

# A study guide to Information Security for systems administrators

Daniel Bosk

Department of Information Systems and Technology  
Mid Sweden University, Sundsvall

School of Computer Science and Communication  
KTH Royal Institute of Technology, Stockholm

24th April 2019

## **Abstract**

The study guide covers provides an overview of the course: the scope and intended learning outcomes, how the teaching is organized to achieve that, what is studied when, what to do if you miss the due times for assignments etc.

# Contents

<b>1</b>	<b>Scope and aims</b>	<b>3</b>
1.1	Intended learning outcomes . . . . .	3
<b>2</b>	<b>Course structure and overview</b>	<b>3</b>
2.1	Teaching and tutoring . . . . .	4
2.2	Schedule . . . . .	4
<b>3</b>	<b>Course contents</b>	<b>4</b>
3.1	S0 What's up with security? . . . . .	4
3.2	Foundations . . . . .	6
3.3	Managing information security . . . . .	7
3.3.1	MSB part I . . . . .	7
3.3.2	M1 Information security management system . . . . .	7
3.3.3	MSB part II . . . . .	7
3.3.4	M2 and S3 Assessment and risk analysis . . . . .	7
3.3.5	Information security from a records management perspective . . . . .	7
3.4	Cryptography . . . . .	8
3.5	Authentication . . . . .	9
3.5.1	L4 Evaluating and designing authentication . . . . .	9
3.5.2	L5 Private communication . . . . .	10
3.6	Protocols . . . . .	10
3.7	Access control . . . . .	11
3.8	Accountability . . . . .	11
3.9	Differential privacy . . . . .	11
3.10	Software security . . . . .	12
3.11	Trusted computing . . . . .	12
3.12	P6 Analysing information security in an organization . . . . .	13
<b>4</b>	<b>Assessment</b>	<b>13</b>
4.1	Handed-in assignments . . . . .	13
4.2	'What if I'm not done in time?' . . . . .	14

# 1 Scope and aims

The aim of the course is that after the course you should be able to make high-level designs for secure solutions, i.e. combine relevant research results based on their high-level properties into a solution with the desired security, privacy and usability properties. The problems and solutions can be in both the technical or organizational domain.

## 1.1 Intended learning outcomes

More concretely, after completing the course, you should be able to:

- *evaluate* the usability of security solutions and *suggest* improvements that improve usability and security.
- *evaluate* threats, possible protection mechanisms and *suggest* a high-level approach to protection which considers usability.
- *overview* the field of information security, *understand* your own limits and where to search for solutions, e.g. experts or published research results that are relevant to the solution of a problem.
- *analyse and apply* the results of published research in the security field.
- *apply* the Swedish Civil Contingency Agency's Framework for Information Security Management Systems (ISO 27000) to *analyse, assess and improve* the information security in an organization.

The course has a variety of learning sessions designed to ensure that you learn these intended learning outcomes (ILOs). Each such session has a set of further specified ILOs that will help you achieve the ILOs above.

We will apply the following grading criteria.

**Grade E** You fulfil all the ILOs at the minimum level.

**Grade A** You fulfil all the ILOs, your evaluations and designs are extensive and well-founded in theory and, where applicable, the research literature and otherwise show deep insights in how to use the building-blocks from the literature.

The grades B, C and D are intermediary grades. When assessing the multi-dimensional domain of your knowledge we will try to make as fair a projection as possible onto this linear scale.

## 2 Course structure and overview

The course is divided into three parts. The first part of the course covers the foundations of security: what it is, how to evaluate new knowledge in the field. This covers both purely technical aspects, but also includes human aspects such as usability — even if a system is proved secure, it will offer no security if its human users cannot use it.

The second part of the course covers information security on a strategic level, this concerns organizational management systems for information security: how

to implement these and how to continuously run them in an organization. It also includes threat and risk analysis. The main material is produced by the Swedish Civil Contingencies Agency (MSB) and is based on the ISO 27000 standard.

The third part of the course covers the technical aspects: how to design security (and not to design security). The focus in this part of the course is on security mechanisms and how to use these in secure systems.

## 2.1 Teaching and tutoring

The teaching of the course is oriented towards active learning. I.e. the course consists of learning sessions which requires active participation.

Generally, you are expected to read the material in advance. During the learning session the most important parts of the material will be discussed and you will perform some tasks to work with the topic in groups, i.e. to apply it to learn it more efficiently. Some modules of the course will have several learning sessions linked together, e.g. a starting seminar, followed by laboratory work which is then summarized and used in a final seminar.

## 2.2 Schedule

In Table 1 you will find an overview of the schedule for the course. The detailed schedule can be found in the University's central scheduling system. The details for each session can be found in Section 3.

# 3 Course contents

This section summarizes each of the learning sessions, i.e. what they cover, what you are expected to learn and its reading material.

## 3.1 S0 What's up with security?

*Summary:* The purpose of this assignment is to get an idea of how security affects products, which in turn affects not only the companies behind them, but also the consumers and can have effects on a societal scale.

*Intended learning outcomes:* The aim of this assignment is

- to *reflect* on the effects of security, or lack thereof, on both individual and society.
- to *value and argue* about the responsibilities of engineers.

*Reading:* To be able to reason and have a discussion, we will have some ethics guidelines as a base: *Code of Ethics: ACM Code of Ethics and Professional Conduct* [1], *Software Engineering Code of Ethics and Professional Practice* [2] and *IEEE Code of Ethics* [3].

First, you must read up on the influence campaigns during the 2016 US election [4]. Then you must read up on the Cambridge Analytica scandal [e.g. 5–8] and the Mirai botnet incident [9].

