Chapter XVIII

Security and Online Learning: To Protect or Prohibit

Anne Adams
Middlesex University, UK

Ann Blandford
UCL Interaction Centre, UK

ABSTRACT

The rapid development of online learning is opening up many new learning opportunities. Yet, with this increased potential come a myriad of risks. Usable security systems are essential as poor usability in security can result in excluding intended users while allowing sensitive data to be released to unacceptable recipients. This chapter presents findings concerned with usability for two security issues: authentication mechanisms and privacy. Usability issues such as memorability, feedback, guidance, context of use and concepts of information ownership are reviewed within various environments. This chapter also reviews the roots of these usability difficulties in the culture clash between the non-user-oriented perspective of security and the information exchange culture of the education domain. Finally an account is provided of how future systems can be developed which maintain security and yet are still usable.

INTRODUCTION

The World Wide Web is facilitating new forms of remote education. These online environments provide a wealth of possibilities for supporting learning throughout the world. Yet, with the many opportunities come a myriad of risks. Risks to the system and its data can dramatically affect users' perceptions of a system's reliability and trustworthiness. Whether these infractions are malicious or accidental, they can have serious repercussions for a system and its administrators. Security is therefore essential to retain users' trust in an online learning program.

Although security is an essential part of any system it should not impede the original objectives of that system. However, security mechanisms and their poor implementation have been found to present serious usability problems. There are two principal security issues, authentication and privacy, where usability is a source of problems for online learning systems (OLS). Initially, users encounter a variety of usability problems with authentication procedures, such as passwords, which incur high user overheads or are simply unworkable. The result is that users either try to circumvent the mechanisms or use other systems to complete their task (Adams & Sasse, 1999c; Adams, Sasse, & Lunt, 1997; Holmström, 1999; Preece, 2000; Whitten & Tygar, 1999). Users seeking to protect their privacy encounter further complex usability problems. These usability issues often relate to concepts of ownership (e.g., intellectual property rights, copyright, privacy rights). Many OLS, however, do not provide adequate feedback or control rights (Adams, 1999; Bellotti & Sellen, 1993; Preece, 2000). Although some usability issues only relate to specific online settings, others are more universal.

For security mechanisms in OLS to effectively protect our information they must be designed appropriately to the users' needs. Usability, in this sense, would relate to providing users with adequate control to protect their data. In this context, users may be the providers of learning materials, in which case the concern is commonly over authorised access to proprietary learning materials. Alternatively, users may be learners, in which case the concern may be over their answers to questions, their results or even their images (notably in videoconferencing systems, where even matters as apparently trivial as the quality of a video image can affect perceptions enormously). Various OLS, however, do not provide adequate feedback or control rights to allow this control.

This chapter details why we need security in OLS and the factors underpinning how that security is provided within various environments. A review is also provided of the fundamental differences between the culture of security and online learning that produce clashes between the two disciplines. These clashes are often the root cause of usability issues in security mechanisms for OLS. Finally, an account is provided of how future systems can be developed which maintain security and yet are still usable.

Ultimately, this chapter seeks to review three important concerns:

- why current security mechanisms, frequently used in online learning programs, lack usability;
- why the current security discipline, which is not user centred, leads to serious security risks being overlooked;
- how security mechanisms in online education programs can be developed to be both usable and secure.

BACKGROUND

Security issues such as authenticating users, intellectual property rights and privacy are certain to increase in the new millennium with the development of new ubiquitous learning technologies. With the growth of such technologies, security breaches are becoming more frequent and their impact is increasing. Security is, therefore, a vital part of an online learning system (OLS) to ensure that only appropriate people have access to it and the information it contains. Computer security has developed various mechanisms to aid in system and information protection within online environments. However, there are many issues that reduce the effectiveness of these devices.

Despite considerable resources being spent on security mechanisms and their maintenance (e.g., password resetting, encryption techniques), breaches and associated problems are still increasing (DeAlvare, 1990; Hitchings, 1995; Sasse, Brostoff, & Weirich, 2001). Many of these security breaches are directly related to users (e.g., poor password design, security knowledge). The technique of *social engineering* specifically exploits users' lack of security awareness to breach security (i.e., obtaining access to information by deception or persuasion). It appears that, currently, hackers pay more attention to human factors than do security designers. Davis and Price (1987) have argued that, as security is designed, implemented, used and breached by people, human factors should be considered in the design of security mechanisms. However, the security domain relates the problem to user weaknesses rather than usability issues (Adams & Sasse, 1999c; Sasse et al., 2001; Schneier, 2000).

When assessing the level of security required for different information, the security domain again disregards users' perceptions. It has been argued that ethically there are many inalienable privacy rights that should never be disregarded when developing systems (Davies, 1997). Similarly it is also maintained that privacy experts understand potential privacy risks at a greater depth than users (Bennett, 1997). However, privacy is socially determined, being defined by our perceptions of it. To be private, therefore, relies on our perception of ourselves as secluded from a public environment (Goffman, 1969; Wacks, 1989). Taking this into account, therefore, the importance of users' perceptions in designing privacy mechanisms is paramount. It is interesting to note that of all the invasions of privacy identified by

Adams and Sasse (1999a, 1999b, 2001), none was intentional or malicious but all were related to design issues (e.g., poor feedback, inappropriate design, inadequate user control).

The culture of the security discipline thus has a significant effect on how security is developed and administered. Of key importance is that usability, until recently, was not considered an important aspect of security design. We highlight how this oversight relates to the culture of the security discipline. Furthermore we highlight how the culture of security clashes with that of the online learning domain to produce further usability problems.

Culture of Security

Despite the importance of usability of security mechanisms, there is very little research in this field. The handful of publications that exist all argue that previous research is limited, technically biased and for use by professionals (Adams, 2000; Adams & Sasse, 1999; Adams et al., 1997; Holmström, 1999; Sasse et al., 2001; Whitten & Tygar; 1999). Users' poor security knowledge, behaviours and education are often criticised rather than the usability of security mechanisms. To understand the lack of usability research in this field and the adversarial approach to security implementation we must review the cultural roots of this discipline.

The security discipline has, until recently, regarded the development of security systems as solely a technical issue. Users' work practices, organisational strategies and usability factors are rarely considered during the design and implementation of most security mechanisms today. It could be argued that many of these issues are not reviewed because the off-line roots of security lie in the militia and mathematics. It should therefore be of no surprise then that online solutions should be technically biased, mathematically complex (e.g., cryptography) and dependent on organisational hierarchies. Hitchings (1995) argues that this perspective has produced security mechanisms that are much less effective than they are generally thought to be. This technically biased approach could be the cause of poor usability design in many security systems. However, within the security domain, these problems are further complicated by its military-style culture.

The authoritarian approach of security has led to the security discipline's reluctance to communicate with users. Parker (1992) has noted that a major doctrine of security, adopted from the military, is the *need-to-know* principle. This principle assumes that the more known about a system's security, the easier it is to attack. Informing users about security mechanisms and threats is seen as lowering security by increasing the possibility of information leaks. Part of a system's defence, therefore, is to restrict information only to those who *need-to-know*. Ultimately this approach produces a tendency to inform users as little as possible. This lack of communication results in users being uninformed and thus lacking security awareness. Security departments, conversely, lack knowledge about users and produce security mechanisms and systems which are not usable.

It is important to note that the security discipline's perspective of users is as a risk to be controlled. When users are considered within security, it is often as the *weakest link* in the security chain (Schneier, 2000). Users' insecure work practices and low security motivation have been identified by information security research as a major problem that must be addressed (Davis & Ganesan, 1993; DeAlvare, 1990; Ford, 1994). Security departments' approach to these problems, however, is not to discover the specific causes to address, but to place the blame on users' security knowledge and motivation. The traditional military culture of security assumes that users are not inherently motivated towards these behaviours. It is assumed that users will lack security motivation until they are made aware or forced into completing secure behaviours. However, recent research reveals that users' insecure work practices and low security motivation can be caused by poor user-centred design of security mechanisms and policy. Moreover, forcing users to conform may only produce a *facade* of them having completed secure actions (Adams & Sasse, 1999c, 2001).

