scour the Web and retrieve information and display it to the individual learner or group in a way which best matches their display preferences. This could mean information should be presented in textual format or a hybrid multimedia display.

Agent Procedures

The procedures of agents (also referred to as partial compositions of Semantic Web Services) such as an assessment procedure, needs to be marked up in order for sharing and re-using by other users to take place (Devedzic, 2004). If agents are to co-exist and share information using collaborative filtering, the page ranking, filtering techniques and evaluation procedures need to be open for review in order to provide a better understanding amongst themselves. Furthermore, agents who are searching similar topics should share the same ontologies, ensuring the results one agent produces regarding a particular search category matches the results produced by another agent executing the same query.

6.4.5 Standardizing Ontologies

In a perfect world, the creation of educational Web contents with ontological annotation, such as that used within the Semantic Web environment, should be supported by ontology-driven authoring tools and class hierarchies based on a number of standard ontologies for a particular subject domain (Devedzic, 2004). These standard ontologies will need to be created in order to provide a baseline from which all other information security content can be derived. Once this is in place, teaching and learning contents of Web-based information security educational applications can then be presented, edited, modified, and mixed consistently by the producers of the system, collaborating with one another (Devedzic, 2004). This form of group collaboration in learning promotes socio-constructivism which was highlighted in the previous chapter as the learning methodology required for a new era of information security education.

The standard ontologies for (information security) learning systems should cover a number of different domains, curriculum sequencing, student modelling, pedagogical issues, grading, and many more (Devedzic, 2004). Although the support for all possible domains and theories is not possible within an authoring system, the system should support easy access to Web pages created by other authors containing similar class hierarchies and using them as points of reference (Devedzic, 2004).

The only way learning systems on the Web which share domain and pedagogical knowledge amongst themselves will work is if a large number of ontologies surrounding these systems exist (Devedzic, 2004). Currently, this is not the case as there are few domain ontologies in existence and even fewer which cover instructional design and learning theories (Devedzic, 2004). For this reason, the learning community needs to come together and develop the standard ontologies in a collaborative way, much like the contributions to a wiki, where all users input is valued, condensed and refined by the community working toward a common goal.

One of the main reasons for the lack of standardized ontologies for learning is the apparent lack of standard vocabulary in the domain of education and instructional design (Devedzic, 2004). Many standards groups are in the process of addressing these and other issues, including IEEE Learning Technology Standards Committee - http://grouper.ieee.org/groups/ltsc/, Technical Standards for Computer-Based Learning, IEEE Computer Society P1484 - http://www.manta.ieee.org/p1484/, IMS Global Learning Consortium, Inc. - http://www.imsproject.org/, and ISO/IEC JTC1/SC36 Standard - http://jtc1sc36.org/ (Devedzic, 2004).

6.5 Conclusion

This chapter introduced a solution to the educating of users of computer systems world-wide. The problems associated with current e-Learning 2.0 systems were addressed through the use of the Semantic Web as a content storage and transport platform. It was argued that as most users today are affiliated with at least one social network (more often, multiple (Golbeck & Rothstein, 2008)) it is possible to harness the profiles and content these users created if they are divulged to the Semantic Web. This was shown to be possible using the Friend Of A Friend (FOAF) project, which allows the sharing of user profiles amongst various social networking Web sites.

By being allowed access to such profiles, an information security education system was shown to be able to generate its own FOAF object for each user, making it act as the student model for the learning environment. The FOAF profile was shown to be able to store information pertaining to the contributions the learner made to the system, their current level of understandings of various topics and their competency or credibility score. By creating this FOAF object, external applications would be able to query it and ensure that a potential user of their Web site is properly educated in information security and the risks the Web site may pose before allowing them entry. If the user was found to lack education (albeit a low or non-existent score), the user could be referred to the education system in order to complete the required education.

The following chapter illustrates the design of such an information security education system by way of example. It was discussed previously that one such service which an information security education system could make available, is that of password selection, management and protection. The example shows how such a system is developed and deployed and integrated into external applications running on the Semantic Web.

Chapter 7

Educating Users in Secure Password Management - A Case Study

7.1 Introduction

The previous chapter showed that it is possible to enhance information security education systems and allow them to reach all users of computers world-wide. It was argued that all of these users require education and this is made possible by implementing e-Learning 2.0 methods and technologies in conjunction with the Semantic Web.

The chapter also presented an example involving a semantic service, whereby information relating to passwords in computer systems could be taught to users of them. Passwords are often written down for easy recollection by the user; furthermore, the passwords chosen, if not managed correctly, are often simple dictionary words or important dates, such as the user's birthday. By following these password generation techniques, users make their passwords susceptible to brute force attacks or simple guessing by would-be attackers.

This chapter shows by way of an example case study that an e-Learning 2.0 and Semantic Web-based information security education system can aid in educating users in information security concepts, such as good password practices. The layout of the case study is presented in a format described by Creswell (2007), who recommends the presentation of case studies according to the following structure.

- Entry vignette
- Introduction
- Description of the case and its context
- Development of issues
- Detail about the selected issues
- Assertions
- Closing vignette

7.2 The Study

Users of computer systems are the weakest link in information security and need to be educated. One problem to address in this education is that of suitable password management practices. This includes the selection of a strong password and the confidentiality of the selected password. If a user selected a weak password, such as simple English words like "dog", "cat" or even their name or the name of a loved one, a would-be attacker could potentially guess it or use a brute force software application to run dictionary checks against it. If the password is found, the attacker could use the user's login credentials to access sensitive organizational or individual data, compromising its integrity. Likewise, if a user was negligent in keeping their password confidential, it could be accidentally disclosed to a passer-by who could later login with the user's credentials and access the same information. For these reasons, users should be educated in selecting good, strong passwords and furthermore be encouraged to keep them confidential.

7.2.1 Introduction

This case study demonstrates, by way of an example, the implementation of an information security education system using e-Learning 2.0 concepts, backed by the Semantic Web as a knowledge storage, filtering and transport agent. The example shows how the various components described in previous chapters fit together in order to educate the user in secure password management techniques. It further provides mechanisms for promoting awareness to the user after the education has been completed, in order to mitigate the risk of them forgetting what they learnt and acting insecurely.

7.2.2 Description of the Case and its Context

The example setting follows a computer user who signs up at two popular social networking Web sites, namely Facebook (http://www.facebook.com/) and MySpace (http://www.myspace.com). As far as could be determined, these applications do not currently exhibit any Semantic Web or FOAF support natively. This example illustrates certain advantages they would gain if they were to do so. Figure 7.1 depicts a sequence diagram, drawn in unified modeling language (UML), showing the sequences of events that take place in this case study.

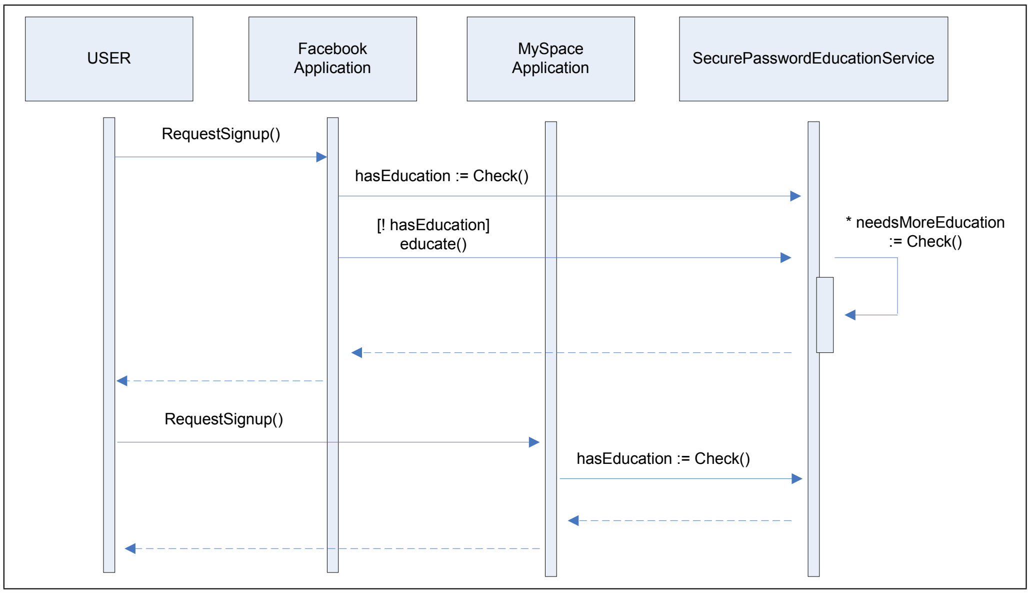
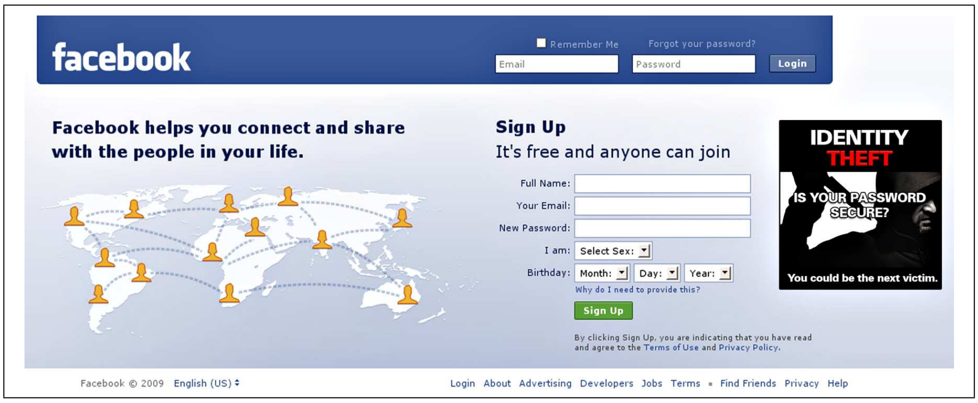


