The Complete Study Guide for DV026G Information Security

Daniel Bosk[1,2]

[1] Department of Information and Communication Systems
Mid Sweden University, Sundsvall
[2] School of Computer Science and Communication
KTH Royal Institute of Technology, Stockholm

1 Scope and Aims

The course treats information security from a user, organization and technological perspective. The first part of the course concerns security on a strategic level, i.e. working with security in general 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 for threats to security and how to work to protect against these.

A more concrete summary of the course achievements are the following, after completing the course you should be able to:

- Explain basic concepts and models in information security.
- Analyse threats and possible protection mechanisms.
- Apply the Swedish Civil Contingency Agency's Framework for Information Security Management Systems to analyse, assess and improve the information security in an organization.

2 Overview of Structure and Content

The first part of the course, the one covering information security on a strategic level, 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]. Gollmann's book *Computer Security* [21] is also useful, it has more technical details than [20]. Although references to [21] is provided in the reading instructions, those are not necessary for this course.

The focus of the second part is on actual attacks, security mechanisms, and how to use these in secure protocols. There are also some additional material for this part of the course, e.g. research papers [22, 23] and some other material [24, 25]. In addition to these there will also be some news articles [26–32] which has documented some of the major security incidents during the past few years. MSB also has the website CERT-SE [33] which has some interesting references and security news, e.g. virus epidemics in Sweden.

2.1 Teaching

The course is taught using lectures, individual laboratory assignments, seminars, a project, and finally an exam. You can find a more detailed timetable, containing lab sessions etc., in the following section. All assignments are numbered consecutively prefixed with an 'L' for laboratory assignments, 'S' for a seminar assignment, and 'M' for memos. For details on the examination of these and more information about deadlines, see section 4.

2.2 Course Schedule

To make your reading of the course easier you are presented with a suggested schedule in this section. You are free to follow this schedule or any schedule you make for yourself, but the deadlines, laboratory sessions, and lectures will follow this schedule. You will find a short summary of schedule in table 1. 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.

3.2 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.

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 on half-time study rate.

Course Week	Work
1	Course Start/Foundations of Security Lecture on MSB's Framework, Part I Start working on M1 (isms) Lecture on MSB's Framework, Part II Start working on M2, prepare S3 (risk) Lecture on Records Management
2	Lecture on Information Theory Lecture on Cryptographic Mechanisms, Part I Lecture on Cryptographic Mechanisms, Part II First grading of M1 (isms), M2 (risk)
3	Lecture on Identification and Authentication Lecture on Security Usability Seminar session S3 (risk)
4	Lecture on Access Control Lecture on Secure Protocols Lecture on Accountability and Non-Repudiation Seminar session S5 (pwdpolicies) Lab session L4 (passwd), L6 (privcomm)
5	Lecture on Software Security Lecture on DRM and Trusted Computing Lecture on Side-Channels Lab session L4 (passwd), L6 (privcomm)
6	Tutoring session for project, L4 (passwd), L6 (privcomm) First grading of L4 (passwd), L6 (privcomm)
7	Tutoring session for project, L4 (passwd), L6 (privcomm)
8	Tutoring session for project, L4 (passwd), L6 (privcomm)
9	Tutoring session for project, L4 (passwd), L6 (privcomm)
10	First exam First grading of project Second grading of M1 (isms), M2 (risk) Second seminar session for S3 (risk), S5 (pwdpolicies) Second grading of L4 (passwd), L6 (privcomm)
+3 months	Second exam Second grading of project Final grading of M1 (isms), M2 (risk) Final seminar session for S3 (risk), S5 (pwdpolicies) Final grading of L4 (passwd), L6 (privcomm)
+6 months	Final exam Final grading of project

3.3 M1 Information Security Management System

Before starting this PM, you should have read the following documents:

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

Alternatively

- [34, Chapter 3]

3.4 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.

3.5 M2 and S3 Assessment and Risk Analysis

Du ska inför denna promemoria ha läst dokumenten

- *Verksamhetsanalys* [4], och
- *Riskanalys* [5]

i MSB:s metodstöd.

3.6 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* [35] and the standard ISO 30300:2011 [36].

3.7 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* [37] and applied in 'How Unique Is Your Browser?' [38], but also in 'Chapter 6: Shannon entropy' [39]. This is then utilised in the text 'Grundläggande lösenordsanalys' [24] (in Swedish), and 'Of passwords and people: Measuring the effect of password-composition policies' [23] which treats passwords.

3.8 Cryptographic Mechanisms

To fully understand how many security mechanisms can be implemented we need cryptography, as cryptography has a central role in a lot 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.

We will treat 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].

3.9 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].

3.10 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' [23] and its follow-up article 'Can long passwords be secure and usable?' [40].

3.11 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].

3.12 Secure Protocols

As soon as two principals need to interact, there is need for a protocol which secures the communication, 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. We will explore how to design secure protocols and introduce some tools for verification.

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].

3.13 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 [41] for this assignment, for this you are recommended to read 'Chapter 6: Shannon entropy' [39].

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* [42] and 'Of passwords and people: Measuring the effect of password-composition policies' [23]. You should then read the follow-up paper to the latter: 'Can long passwords be secure and usable?' [40]. After that you should read about some recent incidents where password databases have leaked, e.g. [29–32].

