APPROACHES TO THE TEACHING OF INFORMATION SECURITY

Ileana Hamburg[1]/Oleg Cernian[2]/Dan Mancas[2]/Adina Basandica[3]

[1]Institut Arbeit und Technik Gelsenkirchen, [2]University of Craiova, [3]High School "G. Bibescu" Craiova

Abstract: Information system security teaching is very complex because of the wide range of domains involved: computer architecture, criminology/law, cryptography, database, human-computer interaction, information retrieval, information theory, management/business, mathematics, military science, mobile computing, networks, operating systems, philosophy/ethics, programming languages, software engineering, statistics/probability, and web programming. This paper synthesizes previous and existing approaches on teaching information system security (Section 2) and gives some examples of such approaches developed within the European Project "ViReC e-Initiative" – University Virtual Resource Centre based on a DLE (Distributed Learning Environment) (Section3), developed in the framework of MINERVA Scheme funded by the European Commission.

Keywords: e-Learning, Internet, network security, tutorials, virtual laboratories, e-Training, European project.

1. INTRODUCTION

It is known that the development and widespreading of the Internet and other communications media required more information system security professionals. In this context, in (Bishop, 1993) there are explained the standviews acting in this field and requirements of major players.

Universities need educators who can communicate underlying theory to students in order to have them prepared to apply design principles to security mechanisms.

Companies need immediate support in protecting their investments in people, products, equipment. Government needs professionals to design tools to protect national economic and defense infrastructures from cyber terrorists (Yurcik, 2000).

The present situation in the companies is difficult and cumbersome. To help fend off spam and viruses, identity theft and corporate sabotage, IT managers need to train company employees to protect themselves and the corporate network. But, constant budget cuts and staff shortages are making it difficult for IT managers to focus on anything beyond putting out daily fires and staying current with software updates, patches and security alerts.

In a recent survey it was estimated that 90 percent of IT managers did not provide any employee training on how to manage spam and junk mail; this important conclusion was mentioned in a report of SurfControl Plc, a Web and email filtering company based in Scotts Valley, Calif. (Gaudin, 2003).

"It's not just up to the IT people to keep the network secure anymore," comments Susan Larson, vice president of global product content at SurfControl company. "If employees don't understand how they can help, they become part of the problem," added Larson (Gaudin, 2003). "Employees are ultimately critical. It's not just 'my mailbox'. Multiply that by 10,000 users. Obviously, they shouldn't be answering spam. They shouldn't be using Outlook's Preview page because that sends tracking information back. There's a lot to it", considered Larson (SurfControl)

Tony Magallanez, a systems engineer at F-Secure, Inc., a data security and anti-virus company (Gaudin, 2003), appreciates that training can't be a one-time proposition. He says that security awareness needs to be part of new employee orientation and that training sessions for all employees should be held periodically. Furthermore, email alerts to end users, keeping them updated about the threat of new viruses, spam tactics and hoaxes, are, strongly recommended.

One solution to face such critical requirements is to propose information system security approaches based on previous work and "best practices" of teaching information system security both for

Universities and for companies. Virtual learning environments offer flexible means to such approaches being independent of time and place. It is known that through the development of virtual learning environments, particularly Web-based ones, the potential of the Internet and other media can be better used to support teaching and learning having the learner as focus.

Information system security teaching is very complex and cumbersome because of the wide range of domains involved: computer architecture, criminology/law, cryptography, database, human-computer interaction, information retrieval, information theory, management/business, mathematics, military science, mobile computing, networks, operating systems, philosophy/ethics, programming languages, software engineering, statistics/probability, and web programming (Spafford, 1998).

This paper synthesizes past and current approaches on teaching information system security (Section 2) and gives some examples of such approaches developed within the European Project "ViReC e-Initiative" in the framework of the European programme MINERVA.

2. PREVIOUS AND EXISTING APPROACHES

Many authors like Neugent (1982), Highland (1982), Higgins (1989), Spillman (1992), Arsenault and White (1991), justify the need for the teaching of information system security and describe course specifications, including instructional materials, like textbooks, laboratory works, individual study guides etc. The courses proposed so far were survey courses or introductory courses, which provided only orientation and guidelines in the field, but not the technical in depth approaches, thorough, needed for professional specialization.

Higher level approaches have been developed by Cook (1985) and later by, Irvine *et al. (*1998). They underlined that information system security should be integrated into the entire curriculum. In fact, Bishop states, "Computer Security is not merely a technical subject, but requires a broad knowledge of the practice of engineering and organization, psychology, history, philosophy/ethics, and other humanistic fields."