Figure 7.1: UML Sequence Diagram for the Case Study

A particular user browses to the Facebook homepage in an effort to sign up for an account. On the registration page, suppose a small advert is displayed, making the user aware that insecure passwords could lead to a compromise in their identity (see Figure 7.2). After the user has entered their email address, the primary key used by Facebook to identify a user, an SHA1 checksum is generated and the code is forwarded in realtime (unbeknownst to the user) to an information security education system which checks if it has any record of this user being educated in secure password selection. The system searches its database for records of the user and determines that the user has **not** had education in secure password selection. This result is then returned to the Facebook page and the user is presented with a popup, informing them that Facebook was unable to determine if they had been educated in secure password selection and stressing the need for such. It further asks the user if they would like to be educated before proceeding, which Facebook recommends. The user chooses to do so and the Facebook application provides an interface whereby interaction between the user and the secure password education service are facilitated.



Facebook helps you connect and share with the people in your life.

Sign Up

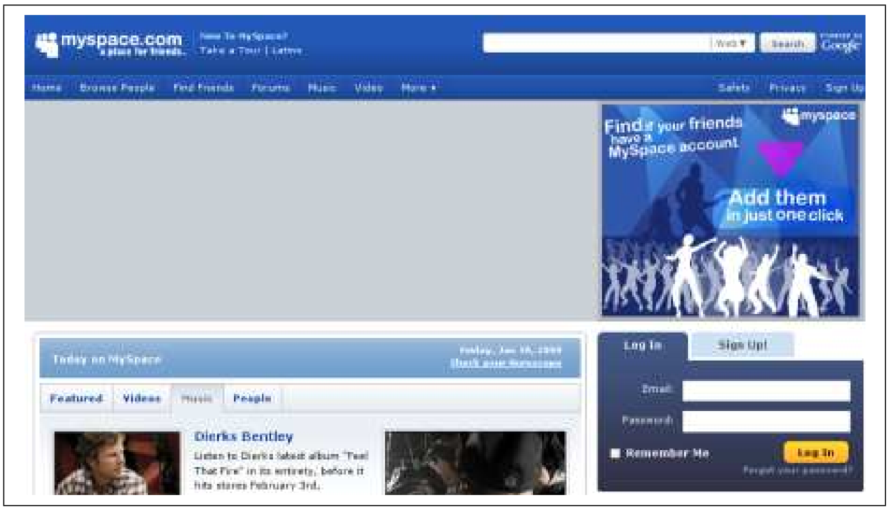
It's free and anyone can join

By clicking Sign Up, you are indicating that you have read and agree to the Terms of Use and Privacy Policy.

Facebook © 2009

Figure 7.2: Security Messages on Facebook

The password education service is unable to find an existing profile for this user on the Web and, therefore, requests that the user provide basic information such as their name and email address, so that it can build a profile. Once the user does so, they begin to interact with the information security education system. At the bottom of all content presented to the user is a link saying ”edit this information”, which allows the user to make changes to the information they were presented with for other users to see. The user opts not to make changes but rather continues to interface with the system until such time as the system determines the user is fully skilled in the selection of secure passwords and password management. Once this has been completed, the system asks the user if they have any content they would like to add to the process, to which the user answers ”no”. They are then redirected to the Facebook sign-up page. Facebook has already filled in the user’s name, email address and other information that it managed to receive from the information security education system. The user chooses a secure password, which Facebook accepts, thereafter permitting the user to complete the sign up process.



Listen to Dierks latest album "Feel That Fire" in its entirety, before it hits stores February 3rd.

Figure 7.3: MySpace Homepage

A few weeks later, the same user decides they would like to sign up with MySpace as well and so browse to the MySpace homepage (Figure 7.3). Upon entering the signup process and entering their email address, the system determines that the learner has an existing profile on Facebook and offers for this profile to be imported and synchronized with MySpace. The user requests this and after authenticating themselves to Facebook, their profile is synchronized. The MySpace signup process does not prompt the user to perform any education relating to secure password creation and management, but rather opts to display some awareness advert, reminding the user to act securely. The MySpace system did so as it had determined that the user was fully skilled in the concept of password management by providing the SHA1 checksum it generated from the user's email address to the information security education system, without interrupting the user's browsing experience. Once a secure password is selected, MySpace allows the user to complete the sign up process and begin modifying their MySpace profile.

7.2.3 Development of Issues

System Design

In this example, the system is comprised of a single semantic service, called "SecurePasswordEducationService". This service is described by an ontology called "SecurePasswordEducation", to which the SecurePasswordEducationService links by way of semantic markup, illustrated in Figure 7.5.

When a user arrives at the Facebook Web site and enters their email address on the sign up page, the Web site makes a call using AJAX, a technology driving Web 2.0, which provides asynchronous interactions between the client side and server side on Web applications using XML. This call is to the Facebook Information Security Education System, a pedagogical agent, which in turn calls the SecurePasswordEducationService, providing the SHA1 checksum of the user's email address. The SecurePasswordEducationService checks its list of FOAF objects and cannot find one with the same ID, thereby inferring that the user has not been educated by it in secure password selection and management (Figure 7.6). The service returns this information to the Facebook information security education pedagogical agent, which in turn forwards the result to the Facebook application, which recommends to the user that they should be educated in secure passwords in order to prevent them being a target of attack. The whole process, up to the time of Facebook recommending education to the user, is transparent and happens in the background. This process is described in more detail in Section 7.2.4

The user, who opts to follow such education, is presented by Facebook Web 2.0 tools, a subset of the Facebook pedagogical agent, which connects to the SecurePasswordEducationService, initializing a new education session.

