Teaching Network Security in a Virtual Learning Environment

Laura Bergström, Kaj J. Grahn, Krister Karlström, Göran Pulkkis, and Peik Åström
Arcada Polytechnic, Espoo, Finland

laura.bergstrom@arcada.fi kaj.grahn@arcada.fi
krister.karlstrom@arcada.fi
goran.pulkkis@arcada.fi peik.astrom@arcada.fi

Executive Summary

This article presents a virtual course with the topic network security. The course has been produced by Arcada Polytechnic as a part of the production team Computer Networks, Telecommunication and Telecommunication Systems in the Finnish Virtual Polytechnic.

The article begins with an introduction to the evolution of the information security requirements, the different areas and uses for cryptography and to the need of an active network security administration.

The structure of the Finnish educational system is presented together with the strategy, goals and structure of the Finnish Virtual Polytechnic. The course development process is described in detail together with the software tools used to produce the course material.

The contents in each chapter of the virtual course are also presented in this article. The seven course chapters are: Introduction, Network Security Administration, Antivirus Protection, Firewalls, Cryptography and Network Security, Network Security Software and Security of Wireless and Mobile Networks. All animations and exercises are described in their context.

The didactical approach of the virtual course is a guided excursion to which students enroll. The task sets, consisting of exercises and study directives, that the course teacher assigns each week to the students are introduced and explained in detail. The concept of step-by-step skill assimilation, which lies behind the student guidance process, is outlined together with descriptions of the different user skill levels.

The background to the graphical design of the learning platform is illustrated and motivated. Both the communicating dimension, *the interface*, and the esthetical dimension, *the layout*, of the course graphical design are explained and analyzed in depth.

The IT infrastructure needed to implement and use the learning platform of the course is described and assessed. Issues like how the students are registered and authenticated to the course are presented together with the tools for communication and interaction between student and teacher. General IT requirements together with

The original version of this paper was published as one of the 24 “best” papers in the proceedings of the 2003 Informing Science and IT Education Conference in Pori, Finland http://2003.insite.nu

specific both server (course provider) and client (student) side IT requirements are presented.

Teaching and learning experiences, gathered from assessment forms and interviews, are presented. General experiences and experiences from doing and supervising exercises during a test course held in spring 2003 are presented both from student and teacher perspective. Changes made on the course contents after the test course are presented together with planned future development of the course.

Production of a virtual course has proved to be a demanding task where experts, like graphical designers, have to be included in the production team. Important issues in producing a virtual course are the proper choice of computer software and IT technology and a sufficient and realistic budget.

Introduction

The requirements of information security have undergone three major changes in the last decades. The first major change was the introduction of the computer. The need for protecting files and information became evident. Collection of tools and procedures designed to protect data and to control access to computing resources has the generic name *computer security*. The second major change was the introduction of distributed systems, networks, and facilities for data communication. *Network security* measures are needed

to protect data during transmission and storage

to control access to networks and network nodes.

The third change is the current, rapid development of wireless networks and mobile communications. *Wireless security* is therefore of high priority today.

Network security implies restrictions such as

network traffic filtering with firewall technology

defense against distribution of malicious programs like viruses

prevention, detection and management of intrusion

prevention of unwanted data communication like email spamming.

Cryptography is needed for

reliable authentication

integrity of information content

confidentiality

nonrepudiation

in data processing, in data communication, and in the storing of data (Stallings, 2002). ***Reliable authentication*** means that network resource users and communication partners can be unambiguously identified. ***Integrity of information content*** requires reliable methods to check that transmitted and stored information remains unchanged. ***Confidentiality*** means that the originator of information can determine who has (have) the right to read the information content. ***Nonrepudiation*** means that the authenticated information exchange can afterwards be unambiguously proved to have happened. Nonrepudiation is achieved by attaching to information records cryptographic digital signatures, which can be verified at any future moment of time. The importance of cryptography and the number of application areas are steadily growing.

Network security requires active administration. Security policies, standards and administrative procedures must be worked out, implemented and followed up.

Network security skills are thus needed by practically any user of a computer connected to a network. Presently there is a growing demand for network security professionals for

security administration of data and IT infrastructures

development of network security technology and methodology

delivery of support and training to network user in security related issues.

A virtual, survey oriented Network Security course, available to students of all polytechnics in a country, encourages individual polytechnics to concentrate their educational resources on highly needed, specialized, and also custom designed network security education.

Course Development

The Finnish Virtual Polytechnic

The Finnish educational system in a nutshell is illustrated in Figure 1. Compulsory basic education at comprehensive schools is given to all children between the ages of 7 and 16. Education is voluntary after completing the comprehensive school. Students may go to upper secondary school providing three years of general education, or to vocational education lasting from two to five years. Both of these give a general qualification for polytechnic and university studies ("The Finnish educational system," 2002), see Figure 1.

The action plan of the Ministry of Education in Finland for years 2000 – 2004 includes Virtual School, Virtual Polytechnic and Virtual University. Briefly the strategy and goals for the Finnish

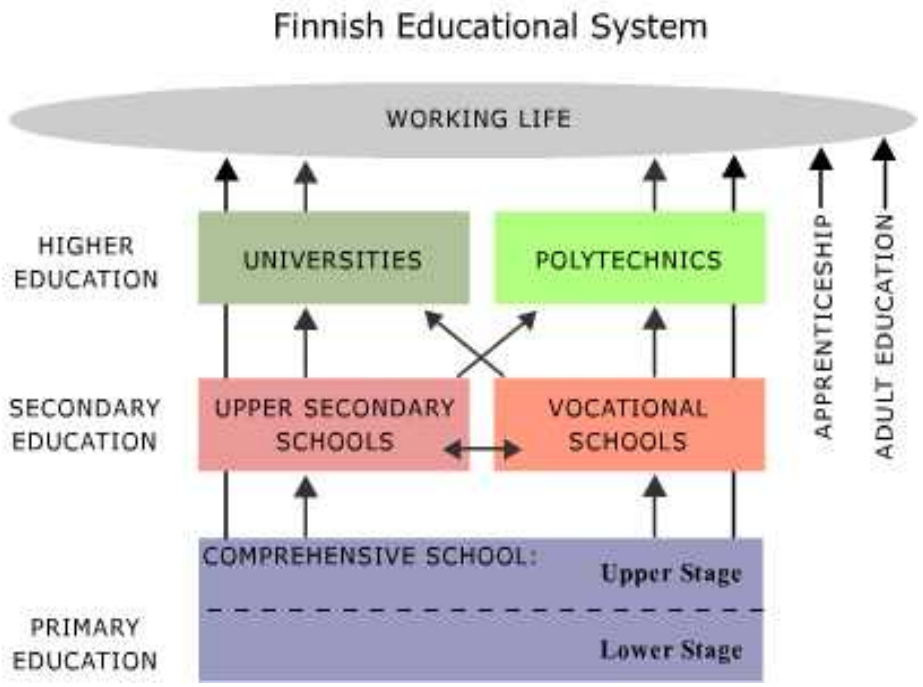

Figure 1. The Finnish educational system

Virtual Polytechnic are: (The Virtual Polytechnic of Finland, 2002):

The Finnish Virtual Polytechnic is common for all Finnish Polytechnics

It produces and provides high level learning services

The Finnish Virtual Polytechnic uses modern information and communication technology

The Finnish Virtual Polytechnic uses modern pedagogical solutions in networks

Increase co-operation between polytechnics and the knowledge of virtual learning

Build up a common portal for all students in Finnish polytechnics

Co-operation with other local and international projects

Quality assurance

Copyright questions (teacher – institution – outer world)

Support for teachers who are producing material

Standardization including learning platforms, material modules meta data, student administration and economical aspects

The main result of the Finnish Virtual Polytechnic will be more cooperation between different polytechnics. Teacher education must cover new skills like coaching students through learning environments on a net platform. Virtual learning in the information society in Finland will cross borders not only between polytechnics but also to other schools and to other nations. The Finnish Virtual Polytechnic will also support the following vital interests of the student: more personal studies, many study options, a broader curriculum, and a new didactic approach.

Content production teams

The Finnish Virtual Polytechnic has 31 polytechnics as members and a potential of 120000 students and 6000 teachers. Content production is being done in 28 production teams, in year 2003. The aim is to have virtual courses of more than 200 credit units. The network security course has been produced in the production team Computer Networks, Telecommunication and Telecommunication Systems. The total amount of credit units in this production circle is 11.

Course development process

Text and table based information has been produced by teachers and students. Figures, animations, and other graphical material production have been supported by other expertise within the polytechnic. The production team consists of 2 IT teachers, 3 IT students and 1 graphical designer. The effort needed to develop the course:

both IT teachers have worked 4-5 hours/month during about 10 months to plan the course, with content production, and to supervise the 3 IT students and the graphical designer

two IT students have worked about 20 hours/month during 6 months with content production for the course.

one IT student worked 6 hours/week as course assistant, when the course was given as a test course in January-May 2003.

the graphical designer has worked full time during about 6 months with

- the web based learning environment

- the Flash animations
- picture design for the course content.

