A Virtual Course on Network Security

Laura Bergström, Kaj J. Grahn, Krister Karlström,
Göran Pulkkis, and Peik Åström
Arcada Polytechnic, 02130 Espoo, Finland

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

Abstract

This paper presents a virtual course on network security. The course has been produced in a production circle of Virtual Polytechnic of Finland. A detailed description of course development and course content is given. The chosen didactical approach is outlined. The graphical design of the learning platform is presented and motivated. The IT technology and the IT infrastructure needed to implement and use the learning platform of the course are described and assessed.

Keywords: network security, distance education, learning environment, learning platform, graphical web design

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
- defence 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

Paper Accepted as a Best Paper

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 Virtual Polytechnic of Finland

The Finnish educational system in a nutshell is illustrated in Figure 1. Compulsory basic education at

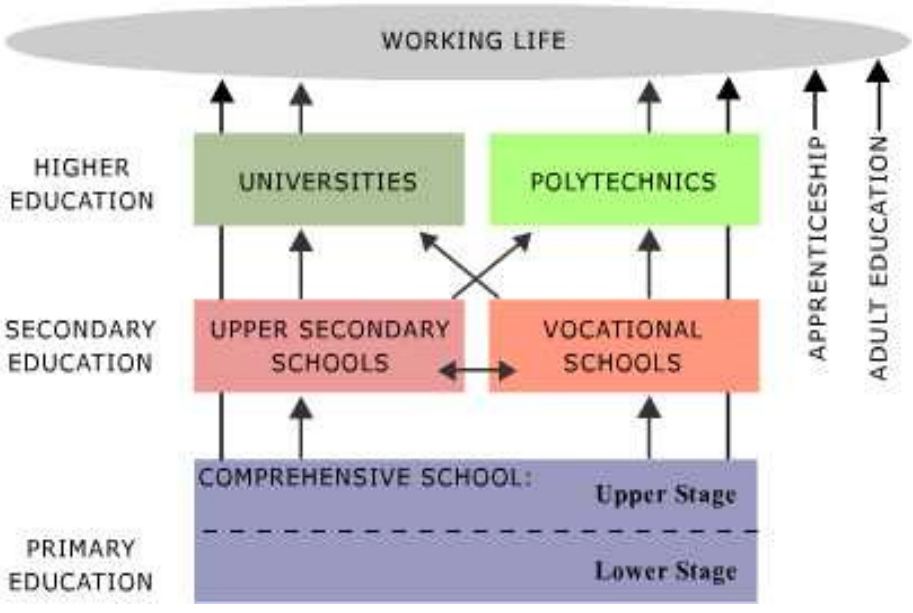

Figure 1. The Finnish educational system

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 in a nutshell, 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 Virtual Polytechnic are: (The Virtual Polytechnic of Finland, 2002):

- Virtual Polytechnic is common for all Finnish Polytechnics
- It produces and provides high level learning services
- Virtual Polytechnic uses modern information and communication technology
- 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 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 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 circle

The Virtual Polytechnic of Finland has 31 polytechnics as members and a potential of 120000 students and 6000 teachers. Content production is being done in 28 production circles. The aim is to have virtual courses of more than 200 credit units. The network security course is produced in the production circle Computer Networks, Telecommunication and Telecommunication Systems. The total amount of credit units in this production circle is 10.

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, 2 IT students and 1 graphical designer. The effort needed to develop the course:

- both IT teacher have worked 4-5 hours/month during about 10 months to plan the course, with content production, and to supervise the 2 IT students and the graphical designer

- both IT students have worked about 20 hours/month during 6 months with content production for the course
- 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)

Animations are produced using Macromedia Flash 5 (.swf)

The course material has been organized in modules. Course testing and evaluation will be done by the production circle, 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 eight chapters that include the total course material. An Index and a Website Map provide navigation options.

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. The course content structure developed by the course production team is different from the chapter division of the course book. All topics of the course are not treated in the course book and all topics of the course book are not covered by the course.

Chapter 1 - Introduction

The introduction chapter is a short and illustrative overview of the course. An interactive audiovisual presentation takes the user on a journey through the chapter consisting of