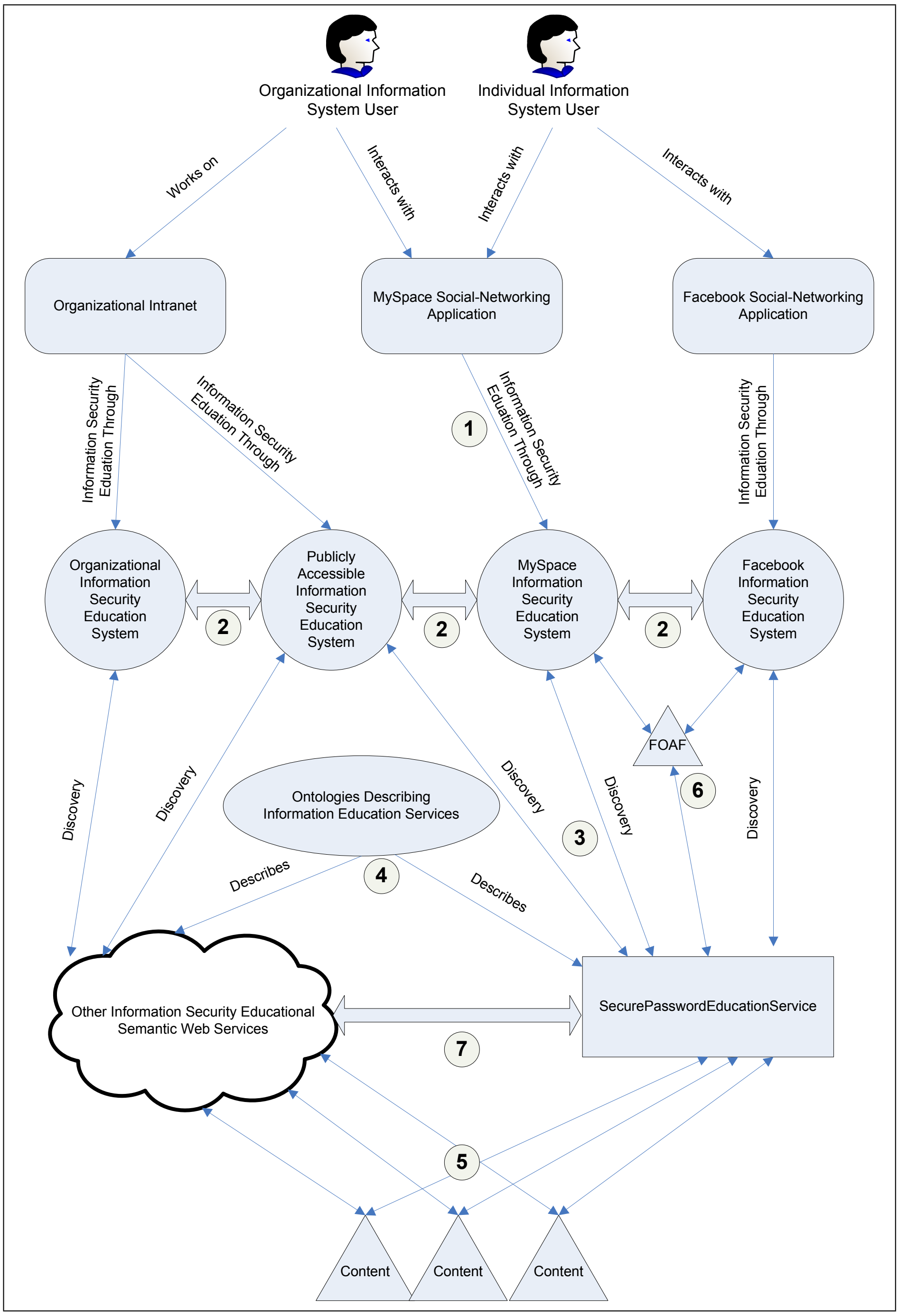

Organizational Information System User
Individual Information System User
Works on
Interacts with
Interacts with
Interacts with
Organizational Intranet
MySpace Social-Networking Application
Facebook Social-Networking Application
Information Security Eduation Through
Information Security Eduation Through
Information Security Eduation Through
Information Security Eduation Through
1
Organizational Information Security Education System
Publicly Accessible Information Security Education System
MySpace Information Security Education System
Facebook Information Security Education System
2
2
2
FOAF
6
Discovery
Discovery
Discovery
Discovery
Discovery
3
Ontologies Describing Information Education Services
4
Describes
Describes
Other Information Security Educational Semantic Web Services
SecurePasswordEducationService
7
5
Content
Content
Content

Figure 7.4: Graphical Representation of Information Security Process

During this time, a new FOAF object for this learner is created at the SecurePasswordEducationService and a new student model is populated, indicating their current state of information security education (at this point, nothing). If the user had an existing Facebook profile at the time of starting

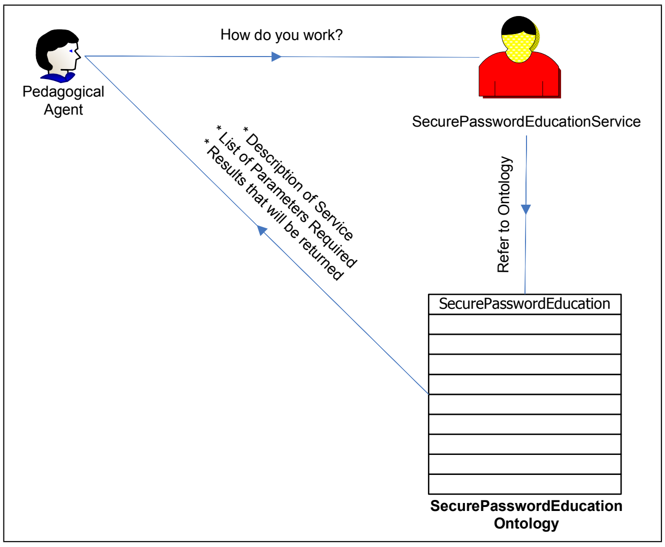

Pedagogical Agent
How do you work?
SecurePasswordEducationService
Refer to Ontology
* Description of Service
* List of Parameters Required
* Results that will be returned
SecurePasswordEducation
SecurePasswordEducation Ontology

Figure 7.5: Password Education Service Described by Ontology

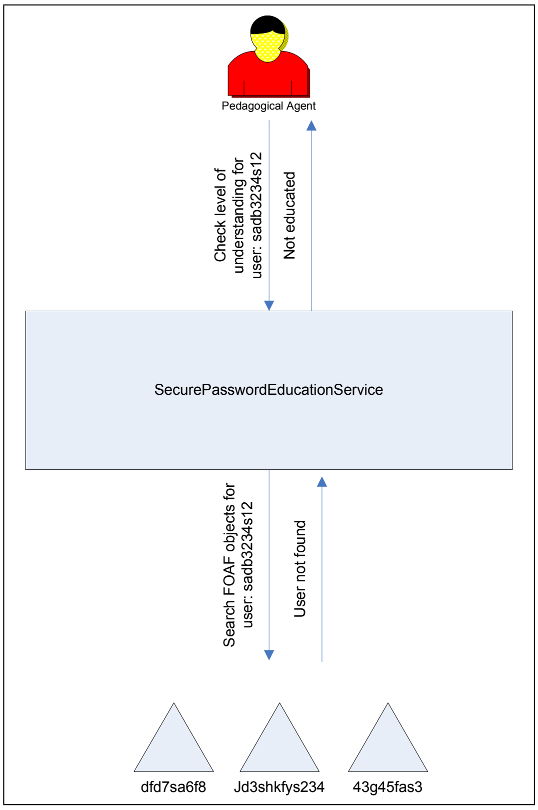

Pedagogical Agent
Check level of understanding for user: sadb3234s12
Not educated
SecurePasswordEducationService
Search FOAF objects for user: sadb3234s12
User not found
dfd7sa6f8
Jd3shkfys234
43g45fas3

Figure 7.6: User FOAF Not Found Implies Not Educated

the education course, Facebook could have supplied additional information to the secure password service, allowing it to present information to the user based on their preferences for display. This information would serve as a basis for the creation of their personalized student model (Figure 7.4 [6]).

The education system begins by presenting the idea of securing passwords in its simplest forms, starting with easy-to-understand concepts, such as ensuring users opt for passwords including extreme characters and not just alphanumerics, for example. At each point of the education process, the content presented to the learner provides a link titled "edit this content". If the user clicks on the link, they are presented with a graphical editor window, which allows them to change the content or post a comment for others to see. The system, before accepting the change, checks the rating of the content and that of the user who last updated the content. If the new learner has a lower rating and thus less experience with this topic than the last learner who modified the content, the new values will be disregarded or only allowed as a comment, in favour of the more credible existing content. If the new user has a higher rating than the previous user, the system uses its internal reasoning capabilities and will decide to accept the change the higher rated user supplied, thus adjusting the content for all future learners. As the information is saved, so the underlying semantic markup is modified to reflect the changes in content, so that applications, such as the Facebook pedagogical agent, are able to read and understand them.

Once the rating of the learner has reached sufficient levels, the learner is informed that they are now far more equipped to operate securely with passwords. At this stage, the learner is provided the opportunity to supply **new** content to the system for future learners to traverse. This content will be captured and stored on the system with semantic markup being created immaterial of the learner's rating in information security education. Future learners who traverse this content will be warned that the information they are viewing is not posted by a credible user (or the inverse) and they can make their own assumptions as to whether or not they will accept it or not. If the viewer of such knowledge is of higher rating than the learner who posted the new content, they have the option to correct or completely remove the content if they feel it harbours inaccuracies.

Once the learner has finished with their contributions and is sufficiently educated in secure password management, they are redirected to the Facebook sign up page. The secure password service, at this time, stores information relating to the level of understanding the user has achieved and the credibility of the user in their student model within the FOAF object describing them and stored on the Semantic Web. This FOAF object can then later be referenced and updated if the student performs additional education or other Web sites request credibility of the user in terms of certain information security concepts.

This is evident when the user attempted to sign up at MySpace some time later. MySpace, after receiving the user's email address, produced a SHA1 checksum for it and passed it to the secure password service for verification of information security education using an AJAX function similar to that used by Facebook. The service determined that this user was, infact, educated in secure password management, therefore, did not recommend that they require additional education at the time. MySpace thus opted to present a simple banner reminding users to choose secure passwords and offering a link to the education system, should the user require a refresher course.