Course development continues during the study process of an accepted group of course students:

weekly tasks and given exercises are integrated in the web based learning environment

the course schedule is updated every week

feedback and comments from course participants as well as response of the course teacher to this feedback is promptly published on the learning environment

course content is updated and revised based on the experiences from the ongoing course.

For this work a graphical designer is needed about 10-16 hours/week to support the course teacher.

Course material

Course material is produced using:

word processing (.doc), FrontPage or Netscape Composer (.html) for text

Adobe PhotoShop and Macromedia Flash 5 for pictures (.gif, .jpeg)

Macromedia Flash 5 for animations (.swf)

The course material has been organized in modules. Course testing and evaluation will be done by the production team, by IT teachers, and by students who will use the course material. Accessibility and navigation will be tested using IE and Netscape browsers.

Course Content

The course is divided into seven chapters that make up the course material. These chapters can be found from a navigational menu on the course portal. In the menu there are also links to the course index, all the exercises and the weekly topics.

The first chapter of the course is an introduction to the course material. The topics of the other chapters are:

Network Security Administration

Antivirus Protection

Firewalls

Cryptography and Network Security

Network Security Software

Security of Wireless and Mobile Networks

The course material published on the web has been developed to be used in parallel with the course book (Stallings, 2002). The course content structure, developed by the course production team, is different from the chapter division of the course book. All of the course topics are not treated in the course book and all of the course book topics are not covered by the course.

Chapter 1 - Introduction

The “Introduction” chapter gives the student a short and illustrative introduction to the basic concepts of network security. The chapter consists of four sections

Main Introduction

Taxonomy Diagram

Network Security Threats

Features of Secure Networks.

The “Main Introduction” section summarizes the main network security concepts and important information needed in the following course chapters.

The “Taxonomy Diagram” section shows the fundamental properties of network security - integrity, protection, and security administration – as an interactive, animated Network Security tree (see Figure 2). The main branches of this tree are Integrity and Protection. Both man branches have many sub-branches, which represent the variety of the fundamental properties. The leaves covering the whole tree visualize Security Administration, which is needed everywhere.

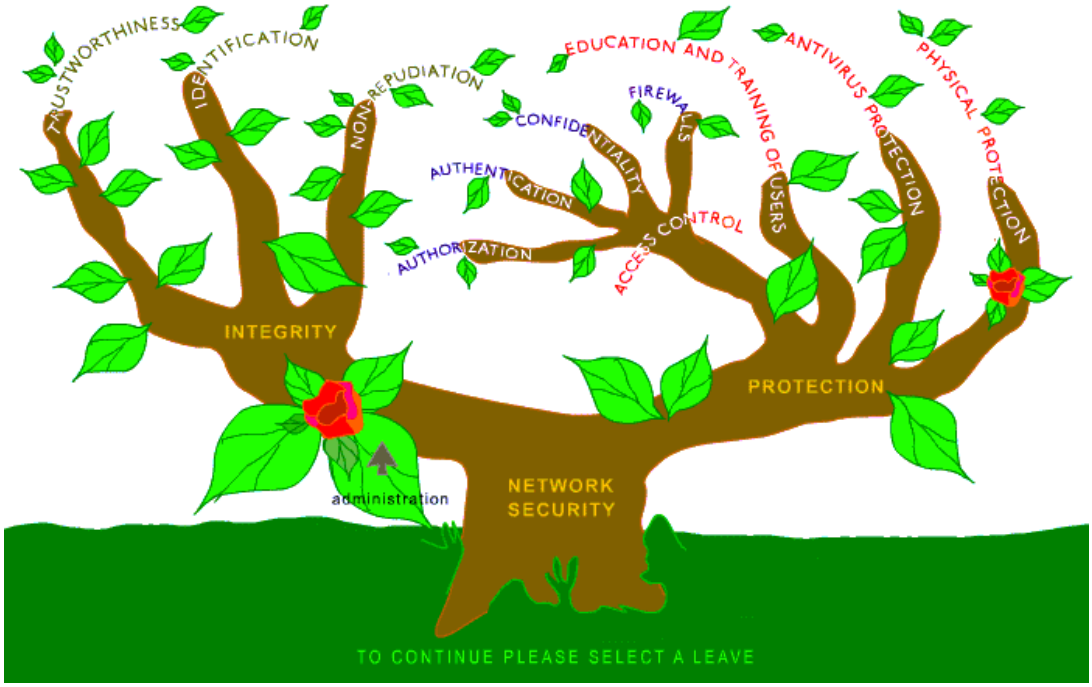

Figure 2. The interactive animated Network Security tree.

The “Network Security Threats” section shows a classification consisting of three network security threats, damage, eavesdropping, and intrusion. The section is implemented by an interactive audio-visual animation (see Figure 3). By activating different sectors of the animation the user gets advice how to manage these threats.

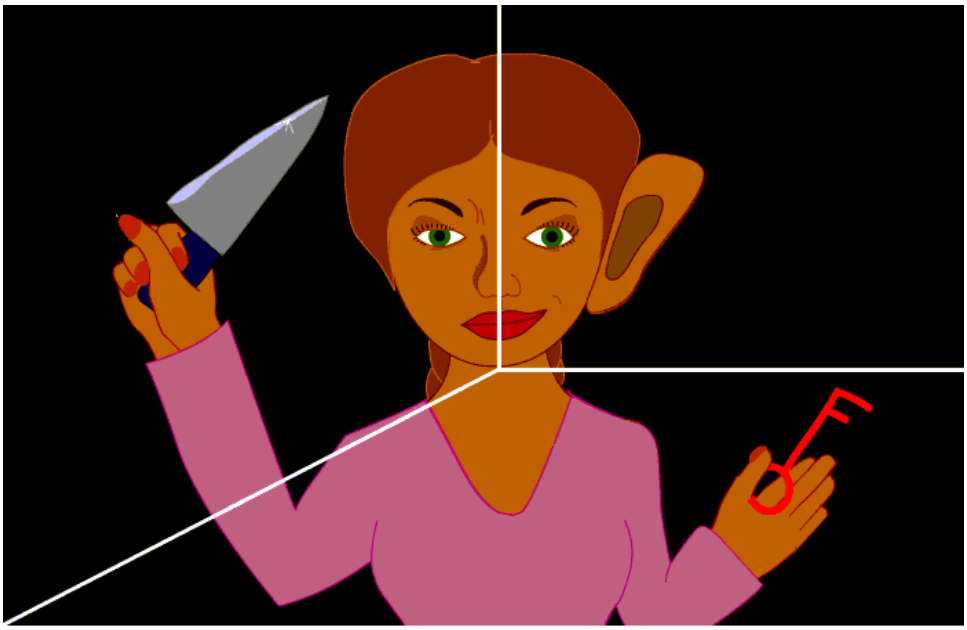

Figure 3. Interactive animation of network security threats.

The “Features of Secure Networks” section illustrates different technologies and methods needed to build up secure networks. These technologies are needed for access to a private network from other networks, from different segments of the same private network or from a computer connected to Internet. The illustrated technologies are:

SSH Tunneling

VPN Access

VPN Connection

The section describes also other important concepts related to the illustrated technologies, e.g. Home User, Other LAN and ISP.

The section is implemented with an interactive graphical animation for highlighting network security architecture features (see Figure 4).

Chapter 2 – Network Security Administration

The “Network Security Administration” chapter presents important security related issues of the broad concept of network administration together with information about user support and education. The roles of Security Incident Response Teams and Standardization organizations are presented together with examples of important network security standards and security administration software. The chapter includes three exercises to help students understand the chapter contents. The chapter is divided into the following sections:

Introduction

Security Policy

Intrusion Detection

Vulnerability Assessment

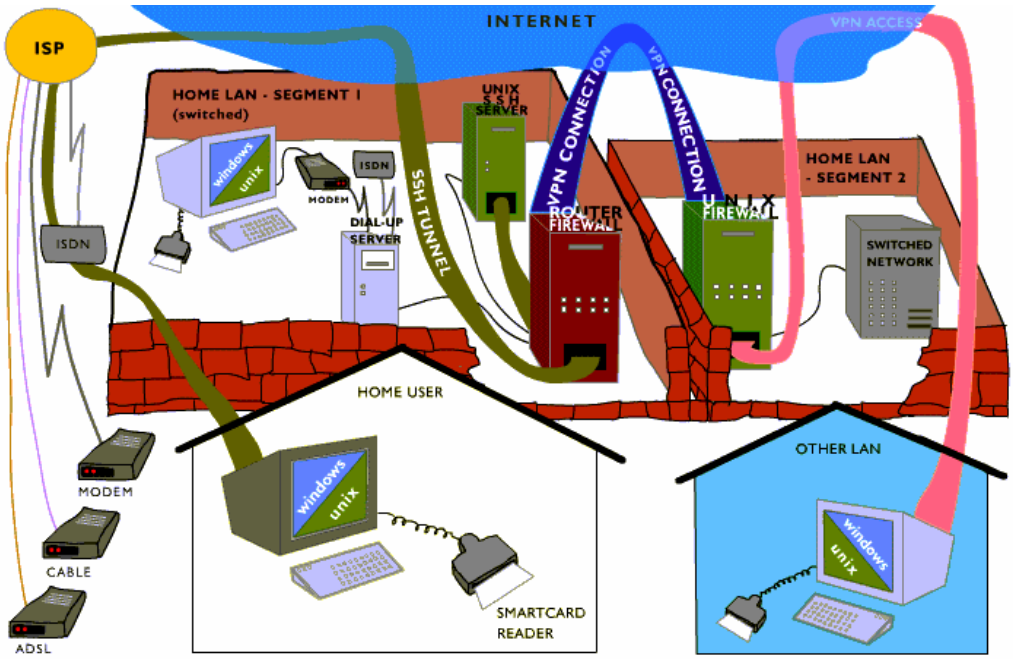

Figure 4. Interactive animation of a network security architecture.

