The Complete Study Guide for IG036G Information Security

Daniel Bosk

Department of Information Systems and Technology
Mid Sweden University, Sundsvall

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

14th May 2018

1 Scope and aims

The course treats information security from a user, organization and technical perspective. The first part of the course concerns security on a strategic level, i.e., managing security within an organization. The second part of the course focuses on the operative parts, i.e., security mechanisms and principles for design of secure systems. In full, the course aims at giving you an understanding of threats to security and how to work to protect against these.

More concretely, the intended learning outcomes (ILOs) of the course are the following. After completing the course, you should be able to:

- *apply* basic concepts and models in information security.
- *evaluate* the usability of security solutions and *suggest* improvements that improve usability and security.
- *analyse* threats, possible protection mechanisms and *design* an approach to protection which considers usability.
- *apply* the Swedish Civil Contingency Agency's Framework for Information Security Management Systems to *analyse, assess and improve* the information security in an organization.
- *review and apply* the results of published research in the security field.

The course has a variety of learning sessions designed to ensure that you learn these ILOs. Each such session has a set of further specified ILOs: e.g., the first outcome above refers to 'basic concepts and models', the ILOs of a learning session would specify which concepts and models it covers.

2 Course structure and content overview

The first 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. The main material used for this part [1–19] is produced by the Swedish Civil Contingencies Agency (MSB) and is based on the ISO 27000 standard documents.

The second part of the course will focus on the content of Anderson's book *Security Engineering* [20] and Gollmann's book *Computer Security* [21]. The focus in the second part of the course is on security mechanisms and how to use these in secure systems. There is also some additional material for this part of the course, e.g., research papers and some other material.

2.1 Teaching and tutoring

The course is taught using lectures, seminars, laboratory assignments and, finally, a project. All assignments are numbered consecutively prefixed with an 'L' for laboratory assignments, 'S' for seminar assignments, 'M' for memos and 'P' for projects.

2.2 Schedule

You will find an outline for a schedule for the course in Table 1. You are free to follow this schedule or any schedule you make for yourself, but the learning and tutoring sessions, deadlines etc. will follow this schedule. The detailed reading instructions for each item in the schedule can be found in the following sections.

3 Course content

This section summarizes the material covered by the lectures and assignments, i.e., what you should read for each of them. It is divided by topics and ordered according to progression of the course.

3.1 Foundations of security

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

We will focus on Gollmann's chapter on 'Foundations of Computer Security' [21, 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. After reading this chapter you you are encouraged to do exercises 3.2, 3.5, 3.6, 3.7 and 3.8 in [21]. Anderson also covers this in Chapter 1 of [20]. He also treats a wider area than just *computer* security, which is good for us, he covers many aspects of security in different examples.

Finally, you should read 'How to Design Computer Security Experiments' [22]. This paper discusses the scientific method 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' [23].

Week	Work
1	Lecture: Course start/Foundations of security Lecture: Security usability
2	Lecture: MSB's Framework, part I Start working on M1 (isms) Lecture: MSB's Framework, part II Start working on M2, prepare S3 (risk) Lecture: Records management
3	Lecture: Information theory Lecture: Cryptography, part I Lecture: Cryptography, part II First grading of M1 (isms), M2 (risk)
4	Lecture: Identification and authentication, part I Lecture: Identification and authentication, part II Lecture: Protocols and formal verification First seminar session S3 (risk)
5	Lecture: Access control Lecture: Accountability Lab: L4 (pwdguess), L6 (pricomlab) Seminar: S5 (pwdpolicies)
6	Lecture: Trusted computing Lecture: Software security Lecture: Course conclusion Lab: L4 (pwdguess), L6 (pricomlab)
7	Tutoring: P7 (research) Lab: L4 (pwdguess), L6 (pricomlab)
8	Tutoring: P7 (research) Lab: L4 (pwdguess), L6 (pricomlab)
9	Tutoring: P7 (research)
10	Presentation: P7 (research) Second grading of M1 (isms), M2 (risk) Seminar: second call for seminars (S3, S5) Lab: final call for labs
+3 months	Presentation: second call for presentations (P7) Final grading of M1 (isms), M2 (risk) Seminar: final call for seminars (S3, S5)
+6 months	Presentation: final call for presentations (P7)

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 Security usability

One important aspect of security, which traditionally is forgotten, 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. How the users function and how to adapt systems to their limitations is at the centre of the usability area.