The pedagogical agents that Facebook and MySpace use are able to exhibit forms of collaborative filtering (Figure 7.4 [2]), allowing various discoveries (such as that of new information security education services) to be shared, to optimize searches by learners of the system. Just like the pedagogical agents collaboratively filter services, so do the various services collaboratively filter and share information about content they have located and indexed (Figure 7.4 [7]). To facilitate the automatic discovery of Semantic Web services and their usage instructions, ontologies are created and linked by way of semantic markup (Figure 7.4 [4]).

A few implementation issues surround the case in question, which need investigating and further information provided in order to justify the case. Some of these issues include **the generation of suitable educational content**, the **adaption of the education interface to the preferences and learning style of the user** and the **accurate describing of semantic services for automatic discovery by semantic agents**. These issues are addressed in the following section.

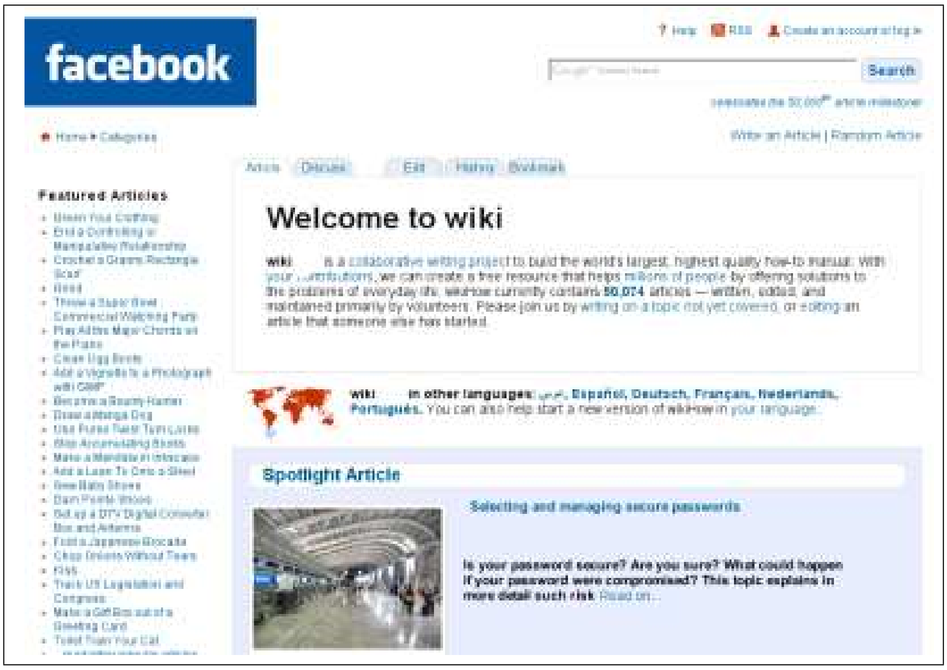
7.2.4 Detail about the Selected Issues

One of the most costly and time-consuming aspects of education is the development of course material. In addition to this, planning the sequence in which to educate users adds further complications. The following section illustrates how course material is created in this example and, therefore, shows how it could be done in other similar information security education systems.

Content Generation

Content generation for systems, such the one in this example, is generated by the users of such systems. Consider, for example, a user of an organization, who is prompted by the intranet, on which he is working, that it cannot determine his level of understanding of password management (Figure 7.4 refers). The system made a call to its pedagogical agent, having it query the SecurePasswordEducationService transparently and inquire as to the level of understanding the user has with secure passwords. As the semantic service did not find a FOAF object for this user, detailing their level of understanding in password management, it had no point of reference and so reasoned that the user is, therefore, uneducated. The user opted to initiate an education session and ran through the various questions, providing answers and reading other learner's posts to the same topics. At the end of the education session, the user decided they had some knowledge to contribute which would benefit other learners and so directed the system to creating a new post. The system presented the user with a wiki-style interface (Figure 7.7), on which they captured the content. As this was the first time using the system, it had no previous rating for this user and so the content posted was done so under a low score.

By scoring, or rating, the content with a low score, the system warns would-be learners traversing the content of the lack of credibility of such information, as determined by the rating of the author who created it. As a more credible author RIPs the initial content, MIXing it with their understanding of it and then FEEDing it back to the system, the rating of the



Welcome to wiki

wiki is a collaborative writing project to build the world's largest, highest quality how-to manual. With your contributions, we can create a free resource that helps millions of people by offering solutions to the problems of everyday life. wikiHow currently contains 50,074 articles — written, edited, and maintained primarily by volunteers. Please join us by writing on a topic not yet covered, or editing an article that someone else has started.

wiki in other languages: عربي, Español, Deutsch, Français, Nederlands, Português. You can also help start a new version of wikiHow in your language.

Spotlight Article

Selecting and managing secure passwords

Is your password secure? Are you sure? What could happen if your password were compromised? This topic explains in more detail such risk Read on...

Figure 7.7: Example of Wiki in Education

content now changes to a higher value due to the increased credibility of the second author. This rating value is associated to the content and stored as semantic markup within it for easy reference by machine users. This is useful, as **when users are searching for information** within the system, they have the **ability to filter out content which does not meet a minimum level of credibility**. In addition to the credibility of the document, the authoring software used to modify the content automatically added additional semantic markup to the information, including "tags" specifying the categories this information is associated with. These tags are used by semantic web crawlers to match specific search criteria supplied to them by their users and, therefore, assist in indexing information for easy retrieval.

A certain level of control is required in order to ensure the quality of the information does not depreciate. In this example, it would make no sense that a seemingly uneducated user could open an existing topic, created by an expert in the field of password security, and change it to reflect a totally different perspective. For this reason, the system is able to reason as to who can modify data, using the internal inference rules of the ontologies which describe the data. If the user has a lower credibility rating than the original author of the content, the user should not be permitted to make changes to the information, but rather only provide side comments. These comments can be picked up by other learners and potentially integrated into the content itself by a more credible author. In so doing, the rating for the less experienced author increases, as does the rating of the content.

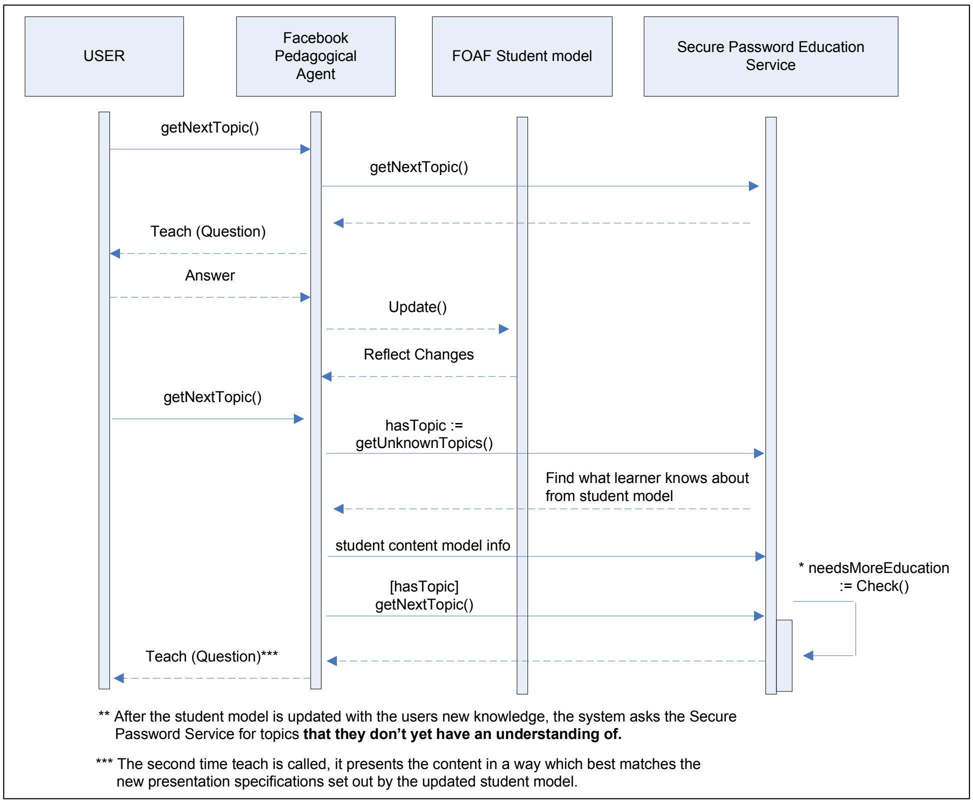
By allowing content creation to be a social endeavour, the learners of the system are held responsible for their and their peer's education success. Content generated with semantic markup can not only be read by machine users, but also understood, allowing machines to adapt the information to the learners of the system.

