Identifying the security requirements for virtual university environments

V-C.Ruiz[1], S.M.Furnell[1], A.D.Phippen[1], P.S.Dowland[1], I.Stengel[2] and U.Bleimann[2]

[1] Network Research Group, University of Plymouth, Plymouth, United Kingdom
[2] University of Applied Sciences, Darmstadt, Germany

info@network-research-group-org

Abstract

Virtual universities (VUs) are meant to provide a new learning model for students and a way to study away from traditional facilities. Security is now regarded as a high priority within computer systems, and has been increasingly introduced to the public over the years. Many new technologies have been presented as means to secure computer systems, especially when connected on large scale networks such as the Internet. As in every IT system, virtual universities are faced with potential attacks from outside or inside its network. This paper proposes a security model for such universities, in order for the students, staff, and the administrators to work in a safe environment, and provide the same degree of confidence as in a traditional learning environment.

Keywords

Security, Online Distance Learning, E-learning, Virtual University.

1. Introduction

In recent years, national studies concerning security within organisations (among them educational organisations) have been published to the public. The Department of Trade & Industry from United Kingdom and the Computer Security Institute in the United States have both published a survey concerning security problems encountered by companies during the year 2003 (DTI, 2004; CSI, 2004).

Many aspects of these survey results show an increasing number of incidents detected by companies during the past year, compared to previous years. This increase in the number of reported incidents may be viewed either as an increased awareness about what is really happening in an organisation's network, but could also represent an actual increase in the number of incidents. Nevertheless, results regarding these surveys can explain part of what an institution such as a virtual university may be faced with when connected to the Internet.

In the Symantec Internet Threat Security Report (Symantec, 2004), educational organisations are identified as one of the primary targets for attackers. In this report, Symantec noted that the education industry is the 8th most targeted on the Internet. From another perspective, recent years have also witnessed a number of attacks being launched onto the Internet from *within* universities. Since university networks are usually composed of a high number of machines connected to the Internet by a huge amount of bandwidth, it makes them prone to host attackers (students or external hackers that gained access to a machine on the network) (Borland, 2000; Roberts, 2004).

Adding to the threats of security breaches coming from the Internet and users, virtual

universities are keeping highly sensitive information regarding its users, protected in the UK by the Data Protection Act from 1998. This information, along with copyrighted material, makes VUs highly sensitive organisations.

This paper intends to describe potential security issues that may occur in online distance learning environments such as virtual universities, and proposes a security model in the perspective of future integration in applications.

2. Security issues facing Virtual University environments

E-learning platforms (and therefore VU), rely on a client-server approach. Requirements regarding their security can be decomposed into three sub-categories: the server, the client, and the network. Issues may be addressed by implementing security measure in one or more categories.

Traditional universities secure their network from improper outside use by using the latest anti-virus software, installing firewalls, preventing unauthorised software installations, etc. They usually also establish an IT policy usage that the users must agree with, in order for them to be able to use the network (Kvavik et al, 2003). A traditional university network is a private network which can be monitored, and if a student is spotted performing an unauthorised action, their account can be revoked immediately. Virtual universities, due to their distance approach and use of large scale networks, are more complex to monitor and maintain. Depending on the user's rights and actions on the server, issues may vary.

2.1 Authentication, authorisation

Authentication is a mechanism whose goal is that only registered and legitimate users get access to the system. In VUs, authentication is a crucial part of the security processes as it is used to grant access to sensitive material.

Once the authentication has been established successfully, authorisation of access to certain parts of the server may be granted.

2.2 Confidentiality

Confidentiality within a university is not only a requirement for the university itself but also for the students. Indeed, communications between students and instructors are confidential, and therefore should not be spied on.

In terms of data confidentiality, the virtual university stores different information regarding the users; students' grades are required to be kept secret, personal information about each individual must not be released on the Internet.

2.3 Copyright

Every piece of material on the server (e.g. instructors' lecture notes, books in the library, research paper, etc.) is copyrighted. Each individual who writes a paper would rather not see their work published under another name somewhere else in the world.

2.4 Other issues

Depending on its implementation, virtual universities may be faced with other issues. There are various ways to set up an online distance learning platform, one of the most common is by using a traditional web server (WebCT, Archimed Campus Virtuel, etc.). This approach has the advantage of being easy to set up, but lacks flexibility for implementing the best technologies available. Additionally it has the disadvantage of the incompatibility of different web browsers, and is prone to the different security bugs and vulnerabilities that they may contain.

The second approach to creating an e-learning platform is by creating custom software (Wang, 2001). This approach requires the users to have the software installed on the computer from which they want to access the university. This latter approach therefore decreases the flexibility regarding mobility. Bespoke software developed in-house may also be prone to cracking from badly intentioned users if it has not been exposed to sufficient prior testing.

