Security issues in Online Distance Learning

by S.M.Furnell and T.Karweni, University of Plymouth

This paper considers the issue of security in the provision of online distance learning. Security represents an aspect that may not suggest itself as a high priority in an educational environment, but evidence indicates that it is definitely required. The discussion presents an overview of the key security requirements and the main technical elements needed to address them.

Introduction

Online Distance Learning (ODL) represents an area of significant interest in the academic environment. It is attracting attention from both established providers of distance-based education (such as the Open University) and traditional education institutions, whose mainstay courses are typically attendance-based. A major catalyst for this interest is the widespread adoption and accessibility of the Internet / WWW platform. However, whilst a significant amount of work has proceeded in areas such as the development of online materials, the attention to the issue of security has been inconsistent. It is, nonetheless, an aspect that is required by both remote students and Learning Resources Providers (LRPs – which may be universities, colleges or, indeed, training departments within commercial organisations).

The content of this paper is drawn from work conducted as a part of the SDLearn (Secure Distance Learning) project, a collaborative initiative between the University of Plymouth (UK) and the Fachhochschule Darmstadt (Germany). The aim of the project was to develop a standardised security framework for ODL applications – details of which are presented in the sections that follow. The British Council and Deutscher Akademischer Austauschdienst (DAAD) jointly funded the project.

The need for security in online education

The Internet medium is well known to play host to numerous threats, including all of the following:

- Malicious software such as viruses, worms, Trojan Horses
- Hacking, Denial of service attacks
- Masquerading, spoofing
- Fraud, data theft, malicious damage

It can be argued that, being based on an Internet platform, ODL potentially leaves the way open to all of these. At the same time, however, the question arises of whether security is really an issue for the educational environment. The majority of traditional universities can typically be seen to have a number of protection measures in place, such as the following:

- anti-virus controls;
- IT usage policy (e.g. in the UK this would likely be based on the JANET Acceptable Use Policy[1]);
- scanning and monitoring;
- prevention of unauthorised software installation.

Looking at such a list, however, the question arises of whether this protection is included for the benefit of students or whether it is actually to guard against them. Although it can be argued that students themselves will benefit from these security measures, the underlying objective would appear to be the protection of the university's interests. In an ODL scenario, remote students will have more direct security concerns than their on-campus counterparts, potentially necessitating a wider range of protection methods.

If there are doubts about whether security problems are likely to be an issue in education, then the following survey-related observations provide some persuasive evidence:

- in the 1998 Audit Commission IT Fraud & Abuse survey[2], 59% of education

respondents reported IT abuse (representing a 23% increase when compared to the 1994 results).

- in the 1998 NCC/DTI Business Information Security Survey[3], 48% of education respondents reported security breach incidents.

- Attrition.org, a web site within the security/ hacker community, maintains an archive of hacked web sites. During September 2000, this included 26 universities[4].

As an example of how academics consider issues relating to security, it is possible to make reference to the issue of student authentication and authenticity, which appeared as an issue on the *Educational Telematics* list in October 2000[5]. *Educational Telematics* is an email-based discussion forum, which (at the time) had 170 members from 35 countries. On 6 October 2000, the convenor of the list posed the following question:

> "What about authenticity in on-line learning environments? How are we to check that the student submitting assignments is who s/he say s/he is?"

Examples of three typical responses from list subscribers are given below:

- "I don't see authenticity as a problem at all…"

- "I don't think that we should worry about authenticity. People who have enough drive to study at a distance and online are already committing themselves to hard work"

- "I think the authenticity can be solved with digital signatures attached to accounts"

As can be seen, only one of the respondents actually seems to consider the security issue to be a problem. In view of the abuse statistics previously mentioned, there is clearly a disparity between the opinions of some academics and the actual situation.

Trust in the status and credibility of the LRP is vital for both online students and prospective employers, as it obviously reflects upon the value of the associated awards. Unfortunately, the credibility of online courses may already have begun to be undermined by the plethora of bogus qualifications that can be obtained via the Internet. An example of an advert for such offerings is shown in Figure 1, which depicts the content of a message that the authors have frequently received by email. From the perspective of people wishing to pursue or offer ODL-based courses, such messages are not at all beneficial, as they may lead to suspicion and adverse publicity about the online medium as a legitimate learning environment and tarnish the credibility of genuine ODL courses and their providers.

```
U N I V E R S I T Y   D I P L O M A S

Obtain a prosperous future, money earning power, and the admiration of all.

Diplomas from prestigious non-accredited universities based on your present
knowledge  and life experience.

No required tests, classes, books, or interviews.

Bachelors, masters, MBA, and doctorate (PhD) diplomas available in the field of
your choice.

No one is turned down.

Confidentiality assured.

CALL NOW to receive your diploma within days!!!

1 - 3 1 2 - 5 7 7 - 1 6 7 7

Call 24 hours a day, 7 days a week, including Sundays and holidays.
```

Figure 1 – Qualifications for sale in email message

In view of these points, it can be seen that the ODL domain merits attention in terms of security. As such, the next section will proceed to assess where the main requirements may exist.