Content Adaption

Pedagogical agents, by implementing a student model within the FOAF object describing a learner, are able to adapt both the content presentation techniques as well as the content information to the learner. The user attempting to sign up at the Facebook Web site was referred to education prior to being allowed to complete the sign up process. As the Facebook application did not have an initial understanding of the level of understanding the user had with password security, it presented the user with a set of questions and answers, posed in a variety of ways, including textual and graphical formats. The responses generated by the user were noted in the student model and the agent was able to analyze these results, generating an understanding of firstly the extent of knowledge the user currently has with regard to subject domain and secondly, the best and most effective way to present such information back to the user (Figure 7.8).

The pedagogical agent stores this information within the FOAF object it creates for the user, for use in this and future education sessions. The agent uses this information to gauge the level of understanding the user has in certain concepts and provide insight as to the best way to present the unknown content to the user. The updating of the student model by the pedagogical agent is a continual process, with changes being reflected immediately.

For example, suppose the user signing up for Facebook in this example


USER
Facebook Pedagogical Agent
FOAF Student model
Secure Password Education Service
getNextTopic()
getNextTopic()
Teach (Question)
Answer
Update()
Reflect Changes
getNextTopic()
hasTopic := getUnknownTopics()
Find what learner knows about from student model
student content model info
* needsMoreEducation := Check()
[hasTopic] getNextTopic()
Teach (Question)***

** After the student model is updated with the users new knowledge, the system asks the Secure Password Service for topics **that they don't yet have an understanding of.**

*** The second time teach is called, it presents the content in a way which best matches the new presentation specifications set out by the updated student model.

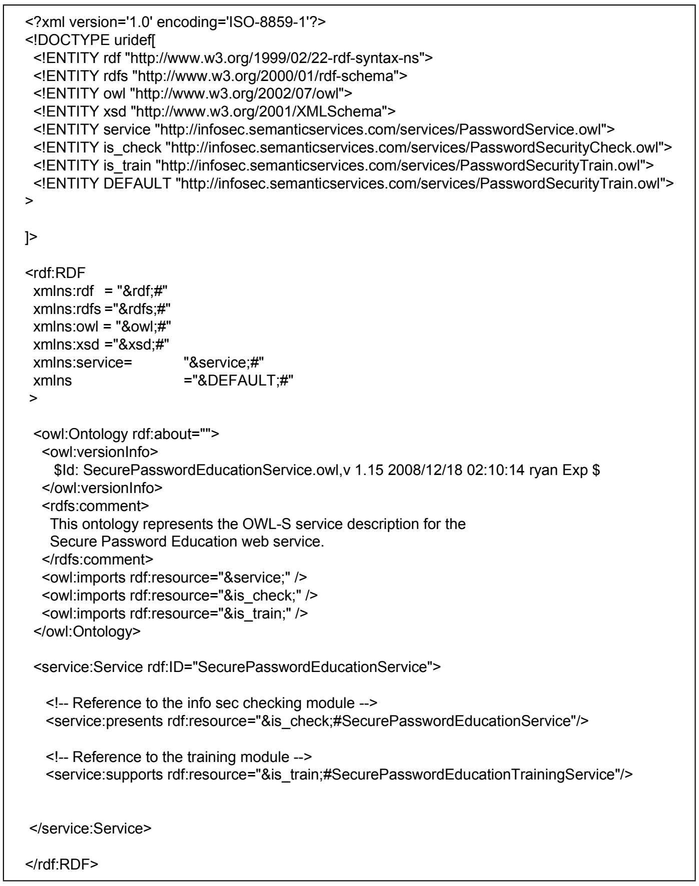
Figure 7.8: Adaptivity Process of System

preferred a textual representation of content, presented in simple, concise bullet points on a Web page. The pedagogical agent would pick up on this during the questions and answers process and thus all concepts related to secure passwords would be presented to the user as such. As each concept is presented, the learner interacts with it, by posting comments, editing the current content or simply reading it. As an understanding of each concept is acquired, determined by the agent based on the responses the user makes whilst interacting with the system, it is stored within the student model and a rating of understanding assigned to it.

Retrieval of content for display is notably difficult on the existing Web, as information is stored mostly in a format only suitable for human understanding. The Semantic Web aims to change that, by providing more machine understandable content by use of ontologies, describing various content and services. This case study followed the use of one such service, the SecurePasswordEducationService, which was used to firstly establish the current level of understanding a user has with secure passwords and then secondly to provide content related to educating users in secure password management.

The SecurePasswordEducation Ontology

The OWL-S (Web Ontology Language for Services) code for the SecurePasswordEducation ontology which describes the use of the SecurePasswordEducationService is provided in Figure 7.9.



```
<?xml version='1.0' encoding='ISO-8859-1'?>
<!DOCTYPE uridef[
 <!ENTITY rdf "http://www.w3.org/1999/02/22-rdf-syntax-ns">
 <!ENTITY rdfs "http://www.w3.org/2000/01/rdf-schema">
 <!ENTITY owl "http://www.w3.org/2002/07/owl">
 <!ENTITY xsd "http://www.w3.org/2001/XMLSchema">
 <!ENTITY service "http://infosec.semanticservices.com/services/PasswordService.owl">
 <!ENTITY is_check "http://infosec.semanticservices.com/services/PasswordSecurityCheck.owl">
 <!ENTITY is_train "http://infosec.semanticservices.com/services/PasswordSecurityTrain.owl">
 <!ENTITY DEFAULT "http://infosec.semanticservices.com/services/PasswordSecurityTrain.owl">
>

]>

<rdf:RDF
 xmlns:rdf   = "&rdf;#"
 xmlns:rdfs ="&rdfs;#"
 xmlns:owl = "&owl;#"
 xmlns:xsd ="&xsd;#"
 xmlns:service=          "&service;#"
 xmlns                   ="&DEFAULT;#"
 >

 <owl:Ontology rdf:about="">
  <owl:versionInfo>
    $Id: SecurePasswordEducationService.owl,v 1.15 2008/12/18 02:10:14 ryan Exp $
  </owl:versionInfo>
  <rdfs:comment>
   This ontology represents the OWL-S service description for the
   Secure Password Education web service.
  </rdfs:comment>
  <owl:imports rdf:resource="&service;" />
  <owl:imports rdf:resource="&is_check;" />
  <owl:imports rdf:resource="&is_train;" />
 </owl:Ontology>

 <service:Service rdf:ID="SecurePasswordEducationService">

   <!-- Reference to the info sec checking module -->
   <service:presents rdf:resource="&is_check;#SecurePasswordEducationService"/>

   <!-- Reference to the training module -->
   <service:supports rdf:resource="&is_train;#SecurePasswordEducationTrainingService"/>


 </service:Service>

</rdf:RDF>
```

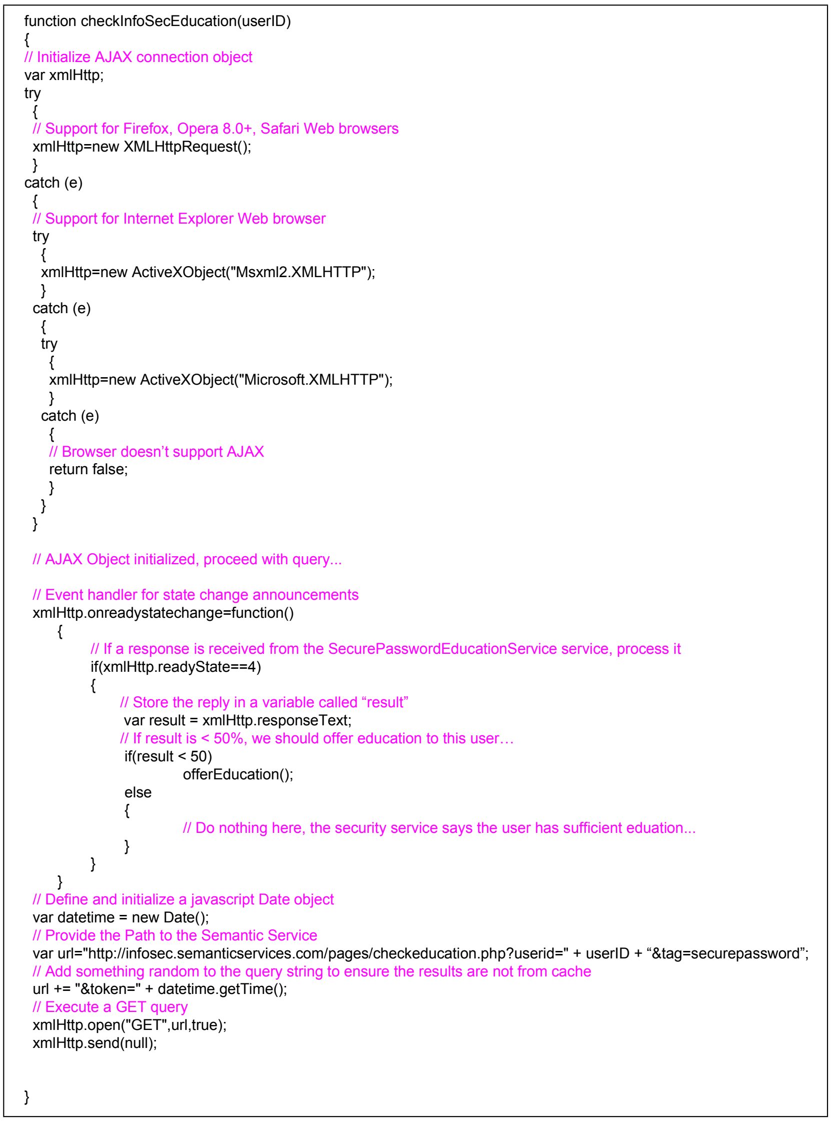
Figure 7.9: Ontology Describing SecurePasswordEducationService

