On the Learning Activities and Outcomes of an Information Security Course

Timo Hynninen

February 9, 2023

On the Learning Activities and Outcomes of an Information Security Course

TIMO HYNNINEN, South-Eastern Finland University of Applied Sciences

This paper presents an early information security course for IT students. We followed teaching methods and good practices presented in relevant literature to design our course outline. As a result, we arranged a semester long course which covers information security topics, offensive and defensive training activities, and overall security mindset. Finally, the initial findings from running the course are discussed.

CCS Concepts: • **Social and professional topics** → *Computing education*; • **Security and privacy**;

Additional Key Words and Phrases: Teaching information security, Security mindset, Offensive security, Defensive security

ACM Reference Format:
Timo Hynninen. 2019. On the Learning Activities and Outcomes of an Information Security Course. 1, 1 (February 2019), 4 pages.
https://doi.org/10.1145/3364510.3366158

1 INTRODUCTION

Information security and assurance topics should be tightly integrated into computing education [7, 12], and security in software should not be an afterthought [6]. In addition information security includes both CS topics and general knowledge that is important in the work life. As students first go work in the industry as early as 1.5 years into their studies [13], teaching information security concepts early on is important in the CS curriculum. The security mindset has previously been successfully taught as early as in conjunction with CS1 [9].

This paper presents the experiences of teaching information security concepts on a holistic first year course. The objective of the course was to familiarize the students with a security mindset, understand the role of people and technology in the overall security picture, and to have an understanding of the different types of tools to implement computer and network security. To implement the course we started by reviewing relevant literature on the teaching methods in information security topics. An overview of how information security is taught is summarized as follows in the literature review by Riihelä [10]: Security topics should be taught in virtual laboratory environments using the offensive approach and spread across the entire curriculum. We used the findings and proven teaching methods distinguished in the literature, in addition to our teaching experience to design the activities for our course.

2 COURSE IMPLEMENTATION AND OBSERVATIONS

The IT programme at the South-Eastern Finland University of Applied Sciences focuses on the networking and software engineering skills. These competencies are complemented by two 5 ECTS course modules in information security, the first being an early fundamentals course on information security topics. During the latest implementation in the academic year 2018-2019 the course consisted of 12 weeks worth of lectures and practical work. At the end of the course there were mandatory exams which formed 80% of the final grades. Practical work in the form of exercises and lab works was worth 20% towards the final grade.

Author's address: Timo Hynninen, South-Eastern Finland University of Applied Sciences, P.O. Box 68, Mikkeli, Finland, 50101, timo.hynninen@xamk.fi.

2019. Manuscript submitted to ACM

The practical work was not stirctly mandatory but as the best grades would not be possible to achieve without it, most students chose to complete the tasks.

As a rough guide for weekly lecture topics, and as the main course book, we used *Secrets and lies: digital security in a networked world* [11]. We also used *Security Fundamentals* [5] as an additional textbook. The lecture topics were as follows: *cybersecurity concepts, threats, attacks, attackers, security needs, security technologies, computer security, access control, network security, network defenses, certificates*, and *security processes and users in the process*.

Following the suggestions of Chatmon et al. [4] we employed an active learning approach. We wanted to facilitate active learning during the lectures so we presented many case studies and stories from history, where investigations into both attacks and security solutions against them were discussed. In addition we used many real world analogues to explain information security terms, for example explaining how a denial-of-service attack would look like in the physical world.

To further support the active learning our course also consisted of weekly hands-on exercises or laboratory works. Hands-on activities are considered paramount in security education [8]. We generally tried to choose an equal amount of both defensive and offensive activities, as offensive training is considered essential in order to produce security professionals [14]. The activities are summarized as follows, categorized into themes consisting with offensive and defensive activities:

(Human) Information processing

Offensive: The students researched ways to attack a real world process where information processing is done by people, following the principles presented by Yuan et al. [15].

Defensive: We reviewed the use of security policies as a tool to control the information assets within an organisation.

Computer security

Offensive: The students researched USB HID devices and bad USB attacks using the Malduino usb devices [2].

Defensive: The students researched ways to mitigate the bad USB attack.

Cryptography concepts

Offensive: We reviewed historical ciphers and how to break them.

Defensive: The students implemented the one time pad in either Python code or Microsoft Excel.

Password protection and encryption

Offensive: The students used Ophcrack [3] and John the Ripper [1] to crack Windows and Linux passwords.

Defensive: The students familiarized themselves with different encryption software in order to protect files.

Trust and certificates

Offensive: The students researched clipboard poisoning and captive portals.

Defensive: We reviewed the concepts of certificates and digital signatures on the internet.

Computer security

Offensive: The students followed a tutorial in a lab exercise where they used different software for detecting threats and vulnerabilities in a Linux system.