- Main Introduction
- Taxonomy Diagram
- Network Security Threats

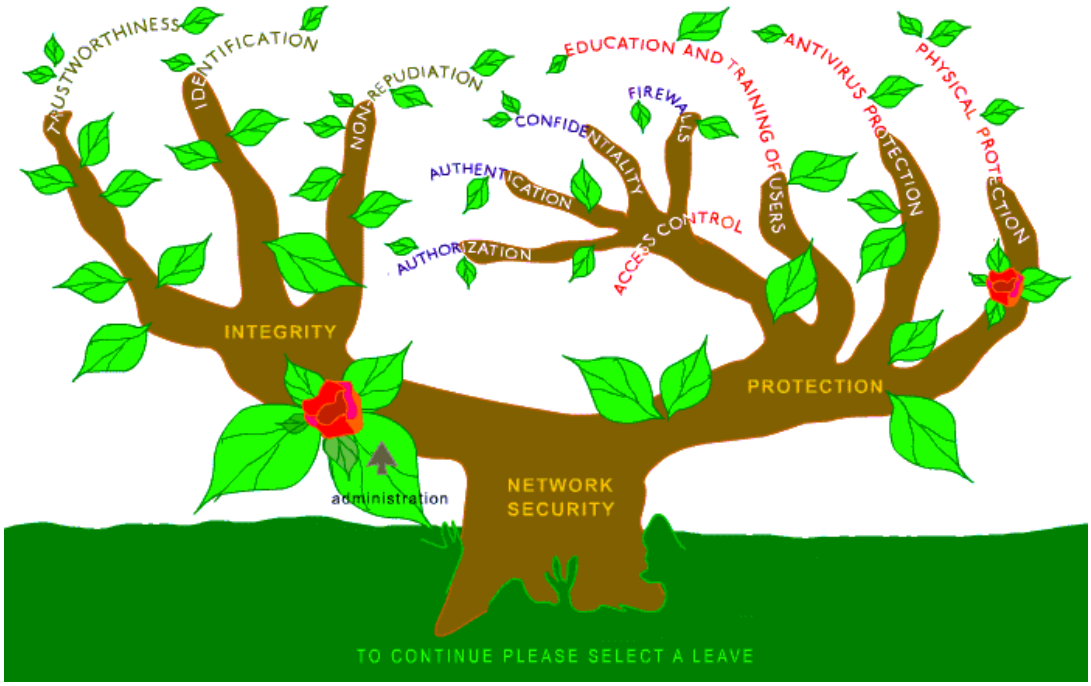

Figure 2. The interactive animated Network Security tree.

- Features of Secure Networks.

"Main Introduction" summarizes the course and gives the user concepts and information needed in all chapters.

"Taxonomy Diagram" shows the fundamental properties of network security - integrity, protection, and security administration – as an interactive, animated Network Security tree (Figure 2). The main branches of this tree are Integrity and Protection. Both man branches have many sub-branches, which

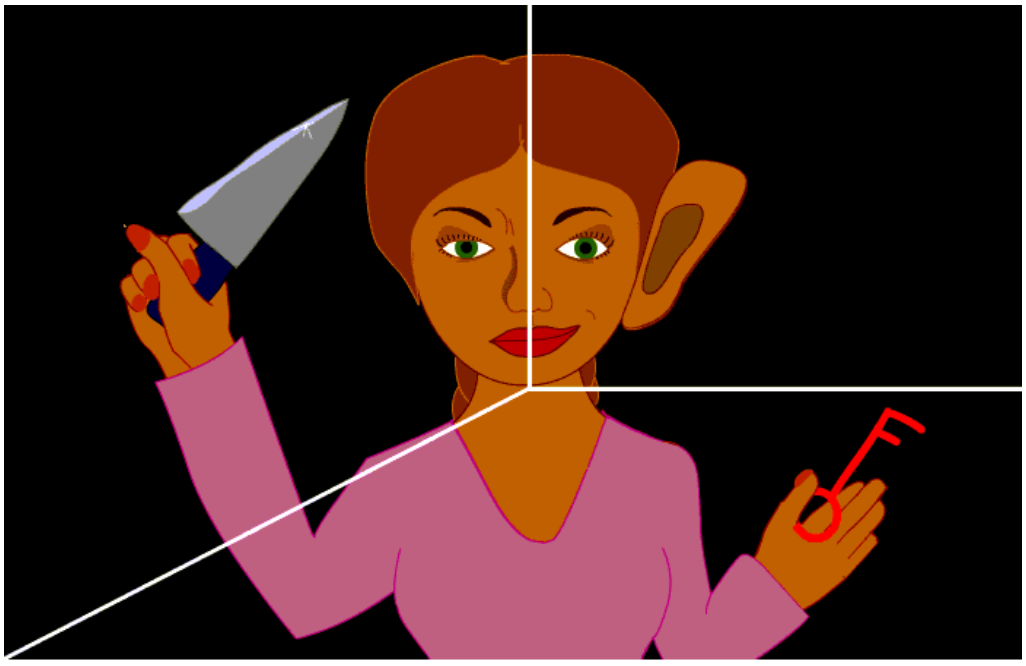

Figure 3. Interactive animation of network security threats.

represent the variety of the fundamental properties. The leaves covering the whole tree visualize Security Administration, which is needed everywhere.

“Network Security Threats” is a classification consisting of damage, eavesdropping, and intrusion. By activating sectors of an interactive audio-visual animation (Figure 3) the user gets advice how to manage these threats.

“Features of Secure Networks” 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

“Features of Secure Networks” is an interactive graphical animation for highlighting features of a network security architecture (see Figure 4).

Chapter 2 – Network Security Administration

In the Network Security Administration chapter Administrative security issues are presented in combination with information about user education needed to achieve network security. Standardization organizations and standards related to network security are also presented. The issues covered are:

- Security Policy

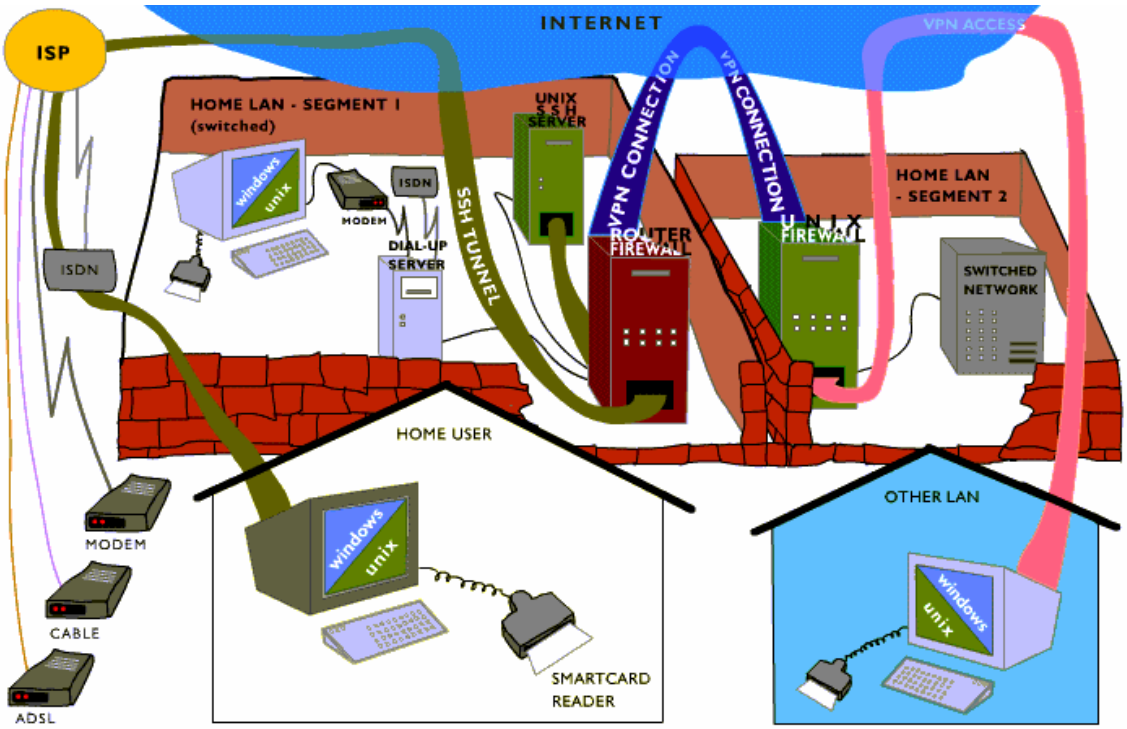

Figure 4. Interactive animation of a network security architecture.

- Intrusion Detection
- Vulnerability Assessment
- User Support and Education
- Security Incident Response Teams
- Network Security Standards.

A well-defined security policy managed by a security team is the basis for network security administration. The security policy defines the network security goals and responsibilities as well as the administrative procedures and methods needed to achieve these goals.

The concept of "intrusion detection" and the software needed for intrusion detection is presented. The use of intrusion detection software is vital for the identification of security breaches in the network.

Vulnerability Assessment Systems are used as a complement to intrusion detection. Security vulnerabilities like configuration errors and system problems can be found using these systems, which are presented in the "Vulnerability Assessment" section.

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.

Both international and national standardization organizations are presented in the "Network Security Standards" section. This provides the user with a picture of the wide range of different security standards. 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) are presented. The concept of network security standards is a very broad subject, stretching from physical network components to software and protocols.

Chapter 3 – Anti-virus Protection

This chapter describes different types of malicious programs with emphasis on how they behave and how they are spread. Virus characteristics and the activity phases of viruses are also explained. Viruses are classified by the way they propagate and behave. The historical development of antivirus protection is presented starting from simple scanners to advanced modern methods. The anti-virus protection levels needed for optimal network wide anti-virus protection are outlined and illustrated with examples. The importance of an anti-virus strategy is pointed out together with the necessity of updating the virus definitions. The "Anti-virus Protection" chapter is implemented as an interactive hypertext animation with text and pictures (see Figure 5).

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 network. The Firewall chapter consists of six sections:

- Design Goals
- Access Control Methods
- Firewall Types

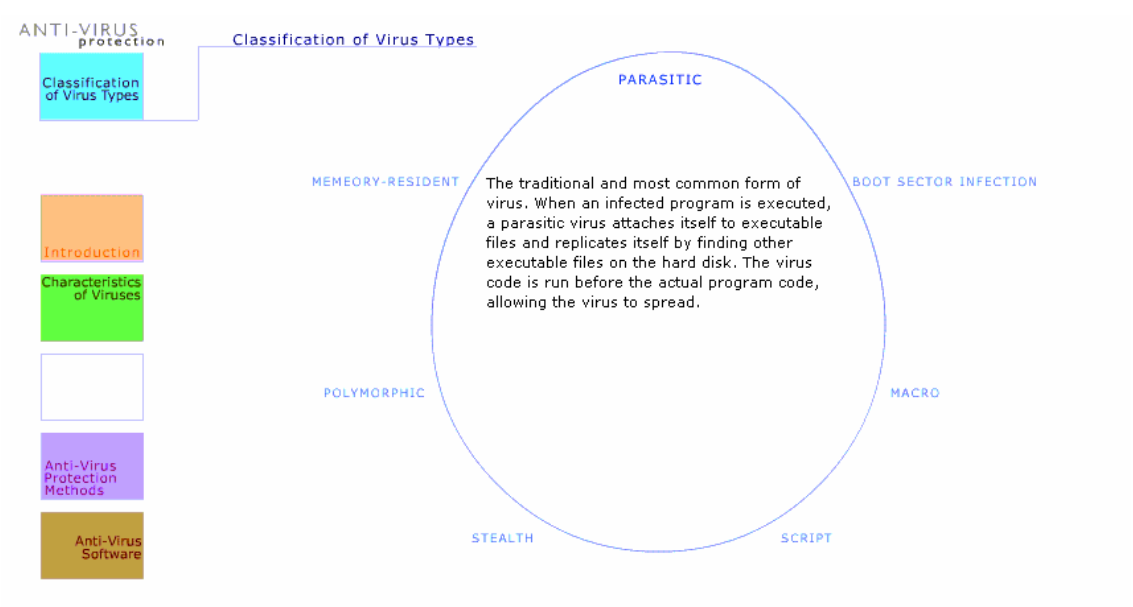

Figure 5. Interactive animated presentation of anti-virus protection.