Finally, you should search for and read current news articles of your own choice illustrating the problem of lacking security.

Course week	Work
1	Session: Introduction Seminar: What's up with security? (Section 3.1) Foundations: What is security?, The scientific method, Attacking humans, Psychology (Section 3.2) Session: Foundations
2	Lecture: MSB's framework, part I (Section 3.3) Start working on M1 (Section 3.3.2) Lecture: MSB's framework, part II Start working on M2, prepare S3 (Section 3.3.4) Lecture: Records management
3	Crypto: Shannon entropy, Some applications of info theory (Section 3.4) Crypto: High-level overview of modern crypto Authentication (Section 3.5) Session: Crypto, Authentication
4	Seminar: L4 (Section 3.5.1) part I Seminar: L4 part II Seminar: L5 (Section 3.5.2)
5	Protocols (Section 3.6) Access control (Section 3.7) Accountability (Section 3.8) Session: Protocols, Access control, Accountability
6	Privacy (Section ??) Software security (Section 3.10) Trusted computing (Section 3.11) Session: Privacy, Software and Trusted Computing
7	Tutoring: P6 (Section 3.12) Seminar: S3 (Section 3.3.4)
8	Tutoring: P6 (gaproject)
9	Tutoring: P6 (gaproject)
10	Presentation: P6 (gaproject) Second grading: M1 (isms), M2 (risk) Second seminar: S3 (risk), L4 (pwdeval), L5 (pricomlab)
+3 months	Second presentation: P6 (gaproject) Final grading: M1 (isms), M2 (risk) Final seminar: S3 (risk), L4 (pwdeval), L5 (pricomlab)
+6 months	Final presentation: P6 (gaproject)

Table 1: A summary of the parts of the course and when they will (or should) be done. The table is adapted to taking this course at half-time pace, i.e. 20 hours per week for 10 weeks.

## 3.2 Foundations

**What is security?** *Summary:* In this learning session we will cover the foundations of security. By this we mean what security is all about, e.g. what types of properties we are interested in and what we want to achieve in our security work.

*Intended learning outcomes:* After this session you should be able:

- to *understand* the what security is generally about.

*Reading:* You should read Gollmann’s chapter on ‘Foundations of Computer Security’ [10, Chap. 3]. There he attempts at a definition of Computer Security and related terms, e.g. confidentiality, integrity, and availability, which we need for our treatment of the topic. Anderson also covers this in Chapter 1 of [11]. He also treats a wider area than just *computer* security, which is good for us, he covers many aspects of security in different examples.

**The scientific method** *Summary:* In this learning session we will give an introduction to the scientific method and particularly how this can be applied in the area of security.

*Intended learning outcomes:* After this session you should be able:

- to *differentiate* which types of scientific methods are appropriate to answer a given question.

*Reading:* You should read ‘How to Design Computer Security Experiments’ [12]. This paper discusses the scientific method of (parts of) the security field. For a more in-depth reflection on the state of security as a scientific pursuit, we recommend ‘SoK: Science, Security and the Elusive Goal of Security as a Scientific Pursuit’ [13].

**Attacking humans** *Summary:* One important aspect of security is users’ weaknesses. There are many ways to attack systems through their human operators. During this learning session we cover a variety of examples of such attacks.

*Intended learning outcomes:* After this learning session you should be able:

- to *adopt* an adversarial thinking for situations involving humans.

*Reading:* Anderson gives a short summary of the psychology of users, their strengths and weaknesses, in Chapter 2 “Usability and Psychology” of *Security Engineering* [11].

**Psychology** *Summary:* One important aspect of security, which technical people tend to forget, is the users’ weaknesses. The psychology of the human mind is therefore an important subject to discuss in the context of security. And consequently, we must adapt our systems to those limitations. In this learning session, we will focus on relevant parts of our psychology.

*Intended learning outcomes:* After this learning session you should be able:

- to *incorporate* basic psychology in the design of a system to increase its security.

*Reading:* Anderson gives a short summary of the psychology of users, their strengths and weaknesses, in Chapter 2 ‘Usability and Psychology’ of *Security Engineering* [11].

### **3.3 Managing information security**

#### **3.3.1 MSB part I**

This lecture covers the first part of MSB’s framework [14–18], i.e. ISO 27001. This part covers how to initialise the work with security in an organisation, i.e. how to set up an Information Security Management System (ISMS). We will talk about the most important steps in this process.

#### **3.3.2 M1 Information security management system**

Before writing this memo, you should have read the following:

- *Introduktion till metodstödet* [14],
- *Säkra ledningens engagemang* [15], and
- *Projektplanering* [16].

#### **3.3.3 MSB part II**

This lecture covers the remaining part of MSB’s material [19–31]. This part of the material treats how to run an ISMS. The largest part is the gap analysis, i.e. finding the gap between the security practices in the organisation and the practices recommended by ISO 27000. The main point of this part is not something done once and never again, an ISMS is a continuous process.

#### **3.3.4 M2 and S3 Assessment and risk analysis**

Before doing this assignment you should have read the following:

- *Verksamhetsanalys* [17] and
- *Risicanalys* [18]

#### **3.3.5 Information security from a records management perspective**

Records and Archives management deals with certain kinds of information that is related to business processes, and serve as evidence of activities. Why it can foreexample be used for accountability purposes, contracts, regulate business relations and more. Therefore it is important to ensure the quality of the information, and that it is not manipulated for example. The trustworthiness of the information is central, and gaprojectopment of criteria and practices to ensure that. The emphasis is on the information, and also to understand the context in which the information is created and managed. Business process analysis is therefore a central activity. The National Archives of Sweden and the Swedish Civil Contingencies Agency has for example had some collaboration in that area.