Irvine *et al.* (1998) showed that, ideally, textbooks, course materials, and hands-on laboratory exercises should have information security subject integrated into appropriate topics across the entire curriculum rather than being treated separately.

The traditional lecturing (passive) approach dominates the current teaching of information system security. Bishop (1993) underlay some of the basic types within traditional lecture: a survey breadth course, a cryptography course focused on mathematical foundations; and a systems course translating theory into real systems.

Students use this material in different learning styles and, from examples, students can chose their adjust as well own pace (repeating the examples covered in class).

Teachers report that students are attracted in such form of courses, more in analyzing computer programs devised for problems than on theoretical topics. Therefore at this level, informal explanations dominate over formal mathematical proofs and the students like running examples of computer applications security.

One critical point is that within traditional lecture approaches students may become too passive and not actively attempt to understand difficult material.

Another form of teaching is tutorial. There are many definitions of tutorials.

We use the tutorial approach as a "step by step" teaching and explanation, based on examples to be utilized also as self-learning by people who would like to learn and get experience quickly in a specific domain.

The goal of these approaches is often certification in different specialties. The certified information systems security professional (CISSP) is the most respected in the field of computer/network security and many resources related to the test are available online.

Tutorial essays on most security topics can be found on the www by using a search engine. Obtaining original information from leading experts is often worth the hassle and delay factor compared to misinformation from potentially untrusted sources.

In many universities it is used the Research/Teaching Approach. It is important for students to remain attuned to information system security research so that they would be able to incorporate the latest techniques into their future products and processes. While it is the goal of most university-level educational programs to benefit from the synergy of research and teaching, in the area of information systems education this is difficult due to the level of complexity in specialized security research. Lindskog *et al.* (1999) related about a course that incorporates both research and education on three different types of laboratory research projects: intrusion experiments, intrusion analysis and remediation, and intrusion detection.

Empirical surveys ascertained that students were motivated by this research connection to learning approach.

Another approach corresponds to Laboratory methodology.

Traditionally, the laboratory has been an integral component of engineering education for relating fundamental concepts to basic real-world phenomena (Gaudin, 2003). Conducted largely within the confines of the lecture-classroom format, the laboratory involves the use of largely pre-determined or recipe-like experiments that simulate basic phenomena found in real-world situations. Unfortunately, the lecture-classroom-laboratory system has its flaws or demanding requirements: time-space dislocations of what is taught, what is explained and learned, and what is practised and internalised, as well as the need for large amounts of space and complicated logistics to create and maintain an appropriate learning environment.

A real network security laboratory requires specific requirements: (1) all components of the laboratory connected to a single router; (2) the router's gateway is through a proxy firewall server. Students can access the laboratory remotely only by logging into the firewall. There is a problem with this approach in that significant resources are required to build and maintain an isolated network security laboratory with a mix of operating systems at different levels of security.

Virtual laboratories seem to be preferable to real laboratories due to some reasons like:

- The learning procedure through real laboratories puts students' life in jeopardy.
- Some experiments cannot be performed due to time constraints or hazards.
- The cost to set up or to preserve/maintain a real laboratory is prohibitive.
- There are experiments that can be simulated only in computers.

Among the benefits of virtual laboratories, the following are particularly important:

- Resource sharing becomes a reality, improving the utilization of costly equipment.
- Access to educational and research materials is facilitated for both students and professionals.
- Scientific investigation standards are established in areas where practical experimentation is a required part of research.
- Reduction in travel time leads to productivity enhancements.

In addition, the virtual laboratory has the potential to be an e-Learning and e-Training hosting infrastructure that can align with the needs and practice of curricula programmes and industrial attachment scenarios. In order to be efficient, the necessary architecture and key details that will allow developing the virtual laboratory as a computer environment that can support different kinds of experiments and analytical requirements over the Internet have to be found. The aim is to make the virtual laboratory a reasonably extensible and reusable platform that can be used collaboratively by large groups of students through a distance-learning format, thereby overcoming several weaknesses of the conventional laboratory-based educational system.

3. EXAMPLES

Our example refers to the project ”ViReC e-Initiative” – University Virtual Resource Centre based on a DLE (Distributed Learning Environment) – which represents an European dimension attempt for applying collaborative distance learning environments in higher education institutions. The project was financed by European Commission within Socrates-Minerva programme. The partnership incorporates several universities and research institutions from four countries: Romania, Germany, Ireland and Greece. The major background for this application is represented by an initial experience approached by one of the partners – Fachhochschule Regensburg – consisting in setting up the Bavarian Virtual University, where an important contribution belongs to the teaching staff from the University of Craiova (Romania).