Security requirements in course delivery

Figure 2 depicts a top-level view of an Internet-based ODL solution, with a number of remote students accessing one or more LRP servers. In terms of security, requirements can be seen to exist at both ends and during data transport.

The underlying requirements are considered in more detail in Table 1. This highlights the main issues that must be addressed and indicates whether they are of interest from the student and/or LRP perspectives.

It is also interesting to consider where security requirements fit into the overall delivery of an ODL programme. 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 *course / module lifecycle* illustrated in Figure 3.

The elements of this lifecycle, and their associated security requirements, have previously been described[6], but summary details are provided below.

Enrolment

Initially identifying the remote students to the LRP and enabling their access to the facilities allocated to the module / course.

Security issues:

- Register user & establish authentication parameters;
- Payment of registration fees;
- Verification of previous qualifications.

Study

The period in which the student is actively engaged in work for the module. This may be divided into further distinct stages / activities, such as the consumption of course materials, the submission of coursework assignments, and tests and examinations.

Security issues:

- Access control on module content;
- Secure submission of work;
- Confidentiality and non-repudiation of communications;

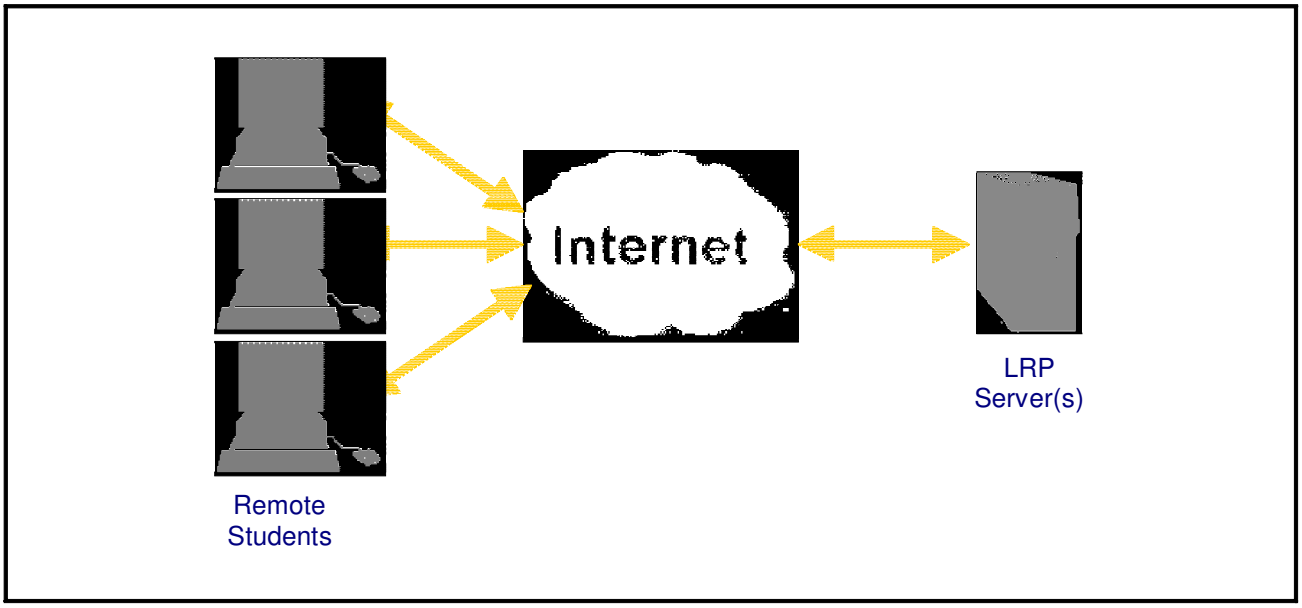

Figure 2 – Overview of ODL environment

Security Issues	Student Interest	LRP Interest
Privacy and confidentiality of personal data	✓	✓
Security of service usage - Authentication and accountability - Access control to LRP's system - Intrusion detection system	✓	✓ ✓ ✓
Secure communications between staff and students	✓	✓
Security of payment - Non-repudiation of payment - Integrity of payment - Prevention of fraud	✓ ✓	✓ ✓
Security of submitted work - Authentication - Confidentiality - Non-repudiation - Integrity	✓ ✓ ✓ ✓	✓ ✓ ✓
Security of course material - Prevention of unauthorised access - Prevention from illicit distribution - Software licence control		✓ ✓ ✓
Digital certificate for course completion - Verification of issuing establishment - Verification of certificate integrity	✓	✓ ✓
Confidentiality of student grades	✓	✓
Reliability and availability of LRP's system	✓	✓
Confidentiality and secure conduct of exams/tests	✓	✓