User Support and Education

Security Incident Response Teams

Network Security Standards.

Security Administration Software

The importance of using a well-defined security policy, managed by a security team, as the basis for network security administration is presented in the “Security Policy” section. A security policy defines the network security goals and responsibilities as well as the administrative procedures and methods needed to achieve these goals. The section includes an exercise (“Security Policy”) where the course student is asked to outline a Security Policy.

The concept of intrusion detection and the software needed for intrusion detection is presented in the “Intrusion Detection” section. The use of intrusion detection software is vital for the identification of security breaches in the network.

Vulnerability Assessment Systems that are used as a complement to intrusion detection are presented in the “Vulnerability Assessment” section. Security vulnerabilities like configuration errors and system problems can be found using vulnerability assessment software. The section includes an exercise (“Vulnerability Assessment”) where the course student uses a port scanner and a password cracker to find network security vulnerabilities.

The need for user support and user training to achieve certain user skill levels is presented in the “User Support and Education” section. User training and user support are both important in network operation and are therefore needed to maintain network security. The absence of education and support could lead to serious security hazards caused by human errors.

Fundamental information about Security Incident Response Teams is presented together with examples of such teams in the “Security Incident Response Team” section. These teams register

different network security problems, find solution to these problems and make the solutions publicly available.

Both international and national standardization organizations are presented in the “Network Security Standards” section. The section describes a wide range of different network security standards and recommendations by organizations like, IETF (IETF, 2002), ISO (ISO, 2002), IEC (IEC, 2002), RSA Security Inc. (RSA Security Inc., 2002) and FINEID (FINEID, 2002). The concept of network security standards is a very broad subject, stretching from physical network components to software and protocols. The section includes an exercise (“Network Security Standards Quiz”), a quiz with several short questions concerning network security standards.

The “Security Administration Software” section summarizes software already presented earlier in the sections “Intrusion Detection” and “Vulnerability Assessment” together with management software used to centrally manage the use of other network security software.

Chapter 3 – Antivirus Protection

This chapter describes different types of malicious programs, often called viruses, with emphasis on how they behave and how they are propagated. Viruses are classified by the way they propagate and behave together with explanations about the different activity phases of viruses. The historical development of antivirus protection is presented starting from simple scanners to advanced modern methods. The antivirus protection levels needed for optimal network wide antivirus protection are outlined and illustrated with examples. The importance of an antivirus strategy is pointed out together with the necessity of regularly updating the virus definitions. The chapter includes an exercise (“Antivirus Protection Quiz”), a quiz with several short questions about antivirus protection.

The “Antivirus Protection” chapter is implemented as an interactive animation with text and hypertext features (see Figure 5). The Firewall chapter animation consists of six sections:

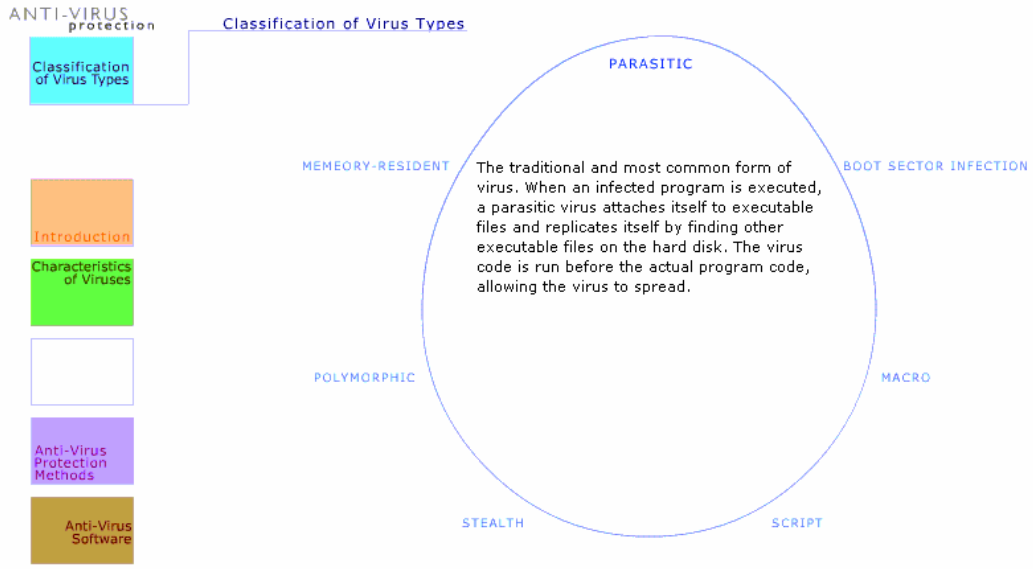

Figure 5. Interactive animation of antivirus protection.

Introduction

Characteristics of Viruses

Classification of Virus Types

Antivirus Protection Methods

Antivirus Software

The definition for a virus is presented in the “Characteristics of Viruses” section where also different ways of grouping viruses is discussed. The section describes the different activity phases of viruses together with information about how viruses propagate.

The classification of viruses is presented in the “Classification of Virus Types” section. The section includes basic information about the classified virus types (Memory-Resident, Parasitic, Boot Sector, Macro, Script, Stealth and Polymorphic).

The “Antivirus Protection Methods” section describes how antivirus protection should be set up to give the best practical protection against viruses. The section also presents the different antivirus software generation.

The section “Antivirus Software” introduces the different levels of antivirus protection that can be achieved using modern antivirus software together with examples of such software. The importance of combining the different levels of antivirus protection is pointed out as well as the need to update the virus definition databases.

Chapter 4 – Firewalls

The Firewalls chapter provides the user with basic knowledge about firewalls. Firewalls should prevent intrusion into private networks. Many programs used in a typical network are vulnerable. This is one important reason to include a network access controlling firewall in the gateway to a

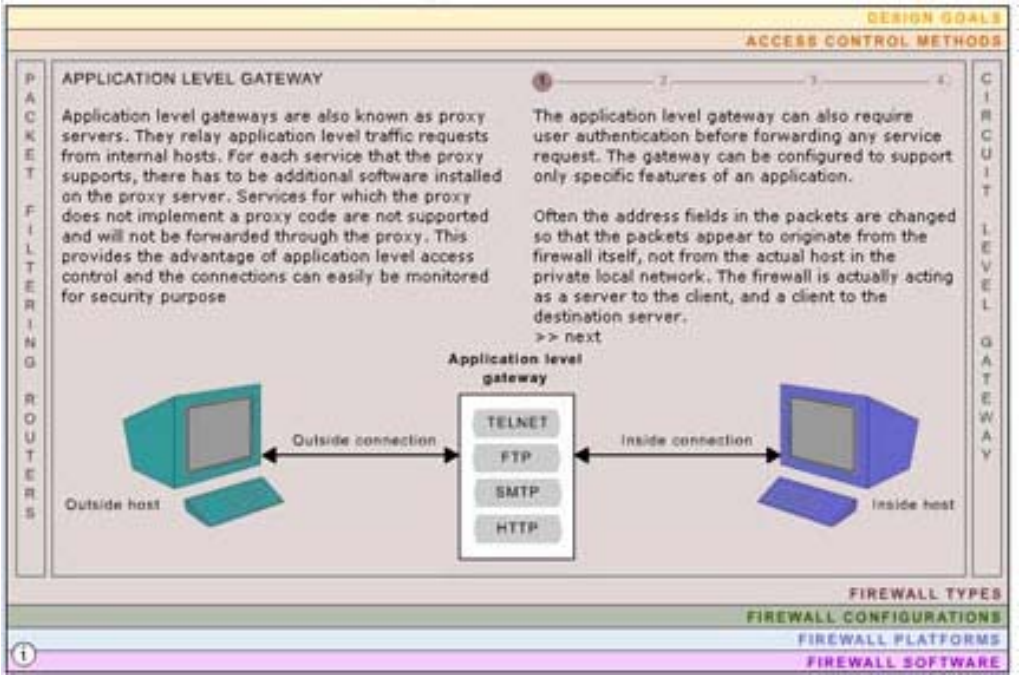

Figure 6. A screen from the Flash implementation of the “Firewalls” chapter.

network. The chapter includes an exercise (“Firewall Rules with IPTables”) where the student is asked to explain firewall functionality and design iptables rules.

The “Firewalls” chapter is implemented as an interactive animation with text and hypertext features (see Figure 6). The Firewall chapter animation consists of six sections:

Design Goals

Access Control Methods

Firewall Types

Firewall Configurations

Firewall Platforms

Firewall Software

The “Design Goals” section describes the reasons to use a firewall and the general operational principles of a firewall. The importance of a secure firewall is underlined because a network is just as secure as the firewall protecting it.

