A security framework for online distance learning and training

S.M. Furnell
P.D. Onions
U. Bleimann
U. Gojny
M. Knahl
H.F. Röder and
P.W. Sanders

The authors

S.M. Furnell, P.D. Onions, M. Knahl and P.W. Sanders are at the Network Research Group, School of Electronic, Communication and Electrical Engineering, University of Plymouth, Plymouth, UK.

U. Bleimann, U. Gojny and **H.F. Röder** are at the Fachhochschule Darmstadt, Haardtring 100, Darmstadt, Germany.

Abstract

Considers the requirement for information security within the domain of online distance learning. A generic module structure is presented which represents a high level abstraction of the different stages of the educational process. Discusses the main security issues that must be considered at each stage. These various requirements are being addressed in practice by the security framework being developed by the SDLearn research project, a collaborative initiative between higher academic establishments in the UK and Germany.

Internet Research: Electronic Networking Applications and Policy
Volume 8 · Number 3 · 1998 · pp. 236–242
 · ISSN 1066-2243

Introduction

The provision of education and training facilities at a distance has long been recognised as a means of broadening access to knowledge and enabling study by those for whom it might otherwise be denied (e.g. persons engaged in part-time employment or living in remote rural communities). In recent years, the advent and widespread use of information technology (IT) and, in particular, the mass popularisation of the Internet/World Wide Web (WWW), has meant that opportunities have been identified for developing the distance learning activity into a more advanced online environment.

It has been established that it is possible to support all aspects of the educational process to at least some degree within an online distance learning scenario. At a high level, the key elements can be seen to include the following (Thomas, 1997) :

- Provision of learning materials.
- Providing facilities for practical work (e.g. via simulation).
- Enabling questions and discussion (between students and/or lecturers).
- Assessment.
- Provision of student support services (e.g. careers and personal advice).

Indeed, there is already significant evidence of a move towards online distance learning (ODL), including funded research by bodies such as the European Commission and the adoption of IT-based methods by long-established distance learning providers, such as the UK Open University (Nuttall, 1997) and UNED, the Spanish National Distance Education University (DEMOS, 1997).

This paper proceeds from the basis that online distance learning is an inevitable direction for at least some aspects of the educational process and it does not attempt to adopt a position regarding the pros and cons of the medium from a pedagogical point of view (readers interested in this aspect are referred to work by Paulsen (1995)). Instead, the discussion is focused around the need for appropriate security mechanisms within the environment – an aspect which does not appear to have been given any significant consideration in the work conducted to date. While education is not a domain in which security considerations normally

Internet Research: Electronic Networking Applications and Policy
Volume 8 · Number 3 · 1998 · 236–242

feature prominently, this changes when the online/distance scenario is considered.

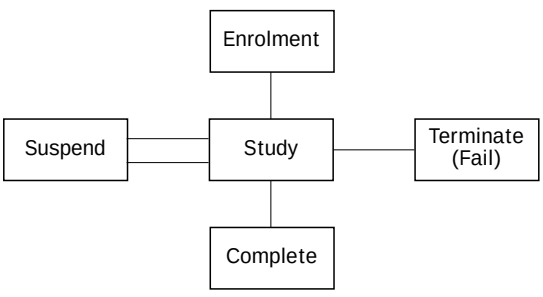
A generic reference model for online distance learning

The discussion can be set in context by introducing a number of entities and activities that will generally be involved in the ODL scenario and identifying the relationships between them. A learning resources provider (LRP) supplies the necessary materials (e.g. course notes, video, etc.) and services (e.g. tutorials, software, etc.) to the remote student over the public multimedia network. Similarly, the student can submit work and otherwise interact with the LRP (and other students) over this network. It should be noted that, in the distance learning scenario, the LRP may not necessarily be a single establishment and may itself be a distributed entity with different module contributions being made from different physical locations. The public multimedia network is currently best characterised by the Internet, which is already used as the basis for a number of trial efforts in this area (Bray, 1997).

Working on the assumption that a student's programme of work is organised around a number of modules (each of which represents a complete, self-contained and assessable portion of the course), the security requirements of distance learning can be examined with reference to the generic module lifecycle illustrated in Figure 1.

The stages identified, and the associated security issues, are detailed in the sections that follow (the list does not claim to be exhaustive but, nevertheless, highlights a number of security issues relating to ODL that might not be immediately apparent).