- Firewall Configurations
- Firewall Platforms
- Firewall Software.

The “Design Goals” section describes the reasons to use a firewall and the operation principle of a firewall. The firewall must of course prevent penetration to the firewall itself.

A firewall implements access control with four network traffic filtering techniques:

- Service control
- Direction control
- User control
- Behavior control

The “Access Control Methods” section gives a basic understanding of these techniques.

Firewalls can be classified into three types:

- Packet Filtering Router
- Application Level Gateway
- Circuit Level Gateway

The operation principles and security features of these firewall types are described in the “Firewall Types” section.

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 firewall implementations and the “Firewall Software” section presents available firewall software.

The “Firewalls” chapter is implemented as an interactive hypertext animation with text and pictures (see Figure 6).

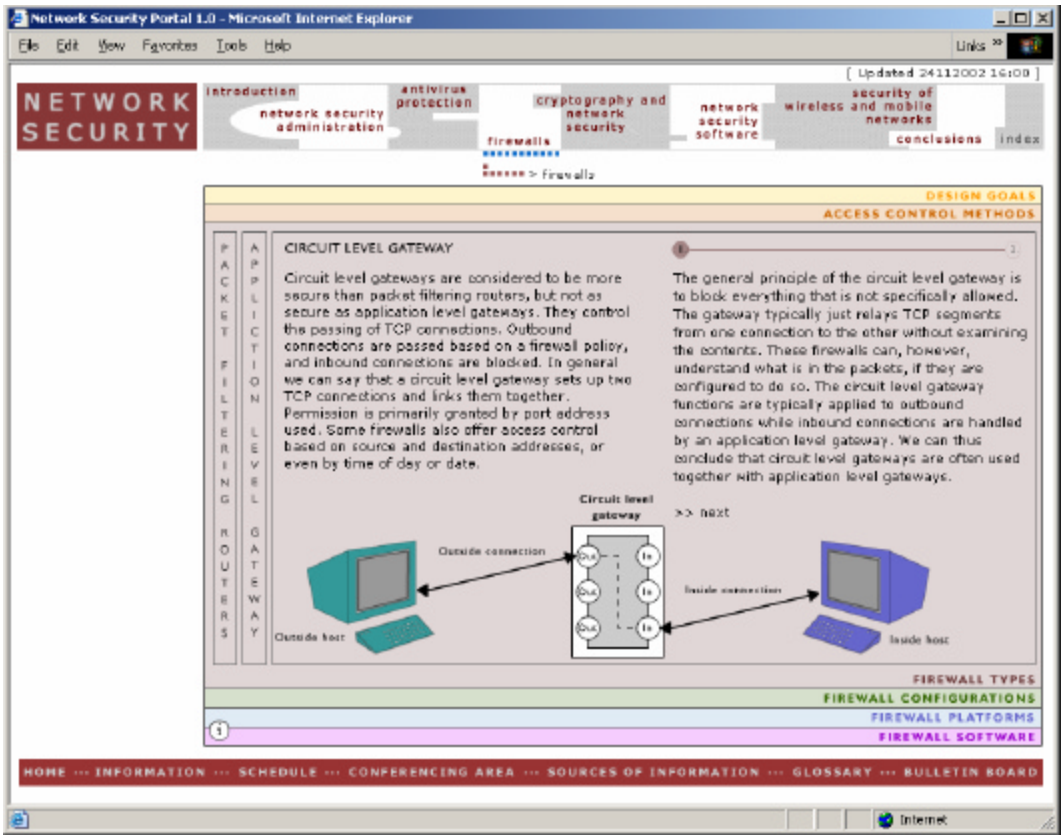

Figure 6. A screen from the Flash implementation of the “Firewalls” chapter.

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 consists of six sections:

- Introduction to Cryptography
- Theoretical Foundations
- Cryptographic Algorithms
- Cryptographic Protocols
- Encryption Key Management
- Cryptographic Software

The first section describes the idea of cryptography with an animated audiovisual slideshow. The "Theoretical Foundations" section presents the theoretical background of modern cryptography: information theory, complexity theory, integer algebra, modulo arithmetic's, factoring, prime number generation, primality testing, secure random number generation, elliptic curves, etc.

The "Cryptographic Algorithms" section contains a detailed characterization of the fundamental cryptographic algorithms, the secret key algorithms, the public key algorithms, and the hash algorithms. 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 data flow logistics of the Diffie-Hellman key agreement protocol and the Kerberos authentication is also visualized by audiovisual animations.

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 "Cryptographic Software" 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 use of hardware security tokens like SIM card chips, smart card chips, and USB tokens is also covered.

Chapter 6 – Network Security Software

This chapter merges the information about software from the other chapters in the course. It contains information about:

- Security Administration Software
- Anti-Virus Software
- Firewall Software
- Cryptographic Software
- Security Software Development.

