ROYAL INSTITUTE
OF TECHNOLOGY

School of Electrical Engineering and Computer Science
Division of Theoretical Computer Science

LAB S

Seminar: Report, Peer-review and Presentation

Computer Security

DD2395 / HT2022

r(None)

(None)

Contents

1 Introduction

The idea of this lab is to dive into one specific topic in Computer Security more deeply, to practice literature research and report writing as well as peer-reviewing of a report, written by others. The lab consists therefore of a report (**first draft**, then **revision**), a review (**individual**), and a presentation **in front of other groups** at a seminar. All these parts need to be accomplished in order to pass the seminar.

⚠ **Deadline**

> The deadlines for the lab can be found on the course website
> `https://kth.instructure.com/courses/35479`
> Do not forget to sign up on time on the course web page for you preferred topic, but also for the time slot of the presentation of your work!

2 Forming a Group and Choosing a Topic

You should start by forming a group of **three** people. Once that has happened, all of you should agree on one of the topics listed in Section 8 at the end of this document, but if you would like to work on something else, you are welcome to send a suggestion to the course administrator or post it in the discussion thread on Canvas. If it is approved, it will be added to the list for you to sign up. Finally, you will have to choose a presentation slot to present your work to some of your classmates.

ℹ **Page Count and Presentation Time**

> The expected size of your report and the length of your presentation varies depending on your group size:
>
> - Two people
>   - Report size: 2 written pages (excluding cover and references)
>   - Presentation time: 10 minutes
> - Three people
>   - Report size: 3 written pages (excluding cover and references)
>   - Presentation time: 15 minutes

3 Writing the Report

The goal of your work with the topic is for you to get a deeper understanding of it. You don't need to be an expert to be able to work on a topic, neither do we aim at you becoming one. But we want you to be able to research good sources for the topic, learn how they are related and how they explain it.

Report Language: English

For your own practice, and the benefit of other (also international) students, the report is to be written in English.

After reading your report, one should have gotten answers to the guiding questions below. The idea is *not* that you explicitly list these questions and answer them, but rather that you use them as a test, if you covered all important aspects.

- **What is the problem?**
  If you talk about an attack or security, describe what happens.
  If you talk about a solution, say what problem it solves.
- **Why is it a problem?**
  What is the underlying technology/behavior/economics problem that enables an attack in this area?
- **Why should we care?**
  What are the consequences of an attack succeeding, or of a solution failing/succeeding?
- **What are solution approaches?**
  What solutions are there for an attack or security issue?
- **What are your conclusions?**
  Do you think this attack/solution works?
  What did you learn in your research?
  What needs to be done?

Good and Bad Sources

Not every piece of text available digitally or printed is valid when researching on a topic.

- **Wikipedia**
  It is a good starting point to get an overview, but it is **not** enough.
- **Conference or Journal Papers**
  They are the expected minimum sources, but do not get drowned into too many of them, choose a few that are most relevant and useful.
- **News articles**
  They are additional sources that you can use, and sometimes explain things in an easier way than a book or a paper.

3.1 Structuring your report

Note that you are free to decide the organization of the content that describes your research topic. This means that you do not have to organize your work in terms of the guiding questions. The report should, however, include at least the following:

- **A descriptive title**

- **The authors' names**
- **A short abstract**
  Concisely describing the topic while addressing the guiding questions in very few sentences.
- **The report body**
- **Bonus point plan** Mention if you go for a bonus point and write a short description of what you (plan to) do.
- **The sources used**
  Not only a list of the material that you use but also the citation at the appropriate places in the report.

3.2 Submitting your work

Please submit your report on the canvas course page. Depending on your interface language, you find corresponding assignments under the menu Assignments or Uppgifter. There is an assignment for the draft (first version) of the report and another for the final (revised version of the) report.

4 Peer Review: Evaluating another Team's Report

Some time or days after the deadline for submitting the reports has passed, each member of your group will a report from another group of the course to review. Your reviews are individual, should be **about one page long** and contain the following: state whether the guiding questions have been answered (and very briefly what you understood the answers to be), whether the format was correct, whether enough and appropriate sources have been used and correctly cited, and what additional information you would want to better understand the topic. If there was a description of a bonus-point attempt, give feedback on whether you think this is worth a bonus point or what would need to be changed.
Try to give as much constructive feedback as possible, stating **what the group could improve for the final version and for the presentation of their topic**. You may start your review with a very short summary of the report (e. g., using the guiding questions), but you should spend most of the space on giving feedback.
Your review should also include the following information:

- the title and author names of the report you are reviewing.

Submit your review on the peer review part of the draft assignment on Canvas, as a pdf.

5 Revising the Report

Take into account the instructions on the report (go over them again) and the feedback you got from peer review and take both as a basis for improving your report draft. Submit the revised, final report as an upload to the corresponding assignment on Canvas.

6 Presenting Your Work

With the presentation of your work, we would like you to think how you can demonstrate, in 10 (15) minutes, an interesting aspect of the topic you have chosen.
We require all members of the group to contribute (talk) equally to the presentation and everyone should have a similar understanding of the topic since you all worked together. Do not forget to cite the sources you use for the presentation as well.

Presentation Language: English

> For your own practice, and the benefit of other (also international) students, the presentation is to be done in English.

Think of the presentation as the way to answer what you mean with the title of your report if you would have to explain it to someone that you meet in the elevator.