3. Security model and available technologies

In order for the VU to address and resolve issues it is faced with, a security model needs to be implemented. Various technologies can be used to fulfil the goal of securing the university, and some of the principal aspects are discussed in this section.

3.1 Server

The server is one of the most important parts of the virtual university. VUs usually use a web server which provides services to the user (Dean, 2002). It must therefore be able to handle at least authentication, integrity and privacy.

The virtual university may rely on multiple servers (for example one for each service or for balancing the users to one another in order to increase the availability), which need to be administrated. A set of multiple servers is harder to maintain, but generally provide better availability. In this scenario, the whole server cluster needs to be secured, on software as well as on a physical basis.

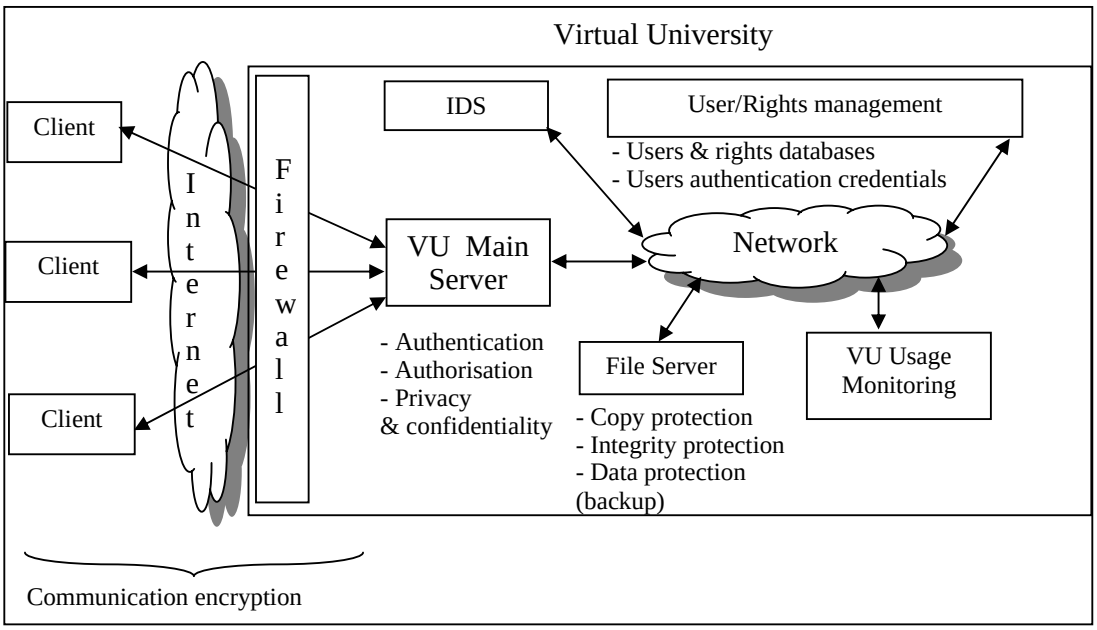

Figure 1: Architectural diagram of a VU implementing the security model

Figure 1 shows how a virtual university can apply some protection measures, as part of the security model presented below.

3.2 Access control

3.2.1 User Authentication

One of the primary goals of the server is to be able to authenticate and identify the users reliably. Since the virtual university contains sensitive information, regarding the users as well as the taught material, this authentication process must be as thorough as possible and provide certainty concerning the users attempting to log in.

Three main types of user can be defined in a virtual university: the students, the instructors and the administrators. Since each one of these users have different rights within the university, their authentication method should be set accordingly. As an example, students could be required to only provide a user name and password combination (restriction may be applied on the chosen password length, form, etc.). A secure password authentication scheme should be preferred for this scenario (Lin, C-L. et al, 2003). Instructors would use a token, provided to them by the university, to answer a challenge from the server (Federal Financial Institutions Examination Council, 2001). Finally, the administrators would have to use a combination of digital signature (using public/private key pairs delivered to them by the university) and challenge-response authentication to prove their identity. A single sign on (SSO) approach is desirable since different services are used in a virtual university.

When someone connects to a server on the Internet, it should be sure that it is not connecting to an impostor. For this reason, the server should send a digital certificate (validated by a certificate authority) to its connecting clients, proving its identity.

3.2.2 User management

In order to authenticate each user, a user management policy must be put in place. An easy way to add, change, and revoke users from the system must be introduced. This user management system is a critical part of the virtual university functionality and should only be accessed by individuals having the right to do so, i.e. the university administrators. The implementation of the user management should support directory services such as LDAP.

