Tampere University / ITC Faculty / Computer Science / Comp.Sec.100-02 / Jukka Koskinen

Cyber security I Course handbook

This document, version 1, 23.8.2020 explains …
most everything you need to know for successful study after obtaining a study right, access to the study management systems and enrolling to the course. If something is missing here, contact the teacher firstname.lastname@tuni.fi and he will update this document.

OBJECTIVES

The concise definition of objectives in the official syllabus is reproduced here in italics. More detailed explanations follow each line.

The aim is to learn basic skills about cyber security, needed by everyone who is studying information technology.
This objective must be understood in a wide sense. The studies themselves impose a need of some cyber security skills, but the main motivation comes from the professions where the students of information technology will end up. In addition, this covers skills needed in society and not only as citizens but also as technology-aware counselors of fellow-citizens who are not likely to be able to take sufficient care of their own security. Lastly, the student will also be prepared for further studies in the infosec curriculum.

The student
- *identifies security and privacy threats and responsibilities;*

This is an obvious but not simple starting point of anything you do in the field of information security, and privacy can be considered just a branch of it. You must understand what bad can happen even if everything seems to be fine. In addition, in your work and to some extent in your private life it is not only good but obligatory to act properly in the face of security threats.

- has a wide knowledge of the concepts, principles and mechanisms of information security;
This course covers a very large spectrum of them. After passing this course there is not going to be many completely new things you encounter even if you continue your studies in information security. Even if there will always appear new kinds of vulnerabilities and attacks, you already know this (i.e. what the previous clause just said) and most likely you will be able to categorize them in the spectrum. It is of course clear that you cannot obtain very deep knowledge over very wide range of things during a short course. This is why there is the third objective.

- *knows what kind of additional knowledge and skills is needed to perform various information security tasks in different application areas.*
This is a very important goal of a basic course, but it is difficult to measure. Your way of learning this will mainly be getting familiar with small parts of large documents, web sites that you found and judged yourself, and the constant flow of news during the process of doing an exercise on them. Thereby you are likely to start appreciating these sources of knowledge and understanding the depth of skills that is required in information security professions.

CONTENTS

THE OFFICIAL SYLLABUS TEXT

Core content

- Information, computing, networking and cyber systems as platforms of threats.
- Cyber security as a special form of security and a variation of information security.
- Application areas of information security.
- General mechanisms and principles of information security.
- Key sources of security knowledge: standards, guidelines and legislation.
- Different levels and areas of security expertise.

Complementary knowledge

- The way of thinking: "What is an asset to be protected and what can go wrong?"
- Keeping cyber security in mind from the design phase of systems.
- Cost-benefit thinking, evaluation and measurement of information security.
- How standards and guidelines are applied and interpreted in practical security work.
- Security work and knowledge of its target areas. In addition, introduction to cyber security studies at TAU.

Specialist knowledge

- The way of thinking: "What goals does the attacker see in the target that is being defended and what are the easiest routes for the attacker to reach them?"

THE CONTENTS WILL ARISE FROM AN ONTOLOGY

The course contents follow an ontology of information security developed for this purpose. There are 3 major categories subdivided into 11 classes. This division is used to distribute the questions for Exams 1 and 2 (see below). The indented paragraphs below describe the classes more widely than the exam questions ask. For instance, there is nothing about p2p, voting systems or diffuse radiation in the Exams 1 and 2, but you can invent an essay topic for yourself out of such fields. The next section shows how the actual contents in the Exams 1 and 2 were made.

(1-3) What can happen if there is a lack of security, what can then be done, and how can everything be understood?

1. Information security defined by looking at information and threats to it.
What needs to be protected and why, what can go wrong, what or who is threatening, how to survey the threats, what is a threat model? (Detailed threats appear in later classes – especially such that are against protections.)

> Nature and vistas of information (incl. everything from human memory and hardware tokens to cloud services and internet as a whole). General definitions of information security (content of the concept: data processing peace, "CIA", etc.), threatening natural forces, technical problems, human error, administrative failures, intentional threats (from hacker ethics to malware economy to cyber warfare).