The lecture will be an introduction to archives and information science, basic concepts, processes, business process analysis and information mapping. It covers material from primarily *Vägledning för processororienterad informationskartläggning* [32] and the standard ISO 30300:2011 [33].

### 3.4 Cryptography

**Basic informatino theory** *Summary:* The area of Information Theory was founded in 1948 by Claude Shannon. It is a mathematical theory to reason about how much information is contained in certain data. Equivalently, it is also a measure of uncertainty in information, and has thus plenty of application in security and cryptography. This learning session covers the basic concept: Shannon entropy.

*Intended learning outcomes:* After the session you should be able

- to *apply* Shannon entropy in basic situations.

*Reading:* The concept of Shannon entropy, the main part of information theory, is treated in a few short texts: *A Primer on Information Theory and Privacy* [34] and ‘Chapter 6: Shannon entropy’ [35].

**Some applications of information theory** *Summary:* There are various uses for information theory. In this session we will explore some of them.

*Intended learning outcomes:* After this session you should be able

- to *understand* how Shannon entropy can be applied in various areas.

*Reading:* You should read on the use of entropy to estimate anonymity: ‘How Unique Is Your Browser?’ [36]. This is then utilised in the text ‘Grundläggande lösenordsanalys’ [37] (in Swedish), and ‘Of passwords and people: Measuring the effect of password-composition policies’ [38] which treats passwords.

**A high-level overview of crypto** Cryptography has a central role in security. To fully understand how many security mechanisms can be implemented we need cryptography. For this reason, we also need higher-level knowledge about what can be achieved with cryptography to not limit our thoughts about possible solutions. This learning session is intended to give a high-level overview of cryptography: symmetric-key encryption, public-key encryption, digital signatures, zero-knowledge proof and secure multiparty computation. In particular, the ILOs are that you should be able to

- *understand* what properties can be achieved with cryptography.
- *analyse* a situation and *suggest* what cryptographic properties are desirable.

The basics are covered by Chapter 5 in Anderson’s *Security Engineering* [11] and Chapter 14 in Gollmann’s *Computer Security* [10]. (To practice your understanding of these mechanisms it is recommended to do exercises 14.2, 14.3 and 14.7 in [10].) For the remaining topics, however, we refer to the *Encyclopedia of cryptography and security* [39] (and cited papers and books).

## 3.5 Authentication

Authentication is part of the core of security. An entity claims something, a property or an identity, authentication is about verifying or rejecting any such claim. We will discuss three aspects of authentication: user-to-machine (and user-to-user), machine-to-user, machine-to-machine. For user authentication we will start with the traditional something you know, something you have and something you are and then look beyond.

More specifically, the session should prepare you to be able to

- *understand* the authentication and usability problems of authentication involving users.
- *analyse* the requirements for authentication in a situation and *design* an authentication system with desired authentication properties and usability.

Why we want to do this and how we can accomplish this is treated in Chapter 4 in [10]. Anderson also treats this topic [11, Chap. 2], although in a wider perspective with less technical details. When you have studied this material you should do exercises 4.2, 4.3, 4.4 and 4.6 in [10]. For the treatment of anonymous credentials, we refer to ‘Electronic Identities Need Private Credentials’ [40] and ‘Anon-Pass: Practical Anonymous Subscriptions’ [41].

### 3.5.1 L4 Evaluating and designing authentication

A lot of user authentication is based on passwords. We use password policies to aid users in selecting a secure password. Unfortunately, research has shown that the common password-policies do not have the expected effect: users can still choose easy-to-guess passwords and the policies actually makes guessing easier. It is thus important to *scientifically* evaluate the actual effects of any user-authentication mechanism, otherwise our security might be at risk. Here we will focus on exactly that. More specifically, after this lab you should be able to

- *evaluate* the effective security by considering security and usability.
- *analyse* research results in usable security and *apply* those relevant to a given situation.
- *design* security policies aligned with usability.

To do this, we must be familiar with several topics: usability [11, Ch. 2], cryptography [11, Ch. 5] [42], information theory [35] and the scientific method [43]. The main contents is some research papers on password security and usability: ‘Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms’ [44], ‘Of passwords and people: Measuring the effect of password-composition policies’ [45], ‘Can long passwords be secure and usable?’ [46] and ‘The Password Life Cycle’ [47]; complemented by a paper on the usability of password managers: ‘A comparative usability evaluation of traditional password managers’ [48].

### 3.5.2 L5 Private communication

The more our society depends on digital systems, the more important private communication becomes. We need private communications to sustain democracy, thus we need it to be available to everyone. The purpose of this laboratory work is to introduce some practical aspects of private messaging. More specifically, after it, you should be able to

- *apply* (securely!) some common implementations of cryptography for private communication — also including any set-up (e.g. key verification).
- *analyse* different systems for private communication based on their security properties and *evaluate* which is suitable in a given situation.
- *evaluate* different implementations of private communication from a usability perspective.

The topics of this assignment are: usability [11, Ch. 2] and cryptography [11, Ch. 5] and privacy-enhancing technologies [11, Ch. 23.4]. We then rely on the ‘Why Johnny can’t encrypt’ papers:

- ‘Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0.’ [49],
- ‘Why Johnny still can’t encrypt: Evaluating the usability of email encryption software’ [50],
- ‘Why Johnny still, still can’t encrypt: Evaluating the usability of a modern PGP client’ [51],
- ‘Can Johnny finally encrypt?: evaluating E2E-encryption in popular IM applications’ [52].

