INFORMATION SYSTEMS SECURITY EDUCATION FOR FUTURE TEACHER AT SECONDARY AND PRIMARY SCHOOLS

Ladislav BERANEK

Abstract: *Information systems security includes a number of computer science disciplines, from operating systems and computer networks to software design and business continuity securing. This paper discusses the content of topics and the usage of selected software for the education of computer security on Faculty of Education of South Bohemian University in Ceske Budejovice, Czech Republic. Some aspects of teaching information security for future teachers of secondary and elementary schools are analysed in this paper. The aim of this subject is to provide the students, future teachers, with knowledge and skills which will be useful for their future teaching praxis and especially for improving the information security awareness amind not only secondary school but also primary school students, for example in the field of trust in Internet and other fields.*

Key words: *Information system security, laboratory education, applied cryptography, web security, information security awareness, secondary school, trust on Internet.*

VÝUKA BEZPEČNOSTI IS PRO BUDOUCÍ UČITELE STŘEDNÍCH ŠKOL

Abstrakt: *Informační bezpečnost prolíná řadou disciplín, od operačních systémů a počítačových sítí až po projektování software a zajištění kontinuity provozu informačních systémů. V příspěvku je naznačen obsah témat, používání software při výuku bezpečnosti pro cvičení tohoto předmětu na Pedagogické fakultě Jihočeské university v Českých Budějovicích. V příspěvku jsou zejména diskutovány některé aspekty výuky informační bezpečnosti pro učitele středních a základních škol, aby získali takové znalosti a dovednosti v oblasti informační bezpečnosti, které by byly přínosné pro jejich další učitelskou praxi a zejména při zlepšování povědomí o informační bezpečnosti nejen u studentů středních škol ale i žáků základních škol, například v oblasti důvěry na Internetu a dalších oblastí.*

Klíčová slova: *Výuka bezpečnosti informačních systémů, výuka učitelů středních škol, laboratorní výuka, povědomí o bezpečnosti, výuka na střední škole, důvěra na Internetu.*

Introduction

The paper deals with the description of information security education at the Faculty of Education in the South Bohemian University in Ceske Budejovice, Czech Republic. The first chapter gives a description of the content of the information security standard course, including the description of a software used at seminars in this subject. The other chapters discuss the need to incorporate an additional modulus with specific content intended specifically for teaching information security to future primary and secondary school teachers. The aim is to convey future teachers certain methodology and enable them to pass on to their students some basic principles of computer usage, especially, for example, the Internet. We are further developing this field with the assisitance of seasoned teachers with practical experience with the aim that education of information security reflect the needs of teacher's practical usage.

The content of standard course

The education of information security at the South Bohemian University in Ceske Budejovice is based on the topics which pervade a number of computer science branches, from operating systems and computer networks to software projection and ensuring of business continuity of information systems. It was necessary in education of information systems security to choose such topics which were not taught in others subjects. Following points cover the sylabus of courses of information systems security on most Czech universities that teach information science [1] with possibility to emphasis some of them:

- security architecture design (risk analysis, security policy, criterion for evaluation of information system security),
- security projection (software audit, buffer overflow, autentization methods),
- security models (reference monitor, multilevel models),
- methods of applied cryptography (encryption, keys, PKI),
- security protocols of computer networks (IPSec, S/MINE and next),
- network security (firewall, IDS),
- security of application (electronic business security, database security etc.),
- law aspects of security problems.

Mentioned areas are standard and they are covered by a number of instructional materials. Some of them are accessible only in English, nevertheless it is not a problem to provide the students with corresponding theoretic principles. The opposite situation, at least according to our experience, is in the area of practical training whose aim is to provide students with concrete ideas and skills in usage of some tools and practical experience with information security.

Feedback from teachers

The subject of information system security has been taught for two years approximately in above mentioned form. Students of computer technology teaching for secondary school entered this subject because it is centered around real-life problems, and these questions are very interesting for the students.

Approximately a year ago the subject of information system security was introduced into supplementary courses for teachers of primary and secondary schools. Education proceeded approximately according to the mentioned pattern. We realized on the basis of feedback from active teachers that it is necessary to complete the subject of information system security especially for future teachers of computer science with specific topics.

Typical computation infrastructure of secondary schools has following features:

- Traditionally “open” environment;
- Environment which is critical of „authorities“ but also with high degree of (uncritical) trust to those who understant how to manipulate students (in particular via Internet);
- Critical for students’ learning, high utilization by students;
- Higher education comprise of 15% of the Internet address space;
- Often campus-wide wireless access;
- Some students have deap technical knowledge and also praktical skills.

Secondary and primary school teachers also observed the following from the point of view of information security:

Students (secondary school) begin to be aware that the threats are real. Security incidents and attacks are publicized in daily newspapers (e.g. attempt at fishing with electronic banking). Students are also aware of problems concerning their online privacy, however they miss basic rules concerning computer security and they often do not want to accept „ rules of adults".