Figure 1 Generic module lifecycle



Enrolment

This refers to the process of initially identifying the remote students to the LRP and enabling their access to the resources allocated to the module. Security issues here principally include the points below:

(1) Initialisation of an authentication scheme for later use within the study phase. The parameters for both user authentication and non-repudiation would be established. Such a scheme would be likely to involve the use of public and/or secret-key cryptography and utilise interactive protocols, digital signatures and certificates (ISO, 1987).

(2) Eliciting payment for the module from the student. This could involve the use of an Internet-based secure payment protocol, such as the secure electronic transaction (SET) scheme that has been established by credit card companies (MasterCard, 1997), or the direct payment of electronic cash, in a similar manner to experimental schemes already under investigation (Chaum, 1992).

(3) Verifying a student's previous qualifications. These may be from previous modules completed at the same LRP or from other establishments. An electronic certification scheme could be utilised here (as further described in the completion section below).

Study

This phase relates to the period in which the student is actively engaged in work for the module and may itself be subdivided into a number of further distinct stages (e.g. consumption of course material, submission of assignments, tests and examinations). During the course of a module, the following security issues arise:

(1) The student must have access to the necessary LRP material, but should be prevented from viewing or retrieving any which is not relevant to them. Access restrictions may be implemented using either a password scheme or a more complex cryptographic protocol.

(2) The student must be able to submit work to the LRP. This work must be authenticated as having originated from the student and must remain confidential between the student and the LRP. Once submitted the integrity of the work should be inviolable

and it should not be possible for the LRP or student to deny either the receipt/submission or the content of the work.

(3) It is envisaged that real-time lecture/tutorial sessions may be arranged (using audio and/or video-conferencing facilities), involving single students or groups. The communications between those involved should be confidential and not be decipherable to those outside.

(4) It may be desirable for the dissemination of grades (and other similar information) to be confidential between the LRP and the individual students concerned.

(5) The LRP may provide general services to students (e.g. information search and retrieval). It may be advantageous for the LRP to monitor the usage of these services at both the individual level (e.g. for charging purposes) and at the global level for gathering statistics. This information may well be confidential to the LRP.

(6) The LRP may wish to offer the service of a trusted repository. For example, a student may want to submit a piece of original work for which he/she claims ownership. The LRP will be able to verify student identity and submission date in the case of dispute. Such a scheme could be implemented using electronic certification, as described in the next section.

It is considered that some traditional academic scenarios will be extremely difficult to realise securely in the online distance learning context. For example, closed-book tests and examinations could not be performed satisfactorily over the network as it would be impossible to ensure that students were not cheating (e.g. using books or enlisting the help of colleagues) without employing a prohibitive level of technology (e.g. some form of video surveillance of the candidate). As such, examinations would be easier to stage at a regional centre using traditional invigilators (as with existing distance learning providers such as the Open University).

Completion

On successful completion of the module, the following points need to be considered:

(1) The LRP may want to issue some kind of electronic certificate to the student as proof that the module has been completed. This would need to be unforgeable and incorporate information concerning the student, the LRP and the module in question. These certificates could be used to restrict access to information relating to future modules, such that the student is required to complete the current stage of work before proceeding to the next.

(2) The LRP will need to update its records concerning the student in question. This may involve revoking certain rights that the student previously held and invalidating the student's identifier for the module in question.

Termination

In certain circumstances (e.g. the failure of a student to complete a module successfully within a predetermined time period) the LRP may wish to terminate (or renegotiate) the student's enrolment. Security issues involved here are similar to those of the enrolment and completion phases. One possible complication may be that, in renegotiation, proofs of LRP/student actions during the lifetime of the module may be required. Thus, access to student-related information held by the LRP should be available for examination.

Suspension

It is envisaged that, under some conditions, students may wish to suspend their study for long periods and then resume later. This issue again raises some security considerations, as detailed below:

(1) Given that suspension of study may also lead to suspension or reduction of fee payments, students should not be permitted further access to LRP material until study is resumed. Controls would, therefore, need to be incorporated to restrict access.

(2) The LRP will still need to maintain registration details, etc., for suspended students. As such, there will still be protection requirements to be observed in this respect.

It can be seen that the requirement for protection in several of the above examples does not arise for the traditional reasons. For example, safeguarding the confidentiality of course materials is not required owing to the sensitivity of any of the information involved (as most, if not all, of it will already exist in the public domain),

but rather to safeguard the LRP's franchise as a service provider. Only those persons who have enrolled on the module (and paid the appropriate fees) should be permitted access.