7 Bonus Point

For a bonus point, include a short demo or animation to illustrate your topic. Given the variety of topics and their differing suitability for demos, it is not straightforward to say in general terms what qualifies for a bonus point. As a rule of thumb, it should be something that shows rather than tells about the topic, something that clearly had some thought, substantial effort, and preparation going in. For example, only showing a video someone else made or low effort animations of the topic or low effort slides are not counted as a demo. Please note that the demo should not also attack someone else's system without consent. You can get the chance to receive feedback on your idea in the peer reviews of your topic (if you specified your intention and plan in the draft), on the discussion thread on Canvas, or by asking a teacher.

8 Research Topics

The following is a list of suggested topics that you can choose from. It is not meant to be an exhaustive list. If you have a topic related to Computer Security that you would like to choose instead, you can suggest the topic yourself by e-mailing it to the course administrator. If it is approved, it will be added to the list of topics which you can register for.

- **Computer Security**
  - Top 3 Internet Security Threats
  - Top 3 Computer Security Threats
  - Famous Malware
  - Famous Hacking incidents
  - Famous Exploitable Bugs
  - User Behavior Studies
- **Security in Networks**
  - VPN
  - SSH Tunneling
  - IPSec
  - Advanced Firewalling
- **Security in Wired Networks**
  - ARP Spoofing
  - DNS Attacks
  - DNSSEC, DANE
- **Security in Wireless Networks**
  - WEP (aircrack-ng), WPA
  - Vehicular Networks Security
- **Security in Large Scale Networks**
  - Specific (D)DoS Attacks
  - Specific Botnets
- **Web Security**
  - Session Hijacking
- **Anonymous Networks**
  - TOR
  - I2P
  - Freenet
  - OneSwarm
  - GNUnet
- **RFID Security and Privacy**
  - ePassport
  - KTH's library card, SL card,...
- **Security in Smart-cards**
  - SwedishID, BankID
  - general smart-card security
- **Security Banking and E-Business**
  - Modern Online Banking Authentication methods

  - Security of Micropayments
  - NFC payment
  - Crypto-currencies (Bitcoin, Litecoin,...)
  - Blockchain

- **Security Monitoring and Auditing**
  - IDS, Traffic analysis (Kismet, Nmap,...)
  - Information Flow Analysis
  - Synthesis of User Behavior

- **Security in Software**
  - Sandboxing (Chrome NACL, Caja for Javascript, HTML5,...)
  - Separation Kernels
  - Heap/Stack/Arithmetic overflow
  - Specific Worms/Rootkits/Viruses
  - Bug exploiting
  - Trusted Computing
  - Smartphone Application Security
  - Return Oriented Programming

- **Digital Access and Usage Control**
  - Digital Rights Management (Ebooks, films, music,...)
  - Digital Watermarking

- **Identity Management**
  - OpenID
  - OAuth
  - Facebook Connect
  - Anonymous Credentials (Idemix/U-Prove)

- **Cryptography**
  - Classical Crypto-systems (Enigma,...)
  - Secure Multiparty Computation
  - Zero-knowledge Proofs
  - Password Cracking
  - Steganography
  - Homomorphic Encryption

- **Authentication**
  - Specific Biometrics
  - Alternatives to Passwords (Apple TouchID,...)
  - Two-Factor Authentication

- **Privacy**
  - Browser Fingerprinting
  - Security/Privacy Enhanced Social Networking
  - Decentralized Online Social Networks
  - User Behavior Studies on Privacy

  - Deniable messaging: OTR, Signal
  - Differential Privacy
  - Anonymity (k-anonymity, l-diversity,...)

- **Surveillance**
  - Prism/Tempora
  - State Malware (e.g. surveillance trojan horses)
  - State Internet Surveillance

- **Ethics of Computer Security**
  - Privacy vs. Surveillance
  - Controversial and recent cases

- **Machine learning and security**
  - Adversarial Machine Learning
  - ML for security
  - Privacy-preserving ML
  - FAT (fairness, accountability, transparency) of ML
  - Federated Learning

- **Other**
  - Computer Games Security
  - Mobile Phone Security
  - Security in the Cloud

9 History

Version	**Contribution**	**Author** (Affiliation)	**Contact**
1.0	First development	Sonja Buchegger (CSC/KTH)	buc@csc.kth.se
1.1	Added submission instructions	Sonja Buchegger (CSC/KTH)	buc@csc.kth.se
2.0	Adaptations for HT2013	Guillermo Rodríguez Cano (CSC/KTH)	gurc@csc.kth.se
2.1	Restructuring and editorial changes	Benjamin Greschbach (CSC/KTH)	bgre@csc.kth.se
2.2	Adaption for HT2018	Andreas Lindner (EECS/KTH)	andili@kth.se
2.3	more adaption for HT2018	Sonja Buchegger (EECS/KTH)	buc@kth.se
2.4	Adaption for HT2019	Md Sakib Nizam Khan (EECS/KTH)	msnkhan@kth.se
2.5	Adaption for HT2020	Md Sakib Nizam Khan (EECS/KTH)	msnkhan@kth.se
2.6	Adaption for HT2021	Md Sakib Nizam Khan (EECS/KTH)	msnkhan@kth.se
2.7	Adaption for HT2022	Anoud Alshnakat (EECS/KTH)	anoud@kth.se