SECURITY CONSIDERATIONS IN ONLINE DISTANCE LEARNING

Steven Furnell[†], Udo Bleimann[‡], Johnni Girsang[†], Horst Röder[§], Peter Sanders[†] and Ingo Stengel[‡]
[†] School of Electronic, Communication and Electrical Engineering, University of Plymouth, Plymouth, UK
[‡] Department of Computer Science, Fachhochschule Darmstadt - University of Applied Sciences, Haardtring 100, Darmstadt, Germany
[§] Department of Electrical Engineering / Telecommunications, Fachhochschule Darmstadt - University of Applied Sciences, Haardtring 100, Darmstadt, Germany

e-mail: sfurnell@plymouth.ac.uk

KEYWORDS

Online Distance Learning, Security, Authentication, Digital Copyright, Firewalls.

ABSTRACT

The paper considers the need for information security within the emerging field of online distance learning (ODL), which is currently gaining popularity amongst universities and other training institutions. General security requirements are considered, leading to specific consideration of issues relating to user authentication and electronic copyright protection, both of which are important concerns from the perspective of the organisation offering the ODL service. The discussion is based upon work being undertaken within the SDLearn research project, a collaborative initiative between higher academic establishments in the UK and Germany, with the overall aim of producing a standardised ODL security framework.

INTRODUCTION

Online distance learning (ODL) represents an area of significant interest in the modern academic environment. The mass popularity and acceptance of Internet and World Wide Web technologies has served to provide a platform from which potential students can gain access to remote expertise and resources, on either an individual or organisational basis. The ODL concept has attracted attention from established providers of distance-based education (e.g. the Open University in the UK), as well as encouraging traditional higher education establishments to enter the market. As a result, a number of different ODL approaches are currently either under development or in the early stages of live operation (see, for example, DEMOS 1997; Nuttall 1997).

Whilst current efforts have all generally focused upon the key issues of how to usefully create or migrate courses for the online context and deliver an effective learning experience, the attention to supporting requirements has been less consistent. This paper examines one such requirement – namely, the need for security of the service.

From the Learning Resource Provider (LRP) perspective, the key driver for security is to ensure that its ODL resources are only made available to registered users. This assumes the (likely) scenario in which the ODL facility is being offered as a payment-based service and that the LRP consequently does not wish to see its offerings made available to those who have not done so. Addressing this requirement implies protection at a number of levels:

- authentication of ODL service users;
- the ability to trace the dissemination and/or prove ownership of LRP materials in order to prevent unauthorised copying, redistribution and reuse.
- protection of the LRP server / core systems from unauthorised access.

There are also obvious security concerns that may be raised from the remote student perspective, including confidentiality of personal registration details, privacy of communications with tutors, safeguarding of submitted work and the like. For the purposes of this discussion, however, these are considered to be secondary issues against the concerns of the service provider. In practice, of course, the concerns of both sides will need to be addressed for the service to be viable.

THE SDLEARN PROJECT

The discussion is based upon work currently being conducted by the SDLearn research project, a collaborative initiative between researchers in the University of Plymouth (United Kingdom) and the Fachhochschule Darmstadt (Germany), with supportive funding from the British Council, the Deutscher Akademischer Austauschdienst (DAAD) and industrial companies (namely Nortel and Cabletron Systems in Germany). The aim of the project is to develop a standardised security framework for ODL applications, with the implementation of key elements in prototype form to illustrate the concept.

The SDLearn approach focuses upon two main actors – namely the LRP and the Remote Student. The LRP is the institution that provides the distance learning services. It may be a university or training company, but in either case will

operate one or more servers to support the delivery of material.

The security approach adopted within SDLearn is based around the concept of a generic module lifecycle, which represents the various potential stages of a remote student's relationship with the LRP. This is illustrated in figure 1 below.