The culture of the security domain determines the type of security problems identified and the approach to potential solutions. To date, the security discipline has focused on malicious intruders and technological solutions rather than users' perceptions and usability. These guiding principles have produced technical mechanisms that are both unusable and inappropriate solutions.

Whitten and Tygar (1999) propose that users' understanding of security is impeded by the complexity of security mechanisms (e.g., email encryption mechanisms). Current mechanisms, such as PGP (pretty good privacy), are identified as too difficult and confusing for a conventional computer user. Holmström (1999) and Adams and Sasse (1999c) argue that this is because security features in current software are technology orientated. This impedes the systems' usability, as users are required to have a basic knowledge of the underlying technology to use the systems correctly.

Within the sphere of user authentication, the technical bias of the discipline has produced mechanisms that are restrictive and authoritarian. Security measures have centred on forcing the user towards secure behaviours by enforcing more restrictive authentication regimes, such as:

- increasing change regimes (change password once a month);
- longer and more complex passwords (alphanumeric and required length);
- reduction in allowed input error rates.

Adams et al. (1997) found, however, that the effect of these measures is the opposite of that intended. The more restrictive security mechanisms are, the more likely it is that users will evade them, resulting in behaviours which are even less secure. A dramatic decrease in usability is identified as the cause of this apparent paradox, as more restrictions in authentication mechanisms create more usability problems. Current procedures are circumvented because user costs are too high

(e.g., time-consuming) while the benefits (i.e., increased security) are rarely established for users. The causes of these user costs are often security mechanisms and policies that do not take account of users' work practices. Systems are subsequently designed which, in practice, are at best impractical and at worst impossible. Users were also found to be highly security-conscious if they perceived the need for these actions (i.e., obvious external threats).

The field of privacy has concentrated more on policies and mechanisms that increase users' trust in the systems (Preece, 2000). However, experts' rather than users' viewpoints direct the identification of problems and potential solutions. To date, security experts have concentrated on protecting the individual against a malicious invasion of privacy. This perspective reveals the adversarial nature of the security domain. However, as this chapter will identify, many invasions of privacy occur unintentionally through poor interface design.

The technical predisposition of the security discipline has resulted in a focus on the security of data rather than the user (Clarke, 1997). Privacy solutions centre on technical mechanisms (e.g., encryption tools) and policies without understanding how users perceive online systems or the mechanisms in question (Diffie & Landau, 1998; Needham & Schroeder, 1978). These mechanisms are based on the traditional *personal information* assumptions, i.e., that potentially invasive information only relates to data that identifies the individual. This approach leads to the conclusion that to make the data, or the user, anonymous would take away the ability to identify them personally and thus secure their privacy. However, with the development of complex online learning environments, the issues of the future may not be well met by this narrow perspective.

Online Learning Systems Culture Clash With Security

Within the realm of education and learning, an ethos tends to prevail of cooperation and collaboration. A course of study is presented so as to encourage students to assimilate and understand it. Online learning systems (OLS) seek to encourage trust, information sharing and freedom of expression to develop an environment that is appropriate for learning.

With the growth of networked services, more and more people from different backgrounds and cultures with varying skills are using online learning programs. Online services seek, if sometimes inadequately, to support and aid these students in their educational goals. It is important to understand when designing these systems that we are social creatures who relate to each other via social norms for specific situations and surroundings. Online learning systems must facilitate users from vastly different cultures and backgrounds in establishing a joint understanding of the social norms for that system. Furthermore the continual intake of new users at the beginning of courses means that the acquisition of the OLS culture must be quickly and easily assimilated. To facilitate the effective development of these norms requires the communication and adaptability often provided by reputable educational establish-

ments and their online systems. The theme of this book also highlights the importance within the education discipline and for usability principles of communication, feedback and the free flow of information.

It is important to understand how the non-user-orientated perspective of security clashes with the information exchange culture of the education domain. The current focus of the security community on technical mechanisms to enforce and protect desired behaviours does not fit well within a learning environment. The learning arena thrives upon a tradition of trust, information exchange and discussion. The security domain, in contrast, relies on a culture of distrust, restricted information flow and autocratic rules. It should also be noted that students do not respond well to the traditional authoritarian approach of many security departments.

What is of increased importance is how the clash between these two disciplines can be seen as the root of many usability difficulties with security in online learning systems. Within the domain of online learning, users relate to the established norms of feedback and help when they encounter usability problems. However, usability problems encountered with security mechanisms are often not supported by traditional help facilities. Users' isolation encourages contrary perceptions of the system working against, rather than with, them. The segregation of those traditionally placed to help users (e.g., tutors, administrators) form an understanding of security mechanisms further increases potential usability problems.

Ultimately, a new approach is required that promotes the protective aims of security without confronting the users with unusable systems. The beginning of many solutions starts with a reengineering of the security culture to work with, rather than against, the user. The user, as previously noted, is a crucial link in the security chain that must be considered as a valued asset rather than a flawed chink in the armour. A recent move within security research has tried to counteract current security limitations by highlighting the importance of users' conceptual models and their understanding of security mechanisms (Adams & Sasse, 1999c, 2001; Holmström, 1999; Whitten & Tygar, 1999). The need for more research into user-directed security is imperative, however, as the need for security increases and our understanding of trust is diluted in online environments.

ONLINE LEARNING SYSTEM ACCESS: AUTHENTICATION

Security, in general terms, is often taken to mean *protection from danger*. With regard to computer security, that danger relates to malicious or accidental misuse (Neumann, 1995). Computer security, therefore, tends to concentrate on human misuse rather than computer malfunctions. Two important aspects of security are *confidentiality* and *integrity*. Confidentiality is concerned with protection of information from unauthorised access, while integrity refers to maintaining the

unimpaired condition of both the system and the data used. Both confidentiality and integrity closely relate to the endeavour of making sure that misuse does not impact on computer reliability. Ultimately, security seeks to ensure that learning resources are available, unimpaired, to all authorised users when they are needed. To maintain the commercial viability of online learning systems (OLS) it is therefore vital to ensure that the people who pay for services have access while other non-authorised users are excluded. To retain this access to unimpaired data it is necessary to deal with issues of authentication and ownership. It is essential that the appropriate people have access to information with the correct data manipulation rights (Preece, 2000).

Security issues, however, are often not directly considered by online learning administrators. Articles that do review security issues for online learning systems tend to concentrate on issues of intellectual property rights and copyright law (Diotalevi, 2000; McAlister, Rivera, & Hallam, 2001). Recent articles, however, are identifying further security issues for OLS, especially with regard to user feedback and assessment (Bateman, 2000; McAlister et al.). McAlister et al. notes that authenticating a user is especially important when assessing students' progress online. However, administering this authentication is troublesome as normal security procedures (e.g., seeing the student complete the assessment unaided) are not applicable in many online scenarios. It is suggested that if identification for assessment purposes is essential then local supervised sessions could be provided.

Authentication Stages and Methods

Authentication is pivotal to the concept of confidentiality but it also relates to integrity. To maintain appropriate access to information and yet protect it from unsanctioned manipulation, it is crucial accurately to authenticate users.

Authentication procedures are usually divided into two stages. The first stage, *user identification* (User ID), identifies the user interacting with the system. As it is merely a means of specifying who the user is, this ID does not have to be secured. Once the user is identified the second stage, *user authentication*, verifies them as the legitimate user of that ID. The means of authentication, therefore, must remain secret.