3.2.3 Rights management

Part of the user management system may be used for rights management. In a virtual university, three different types of individual have been defined. Each type of users can be given a set of rights to different parts of the university.

Students, who can be considered as the end-users, may be able to read the material given for their lectures, post and read messages on forums, manage a calendar, access a virtual library and send or receive emails. They must not be able to change in any way the configuration of any part of the virtual university, except regarding their personal preferences.

Instructors are given more rights than students. Since they provide the knowledge, they should be able to post new material, change their lecture content, retrieve students' work, mark them, manage a students list and their marks, post new quizzes and exams.

Administrators are power users regarding the VU. They can be divided into many different categories, such as technical, program, accounting administrators, etc. Each one of these sub-categories may change one aspect of the university's configuration, and may access the university's sensitive data.

3.2.4 Usage monitoring

Universities usually put in place usage policies concerning their computer systems and networks. This kind of policy must also be put in place in a virtual university to prevent unauthorised actions within the university's computer system. On servers, every user's actions should be monitored and recorded. For extra protection, a dedicated server can be put in place for the purpose of collecting and storing logged data.

3.3 Protection from external threats

Virtual universities using the Internet as a communication medium should be especially careful regarding the data coming into the servers. Users, without knowing it, could easily bring down the network or server and stop the university from functioning correctly.

3.3.1 Malware protection

Viruses and worms are the most common threats for online servers (CSI, 2004; DTI, 2004; Symantec, 2004). Whereas viruses usually arrive through emails, worms propagate from one server to another by exploiting flaws in different services. The most effective method to protect the servers would be to put anti virus software in place to scan every document arriving on the server (via email, or directly uploaded).

3.3.2 Firewall protection

To be protected against attacks, firewalls have proven to be very useful. The VU servers must integrate one as a basic security measure.

3.3.3 Intrusion detection system

An Intrusion Detection System (IDS) is a tool used to detect attempted of attacks or intrusions. Such a tool can detect incoming viruses, worms, etc. on a system. They can use heuristics in order to be able to detect unknown malware. Using such a tool would help the administrators detecting hostile activity within the university's network and react accordingly.

3.4 Data protection and storage

A sensitive part concerning virtual universities is related to data storage. Data is a broad term but in organisations such as VUs, everything should be considered as sensitive information.

Different types of data may be considered in a virtual university. Depending on the user, different information is kept by the university. Whereas the university keeps records of its students' performances (e.g. grades over the years), their payments, etc., it also keeps other information regarding the instructors and administrators, such as their salary, their taught courses, etc. All this information needs to be stored in a secure place and be made inaccessible from unauthorised users. For this reason, each item of sensitive information must be kept in a dedicated format (e.g. passwords should be kept encrypted) and in a dedicated space.

In order for the VU to face every possible event, this information needs to be backed up regularly, by using specific features of each storage and operating system the server uses (e.g RAID). Sensitive data should be evaluated to get the best available technology for protecting and storing them.

3.5 Services management

Virtual universities provide services to the students, such as email, chat, calendar, etc. These services may depend on the users that are using it and therefore need a services management policy.

3.6 Communications confidentiality

On the Internet, communications can be eavesdropped by badly intentioned people, providing them with sensitive information they could use wrongly. The only way to prevent this kind of attack is to encrypt data passed on the network between the server and its clients, therefore preventing anyone who is not part of client-server "conversation" to understand what is being said. SSL/TLS protocols have been developed for that purpose.

3.7 Document Copyrights & Integrity

Even if outside intruders can be stopped from getting sensitive data passed between the different parties, users who have access to the provided material can still make inappropriate use of it. Lecturers notes, virtual libraries books, research papers, and magazines are required

to include either copy protection mechanisms or copyright notes (visible or invisible). Depending on the type of document (images, videos, text, etc.), different measures may be applied. Whereas text can use software specific features (e.g. Adobe Acrobat PDF protections) as well as electronic marking techniques (Brassil et al, 1995), images and videos can be marked by watermarking or steganography. These two technologies hide information invisible to the naked eye, but can help to trace wrong uses.

Ensuring that documents have not been tampered with should be an added feature to the environment. Lecturer's notes, as well as students' homework uploaded to the server are documents that require an integrity check. When uploading a file, the users should be required to provide a signature concerning the file (e.g. using a program to sign the resulting data with a private key) (Van Vlerken, 2000). This process could be automated, and students or lecturers would be sure that what they are reading is the original handed-in work.

3.8 Server upgrades/updates

To guarantee that the server does not have outdated software which could have security flaws, the technical administrators have to be very careful about announcements made by their software providers. Depending on their budget, and the expected services from the manufacturer, organisations have a lot of different software to choose from. The choice of software to use should be considered thoroughly in terms of services and support associated to it.

