From a technological focus to a human emphasis: re-introducing the end-user in information security education

Jorma Kajava
University of Oulu, Department of Information Processing

Rauno Varonen
University of Oulu, Language Center

Jorma.Kajava@oulu.fi
rvaronen@cc.oulu.fi
BOX. 3000, FIN - 90014 Oulu University
BOX. 7200, FIN - 90014 Oulu University

Keywords: *Information security education, end-user perspective*

Abstract: *The end-user oriented perspective to information security education is a new way of motivating students. It is essentially a human-oriented approach ranging from guidelines and awareness to management and ethics. In this paper, we first present an educational model and a matrix for teaching. Then we will expand our approach to include encryption and network security related educational modules, because current technological changes are shifting the main emphasis in security education toward increased end-user security awareness. Rather than narrow-minded specialists, the IT industry needs people who understand the multifaceted nature of security and are able to apply their knowledge in their daily work. The work reported in this paper is based on practical experiences and feedback received from students and IT employers.*

Introduction

Our experiences of information security education are based on practical teaching work carried out at the University of Oulu since 1990. Besides teaching, we have been involved in a number of practical industrial projects. During these years, we have created an educational model based on the non-technical side of security learning. The nature of this model is dynamic as its structure is reviewed on a continuous basis and new details are added to it each year.

Information security tends to be heavily biased on the technical side, perhaps because technical solutions are fairly easy to realize. Thus, there are cryptological methods and tools for information system and network security, security protocols and standards for telecommunication security and so on. If a problem arises, a technical solution is relatively easy to find - as long as you have money or technical co-operation potential to throw at it. This claim also holds for information security education. Technical solutions are straightforward to teach, but the crux of the matter is that most security violations are human related. The realization that technical solutions are only a part of the answer to the problem is the reason we have developed our curriculum in a human-oriented direction.

In this paper, we present a security education model, its practical contacts and its goals. The educational matrix presented in Fig. 1 depicts every module (or stage) of the model along with some practical results associated with each module and their effects on the environment. The final column shows the goals of the modules. The model, as presented here, serves a double purpose: firstly, it has an educational purpose and, secondly, it can be used as an aid in finding better solutions for the human aspects of security.

Broad curricula for information security education have been presented at the Sec'93 IFIP conference [Dougal & Jones 1993] and at IFIP conferences on information security education, i.e., Sec'98-WG11.8 and WISE 1 [Yngström & Fischer-Hübner 1998, 1999].

Katsikas and Grizalis (1995) have compiled a summary on various kinds of information security related degree programs, while Gallegos et al. (1998) have presented an extensive degree program with a particular emphasis on information systems auditing. In addition, Kajava & Siponen (1998) have proposed an outline for a security program from the end-user perspective, which was later expanded by Kajava & Varonen (2000).

Security Teaching Model

Traditional university education has been criticized for producing knowledge that is useful only for passing examinations. Since this is hardly motivating for students, teaching should be integrated with practical experiences to give students opportunities to learn such professional skills as are required in their future IT careers. These skills include the ability the utilize various forms of information and information sources, distinguish between relevant and irrelevant information and to develop and adapt information into new forms. These abilities presuppose the development of cognitive skills such as abstract thinking, being able to see the big picture instead of endless details, understanding complex processes and the backgrounds of various problems, and, last but not least, co-operation and communication skills.

Such skills and abilities do not develop overnight, they require a gradual build-up enabling students to enhance their theoretical knowledge and hone their practical skills. The end-user oriented security education model has been designed to answer (in part) to these needs. The basic idea is to enable students to construct expert knowledge in their field, to train the aforementioned general cognitive abilities and to combine theory with hands-on practice.

During the introduction of the model in 1990 - 1994, only the first module, Information Security Basics, was in existence. The module was based on lectures and a final examination. Some of these lectures were given by experts working in the IT industry. In addition, all students were encouraged to participate in the learning process by corresponding with the teacher responsible for the course by e-mail. The module was weighted toward the end-user direction.

Fig.1 presents the second developmental stage of the model. Information Security Basics, the first module in the improved model, is end-user oriented including traditional lectures, correspondence with the teacher, visiting lecturers with an active industrial background and examinations. The module comprises such educational materials as [Parker 1981, Russel & Gangemi 1991, The NIST Handbook 1993, ISO/IEC 1995).