The “Access Control Methods” section gives a basic understanding of the basic four network traffic filtering techniques used to implement access control. These techniques are:

Service control

Direction control

User control

Behavior control

The operation principles and security features of three classified firewall types are described in the “Firewall Types” section. These firewalls types are:

Packet Filtering Router

Application Level Gateway

Circuit Level Gateway

Four fundamental configurations are presented in the “Firewall Configuration” section:

Screened Host

Single Homed Bastion

Dual Homed Bastion

Screened Subnet

Screening is used in all these configurations. Some configurations combine screening with bastion hosts, one of them even uses double screening hosts. The concept “bastion host” and the properties of the different firewall configuration types are described.

The “Firewall Platforms” section presents different physical firewall implementation platforms and the “Firewall Software” section presents examples of available firewall software.

Chapter 5 - Cryptography and Network Security

This chapter presents the theoretical foundations of cryptography as well as information about fundamental cryptographic algorithms and protocols. The chapter includes fourteen exercises and consists of seven sections:

Introduction to Cryptography

Theoretical Foundations

Cryptographic Algorithms

Cryptographic Protocols

Encryption Key Management

Cryptographic Hardware

Cryptographic Software

The section “Introduction to Cryptography” describes the basic concepts of cryptography using an audiovisual slideshow.

The “Theoretical Foundations” section presents the theoretical background of present cryptography: information theory, complexity theory, number theory (modulo arithmetic’s, finite (Galois) fields, factoring, prime number generation, elliptic curve arithmetic’s and secure random number generation). The section includes two exercises. In the first exercise (“Basic math of cryptography I”) the student is asked to perform basic calculations and answer to questions related to complexity theory and modular arithmetic. In the second exercise (“Basic math of cryptography II”) the student is asked to perform basic calculations and answer to questions related to finite (Galois) fields and elliptic curve arithmetic’s.

The “Cryptographic Algorithms” section contains presentation of the essential features of cryptographic algorithms and a detailed characterization of the fundamental cryptographic algorithms, the secret key algorithms (symmetric), the public key algorithms (asymmetric), and the hash algorithms. The section includes two exercises; the first exercise (“RSA algorithm”) is about the general purpose asymmetric RSA algorithm and the second exercise (“Diffie-Hellman Key Agreement”) is about the asymmetric Diffie-Hellman key agreement algorithm. The section also includes an animation that visualizes the data flow logistics of the cryptographic protocol that uses the Diffie-Hellman key agreement algorithm.

In the “Cryptographic Protocols” section the fundamental cryptographic protocol types, the digital signature protocols, the secret key agreement protocols, and the authentication protocols are presented. The functionality of the Kerberos authentication protocol is visualized by an audiovisual animation included in the section.

The “Encryption Key Management” section explains how symmetric and asymmetric encryption keys are generated, stored, distributed, revoked and destroyed. Also the significance of trusted public key ownership of and principles of standardized Public Key Infrastructures (PKI) are presented. PKI is also visualized by an audiovisual animation of the sending and the reception of a signed email message. The section includes two exercises; the first exercise (“Cryptographic Key Management Quiz”) is a quiz about cryptographic key management and the second exercise (“Security Token Quiz”) is a quiz about private key protection with security tokens.

The “Cryptographic Hardware” section covers different types of cryptographic hardware used for generation, protection and use of sensitive cryptographic data structures, e.g. cryptographic keys and irreproducible random numbers, and for acceleration purposes. Examples of such hardware are:

smart card chips,

USB tokens,

PC Card cryptographic tokens,

True Random Number Generator (TRNG) and

cryptographic processors/acceleration chips.

The “Cryptographic Software” section surveys software and applications for network security. VPN solutions based on the IPSec standard implement network level security. Application level security can be achieved using software and application based on the SSL/TLS standard or by using custom designed security software. The software used for accessing smart card based cryptographic tokens is also covered. The section includes the following exercises:

“IPSec Quiz” – Quiz about IPSec concepts

“VPN configuration with FreeS/WAN” – Configuration of a VPN connection

“Public Key user authentication in OpenSSH” – Creation of a RSA or DSA authentication string

“Protected Email Communication to a Mailbox” – Use of the SSL protected IMAP protocol

“Secure email with S/MIME” – Signed and Encrypted email communication with S/MIME

“Setting up use of PGP for secure electronic mail” – PGP configuration and use

“Secure Remote Browsing of an Intranet” – Setting up an SSH tunnel

“Cryptographic Software Quiz” – Quiz about cryptographic software

Chapter 6 – Network Security Software

This chapter includes information related to software used in different parts of the broad subject of Network Security. It contains the following seven sections:

Introduction

Security Administration Software

Antivirus Software

Firewall Software

Cryptographic Software

Security Software Development

Design of Security Software

The “Introduction” section gives a short introduction to the topic of Network Security Software and the contents of the chapter.

The following four sections (“Security Administration Software”, “Antivirus Software”, “Firewall Software” and “Cryptographic Software”) are also included in other chapters, of the course, devoted to field of the software category. The section “Security Administration Software” is also reachable from chapter “Network Security Administration”, the section “Antivirus Software” from chapter “Antivirus Protection”, the section “Firewall Software” from chapter “Firewalls” and the section “Cryptographic Software” from chapter “Cryptography and Network Security”.

The last two sections, “Security Software Development” and “Design of Secure Software”, are reachable only from this chapter. The section “Security Software Development” introduces available software libraries and tools for development of secure network applications and for integrating security features in all types of software. The section includes an exercise (“OpenSSL programming example”) where the student is asked to set up SSL protected communication using OpenSSL. The section “Design of Secure Software” covers the different security requirements of network software and how to take them into consideration while designing network software. The section includes an exercise (“Secure Software Design Quiz”), a quiz about the section contents.

Chapter 7 – Security of Wireless and Mobile Networks

This chapter gives a topical overview of wireless and mobile network security aspects. Security measures taken depend on the protocols, standards, techniques and systems available. A survey of security protocols, standards and corresponding technologies is given. The chapter focuses on 2G, 2.5G, 3G and wireless local area networks. Standards, like WAP (“What is WAP?”, 2002), IEEE 802.11 (IEEE 802.11, 2002), HomeRF (HomeRF, 2002), HIPERLAN/2 (ETSI Hiperlan/2 standard, 2002), IPSec (IP Security Protocol (ipsec), 2002), and Bluetooth (Bluetooth, 2001) are presented. The chapter include an exercises (“Wireless and mobile security Quiz”), a quiz where the student is asked to answer short questions concerning the chapter contents.

Didactical Approach

The chosen didactical approach is a guided excursion to which students from different polytechnics enroll. A team consisting of a responsible teacher, a course assistant, and a graphical designer, the maintainer of the web based learning environment, provides the guidance.

Guidance

The guidance is based on step-by-step skill assimilation, starting from user level skills. The following skill levels are the network administrator level and application development level. Skill assimilation will proceed to a point from which course students can continue with advanced follow up courses leading to scientific network security skills.

Course Book

The newest edition of the rewarded network security textbook authored by Stallings (Stallings, 2002) has been chosen as course book to be used in parallel with the course material published on the web.

Weekly Task Sets

The course proceeds with task sets distributed weekly to the course participants using the course mailing list and the web based course portal. The weekly task sets consist of configuration, installation, calculation, testing or programming exercises or topical quizzes and of study directives. Each weekly task set has a deadline.

The exercises assigned in the weekly task sets are included in the course material. The first four exercises have a special function. They act as an authentication “gateway” that needs to be passed before access to parts of the learning environment and to the rest of the exercises is obtained.

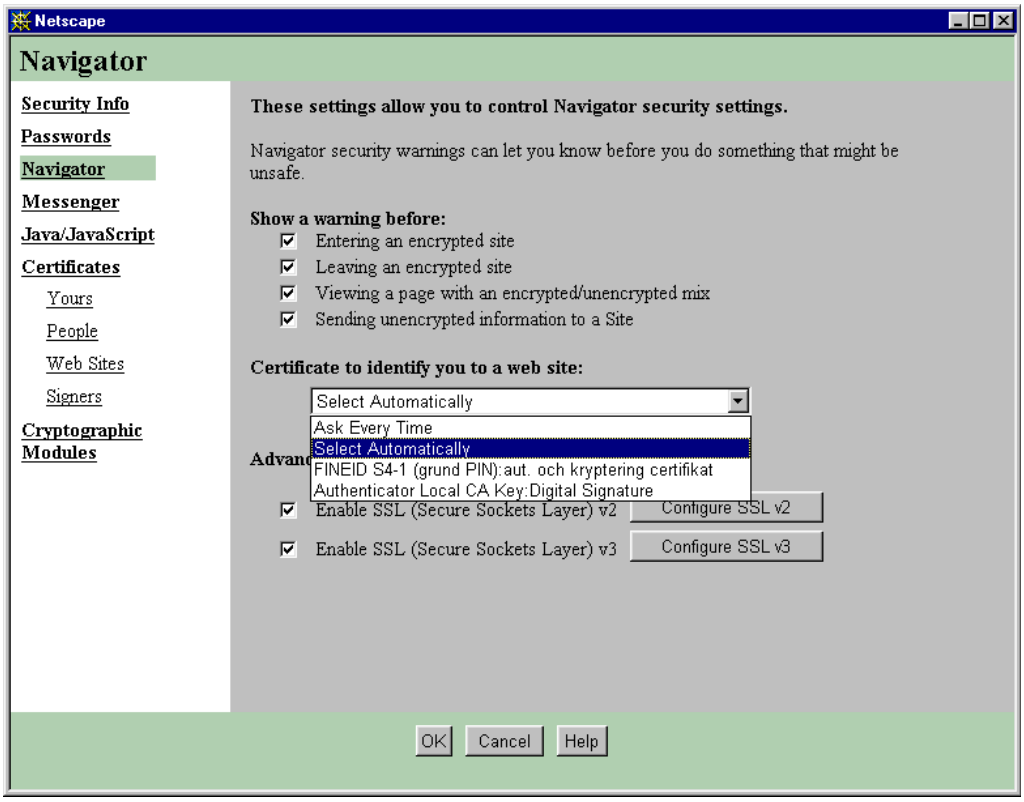

Figure 7. Security settings in Netscape Communicator v4.79.