Some problematic areas concerning to the field of information security at secondary and primary schools in Czech Republic were chosen in cooperation with teachers, especially:

- Open environment is a fertile ground for attacks and risks,
- Web hosting and file sharing,
- Malware (e.g. viruses, worms, Trojan Horses) are becoming more sophisticated,
- Underestimation of information security by students, non-acceptance „of rules of grown-ups“,
- Often multiple roles of educational institutions,
- Acess points (wireless networks),
- Privacy, data protection,
- Poisoned Peer-to-Peer (P2P) networks and torrents,
- Malware spreading through instant messaging, social networking sites, mobile phones and SMS and MMS.

We then evaluate, again in cooperation with teachers, which problems of information security in schools are most acute given their practical experience.

Teachers (29 surveyed teachers) evaluated single problematic areas and ranked them into several specific categories that were defined this way: 0 - 4 low level, 5 - 9 middle level, 10 - 14 high level and 15 - 19 very high level of risk.

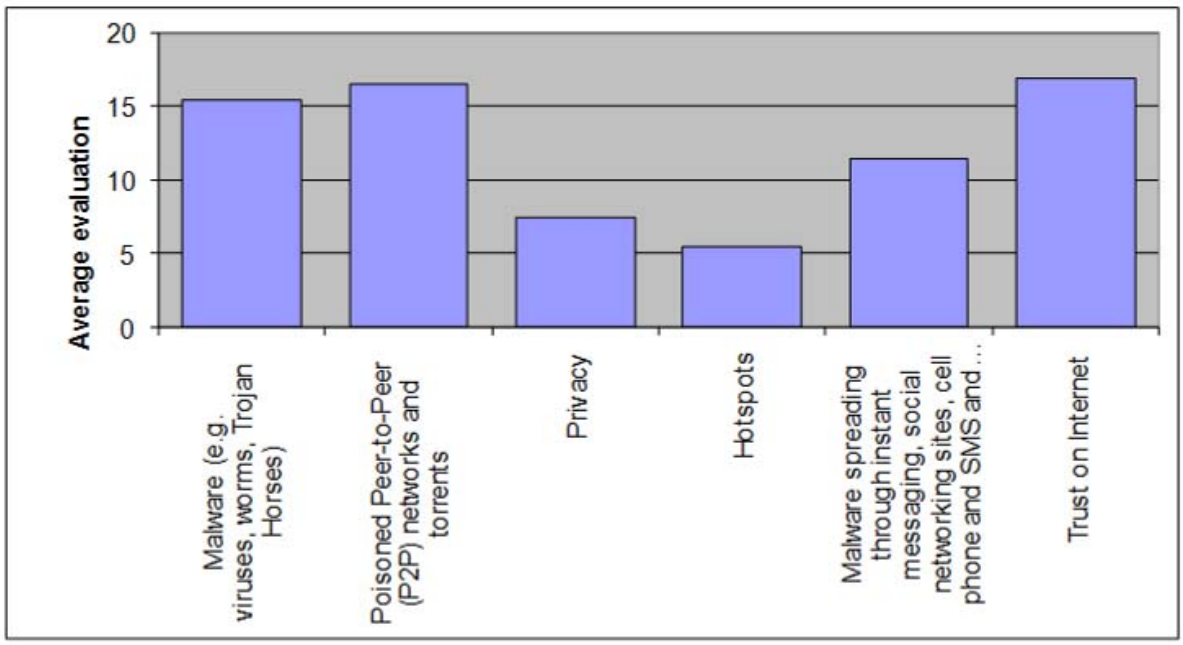

Figure 1: *Evaluation of some problematic fields.*

Proposal of modulus for completion of information security seminars for teachers.

Based on this feedback and cooperation with teachers, we modified the seminar of information security so that it reflected better topical problems of schools and would be aimed especially for education of teachers. We added some modules to the seminar. We especially tried to incorporate suitable examples within these modules, with the help of which teachers can convey the area of information security to students of primary and secondary schools. These are especially the following modules:

Module general question of information security

Procedures of general information security are taught using practical examples. For instance: computing security, like any other kind or security, tends to follow the 90/10 rule. It means that 10% of the protection is the technology, and the other 90% relies on people to know what to do and what not to do to so that the technology can do its job.

We can describe it on the bolt lock example: it is like a bolt lock on a door. The lock, itself, is the technology - the 10%. Making sure the lock is locked and the keys aren't sticking out of the lock are the remaining 90%.

Discussion and demonstration on the topic of what an attacker can do to your computer is shown on the following example:

- Hide programs that launch attacks;
- Generate large volumes of unwanted traffic, slowing down the entire system;
- Distribute illegal software from your computer;
- Access restricted information (e.g. identity theft);
- Record your keystrokes and get your passwords.