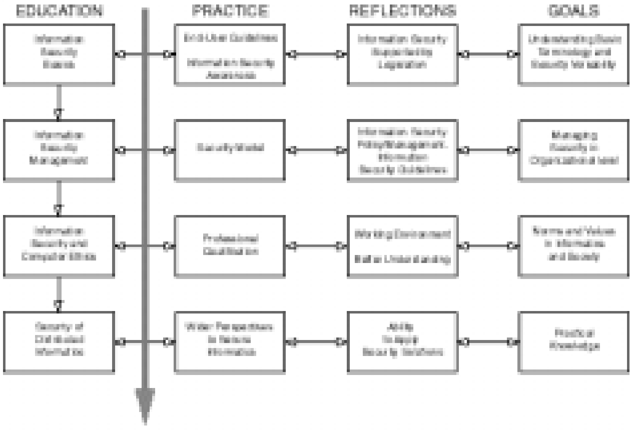
EDUCATION
PRACTICE
REFLECTIONS
GOALS
Information Security Basics
End-User Guidelines
Information Security Awareness
Information Security Supported by Legislation
Understanding Basic Terminology and Security Versatility
Information Security Management
Security Model
Information Security Policy/Management, Information Security Guidelines
Managing Security in Organizational level
Information Security and Computer Ethics
Professional Qualification
Working Environment
Better Understanding
Norms and Values in Information and Society
Security of Distributed Informatics
Wider Perspectives to Secure Information
Ability to Apply Security Solutions
Practical Knowledge

Figure 1. The security teaching model (on the left) and the educational matrix.

The second module, Information Security Management, is more organization-oriented in content. After an introductory lecture, students are directed toward autonomous learning based on printed materials. Their progress is controlled by a “closed book“ examination, which is the only compulsory requirement during the course. The reading list for the module includes [Code of Practice 1993, ISO/EIC 1995].

The third module is Information Security and Computer Ethics. It consists of introductory lessons, various working groups and seminar presentations. Students are required to work autonomously at home, gather together and work as a team to combine their results, give seminar papers and act as opponents. There is no separate examination, so a pass grade involves active participation in course work. Parallel to the these contact teaching groups, there are some distance learning groups whose members work in industry and are consequently unable to attend regular classes. Their learning process is based on remote tasks that they are required to do and report the results to the teacher. To complete their assignments, they need to acquaint themselves with pre-selected printed materials. They also take a traditional examination. The educational material for the module includes [Johnson 1994, Langford 1995, Kallman & Grillo 1993, Gotterbarn 1995, Siponen & Kajava 1998).

Module number four is called Security of Distributed Informatics. It is based on independent work in some special area of research or practical work, an extensive assignment and a seminar presentation. The module comprises a variety of topics and educational materials including network-oriented work such as [Davies 1994, Stallings 1995]. In this module students have a wider range of study options open to them than previously. Increased freedom, however, also correlates with increased responsibility.

Special topics within the Security of Distributed Informatics module include networks and the Internet. Recently, some new areas, geared toward mobile service security, have been added to the range of options. Among these are WAP and electronic payment systems security.

In addition to this security curriculum students specializing in software engineering or systems engineering have been able to select a security-related topic for their Master’s thesis.

Experiences

It is probably fair to say that students in general appreciate the way security education has been arranged. The problems we have had have tended to be of a positive nature: it has on occasion been rather hard to find enough seats for all those wishing to attend the courses!

Moreover, no special motivational tricks have been necessary to achieve this effect, because even our youngest students are aware of what is going on in industry. They know that security related issues are increasingly important and that security education is highly valued by employers. Furthermore, comments gleaned from students’ course feedback forms indicate an appreciation of this kind of teaching, students know that there are business organizations that provide similar courses - for a substantial participation fee. The university provides this education free of charge, and students also get academic credit for their work.

From the teachers’ point of view this kind of education is very valuable :

1. Students are largely self-motivated
2. The pedagogical emphasis has shifted from passive listening during lectures to active participation, from a passive learner’s role to an active one
3. A number of students are interested in continuing their studies to reach a security specialist status
4. Visiting experts from the industry have shown an interest in co-operation and have motivated students to pursue further studies in the area
5. The IT industry wants to recruit students with a wide security knowledge.

Developing Computer Ethics Education

We would like to discuss one module in closer detail, namely, Information Security and Computer Ethics.

People involved in IT security or systems development often seem to use the term ’computer ethics’ to refer to technical solutions that include human considerations (such as the user acceptance of some IT solutions). That is no more correct than to equate computer ethics with human management, as some SE people tend to do. There is also a difference in content and orientation between such courses as “Society and Computing“ and “Computer Ethics“. In spite of some inescapable points of contact, there are fundamental distinctions. Their reference sciences, for instance are different, in this case sociology and ethics. Sociology describes social order and change, social conflict and problems, while ethics focuses on questions such as right and wrong actions, how we should act in the final analysis or where do responsibilities lie in a particular problematic situation.

Although computer ethics relates to every aspects of IT, information security and ethics share some special interests. These include the following:

1. Ethics and morality have an effect on legislation, which, in turn, affects information security requirements.
2. Morality may also be a direct requirement. It is hard to see, e.g., how anyone could determine privacy issues without ethical reflection.

Another central, albeit neglected, issue concerns professional qualifications and their role. The academic world, at least in Finland, lacks even a qualification framework. In our view, a valid educational approach should include both pragmatic and theoretical views. The objectives of educational courses need to reflect the needs of the industry in some respects, but they should also reflect theoretical considerations (including theoretical approaches that are not currently used in the industry). However, crucial practical aspects such financial and political issues must not be overlooked in an educational context. As a result, educators should find out what the real problems in the field are to decrease the gap between research and practice.