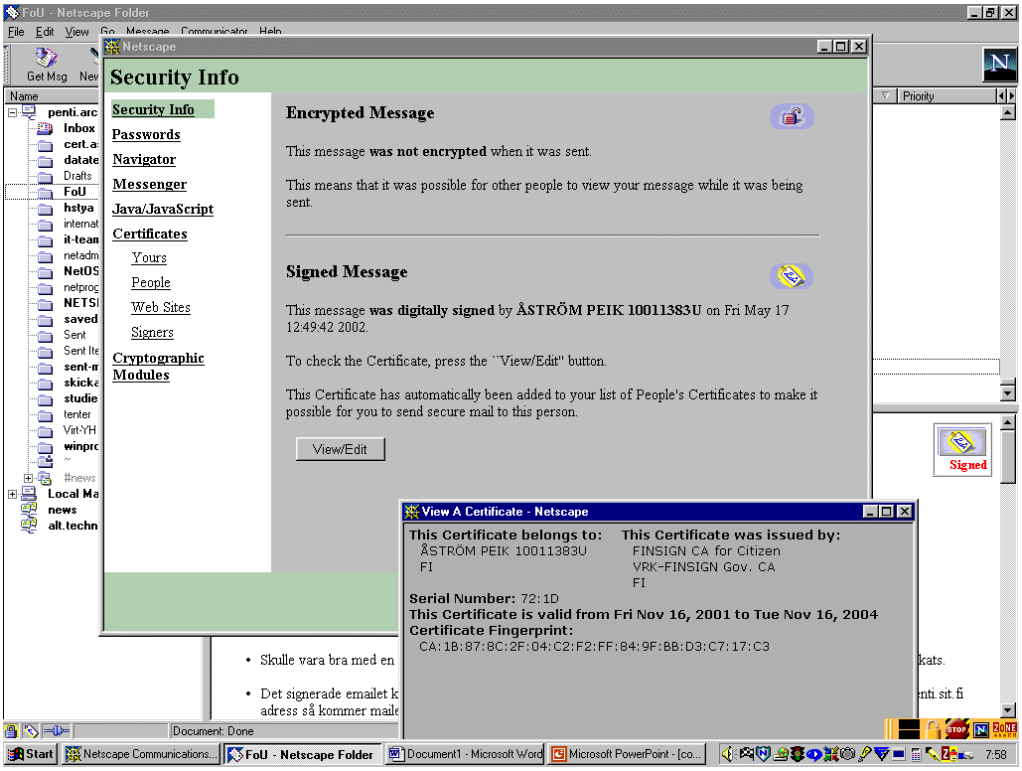

Figure 8. Inspection of the signature of a signed email message in Netscape Messenger v4.79.

Administrator Level Skills

The next level of network security skills is the **network administrator level**, which should include

skills to install, configure and update network security software (see Figure 9) and hardware

security policy outlining skills

network user support and training skills in security related issues.

Education of IT engineers and other IT professionals should provide network administrator skills in network security.

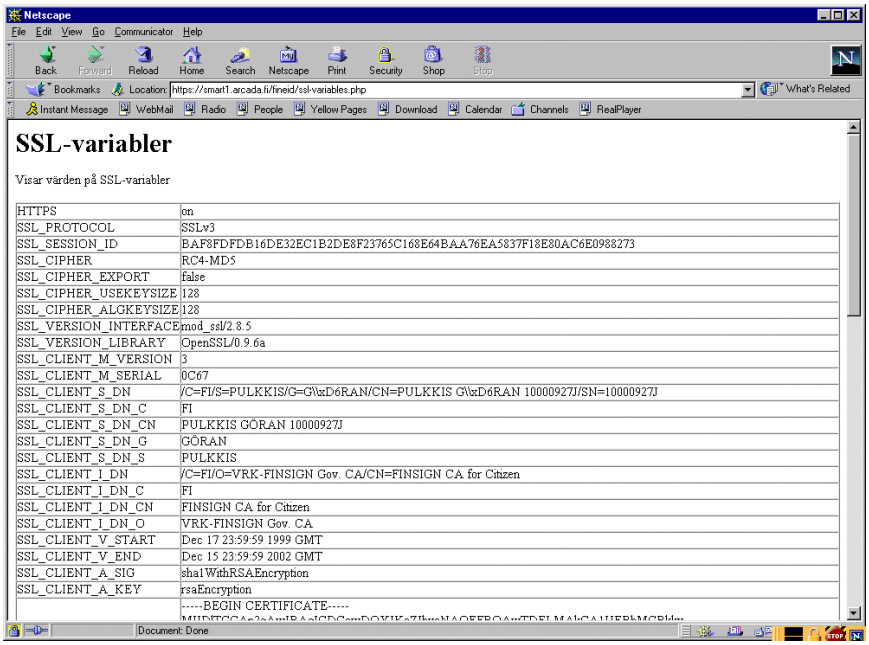

Figure 9. SSL variables in the configuration file of a web server configured for HTTPS – the secure HTTP protocol.

Application Development Level Skills

The highest level of network security skills in *polytechnic education* is the **application development level**. On this level advanced programming and hardware design skills are combined with a profound and detailed knowledge of

behavior of viruses and other malicious programs

TCP/IP and other network protocols

cryptographic algorithms, protocols and standards.

For example, the knowledge and skills needed for development of PKI client software based on the PKCS#11 standard (RSA Laboratories, 2002) are based on advanced C programming in combination with a profound knowledge about accessing software and hardware implementations of cryptographic tokens. Education of software and programming professionals should provide network security technology development skills.

Network Security Skills on a Scientific Level

The highest level of network security skills in *university education* is the **scientific network security level**. This level covers knowledge and skills

to propose new protection methods against viruses and other malicious programs

to propose new firewall types and configurations

to further develop the mathematics of cryptography and

to propose new cryptographic algorithms, protocols and standards.

It should be possible to acquire this skill level in postgraduate IT education in universities.

The Graphical Design of the Learning Environment

Background and Presentation

The design of the learning environment has been primarily motivated by the aim of the course (learning) and its target group (students of computer and telecommunication engineering). The starting point of the design for the web course 'Network Security' is that a high bandwidth Internet connection is available to users. Therefore it was decided to add elements like animations and sound, since such elements stimulate the senses more than just plain static text. Nevertheless, the static text is still the most important element of the course. The learning environment with the material of the course is built on frames and HTML with some JavaScript files. All animations are made with Flash 5, which means that users need a Flash 5 Plug-In, which can be downloaded from Macromedia's website (Macromedia – Flash MX, 2002). Some animations include an audio part. A user without the possibility to listen to audio can find the spoken text written next to the animation.

The graphical design has two dimensions, the communicating dimension and the esthetical dimension. The communicating dimension, *the interface*, describes the interaction between the user and the learning environment. It has two parts, the informative part with the course material and the interactive part with the information needed for communication between the student and the teacher. The esthetical dimension, *the layout*, describes the visual style of the whole website, see Figure 10. As communication goals are more easily achieved with a strong esthetical structure, these two dimensions are very much dependent of each other and only together they make the learning environment good.