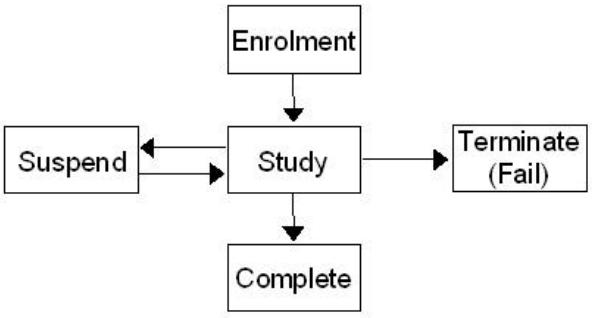

Figure 1: Generic Module Lifecycle

Each of these stages is considered to have a number of associated considerations from the security perspective, as summarised in table 1. These are discussed in detail in Furnell et al (1998).

SDLearn is not the only approach to security in ODL. An example of another notable initiative is the Instructional Management System (IMS) project (Educom 1997). The overall aim of IMS is to enable an open architecture for online learning (i.e. addressing more than just the security issues alone), based upon standard Internet protocols. The work represents a collaboration between academic, commercial and government organisations in the United States, as part of the National Learning Infrastructure Initiative. The security approach in IMS is specifically focused on the provision of a framework within which course modules (termed 'containers') from different LRPs may be integrated to form an overall programme of study. As a consequence, the security requirements identified are most closely related to issues of access control on the content (although authentication and secure communications issues are also identified). The SDLearn approach takes a potentially wider view and encompasses the full range of issues to be considered by an individual LRP. It will also be of use as a reference point for systems that have been designed / implemented without an overall guiding approach such as IMS in mind.

Stage	Security Requirements / Issues
Enrolment	• Register user and establish authentication parameters • Electronic fee payment • Verification of previous qualifications
Study	• Access control on module content • Secure submission of work • Confidentiality and non-repudiation of communications • Service monitoring • LRP provision of a trusted repository
Completion	• Issue of electronic certificate • Update of student access rights
Termination	• Revocation of access
Suspension	• Restriction of access • Continued protection of registered details

Table 1 : ODL Security Considerations

The next sections will now proceed to discuss the LRP security issues that were identified earlier.

AUTHENTICATION

In common with other applications, authentication is a key security requirement in ODL. Reliable facilities are required for two main reasons:

1. To ensure that only registered users can gain access;
2. To ensure that any online / remote examinations are conducted by the correct / claimed individual only.

The realisation of user authentication in existing ODL implementations can generally be seen to be fairly basic. The approaches taken can be categorised at three general levels, as follows:

- use of the simple user ID and password (in some cases the password is provided by the LRP, which may be considered to provide increased protection, as it should avoid the use of obvious / more easily guessed passwords that might be selected by the students)
- authentication via the terminal profile (e.g. IP address, browser version etc), normally in conjunction with password protection. This system is useful if the remote student can be assumed to always access the LRP from the same computer.
- use of specially designed or modified browser software to access the LRP location (with the browser only being made available to registered students).

Approaches such as these may be considered to provide sufficient security in most scenarios, but it should be recognised that the protection is not totally comprehensive. For example, none of the above would necessarily prevent the legitimate student from sharing his/her access rights with unregistered colleagues (although the use of a terminal profile would complicate things slightly, it would still be possible for a determined user to work around it – e.g. by duplicating the configuration of the registered system). As such, it could be desirable to utilise authentication techniques that are more closely tied to the legitimate student. One approach here could involve anomaly detection based upon departures from the users 'normal' behaviour. This could be profiled over time during the student's initial ODL sessions (using factors such

as time and location of access, and the patterns of interaction observed) to determine consistent elements that could then be utilised as potential future authenticators. Such techniques form the basis of various intrusion detection architectures (e.g. the Intrusion Detection Expert System (Lunt 1990) and the Intrusion Monitoring System (Furnell et al. 1997)) and typically utilise expert system and neural network approaches to facilitate profiling.

In the context of a normal university-type course, it is unlikely that an advanced authentication approach would be considered warranted (i.e. given that the core information itself is likely to be in the public domain and the LRP role has largely been in terms of its 'packaging'). However, the SDLearn approach is also intended to cater for other ODL scenarios where the disseminated material may be of a more sensitive nature. An example of where this might be the case is with company-based training programmes, where proprietary or commercially sensitive information might be involved.

