JÖNKÖPING UNIVERSITY
School of Engineering

Assignment

-

Seminars, 2.5 ECTS

COURSE: - *Information security, 7,5hp*
AUTHOR: *Erik Bergström*

JÖNKÖPING October 2020

1 Introduction to Seminars, 2.5 ECTS

1.1 Objectives

There are several objectives related to the seminar part of the course. To be able to read and understand scientific papers is central in this assignment. Also, to be able to find information supporting a claim is an objective, and to be able to view, for example, threats, and vulnerabilities from different viewpoints are central. In practice, the seminars are aligned according to the following intended learning outcomes:

- Display knowledge of recent cases of data breaches and/or information leakage, and show an understanding of the underlying reasons.
- Demonstrate the ability to search for and present relevant research results related to current events and/or trends within the field of information security.
- Demonstrate the ability to analyze and reflect over current events and/or trends within the area of information security.
- Demonstrate the ability to reflect over how vulnerabilities in information systems affect organizations and society.

1.2 General about the seminars

A seminar is an ancient form of academic instruction that brings together small groups for recurring meetings on a topic or series of topics. A seminar is supposed to be a place where, for example, scientific papers are discussed, and questions are debated.

Optimally, seminars are performed physically around a table, but social distancing is impacting, and online seminars are scheduled. In order to convey presence, camera use is suggested during seminar sessions.

Active participation is necessary, and a virtual system of round the table will be used. Active participation is about asking specific questions and relating questions to other papers, terms or contexts.

Presentations and dialogue at the seminars need to be performed in English.

The scheduled supervisions are mainly intended for discussion, between the groups, and with the supervisor, and for claiming and registering topics.

1.3 General about the reports

You will submit three texts as a part of this seminar series. In seminar 1 will you author a small summary, and in seminar 2 and 3, will you write two short reports.

You must support your claims when you write the reports. When you refer to previous work, it strengthens your credibility. If you do not cite, it implies the text is yours, and you could face plagiarism charges. It is, therefore, a mandatory requirement to use proper citing using an established standard such as APA. You can find information

about how to cite according to APA on many websites, including a guide by our own University Library (n.d.). The guide from the University Library (n.d.) is also available in Swedish if preferred.

The reports should cite relevant peer-reviewed literature. Use databases such as Primo available from the university library (https://ju.se/library) or Google Scholar (https://scholar.google.se/) to find such relevant literature. Peer-reviewed literature is especially crucial in Seminar 2, and for explaining the foundations of, for example, the attacks in Seminar 3. It is not forbidden to use non-peer-reviewed sources. Rather the opposite as it will be necessary for the report in Seminar 3, where sources might be newspapers and websites.

The reports should have a clear structure and have correct spelling and grammar. No template is provided as very short texts are expected and required. The reports should be written with your peers as intended readers.

The reports should be written in either Swedish or English. Use the language you feel most comfortable with. No “bonus” or extra consideration is given if the reports are written in English.

2 Seminar 1 - Ethics in cybersecurity research and practice

Seminar 1 aims at introducing ethical issues in the field of information security. The seminar is based on a paper by Macnish and van der Ham (2020). The paper introduces and discusses ethical issues in two cybersecurity case studies. The first case is related to university-based development, while the other case relates to the community of practicing cybersecurity experts.

2.1 Assignment

The assignment is individual, and before the seminar, a summary is to be submitted in Canvas. The summary should contain key learnings from each case described above, from your personal perspective. The deadline is posted in Canvas and is before the seminar.

The summary should be approximately 500 words and include aspects of both cases. In addition, two questions for the seminar should be included.

The summary does not need referencing, as it is a summary of one specific paper.

3 Seminar 2 - Encryption

Seminar 2 aims at highlighting an ethical dilemma in the information security field. To allow public use of any encryption has been debated for decades, and the topic is continually relevant.

Law enforcement and intelligence agencies need weak or nonexistent encryption to be able to snoop at, for example, terrorists. Robust encryption algorithms render lawful interception practically impossible, and at the same time are there increased demands from governments and citizens to handle our data in a more secure way, and thereby inviting to the use of strong encryption.

There are many possible questions surrounding the ethical dilemma of encryption, such as:

- Should companies be able to read stored encrypted user data?
- Should companies answer legal law enforcement requests?
- Should companies answer legal law enforcement requests only for certain types of threats, such as terrorists?
- Should we have backdoors?
- Should we limit automatic encryption?
- If we don't encrypt, how can we safely store and transmit sensitive information?
- Is it not my individual right to protect my (sensitive) information?

3.1 Assignment

In this assignment, a stance needs to be taken. The stance is essentially either for or against the free public use of encryption. More specifically, you will need to choose either to read up and debate for:

- *limiting the use of encryption for companies and individuals so that law enforcement and intelligence agencies can get access to information*, or for
- *allowing companies and individuals to use any encryption they wish, regardless of the consequences*.

You will motivate and debate your stance. As the debate is impossible without two sides, is it necessary first to choose if you would like to present for or against the free use of encryption. In practice, you will need to assign yourself to a for group or an against group as there will be an equal number of students taking each stance.

The assignment is individual, and before the seminar, a report is to be submitted in Canvas. The report should contain at least five scientific references supporting your claims. The report should be approximately one page, excluding references.

4 Seminar 3 - Threats and vulnerabilities

Seminar 3 aims at giving an understanding of recent data breaches by analyzing the threats and vulnerabilities that made the breach possible. Furthermore, as all groups will select and present different breaches, the seminar will make you reflect over current events and trends in the information security field.

4.1 Assignment

In this part, you will work two-and-two in self-organized groups. You have to select a recent (maximum four years old) security breach featured in the national or international press as a starting point. Based on the breach, you need to identify:

- What type of attack was it?
    - Describe the general type of attack.
- What was the vulnerability?
    - Describe the general type of vulnerability.
- Describe the threat.
- What can/could be done?
    - Both in general and specific.

Based on the identification, you will author a two-page report (excl. references) that is to be submitted before the seminar.

The breaches and attack types should be unique in each seminar group, and allocation is based on the first-come-first-served principle. Three weeks into the assignment is the deadline for selecting a topic, and a mandatory check with the supervisor scheduled.

At the seminar, you will need to present and discuss your findings. You should prepare a 7 minutes presentation using presentation aids such as slides, and allow for ca. 3 minutes of questions. Both group members need to present during the presentation.

References

Macnish, K., & van der Ham, J. (2020). Ethics in cybersecurity research and practice. *Technology in Society, 63*, 101382. doi:https://doi.org/10.1016/j.techsoc.2020.101382

University Library. (n.d.). Why do you cite? *University Library Guides.* Retrieved from https://guides.library.ju.se/apa