The Interface

The interface of a product is about *usability* and *comprehensibility* of the product, and should support the user to achieve the goal that is set for using the product. In this case the goal is to learn, which makes the design of the interface even more important. The time to study and understand the interface should be minimal, so that the user doesn't have to use the time that is meant for learning the contents of the course, to learn how to use the learning environment. This means that the design should be carefully planned and the same throughout the whole website. The description of the interface consists of

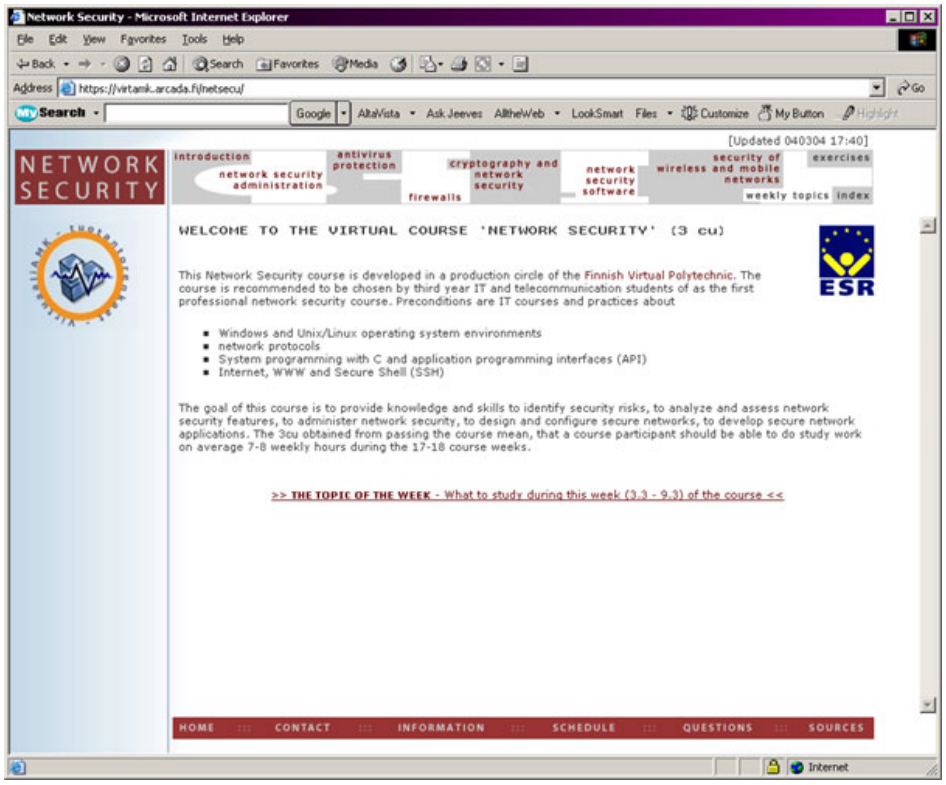

Figure 10. The layout of the learning environments' home page.

the usability of the website and

the comprehensibility of the course.

The usability of the website

The usability of the website is the way the elements of the website are used separately and together. The three milestones of usability are

the *navigation* on the website, designed both from the informative part and the interactive part,

the *elements of interaction* between student and teacher and

the *index* of the course and the whole website.

The index is included as the third part of the usability because it is one of the most important elements of an interface for a learning platform. The user should find the index easily and fast, without having to select many hyperlinks, as this page will probably be an often visited page of the user.

The navigation on the website. The navigational system consists of two main parts, the informative part that is the navigation of the course and the interactive part that is the navigation of the learning platform, which includes the informative part.

Since the website is built on frames, a user will always start his session at the homepage of the learning environment. The homepage is composed of three frames: top, middle and bottom frame. The user can find two menus on this page, which are also the main menus of the learning envi-

ronment; one formed like a puzzle in the top frame and the other in the bottom frame. The top menu is the course menu and thus the most important menu. It is placed on the top of the screen, because this is the place where the eye normally goes first when a web page is opened. The form of the menu is different and bigger compared to the bottom menu, so it is more noticeable and awakes interest. The menu on the bottom of the screen is the menu for the interaction between the student and the teacher. It has no elements linked to the actual course and no submenus unlike the top menu, which contains of much more information. A page opened from either menu appears in the middle frame and both main menus are always visible.

The top menu contains nine puzzle pieces describing the seven chapters of the course, the index, the weekly topics and the exercise page where all the exercises of the course are gathered. All chapters except Index contain a submenu. Some submenus have own submenus. The submenu of the pages is placed on the left side of the middle frame except in Chapter 4, which is a flash animation and therefore has a different kind of structure. The navigational structure of Chapter 4 needs some studying before using, but some difference in-between the chapter's internal composition is good for the user's ability to remember (See Figure 6).

The chapters are all composed of a left frame and a right frame. The left frame is for the submenu and the right for the contents of the submenu. A submenu of a chapter submenu, thus a sub-submenu, is placed on the top of the right frame. Then all menus (the two main menus, the submenu and the sub-submenu) of a chapter are always visible. The right frame is placed under the main top menu, and has a marker on the top of the page pointing out to which chapter the contents belongs. The path to the current page is also written in the heading of the contents page – for example *chapter 4 / submenu 3 / sub-submenu 2 / header of the page*.

The start page of the course can be opened from the course logo on the left in the top frame and from a hyperlink named '*home*' in the bottom menu.

The elements of interaction between student and teacher. To become a course that can be used independently on the web, the Network Security course needs a learning environment. This means that the website needs elements for interaction between the student and the teacher. These elements can be found in the bottom menu and on the home page of the learning platform, and represent information widely used throughout the course. Before continuing it is necessary to mention that the composition of the home page changes week after week, and is therefore one of the active elements of the learning environment. In the beginning of the course, the home page consists a big amount of information, information that the student will need less and maybe just in the beginning the course. Some of it is later placed under the links of bottom menu. This start information describes how the course is lead, how to use and understand the learning environment and which are its' IT requirements. To avoid an unorganized and distracting design, the amount information on home page is reduced to its minimum during the course. Just a short description of the course and the preconditions of the students, a link to a page with the topic of the week and announcements of the week are necessary.

The six links in the bottom menu are.

A link to the *home* page.

A link to a page with the *contact* information of the teachers, assistants and other students.

A link to *information* about the conferencing area, bulletin board and newsgroups of the course, and a list of IT requirements that need to be fulfilled to be able to follow the course. On this page is also explained the two menu system.

A link to a *calendar* outlining the significant events of the course.

A link to a *questions* page where all the questions and feedback that the students give during the course are gathered.

A link to the *sources* of information.

On the very top of the page it is communicated when the learning environment was last updated. This function is an important element of the interaction between the teacher and student as it confirms to the students the maintenance of the environment.

The index. The Index of the website is situated in the puzzle menu on the top, although it is an element to serve the entire website. This was done because the importance of the course indexes. The index consists of two parts; the course index, which is a JavaScript file, and the learning platform index.

The use of the course index suffers from the frame structure of the website. A submenu or a sub-submenu of a chapter cannot be opened directly. A chapter can only be entered from its start page.

The comprehensibility of the course

To make the comprehensibility of the course and the entire website more clear and obvious for the user, the website should communicate with the user. The elements need to give feedback for any action made by the user. This means for example that if the user rolls over a link with the mouse, the link ought to react in some way so that the user recognizes this as a link. The feedback in the main menus and in the submenus is given using a blue rollover color. In the sub-submenus the feedback is given by highlighting the graphic with red color. Already visited text hyperlinks remain light red. Because the two main menus are graphics (not text), they leave no trace of visited links. But as the trace of a visited chapter is important, a visited link in the top menu is designed in an alternative way: a line of blue dots below the puzzle piece of the visited chapter. This JavaScript is supported only of Internet Explorer and the dots disappear when the page is reloaded.

For clarity all links to other pages in the Internet are opened in a new window. All animations, which are independent of the body text, are opened in a new window. The animation is then seen as a story of its own and can easily be managed. (See Figure 11)

The Layout

The goal of the communication between the user and the course website is more easily achieved with a strong esthetical structure. It is important to make the user motivated and interested by using inviting colors, a sober font on a calm background, a clear and organized positioning of the elements. The quality of the user interface is very important. The screen should always look like an organized workspace. Of course the opinion of what is aesthetically beautiful is personal, but a good rule is: simplicity is elegance. It is always good to remember the target group and the purpose of a website. The three most important layout issues in the design of this learning platform are:

the visual structure

the colors

the font type

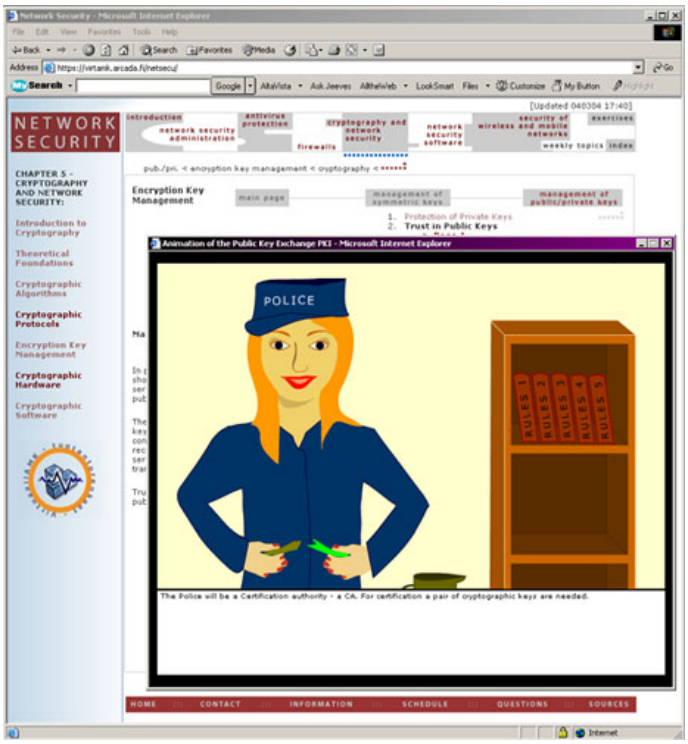

Figure 11. The animations are opened in a separate window.