Table 1 – ODL security requirements summary

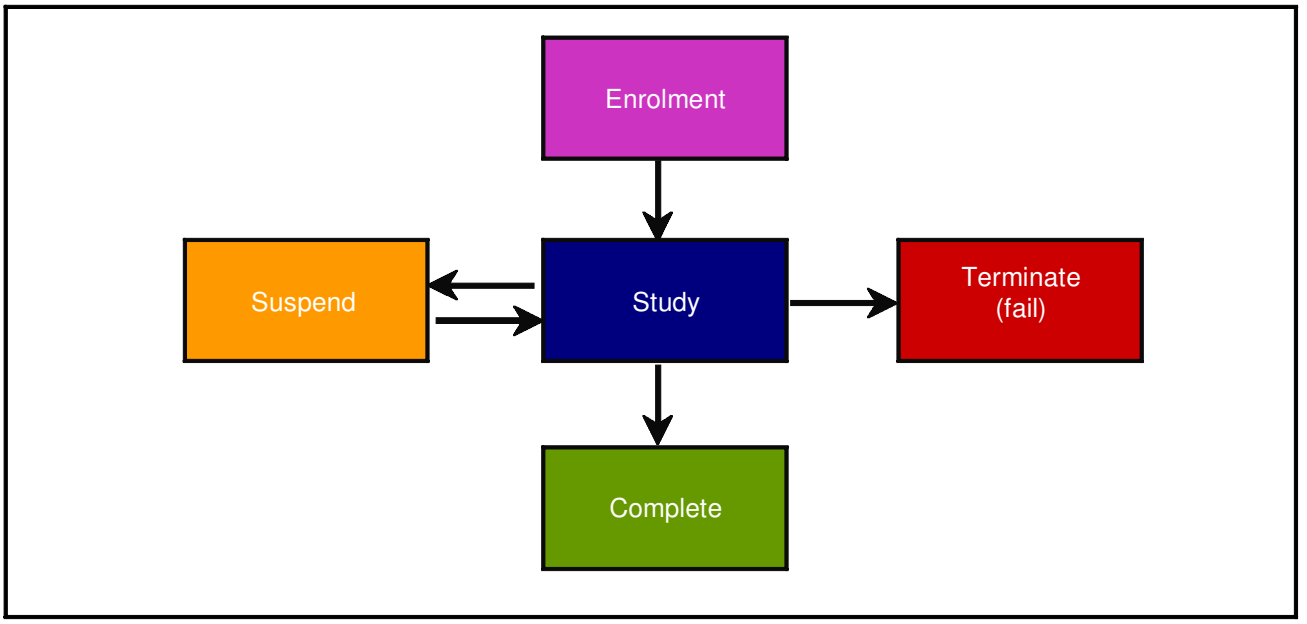

Figure 3 – Generic course / module structure

- Service monitoring;
- LRP provision of a trusted repository.

Completion

Upon successful completion of a module, the LRP will need to issue a certificate and update the student records accordingly.

Security issues:

- Issue of electronic certificate;
- Update of student access rights (e.g. revoking / restricting rights to the completed module).

Termination (optional)

In certain circumstances, the LRP may need to terminate a student's enrolment (e.g. due to failure to complete a module).

Security issues:

- Revocation of access.

Suspension (optional)

Students may wish to suspend their study and then resume it at a later time.

Security issues:

- Restriction of access;
- Continued protection of registered details.

A security framework for ODL

Looking at the requirements from the previous section, it may already be apparent that many of the security issues relevant to ODL are relatively standard and also apply in other domains. As a result, off-the-shelf security solutions may suffice in some cases. Having said this, it is still necessary to determine the stages at which they are required and it is also desirable for them to be *integrated* within the overall ODL platform. With this in mind, this section summarises the elements of a recommended security framework.

It is considered that the online distance learning scenario principally demands attention in the following areas:

- authentication and accountability;
- access control;
- protection of communications;
- non-repudiation issues;
- LRP server protection.

Authentication and accountability

Authentication facilities are required for two main reasons:

- to ensure that only registered students can gain access;
- to ensure that any online / remote examinations are conducted by the correct / claimed individual only.