Anderson gives a short summary of the psychology of users, their strengths and weaknesses, in Chapter 2 "Usability and Psychology" in [20]. Also treated here is the ever-recurring problem of password policies. The material covering this area is the article 'Of passwords and people: Measuring the effect of password-composition policies' [24] and its follow-up article 'Can long passwords be secure and usable?' [25].

3.3 MSB's framework, part I

This lecture covers the first part of MSB's framework [1–5], 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.

3.4 M1 Information security management system

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

- *Introduktion till metodstödet* [1],
- *Säkra ledningens engagemang* [2], and
- *Projektplanering* [3].

3.5 MSB's framework, part II

This lecture covers the remaining part of MSB's material [6, 8–19]. 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.

3.6 M2 and S3 Assessment and risk analysis

Before doing this assignment you should have read the following:

- *Verksamhetsanalys* [4] and
- *Riskanalys* [5]

3.7 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 forexample 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 development 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 processorienterad informationskartläggning* [26] and the standard ISO 30300:2011 [27].

3.8 Information theory

The area of Information Theory was founded in 1948 by Claude Shannon. It concerns information, e.g. 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.

The concept of entropy, the main part of information theory, is treated in a few short texts: *A Primer on Information Theory and Privacy* [28] and applied in 'How Unique Is Your Browser?' [29], but also in 'Chapter 6: Shannon entropy' [30]. This is then utilised in the text 'Grundläggande lösenordsanalys' [31] (in Swedish), and 'Of passwords and people: Measuring the effect of password-composition policies' [24] which treats passwords.

3.9 Cryptography

To fully understand how many security mechanisms can be implemented we need cryptography, as cryptography has a central role in many parts of security. This learning session is intended to give a high-level overview of cryptography: symmetric cryptography, public-key encryption, digital signatures, zero-knowledge proofs, and multi-party computation.

The basics are covered by Chapter 5 in Anderson's *Security Engineering* [20] and Chapter 14 in Gollmann's *Computer Security* [21]. (To practice your understanding of these mechanisms it is recommended to do exercises 14.2, 14.3 and 14.7 in [21].) For the remaining topics, however, we refer to the *Encyclopedia of cryptography and security* [32] (and cited papers and books).

3.10 Identification and authentication

Authentication has always been a central part of security. An entity claims something, a property or an identity, authentication is about verifying or rejecting any such claim. We will cover a few different ways to do authentication: the traditional something you know, something you have and something you are; but also look beyond.

Why we want to do this, and how we can accomplish this is treated in Chapter 4 in [21]. Anderson also treats this topic (Chapter 2 in [20]), 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 [21]. For the treatment of anonymous credentials, we refer to 'Electronic Identities Need Private Credentials' [33] and 'Anon-Pass: Practical Anonymous Subscriptions' [34].

3.11 L4 Password cracking and social engineering

Before doing this laboratory assignment you should read Chap. 2 "Usability and Psychology" and Chap. 5 "Cryptography" in *Security Engineering* [20]. Further, you need a basic understanding of information theory [35] for this assignment, for this you are recommended to read 'Chapter 6: Shannon entropy' [30].

Now that you have the basic theory, you should start reading the main material of this assignment. Start by reading the papers *Human Selection of Mnemonic Phrase-based Passwords* [36] and 'Of passwords and people: Measuring the effect of password-composition policies' [24]. You should then read the follow-up paper to the latter: 'Can long passwords be secure and usable?' [25]. Finally, you should read 'Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms' [37].

After that you should read about some recent incidents where password databases have leaked. There is a list of breaches maintained by the 'Have I been pwned' service[1], you can search for news articles to read the details. (And we encourage you to use this service.)

For a more in-depth treatment on password guessing, you are recommended to read 'Guessing human-chosen secrets' by Bonneau [38]. However, this is not a mandatory part of the assignment.

The final part of the theory concerns social engineering. You should read about an incident striking the security company RSA, covered in 'RSA: SecurID Attack Was Phishing Via an Excel Spreadsheet' [39].

3.12 S5 Password policies

The part of security that perhaps most affect the users is user authentication. The predominant mechanism to achieve this is passwords. Thus, design decisions in this are are important for both the usability and the security of the system.

During this seminar you will train your ability to comprehend and apply research results in the area of security and usable security. You will combine results from different areas to analyse different aspects and to evaluate the security and usability of different designs.