There are three different ways to authenticate a user by an online learning program (Garfinkel & Spafford, 1996):

1. Knowledge-based authentication: The user *tells* the computer something only they know (e.g., password).
2. Token-based authentication: The user *shows* the computer something only they possess (e.g., a key card).
3. Biometrics: The user themselves is *measured* by the computer (e.g., fingerprint).

Security research has tended to concentrate on technical mechanisms for authentication (e.g., iris scanning, smart cards). However, although these technolo-

gies have great potential in future applications, passwords and personal identification numbers (PINs) are currently the most widely used form of authentication. Even where the other forms of authentication (i.e., token-based or biometrics) are used, they are invariably reinforced by the use of a PIN or password. Knowledge-based authentication has the advantage of being both simple and economical. These two factors probably account for its universal appeal and ensure its use for many systems and years to come.

One of the problems with popular knowledge-based authentication mechanisms, such as passwords and PINs, are their poor usability. Current mechanisms rely on users to recall data to be input rather than recognising the correct authorisation information. To counteract these problems there are a wide variety of knowledge-based authentication mechanisms that claim to be more usable and yet secure:

- passphrases (a phrase required instead of a word);
- cognitive passwords (question-and-answer session of personal details);
- associative passwords (a series of words and associations);
- passfaces (user selection of faces).

However, the take-up of these mechanisms has, to date, been limited (Sasse et al., 2001). One-word passwords and PINs are still the easiest and cheapest to apply and thus most often implemented.

Passwords: Security Issues

Passwords are either system- or user-generated, with the former ensuring a more "secure" combination of characters in the password than the latter. However, users find *system-generated* passwords are not usable (i.e., hard to remember correctly) and so have been found to write them down, thus decreasing security. Furthermore, the process of distributing system-generated passwords often led to increased security risks (i.e., unauthorised access to the passwords). Both of these reasons have led to *user-generated passwords* as the most widely used process for password production.

The level of security provided by *user-generated passwords* can vary greatly, depending on the individual user's password design expertise and security awareness. When generating a password its *crackability* is often vastly underrated by users (Davis & Ganesan, 1993). There are, however, several criteria that should be used to ensure a reasonable level of password security (Federal Information Processing Standars, 1985).

Password composition is a vital element in a password's *crackability*. A password composed of characters chosen from a large character set decreases its level of crackability. An alphanumeric password is therefore more secure than one composed of letters only. The *lifetime* of a password (i.e., *change regimes*) relates to the frequency with which the composition of a password is required to be changed. Some systems apply a strict *change regime*, e.g., requiring passwords to be changed

every 30 days and not to repeat one of the past 10 chosen. However, it must be understood that *change regimes* do not actually increase security, but decrease the damage that can be done once a breach has occurred. In addition, frequent *change regimes* are only required for highly confidential information. The sensitivity of the information protected should, therefore, be considered before introducing frequent *change regimes*. Finally, the security domain emphasises the importance of individual ownership of passwords because they:

- increase individual accountability;
- reduce illicit usage;
- make it possible to audit system usage;
- reduce frequent password changes due to group membership fluctuations.

Ultimately, the level of security a password affords is tightly interwoven with its design. However, support for users on password design is often very limited.

Passwords: Usability Issues and Solutions

Security systems should be deemed ineffective and unusable if the user costs (mental overhead, time-consuming, etc.) and computer costs (costly implementation, continual system updating) are high and yet the overall security of the systems is low. By these standards, the desired performance of most security mechanisms is unacceptable. The consequences of inadequate usability, however, are high : Poor usability of security mechanisms can result in excluding intended users while allowing sensitive data to be released to unacceptable recipients. There are a wide variety of usability problems within password systems. However, this section will initially review the major issues associated with users' memory limitations and how to counteract those problems by increasing password memorability. Further issues of poor feedback and guidance are presented with potential solutions including guidance in password design. Finally the importance of understanding the *context of use* with regard to password usability is evaluated.

Memorability. As technology infiltrates more aspects of people's lives, the number of PINs and passwords required can become excessive. Most people have a PIN for a bank card, mobile phone, voice mail and even entry door systems. A multitude of passwords is also required in our daily lives; for logging on to networks, specific applications and a multitude of Web sites. Online learning programs are also inclined to use passwords rather than other forms of authentication. The result is a considerable challenge for users, not just in terms of the number of items to recall but the complexity of the information to be memorised.

Authentication mechanisms, often unnecessarily, increase the memory load on users. Most systems allow the user to choose a PIN or password, to increase its memorability. However, the user's choice is often constrained by security parameters, for example, that it has to be of a certain length or format. This is because the

security of a password system ultimately relies on the level of security afforded by the password content. With the use of dictionary checkers, a short alphanumeric password affords more security than a longer word (since alphanumeric strings are not listed in such dictionaries). A password's content, though, also affects its level of memorability. As Carroll (1996) observes, the very characteristics that make a password more secure (e.g., long, nonsensical combinations) also make it less memorable. A word can be far more memorable than a nonsensical combination, but the security afforded by the former is far less than the latter. A password system's security and its memorability, therefore, lie in the hands of the user. Users are required to construct a memorable combination within the security constraints provided, often within a short time frame, and are rarely given feedback on how to construct these passwords (Adams & Sasse, 1999c; Adams et al., 1997; Sasse et al., 2001). Many users feel they are forced into circumventing unusable security procedures, which decreases their security motivation. Hackers using *social engineering* techniques rely on the lowered security motivation of users to breach security mechanisms. A simple phone call or email, together with users' poor security awareness, is all that is required.

Another serious constraint on password memorability is the implementation of *change regimes*. Harsh *change regimes* (e.g., password changed once a month, once every 3 months) not only decrease the memorability of a password system but also increase security risks. Adams and Sasse (1999c) found that users who were required to change their passwords frequently produced less secure passwords and disclosed their passwords more frequently. The increased security risks (e.g., writing down passwords, poor security motivation) incurred by introducing frequent *change regimes* should also be considered before introducing these measures.

Finally another interface flaw, which increases the users' memory burden, is a failure to clearly distinguish between the openly disclosed aspects of user identification (ID) and the undisclosed secret aspects of the password section. Adams et al. (1997) found that many users confused user identification (user IDs) and the password sections of the authentication process. Without knowledge of the authentication process, users assumed that these IDs were another form of password to be secured and recalled in the same manner. Recall of the user ID then became an extra memory burden on the user. User confusions were found to be related to authentication mechanisms which automatically allocated user IDs as nonwords without meaning. Even when authentication systems require a user's name, they do not state the format that it is required in. Consequently users returning to one of many systems they use encounter problems remembering which form of their name they need for this system (e.g., A. Adams; A. L. Adams; Anne Adams; anne adams).

Increasing password memorability. An important aspect of usability is to design user recognition into a system rather than relying on users' abilities to recall information. However, passwords rely on users' long-term memory, with all its

limitations and flaws. This has produced efforts to identify mechanisms for generating memorable yet secure passwords which rely on users' recognition rather than recall abilities (Barton & Barton 1988; DeAlvare, 1990; Sasse et al., 2001). The impact of these recommendations, however, seems to have been limited, in that few developers are aware of them (e.g., passfaces, associative passwords, etc.).

One serious impediment to the recall of passwords is the interference in retrieving the information from memory caused by the increasing numbers of passwords requiring memorisation. A technical solution to this problem has been suggested, in the form of a single sign-on (Adams & Sasse, 1999c). With this method of authentication, systems are interlinked only for authentication purposes and the user can use one password for multiple systems. However, if this approach is technically inappropriate or too expensive, there are non-technical solutions. If the security afforded by a single password is acceptable, users should be advised to use a single password for all systems. It should be noted, though, that from a security perspective there could be some problems with this approach as different systems hold more sensitive information (e.g., exam marks, tutors' course-work comments) than others and require tighter security protocols. What must be emphasised to the users is that linked (e.g., tom1, tom2, tom3) passwords should *not* be used for different systems as they have a lower memorability than unlinked (e.g., to2m, pofad, sa11y) passwords (Adams et al., 1997), in terms of which password applies to which system. It must also be noted that the memory advantages of single sign-on can be counteracted if frequent change regimes are introduced since interference will still reduce password memorability (i.e., interference between old and new passwords).