## 3.6 Protocols

As soon as two principals need to interact, there is need for a protocol — be it inside or between systems, even one principal communicating with itself in different points in time (which is the case when storing something for use at a later time). These protocols need different properties. We will explore how to design secure protocols and introduce some tools for verifying security properties of protocols.

More concretely, after this session you should be able to

- *understand* the different approaches and their limits to verify the security of protocols.

Anderson gives an overview of this area in *Security Engineering* [11], Chapter 3 ‘Protocols’. Gollmann has a more technically oriented treatment of a part of this topic in Chapter 15 of *Computer Security* [10]. To complement these texts we will also touch upon some of the material in ‘Modeling and Verifying Security Protocols with the Applied Pi Calculus and ProVerif’ [53].

### 3.7 Access control

Once you have authenticated users you can support access control — and this is also one of the main reasons to authenticate them in the first place. Access control aims at controlling who may access what and how they may access it. There are different models and ways to implement access control. Here we will give an overview of the possibilities. In particular, the ILOs are that you are able to:

- *understand* the fundamental access control models — discretionary access control, mandatory access control, role-based access control and attribute-based access control — and their relations.
- *evaluate* advantages and disadvantages of different access control solutions.
- *analyse* a situation and *design* a proper access control solution.

The reading material is Chapter 5, followed by Chapters 11 and 12, in *Computer Security* [10]. You are also recommended to read Anderson’s treatment of the subject, he treats this in Chapters 4, 8, and 9 in *Security Engineering* [11]. Finally, you should be able to do exercises 5.1 5.2, 5.5, 5.6, 5.8 and 5.9 in [10].

### 3.8 Accountability

The need for accountability has been apparent in civilisations for as long as they have existed. One of today’s institutions which is historically renowned for keeping strict accounts is the state tax office, another is, of course, the banks. We will explore some principles in keeping accounts and discuss ways to implement it in different, sometimes challenging, environments. In particular, the ILOs are that you are able to:

- *evaluate* advantages and disadvantages of different levels of accountability.
- *analyse* a situation and *design* proper accountability and, in particular, with privacy considerations.

Anderson describes accountability through his experience from banks in Chapter 10 ‘Banking and Bookkeeping’ in *Security Engineering* [11]. We will also use the secure logging system of Schneier and Kelsey [54] as an example of how to achieve secure logging in a challenging environment. The construction described therein is a method to safely store audit logs in an untrusted machine; in the scheme, all log entries generated prior to a compromise will be impossible for the attacker to read, modify, or destroy undetectably.

### 3.9 Differential privacy

In this session we look at differential privacy [55]. We review the definitions of what it is and look at a variety of uses.

The literature we rely on consists of the following:

- ‘Differential privacy’ [55]
- ‘Differential privacy: A survey of results’ [56]

The above cover the basic theory of differential privacy. We will furthermore look at an interesting application of differential privacy in:

- ‘Challenging Differential Privacy: The Case of Non-interactive Mechanisms’ [57]
- ‘Private Similarity Computation in Distributed Systems: From Cryptography to Differential Privacy’ [58]
- ‘BLIP: Non-interactive Differentially-Private Similarity Computation on Bloom filters’ [59]

### 3.10 Software security

Perhaps the part of security most people intuitively associate with security, and computer security in particular, is software security. This part of computer security treats vulnerabilities in software, e.g. buffer overruns or code injections. This is a very important part of security, because although the design is flawless, its implementation might have vulnerabilities. As an example, most phones are designed to keep the user and applications unprivileged, thus all applications will run with the principle of least privileges and compartmentalized from each other. However, software bugs in the operating system can allow malicious apps to gain privileges to e.g. monitor other apps.

After this session you should be able to

- *understand* the need to consider software security in software development.
- *evaluate* the software security requirements for different situations.

Gollmann treats this area in Chapter 10 of his book, *Computer Security* [10]. The recommended exercises to do after reading this material are 10.1, 10.3 and 10.4 in [10]. Anderson also treats this subject — in Chapter 4.4 and Chapter 18 of *Security Engineering* [11] — albeit with less technical details. We also treat the results of ‘Four Software Security Findings’ [60].

### 3.11 Trusted computing

One can only do so much with software. The problem with software and general purpose processors is that the software can be modified and the processor will still execute it. Some examples: Alice left the laptop in the hotel room while having breakfast, perhaps the hotel aide replaced the bootloader to break Alice’s full-disk encryption? Or, how can Alice even trust the computer when it is brand new? Another aspect of this is to protect parts of the system from Alice herself, e.g. this is what digital rights management is all about. We also have the compartmentalization of apps in a smartphone. If Alice accidentally installs a malicious app, it shouldn’t be able to compromise the banking app. Here we will explore how to ensure the integrity of the computer system.

More concretely, after this session you should be able to

- *understand* the problem of trusted computing, its approaches to solutions, the underlying assumptions and its limitations.

LADOK	ECTS	Grade	Course assignments
X104	0.0	P, F	S0
I104	1.5	P, F	M1, M2, S3
L104	1.5	P, F	L4, L5
R104	4.5	A–F	P6
Total	7.5	A–F	P6

Table 2: Table summarizing course modules and their mapping to LADOK. P means pass, F means fail. A–E are also passing grades, where A is the best.

- *analyse* different approaches to trusted computing and their limitations and *apply* them in a solution to a given problem.