We need Chap. 2 'Usability and Psychology' of [20]. Further, we need a basic understanding of information theory [35], for this you are recommended to read 'Chapter 6: Shannon entropy' [30]. Finally, we will discuss the results of 'Of passwords and people: Measuring the effect of password-composition policies' [24], 'Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms' [37] and 'Can long passwords be secure and usable?' [25].

[1] URL: `https://haveibeenpwned.com/`.

3.13 Protocols and formal verification

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.

Anderson gives an overview of this area in *Security Engineering* [20], Chapter 3 'Protocols'. Gollmann has a more technically detailed treatment in Chapter 15 of *Computer Security* [21].

3.14 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. We will give an overview of the possibilities.

This is treated by Chapter 5, followed by Chapters 11 and 12, in *Computer Security* [21]. You are also recommended to read Anderson's treatment of the subject, he treats this in Chapters 4, 8, and 9 in *Security Engineering* [20]. Finally, to establish your newly gained knowledge in this area, you should do exercises 5.1, 5.2, 5.5, 5.6, 5.8 and 5.9 in [21].

3.15 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, banks. We will explore some principles in keeping accounts and discuss ways to implement it in different, sometimes challenging, environments.

Anderson describes accountability through his experience from banks in Chapter 10 'Banking and Bookkeeping' in *Security Engineering* [20]. We will also use the secure logging system of Schneier and Kelsey [40] 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.

3.16 L6 Private communication

Before starting this assignment you should have read chapters 5 and 23.4.4–5 in *Security Engineering* [20]. You should also read the paper 'Exploring steganography: Seeing the unseen' [41] to fully understand how steganography works in practice. (Other recommended papers are 'On the limits of steganography' [42] and 'Hide and seek: An introduction to steganography' [43].)

During this assignment you should consult the documentation [44–47] for instructions on how to use the specific softwares.

3.17 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. Here we will explore how to ensure the integrity of the computer system before use. As an example, Alice has a laptop while travelling, how can she be sure no foreign intelligence agency inserted a modified version of the operating system during the customs inspection? Or, what about when she left the laptop in the hotel room while having breakfast, perhaps the hotel aide replaced the bootloader to break Alice's full-disk encryption? Another aspect of this is to protect parts of the system from Alice herself, this is what Digital Rights Management is all about. A content owner who only allows using his or her material in a certain way must have some means of ensuring this is enforced. These needs boils down to trusted computing.

We treat the material in Chapters 16, 18 and 22 in *Security Engineering* [20].

3.18 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. possibility of buffer overruns or code injections.

Gollmann treats this area in Chapter 10 of his book, *Computer Security* [21]. The recommended exercises to do after reading this material are 10.1, 10.3 and 10.4 in [21].

Anderson also treats this subject—in Chapter 4.4 and Chapter 18 of *Security Engineering* [20]—albeit with less technical details.

3.19 Course conclusion

During this lecture we will shortly review the course and try to fit things into a bigger picture.

3.20 P7 A short study in information security

The project is a smaller study within the area of information security. The idea is to deepen your knowledge in some areas of information security, so during the project you must select and read papers which are related to the course. For example, you can focus on areas such as:

- usable security,
- privacy enhancing technologies (PETs), or
- more advanced methods for guessing passwords.

These are just examples, you are free to choose the area and papers in corroboration with the tutor. More details are provided in the separate instruction.

LADOK	Credits (ECTS)	Grade	Course Assignments
I104	1.5	P, F	M1, M2, S3, S5
L104	1.5	P, F	L4, L6
R104	4.5	A–F	P7
Total	7.5	A–F	P7

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.

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 is graded from A to F, where A–E are for passing and F and Fx are for failing. 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 [48] (see also [49] 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] 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`.

[2] 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`.

[3] 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`.

[4] 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`.

[5] Helena Andersson, Jan-Olof Andersson, Fredrik Björck, Martin Eriksson, Rebecca Eriksson, Robert Lundberg, Michael Patrickson and Kristina Starkerud. *Riskanalys*. Dec. 2011. URL: `http://www.informationssakerhet.se`.

[6] 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`.

[7] Helena Andersson, Jan-Olof Andersson, Fredrik Björck, Martin Eriksson, Rebecca Eriksson, Robert Lundberg, Michael Patrickson and Kristina Starkerud. *Gapanalys – Checklistan*. Dec. 2011. URL: `http://www.informationssakerhet.se`.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] Dieter Gollmann. *Computer Security*. 3rd ed. Chichester, West Sussex, U.K.: Wiley, 2011. ISBN: 9780470741153 (pbk.)