Some memory aids are a useful tool in increasing the memorable content of passwords without decreasing its level of security. Initial letters of a sentence or a rhyme can look like a complex secure password combination (e.g., 12Bms34Kotd) and yet be memorable with an appropriate cue (e.g. 1, 2 **B**uckle **m**y **s**hoe. 3, 4 **K**nock **o**n **t**he **d**oor). If the sentence cue relates to the interaction task then for many users this can increase the password memorability still further. For some users, the pattern of the input keys on the keyboard can greatly aid memorability. However, this aid is a better support for frequently used password or PIN numbers and can cause problems if a frequent change regime is employed.

Finally, as previously mentioned, many user authentication mechanisms incur further memorability problems by not distinguishing between the user ID and the password sections of the authentication procedure. It is important that the interface of a user authentication system clearly highlights the difference between these sections. Currently the only distinction provided between these sections is the standard feedback for the ID data input (e.g., anne adams) and a secret feedback for the password data input (e.g., *****). As the user ID section does not require free recall to increase security it can be prompted. It could increase the usability of these systems if, instead of asking for a user ID, they presented a box asking for the user's first name followed by a box asking for a surname. If the ID section accepted

the data in either case (upper or lower), this could further increase the system's usability.

Feedback and guidance. One major problem with all security mechanisms is the distinct lack of user support provided. Adams et al. (1997) found that limited and unsuitable feedback in security systems can produce inappropriate, time-consuming user actions and pointless interactions. Whitten and Tygar (1999) also point out that to prevent dangerous errors, appropriate feedback is essential. An essential aid to system usability, therefore, is the provision of simple, straightforward, accurate documentation for user support and help facilities. However, it is difficult for security mechanisms to provide these facilities because the system needs to aid the user without supporting security breaches (Sasse et al., 2001). There is, therefore, an important balancing act between usability and security. For example, a user having recently returned from a vacation types in their password; the system states it is incorrect; the user is certain that this is their password, so assumes they have typed it in incorrectly and types it again; the system again states that it is incorrect; and the user tries one last time and is shut out of the system. How could the system have supported the user without decreasing security by aiding an unauthorised user? Often to increase usability, prompts are used to guide the user through a task. However, providing prompts or clues about the password to the user would increase security risks. Associative passwords (i.e., a series of words and associations) could be used as a backup, because although they are time-consuming they are cheaper and quicker than password reinstatement procedures. Another prompt that could be provided would be for the user to receive some simple feedback, for example, reminding them that the system is case-sensitive. As noted by Adams et al. (1997), many users have problems with passwords not because they have forgotten the password but simply that they have forgotten that the system is case-sensitive. This feedback would potentially support some users and yet not decrease security since most hackers assume case-sensitivity in their cracking attempts.

Not only do users require support in their use of authentication mechanisms but also in the design or choice of passwords. Users also have to develop rules for using passwords which satisfy the criteria for a secure password and, at the same time, minimise the burden on themselves. As Adams and Sasse (1999c) observe, however, users are rarely given support in these procedures (e.g., how to design effective passwords, manage your security, interact with the system, reinstate forgotten passwords, change passwords). Users' lack of basic knowledge was found to result in them making their own judgements about which practices are secure, and these judgements are often wildly inaccurate. We suggest that the reason behind poor user support and usability of security mechanisms lies in the security culture of reduced communication with users. The solution is to provide open support and guidance in password construction and secure behaviours. The support provided, however, should not take the traditional authoritarian approach (e.g., tell us what you're doing

wrong so we can reprimand you). Two-way communication should be established so that users and security designers are encouraged to think of security as a joint responsibility, with security administrators acknowledging users' needs and work practices.

Understanding the context of use. When designing an authentication screen it is important to understand the user's context of use. The mental model that users have of the relationship between the virtual- and real-world library is essential if security procedures rely on them. A recent study we conducted, within an UK academic setting, identified problems with access to a digital library. Users who initially attempted to access digital libraries online were presented with no information about what specific authentication was required (e.g., an *Athens* ID and password), how to obtain these details and who to contact if they had any problems with the system. As with many online learning programs the only information provided in the authentication process was a screen asking for user ID and password. Users became further confused when they found out (via off-line sources) that they had to physically attend their local library to obtain a password in order to remotely access digital libraries. Further research into these usability problems identified that users' understanding of the context is complicated by the inconsistent use of terminology. In this example, users were confused when the name for the online learning system (i.e., OVID) did not correspond with the name of the system required to access it (i.e., *Athens* password and ID).

Further terminology problems can be encountered when technical terms such as *ID* are used without detailing what they relate to or how to enter the required information (e.g., case-sensitive, limited number of characters). The use of these terms between systems is also frequently inconsistent. For example, one popular online system not only asks for an access ID, but also an authentication ID and a password. There is no explanation about the differences between these components and their different security levels. The use of multiple types of IDs also increases the potential for user errors in remembering and entering these items.

Users confused by inconsistencies within and between systems are even more confused by similarities between different digital library authentication mechanisms. In our digital library study, it was found that users would effortlessly jump between digital libraries, but frequently became disorientated about which library they were currently accessing. Users frequently tried to proceed in library A using library B's password. Other users did not realise they had followed a link from one library to another and that further registration was required. Unaware of their errors, users were often locked out of the system altogether. Ultimately, it is important to understand that users consider authentication mechanisms as a part of the learning interaction. When designing online learning programs we must, therefore, consider their usability with regard to their context of use.

PROTECTING PRIVACY IN ONLINE LEARNING SYSTEMS

Data is increasingly being treated as property, and the ownership of that property is fiercely debated. For example, sports organisations have claimed that online service providers misappropriate their proprietary rights to scores. In contrast, governments sell the rights to potentially *personal information* they collect. The World Intellectual Property Organisation is continually debating the protection of databases and expanding copyright protection for digital works (Computers, Freedom and Privacy, 1997). Legislative developments have not untangled this complexity. Over the last 30 years U.S. courts have increasingly ruled that personal records belong to an organisation and access to the information cannot be restricted by the person in question (Kling, 1996).

In security terms, information ownership (i.e., intellectual property rights, copyright, privacy rights) can determine access and manipulation rights. Issues of ownership, therefore, relate to both confidentiality and integrity. However, it is important to note that the users' concept of ownership is closely intertwined with that of privacy. It is vital, therefore, to understand users' perceptions of information ownership, usage and privacy when developing online learning systems. Privacy and intellectual property rights rely on our perception of them. As well as how well we are protected, it is also important that we perceive ourselves and our information to be safe and private. Therefore identifying users' perceptions of privacy and ownership is an important element in identifying what needs to be protected and how best to protect it.

People often feel they own data about themselves and that security should reflect how much they feel misuse of that data could invade their privacy (Adams, 2001; Adams et al., 1997). However, with the increasing availability and use of various data and applications, associated *privacy risks,* out of users' control, are greatly increasing (Bellotti, 1996; Neumann, 1995; Preece, 2000; Smith, 1993). Kling (1996) suggests that over the past 30 years there has been a growing view that computerisation has decreased people's privacy. Computerisation, however, is not the only culprit in people's perceptions of decreased privacy. Slow-to-react organisations have played a key role in this decline: Organisations that develop privacy policies retrospectively, after an external threat, produce policies that have been outgrown by changes in either society or the organisation's activities (Smith, 1993).

Just as there are many inalienable rights that should never be disregarded when developing systems (Davies, 1997) , it is also maintained that security experts understand potential risks at a greater depth than users (Bennett, 1997). Both these arguments have directed security research and the identification of security requirements in system development towards appraisals by security experts. The problem with *only* taking this approach is that any expert may have a distorted perception of

a situation that does not reflect the perceptions of the users. Ultimately, to satisfy users' privacy needs, it is necessary to understand their perception of the information being used, how it is used and those manipulating it (Adams, 2001; Adams & Sasse, 2001).