We treat the material in Chapters 16, 17, 18, 22 and 23 in *Security Engineering* [11]. The papers [61–63] illustrates just how difficult this can be. The authors extract encryption keys using acoustic side-channels, i.e. they analyse the sound emitted by the electrical circuitry to find the computations done and hence derive the bits of the key used.

### 3.12 P6 Analysing information security in an organization

In this project we will explore information security management in organizations further. In particular, it will provide some practical experience.

After this project you should be able

- to *analyse* threats to information security and to *suggest* suitable protection mechanisms against these.
- to *apply* MSB’s framework to analyse, evaluate and give suggestions of improvements for the information security in an organization.

The work is based on the material by MSB: *Gapanalys* [19] med bilaga [64].

## 4 Assessment

This section explains how the course modules are graded and mapped to LADOK. Table 2 visualizes the relations between modules, credits, grades and LADOK.

The project report is graded from A to F, where A–E are for passing and F and Fx are for failing. The project also includes an oral presentation which is graded pass (P) or fail (F), and is reported with the project to LADOK. The grade of the project will also be the grade of the course total.

### 4.1 Handed-in assignments

In general, all hand-ins in the course must be in a ‘passable’ condition; i.e. they must be well-written, grammatically correct and without spelling errors, have citations and references according to [65] (see also [66] for a tutorial), and finally fulfil all requirements from the assignment instruction. If you hand something in which is not in this condition, you will receive an F without further comment.

All material handed-in must be created by yourself, or, in the case of group assignments, created by you or one of the group members. When you refer to or quote other texts, then you must provide a correct list of references and, in the case of quotations, the quoted text must be clearly marked as quoted. If any part of the document is plagiarized you risk being suspended from study for a predetermined time, not exceeding six months, due to disciplinary offence. If it is a group assignment, all group members will be held accountable for disciplinary offence unless it is clearly marked in the work who is responsible for the part containing the plagiarism.

If cooperation takes place without the assignment instruction explicitly allowing this, this will be regarded as a disciplinary offence with the risk of being suspended for a predetermined time, not exceeding six months. Unless otherwise stated, all assignments are to be done individually.

## 4.2 ‘What if I’m not done in time?’

The deadlines on this course are of great importance, make sure to keep these!

For seminars and presentations there will be three sessions during the course of a year, if you cannot make it to any of those you will have to return the next time the course is given; i.e. up to a year later. All of these sessions will be in the course schedule (in the Student Portal). If you miss a deadline for the preparation for a seminar session, then you have to go for the next seminar even if the first seminar has not passed yet.

Written assignments are graded once during the course, most often shortly after the deadline of the assignment. After the course you are offered two more attempts within a year. In total you have three chances for having your assignments graded over the period of a year. After that you should come back the next time the course is given.

No tutoring is planned after the end of the course, i.e. after the last tutoring session scheduled in the course schedule. If you are not done with your assignments during the course and want to be guaranteed tutoring you have to reregister for the next time the course is given. Reregistration is a lower priority class of applicants for a course, all students applying for the course the first time have higher priority – this includes reserves too.

Thus, if you feel that you will not be done with the course on time, it is better to stop the course at an early stage. If you register a break within three weeks of the course start, you will be in the higher priority class of applicants the next time you apply for the course. You can register such a break yourself in the Student Portal.

## References

- [1] Association for Computing Machinery. *Code of Ethics: ACM Code of Ethics and Professional Conduct*. Accessed on 4 April 2014. URL: <https://www.acm.org/about/code-of-ethics>.
- [2] Association for Computing Machinery. *Software Engineering Code of Ethics and Professional Practice*. Accessed on 27 March 2019. URL: <https://ethics.acm.org/code-of-ethics/software-engineering-code/>.

- [3] Institute of Electrical and Electronics Engineers. *IEEE Code of Ethics*. Accessed on 4 April 2014. URL: <http://www.ieee.org/about/corporate/governance/p7-8.html>.
- [4] Scott Shane and Mark Mazzetti. ‘Inside a 3-Year Russian Campaign to Influence U.S. Voters’. en-US. In: *The New York Times* (Nov. 2018). ISSN: 0362-4331. URL: <https://www.nytimes.com/2018/02/16/us/politics/russia-mueller-election.html> (visited on 21/01/2019).
- [5] Andrea Valdez. ‘Everything You Need to Know About Facebook and Cambridge Analytica’. In: *Wired* (Mar. 2018). ISSN: 1059-1028. URL: <https://www.wired.com/story/wired-facebook-cambridge-analytica-coverage/> (visited on 17/01/2019).
- [6] Carole Cadwalladr and Emma Graham-Harrison. ‘Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach’. en-GB. In: *The Guardian* (Mar. 2018). ISSN: 0261-3077. URL: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-%20influence-us-election> (visited on 17/01/2019).
- [7] Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr. ‘How Trump Consultants Exploited the Facebook Data of Millions’. en-US. In: *The New York Times* (Apr. 2018). ISSN: 0362-4331. URL: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-c%20campaign.html> (visited on 17/01/2019).
- [8] Ishaan Tharoor. *Analysis — The scary truth that Cambridge Analytica under stands*. en. 2018. URL: <https://www.washingtonpost.com/news/worldviews/wp/2018/03/22/the-scary-truth-that-cambridge-analytica-understands/> (visited on 17/01/2019).
- [9] Bruce Schneier. *Lessons From the Dyn DDoS Attack - Schneier on Security*. 2016. URL: [https://www.schneier.com/blog/archives/2016/11/lessons\\_from\\_th\\_5.html](https://www.schneier.com/blog/archives/2016/11/lessons_from_th_5.html) (visited on 17/01/2019).
- [10] Dieter Gollmann. *Computer Security*. 3rd ed. Chichester, West Sussex, U.K.: Wiley, 2011. ISBN: 9780470741153 (pbk.)
- [11] 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>.
- [12] Sean Peisert and Matt Bishop. ‘How to Design Computer Security Experiments’. In: *Fifth World Conference on Information Security Education*. Ed. by Lynn Fitcher and Ronald Dodge. Boston, MA: Springer US, 2007, pp. 141–148. ISBN: 978-0-387-73269-5.
- [13] C. Herley and P. C. v. Oorschot. ‘SoK: Science, Security and the Elusive Goal of Security as a Scientific Pursuit’. In: *2017 IEEE Symposium on Security and Privacy (SP)*. May 2017, pp. 99–120. DOI: 10.1109/SP.2017.38.
- [14] Helena Andersson, Jan-Olof Andersson, Fredrik Björck, Martin Eriksson, Rebecca Eriksson, Robert Lundberg, Michael Patrickson and Kristina Starkerud. *Introduktion till metodstödet*. Dec. 2011. URL: <http://www.informationssakerhet.se>.