This ontology is referenced by the Semantic Web Service using semantic markup, which allows semantic agents to understand the functionality of the service and thus enable it to use it automatically. In this example, the provision of such an ontology allowed both the Facebook information security education pedagogical agent and the organizational pedagogical agent to understand the use of the SecurePasswordEducationService, providing access to the service to users of their respective environments.

It was discussed that the pedagogical agent was invoked transparently to check if a particular user, identified by their email address, had sufficient education in information security. AJAX, one of the technologies responsible for the success of Web 2.0, was used to accomplish this.

AJAX Calls

AJAX was discussed as a transparent process whereby Web-based applications could communicate with server side applications without interfering with the Web browser's experience. Javascript contains certain events which are fired, based on the user's interactions with a Web page. In the example, once the user had typed their email address, the system queried the SecurePasswordEducationService service through the use of AJAX. This was possible by using the onblur event of the html form input box where the user typed their email address. The code for the AJAX function which was called is shown in Figure 7.10



```
function checkInfoSecEducation(userID)
{
// Initialize AJAX connection object
var xmlHttp;
try
 {
 // Support for Firefox, Opera 8.0+, Safari Web browsers
 xmlHttp=new XMLHttpRequest();
 }
catch (e)
 {
 // Support for Internet Explorer Web browser
 try
  {
  xmlHttp=new ActiveXObject("Msxml2.XMLHTTP");
  }
 catch (e)
  {
  try
   {
   xmlHttp=new ActiveXObject("Microsoft.XMLHTTP");
   }
  catch (e)
   {
   // Browser doesn't support AJAX
   return false;
   }
  }
 }

 // AJAX Object initialized, proceed with query...

 // Event handler for state change announcements
 xmlHttp.onreadystatechange=function()
      {
              // If a response is received from the SecurePasswordEducationService service, process it
              if(xmlHttp.readyState==4)
              {
                     // Store the reply in a variable called “result”
                      var result = xmlHttp.responseText;
                     // If result is < 50%, we should offer education to this user…
                      if(result < 50)
                                   offerEducation();
                      else
                      {
                                   // Do nothing here, the security service says the user has sufficient eduation...
                      }
              }
      }
 // Define and initialize a javascript Date object
 var datetime = new Date();
 // Provide the Path to the Semantic Service
 var url="http://infosec.semanticservices.com/pages/checkeducation.php?userid=" + userID + “&tag=securepassword”;
 // Add something random to the query string to ensure the results are not from cache
 url += "&token=" + datetime.getTime();
 // Execute a GET query
 xmlHttp.open("GET",url,true);
 xmlHttp.send(null);


}
```

Figure 7.10: AJAX Code to Check Education Status

The AJAX function called provides the secure password education service with the unique key to identify the learner and awaited a response from the service, expecting a user rating to be returned in integer format. The AJAX method provided statically connects to the Semantic Web Service and knows what to pass the function and what to receive as a reply.

As can be seen, all aspects of system design were catered to using e-Learning 2.0 and Semantic Web technologies to provide an autonomous, self-sustainable education platform for educating all users, from organization information systems to those of individuals. One problem that was noted during this case study, was the **lack of standard ontologies currently available**.

Lack of Standard Ontologies

In order for pedagogical agents to offer services such as the SecurePasswordEducationService, the agent should be able to crawl various ontologies to get information related to shared understandings of information security principles. These shared understandings help to resolve ambiguity and double meanings of terms, which may arise from the development of various services, as they are developed by differing authors. With the lack of standardized ontologies, systems may have access to content which they can understand and semantic web services which they able to locate; however, it would not be able to interpret their usage (Figure 7.11).

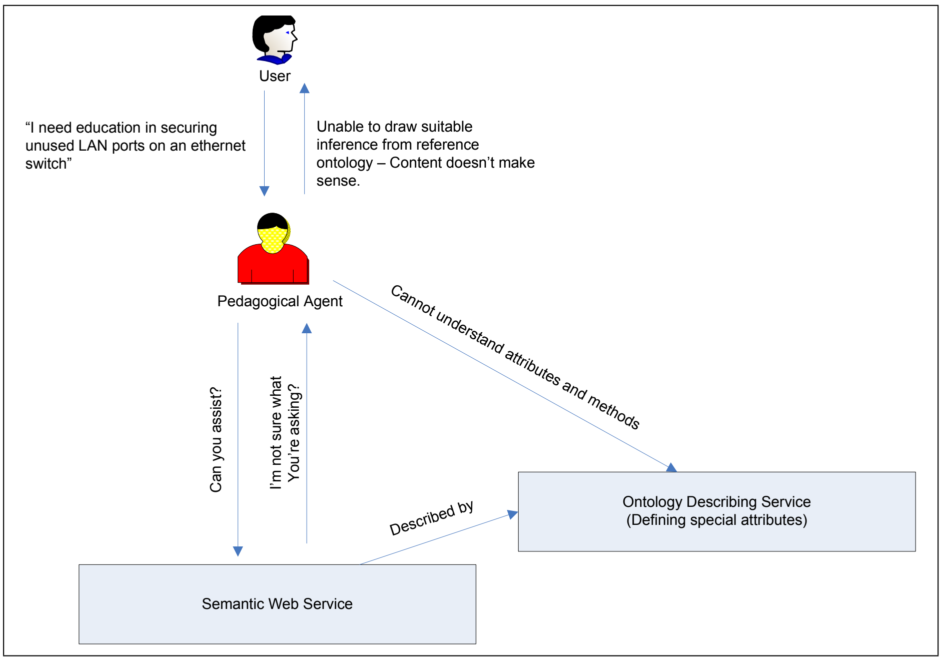

User
"I need education in securing unused LAN ports on an ethernet switch"
Unable to draw suitable inference from reference ontology – Content doesn't make sense.
Pedagogical Agent
Cannot understand attributes and methods
Can you assist?
I'm not sure what You're asking?
Described by
Ontology Describing Service (Defining special attributes)
Semantic Web Service

Figure 7.11: Semantic Web with No Standard Information Security Ontology

Without standard ontologies, pedagogical agents are unable to determine the meaning of certain attributes of information. Fortunately, the need for standard ontologies in order to ensure the continued progression of Web-based technologies has been identified and is currently being addressed by certain working groups, such as the Institute of Electrical and Electronics Engineers Standard Upper Ontology (IEEE SUO) Working Group (http://suo.ieee.org/). With the introduction of such standard ontologies (Figure 7.12), the continued growth of the Semantic Web seems imminent.