Privacy of Learners' Working Materials

The issue of ownership when dealing with distance education can be very complex and is often not written in stone, making it hard to apply accurately (Diotalevi, 2000). McAlister et al. (2001) suggest that it is important to establish ownership rights and compensations prior to offering Web courses to minimise future misunderstandings. However, problems often occur because of difficulties in distinguishing what information needs to be protected and by whom (Adams, 1999a, 1999b, 2000). These fundamental issues often lead to inappropriate design of security mechanisms that, in turn, provide poor usability for safeguarding what users want protected.

Despite information ownership being a complex issue, students perceive their ownership of the essays and course work they produce as straightforward. It is important that users can rely upon an online learning system to protect their information from misuse (Preece, 2000). Users' control over access rights to this information, however, is sometimes negated by system settings. A particular worry for students is that when working online their documents will be viewed before they feel ready for them to be accessed. A student whose course work or assessment mark is available to others, without their prior knowledge, will be less willing to use the system in the future. Previous research into multimedia educational systems has identified the importance of *freedom of expression* in the learning process. However, our ability to express ourselves free from social inhibitors relies upon a secure context for private expression and autonomy (Schoeman, 1992). Adams (2001) found that students were negative when online learning systems allowed tutors automatic viewing rights to them (e.g., video-conferencing systems) or their work without their control or prior knowledge. Cranor, Reagle, and Ackerman (1999) also found that users have a particular dislike of the automatic transfer of data about themselves and their patterns of use.

Although monitoring learners' progress and participation in learning applications is vital, it must be carefully applied. Users' security needs (e.g., privacy) are occasionally overlooked when developing monitoring mechanisms. Tracking devices used to tailor learning situations for the user can be invasive if information is inappropriately obtained and applied. Intelligent agents that identify information requirements can invade users' privacy, depending on how the information is used. These issues are further complicated within an online environment, where trust in a faceless entity is difficult, technology distorts social interactions, and social norms vary across continents. Poor usability in protecting online users' rights can have serious consequences as users lose trust and reject the technology in question (Adams, 1999a, 1999b, 2000; Adams & Sasse, 2001; Preece, 2000).

Ultimately, the importance of correctly applying security for online learning programs should not be underestimated. A study of United States users found that protecting *personal information* privacy should increase Internet usage 78% amongst those who already use it and 61% for those who currently do not (Harris & Westin, 1998). These figures show the economic importance of these issues for online learning systems. One way to protect sensitive information transmitted over the Internet is through encryption. Electronic cryptography provides a collection of techniques for encoding communications so that only their intended recipients can understand them.

Encryption Techniques—PGP

It is important in any communications that the sender is assured that what they send is what is received, without any unauthorised access and manipulation. Encryption tools are often used to ensure the *integrity* of the data and the authorised nature of the recipient. The potential advantages of these tools for online learning are clear: Course work or sensitive emails can be communicated with the students' confidence that they are private. The usability of these techniques, however, is debateable.

The marketers of PGP (pretty good privacy), a popular document transfer encryption tool, claim that its graphical user interface allows novice computer users to utilise complex mathematical cryptography. Whitten and Tygar (1999), however, have identified problems with the terminology used by PGP. The system designers have tried to steer away from complex cryptographic terminology by using real-world terms, but those terms are used in uncharacteristic ways. For example, in the real world the same key is used to lock and unlock a door. However, in cryptography and in particular PGP, there is a distinction made between public and private keys. PGP presents no online help to explain the important distinction between these two key icons. Users were either left to work out the distinctions based on other key type data, thumb through a 132-page manual or misinterpret the metaphor. Similarly *a signature* is another cryptographic term that would imply, invoking the real-world metaphor, the use of a mechanism to sign a document. However, within PGP the term is used to denote a step in the encryption procedure (along with private keys) rather than simply signing a document. Even once users understand the terms used within PGP, their use is further complicated by system inconsistencies. Throughout the process the terms *encryption* and *signing* are used, but once the system is encrypting, it presents feedback on the process stating that the system is currently *encoding*.

Ultimately, the language and structure of security mechanisms can often decrease system usability. Whitten and Tygar (1999) identified that the poor usability of *PGP* meant that two thirds of their study participants could not encrypt their data within 90 minutes of using the application. Worse than this was that one-quarter of the users in the study accidentally emailed their secret data unencrypted. Re-

designing the interface, however, could have solved many of the usability problems. Several usability issues arose from the metaphors used, which encouraged users to develop inappropriate assumptions about the interface (e.g., keys, signatures). A redesign would have to develop the system to comply with real-world metaphor assumptions (e.g., a key opens and locks a door, a signature identifies who sent a communication but does not make it private). The system also used technical jargon inconsistently, which should be avoided.

Group Working in Videoconferencing and Virtual Reality Systems

The primary usability considerations of online security mechanisms varies according to the different types of online learning environments (Preece, 2000). Online learning environments range from one-to-one text communication to videoconferencing and virtual reality many-to-many collaboration. The greatest challenges to security, including privacy, are presented by videoconferencing and virtual reality systems.

Videoconferencing is increasingly being used to support online learning via computer-supported collaborative learning (CSCL). Videoconferencing really began with the transmission of group images from one room to another via a common monitor (Isaacs & Tang, 1997). However, multimedia communications to support online learning came into their own with the advent of desktop videoconferencing. Users sit in front of their computer and communicate in real time via a microphone, camera and, often, a digital workspace. This configuration is often referred to as a *picture-in-a-picture* (PIP) setup.

Virtual reality applications allow human-computer and human-human interactivity through a sensory environment called the *virtual world* which is *dynamically* controlled by the user's actions. Exploration of that world for learning purposes is often achieved via a computer-animated actor (an avatar). An avatar helps the user relate to and collaborate with the world and other users (Granieri & Badler, 1995; Preece, 2000).

Virtual reality (VR) environments rely heavily on the notion of immersion, both physically and cognitively (Preece, 2000). Keyboard and monitor input devices allow a user to be partially immersed, whilst head-mounted displays produce total immersion in the environment. A user is cognitively immersed in the environment when they feel immersed in the action (Fluckiger, 1995; Tromp, 1995). Initially VR was used for entertainment and training purposes. Virtual simulations of complex real-world systems have been used as learning environments for various conditions (Preece, 2000; Smets, Sappers, Overbeeke, & Van Der Mast, 1995). Collaborative VR environments provide remotely located users with the ability to collaborate via real interactions in a shared artificial environment (Brna & Aspin, 1997). It is frequently argued by constructivists[1] that the advantages of VR for collaborative learning relate to the authenticity of the context (Vygotsky, 1978). VR communica-

tion environments have been argued to provide a natural, intuitive environment for communication whilst releasing some of the social taboos from social interactions (Kaur, 1997). However, we note that, as the realism of virtual worlds increases, users are more likely to make inaccurate assumptions about the virtual world's capabilities and limitations, decreasing its usability.

Virtual reality provides an anonymous environment which, this chapter will show, can still allow inappropriate and invasive behaviours. The focus of security protection upon the individual may also be inadequate for threats in the future. It could be argued that a social grouping itself has its own identity, which relates to the individual. This would mean that although an individual is anonymous, if the social grouping is identified then the individual is indirectly identified. Individuals could similarly find it invasive if sensitive information is made public about anonymous individuals from their specific school, church or social group. Online groups formed for learning interactions must therefore be managed as a unit, with their own security needs. It could be argued that, as our societies become larger and more multicultural, the smaller social groupings we join which support our beliefs, feelings and biases become more important.