The "Security Administration Software" section covers software for intrusion detection, for vulnerability assessment, and for management of other security software. The "Anti-Virus Software" section outlines anti-virus defense levels and available software for each level. The "Firewall Software" section surveys available firewall software. The "Cryptographic Software" section surveys network security software and secure network applications. The last 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.

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.

Chapter 8 – Conclusions

The chapter summarises the course and underlines the most essential network security issues. Technologies, protocols, and administration must be properly combined to provide network security. The quality of network security is as good as the weakest link in the security architecture.

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 a maintainer of the web based learning environment provides the guidance.

The course proceeds with topical study directives and exercises distributed weekly to the course participants using email and the web based course portal. Weekly exercises are configuration, installation, calculation, testing or programming tasks or topical quizzes. Each exercise has a deadline. Access to parts of the learning environment is obtained by doing authentication exercises.

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.

User level skills

Every user of computer and computer network needs certain network security skills. This means in practice, that fundamental security policy issues control all computer use. Examples of these issues are

- awareness of the significance of antivirus protection and skills to perform virus scans with installed antivirus protection software
- familiarity with the basic principles of firewalls, skills to install and use firewall software for protection of a workstation connected to a public TCP/IP network
- ability to manage settings of network security software embedded for example in web browsers and remote access software like SSH.
- familiarity with the basic principles of PKI. This covers understanding of security certificates, protected web page browsing skills like management of certificate stores and other security settings in web browsers (see Figure 7), email protection skills like email message signing and signature verification (see Figure 8).

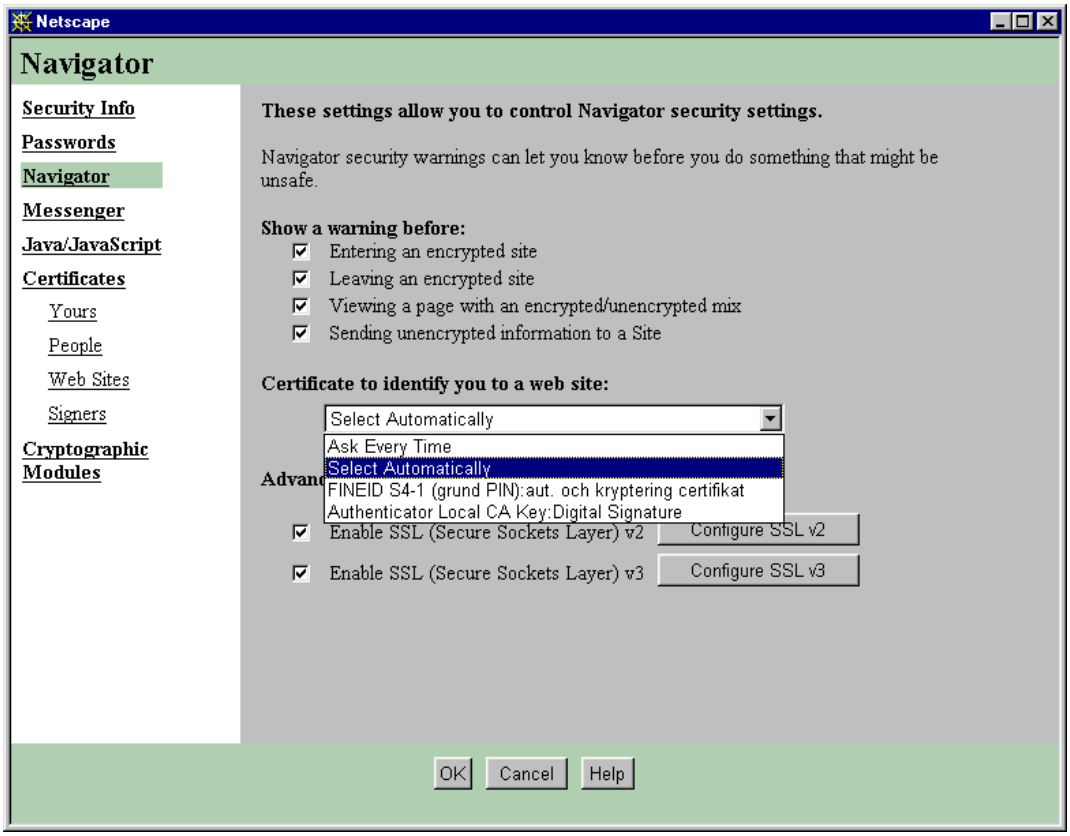

Figure 7. Security settings in Netscape Communicator v4.79.