At the simplest level, authentication could be based upon 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, 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[7]. A further problem of passwords is that there would be nothing to prevent a legitimate student from sharing their access rights with other people. It could, therefore, be considered desirable to utilise techniques more closely tied to the registered student. Options here might include some form of physical token (e.g. a smart card), biometric techniques (e.g. voice or face recognition) and/or anomaly detection based upon departures from a profile of 'normal' behaviour for the legitimate user.

It may be questioned whether enhanced authentication mechanisms are actually merited, particularly

in view of the fact that much of the content disseminated in academic courses can typically be found in the public domain. However, in contexts where the LRP is a company, proprietary or commercially sensitive material may be involved and, therefore, require additional protection. Stronger authentication may also be useful in the context of online examinations.

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 were 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 amongst 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 insured through the maintenance of audit trails, recording significant details of activity based upon *authenticated* user identities.

Access control

Once logged-in, access to specific information would be controlled using the rights allocated at enrolment. There may be various levels of confidentiality within the framework:

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

Control of student access would be achieved by associating the module content with the correct privilege level. A successful login would invoke this privilege level, allowing them to access:

- all appropriate modules taken by student;
- proprietary software applications hosted on the LRP's server;
- student tools (such as personal notes, calendar, email, chat rooms etc.);
- personal settings and information (such as change of password, address etc.);
- personal records such as own grades, exam results, and assessment feedback;
- general/public announcements, student bulletin boards and newsgroup material.

LRP instructors would, of course, have different privileges and, in this case, successful login would enable access and control of:

- materials relating to their taught modules;
- proprietary software available to students;
- specific instructor's tools (e.g. for designing modules, maintaining student grades etc.).

They would also have access to the same general tools and information sources as the students. It should be noted that, in some cases, the policy of the LRP may be that individual instructors should not have complete autonomy over issues such as the update of their live course materials or the allocation of student access rights to LRP software. In such cases, a further level of administration would be involved to control the update of materials offered on the live courses.

Protection of 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), whilst asymmetric (public-key) encryption would be used for confidential session key distribution and to provide non-repudiation services (based upon 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 the sending party using a secret key electronically signs messages (and signatures can subsequently be verified using an accompanying public 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 MAC to certify message content - see below);
- 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) Message Authentication Code (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.

LRP server protection

The LRP server contains a range of sensitive information, including student details, course materials and assessment information, all of which must be protected against unauthorised access. Network access may be restricted by technologies such as firewalls. In addition, there are more general 'housekeeping' issues to be considered (e.g. back-up and recovery, physical protection for the LRP establishment). It is not considered that the ODL context dictates 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.

Conclusions

ODL represents a growing area of interest in the education and training domains. It is considered that this trend is likely to increase as a result of both improved technologies (e.g. for information delivery) and an increased emphasis on lifelong learning. In such a context, security will increasingly be a feature that end users expect. Indeed, they are likely to be attuned to the potential risks as a result of the general publicity that surrounds security issues on the Internet. From the perspective of the learning providers, the recognition of the threats is as much of an issue as identifying appropriate countermeasures. As the discussion has highlighted, the types of control that are required (e.g. authentication and access control) are by no means unique to the ODL context and, in many cases, the strength of protection required will be considerably less than in other environments. What is required is a realisation that, despite its benevolent objectives, the educational domain is not immune to security problems and, therefore, security controls need to be built into any online delivery frameworks that are to be used.

References

1. UKERNA. 1999. JANET Acceptable Use Policy. Version 5.0. February 1999. http://www.ja.net/documents/use.html.

2. Audit Commission. 1998. *Ghost in the Machine - An Analysis of IT Fraud and Abuse*. Audit Commission Publications, United Kingdom. ISBN 1-86240-05603.

3. NCC. 1998. *BISS '98 – Information Security, The True Cost To Business.* National Computing Centre, Manchester, UK. http://www.ncc.co.uk/

4. ATTRITION. 2000. ATTRITION Web Page Hack Mirror. September 2000. http://www.attrition.org/mirror/attrition/2000-09.html

5. Educational Telematics. 2000. http://www.fae.plym.ac.uk/tele/tele.html.

6. Furnell, S.M, Onions, P.D, Bleimann, U, Gojny, U, Knahl, M, Röder, H.F and Sanders, P.W. 1998. "A security framework for online distance learning and training", *Internet Research*, vol. 8, no. 3: 236-242.

7. Jobusch, D.L. and Oldehoeft, A.E. (1989), "A Survey of Password Mechanisms: Part 1", *Computers & Security*, vol. 8, no. 7: 587-604.

Contact details

S.M.Furnell
Email: sfurnell@plymouth.ac.uk

T.Karweni
Email:titis@jack.see.plym.ac.uk

Network Research Group
Department of Communication and Electronic Engineering
University of Plymouth
Plymouth
PL4 8AA