User's VC/VR Representation Projected to Others

As we move into the future of online learning systems, there are interesting challenges for security mechanisms and their usability. The great advantages of video-conferencing (VC) and virtual reality (VR) are already being realised by many students. However, for us wisely to implement these technologies we must understand potential security problems before they arise. This section reviews many of the foreseeable usability problems through reviews of current multimedia applications (i.e., VC and VR). It is important to note that most multimedia invasions of privacy are not intentional or malicious but design related. Designers' failure to anticipate how information could be used, by whom, and how this might affect users is a significant factor in users perceiving their privacy as having been invaded.

One significant multimedia usability issue relates to technology's ability to distort interactions, thus making them invasive. Ensuring that users are protected from disclosing information they would not wish to have disclosed requires an understanding of these issues. For example, interpersonal distance has been found to dictate the intensity of a response: Faces in a close-up are scrutinised more often than those in the background. Reeves and Nass (1996) argue that, because the size of a face is more than just a representation of an individual, it can influence psychological judgements of a person and thus become an invasive piece of information. Similarly, image quality and camera angles might result in a perception of the user that they regard as inaccurate. Many learning environments rely on social interaction with peers and teachers to aid in the learning process (Preece, 2000). However, users can misjudge the sensitivity of these interactions and the potential threats, resulting in them not adopting appropriately secure behaviours. Similarly

inaccurate assumptions could also occur because multimedia communication environments often lack the social, physical and context cues required for users to accurately judge the situation and adapt their behaviour accordingly. A student collaborating in a home setting will act differently from one in a public college setting. Videoconferencing systems that mix the two settings can produce misinterpretations of the situation and inappropriate behaviour for a public interaction (Adams, 2001).

Privacy invasions are frequently due to inaccurate interpretation of the data being received within an interaction. If a user's image has been enlarged (without their knowing it) by a recipient, this can produce the misconception that no one is staring directly at them. In turn the user does not adjust their behaviour accordingly, as they would if someone were staring directly at them in the real world. However, the person receiving the data often does not realise how their actions or potential actions with the user's data may invade the user's privacy. A lack of the facial and body cues that we take for granted in real-world situations can produce an isolating and inhibiting situation for a user. Many virtual reality environments have usability problems with relaying proximity to the users (Preece, 2000). One result of this, which was identified in a virtual reality learning environment, left a user feeling she was being stalked (i.e., followed throughout the environment, stared at). However, the *stalker* had no knowledge of their actions except that they had encountered usability problems (e.g., judging their location within the environment and proximity to other users) with their avatar.

Ultimately, technology can be used, intentionally or unintentionally, to distort assumptions made by those using it. Multimedia environments, in particular, can incur varied and complex privacy problems. The more realistic an environment appears, the more assumptions a user unconsciously accepts. Video-conferencing users will typically assume that the audio is connected to the image on screen, similarly that in virtual reality that a wall has real-world properties and cannot be walked through. However, these assumptions can be either maliciously or unintentionally breached. To take a simple example, a video-conferencing system that allows someone to freeze their video streams (e.g., so that they appear to be avidly viewing the screen but instead have actually gone to make themselves a cup of tea) could produce an inaccurate appraisal of their attention within the interaction. This scenario could also produce a mismatch between the person who is actually watching the images and the assumed person receiving the data (based on the frozen image). The user's resulting behaviours can be inappropriate and the potential invasiveness of the interaction increased.

Online Learning Usability Inhibits Social Interaction and Privacy

Previous research has identified that unacceptable behaviours can unintentionally occur as a result of poor feedback, isolating users from the acceptable social

norms for the situation they are in. Often this is caused by poor interface design but it can also arise from misconceptions of user perceptions by organisations and system designers (Adams & Sasse, 2001). With the increase in online learning environments supporting students throughout the world, there is an increasing variation in social and cultural norms. With this diverse population of users, the need for accurately establishing what is acceptable behaviour is becoming a crucial issue. As privacy perceptions are complicated and online environments often defy real-world assumptions, there is a need to identify users' perceptions within these environments.

Dourish (1993) argues that if a system is embedded in the organisational culture, social controls will establish a culture of use that will restrict unacceptable activities. However, many online learning systems rely on establishing a culture and associated norms purely through online interactions (Adams, 2001). We would argue that, although social controls are vital (especially in flatter, more open organisations), relying on them as the only safeguard for privacy is insufficient. It is important to understand that trust and thus social control evolves with a new technology. To nurture this the technology must not breach users' privacy assumptions, especially if those assumptions are based on social cues that are distorted by the technology.

Another important factor in perceived privacy invasions is the role of those receiving the information (Adams, 2001). Someone highly trusted may be able to view highly sensitive information but only if they are deemed, by the user, to have an appropriate role in the information's usage. A tutor viewing a student's course work may be acceptable because of their role, the trust ensured by that role and the organisational context. However although a student may highly trust a close friend (e.g., disclosing relationship details not acceptable for the tutor to know), they may not be acceptable to view their course work.

Many online systems assure users' privacy requirements by stating their privacy procedures and policies, assuming that this will set the user's mind at rest. Others use a third-party service, such as TRUSTe (Benassi, 1999), to assure users that the company keeps within certain guidelines. However, the policies are often rigid and do not allow for variations in how users perceive different types of information. The usefulness of third-party services also depends upon how much the user trusts these virtual, often unknown organisations. Reagle and Cranor (1999), however, have found that the use of brand or real-world organisational names linked to trust badges could reduce these problems. Providing users with links to real-world contacts and help lines, to ensure their privacy is actively being protected, helps to encourage trust within their virtual interaction (Adams, 2001; Preece, 2000).

Security Problems Caused by Recording and Reuse

It is important to review the permanent quality that technology can give to an interaction. When learning interaction occurs without the aid of technology, the only durable element is in the memories of the parties involved and the notes they take.

However, technology-mediated interactions, whether they are text or video controlled, can be recorded and reused. The implications of recording learning interactions should not be underestimated. Adams and Sasse (2001) found that users' perception of control is essential in building trust relationships for effective social interaction. A student's ignorance of a session being recorded or how the information was to be used could cause them great discomfort. Imagined embarrassing scenarios, which may be no less likely if the user had known of the recording, trigger students' anxiety. The important difference is the users' perception that they would have more control of the situation if they knew it was being recorded (Bellotti, 1997).

The simple act of recording users' interactions can increase the sensitivity of the data. Once an interaction is recorded it can frequently be reviewed, edited and seen by unintended and unknown recipients. All of these events can unintentionally, and without malice, become an invasive act. Adams and Sasse (1999b) detail how a presentation at a conference, which was broadcast over the Internet, was recorded initially for later viewing by students and academics. However, the recording was later shown, without the presenter's awareness, at a seminar to demonstrate the technology. The presenter was later met by a friend and told of his appearance at the seminar. The presenter was then worried about how he would appear, out of context, to an unintended audience. The essential point illustrated by this example is that it is important to consider the outcome of reusing information out of context: Even if actions are not meant maliciously, they may be perceived as invasive.

Of key importance is the feedback that users are given about who is receiving their information both currently and at a later date. Ultimately, a careful balance must be maintained between developing an appropriate learning system and protecting the user's rights. It is also important to inform the students if the information is to be used for any purpose other than those previously flagged to them.

Solution: The Importance of Feedback and Control

The escalating variety of technologies available to support online learning increases the likelihood of complicated usability problems. With the use of multimedia applications, the complexity of those problems increases tenfold.

One usability problem with online learning environments arises from the control afforded students and tutors by the environments. Automatic viewing rights for tutors or other students without users' control or prior knowledge can cause problems. Similarly, monitoring and tracking users' learning interactions can be useful for tutors, but also potentially invasive if obtained and used inappropriately. For videoconferencing, Mackay (1995) and Bellotti and Sellen (1993) suggest that people should be made aware that their images are being transmitted. Ultimately users should be allowed to weigh up the information value (e.g., increased learning capabilities) against potential privacy risks involved (e.g., embarrassing slipups) prior to the interaction taking place. Users evaluating these factors prior to the interaction reduces the likelihood of these invasions occurring.

