Computer Science Students' Perception of Computer Network Security

Volkan Cambazoglu
Department of Information Technology
Uppsala University, Uppsala, Sweden
e-mail: volkan.cambazoglu@it.uu.se

Neena Thota
Faculty of Creative Industries
University of Saint Joseph, Macau, S.A.R.
Uppsala Computing Education Research Group, UpCERG
Uppsala University, Uppsala, Sweden
e-mail: neenathota@usj.edu.mo

***Abstract*—In the last decade, the progress of internet technologies has led to a significant increase in security and privacy issues for users. This study aims to investigate how computer science students perceive computer network security. Thirty three students participated in the study in which we gathered data through a questionnaire. In this paper, we present an analysis that is inspired by the phenomenographic approach. Our conclusion is that the students have different levels of understanding of computer network security depending on their usage of the concepts they have learned, their theoretical or practical orientation to the subject, and their interest in the field.**

***Index Terms*—Computer Network Security; Computer Science Education Research**

I. Introduction

Computer Networks Security (CNS) is becoming more important nowadays because of increasing demand for internet based technologies. The increase in users' privacy concerns is related to the increasing use of the internet [1]. However, security mechanisms that prevent such issues might deteriorate a user's experience. A user might find these mechanisms cumbersome or unnecessary and neglect using them, which might lead to security breaches in certain systems or simply loss of privacy of the user.

Computer Science (CS) students are expected to have a better understanding of CNS concepts/mechanisms than most other people. Students receive both theoretical and practical knowledge. However, an undergraduate student can learn about the theories in computer security, but may not be able to apply the knowledge in practice. On the other hand, a person, who receives certificate training, can practically apply the gained knowledge while lacking a deep theoretical understanding of security issues. If CS students have a hard time understanding or following a CNS concept/mechanism, then an ordinary person might experience the same problems as well. Therefore, the aim of this study is to capture how CS students perceive CNS. We explore what CS students know about CNS and how they approach it in their daily lives.

In this paper, we report some of the results of an on-going analysis of the data that has been gathered. The rest of the paper is organized as follows. Related work is mentioned in section II and the methodology is described in section III. We share our findings in section IV and discuss in section V that CS students show increased awareness of CNS in five progressive stages. The paper concludes with the implications of the study.

II. Related Work

Related work reviewed here focuses on the organization of courses to teach computer security and on a phenomenographic study that investigated students' perceptions of network protocols.

The increasing importance of network security issues has led universities and colleges to focus on the organization of programs to incorporate the fast developing area of information security [8] and to issue curricula guidelines for teaching [5]. Researchers/teachers think about what to teach in computer security courses and how to teach it [10]. The advantages and the disadvantages of different approaches to teaching computer security are a matter for discussion [3]. The related work on education in computer security seems to discuss the trade-off between theory and practice-based education in general [11]. University education aims to give students a broad understanding of theories in computer security; however the issues in computer security are highly practical in real life and require hands-on experience. [12] discusses how to mix theory and practice, in order to teach information security to students, so that the students can conform to the existing standards. These approaches can be traditional lecture, scribe, expert/mentor, tutorial, project, research/teaching synergy, and attack/defend isolated lab. The approaches are identified according to the audience's active/passive role in the course and the content of the course.

Students' conceptions of computer networking protocols have been investigated by [2] using a phenomenographic approach [6]. In this study, students participating in an internationally distributed project course were interviewed about their experience of three network protocols (TCP, UDP, and RMI). The study found similarities and also differences in students' understanding of the protocols due to the contextual shifts in the students' experiences. These understandings were also seen as related to the different characteristics and ideas behind the protocols. Four categories of the general concept of a network protocol were identified that showed critical differences in hierarchically qualitative ways of understanding

978-0-7695-4960-6/13 $26.00 © 2013 IEEE
DOI 10.1109/LaTiCE.2013.19

a protocol. The more advanced understandings were deemed desirable from a learning perspective. It is with this study in mind, that we initiated the investigation of CS students' understanding of CNS concepts.