Visual structure

The unity of the pages and the design of the elements create an elegant website. The same font style is kept throughout the learning platform, while the structure of the material however differs some in the Flash implementations from the html-pages. Nevertheless, these implementations are just a small part of the course, and are planned to stimulate the user. The major part of the learning environment has a coherent structure of the submenus, the sub-submenus, the headers and the text.

Contrast enhances the difference between separate elements in one area and it creates clarity and harmony in the entire layout. When the user opens a chapter, the text area differs from other areas. This makes reading the content easier than if there would be another text field visible on the screen. Elements belonging together in relationship to the rest of the page layout are grouped to balance the whole screen.

The last, but almost the most important element of a successful visual structure is space. Without space the elements of the website do not get their earned attention. For example, if the two main menus where placed close to each other, it would be difficult to comprehend these as two separate and important elements of the communication between the user and the product. When designing a visual structure it is good to remember not to mislead the user's eyes to an unwanted place with elements that draw attention.

Colors

When the colors to the interface were designed the goal was to use white as the main color. Calm and non-disputable color combinations were chosen. To make the reading and concentrating eas-

ier strong colors that irritate the eye were avoided. These factors are important when designing a website to be used frequently by the same user.

Colors can have several effects on the user. They attract and create feelings, e.g. the bottom menu that is in red color to make it more noticeable from its hidden position in the page layout. In the top menu blue was chosen as the “mouse over” color since it is the contrast color of red, which is used as the font color in the menu. All this awakes interest and attraction to this important feature of communication. Colors can also help remembering, especially if they distinguish from the group. In Chapter 4 (Firewalls) this is tried out, since the whole chapter has a different kind of structure and more colors than the other chapters. The colors help grouping. For example, when a page from the bottom menu is selected, then the page is combined with the menu and with red lining of the page. The same applies to the pages opened from the top menu, with the exception that these pages have a gray lining in conformance with the top menu, which also has a gray lining. The colors highlight hierarchy or path, and demonstrate that something is available or not available. For example, the sub-submenu, which is not opened, is light gray and the one, which is open, is strong purple.

The font type

The font type used on the html pages is Verdana (Arial). The normal text is dark gray and the size is 11 points. This is a font without serifs (without end curves in the letters) and because of that it has a better legibility on the computer screen. Also the font used in the graphics and in the pictures is Verdana. When a word or a phrase is highlighted in a text, it is bolded instead of, for example, underlined that should be explicitly used for hyperlinks or titles because of its strong convention.

Long passages of unbroken text are avoided, because text on screen is tiring to read. The rule is that the information of a page, which has no pictures, should fit the screen without scrolling, and that one page only contains one heading. If this rule is followed the user experiences more variety and change in between the different subjects. For a good legibility of the body text in the HTML pages, the background color of the page is white.

The IT Infrastructure of the Learning Platform

Registration to the Finnish Virtual Polytechnic

The registration process will be handled by the Finnish Virtual Polytechnic’s student office, which will probably be an electronic online office. Once the users have registered, and received their study place, the Finnish Virtual Polytechnic will create an account for them. There are two choices of accessing this account; using standard username and password authentication or by using a PKI certified cryptographic key pair. The private key of this key pair and the cryptographic operations using this private key may be hosted on a smart card based electronic ID card. If the student has an electronic ID card, the student’s SATU number will be registered and stored in a LDAP directory. The SATU number is a unique public personal code in a Finnish electronic ID card (FINEID, 2002).

Authentication

Once the course participants have successfully applied and registered to the Finnish Virtual Polytechnic they will be authenticated and granted access to the learning environment of the network security course, hosted by a web server, a news server, and SSH servers. Authentication is prefer-

able achieved using a Finnish electronic ID card, a FINEID card (FINEID, 2002). Anyone permanently living in Finland can apply for a FINEID card. Any granted web server can look up the access information stored in the LDAP directory, hosted by the Finnish Virtual Polytechnic.

Communication

In the real world, like in a class in any normal university or polytechnic, communication is a very important part of the learning process. The students have to be able to interact with the teacher, and with each other. Students need to exchange information by establishing a fruitful dialogue. Therefore, it is important that an online course can provide these same conditions. Students need to be able to exchange information with each other, even though they may be geographically scattered over a big area. The communication described above will be established using three different techniques: email, newsgroups and real time chat functionalities.

Email

The course will have a mailing list hosted by a majordomo server. When students register to the course they will also be registered on a mailing list. This mailing list is used for sending out information to all course participants, for instance topical study directives, exercises, examination dates, etc. It may also be used to distribute urgent information, since every student attending the course will receive a copy of the emails sent to the list. Emails can of course also be used for direct communication between student and teacher or between students.

Newsgroups

The course will have a newsgroup where the participating students can discuss topics related to the course. This is the main forum for the students. The information sent to the newsgroup should not be urgent, for urgent information it is preferable to use the mailing list.

An un-moderated newsgroup is very suitable for creating the communication environment mentioned earlier. Since the news system is threaded, it is very easy to navigate between the articles found in the newsgroup. Each new subject will be a new top-post and all comments concerning this subject will be added as a follow-up to that specific thread.

The message board of the course is another moderated newsgroup.

It is up to the student to check the newsgroup for new information independently. The students will not be notified when there is new information available in the newsgroups.

Real time chat, IRC (Internet Relay Chat)

It can sometimes be hard to have a serious dialogue with someone using email or newsgroups. If you need answers to your questions fast, and if you have resulting questions, it is preferable to use real time communication. Especially when there are many people involved in a discussion, it is much easier to have a real time chat. This real time chat functionality will be accomplished by using the already existing IRC network, the Internet Relay Chat.

The IRC network consists of a number of servers scattered across the world (and Internet), mentioned here as IRC servers, connected to each other to form a network. They exchange information in real time so that all users across the world can read the messages sent out by all users. The user selects which messages to receive by joining a specific channel. One can then communicate (in public or in private) in real time with all the other users currently online in the same channel.

A possible use of a newsgroup is a weekly scheduled moment where an expert on the course would be virtually present in the IRC channel answering to questions asked by the students. The communication could be recorded so that it afterwards could be presented on the web for all participating students.

Other alternatives to real time communication are the MSN messenger (.NET Messenger Service, 2002) and the ICQ network (ICQ.com 2002). These chat clients provide private communication between two participants. They are both very similar and offer about the same services. The MSN messenger is included in Windows XP while the ICQ client can be downloaded from Internet (ICQ.com, 2002). The very popular IRC client, the mIRC, can be found and downloaded from the Internet (mIRC, 2002).

IT-Requirements

The course is intended to be an online course. The start version of the web based course portal can also be distributed on a CD instead of being hosted by a web server. For online viewing, a permanent high bandwidth (or broadband) Internet connection is recommended. However, it is possible to view the course using an ISDN line or even a modem dial-up connection. The parts of the course containing flash animations will of course not load very fast on a dial-up connection.

Server side

The course is hosted by a web server, preferable by an Apache server (The Apache Software Foundation, 2002), running on Linux, with integrated support for SSL (OpenSSL, 2002) and smart card authentication. The Finish electronic identity card (FINEID) can be used to identify users and to authenticate them. The access information has to be looked up in an LDAP directory (OpenLDAP, 2002). If the authentication is successful, the user will be granted access to the web server. The web server needs proper configuration for the PKI (or smart card based) authentication to work. However, old fashion password authentication is also possible to use.

Client side

The user needs a new version of a web browser with a Flash Player in order to correctly view the course. Internet Explorer provides the best support for the course layout. To be able to hear the audio in the animations, a standard sound card and loudspeakers are needed.

For communication purpose, the user needs an email client and additionally also an IRC-client (or any other real time communication client) for real time communication. To read the conferencing area and message board of the course a news client is needed. The news client is often integrated in the email client. Access to the online course will only be given students registered at the Finnish Virtual Polytechnic.

Teaching and Learning Experiences

This chapter presents test course experiences, from both student and teacher perspective, as well as general experiences from the whole course development process. The student feedback is gathered from an assessment form, which the students filled out at the end of the test course, and from interviews with test course students. The teacher experiences are mainly gathered from interviews with the test course teacher.

This chapter also presents course development experiences, changes already made to the course and further course development planned based on the course experiences. This information is gathered from the test course teacher and the course development team.

Test course experiences

Totally 33 students enrolled to the test course, held in spring 2003. 19 students completed the first half of the course. In the final exam attended 6 students of whom all passed the course with good grades.

Student experiences

The students filled out an assessment form to give the course development team information about what is good about the course and which areas need further development. The assessment form gave both praises and criticism to the test course.

The students praised the course contents for covering a broad area of network security and the course environment for being well implemented and structured. Also the freedom of not being bound to classroom schedules together with mandatory weekly assignments was considered positive.

The criticism was mainly about the low number of credit units compared to the amount of work needed in the course and about the difficulties to learn the mathematical foundations of cryptography section of the course. This feedback is supported by the fact that most of the students that didn't finish the course interrupted the test course during the study of the weekly topics about the mathematical foundations of cryptography. Criticism was also raised to the navigational inconsistency on some of the course pages. Some students also wished for more practical examples within the course material.