Module computer security principles

The basic procedures and behaviour of information security are discussed in this module --- for instance, the following principles:

- Back-up your data.
- Make backups a regular task, ideally at least once a day. Backup data to removable media such as portable hard drives, CDs, DVDs, or a USB memory stick. Remember, your data is valuable. How effective would you be if your email, word processing documents, excel spreadsheets and contact database were wiped out? How many hours would it take to rebuild that information from scratch?
- Use cryptic passwords that can't be easily guessed and protect your passwords - don't write them down and don't share them.

- Make sure your computer has anti-virus, anti-spyware and firewall protection as well as all necessary security patches.
- Don't install unknown or unsolicited programs on your computer.
- Practice safe e-mailing. It means: don't open, forward, or reply to suspicious e-mails, don't open e-mail attachments or click on website addresses.
- Practice safe Internet use. Example explanation can be: accessing any site on the internet could be tracked back to your name and location. Accessing sites with questionable content often results in spam or release of viruses. And it bears repeating. Don't download unknown or unsolicited programs.

Module security projects

Within this module, we tried to demonstrate examples of simple projects that the teachers of secondary schools could solve with their students and thereby manage better the area of computer security. There is nothing better then the situation when one student get knowledge of computer security from another student. Here are exaples of projects (usually for more advanced students):

- Develop Visualization Tools;
- Profiling users and traffic;
- Linking relationships;
- Network traffic classification;
- Detecting abnormalities;

Module trust on Internetu

Other current big topics have to do with trust of the Internet. According to available information, Czech children are very careless when using the Internet. Every third student admits that they already met with someone that they knew only over the Internet [6]. On the other hand, students from "old" EU countries are more careful – in these European countries only every tenth child has had this experience. Further discussion and searching for a recommendation of how teachers should explain how to trust the Internet and how to correctly behave around the Internet are the content of this module. The aim is not to preach but rather demonstrate examples of incorrect behaviour or teach different kinds of projects solving. In this module some privacy risks for social networks are discussed too.

Information security politics modulus

This modulus is intended for teachers; it is intended for facilitation of elaboration e.g. rules of the operation of computer networks or computer schoolrooms. Various demonstrations and rules for designing a security policy (for school or other educational institution etc) are the content of this, such as:

- Create a documentation of what system support staff and users need to do in respect to network and information security;
- Establish baseline security configurations for all appropriate technology platforms (e.g. web browser);
- Establish a vulnerability management process;
- Use vulnerability assessment tools to periodically conduct self-assessments;
- Monitor log files from critical systems on a daily basis;
- SANS [7] have excellent policy templates.

Conclusion and discussion

The aim of this paper was to show the problems of teaching the subject of information security to teachers so that they gain the knowledge and skills that they can put into effect in their future teacher's practice. The aim of this paper was to give an overview of education, software and topics analysed and used at teaching the subject information security at the Faculty of Education of the South Bohemian University, and its aim was also to create discussion about experiences of other interested parties that could be used in teaching the subject of information security to primary and secondary school teachers.

Experience from teaching information security to teachers evokes a number of other questions, especially:

- What preliminary knowledge students (future teachers) should have (some exercises are trained on diskless distributions of LINUX with only a command prompt),
- What other specific problems to demonstrate to these students (future teachers) from the area of information security, what procedures, programs or software,
- What knowledge should a teacher have to be able to convey students of secondary and primary schools basic principles of

information security so that the students are able to accept these,
- How can this be taught,
- Eventually next questions.

Reference

(1) DOCKAL J.: Teaching of object Information security on universities in Czech republic, 18-20, DSM VI, 4/2002 (in Czech)
(2) BERANEK, L.: Software for IS security education, Conference Pedagogical software, Ceske Budejovice 2004 (in Czech)
(3) HacmeBankTM v2.0 [online]. [cit. 2005-08-15]. Available from WWW: <http://www.foundstone.com/us/resources/proddesc/hacmebank.htm>.
(4) Paros [online]. [cit. 2008-10-15]. Available from WWW: <http://sourceforge.net/project/showfiles.php?group_id=84378>
(5) BERANEK L., KNIZEK, J.: Education of information systems security, Conference Pedagogical software, Ceske Budejovice 2008
(6) The children trust the people which they known only from Internet, the exploration proved [online]. [cit. 2008-10-15]. Available from WWW: <http://zpravy.idnes.cz/deti-veri-lidem-ktere-znaji-jen-z-internetu-ukazal-pruzkum-pa7/domaci.asp?c=A081014_215331_domaci_zra> (in Czech)
(7) SANS InfoSec Reading Room - Security Policy Issues [online]. [cit. 2008-10-15]. Available from WWW: <http://www.sans.org/reading_room/whitepapers/policyissues/>.

Ing. Ladislav Beranek, CSc., MBA
South Bohemian University
Department of Applied Mathematics and Informatics
Studentska 13
37005 Ceske Budejovice
Czech Republic
E-mail: beranek@pf.jcu.cz