Further issues that need to be studied include the following: should we teach particular methods or methodologies and what kind of learning/teaching methods or approaches should be used? One way of meeting the requirements set by theory on one hand and pragmatics on the other would be to combine problem-based learning and "ordinary" lectures. If properly done, this could also help to resolve the issue of whether what should be taught is methods or methodologies.

New Directions

During the past 10 years, the emphasis in organizational communication (EDI) has moved from point-to-point transfer of information to an environment where practically all computers are interconnected through intranets and the Internet. The problem is that information security has largely remained at the EDI level (1:1), although technology in the Internet environment has an entirely new approach (N:N).

In the current situation, information security is focused on technology and protocols. Hot topics include the security of PKI and the inbuilt security enhancements of IPv6, which are thought to make the prevalent technology-based security solutions part and parcel of modern communications.

However, technology and protocols are hardly likely to achieve such a state of sophistication as to render the human users of communication systems incapable of causing any harm to the systems. Particularly the development of information networks has brought to the fore end-user dependent factors on organizational information security. Such key concepts as openness and transparency entail a paradigm shift in praxis which must also be reflected in security thinking. If end-users have more choices available to them, they can also be held more responsible for the choices they make, especially if these choices have repercussions in terms of security. As a consequence, information security education has to take into account the significance of the most important element in information security - the human end-user.

That is by no means an easy task. To be sure, basic security education, complemented with topical courses on an on-going basis, increases security awareness. The crucial factor, however, is getting all users to accept the necessity of information security and the little chores that it entails. The management plays a central role in this undertaking by setting an example for every employee to follow. In our view, there is no better way to make information security an integral part of our daily routines.

The role of information security changes in step with improved security solutions. The introduction of firewalls, for example, has made illegal access into computer systems considerably more difficult than before. This development has served to emphasize the role of company employees. Since they have legal, albeit often limited, access to these systems, they must be careful to keep outsiders at bay. Thus, employees have a responsibility to follow security guidelines in their daily work. This they will do only if they are first made fully aware of the significance of information security and the role of every single employee in this task. Increasing information awareness is a key factor in information security during the next few years.

Conclusions

End-user oriented security education faces several challenges. The first one concerns how to teach information security to students. The second challenge is co-operation with industry. The third one is international educational and research co-operation, particularly within the Erasmus and Socrates programs of the European Union. Current projects include the development of an international security curriculum and the realization of the new postgraduate program, Intensive Program on Information and Communication Security (IPICS) .

The security teaching model depicted in Fig. 1 is an attempt to organize our efforts to answer these challenges. The model is by no means a finished product; rather, it describes a dynamic process that will probably never terminate. The practical experiences accumulated during the use of the security model and the project based co-operation projects with industry are an invaluable asset when developing the model to meet both current and rising requirements in security education.

End-user oriented information security education is only a part of security education and is not sufficient ***per se***. It must be augmented with mathematics-based knowledge which can be used, for example, in cryptography and risk analysis. Then, security experts must have technical knowledge of networks and communications which can be applied to security solutions based on hardware and security protocols. And finally, security experts must have a good communication ability to be able to co-operate with other people, end-users in particular.

The ultimate aim of end-user oriented security education is to increase computer security to as high a level as possible. One small step toward that goal is to publish security articles, books, trusted materials and so on on the WWW, thereby making them available for everyone.

As a discipline, information security draws on areas such as computer and information processing sciences, mathematics, technology, economics and human sciences. These fields of study constitute a platform for the new discipline. Due to the extent of the discipline, no one can master it in its entirety, only smaller sections of it. Information security education is also characterized by a range of approaches. In our department, the focus of interest lies on the human side of security, particularly on the end-user perspective. But we cannot limit our projects or teaching to that aspect, there must also be co-operation with specialists working in other areas of security.

Bibliography

Ed.: Yngström L; Fischer-Hubner S: Stockholm, Sweden, WISE 1, Proceedings of the IFIP TC 11 WG 11.8, 1999

Information Security Education - Current and Future Needs, Problems and Prospects. Ed.: Yngström L; Fischer-Hubner S: Vienna, Austria and Budapest, Hungary, IFIP TC-11 Working Group 11.8 Fourth Workshop, 1998

Stallings W: Network and Internet Security - Principles and Practice. Englewoods Cliffs, New Jersey, USA, Prentice-Hall, 1995

Department of Trade and Industry: A Code of Practice for Information Security Management. Vol.DISC PD003. London, UK, British Standard Institution, 1993

Davies, P.T.: Complete LAN Security and Control. San Francisco, USA, McGraw-Hill, 1994

Computer Security: Discovering Tomorrow. Ed.: Dougal E.G; Jones D: Vol.IFIP Sec'93. Deerhurst, Ontario, Canada, 1993

ISO/IEC JTC1/SC27: Guidelines for the Management of IT Security. ISO/IEC JTC1/SC27, 1995

Siponen M; Kajava J: Some Perspectives Concerning Two Elements of Computer Ethics. Vol.ETHICOMP '98; The Fourth International Conference on Ethical Issues of Information Technology. Rotterdam, the Netherlands, 1998