The benefits of the Distributed Learning Environment (fig.1) consist of:

- project-based learning in an information-rich, tool-rich environment;
- collaborative learning when communication can be synchronous and asynchronous;
- learning in places and at times of students' choosing;
- learning marked by continuous improvement of a piece of work;
- improved student-faculty and student-student interaction, including an enhanced feedback.

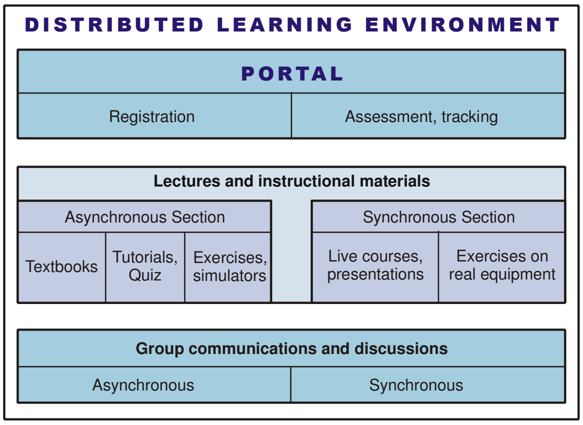

DISTRIBUTED LEARNING ENVIRONMENT
PORTAL
Registration
Assessment, tracking
Lectures and instructional materials
Asynchronous Section
Synchronous Section
Textbooks
Tutorials, Quiz
Exercises, simulators
Live courses, presentations
Exercises on real equipment
Group communications and discussions
Asynchronous
Synchronous

Fig.1 Distributed Learning Environment

The main goal had in view during the development of the distributed learning environment was to obtain the following advantages:

Student-centered, collaborative learning environment. Many of the distributed learning models implemented on the WWW emphasize a student-centered environment and encourage greater collaboration among students. Emphasis is placed on interactive problem-solving; the teacher is not just an expert, but increasingly takes the role of the facilitator.

Convenience. Teaching and learning are not confined by space or time. Students and faculty can access the virtual classroom from their home or office. This is increasingly important to many institutions interested in drawing non-traditional students into their programs.

Ease of use. WWW navigation software (such as Netscape Navigator or Mosaic) nicely integrates access to all types of Internet resources in one easy-to-use interface. Both faculty and students can quickly and easily learn to use this software to navigate the Web, access course materials, post homework assignments, and communicate with colleagues.

Development is relatively quick and easy. Developing instructional materials for the WWW is surprisingly easy and can be done relatively quickly. The skill level of faculty who are using the WWW for instruction ranges from novice to sophisticated. Many faculties create their own very sophisticated WWW pages using HTML, the HyperText Markup Language, that underlies WWW hypertext programming and linking. At some institutions, programmers develop the basic design of a system, and faculty need only have basic e-mail and WWW navigation skills to enter assignments and communicate with students.

Resources are readily available. The profusion of readily available source materials on the WWW is ideal for education and research. The true beauty of the WWW lies in the ease with which one can create a hyperlink to existing information, allowing to take advantage of the expertise and creativity of others without having to "reinvent the wheel." In addition, "human resources" are often readily accessible on the Internet -- allowing to enhance the virtual classroom with the introduction of guest speakers and content experts into chat areas or discussion groups.

Updating and disseminating information is easy. Unlike printed resources, once materials have been posted to the WWW, information is easily updated and disseminated. The convenience and cost advantages of publishing information in this digital format should be obvious.

Easy standardized access. The software for accessing the Internet is easily obtained either by downloading directly from the Internet or by shopping in computer stores and bookstores. This easy access allows distance learners to readily access course materials from their home or office computer. And because the Internet is based on standard communications protocols, the students accessing the Internet in Craiova will be able to access the same resources as the students in Duisburg, Regensburg and Limerick.

Among several remarkable foreseen outputs, the creation of virtual laboratories (fig.2) crossed with some real equipment, represents a challenging achievement.