III. Methodology

The participants in this study consisted of a mixed set of CS students having different levels of education and coming from different countries. Thirty three students (2 undergraduate, 19 master and 12 PhD students) participated. The students were from 12 countries: Australia, China, Colombia, Germany, India, Iran, Lithuania, Singapore, Spain, Sweden, Turkey and Vietnam. The majority of the students were from Uppsala University, Sweden. The participants have received previous degrees from their home countries or from Switzerland or the USA. Most of the participants are currently students, while others are recently graduated.

In a phenomenographic study, data is collected through interviews. In this study, we invited the participants to fill in an online questionnaire that we prepared. There were two reasons why we chose a questionnaire as a data collection instrument: (a) the participants were located in different parts of the world and distributing an online questionnaire to people, who are located far apart, is a time and cost effective way of reaching them; (b) the participants from Sweden have different schedules and workloads and they could fill in the details in the online questionnaire at their convenience.

In the questionnaire, we asked open questions about computer security with a focus on CNS. Text books and courses about computer security generally include a chapter/lecture about CNS. As CNS is a subtopic within computer security, we choose not to dive into it without referring to more general computer security concepts/mechanisms. Thus, we started with a few questions about computer security before leading to the CNS questions, which form the core of the study. In order to have an understanding of the profile of the participants, we also extracted some statistical data from the participants, such as exposure to computer security training and the duration of the training. The remaining answers were mostly expected as paragraph text, where the length of an answer depended on the knowledge and experience of the participant. In the questionnaire, we had branching so that participants could follow different questions depending on their answers to yes/no questions.

After preparing the questionnaire, a pilot study was done with a PhD student whose focus is on CNS. The ambiguities in some of the questions were fixed by either rewriting the question or a help text accompanying the question. We intended to ask questions so that the participants felt they were being interviewed for their opinion, rather than being assessed for their knowledge of CNS concepts/mechanisms.

We analyzed the participants' answers using an approach inspired by phenomenography. We aim to understand how the phenomenon of CNS is experienced by the CS students. As Booth says, "Different contents of learning and different types of learning task give rise to different kinds of opportunity for developing awareness" [4]. We surmised that each student has a different degree of knowledge of CNS, encounters different events related to CNS, receives different kinds of education/training of CNS, and reaches different learning outcomes. For example, a concept can be understood in different ways by different students. While one student understands the concept with the help of an example, another student can directly understand from the theory itself. In another case, a student might not fully understand the concept; but just knows that one of his/her experiences comes from that concept. Therefore, with the help of phenomenographic methodology, a researcher observing these students can categorize how the concept or the phenomenon can be learnt or experienced in different ways [6]. The outcome of a phenomenographic analysis is a series of categories that focus on fundamental characteristics and preserve the specific content of the phenomena in the description [9]. These categories are exemplified with quotes so that the fundamental characteristics are illustrated with the specific content from the participants.

IV. Findings

In this section, we share our findings from the questionnaire. Nine students have not taken any training in computer security. One student has studied computer security by him/herself. One student has had training in computer security at a company. Twenty two students have taken courses that are directly or indirectly related to computer security. A subset of 22 students has also had private seminars in computer security. After considering different, yet related questions (see the Appendix for the questions), we draw a high level categorization of the CS students' perception of CNS. In this high level categorization, we have five categories in increasing order of deeper understanding.

(1) Misconception or confusion, yet still know that something is important and attention must be paid:

In this base category, we witness CS students that have learnt something about CNS; however, there is either confusion or misunderstanding in the gained knowledge. For example, a student thinks that Linux helps to secure one's communication from other people.

I do not use any app for security but I use linux.

Linux is just another operating system that has no guarantee for securing communication from other people. It might be more secure than other operating systems because of the market share or not being a favorite for attackers' target. However, the student thinks that it is a way to secure communication from other people.

