Mittuniversitetet
MID SWEDEN UNIVERSITY

Project:
A Short Study in Information Security

Daniel Bosk*

–sourcefile– –revision– –time– –owner–

Contents

1 Introduction

The area of information security paces forward at high speed due to the constant arms race between attackers and defenders. It is thus very important to continuously review and improve one's security. If you do not, then your adversary is the only one who will—and your adversary will not tell you about the findings.

There are also other reasons for having security. For instance, when enormous amounts of information about people is collected into databases it is advicable to oversee the protection of that information. Firstly for the organisation holding this information. Secondly, and more importantly, for the individual whose information is stored in such a database; e.g. the organisation owning the database might choose to change their "terms of service" and start using the information in other ways—ways which might be unacceptable to the individual.

2 Scope and Aim

The aims of this assignment is that you should deepen your knowledge of security by making a short study in one of the areas in security.

After completing this assignment you should be able to:

- Use scientific methods to explore problems in the area.
- Read and understand the research literature in the area.

3 Theory

The base theory of this assignment is the foundational knowledge in security. Then you will also need to deepen your knowledge by looking into current research.

4 Assignment

You are going to make a short study within the area of information security. The area is chosen in corroboration with the tutor. The first thing you should do is to find a proper set of research questions. For inspiration see the section "Research Problems" in the end of each chapter in Anderson's *Security Engineering* [1]. Other ideas for this project are the following:

Security in an organisation Agree with the head of security in some organisation and analyse the security in their organisation. This can be some form of penetration testing, e.g. performing a social-engineering-based attack, or performing a gap analysis. This is a prestudy, but the methodology should be very well worked out for a larger follow-up study. (Do not forget the research connection, e.g. methodology: why this study is best designed this way.)

Advanced Persistent Threats Examine weaknesses in large systems which are common in different organisations, then connect these into an APT-scenario. This scenario should be well founded by documented vulnerabilities and research.

Security usability An example study could look into increasing the usability and security of e.g. payment systems. First look at the current usability and security, then suggest improvements and methods to test these. The emphasis should be on security: it must be more usable and at least as secure.

Applied security Improve a current product, or invent a new one, using research results from the area of information security. E.g. better privacy properties in streaming services [3]. Then your presentation will be a sales pitch to your security-aware classmates—the focus must be on the security details. Your report should then be usable for selling this product to a company for production.

Reproducible research Read and replicate "some cool paper", e.g. [2]. Read how they did it, then you do the same setup and show it off to the class. You should present your insights, e.g.: how difficult this is to perform, what is required to perform it. In summary, who is the adversary and what can he or she do with this.

Once you have chosen a problem to focus on you start your work. Your results must be scientifically founded. You have inspiration for your methodology from experiences from earlier courses, but also from the methods presented in the research papers.

Start writing the report directly from the start, it is usually much easier to write the report while doing the work. Start by writing the introduction with aims and what problem to solve. Then continue with the section on theory and methodology as you work on developing how to answer your questions. After this you can go ahead and do the actual work, then write the results and analyse them. Finally discuss and conclude your findings in the last section of the report.

5 Examination

Your study should result in a written academic report, and an oral presentation of said report. The report must be handed-in in the course platform in PDF or PostScript format, no other formats are accepted. You can find the timeslots for presentations in the course schedule.

The report (and presentation) must provide the reader with a short overview of the security field to illustrate wherein the treated topic belongs.

The assignment may be done in groups of up to two people. However, if the project proposed is of proper size you may be excused from this limit. Talk to the tutor and motivate well why you have to be a larger group.

References

[1] Ross J. Anderson. *Security Engineering. A guide to building dependable distributed systems*. 2nd ed. Indianapolis, IN: Wiley, 2008. ISBN: 978-0-470-06852-6 (hbk.) URL: http://www.cl.cam.ac.uk/~rja14/book.html.

[2] Daniel Genkin, Adi Shamir, and Eran Tromer. "RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis". In: *Advances in Cryptology – CRYPTO 2014*. Ed. by JuanA. Garay and Rosario Gennaro. Vol. 8616. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2014, pp. 444–461. ISBN: 978-3-662-44370-5. DOI: 10.1007/978-3-662-44371-2_25. URL: http://dx.doi.org/10.1007/978-3-662-44371-2_25.

[3] M.Z. Lee, A.M. Dunn, B. Waters, E. Witchel, and J. Katz. "Anon-Pass: Practical Anonymous Subscriptions". In: *Security and Privacy (SP), 2013 IEEE Symposium on*. 2013, pp. 319–333. DOI: 10.1109/SP.2013.29. URL: http://dx.doi.org/10.1109/SP.2013.29.