The issue of online examinations represents a problematic concept. The concerns here are to ensure: that it is the registered student taking the exam; that he/she is working alone; and that no other form of cheating is taking place (e.g. unauthorised use of books / notes etc.). These issues could be addressed using technological solutions that would feasibly form part of a standard ODL system configuration, although the requirement in this case moves beyond authentication and towards supervision / monitoring. For example, a combination of Internet audio and video could be utilised to keep the student under 'surveillance' during the defined examination period. The workability of this idea obviously depends upon user acceptance, but it is essentially creating a scenario that is no different from the conditions under which traditional exams are sat. It is, however, conceivable that particularly devious students could still compromise this approach (e.g. by enlisting the help of a silent collaborator out of camera shot) and, therefore, some LRPs may not consider the remote exam scenario a suitable option.

ELECTRONIC TRACKING AND PROOF OF COPYRIGHT

One of the LRP's most significant assets in the ODL scenario is the content that it creates and disseminates. As such, consideration must be given to affording it appropriate protection. Problem scenarios here may include:

- a single student registering legitimately and then passing the materials on to his/her colleagues;
- a representative from another LRP registering as a student, enabling materials to be obtained, which are then repackaged for use in their own programmes.

Provision of a facility to enable the automatic tracking or tracing of disseminated material represents a non-trivial undertaking. Tracking the initial dissemination from the LRP to the remote student would be simple enough (and the recording / archiving of such 'transaction' information is recommended by the SDLearn approach for audit purposes). However, what can be done beyond this? How can one track any further (unauthorised) dissemination of the material by the remote student once the material is in his/her possession? The issue is not impossible to resolve, but it is difficult to identify a method that would not have potentially significant adverse impacts upon the usability of the material for legitimate users. For example:

- Placing content within an intelligent 'wrapper' which is able to maintain contact with the originating LRP (e.g. in the same way as a mobile agent) so that unauthorised dissemination / duplication would be identifiable. This situation would be quite complicated in the sense that each element of content would effectively become a program in its own right (which could restrict portability between different platforms). It would also be necessary to ensure that it is impossible to extract the material from within the wrapper and distribute it independently (which could restrict usability).

- Preventing students from being able to obtain a permanent local copy of the material. Viewing of information could be restricted via use of a bespoke browser (provided by the LRP at registration time), without 'Save' or 'Copy/Paste' options. ODL materials would be disseminated in a proprietary file format, only readable within this special software. Whilst this might solve the problem from the LRP perspective, it would be restrictive on the students, requiring them to connect to the LRP each time they want to obtain the same piece of information and preventing legitimate reuse of material.

If it is not possible to actually trace the path of material as it is disseminated, then the next best approach would be to enable proof of ownership in the case where unauthorised use is suspected. In minor cases (e.g. one user providing a copy to a friend) the event could obviously go unnoticed. However, on a larger scale (e.g. one LRP reusing the materials of another), the chances of detection would be greater. This would generally be sufficient, as it is such larger cases that would have the potential for the greatest adverse impact upon the LRP creating the material (e.g. losing potential business to a rival). For this reason, the SDLearn work is considering the issue of Electronic Copyright.

Proving that certain material belongs to a claimed LRP is not problematic in the initial instance, as it can be provided to students after having firstly been *signed* using the private key of the LRP (assuming a digital signature service within an asymmetric cryptosystem such as RSA). However, the problem exists in proving LRP ownership beyond this. What is required is some means of encoding or determining a suitable copyright identifier within the material itself – i.e. digital watermarking. Such techniques are widely discussed in relation to image data and various potential approaches have been recommended (Delaigle at al. 1996). However, an issue