- [15] Helena Andersson, Jan-Olof Andersson, Fredrik Björck, Martin Eriksson, Rebecca Eriksson, Robert Lundberg, Michael Patrickson and Kristina Starkerud. *Säkra ledningens engagemang*. Dec. 2011. URL: <http://www.informationssakerhet.se>.
- [16] Helena Andersson, Jan-Olof Andersson, Fredrik Björck, Martin Eriksson, Rebecca Eriksson, Robert Lundberg, Michael Patrickson and Kristina Starkerud. *Projektplanering*. Dec. 2011. URL: <http://www.informationssakerhet.se>.
- [17] Helena Andersson, Jan-Olof Andersson, Fredrik Björck, Martin Eriksson, Rebecca Eriksson, Robert Lundberg, Michael Patrickson and Kristina Starkerud. *Verksamhetsanalys*. Dec. 2011. URL: <http://www.informationssakerhet.se>.
- [18] Helena Andersson, Jan-Olof Andersson, Fredrik Björck, Martin Eriksson, Rebecca Eriksson, Robert Lundberg, Michael Patrickson and Kristina Starkerud. *Risikanalys*. Dec. 2011. URL: <http://www.informationssakerhet.se>.
- [19] Helena Andersson, Jan-Olof Andersson, Fredrik Björck, Martin Eriksson, Rebecca Eriksson, Robert Lundberg, Michael Patrickson and Kristina Starkerud. *Gapanalys*. Dec. 2011. URL: <http://www.informationssakerhet.se>.
- [20] Helena Andersson, Jan-Olof Andersson, Fredrik Björck, Martin Eriksson, Rebecca Eriksson, Robert Lundberg, Michael Patrickson and Kristina Starkerud. *Välja säkerhetsåtgärder*. Dec. 2011. URL: <http://www.informationssakerhet.se>.
- [21] Helena Andersson, Jan-Olof Andersson, Fredrik Björck, Martin Eriksson, Rebecca Eriksson, Robert Lundberg, Michael Patrickson and Kristina Starkerud. *Utforma säkerhetsprocesser*. Dec. 2011. URL: <http://www.informationssakerhet.se>.
- [22] Helena Andersson, Jan-Olof Andersson, Fredrik Björck, Martin Eriksson, Rebecca Eriksson, Robert Lundberg, Michael Patrickson and Kristina Starkerud. *Utforma policy och styrdokument*. Dec. 2011. URL: <http://www.informationssakerhet.se>.
- [23] Helena Andersson, Jan-Olof Andersson, Fredrik Björck, Martin Eriksson, Rebecca Eriksson, Robert Lundberg, Michael Patrickson and Kristina Starkerud. *Planera genomförande*. Dec. 2011. URL: <http://www.informationssakerhet.se>.
- [24] Helena Andersson, Jan-Olof Andersson, Fredrik Björck, Martin Eriksson, Rebecca Eriksson, Robert Lundberg, Michael Patrickson and Kristina Starkerud. *Konstruera och anskaffa*. Dec. 2011. URL: <http://www.informationssakerhet.se>.
- [25] Helena Andersson, Jan-Olof Andersson, Fredrik Björck, Martin Eriksson, Rebecca Eriksson, Robert Lundberg, Michael Patrickson and Kristina Starkerud. *Införa*. Dec. 2011. URL: <http://www.informationssakerhet.se>.