Within multimedia environments, the data transmitted is likely to be distorted and the information received completely different from that expected by the users. Within online learning situations, users can inaccurately judge the sensitivity of the information they are releasing (Adams, 2001). It is important for users receiving the data to understand how users who have transmitted it may interpret their actions with that information. In the real world, standing too close to someone or staring at them for too long would result in disapproving looks, coughs, sighs, etc. The user who enlarges a student's videoconferencing image or has their avatar standing on top of another's avatar receives no feedback of the inappropriateness of these behaviours. One solution to these problems lies in providing appropriate feedback to both users about what is being received and how distorted it is likely to be, to develop a joint understanding of the data being transmitted. A visual representation of how they are being seen, including the size of that image, is an essential aid to assessing its sensitivity. It may also be useful for users to receive instructions on where to place their cameras, with instant feedback prior to interactions taking place. Allowing the student to review potential risks involved in a multimedia interaction can also aid them in avoidance behaviours. This feedback is easier to administer within video-conferencing than virtual reality environments. Some researchers, however, have realised the importance of body cues and gestures within virtual reality environments and are seeking to replicate them (Marsh, 1998; Rime & Schiaratura, 1991). Ultimately, there is a need for accurate contextualisation of data for all parties within multimedia interactions. The more appropriate feedback parties receive about the social aspects of that interaction, the easier it will be to develop social norms for acceptable behaviours within these environments.

Finally, the implications of recording learning interactions should not be under-estimated. The simple act of recording users' interactions can increase the sensitivity of the data and the potential risks (e.g., repeated usage, out-of-context viewing, editing). Initially it is important, where possible, to obtain the user's permission to record information. If this is impractical then feedback to users who are recorded must be provided. Any later changes to those who will be viewing the information should also be provided to the user. Finally an attempt to try and contextualise data (e.g., date stamping, country of origin for transmission) should be made. For highly sensitive information, digital watermarking and watercasting should be considered. With the aid of these mechanisms, the copying and editing of multimedia data can be identified and potentially traced (Adams & Sasse, 2001; Brown, Perkins, & Crowcroft, 1999; Craver, Yeo, & Yeung, 1998). Copied multimedia data, once identified, could be traced back to its origins. However, these mechanisms are not automated and thus rely on the user trawling through data trying to find out whether their data is on public display somewhere. Furthermore, there is no mechanism that would inform the person receiving the data that it has been tampered with *against* the user's wishes.

THE FUTURE OF SECURITY FOR ONLINE LEARNING

The rapid progress in providing innovative forms of online learning is opening up many new learning opportunities. As these systems develop, the enrichment of students' learning potential throughout the world will be greatly enhanced. Students can receive information throughout the world in text, audio, video and graphic forms. A myriad of virtual worlds can mediate student interactions and support their learning capabilities. However, with these developments comes a heavy burden of responsibility. Ensuring usability in the security of these systems, their users and their data will allow them to thrive and flourish. Avoiding these issues will ultimately result in their downfall from the weight of users' distrust.

With increasing threats to online programs, security will become a high priority in the systems of the future. What is debatable, however, is how that security will be approached. Current security methods manage potential risks with restrictive, autocratic mechanisms that ignore users, their tasks and the organisational setting. The result is a dramatic decrease in the usability of online programs. Another approach is to develop security and its mechanisms for and with its users. Whichever approach is taken, security is set to be the burning issue of the future, as users trust the global online world less and the threats from unauthorised access increase.

CONCLUSIONS

We have argued that appropriate security mechanisms are essential to prevent unauthorised access to learning materials on behalf of both providers and learners. The poor usability of security mechanisms results in users' insecure behaviours and low motivation (Adams, 2001; Adams et al., 1997). These behaviours, in turn, present (to security specialists) a stereotyped user who cannot be trusted and should not be conversed with. This circle needs to be broken by improving communication between security specialists and users and providing user-centred training and design of security mechanisms. It is important to take this communication to a different level than simply security specialists dictating to their users. The future, therefore, of security design for online learning systems lies in collaboration between users and experts to develop the usable mechanisms required for the future.

The other aspect of security we have addressed in this chapter is privacy, including the need for socially acceptable behaviours in videoconferencing and virtual reality environments. Again, the need for usable and appropriate user feedback and control is essential for maintaining trust and confidence in the system (Preece, 2000). Users need rapidly to learn socially acceptable behaviours when working with systems that impose less rigid social protocols than familiar face-to-face learning situations. Care also needs to be taken over how users' images appear to others and how they may be used out of context. Designers of online learning

systems must recognise that people's interpretation of images is strongly influenced by real-world experience and may therefore be inaccurate in the electronic world.

Many of these issues are related to communication and control between the providers of learning resources (at the organisational level) and the users, including both the providers of particular learning materials and the learners. The balance between these two bodies could affect users' perceptions of trust levels, confidence and legitimate use. Imposing mechanisms that circumvent communication or user control may creates perceived feelings of distrust and a lack of confidence in the providing organisation. Krull (1995) suggests that the appropriate use of authority is direction, not control, since explicit, inflexible rules undermine users' confidence. Trust is undermined by force, sending a contradictory message to people that prevents them from judging trade-offs for themselves or feeling part of the proposed solution. A future direction for security would be the development of guidelines and boundaries (but not restrictive controls) that encourage and nurture trust and allow for the natural improvement of users' secure and socially appropriate behaviours.

ENDNOTES

[1] Constructivism is a psychological theory in collaborative learning virtual environments. It highlights the importance of learning environment actions and real interactions. For further information see Vygotsky (1978).

REFERENCES

Adams, A. (1999a). The implications of users' privacy perception on communication and information privacy policies. In *Proceedings of Telecommunications Policy Research Conference* (pp. 65-67).

Adams, A. (1999b). Users' perception of privacy in multimedia communication. In *Proceedings (Extended Abstracts) of CHI'99* (pp. 53-54). ACM Press.

Adams, A. (2000). Multimedia information changes the whole privacy ballgame. In *Proceedings of computers, Freedom and Privacy 2000: Challenging the assumptions* (pp. 25-32). ACM Press.

Adams, A. (2001). Users' perceptions of privacy in multimedia communications. Unpublished doctoral thesis, University College London.

Adams, A., & Sasse, M. A. (1999a). Privacy issues in ubiquitous multimedia environments: Wake sleeping dogs, or let them lie? In *Proceedings of INTERACT'* 99 (pp. 214-221). Springer.

Adams, A., & Sasse, M. A. (1999b). Taming the wolf in sheep's clothing: Privacy in multimedia communications. *Proceedings of ACM Multimedia '99* (pp. 101-107). ACM Press.

Adams, A., & Sasse, M. A. (1999c). The user is not the enemy. *Communications of the ACM*, *42*(12), 40-46.

Adams, A., & Sasse, M. A. (2001). Privacy in multimedia communications: Protecting users not just data. In *Proceedings of IMH HCI'01* (pp. 49-64). Springer.

Adams, A., Sasse, M. A., & Lunt, P. (1997). Making passwords secure and usable. In *Proceedings of HCI'97* (People & Computers XII) (pp. 1-19). Springer.

Barton, B. F., & Barton, M. S. (1984). User-friendly password methods for computer-mediated information systems. *Computers and Security*, *3*, 186-195.

Bateman, B. (2000). Talking tech: Security & Passw***s. *Tech learning*. Retrieved from http://www.techlearning.com/db_area/archives/W…/batetek5.ht

Bellotti, V. (1996). What you don't know can hurt you: Privacy in collaborative computing. In M. A. Sasse, R. J. Cunningham, & R. L. Winder (Eds.), *People and Computers XI (Proceedings of HCI'96)* (pp. 241-261). Springer.