of more interest in the ODL context is how to apply the same sort of approach with a text-based document. Wayner (1997) has discussed a number of potential approaches, but all of these involve changing the content of the document in some way. A copyright identifier could, for example, be encoded by fractionally modifying the spacing between words or lines. However, this restricts dissemination to formats such as postscript, which may limit flexible use by the LRP and the remote students. Alternatively, an identifier could be achieved via word substitution (e.g. replacing certain key words by synonyms so that, for example, "fine" is always changed to "nice"), such that the resulting document is recognisable as having the style of the LRP. This, however, may not always be effective, in that it risks subtly changing the meaning of the text. The problem, therefore, remains of how to achieve an electronic copyright identifier without introducing potential restrictions. The SDLearn project has included some preliminary work in this respect, examining the potential for using grammatical analysis (i.e. the writing style of an author) to determine a measure from which authorship (and, hence, LRP ownership) could be determined. However, the overall results from this work were disappointing, with False Acceptance Rates of 35-72% and False Rejection Rates of 8-23% being observed. Full details of the experimental study can be found in Girsang (1998).

The electronic copyright issue is still under consideration within the SDLearn project.

LRP SERVER PROTECTION

The third requirement identified was to protect the LRP technology infrastructure from general unauthorised access. This relates to the threat of illegal access or interference via routes other than the normal student entry (login) point into the ODL system. Protection in this case can be achieved via appropriate use of accepted security technologies such as firewalls.

The proposed approach is based upon the concepts of packet filter and application gateway firewall technologies. A detailed description of these approaches is outside the scope of this paper and interested readers are referred to Pohlmann (1997) for further information. However, at a summary level, the two approaches can be described as follows:

- **Packet Filter**. Operates at the IP packet level and filters packets as they pass between network router interfaces. A number of packet features may provide basis for filtering, including source / destination IP addresses and source / destination port numbers. The former would be used to restrict access to specific locations, whereas the latter may be used as the basis for restricting access to specific protocols / services, e.g. HTTP, SMTP.

- **Application Gateway**. Provides a *proxy* between external systems and hosts offering services on an internal network. Users then connect to the proxy as a *gateway* to the internal network, with the result that they no longer have direct connections to internal machines. This allows more fine-grain control of connections.

With two packet filters it is possible to define a 'screened-subnetwork', which offers a high level of protection and has a nested security structure (as illustrated in figure 2). In this scenario, the first packet filter blocks everything except the services available in the 'public area' and the services from the internal network that are available to external users. The application gateway and the second packet filter have to let through only the authorised traffic between the LRP internal network and the outside world. The management of the firewall components is located within the internal network. In the SDLearn environment, servers positioned in the 'public area' will offer services like WWW and FTP that the LRP may wish to make available to remote students. These servers would, therefore, be responsible for disseminating ODL course content and the like. More sensitive data (e.g. student registration details), any student submission repositories and any content whose dissemination is restricted (e.g. formal assessments) would be held within the internal network, outside the reach of students or other unauthorised parties. Attacks on the public area servers would not endanger the internal network.

It should also be recognised that the LRP may face threats that are not directly people-related. For example, it would be important to ensure that the LRP is protected against virus attacks or other network threats such as email bombing (both of which could ultimately impact upon the service available to legitimate users). The firewall approach described can be enhanced to cope with these scenarios. This involves the use of new protocols like the Content Vector Protocol (CVP) and the Suspicious Activity Monitoring Protocol, as well as the idea of distributing firewall functionality (Check Point 1998).

CVP provides an open specification to enable the integration of external and third-party content screening software. It is able to vector file content to a different server (i.e. a scanning server) that has the ability to analyse, modify and eventually block different transmitted information. The application gateway will select and distribute the received data to the existing servers. These will scan all the data transmitted for viruses, check Java applets and ActiveX applications. The application gateway and these servers will use the above mentioned protocols (e.g. CVP) to communicate.

Through the inclusion of an approach such as that described, the LRP infrastructure would be effectively protected against hostile external influences.

CONCLUSIONS

Online Distance Learning represents a growth area in the education and training domains. Furthermore, its significance is only likely to increase as delivery technologies improve and greater societal emphasis is placed upon issues such as lifelong learning. A variety of ODL solutions have been developed

(or are under development) and, at the time of writing, no overall standard has emerged. The attention to security in these cases has been variable, with the problem being considered as a secondary issue within many prototype / first release systems. It is, however, likely to become more of a priority over time as competition builds between LRPs and it becomes a required / expected feature from the end-user perspective (which is particularly likely in the context of corporate training).