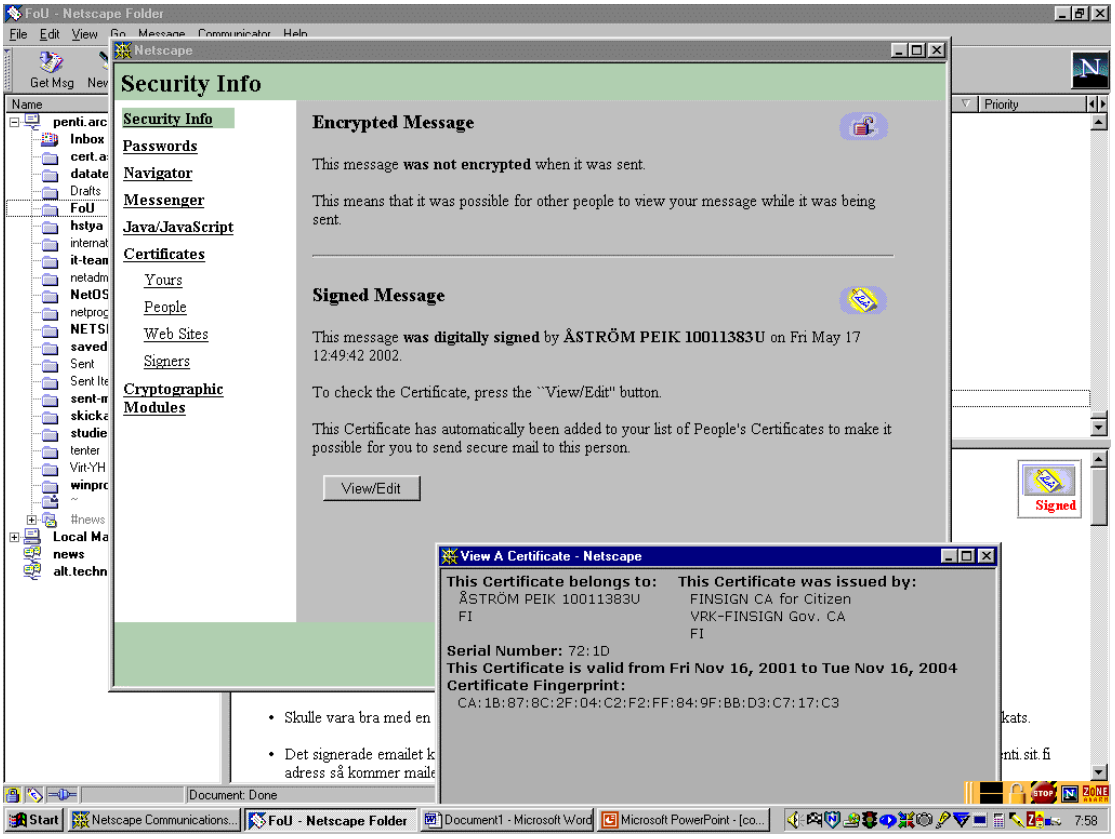

Figure 8. Inspection of the signature of a signed email message in Netscape Messenger v4.79.

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.

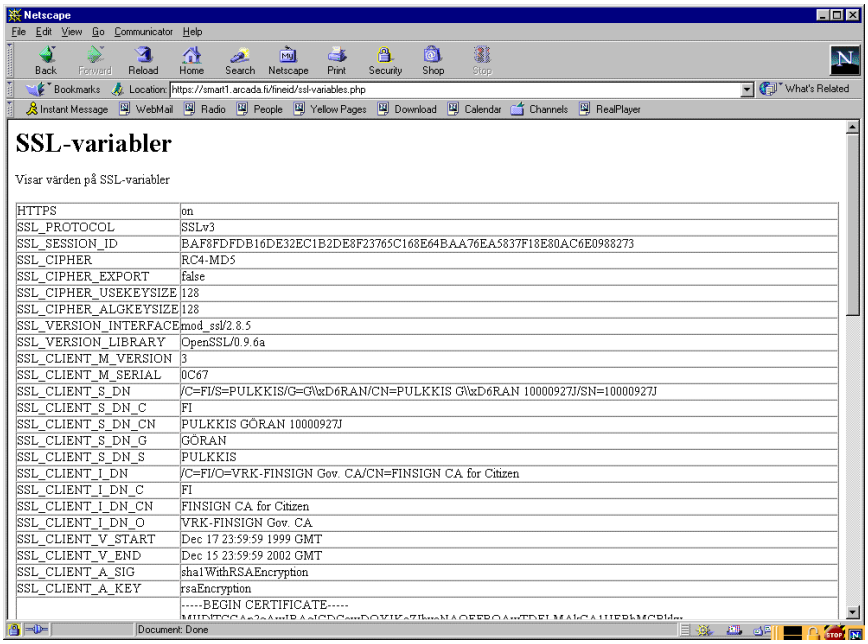

Figure 9. SSL variables in the configuration file of a web server configured for HTTPS – the secure HTTP protocol.

Application Development Level Skills

The highest level of network security skills in *polytechnic education* is the **application development level**. In 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 skills 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 Platform

Background and Presentation

The aim of the course is learning and the target group is students of computer and telecommunication engineering. The starting point of the design of the Learning Platform 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 Platform 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 PlugIn, which that 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 Platform. 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. Communication goals are more easily achieved with a strong esthetical structure (Mullet & Sano, 1995). This means that these two dimensions are very much dependent of each other and together they make the Learning Platform, which is a website.

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 Platform. This means that the design should be carefully planned and the same throughout the whole website. The description of the interface consists of

(1) the usability of the website and

(2) the comprehensibility of the course.