2. General features of security activities.
Most of the topics in this class can be understood without getting familiar with details in other classes, but a new level of understanding will follow that.

> General principles (also “design principles”), perspectives, ontologies, architectural models, organizations, standards, information sources, measurement, testing, assurance, theories, research, security industry, professions, education.

3. Addressing emerging threats
What can be done if a threat is realized? The better prepared you are, the more you can do. However, only in the later classes will the emphasis be proactive in the sense of trying to control what can happen. This class is positioned here to provide a “final frontier” in facing the threats, but many advance preparations are covered here.

> Response preparation (planning, procurement etc.), logging, duplication (including backup), detection (including antivirus and IDS), response, recovery, continuity, tracking (forensics) and follow-up.

(4-6) How are people situated in the field of security?

4. Security features of society
Societies, nations, economies and other large networks of people have structures, trends and missions that make some threats more possible than others.

> Cyber security (also from a corporate perspective), strategies, regulations (including cybercrime, copyrights, data protection), information society, cybercrime ecosystems.

5. Community and individual security aspects
People in their daily life and as members of local or network communities constantly face situations where information security comes to play.

> Infosec culture, protection from harmful information and scams, privacy in practice, usability, awareness, ethics and other human factors, plus identity and trust management.

6. How are security measures selected and managed within an organization?
This class covers administrative information security at the level where employees, plans, euros, etc. are discussed, but not usually bits, volts, or TCP ports (which are the topics in classes 11, 9 and 10 respectively).

> Strategies, policies, infosec management system, risk management, personnel, auditing.

(7-11) How do technologies help in the field of security?

7. What is the secure way to access and operate information and systems?

This class differs most from the traditional ones by putting together operational security, data security and other practices in information systems. This is the result of considering the title question in the case of normal use of information systems, where users and administrators must apply security-enhancing procedures. Some of them are quite independent security mechanisms, such as passwords or encryption, and they cover some topics that would otherwise fall into later classes, mainly cryptology.

Access control, use of passwords, rules for different stages in the life cycle of information (including when to encrypt / sign e-mail), special systems such as healthcare, governmental systems.

8. Cryptologic methods

This class covers almost all cryptologic theory, but not any more practices like key management (in class 6) or usage of crypto (in class 7).

Algorithms, implementations, breaking, protocols (including various forms of authentication), special systems like voting.

9. Physical and hardware security aspects

This class encompasses everything that is "tangible" except for people, though they are included in the biological sense.

Access control, facilities, power supply, anti-tampering, biometrics, security devices, trusted architectures, critical systems and industrial automation, diffuse radiation.

10. Securing the data network and mobile data

The data network is the basis of all kinds of data processing nowadays. This class applies in practice the theoretical knowledge from the classes above, especially from cryptology.

Secure structure (including hardware) and management of a network that is wired / wireless and of type enterprise / backbone / ad hoc; filtering; security protocols in theory and practice (e.g., IPsec and TLS); special systems like p2p, digital TV, WLAN, Bluetooth, 4G, RFID. Vulnerability testing.

11. Securing "stationary" data processing

Although the movement of data has already been covered in class 10, most phenomena in this class still move data in networks. Here, motion is less essential in implementing security than in class 10.

Databases, software, operating system, programming, embedded systems.

CONTENTS FOR EXAMS 1 AND 2

This is a 2-level listing of the distribution of exam questions. The first level is the same as in the previous section, now with shortened headings. The second level has 32 equally short headings and it is from these topics that the 30 Exam 1 questions will be drawn (so two topics will be omitted). The number at the end of each row tells how many subtopics the topic has for Exam 2. The random drawing of 50 questions takes at most one from each of the 82 subtopics.