(2) A vague idea of important security issues without understanding the reasoning behind them:

In this category, the students use CNS mechanisms in daily life; however, they do not know the details of the knowledge they have learnt about CNS. For example, a student does not know why he/she pays attention to network security when connecting to a wireless network. Unlike students in the previous category, the student clearly knows that it is a good practice to be careful when connecting to a wireless network,

even though the reasons seem to be unknown. For example, a student said:

> I always think it is risky and not secure!

(3) A high level theoretical understanding of security issues and their reasons:

What is new in this category is that the students express themselves by consulting theories and concepts. Here, students give ideal explanations to CNS phenomena as a result of abstraction and high level understanding of CNS concepts. For example, a student thinks that wireless network security means a secure network where users do not have any doubt of losing privacy. Ideally, the network should be secured as the student thinks of, yet, it might not be in practice. For the theoretical way of thinking, an excerpt is:

> Security is a broad term, but the first three things that come to my mind are confidentiality (nobody other than the two parties should be able to read the communication), integrity (each party should be able to establish that a message has not been tampered with) and authenticity (each party should be able to establish the origin of a message). These aspects of security are often achieved by cryptography.

(4) Both high level theoretical understanding and practical usage of the theories behind the security issues:

In this category, the students reflect their knowledge both conceptually and practically. Here, we see that students make a claim and support it with an example. In contrast to the previous categories, here the students show deeper insight into learning and a consolidation of what is learnt. In other words, some students put their CNS knowledge in use in their daily lives. For example, a student explains that training in computer security has made him:

> ....more aware of the risks involved in computer networking, especially wireless networking. Therefore, I use strict rules who is able to connect to my home network and use encryption.

(5) High level theoretical understanding, practical usage of the theories behind the security issues, and also increased interest in the security field so that they can keep up-to-date with the new developments:

The last category consists of students that are interested in CNS. These students know the theories, know how they are used practically, and also follow new developments in the field. CNS knowledge of these students evolves as a result of their interest in the field. This category introduces elements of personal insights and actions that deepen understanding gained from the previous categories relating to theoretical knowledge and practical application. An example for this category can be the statement made about a CNS course:

> It definitely increased my awareness and interest in the subject. So that, I occasionally read related articles or tutorials in order to keep my knowledge updated and to take necessary precautions.

V. Discussion

The study aims to look for what CS students know about CNS and how they use that knowledge in daily life. In this section, we try to explain the students' understandings in the light of their contextual experiences.

The first two categories that we identified dealt with misconceptions or incomplete knowledge of CNS. The last three categorise showed increasing theoretical knowledge, practical usage, and personal motivation in learning. This distinction is in line with other findings presented in [7] that show that students' learning progresses from a surface to more inclusive or deeper ways of learning.

We noticed that most of the participants have learnt about computer security and/or CNS in some way and are aware of the CNS issues. Only a couple of students mentioned that they have not studied CNS or computer security before; hence these students are not aware of the CNS or computer security issues present in real-life. If a student confuses or does not remember things from the course taken, it might mean that the student does not need that knowledge in his/her daily life. When such knowledge is frequently used, it remains within the focal awareness [7] of the student.

The difference between practical and theoretical ways of understanding CNS concepts can also be dependent on the kind of education/training the students have received. Some of the participants might think more practically than others because of private seminars or training at a company or through self-training. These students might even have taken computer security courses/classes at the university, yet they might be more technically oriented than other students. On the other hand, some of the participants can be more theoretically oriented than others because of university education.

We also observe the factor of interest among the answers to the questionnaire. Some of the students are definitely more interested in computer security or CNS subjects than some others. These students look for details when studying CNS and follow new developments to be up-to-date. CNS is a subject that goes through great and rapid change. While interested students follow these changes, other students either learn about the changes as they encounter them, or they give up on the security issues.