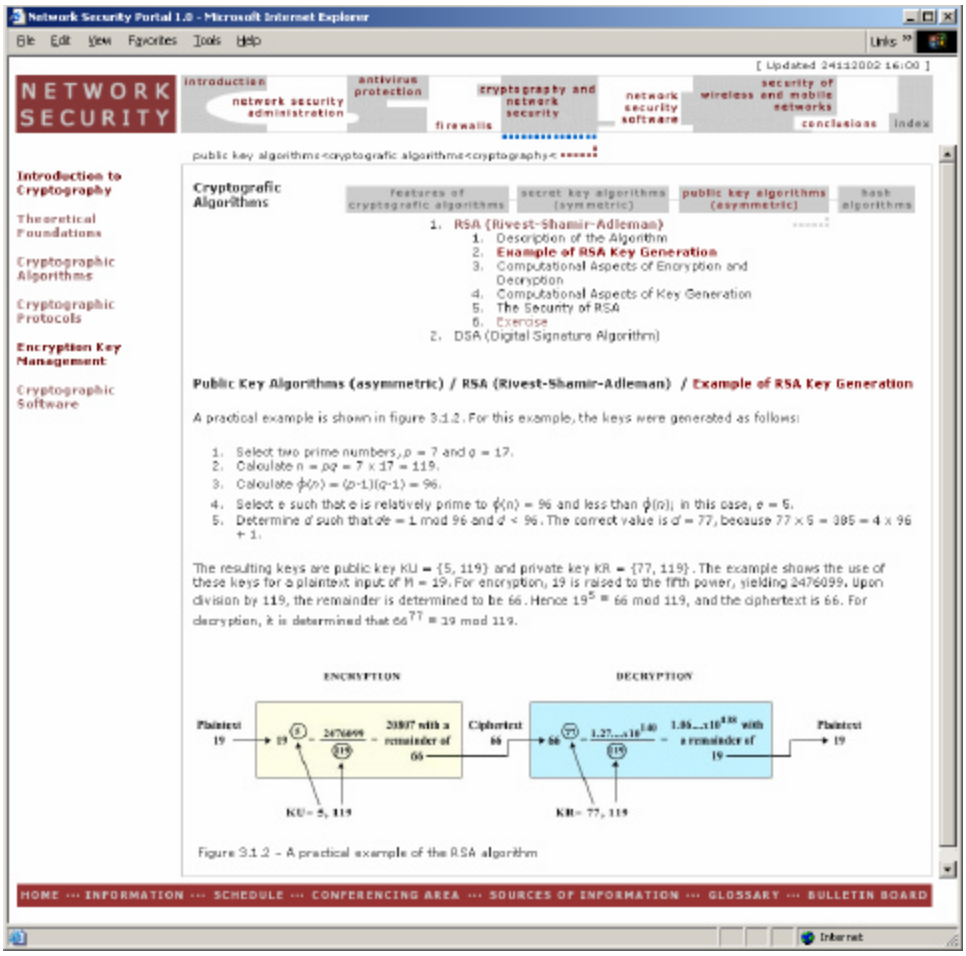

Figure 10. A Print Screen of the layout when a page from Chapter 5 is selected.

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

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

(2) the *elements of interaction* between student and teacher and

(3) 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 the most visited page of the user.

The navigation on the website. The navigational system consists of two main parts,

(1) the informative part that is the navigation of the course and

(2) 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 at the homepage of the website when the Learning Platform entered. The homepage is composed of three frames: top, middle and bottom frame (see Figure 10). The user can find two menus on this page, (1) one formed like a puzzle in the top frame

and (2) 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 other menu, so that 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 therefore both main menus are always visible.

The top menu contains eight puzzle pieces describing the seven chapters of the course and the index. All chapters except conclusions (chapter 8) and 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 chapter pages 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 sub-submenu of a chapter submenu is placed on the top of the right frame. By doing this all menus, the two main menus, the submenu and the sub-submenu, of a chapter are always visible. The page opened from a submenu is placed into the right frame of the middle frame under the main top menu, and has a marker on the top of the page pointing out what chapter the contents belongs to. The path to the current page is also written in the heading of the page, shown in the right frame of the middle frame – for example *chapter 4 / submenu 3 / sub-submenu 2 / header of the page*. To highlight the path of the current page even more, the sub-submenu where the page that is currently open is situated is highlighted with a red color. The same red color is used for all still unvisited text hyperlinks (more about hyperlinks in the part 'The comprehensibility of the course').

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, which can be used independently on the web, the Network Security Course needs a learning platform. This means that the website needs elements for interaction between the student and the teacher (Nyberg, 2000). These elements can be found in the bottom menu and on the start page. Elements in the menu represent information widely used throughout the course. Elements on the start page or behind hyperlinks on the start page represent information that the student will need less and maybe just in the beginning or at the end of the course.

The elements in the menu are

(1) information about the teachers and tutors, links to services like registration, transcripts, guidance etc,

(2) a calendar outlining the significant events of the course,

(3) an un-moderated newsgroup is used as a conferencing area where students and teachers can meet for discussions. Real time chat, IRC, will also be used (see 'IT Infrastructure of the Learning Platform'),

(4) sources of information,

(5) a FAQ for student feedback and questions with answers and comments of the course guidance team members. This FAQ is updated as the course proceeds.

(6) a bulletin board, which is a moderated newsgroup (see 'IT Infrastructure of the Learning Platform').

The start page contains

(1) the most essential information about the course, including the name, title and the needed information of organiser,

(2) a list of credits naming everyone who has been working on the project,

(3) a date of last update,

(4) the course requirements,

(5) the course overview,

(6) the assignments of the course that can also be found in the course schedule page,

(7) the resources of the course and

(8) a form for course evaluation.

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, is on the left. The index on the right is a list of links to pages inside the website. On opening the index page shows only the chapter headlines. Selecting of a header opens the submenus for the chapter. If a submenu has sub-submenus, they are shown when selecting the submenu. The index shows only the submenus of one chapter at a time. If another chapter than one already open chapter is selected, then the earlier opened chapter is automatically closed.