Bellotti, V. (1997). Design for privacy in multimedia computing and communications environments. In P. E. Agre & M. Rotenberg (Eds.), *Technology and privacy: The new landscape*. Cambridge, MA: MIT Press.

Bellotti, V., & Sellen, A. (1993). Designing of privacy in ubiquitous computing environments. In *Proceedings of ECSCW'93, the 3rd European Conference on Computer-Supported Co-operative Work* (pp.77-92). Kluwer Academic Press.

Benassi, P. (1999). TRUSTe: An online privacy seal program. *Communications of the ACM*, *42*(2), 56-59.

Bennett, C. (1997). Convergence revisited: Towards a global policy for the protection of personal data. In P. E. Agre & M. Rotenberg (Eds.), *Technology and privacy: The new landscape* (pp. 99-123). Cambridge, MA: MIT Press.

Brna, P., & Aspin, R. (1997). Collaboration in a virtual world: Support for conceptual learning. In D. Dicheva & I. Stanchev (Eds.), *Proceedings of IFIP WG3.3 working conference* (*Human-computer interaction and education tools*; pp. 113-123).

Brown, I., Perkins C., & Crowcroft, J. (1999, December). Watercasting: Distributed watermarking of multicast media. *Proceedings of Globecom '99*.

Carroll, J. M. (1996). *Computer security* (3rd ed.). Newton, MA: Butterworth-Heinemann.

Clarke, R. (1997). *Introduction to dataveillance and information privacy and definitions of terms*. Retrieved from http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html

Computers, Freedom and Privacy. (1997). Review in the proceedings of the *Seventh Conference on Computers, Freedom and Privacy*.

Cranor, L. F., Reagle, J., & Ackerman, M. S. (1999). Beyond concern: Understanding Net users' attitudes about online privacy. In *Proceedings of the Telecommunications Policy Research Conference*. Retrieved from http://www.research.att.com/projects/privacystudy/

Craver, S., Yeo, B., & Yeung, M. (1998). Technical trials and legal tribulations. *Communications of the ACM*, *41*(7), 45-54.

Davies, S. (1997). Re-engineering the right to privacy. In P. E. Agre & M. Rotenberg (Eds.), *Technology and privacy: The new landscape* (pp. 143-166). Cambridge, MA: MIT Press.

Davis, C., & Ganesan, R. (1993). BApasswd: "A New Proactive Password Checker." In *Proceedings of the National Computer Security Conference* '93, the 16th NIST/NSA conference (pp. 1-15).

Davis, D., & Price, W. (1987). *Security for computer networks*. Chichester, England: John Wiley & Sons.

DeAlvare, A. M. (1990). How crackers crack passwords OR what passwords to avoid. In *Unix Security Workshop II*.

Diffie, W., & Landau, S. (1998). Privacy on the line: The politics of wiretapping and encryption. Cambridge, MA: MIT Press.

Diotalevi, R. N. (2000). Copyright dot com: The digital millennium in copyright. *Online Journal of Distance Learning Administration*, *3*(2). Retrieved from http://www.westga.edu/~distance/diotalevi32.html

Dourish, P. (1993). Culture and control in a media space. In *Proceedings of ECSCW'93* (pp. 125-137). Kluwer Academic Press.

Federal Information Processing Standards. (1985). *Password usage*. Federal Information Processing Standards Publication.

Fluckiger, F. (1995). *Understanding networked multimedia applications and technology*. London: Prentice Hall.

Ford, W. (1994). Computer communications security: Principles, standard protocols and techniques. NJ: Prentice Hall.

Garfinkel, S., & Spafford, G. (1996), *Practical Unix and Internet security* (2nd ed.). O'Reilly & Associates.

Goffman, E. (1969). *The presentation of self in everyday life*. London: Penguin Press.

Granieri, J. P., & Badler, N. I. (1995). Simulating humans in virtual reality. In R. A. Earnshaw, J. A. Vince, & H. Jones (Eds.), *Virtual reality applications* (pp. 253-269). London: Academic Press.

Harris, L. & Associates, & Westin, A. F. (1998). *E-commerce & privacy: What Net users want*. Hakensack, NJ: Privacy and American Business. Hitchings, J. (1995). Deficiencies of the traditional approach to information security and the requirements for a new methodology. *Proceedings of Computers & Security*, *14*, 377-383.

Holmström, U. (1999). User-centered design of security software. *Proceedings of Human Factors in Telecommunications*.

Isaacs, E. A., & Tang, J. C., (1997). Studying bideo-based collaboration in context: From small workgroups to large organizations. In K. E. Finn, A. J. Sellen, & S. B. Wilbur (Eds.), *Video-mediated communications*. Mahwah, NJ: Lawrence Erlbaum.

Kaur, K. (1997). Designing virtual environments for usability. *Proceedings of Human-Computer Interaction* (*INTERACT'97*; pp. 636-639). Aus, Chapman & Hall.

Kling, R. (1996). Information technologies and the shifting balance between privacy and social control. In R. Kling (Ed.), *Computers and controversy: Value conflicts and social choices*. London: Academic Press.

Mackay, W. E. (1995). Ethics, lies and videotape... In *Proceedings of the ACM conference on Human Factors in Computing Systems* (*CHI '95*; pp. 138-145). ACM Press.

Marsh, T. (1998). An iconic gesture is worth more than a thousand words. In *IEEE International Conference on Information Visualisation*.

McAlister, M. K., Rivera, J. C., & Hallam S. F. (2001). Twelve questions to answer before offering a Web based curriculum. *Journal of Distance Learning Administration*, *4*(3).

Needham, R. M., & Schroeder, M. D. (1978). Using encryption for authentication in large networks of computers. *Communications of the ACM*, *21*(12), 993-999.

Neumann, P. G. (1995). *Computer related risks*. New York: ACM Press.

Parker, D. B. (1992). Restating the foundation of information security. In G. G. Gable & W. J. Caelli (Eds.), *IT security: The need for international co-operation*. Holland: Elsevier Science.

Preece, J. (2000). *Online communities*. Chichester, England: Wiley.

Reagle, J., & Cranor, L. F. (1999). The platform for privacy preferences. *Communications of the ACM*, *42*(2), 48-55.

Reeves, B., & Nass, C. (1996). *The media equation: How people treat computers, television and new media like real people and places*. Cambridge, England: Cambridge University Press.

Rime, B., & Schiaratura, L. (1991). Gesture and speech. In R. S. Feldman & B. Rime (Eds.), *Fundamentals of nonverbal behaviour*. Cambridge, England: Cambridge University Press.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the "weakest link": A human-computer interaction approach to usable and effective security. *BT Technical Journal*, *19*(3), 122-131.

Schneier, B. (2000). *Secrets and lies*. Chichester, England: John Wiley & Sons.

Schoeman, F. D. (1992). *Privacy and social freedom*. Cambridge, England: Cambridge University Press.

Smets, G. J. F., Sappers, P. J., Overbeeke, K. J., & Van Der Mast, C. (1995). Designing in virtual reality: Perception-action coupling and affordances. In K. Carr, & R. England (Eds.), *Simulated and virtual realities: Elements of perception*. London: Taylor Francis.

Smith, J. (1993). Privacy policies and practices: Inside the organisational maze. *Communications of the ACM*, *36*(12).

Tromp, J. G. (1995). Presence, telepresence, and immersion: The cognitive factors of embodiment and interaction in virtual environments. *Proceedings of the FIVE conference, Frameworks for Immersive Virtual Environments*.

Vygotsky, L. S. (1978). Mind in society: The development of higher psychological processes. Cambridge, MA: Harvard University Press.

Wacks, R. (1989). *Personal information: Privacy and the law*. Oxford, England: Clarendon Press.

Whitten, A., & Tygar, J. D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. *Proceedings of the 8th USENIX Security Symposium*.