Teacher experiences

Most teacher test course experiences are concentrated to the process of distance teaching, how it differs from traditional classroom teaching and what new possibilities it creates.

The major challenge to the course teacher was how to get confirmation that the course students really study all the course material, not just the material that is needed to complete the exercises. Since the course is kept as a guided excursion it's important that students complete the given weekly task sets and respect deadlines.

Exercise experiences

The test course material included 22 exercises. The exercises were assigned to the student in the weekly task sets together with reading assignments related to the exercises assigned. The test course guided excursion included 17 weekly task sets with deadlines.

Student experiences

The student feedback about the exercises was mostly positive. The students thought the exercises were interesting and they liked to have the option to decide when to do the exercises. The amount of exercises was suitable, which can also be seen from the fact that almost all students – as long as they attended the course - completed all of the weekly tasks, including the exercises, assigned during the test course.

An improvement that some students suggested was some kind of automatic exercise approval system.

Teacher experiences

An issue that proved to be demanding to the teacher was how to help the students with practical exercise problems. An exercise problem, which can be easily noticed in classroom teaching, can be very challenging in distance teaching, e.g. a software configuration problem.

Another issue that proved to be a challenge was the ability to share experiences when the students are such widely geographically spread and therefore cannot easily communicate directly with each other. This communication was done through an FAQ (Frequently Asked Questions) page on the test course portal, but in practice this FAQ page didn't correspond to guidance needs.

Influence of test course on the course content

The course content was updated during and after the test course. Following sections were added to the course material; section "Cryptographic Hardware" to chapter "Cryptography and Network Security" and section "Design of Secure Software" to chapter "Network Security Software". The content of chapter "Network Security Administration" was expanded.

Further Course Development Needs

Based on teacher and student experiences from the test course, further development of the virtual course "Network Security" is planned.

At present the communication between students and teacher is done using email and SMS-messages. This type of communication is only semi-real-time and does only allow communication in written form. This type of communication has proved to be insufficient when it comes to virtual teaching and exercise supervising. The implementation of audiovisual real-time communication to the course is therefore planned. Pure real-time audiovisual communication between students and teacher is hard and expensive to implement. For that reason the course development is concentrated on implementing the use of several technologies in conjunction and by that creating an environment that better supports virtual teaching and exercise supervising. The technologies considered are point-to-point video communication, web casting, telephony and online chat.

The guidance of the course exercises is an area where further development will take place. Based on the problems that the test course students had with the exercises, the basic instructions to the exercises will be developed to avoid unnecessary misunderstandings when it comes to understanding what needs to be done in the exercise. Ready-made special instructions will also be made to help the students solve the most common problems in every exercise.

A constant course development area is the course material. The course material needs to be constantly developed and updated in order to correspond to current state-of-the-art in network security knowledge and skills. The teaching process will be improved to make it easier for the students to learn and for the teacher to teach. This development is mainly based on feedback from course students. Special efforts will be directed to develop the mathematical foundations of cryptography section of the course. That section will be complemented with more examples and animations to support its theoretical context.

As a solution to the relation between credit units and work needed there were student suggestions of splitting the course into a practically oriented network security course and a theoretically and methodologically oriented cryptography course.

Course Development Experiences

The development of a course held on a virtual learning platform has been and is a challenging task. It has proved to be both demanding and rewarding to the development team to build up a course from scratch. The process has also given the involved students insight into the processes of designing and teaching a virtual course.

It has been very resource demanding to build up a course with such wide contents as the Network Security course. It would have been impossible to design the course within the timeframe for the course development process without the contribution from the students involved in the course development process.

Conclusions

The production of a virtual course is a much more demanding task than the production of an ordinary course. Experts, like graphical designers, have to be included in the production team. Before the course is in its final form many prototypes have to be tested and feedback from the students is needed. A proper choice of computer software and IT technology is necessary. Finally, a sufficient and realistic budget is essential.

References

.NET Messenger Service (2002). *Free Instant Messaging service*. Retrieved November 29, 2002 from the World Wide Web http://messenger.microsoft.com/default.asp?mkt=en-us

The Apache Software Foundation. (2002). Retrieved November 29, 2002 from the World Wide Web http://www.apache.org

Bluetooth. (2001). The Official Bluetooth Wireless Info Site. Retrieved November 29, 2002 from the World Wide http://www.bluetooth.com/

ETSI Hiperlan/2 standard. (2002). *ETSI - Telecom Standards*. Retrieved November 29, 2002 from the World Wide Web http://www.etsi.org/frameset/home.htm?/technicalactiv/Hiperlan/hiperlan2.htm

FINEID. (2002). *Population Register Centre*. *The Electronic ID Card*. Retrieved November 29, 2002 from the World Wide Web http://www.fineid.fi/default.asp?todo=setlang&lang=uk

FINEID-specifications. (2002). *Population Register Centre - Technical information*. Retrieved November 29, 2002 from the World Wide Web http://www.fineid.fi/default.asp?path=4%2CTechnical+information%2F8%2CStandards&file=0%2CFINEID%2Dspecifications%2Elink&template=

The Finnish educational system in a nutshell. (2002). Retrieved November 29, 2002 from the World Wide Web http://www.tokem.fi/ects/Information_on_Finnish_Educati/body_information_on_finnish_educati.html

Götz, V. (1998). *Color & Type for the screen*. Crans: RotoVision SA

Home, R.F. (2002). HomeRF Working Group, Inc. Retrieved November 29, 2002 from the World Wide Web http://www.homerf.org/

ICQ.com. (2002). *ICQ Inc*. Retrieved November 29, 2002 from the World Wide Web http://web.icq.com/

IEC International Electrotechnical Commission. (2002). Retrieved November 29, 2002 from the World Wide Web http://www.iec.ch

IEEE 802.11, Working Group for Wireless Local Area Networks. (2002). *IEEE Standards Wireless Zone – Overview*. Retrieved November 29, 2002 from the World Wide Web http://standards.ieee.org/wireless/overview.html#802.11

IETF The Internet Engineering Task Force. (2002). Retrieved November 29, 2002 from the World Wide Web http://www.ietf.org

IP Security Protocol (ipsec). (2002). Internet Engineering Task Force (IETF). Working Group. Retrieved November 29, 2002 from the World Wide http://www.ietf.org/html.charters/ipsec-charter.html

IRC.org. (2002). Internet Relay Chat. Retrieved November 29, 2002 from the World Wide Web http://www.irc.org

ISO International Organization for Standardization. (2002). Retrieved November 29, 2002 from the World Wide Web http://www.iso.ch

Macromedia - Flash MX. (2002). Retrieved November 29, 2002 from the World Wide Web http://www.macromedia.com/software/flash/

mIRC. (2002). An Internet Relay Chat program. Retrieved November 29, 2002 from the World Wide Web http://www.mirc.com

Mullet, K. & Sano, D. (1995). *Designing visual interfaces*. Mountain View, CA: Sun Microsystems, Inc.

Nyberg, R. & Strandvall, T. (2000). *Utbilda via Internet*. Att hitta en plattform för kursproduktion på Internet, 180-200. Vasa: Ykkös-Offset.

OpenLDAP. (2002). OpenLDAP Foundation. Retrieved November 29, 2002 from the World Wide Web http://www.openldap.org

OpenSSL: The Open Source toolkit for SSL/TLS. (1999). The OpenSSL Project. Retrieved November 29, 2002 from the World Wide Web http://www.openssl.org

RSA Laboratories. (2002). PKCS #11 - Cryptographic Token Interface Standard. Retrieved November 29, 2002 from the World Wide Web http://www.rsasecurity.com/rsalabs/pkcs/pkcs-11/index.html

RSA Security Inc. (2002). Retrieved November 29, 2002 from the World Wide Web http://www.rsasecurity.com/

Stallings, W. (2002). *Cryptography and Network Security. Principles and Practice*. Third Edition. USA: Prentice Hall.

The Virtual Polytechic of Finland www.virtuaaliamk.fi. (2002). Retrieved November 29, 2002 from the World Wide Web http://www.tpu.fi/virtuaaliamk/index_eng_tiedostot/v3_document.htm

What is WAP? (2002). Open Mobile Alliance Ltd. Retrieved November 29, 2002 from the World Wide Web http://www.wapforum.org/what/index.htm

Biographies

Laura Bergström, BSc in Media Culture from Arcada Polytechnic, Espoo Finland. Since March 2002 she works for Arcada Polytechnic as graphical designer in virtual education development.

Kaj J. Grahn, Dr. Tech., is presently senior lecturer in Telecommunications at the Department of IT and Electronics of Arcada Polytechnic, Espoo, Finland. He is also Program Manager of the Electrical Engineering Programme.

Krister Karlström is a BSc (Eng) student in Information Technology at Arcada Polytechnic, Espoo Finland. Since May 2002 he works for Arcada Polytechnic as research assistant in network security research and virtual education development.

Göran Pulkkis, Dr. Tech., is presently senior lecturer in Computer Science and Engineering at the Department of IT and Electronics at Arcada Polytechnic, Espoo, Finland.

Peik Åström, BSc (Eng) in Electrical Engineering and Information Technology from Arcada Polytechnic, Espoo Finland. Since May 2002 he works for Arcada Polytechnic as research assistant in network security research and virtual education development.