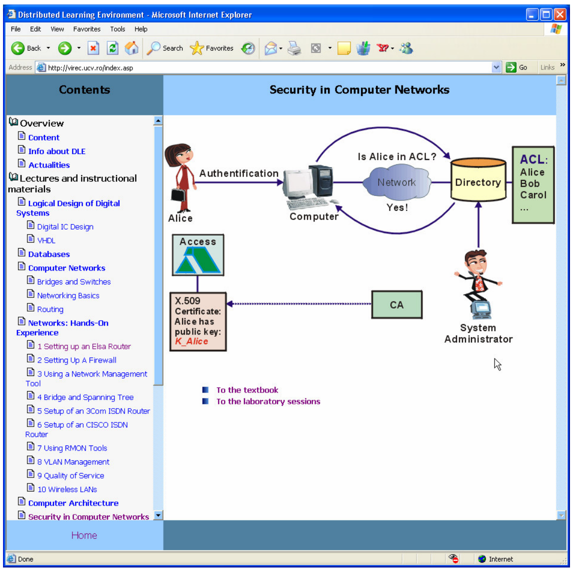
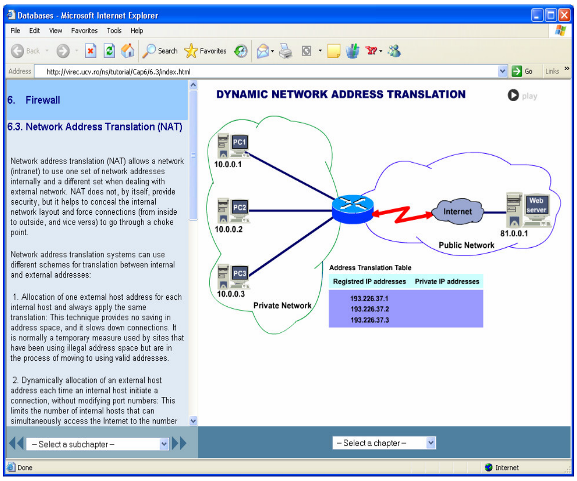


Fig.2 Example of virtual laboratories

The partners were involved in individual developments concerned with some envisaged outputs planned as tutorials and exercises for remote labs in the fields of Network Security, Network Management, Computer Architecture and Database Systems.

The tutorial on network security covers security technologies that can apply to the computer networks. Students have to learn how to protect their application exposed to the Internet, most common ways to attack a web site and the appropriate countermeasures. A methodology to design and realize secure network services is also presented. Privacy, e-commerce, hardening, intrusion detection and cryptography are covered to give a global overview to the students of the risks of having a network connection and the techniques to defend it. Security and privacy implications of new generation of Web platforms and XML based web services are analyzed and discussed. The tutorial benefits of a high quality implementation based on multimedia technology and a flexible navigation system (fig.3).

The main goal of the "Network Security" laboratories is to acknowledge users about network security risks as well as to provide them a reliable set of solutions to avoid these risks. The platform on which the portal is developed is a Linux platform. Linux was chosen because it is a robust secure operating system with respect to attack risks and threats over the Internet.



6. Firewall

6.3. Network Address Translation (NAT)

Network address translation (NAT) allows a network (intranet) to use one set of network addresses internally and a different set when dealing with external network. NAT does not, by itself, provide security, but it helps to conceal the internal network layout and force connections (from inside to outside, and vice versa) to go through a choke point.

Network address translation systems can use different schemes for translation between internal and external addresses:

1. Allocation of one external host address for each internal host and always apply the same translation: This technique provides no saving in address space, and it slows down connections. It is normally a temporary measure used by sites that have been using illegal address space but are in the process of moving to using valid addresses.

2. Dynamically allocation of an external host address each time an internal host initiate a connection, without modifying port numbers: This limits the number of internal hosts that can simultaneously access the Internet to the number

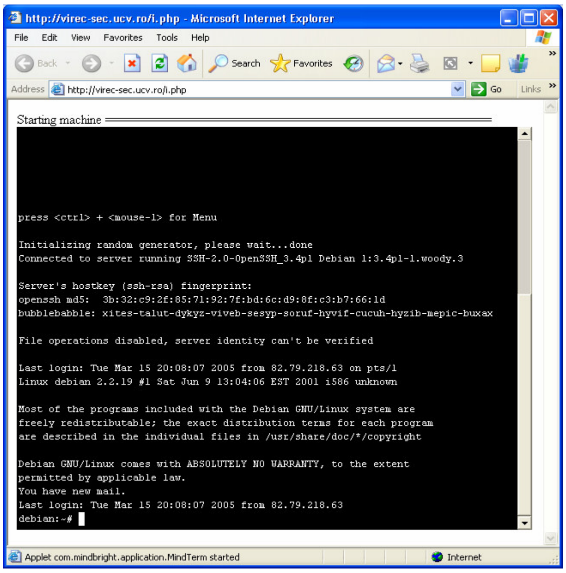
DYNAMIC NETWORK ADDRESS TRANSLATION

Address Translation Table

Registred IP addresses	Private IP addresses
193.226.37.1	
193.226.37.2	
193.226.37.3	