- [26] Helena Andersson, Jan-Olof Andersson, Fredrik Björck, Martin Eriksson, Rebecca Eriksson, Robert Lundberg, Michael Patrickson and Kristina Starkerud. *Övervaka*. Dec. 2011. URL: <http://www.informationssakerhet.se>.
- [27] Helena Andersson, Jan-Olof Andersson, Fredrik Björck, Martin Eriksson, Rebecca Eriksson, Robert Lundberg, Michael Patrickson and Kristina Starkerud. *Granska*. Dec. 2011. URL: <http://www.informationssakerhet.se>.
- [28] Helena Andersson, Jan-Olof Andersson, Fredrik Björck, Martin Eriksson, Rebecca Eriksson, Robert Lundberg, Michael Patrickson and Kristina Starkerud. *Ledningens genomgång*. Dec. 2011. URL: <http://www.informationssakerhet.se>.
- [29] Helena Andersson, Jan-Olof Andersson, Fredrik Björck, Martin Eriksson, Rebecca Eriksson, Robert Lundberg, Michael Patrickson and Kristina Starkerud. 'Utveckla LIS och skyddet'. Dec. 2011. URL: <http://www.informationssakerhet.se>.
- [30] Helena Andersson, Jan-Olof Andersson, Fredrik Björck, Martin Eriksson, Rebecca Eriksson, Robert Lundberg, Michael Patrickson and Kristina Starkerud. 'Kommunicera förbättringar'. Dec. 2011. URL: <http://www.informationssakerhet.se>.
- [31] Helena Andersson, Jan-Olof Andersson, Fredrik Björck, Martin Eriksson, Rebecca Eriksson, Robert Lundberg, Michael Patrickson and Kristina Starkerud. 'Fortsatt arbete'. Dec. 2011. URL: <http://www.informationssakerhet.se>.
- [32] Myndigheten för samhällsskydd och beredskap (MSB) och Riksarkivet. *Vägledning för processororientad informationskartläggning*. Tech. rep. Nov. 2012. URL: <https://riksarkivet.se/Media/pdf-filer/V%C3%A4gledning%C3%B6r%20processororientad%20informationskartl%C3%A4ggning.pdf>.
- [33] *Information and documentation – Management systems for records – Fundamentals and vocabulary*. Standard. Available in Swedish from the library in database "E-nav SIS standarder". Geneva, CH: International Organization for Standardization, Nov. 2011.
- [34] Peter Eckersley. *A Primer on Information Theory and Privacy*. Jan. 2010. URL: <https://www.eff.org/deeplinks/2010/01/primer-information-theory-and-privacy>.
- [35] Daniel Ueltschi. 'Chapter 6: Shannon entropy'. URL: <http://www.ueltschi.org/teaching/chapShannon.pdf>.
- [36] Peter Eckersley. 'How Unique Is Your Browser?' In: *Privacy Enhancing Technologies*. Springer. 2010, pp. 1–18. URL: <https://panopticlick.eff.org/static/browser-uniqueness.pdf>.
- [37] Daniel Bosk. 'Grundläggande lösenordsanalys'. 2013. URL: <http://ver.miun.se/courses/security/compndii/pwdanalysis.pdf>.

- [38] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor and Serge Egelman. ‘Of passwords and people: Measuring the effect of password-composition policies’. In: *CHI*. 2011. URL: [http://cups.cs.cmu.edu/rshay/pubs/passwords\\_and\\_people2011.pdf](http://cups.cs.cmu.edu/rshay/pubs/passwords_and_people2011.pdf).
- [39] Henk CA Van Tilborg and Sushil Jajodia. *Encyclopedia of cryptography and security*. Springer Science & Business Media, 2014.
- [40] J. Camenisch, A. Lehmann and G. Neven. ‘Electronic Identities Need Private Credentials’. In: *IEEE Security Privacy* 10.1 (Jan. 2012), pp. 80–83. ISSN: 1540-7993. DOI: 10.1109/MSP.2012.7.
- [41] M. Z. Lee, A. M. Dunn, J. Katz, B. Waters and E. Witchel. ‘Anon-Pass: Practical Anonymous Subscriptions’. In: *IEEE Security Privacy* 12.3 (May 2014), pp. 20–27. ISSN: 1540-7993. DOI: 10.1109/MSP.2013.158.
- [42] Daniel Bosk. ‘A high-level overview of cryptography’. Lecture. 2016. URL: <https://github.com/OpenSecEd/appliedcrypto/releases/tag/v1.1>.
- [43] Sean Peisert and Matt Bishop. ‘How to Design Computer Security Experiments’. In: *Fifth World Conference on Information Security Education: Proceedings of the IFIP TC11 WG 11.8, WISE 5, 19 to 21 June 2007, United States Military Academy, West Point, New York, USA*. Ed. by Lynn Fitcher and Ronald Dodge. Boston, MA: Springer US, 2007, pp. 141–148. ISBN: 978-0-387-73269-5. DOI: 10.1007/978-0-387-73269-5\_19. URL: <http://web.cs.ucdavis.edu/~peisert/research/Peisert-WISE2007-SecurityExperiments.pdf>.
- [44] Patrick Gage Kelley, Saranga Komanduri, Michelle L Mazurek, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor and Julio Lopez. ‘Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms’. In: *Security and Privacy (SP), 2012 IEEE Symposium on*. IEEE. 2012, pp. 523–537. DOI: <https://doi.org/10.1109/SP.2012.38>. URL: <http://repository.cmu.edu/cgi/viewcontent.cgi?article=1086&context=cylab>.
- [45] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L. Mazurek, Lujo Bauer, Christin Nicolas, Lorrie Faith Cranor and Serge Egelman. ‘Of passwords and people: Measuring the effect of password-composition policies’. In: *CHI*. 2011. URL: [http://cups.cs.cmu.edu/rshay/pubs/passwords\\_and\\_people2011.pdf](http://cups.cs.cmu.edu/rshay/pubs/passwords_and_people2011.pdf).
- [46] Richard Shay, Saranga Komanduri, Adam L Durity, Phillip Seyoung Huh, Michelle L Mazurek, Sean M Segreti, Blase Ur, Lujo Bauer, Nicolas Christin and Lorrie Faith Cranor. ‘Can long passwords be secure and usable?’ In: *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM. 2014, pp. 2927–2936. URL: <http://lorrie.cranor.org/pubs/longpass-chi2014.pdf>.
- [47] Elizabeth Stobert and Robert Biddle. ‘The Password Life Cycle’. In: *ACM Trans. Priv. Secur.* 21.3 (Apr. 2018), 13:1–13:32. ISSN: 2471-2566. DOI: 10.1145/3183341.