The use of the 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 index of exercises was however important enough to reserve an own frames page for each exercise. The frame page with the selected exercise is then directly opened from an exercise link. If wanted, the user can continue from here as normal using the course, and no difference in the structure will be noticed.

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. The submenus are text hyperlinks while both the main menus and all the sub-submenus are graphical. The color of the text hyperlinks is the same red as used in the high lightning of the sub-submenus. Already visited text hyperlinks remain light red. Because the top menu is graphical, it leaves no trace of visited links. Therefore the feedback for a visited link in the top menu is a line of blue dots below the puzzle piece for the visited chapter. This feedback is supported only in Internet Explorer. The dots disappear when the page is reloaded.

To stimulate all senses of the student for learning the course contains pictures, animations and audio. This increases the variation of the content and makes the student more interested and motivated. All pictures are drawn and all animations are created with Flash 5, but the gif graphics in the menus are designed with Photoshop. The static graphics is mostly gif graphics. All audio sequences belong to animations. The spoken text is also shown besides the animation.

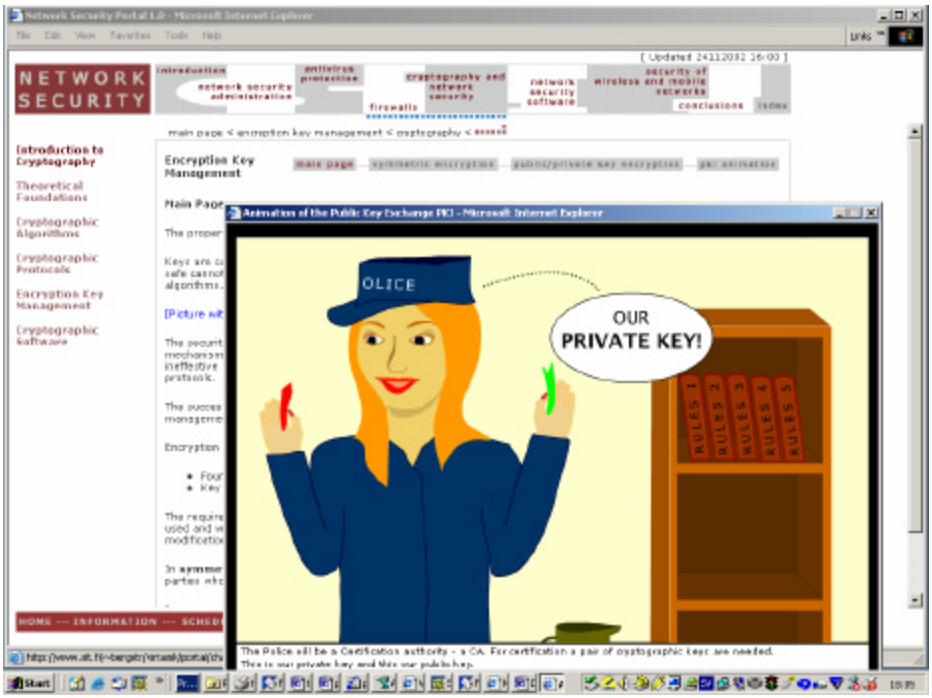

Figure 11. The animations are opened in a separate window.

For clarity all links from any content page 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:

(1) the visual structure

(2) the colors

(3) the font type

Visual structure

The keywords for visual structure are

(1) elegance and simplicity,

(2) contrast and proportion,

(3) organization and

(4) space.

The unity of the pages and the design of the elements create an elegant website. In the course material pages the style of the HTML pages remains the same throughout all the chapters. This also applies to the submenu, the sub-submenu, 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. Strong colors were avoided, because they can create after imagines in the user's eyes. 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, for example the bottom menu that is 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.

Colors also have conscious or unconscious psychological effects on the user, depending subjective experience and moods. Below is listed some effects of the colors which are used on the website (Götz, 1998):

(1) black stands for elegant, firm and negative,

(2) white for affirmative, open and pure,

(3) gray for neutral and unemotional,

(4) dark red for graceful, serious and dignified, and

(5) blue for controlled, intellectual and cold.

The font type

The font type used in the html pages is Verdana (Arial). The normal text is dark gray and the size is 11 points. This is a font without serifs unlike Times New Roman that is a grotesque font and has serifs. Example: Verdana vs. Times New Roman. On web pages this font is found to have a better legibility. In Flash modules (animations) the font Arial Narrow is used, since it has a better legibility than Verdana in a published Flash movie (the outcome of a Flash file and the one that is shown to the user). The font

used in the graphics and in the pictures is Verdana. When a word or a phrase is highlighted it is bolded instead of, for example, underlined to distinguish it from a hyperlink.

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 Virtual Polytechnic

The registration process will be handled by the Virtual Polytechnic of Finland's student office, which will probably be an electronic online office. Once the users have registered, and received their student place, the Virtual Polytechnic of Finland 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 Virtual Polytechnic of Finland 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 preferable 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 Virtual Polytechnic of Finland.

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 on 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 provides 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 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 need proper configu-

ration 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 Virtual Polytechnic of Finland.

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

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 fromthe 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=

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

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

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

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.

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.

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

Krister Karlstöm 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

Peik Åström is a BSc (Eng) student in Electrical Engineering and 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.