SDLearn seeks to provide recommendations and solutions at a generic level, which could then be applied in various practical implementations. It is hoped that this approach will prevent the security issues from having to be re-addressed from the bottom up in each new ODL offering. The work is currently at the stage of investigating and evaluating the individual elements of a solution, such as those described in this paper. Prototypes of partial solutions are already under development. The ultimate intention is to realise an approach in which these are integrated into an overall security framework.

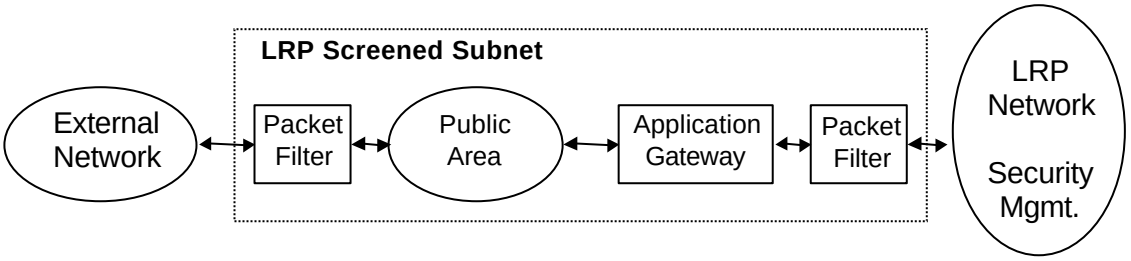

Figure 2: High Level Security Firewall System

REFERENCES

Check Point. 1998. *Open Platform for Secure Enterprise Connectivity (OPSEC) Architecture*, Check Point Software Technologies, Ltd, 1998. http://www.checkpoint.com/opsec/architect.htm

Delaigle, J.F, De Vleeschouwer, C. and Macq,B. 1996. "Digital Watermarking", in *Proceedings of the SPIE – The International Society for OPTOCA; Engineering Optical Security and Counterfeit Deterrence*: 99-110.

DEMOS. 1997. *Distance Education and tutoring in heterogeneous teleMatics envirOnmentS.* Telematics Applications for Users and Providers Project. http://www.redestb.es/personal/softbase/demosfra.htm.

Educom IMS Partnership. 1997. IMS Design Requirements. 19 December 1997. http://mic8.hensa.ac.uk/mirrors/ims-project/req.html

Furnell, S.M, Illingworth, H.M, Katsikas, S.K, Reynolds, P.L. and Sanders, P.W. 1997. "A comprehensive authentication and supervision architecture for networked multimedia systems", in *Proceedings of IFIP CMS '97* (Athens, Greece, Sept. 22-23): 227-238.

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, 1998: 236-242.

Girsang, J. 1998. *Security implications of Online Distance Learning*. M.Sc. Thesis. School of Electronic, Communication and Electrical Engineering, University of Plymouth, Plymouth, UK.

Lunt, T.F. 1990. IDES: An Intelligent System for Detecting Intruders. *Proceedings of the Symposium : Computer Security, Threat and Countermeasures* (Rome, Italy).

Nuttall, N. 1997. "University meets online challenge", *The Times*, "Interface" supplement, 19 February 1997, p11.

Pohlmann, N. 1997. *Firewall-Systems*, Thomson Publishing.

Wayner, P. 1997. *Digital Copyright Protection*. Academic Press Limited, London.

BIOGRAPHY

Dr Steven Furnell is the research co-ordinator of the Network Research Group at the University of Plymouth (UK), where he is the supervisor of seven post-graduate researchers. He holds a first class honours degree in Computing & Informatics and a PhD in data security. His current research interests include information systems security, Internet and WWW technologies and mobile systems. Key application areas in which Dr Furnell has interest are online learning, electronic commerce and healthcare telematics. He has worked on a number of international research projects, the most recent being DOLMEN (Service Machine Development for an Open Long-term Mobile and Fixed Network Environment) and ISHTAR (Implementing Secure Healthcare Telematics Applications in Europe), both under the EU fourth framework programme.