Communication requirements

The online distance learning scenario will involve a variety of communication flows between the LRP and remote students (as indicated below and illustrated in Figure 2), each of which may have different security requirements:

- general broadcasts (e.g. lectures, module material);
- student-specific (e.g. assignment grades);
- submission (e.g. work for assessment);
- interactive (e.g. tutorials).

The motivation for security is largely determined by the nature of these communications, as well as the sensitivity of the information maintained by the LRP. The latter would be likely to include the following:

- student records;
- student assignment and examination grades;
- solutions to assignment and examination questions.

It can be seen that there are (at least) three levels of confidentiality within the framework :

(1) information that is public and can be made generally available (e.g. publicity material for courses);
(2) information that should be restricted to enrolled students (e.g. module notes);
(3) information that is private between the LRP and specific students (e.g. assignment grades).

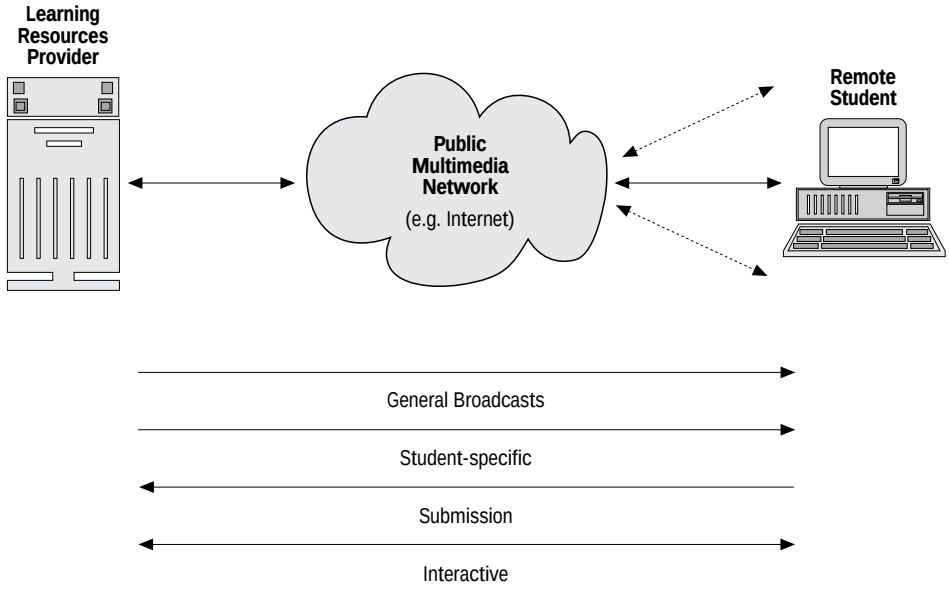
Module notes may also be considered confidential under some circumstances. For example, it may be necessary to hold back future notes until the student has completed the current stage of the work programme and, therefore, access should be controlled. Possession of the notes ahead of schedule could have undesirable consequences, such as giving clues to assignment work in progress or generally detracting from the intended focus of the course.

The SDLearn security framework

This section discusses a number of security techniques that are appropriate to addressing the requirements previously identified. It is considered that the online distance learning scenario principally demands attention in the following areas:

- remote student authentication and accountability;
- access control;

Figure 2 Communication between LRP and remote students



- intrusion detection;
- protection of network communications;
- non-repudiation issues;
- LRP "housekeeping" issues.

These areas will now be examined.

Authentication and accountability

At the simplest level, authentication could be based on traditional password mechanisms. These have the advantage that they can be easily implemented using software methods and are conceptually simple for the user to understand. However, their use could be problematic if applied on a module-by-module basis, as this would result in a number of them having to be remembered. In addition, there are a number of generally accepted weaknesses with passwords (e.g. they are often poorly selected, easily guessed and infrequently changed) that make them vulnerable to compromise (Jobusch and Oldehoeft, 1989).

One suggested enhancement is to incorporate location-based authentication by invoking a call-back facility when students log into the LRP system. This will at least ensure that access is occurring from the expected location (and is, therefore, more likely to be the legitimate student than an impostor). This strategy has disadvantages in that it assumes that the remote student will always wish to gain access from a single place (such as their home) and in that it may introduce complications regarding the payment for connection time (as it will be costing the LRP to call back to the student).