For a more in-depth treatment on password guessing, you are recommended to read 'Guessing human-chosen secrets' by Bonneau [43]. However, this is not a mandatory part of the assignment.

The final part of the theory concerns advanced persistent threats (APTs). You should read about these. First you should read about an incident striking the security company RSA, covered in 'RSA: SecurID Attack Was Phishing Via an Excel Spreadsheet' [28]. Then you will read a paper on different approaches to APT, 'Sherlock Holmes and The Case of the Advanced Persistent Threat' by Juels and Yen [22].

3.14 S5 Password Policies

First you must read Chap. 2 'Usability and Psychology' in [20]. Further, you need a basic understanding of information theory [41] for this assignment, for this you are recommended to read 'Chapter 6: Shannon entropy' [39].

Then, to participate in this seminar you must have read the papers 'Of passwords and people: Measuring the effect of password-composition policies' [23], 'Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms' [44] and 'Can long passwords be secure and usable?' [40]. In these papers the authors have studied how different password-composition policies affects users' choice of passwords.

3.15 Accountability and Non-Repudiation

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 [45] 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 Privacy of 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' [46] to fully understand how steganography works in practice. (Other recommended papers are 'On the limits of steganography' [47] and 'Hide and seek: An introduction to steganography' [48].)

During this assignment you should consult the documentation [49–52] for instructions on how to use the specific softwares.

3.17 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.

3.18 DRM and 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].

3.19 Side-Channels

When looking at secure systems it is easy to assume they are safe just because the secret keys are not directly reachable. This is not always true. Even if the key storage is unreachable, there is some information that can be extracted anyway. For instance the fact *that* two principals are communicating, *when* they are communicating, the time each operation takes to perform, etc., is not provided any confidentiality. The information possible to extract from this is what is called side-channel information.

An overview of this area is provided in Chapters 17 and 23 of [20]. An interesting paper on this topic is *RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis* [53] where the authors extract RSA 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 RSA key used.

There is another aspect of this too, namely covert channels. Covert channels are channels over which communication can take place, even with limited bandwidth, despite the prohibition of this due to the security policy.

3.20 P7 A Short Gap Analysis

The project consists of doing a short gap analysis. As such you must have read MSB's material [1–6, 8–19].

4 Examination

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

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.

LADOK	Credits (ECTS)	Grade	Course Assignments
X104	0.0	P, F	M1
I104	1.5	P, F	M2, S3, S5
L104	1.5	P, F	L4, L6
P104	3.0	A, C, E, F	P7
T104	1.5	A, C, E, F	Exam
Total	7.5	A–F	Average of P7 and exam

The project report is graded from A, C, or E for for passing or F or Fx for failing. The exam is also graded A, C, or E for passing or F or Fx for failing. The final grade for the course is the average of the exam and the project. For example, if you have an A on the exam but a C on the project, then you will get a B as 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 [54] (see also [55] 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 plagiarised 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] Ari Juels and Ting-Fang Yen. 'Sherlock Holmes and The Case of the Advanced Persistent Threat'. In: *LEET*. 2012. URL: https://www.usenix.org/system/files/conference/leet12/leet12-final29.pdf.

[23] 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.

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

[25] Daniel Bosk. 'Introduktion till några klassiska chiffer'. 2013. URL: http://ver.miun.se/courses/security/compendii/krypto.pdf.

[26] Mat Honan. *How Apple and Amazon Security Flaws Led to My Epic Hacking*. Aug. 2012. URL: http://www.wired.com/threatlevel/2012/08/mat-hacked/.

[27] Kim Zetter. *How Not to Become Mat Honan: A Short Primer on Online Security*. Aug. 2012. URL: http://www.wired.com/threatlevel/2012/08/how-not-to-become-mat-honan/.

[28] 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.

[29] Troy Hunt. *A brief Sony password analysis*. June 2011. URL: http://www.troyhunt.com/2011/06/brief-sony-password-analysis.html.

[30] Graham Cluley. *The worst passwords you could ever choose exposed by Yahoo Voices hack*. July 2012. URL: http://nakedsecurity.sophos.com/2012/07/13/yahoo-voices-poor-passwords/.

[31] Jon Oberheide. *Brief analysis of the Gawker password dump*. Dec. 2010. URL: https://duo.com/blog/brief-analysis-of-the-gawker-password-dump/.

[32] Nik Cubrilovic. *RockYou Hack: From Bad to Worse*. Dec. 2009. URL: http://techcrunch.com/2009/12/14/rockyou-hack-security-myspace-facebook-passwords/.

[33] Myndigheten för samhällsskydd och beredskap. *CERT-SE*. URL: https://www.cert.se.

[34] *Information technology – Security techniques – Information security management systems – Overview and vocabulary (ISO/IEC 27000:2016)*. Standard. Available through University Library. Stockholm, Sweden: Swedish Standards Institute, Mar. 2017.

[35] 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.

[36] *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.

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

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

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

[40] 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.

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

[42] 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/.

[43] 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.

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

[45] 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.

[46] 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.

[47] 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.

[48] 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.

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

[50] 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.

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

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

[53] Daniel Genkin, Adi Shamir and Eran Tromer. *RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis*. Tech. rep. Cryptology ePrint Archive, Report 2013/857, 2013., 2013. URL: http://eprint.iacr.org/2013/857.

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

[55] 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/.