Fig.3 Tutorial page of network security

The application uses Java Servlets technology. This Java server side oriented technology is open source and platform independent offering up-to-date support from on-line community. The technology fits best to the Model-View-Control standard, offering distinct separation between presentation and content. The Web server Tomcat from Apache was used; as it is known Tomcat is the proper solution that implements Servlets technology as it can deal with large amount of client requests without speed or performance penalties. Tomcat Web server belongs also to the open source community offering on-line up-to-date support.


http://virec-sec.ucv.ro/i.php - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://virec-sec.ucv.ro/i.php
Go
Links
Starting machine
Applet com.mindbright.application.MindTerm started
Internet

```
press <ctrl> + <mouse-1> for Menu

Initializing random generator, please wait...done
Connected to server running SSH-2.0-OpenSSH_3.4p1 Debian 1:3.4p1-1.woody.3

Server's hostkey (ssh-rsa) fingerprint:
openssh md5:  3b:32:c9:2f:85:71:92:7f:bd:6c:d9:8f:c3:b7:66:1d
bubblebabble: xites-talut-dykyz-viveb-sesyp-soruf-hyvif-cucuh-hyzib-mepic-buxax

File operations disabled, server identity can't be verified

Last login: Tue Mar 15 20:08:07 2005 from 82.79.218.63 on pts/1
Linux debian 2.2.19 #1 Sat Jun 9 13:04:06 EST 2001 i586 unknown

Most of the programs included with the Debian GNU/Linux system are
freely redistributable; the exact distribution terms for each program
are described in the individual files in /usr/share/doc/*/copyright

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Tue Mar 15 20:08:07 2005 from 82.79.218.63
debian:~# █
```

Fig.4 Remote connection to a virtual computer using SSH console

We used virtual machines as a proper solution for simulating network threats and attacks. A Web interface provides each user of the application with a SSH (**s**ecure **sh**ell) console corresponding to a virtual machine (fig.4). Each virtual machine is designed with vulnerabilities to network attacks or services that are not configured (e.g. Apache server without authentication) and the user should discover and treat these vulnerabilities or configure the services.

REFERENCES

Arsenault, A, White,G, (1991). Teaching Computer Systems Security in an Undergraduate Computer Science Curriculum. *Fourteenth National Computer Security Conference*, pp. 582-597.

Bishop, M. (1993), Teaching Computer Security. *Ninth IFIP Intl. Symposium on Computer Security (IFIP SEC)*, pp. 43-52.

Cook, J. M. (1985), Increasing Students' Security Awareness: Article 1. *ACM Technical Symposium on Computer Science Education (SIGCSE)*, pp. 155-165.

Gaudin, S. (2003). Teaching Employees New Security Tricks <http://itmanagement.earthweb.com/secu/print.php/2235341> [06/08/2005]

Higgins, J. (1989), Information Security as a Topic in Undergraduate Education of Computer Scientists. *Twelfth National Computer Security Conference*, pp. 553-557.

Highland, H. (1982). A College Course in Cryptography and Computer Security. *Security and Audit Control Review*, **Vol. 1**, No. 2, pp. 34-37.

Irvine, C. E., Chin, S-K. and Frinke, D. (1998). Integrating Security into the Curriculum, *IEEE Computer*, pp. 25-30.

Lindskog, S., Lindqvist, U. and Jonsson, E. (1999). IT Security Research and Education in Synergy, *First World Conference on Information Security Education (WISE1)*, Stockholm Sweden.

Neugent, W. (Bill) (1982). A University Course in Computer Security. *Security Audit and Control Review*, **Vol. 1**, No. 2, pp. 17-33.

Spafford, E. F. (1998). Teaching the Big Picture of InfoSec. *2nd National Colloquium for Information System Security Education*, James Madison University.

Spillman, R. (1992) A Computer Security Course in the Undergraduate Computer Science Curriculum. *Collegiate Microcomputer*, **Vol. 10**, pp. 91-96.

Yurcik, W., Doss, D. (2000). Information Security Educational Initiatives to Protect E-Commerce and Critical National Infrastructures. *Information Systems Education Conference (ISECON)*, Philadelphia, PA.