More sophisticated user authentication schemes involving smartcard technology permit the construction of strong authentication systems with a minimal complexity interface to the user (Zoreda and Oton, 1994). Their main advantage lies in the secure storage and processing of secret information. In practice this means that user-confidential key material is held only by the smartcard and is not made available to external entities. In an open network environment this prevents malicious software agents from recovering user-stored data (e.g. a password encrypted signature key) and using off-line cryptanalytic techniques (e.g. a dictionary search) to recover the user's secret. The main disadvantage of smartcard systems over simple password-based systems is the additional cost involved in setting up the required infrastructure. However, it seems conceivable that the LRP make provisions for such an architecture based on the cost savings of not having to provide campus facilities. Also it may not be unreasonable for students to supply their own smartcard-enabled hardware. With the latest network computers directly incorporating smartcard technology this may be easier than would previously have been thought (Halfhill, 1997).

Whatever authentication mechanism(s) are selected, it will be desirable for them to be generic for all modules, in order to minimise inconvenience for the end users. For example, if password-based authentication was used, it would be undesirable to have different passwords for each module. Consistency and simplicity should be retained wherever possible.

The accountability issue is closely linked to that of authentication and relates to the fact that it is necessary to instil a sense of responsibility among students when accessing LRP facilities. A step towards achieving this will be to make them aware that they will be held accountable for their own activities. This would principally be ensured through the maintenance of audit trails, recording significant details of activity based on authenticated user identities.

Access control

Once logged-in, access to specific information would be controlled using the electronic certificates mentioned previously. Possession of an appropriate certificate would be a requirement before granting access. These would be used in addition to any access control options already present in the host operating system (e.g. use of file/directory permission to prevent students browsing through the LRP's file space).

Intrusion detection

In addition to the above-mentioned authentication and access control schemes, sophisticated intrusion detection systems could be implemented by the LRP. For example, real-time supervision could be introduced which monitors and compares the behaviour of a logged-in user against a historical profile for the remote student whom they are claiming to be. Such a profile could encompass a range of factors, including time of system accesses,

facilities used and data accessed. The supervision could also consider a variety of general indicators that might be suggestive of an intrusion scenario (Furnell *et al.*, 1996; Lunt, 1993). This approach would have the advantage of being achievable in software and, therefore, avoiding any associated financial cost per workstation (unlike using smart cards on conventional PCs). However, disadvantages could exist in terms of unreliability (particularly the potential for false rejection of legitimate users) and resistance by end-users, who may object to the notion of their activity being monitored in this way. As such, this approach requires further investigation before it can be fully recommended.

Network communications

It is proposed that the necessary protection for network communications could be achieved using data encryption techniques. A hybrid system is advocated in which symmetric (secret-key) encryption would be used to implement a confidentiality service (with both LRP and student parties sharing common session keys), while asymmetric (public-key) encryption would be used for confidential session key distribution and to provide non-repudiation services (based on digital signatures).

Non-repudiation

Requirements for non-repudiation will exist on both sides and will be required in order to prevent repudiation of :

- message origin (e.g. to verify that the work originated from the student);
- message receipt (e.g. to prove the work was received by the LRP);
- message content (e.g. to prove that the received message is the same as that which was sent).

Non-repudiation of origin can be achieved using digital signatures, where communications are electronically "signed" by the sending party using their secret key. Examples of this requirement in the online distance learning context are as follows :

- remote students will sign work to prove that it is theirs;
- LRP will issue signed receipts for work submitted (receipts will include a timestamp and a message authentication code (MAC) to certify message content;
- LRP will sign the certificates that it issues in order to allow access to module material etc.

Non-repudiation of content can be achieved by sending a (signed) MAC, which is essentially the result of a message-digest function, such that any change in the data will result in a discrepancy between the transmitted MAC and the new value calculated at the recipient end. This effectively provides a message integrity service.

Housekeeping issues

These relate to the general considerations that apply to most IT systems (e.g. issues of back-up and recovery, physical protection for the LRP establishment). It is not anticipated that the distance learning context would dictate any special requirements here.

At a general level, system availability and reliability will be important. Given that students may conceivably wish to access the system for reference at virtually any time, a high degree of "up time" will be required for LRP systems.