- [48] Ambarish Karole, Nitesh Saxena and Nicolas Christin. ‘A comparative usability evaluation of traditional password managers’. In: *International Conference on Information Security and Cryptology*. Springer. 2010, pp. 233–251.
- [49] Alma Whitten and J Doug Tygar. ‘Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0.’ In: *USENIX Security Symposium*. Vol. 348. 1999.
- [50] Steve Sheng, Levi Broderick, Colleen Alison Koranda and Jeremy J Hyland. ‘Why Johnny still can’t encrypt: Evaluating the usability of email encryption software’. In: *Symposium On Usable Privacy and Security*. 2006, pp. 3–4.
- [51] Scott Ruoti, Jeff Andersen, Daniel Zappala and Kent Seamons. ‘Why Johnny still, still can’t encrypt: Evaluating the usability of a modern PGP client’. In: *arXiv preprint arXiv:1510.08555* (2015).
- [52] Amir Herzberg and Hemi Leibowitz. ‘Can Johnny finally encrypt?: evaluating E2E-encryption in popular IM applications’. In: *Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust*. ACM. 2016, pp. 17–28.
- [53] Bruno Blanchet. ‘Modeling and Verifying Security Protocols with the Applied Pi Calculus and ProVerif’. In: *Foundations and Trends® in Privacy and Security* 1.1-2 (2016), pp. 1–135. ISSN: 2474-1558. DOI: 10.1561/3300000004. URL: <http://dx.doi.org/10.1561/3300000004>.
- [54] Bruce Schneier and John Kelsey. ‘Secure audit logs to support computer forensics’. In: *ACM Transactions on Information and System Security (TISSEC)* 2.2 (1999), pp. 159–176.
- [55] Cynthia Dwork. ‘Differential privacy’. In: *Automata, languages and programming*. Springer, 2006, pp. 1–12.
- [56] Cynthia Dwork. ‘Differential privacy: A survey of results’. In: *Theory and applications of models of computation*. Springer, 2008, pp. 1–19.
- [57] Raghavendran Balu, Teddy Furon and Sébastien Gambs. ‘Challenging Differential Privacy: The Case of Non-interactive Mechanisms’. In: *Computer Security — ESORICS 2014 — 19th European Symposium on Research in Computer Security, Wrocław, Poland, September 7-11, 2014. Proceedings, Part II*. 2014, pp. 146–164. DOI: 10.1007/978-3-319-11212-1\_9. URL: [http://dx.doi.org/10.1007/978-3-319-11212-1\\_9](http://dx.doi.org/10.1007/978-3-319-11212-1_9).
- [58] Mohammad Alaggan, Sébastien Gambs and Anne-Marie Kermarrec. ‘Private Similarity Computation in Distributed Systems: From Cryptography to Differential Privacy’. In: *Principles of Distributed Systems - 15th International Conference, OPODIS 2011, Toulouse, France, December 13-16, 2011. Proceedings*. 2011, pp. 357–377. DOI: 10.1007/978-3-642-25873-2\_25. URL: [http://dx.doi.org/10.1007/978-3-642-25873-2\\_25](http://dx.doi.org/10.1007/978-3-642-25873-2_25).
- [59] Mohammad Alaggan, Sébastien Gambs and Anne-Marie Kermarrec. ‘BLIP: Non-interactive Differentially-Private Similarity Computation on Bloom filters’. In: *Stabilization, Safety, and Security of Distributed Systems - 14th International Symposium, SSS 2012, Toronto, Canada, October 1-4, 2012. Proceedings*. 2012, pp. 202–216. DOI: 10.1007/978-3-642-33536-5\_20. URL: [http://dx.doi.org/10.1007/978-3-642-33536-5\\_20](http://dx.doi.org/10.1007/978-3-642-33536-5_20).

- [60] G. McGraw. ‘Four Software Security Findings’. In: *Computer* 49.1 (Jan. 2016), pp. 84–87. ISSN: 0018-9162. DOI: 10.1109/MC.2016.30.
- [61] Daniel Genkin, Itamar Pipman and Eran Tromer. ‘Get your hands off my laptop: physical side-channel key-extraction attacks on PCs’. In: *Journal of Cryptographic Engineering* 5.2 (June 2015), pp. 95–112. ISSN: 2190-8516. DOI: 10.1007/s13389-015-0100-7.
- [62] 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](http://dx.doi.org/10.1007/978-3-662-44371-2_25).
- [63] Daniel Genkin, Lev Pachmanov, Itamar Pipman and Eran Tromer. ‘Stealing Keys from PCs Using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation’. In: *Cryptographic Hardware and Embedded Systems – CHES 2015*. Ed. by Tim Güneysu and Helena Handschuh. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 207–228. ISBN: 978-3-662-48324-4.
- [64] Helena Andersson, Jan-Olof Andersson, Fredrik Björck, Martin Eriksson, Rebecca Eriksson, Robert Lundberg, Michael Patrickson and Kristina Starkerud. *Gapanalys – Checklisten*. Dec. 2011. URL: <http://www.informationssakerhet.se>.
- [65] D Graffox. *IEEE Citation Reference*. Sept. 2009. URL: <http://www.ieee.org/documents/ieeecitationref.pdf>.
- [66] Joshua M. Paiz, Elizabeth Angeli, Jodi Wagner, Elena Lawrick, Kristen Moore, Michael Anderson, Lars Soderlund, Allen Brizee and Russell Keck. *In-Text Citations: The Basics*. Nov. 2013. URL: <https://owl.english.purdue.edu/owl/owlprint/560/>.