Defensive: The students followed another tutorial in a lab exercise where the objective was to harden the Linux system against the threats found earlier.

3 INITIAL FINDINGS

All in all 24 students started the course, and at the end 21 received a passing grade. At the end of the course we collected feedback from the students. In the feedback survey we asked the students to *tell what they felt were most important* *topics of the course*, and *what they felt they had learned during the semester*. The feedback was open-ended, and out of the 24 students we collected responses from 12.

We considered the course to be holistic and building on the students' security mindset, as many summarized their learning in terms of security thinking:

"This course slowly but steadily constructed my security concept."

"Data can be used to either improve quality of life or malicious attack again its owners. So for me, protecting and giving the access to the right people are very crucial."

"With sophisticated attacks now commonplace, people need to assume that they will be breached at some point and implement controls that help them to detect and respond to malicious activity before it causes damage and disruption."

"Another thing I didn't know was, how much harder was to secure a system, than a physical item ... The weakest link could be an unaware individual in a billion-dollar company with hundreds of security consultants"

The active learning approach with hands-on activities also seemed help students achieve concrete learning objectives in the cybersecurity domain:

"For me the most important was how to defend your network from different threats. Likewise, instructions about protecting myself from cyberattacks were also very interesting. Encryption was another topic that I liked."

"I got familiar with network and distributed system attacks, defences against them, and forensics to investigate the aftermath."

Finally, the students also learned about individual technical topics through the learning activities:

"I learned that with a system that has password, does not mean that system is perfectly safe ... there are multifactor authentication which can reduce this damage."

"I learned how to password cracking in Linux and Windows and I have the knowledge and the awareness of being cracked so I can improve my security level in the future."

4 CONCLUSIONS

On our early information security course the objective was to concentrate on the big picture of information security. Based on the feedback the students gained a good understanding of the abstract security concepts. However, this approach and the early timing of the course also meant that we could not cover some practical skills which could be useful for graduates in their daily working life, such as writing secure program code or configuring secure network infrastructure. These limitations are covered in our curriculum in following programming and network security courses.

Through the implementation of our course and the learning outcomes reported by students we can summarize our findings as follows. We found that through the combination of theory lectures with real-world case studies, and practical hands-on activities, students are able to adopt a good security mindset early on in their studies, as suggested by the literature. Additionally the students get acquainted with security technologies, both for the offensive and the defensive purposes. In future we will continue to incorporate good ideas and pedagogical best practices to our information security curriculum.

REFERENCES

[1] [n. d.]. John the Ripper password cracker. https://www.openwall.com/john/

[2] [n. d.]. MalDuino. https://malduino.com/

[3] [n. d.]. Ophcrack. https://ophcrack.sourceforge.io/

[4] Christy Chatmon, Hongmei Chi, and Will Davis. 2010. Active learning approaches to teaching information assurance. In *2010 Information Security Curriculum Development Conference*. ACM, 1–7.

[5] Microsoft Official Academic Course. 2011. *Exam 98-367 Security Fundamentals*. Wiley.

[6] John McManus. 2018. Security by design: teaching secure software design and development techniques. *Journal of Computing Sciences in Colleges* 33, 3 (2018), 75–82.

[7] Svetlana Peltsverger and Orlando Karam. 2010. Is teaching with security in mind working?. In *2010 Information Security Curriculum Development Conference*. ACM, 15–20.

[8] Svetlana Peltsverger and Chi Zhang. 2014. Bottleneck analysis with NetKit: teaching information security with hands-on labs. In *Proceedings of the 15th Annual Conference on Information technology education*. ACM, 45–50.

[9] Vahab Pournaghshband. 2013. Teaching the security mindset to CS1 students. In *Proceeding of the 44th ACM technical symposium on Computer science education*. ACM, 347–352.

[10] Lassi Riihelä. 2019. *Teaching information security: A systematic mapping study*. Master's thesis. LUT University, Finland.

[11] Bruce Schneier. 2011. *Secrets and lies: digital security in a networked world*. John Wiley & Sons.

[12] The Joint Task Force on Computing Curricula. 2015. *Curriculum Guidelines for Undergraduate Degree Programs in Software Engineering*. Technical Report. New York, NY, USA.

[13] The Joint Task Force on Computing Curricula. 2017. *Curriculum Guidelines for Baccalaureate Degree Programs in Information Technology*. Technical Report. New York, NY, USA.

[14] Zouheir Trabelsi. 2014. Enhancing the comprehension of network sniffing attack in information security education using a hands-on lab approach. In *Proceedings of the 15th Annual Conference on Information technology education*. ACM, 39–44.

[15] Xiaohong Yuan, Sahana Murthy, Jinsheng Xu, and Huiming Yu. 2010. Case studies for teaching physical security and security policy. In *2010 Information Security Curriculum Development Conference*. ACM, 21–26.