VI. Conclusion and Implications

In this paper, we have described how CS students perceive CNS. We looked for the knowledge that the students have in order to understand how much they know about CNS in general and how this knowledge affects them in daily life. As a result of our questionnaire based survey among an international set of CS students, we deduced five categories that represent increased understanding of CS students' perception of CNS. We have interpreted these in terms of contextual influences on students' learning experiences [2]. The results of this study show that it is desirable to mix theory and practice, as recommended by [12], to teach information security to students. The study thus offers a contribution for teachers in

planning course curricula to integrate theoretical and practical aspects of CNS.

In the future, we would like to investigate CS students' views on

- how authentication systems work and what must be done to ensure the security in these systems.
- how well computer security and usability go together.
- whose responsibility it is to make sure internet applications work in a secure way.

ACKNOWLEDGMENT

We thank the students who participated in the survey.

REFERENCES

[1] A. Anton, J. Earp, and J. Young. How internet users' privacy concerns have evolved since 2002. *Security Privacy, IEEE*, 8(1):21–27, Jan-Feb 2010.

[2] A. Berglund. *Learning computer systems in a distributed project course : The what, why, how and where*. PhD thesis, Uppsala University, Division of Computer Systems, 2005.

[3] M. Bishop. Education in information security. *Concurrency, IEEE*, 8(4):4–8, Oct-Dec 2000.

[4] S. Booth. On phenomenography, learning and teaching. *Higher Education Research & Development*, 16(2):135–158, 1997.

[5] S. Cooper, C. Nickell, L. C. Pérez, B. Oldfield, J. Brynielsson, A. G. Gökce, E. K. Hawthorne, K. J. Klee, A. Lawrence, and S. Wetzel. Towards information assurance (ia) curricular guidelines. In *Proceedings of the 2010 ITiCSE working group reports*, ITiCSE-WGR '10, pages 49–64, New York, NY, USA, 2010. ACM.

[6] F. Marton. Phenomenography: Describing conceptions of the world around us. *Instructional Science*, 10:177–200, 1981.

[7] F. Marton and S. Booth. *Learning and Awareness*. Educational Psychology Series. Taylor & Francis, 1997.

[8] K. Petrova, A. Philpott, P. Kaskenpalo, and J. Buchan. Embedding information security curricula in existing programmes. In *Proceedings of the 1st annual conference on Information security curriculum development*, InfoSecCD '04, pages 20–29, New York, NY, USA, 2004. ACM.

[9] L. Svensson. Theoretical foundations of phenomenography. *Higher Education Research & Development*, 16(2):159–171, 1997.

[10] T. A. Yang. Computer security and impact on computer science education. *J. Comput. Sci. Coll.*, 16(4):233–246, Apr 2001.

[11] A. Yasinsac. Information security curricula in computer science departments: Theory and practice. *The George Washington University Journal of Information Security*, 1(2):135–158, 2002.

[12] W. Yurcik and D. Doss. Different approaches in the teaching of information systems security. In *Proceedings of the Information Systems Education Conference*, 2001.

APPENDIX

We asked the following questions to the participants.

- Have you taken training in computer security before?
- How long did computer security training take?
- How would you evaluate the level of computer security training?
- How did computer security training affect your view and/or use of computer security?
- What is(are) the first thing(s) that comes to your mind about wireless network security?
- Do you pay attention to wireless network security when connecting to a wireless network?
- Why do you pay attention to wireless network security when connecting to a wireless network?
- How do you pay attention to wireless network security when connecting to a wireless network?
- Why do you not pay attention to wireless network security when connecting to a wireless network?
- Which applications can you think of that secure your communication from other people?
- What is(are) the first thing(s) that comes to your mind about securing a communication between two end-users?
- What kind of personal data would you like to keep private/secured from other people?
- What do you think are the implications of the disclosure of your personal data?