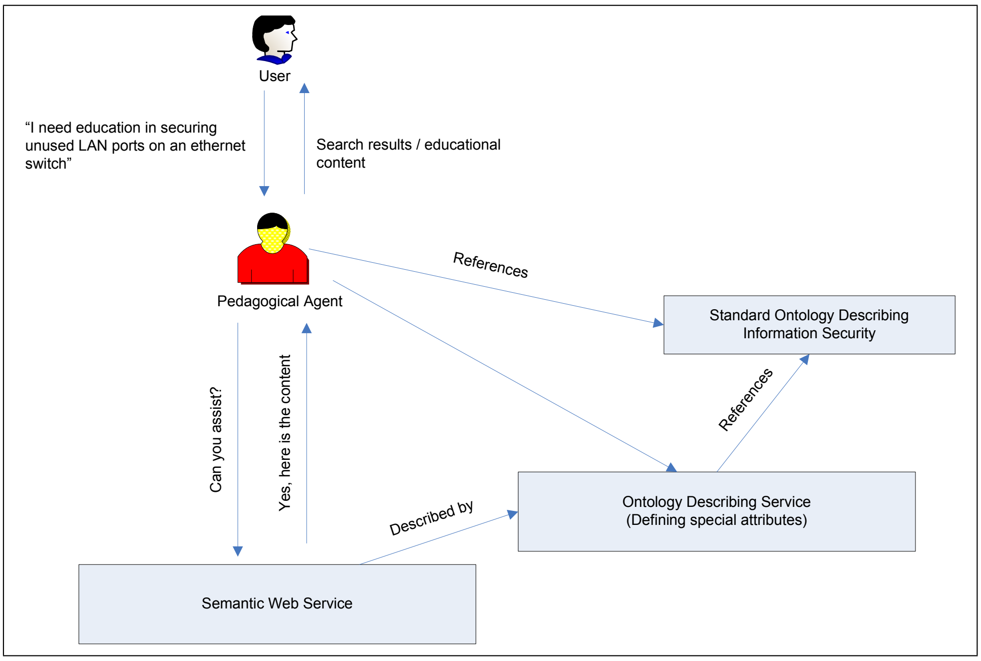

User
"I need education in securing unused LAN ports on an ethernet switch"
Search results / educational content
Pedagogical Agent
References
Standard Ontology Describing Information Security
References
Can you assist?
Yes, here is the content
Described by
Ontology Describing Service (Defining special attributes)
Semantic Web Service

Figure 7.12: Semantic Web with Standard Information Security Ontologies

7.2.5 Assertions

From this case study, the following assertions can be drawn:

- **Content generated by learners of the system can be of high quality and is, therefore, suitable for reference in education systems**. By harnessing the power of collective intelligence, such content stands a chance of being of higher quality than most other content generated for current educational systems.

- **The Semantic Web and its underlying technologies and methods do enhance the e-Learning 2.0 education system, making it suitable for use for information security education**. By providing machine-understanding to content generated and stored in the education system, users are able to run more accurate and concise queries, returning only information pertinent to the search.

This case study serves to show that some, if not all, of the technical issues of educating users in secure password management are able to be addressed by e-Learning 2.0 systems using the Semantic Web. The Semantic Web was found to be able to describe secure passwords using an ontology, written in the OWL ontology language. It is therefore possible that e-Learning 2.0 and the Semantic Web together as an information security education system will be able to educate users in information security concepts and principles.

It is, however, the researcher's opinion that more standard ontologies are required before such an education system becomes a reality. As the Semantic Web continues to grow in modern times, these ontologies will be developed and thus information security education using e-Learning 2.0 and the Semantic Web will be a viable option to consider in educating all users of computer systems, world wide.

7.3 Conclusion

E-Learning 2.0 and the Semantic Web have been used in numerous domains for educating learners. This chapter showed that using such technologies and methods, information security concepts were able to be taught to users of computer systems, giving existing information security systems a much broader reach in terms of accessing users and providing a more sound, flexible and dynamic content model from which to draw inference.

This case study presented an example of how the various components of an e-Learning 2.0 based on Semantic Web education system could be built, if the standard ontologies were available. It is the researcher's belief that the introduction of standard ontologies to the Semantic Web for learning, will see many new fields of study migrate to such systems, including information security education.

Chapter 8

Conclusion

8.1 Introduction

The objective of this study was to provide, by means of argument and a comprehensive example, a solution for the creation of collaborative information security education content and the education of users in information security, based on the principles of e-Learning 2.0 and the Semantic Web as the primary content storage and retrieval mechanism. This was accomplished by addressing the various sub-objectives.

The first sub-objective was to **clearly demonstrate Web 2.0 and its benefits in overcoming the downfalls of current information security education systems in educating all users of computer systems, independent of their role within the system**. Argumentation was provided in Chapters 3-5 that e-Learning in collaboration with Web 2.0 technologies (e-Learning 2.0) could solve many of the problems associated with current information security education, including the customization of course material for learners depending on their roles within an information system. e-Learning 2.0 was further found to enable the users to contribute to the system, allowing them a sense of ownership and thus motivating them in the education process. E-Learning 2.0, furthermore, provided mechanisms to support informal, collaborative learning amongst learners of the system. This was found to be far more effective in educating learners than traditional, formal education, as 80-90% of learning occurs informally, outside of the classroom environment.

The second sub-objective was to **clearly demonstrate the Semantic Web and its benefits for enabling the development and deployment of such an information security education**. The benefits were illustrated in the example presented in Chapter 7, where an implementation of the proposed system was demonstrated. It was found that through the use of the Semantic Web, inter-application sharing of content and knowledge relating to users was possible, the discovery and implementation of such becoming a fully automated process. This was possible through the use of ontologies, which describe the various services and content on the Web, providing more meaning to information published on the Web and therefore providing machines with the ability to understand it.

As far as could be determined, there existed no information security education system suitable for this task available at the time of writing, based on e-Learning 2.0 and the Semantic Web. This meant that much of the information presented within this dissertation could not be based on previous knowledge, but rather had to be discovered as the research progressed.

8.2 Research Contributions

The first part of the project was devoted to the discovery of the importance of information in both the organizational and individual user sectors. This led to the discovery that information was important for both organizations and individuals and, therefore, needed to be protected.

Information security was described as the balancing of risks and controls (safeguards) in order to ensure a minimum amount of protection to information within computer systems. The overall protection of information systems was found to rest on the shoulders of the users of such systems, who were found to be the greatest threat to them. As users are the greatest threat to information, they need to act securely in their interactions with such systems. One way to help them act securely is to change their behaviour, which was discovered to be possible through the development of an information security culture. Although information security culture was recognized as a large and important aspect of information security, it did not form part of the focus of this dissertation. The dissertation rather focused on one of the keys to the successful development of such a culture, namely education.

Most current information security education systems were found to be based on a learning continuum as set out by NIST. This learning continuum was, however, evaluated and it was found that it was **geared toward the education of adults within the organizational context**. As all users of computer systems (organizational and individual) require education, a **new information security education system was required to address the changing target audience**. The target audience of information security education changed from one that is organizational only to **include all users of computer systems of all ages**. The requirements of such users were investigated in order to gather background information for the development of an approach for the education of these users. Current information education systems were discovered to be based primarily on traditional classroom education (objectivist approach to learning), whilst many **learning experts argued that education should be learner-centric** (constructivist-based) for best results. This was attributed to the fact that the **majority of learning occurs informally outside of the classroom environment**. It, therefore, followed suit that information security education systems of the future would benefit from harnessing this fact and promoting information learning within the education environment.

One such technology which was identified as a possible candidate for the development of an information security education system to solve these problems was the World Wide Web. In order for the Web to be successful in the educating of users of computer systems world-wide, it would need to support various learning methods discovered and **include modes of formal, as well as informal, learning**.

A discussion on the development and progression of Web-based education systems showed that **through the use of adaptive and intelligent technologies, e-Learning is able to address many of the problems associated with current information security education**; however, it needed to be enhanced in order for informal learning to occur within it.

Web 2.0, one of the modern trends in the progression of the Web as a whole, was found to add value to e-Learning and thus information security education based on e-Learning, by providing the **ability for learners to contribute to the system, including the facilitation of informal discussions between the learners themselves**. Learners were further encouraged by the technology to contribute to the content base from which the system drew inference whilst educating learners. This raised additional problems, including the credibility of works and authors as well as the filtering of the potentially large volumes of information produced in order to provide learners with concise, accurate search results.

The Semantic Web, it was argued, is able to solve these problems by **creating profiles for each learner and assigning a credibility rating for each user** to their profile. This profile could then, due to the nature of the Semantic Web, **be viewed by any application which had a Semantic Web reach, allowing other Web sites such as social networks to interconnect with the information security education system and determine the level of understanding a particular users has on a certain security topic**. This was made possible using the Friend Of A Friend (FOAF) design specification to represent people as objects within the Semantic Web. Using such systems, social networking Web sites could share profile information relating to the same user and also share such information with information security education systems, assisting in the development of their student model. These contributions **assist the information security education system in further customizing search results and the learning environment's interface to the preferences and specific needs of the learner**.

This concept was argued in Chapter 7 and it was established that **such a system is possible to implement for educating users in information security**. This was **demonstrated by way of an example case-study as the large-scale deployment of standard ontologies on the Semantic Web have yet to be developed**. Chapter 7 thus provided a "proof of concept" for the implementation of the ideas of this dissertation, showing in detail the construction and analysis of such a learning system.