Implementation

The security issues identified are being addressed in practice by the security framework being developed by the SDLearn research project, a collaborative initiative between researchers in the University of Plymouth (UK) and the Fachhochschule Darmstadt (Germany), with supportive funding from the British Council and the Deutscher Akademischer Austauschdienst (DAAD).

The project aims to develop new standards for, and the implementation of, an integrated solution for secure distance learning. The technology base will include multimedia PCs utilising the Microsoft Windows operating system and Internet/WWW browsing software. Underlying telecommunications facilities will be provided by relatively new technologies such as ATM, as well as the more widely available ISDN.

The initial implementation of SDLearn will not attempt to address all of the issues identified in the paper and will instead concentrate on the areas of student authentication and secure communications between students and LRP for

different levels of activity (e.g. from browsing to assignment submission). The framework will be realised through a combination of established and enhanced security technologies. Existing elements that may be used "off the shelf" are considered to include encryption algorithms, smartcard technologies and certification schemes. By contrast, the aspects that are considered to require some degree of bespoke development to address ODL-specific requirements include user authentication and supervision arrangements.

User-friendliness will be a key issue in the design of the framework, as it is vital from a practical point of view that the provision of security does not impede the learning process. As such, non-intrusive methods of security will be given special consideration. Embedding the protection within a standard functional front-end is considered to be one suitable approach, offering end-user options such as "browse notes", "submit assignment" and "contact tutor" which then implicitly invoke the required level of security.

The research will also address aspects such as an ergonomic graphical user interface (GUI) for ODL and the integration of appropriate multimedia technologies (e.g. video-conferencing), although it is anticipated that several aspects here may be inherited from previous work by other initiatives.

Conclusion

The paper has shown that the practical realisation of ODL brings with it a significant number of issues that require consideration. These relate to the wellbeing of the LRP and its students and it is, therefore, in the interests of both parties for matters to be properly addressed.

It is considered that the provision of a secure framework, such as that proposed by SDLearn, may act as a catalyst for online learning, providing the trust and confidence necessary to encourage a variety of future courses to be established and run. The resulting courses would also inherit the more familiar pedagogical advantages of the distance learning scenario, in terms of convenience, flexibility and reduced financial overheads. All of these factors would apply, to some degree, to both the remote students and the learning resources provider.

References

Bray, P. (1997), "Loving to learn the Internet", *The Sunday Times*, "Wired World" Supplement, 27 April, p. 11.

Chaum, D. (1992), "Achieving electronic privacy", *Scientific American*, August, pp. 96-101.

DEMOS (1997), *Distance Education and Tutoring in Heterogeneous Telematics EnvironmentS*, EU Telematics applications for users and providers project, http://www.redestb.es/personal/softbase/demosfra.htm.

Furnell, S.M., Morrissey, J.P., Sanders, P.W. and Stockel, C.T. (1996), "Applications of keystroke analysis for improved login security and continuous user authentication", in *Proceedings of IFIP SEC '96 – 12th International Conference on Information Security*, Samos, Greece, 21-24 May, pp. 283-94.

Halfhill, T.R. (1997), "Cheaper computing: part 1", *Byte*, Vol. 22 No. 4, pp. 66-80.

ISO (1987), *Information Processing Systems – Open Systems Interconnection Reference Model – Part 2: Security Architecture*. International Organisation for Standardization, ISO 7498-2.

Jobusch, D.L. and Oldehoeft, A.E. (1989), "A survey of password mechanisms : part 1", *Computers & Security*, Vol. 8 No. 7, pp. 587-604.

Lunt, T.F. (1993), "A survey of intrusion detection techniques", *Computers & Security*, Vol. 12 No. 4, pp. 405-18.

MasterCard (1997), "SET secure electronic transaction specification – book 1: business description", Version 1.0, MasterCard/VISA, 31 May, http://www.mastercard.com/set/

Nuttall, N. (1997), "University meets online challenge", *The Times*, "Interface" supplement, 19 February, p. 11.

Paulsen, M.F. (1995), "The online report on pedagogical techniques for computer-mediated communication", ISBN 82-562-3690-6, NKI, Oslo, Norway. http://www.nki.no/~morten/

Thomas, P. (1997), "Teaching over the Internet: the future", *Computing & Control Engineering Journal*, Vol. 8 No. 3, pp. 136-42.

Zoreda, J.L. and Oton, J.M. (1994), *Smart Cards*, Artech House.