[22] Sean Peisert and Matt Bishop. 'How to Design Computer Security Experiments'. In: *Fifth World Conference on Information Security Education*. Ed. by Lynn Futcher and Ronald Dodge. Boston, MA: Springer US, 2007, pp. 141–148. ISBN: 978-0-387-73269-5.

[23] 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.

[24] 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.

[25] 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.

[26] Myndigheten för samhällsskydd och beredskap (MSB) och Riksarkivet. *Vägledning för processorienterad informationskartläggning*. Tech. rep. Nov. 2012. URL: https://riksarkivet.se/Media/pdf-filer/V%C3%A4gledning%20f%C3%B6r%20processorienterad%20informationskartl%C3%A4ggning.pdf.

[27] *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.

[28] Peter Eckersley. *A Primer on Information Theory and Privacy*. Jan. 2010. URL: https://www.eff.org/deeplinks/2010/01/primer-information-theory-and-privacy.

[29] Peter Eckersley. 'How Unique Is Your Browser?' In: *Privacy Enhancing Technologies*. Springer. 2010, pp. 1–18. URL: https://panopticlick.eff.org/browser-uniqueness.pdf.

[30] Daniel Ueltschi. 'Chapter 6: Shannon entropy'. URL: http://www.ueltschi.org/teaching/chapShannon.pdf.

[31] Daniel Bosk. 'Grundläggande lösenordsanalys'. 2013. URL: http://ver.miun.se/courses/security/compendii/pwdanalysis.pdf.

[32] Henk CA Van Tilborg and Sushil Jajodia. *Encyclopedia of cryptography and security*. Springer Science & Business Media, 2014.

[33] 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.

[34] 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.

[35] C. E. Shannon. 'A Mathematical Theory of Communication'. In: *The Bell System Technical Journal* 27 (July 1948), pp. 379–423, 623–656.

[36] Cynthia Kuo, Sasha Romanosky and Lorrie Faith Cranor. *Human Selection of Mnemonic Phrase-based Passwords*. Tech. rep. 36. Institute of Software Research, 2006. URL: http://repository.cmu.edu/isr/36/.

[37] 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. URL: http://ieeexplore.ieee.org/abstract/document/6234434/.

[38] Joseph Bonneau. 'Guessing human-chosen secrets'. PhD thesis. University of Cambridge, May 2012. URL: http://www.cl.cam.ac.uk/~jcb82/doc/2012-jbonneau-phd_thesis.pdf.

[39] Dennis Fisher. 'RSA: SecurID Attack Was Phishing Via an Excel Spreadsheet'. Apr. 2011. URL: https://threatpost.com/en_us/blogs/rsa-securid-attack-was-phishing-excel-spreadsheet-040111.

[40] 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.

[41] Neil F Johnson and Sushil Jajodia. 'Exploring steganography: Seeing the unseen'. In: *Computer* 31.2 (1998), pp. 26–34. URL: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4655281.

[42] Ross J Anderson and Fabien AP Petitcolas. 'On the limits of steganography'. In: *Selected Areas in Communications, IEEE Journal on* 16.4 (1998), pp. 474–481. URL: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=668971.

[43] Niels Provos and Peter Honeyman. 'Hide and seek: An introduction to steganography'. In: *Security & Privacy, IEEE* 1.3 (2003), pp. 32–44. URL: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1203220.

[44] Werner Koch. *Using the GNU Privacy Guard*. Mar. 2012. URL: http://www.gnupg.org/documentation/manuals/gnupg.pdf.

[45] The Gpg4win Initiative. *The Gpg4win Compendium*. Aug. 2010. URL: http://wald.intevation.org/frs/download.php/775/gpg4win-compendium-en-3.0.0-beta1.pdf.

[46] Niels Provos. *outguess - universal steganographic tool*. URL: http://manpages.ubuntu.com/manpages/utopic/man1/outguess.1.html.

[47] Eng. Cosimo Oliboni. *OpenPuff v4.00 Steganography & and Watermarking*. July 2012. URL: http://embeddedsw.net/doc/OpenPuff_Help_EN.pdf.

[48] D Graffox. *IEEE Citation Reference*. Sept. 2009. URL: http://www.ieee.org/documents/ieeecitationref.pdf.

[49] 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/.