8.3 Possible Further Enhancements

It is important to realize that the inclusion of Semantic Web technologies opens a lot of doors for future researchers to investigate with regard to information security education. Examples of such include the use of mobile devices, such as cell phones and personal desktop assistants (PDA) to connect to the information security education system and educate users in acting securely wherever they may be at the time. This mobility and easy access to information whilst being mobile is causing a stir in current Web trends, potentially giving rise to the next version of the Web, namely Web 3.0. Web 3.0 is described by many as the movement from connecting people and information on the Web, to the connecting of knowledge. It does this through the use of the Semantic Web and Web 2.0 technologies and is therefore necessary for further investigation.

Additionally, this dissertation noted that the development of standard ontologies held back the development and deployment of the proposed information security education system. It would be reasonable for researchers therefore to investigate the standardizing of information security education ontologies, thereby facilitating the coming to fruition of the proposed system in modern society.

8.4 Conclusion

This project has shown that e-Learning 2.0 is a very suitable tool for information security education and that e-Learning 2.0-based information security education programs are indeed possible through the use of the Semantic Web. It is the author's belief that, **once the problem of creating common ontologies for information security has been addressed, such systems will be the delivery method of choice for information security content.**

References

Ashcraft, D., Treadwell, T., & Kumar, V. (2008). Collaborative online learning: A constructivist example. *MERLOT Journal of Online Learning and Teaching, 4*(1).

Berners-Lee, T., Hendler, J., & Lassila, O. (2001). The semantic web. *Scientific American.*

Brusilovsky, P., & Peylo, C. (2003). Adaptive and intelligent web-based educational systems. *International Journal of Artificial Intelligence in Education, 13.*

Carr, N. (2003). It doesnt́ matter. *Harvard Business Review.*

Clarke, D. (2002). E-learning - big bang or steady evolution. *Learning Technologies.*

Cook, P. (2006). The project approach: An appreciation for the constructivist theory. *Published by the Forum on Public Policy.*

Creswell, J. W. (2007). *Qualitative inquiry and research design: Choosing among five traditions. thousand oaks, ca: Sage 2nd edition, 2007.* Thousand Oaks, CA: Sage.

Devedzic, V. (2004). Education and the semantic web. *International Journal of Artificial Intelligence in Education, 14*, 39-65.

Donnelly, M. (2008). Hypermedia in education. *Research Starters Education.*

Downes, S. (2005). E-learning 2.0. *[WWW document]. URL http://www.elearnmag.org/subpage.cfm?section=articles&article=29-1, Sited 25 May 2008.*

Downs, S. (2006). Learning networks and connective knowledge. it forum. *[WWW document]. URL http://it.coe.uga.edu/itforum/Previous.html, Sited 25 September 2008.*

Flew, T. (2008). *New media: An introduction* (3rd ed.). Melbourne: Oxford University Press.

Froschl, C. (2005). *User modeling and user profiling in adaptive e-learning systems.* Unpublished master's thesis, Graz University, Austria.

Geser, G. (2007). Open educational practices and resources. *[WWW document]. URL http://www.olcos.org/, Sited 27 September 2008.*

Gladun, A., Rogushina, J., Garcia-Sanchez, F., Martinez-Bejar, R., & Fernandez-Breis, J. (2009). An application of intelligent techniques and semantic web technologies in e-learning environments. *Expert Systems with Applications*, *36*, 1922-1931.

Goguen, A., Stoneburner, G., & Feringa, F. (2002). Risk management guide for information technology systems. *NIST Special Publication 800-30.*

Golbeck, J., & Rothstein, M. (2008). Linking social networks on the web with foaf. *In the Proceedings of the 17th international conference on World Wide Web (WWW2008).*

Guild eLearning. (2006). Future directions in e-learning research report 2006. *The e-Learning Guild Research.*

Hardless, C., & Nulden, U. (1999). Mandatory participation as examination. *In Proceedings of the World Conference of the WWW and Internet (WebNet), Honolulu, AACE, 1999.*

Hay, D. (2008). Developing dialogical concept mapping as e-learning technology. *British Journal of Educational Technology.*

Heath, T., & Motta, E. (2007). Ease of interaction plus ease of integration: Combining web 2.0 and the semantic web in a reviewing site. *Web Semantics: Science, Services and Agents on the World Wide Web.*

Johnston, J., Eloff, J., & Labuschagne, L. (2003). Security and human computer interfaces. *Computers and Security*, *22*(8).

Khalifa, M., & Lam, R. (2002). Web-based learning - effects on learning process and outcome. *IEEE Transactions on Education*, *45*.

Lenard, T., & Britton, D. (2006). *The digital economy fact book* (Eighth ed.). The Progress and Freedom Foundation.

Liaw, S. (2001). Designing the hypermedia-based learning environment. *Intl Journal of Instructional Media*, *28*(1).

Mason, J. (1996). *Qualitative researching.* SAGE Publications.

Massy, J. (2002). Quality and elearning in europe summary report 2002.

Mckiernan, G. (2005). Disruptive technologies for dynamic possibilities. *[WWW document]. URL http://www.public.iastate.edu/ gerrymck/TICER2005.ppt, Sited 26 Sept 2008.*

Mejias, U. (2008). Teaching social software with social software. *Innovate: Journal of Online Education*, *2*(5).

Mitnick, K., & Simon, W. (2002). *The art of deception: Controlling the human element of security.* Wiley Publishing.

Nagaraj, N. (1999). No dice. *Praxis - Business Line's journal on management*, *2*.

NIST 800-16: Information Technology Security Training Requirements: A Role- and Performance-Based Model. NIST Special Publication 800-16, National Institute of Standards and Technology. (1998).

Oberhelman, D. (2007). Coming to terms with web 2.0. *[WWW document]. URL http://www.emeraldinsight.com/0950-4125.htm, Sited 20 May 2008.*

Ohler, J. (2008). Web 3.0 - the semantic web cometh. *University of Alaska.*

Puhakainen, P. (2006). *A design theory for information security awareness.* Unpublished doctoral dissertation, OULU University.

Rogers, P., Liddle, S., Chan, P., Doxey, A., & Isom, B. (2007). Teaching social software with social software. *Turkish Online Journal of Distance Education. ISSN 1302-6488*, *8*(3).

Schlenker, B. (2008). What is e-learning 2.0? *Learning Solutions, Practical Applications of Technology for Learning, e-magazine.*

Servitium. (2008). Web and learning 2.0: A servitium whitepaper. *Servitium White Paper.*

Sims, R. (2008). Rethinking (e)learning - a manifesto for connected generations. *Distance Education*, *29.*

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management and Computer Security.*

Siponen, M. (2001). Five dimensions of information security awareness. *Computers and Security.*

Soloway, E., Jackson, S., Klein, J., Quintana, C., Reed, J., Spitulnik, J., Stratford, S., Studer, S., Jul, S., Eng, J., & Scala, N. (1996). Learning theory in practice: Case studies of learner-centered design. *Association for Computing Machinery - Special Interest Group Computer Human Interface (ACM/SIGCHI).*

Thomson, M., & Von Solms, R. (1998). *An effective information security awareness and training program.* Masters thesis, Port Elizabeth Technikon.

Van Niekerk, J., & Von Solms, R. (2004). Corporate information security education: Is outcomes based education the solution? *10th IFIP WG11.1 Annual Working Conference on Information Security Management, World Computer Congress (WCC), Toulouse, France.*

Van Niekerk, J., & Von Solms, R. (2006). Understanding information security culture: A conceptual framework. *Information Security South Africa (ISSA), Johannesburg, South Africa.*

Van Niekerk, J., & Von Solms, R. (2007). A web-based portal for information security education.

Virkus, S. (2008). Use of web 2.0 technologies in lis education: experiences at tallinn university, estonia.

Von Solms, B. (2000). Information security - the third wave. *Computers and Security*, *19*, 615-620.

Vrasidas, C. (2000). Constructivism versus objectivism: Implications for interaction, course design and evaluation in distance education. *International Journal of Educational Teelecommunications*, *6*(4), 339-362.

Wahlstedt, A., Samuli, P., & Marketta, N. (2008). From e-learning space to e-learning place. *British Journal of Educational Technology.*

Whitman, E., & Mattord, H. (2003). *Principles of information security.* Thomson Course Technology.

Yurcik, W., & Doss, D. (2001). Different approaches in the teaching of information systems security. *Information Systems Education Conference (ISECON), Cincinnati, OH, 2001.*

Appendix A

ENABLING USER PARTICIPATION IN WEB-BASED INFORMATION SECURITY EDUCATION

Ryan Goss and Johan van Niekerk (2008). Information Security South Africa Conference 2008, Johannesburg, South Africa. Paper accepted under ”research in progress” category.