4. Summary of requirements

As previously indicated, each user is assigned a set of actions that can be performed on the platform. As a result, each action introduces associated security issues, as summarised in Table 1. For example, when a student hands in a coursework, the instructor marking it should be sure that it is the original one, and that it was genuinely uploaded by the student. The student would also rather not let anybody else see his work and copy it. As a result, the main issues concerning this particular action are copyright, privacy, integrity and non-repudiation.

Action by the user	Security Issue	Protection
Log in (all users)	Authentication & Authorisation	Strong authentication depending on the user. Must be immune to known attacks from outside hackers
Lectures study (students)	Authorisation Copyright	Rights management Copyright protection
Online Exam (students)	Authorisation Privacy Non repudiation	Rights management Monitoring
Online exams marking (instructors)	Privacy Authorisation	Rights management
Hand-in Work (students)	Copyright Privacy Integrity Non-repudiation	Copyright protection Document integrity measures
Coursework retrieval & marking (instructors)	Authorisation Integrity Non-repudiation	Rights management Document integrity measures
Communication (e-mail, chat) (all users)	Malware Privacy Integrity	Anti-virus/Firewall/IDS Communication encryptions and integrity protection measures
Virtual Library access (all users)	Authorisation Copyright	Rights management Copyright protection
Modify lecture & add new material, exam, quizzes(instructors)	Authorisation Copyright	Rights management Copyright protection

Table 1: Usage of the security model depending on the users' actions

5. Conclusions

In computer systems, there is a trade-off between security and ease of use and access to information by the users. Most users are used to passwords and PINs as a mean to authenticate, thus making other available technologies harder to be accepted (Furnell et al, 2004). Nevertheless, in order for the users to trust a VU as much as a traditional university, changes in peoples mind will have to occur.

This paper has proposed a general security model for the learning environment of a virtual university. Although the technological aspects may well become dated or prove ineffective in the future years, the model itself should remain a useful reference for future virtual universities.

Future work on the subject would require a thorough assessment of feasibility and test user acceptance within an actual virtual university. This model relies mostly upon operations done by the server, and therefore performances issues should be looked into; the security model should not undermine the learners experience because of losing time online. The financial aspects for implementing the proposed protection measures should also be a concern.

6. Acknowledgement

This paper has been produced as a result of the authors' involvement in the Security Technology in a Virtual University (Virtusec) project, with funding support from the British Council and the German Academic Exchange Service (DAAD) under the Academic Research Collaboration (ARC) programme.

7. References

Borland, J. (2000), "Universities likely to remain Net security risks", *CNET News.com*, February 2000. Available: http://news.com.com/2100-1023-236933.html.

Brassil, J. T, Low, S, Maxemchuk, N. F. and O'Gorman, L. (1995), "Electronic Marking and Identification Techniques to Discourage Document Copying", *IEEE Journal on Selected Areas in Communications*, Vol. 13, No. 8.

CSI (2004), "2004 CSI/FBI Computer Crime and Security Survey". Available: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf.

Dean, C (2002), "Technology Based Training & On-line Learning – An overview of authoring systems and learning management systems available in the UK", December 2002. Available: http://www.baol.co.uk/PDF/authsys.pdf.

DTI (2004), *Information Security Breaches Survey 2004*. Department of Trade & Industry, April 2004. URN 04/617.

Federal Financial Institutions Examination Council (2001), "Authentication in an Electronic Banking Environment", August 2001. Online: http://www.ffiec.gov/pdf/pr080801.pdf.

Furnell, S.M, Papadopoulos, I. and Dowland P. (2004), "A long-term trial of alternative user authentication technologies", *IMCS – Information Management & Computer Security*, Vol. 12, No. 2, pp178-190.

Kvavik, R. and Voloudakis, J. (2003), "Information technology security: governance, strategy, and practice in higher education", ECAR – Educause Center for Applied Research, October. 2003.

Lin, C-L. and Hwang, T. (2003), "A password authentication scheme with secure password updating", *Computers & Security*, Vol 22, No 1, pp. 68-72.

Roberts, P. (2004), "Attacks at Universities raise security concerns", *Infoworld*, April 2004. Available: http://www.infoworld.com/article/04/04/14/HNuniattacks_1.html.

Symantec. (2004), Symantec Internet Security Threat Report, Volume V, March 2004.

Van Vlerken, P. (2000), "Message Authentication, Integrity, and Non-repudiation from Paper to PKI". Available: http://www.imforumgi.gc.ca/new_docs/authentic_e.pdf.

Wang, Y. (2001), "Security framework for Online Distance Learning", *Master's thesis*, University of Plymouth, Plymouth, UK.