1	Information and threats	
	General	2
	Personal aspects of threats	2
	Crypto-related threats	1
	Program-related threats	2
	Threats in network	2
2	Abstract security	
	Core concepts	2
	Core principles	1
	Auxiliary	1
3	Lost security	
	If things went wrong	2
4	Society	
	Data protection	2
	Identification	2
	Money protection	3
5	Individuals & groups	
	Networked life	2

	Soft issues	2
	Personal specialities	2
6	Organizations	
	Management	5
	Techniques	5
7	Secure practices	
	Access	2
	On computers	2
	Simplifying computing	2
8	Crypto	
	Crypto concepts	2
	Key matters	2
	Symmetric algorithms	1
	Public key algorithms	2
	One-way crypto	1
	General ideas on crypto protocols	1
9	Tangible security	
	Physicalities	7
10	Transporting data	
	Local network	2
	WAN, Internet	3
	Remoteness	3
11	Processing and storing	
	Software	8
	Stored data	6

The subtopic names will probably make more sense when you see the third, or detail level headings. It is not useful to reproduce it here because you will see it in Maso (see the link below).

REQUIREMENTS AND SCHEDULE

Outline from the syllabus:

The exam consists of three strictly consecutive parts, and the first one must be passed during the study period.

The first two exams are multiple-choice questions, the third one has essay questions. The exams contribute 10, 50 and 20 percent to the grade, their individual passing levels being 5/6, 1/2 and 1/2 of the score. The remaining 20% of the grade comes from on-line exercises.

Working methods: Finding information to thoroughly understand the sample exam questions on one of the two web sites of the course and using the other site to do automatically graded exercises to earn 20% of the final grade.

Criteria for grading: With the lowest passing score from the exams, the student needs 1/4 of the available exercise score to pass the course. In general, a full exercise score improves the grade with two steps. On the other hand, it is possible to achieve grade 4 without scoring anything from the exercises.

MAIN PROCEDURE IN DETAIL, ESPECIALLY THE EXAM SUCCESSION

doc ki criteria of course

To understand the descriptions below you must realize that the course does have a schedule even if it is based on self-study. Its timing consists of 49+7 days, i.e. a study period of 7 weeks and an exam week. The rules refer to day numbers ranging from 1 to 56. In year 2020 day 1 is August 24. Some things are possible only after a certain day, some only until a certain day (most stringently you must pass Exam 1 by day 56). And some things must happen in a correct sequence.

The passing grade of this course is determined by scores collected from four components: three supervised exams (80%) and a set of unsupervised exercises (20%). The exercises must be completed before the last exam, and the three exams follow a strict succession: each must be passed before the next one. In principle they can be done at the same session in an EXAM class, but this is too inefficient with respect to time reservations. These are the exams 1, 2 and 3:

1. **Basic concepts:** One hour, 30 multiple choice questions, MCQs, with four alternatives out of which one is correct. A correct choice gives 1 and no choice 0, while a wrong choice adds −1/3 to the score. There is a possibility to make corrections after (once) knowing the score.

EXAM 1:
DAY 8 - 56
PASS : >25/30
=>0-10points
to final grade

90 concept
After day 7 =>
bonus points decrease

First opportunity on day 8 of the course.
Last opportunity to pass on the last day of the exam week (i.e. day 56); otherwise unlimited number of attempts until pass, then no more attempts.
You can discard an attempt during the exam if you are not satisfied with your score.
A minimum of two days (i.e. 48 hours) between attempts.
Passing level 25/30. Brings **0–10 points** toward the final grade.
However, the maximum decreases linearly to 0 on days 15–35 of the course:

Let d = day, s = exam score, $25 < s \leq 30$. Then
if $8 \leq d \leq 15$, points = $2\cdot(s-25)$;
if $15 < d < 35$, points = $(s-25)\cdot(3{,}5-d/10)$ rounded upwards;
if $d \geq 35$, points = 0.

A list of about 90 concepts is given in advance. Each has a related MCQ.
The MCQs are shown on about 32 short text pages that mention the concepts.
The exam is drawn from the MCQs shown and a small portion from hidden variants.
One practice exam is available before each real attempt.
A fixed sample exam is constantly available.
The 90 concepts for Exam 1 and many less common words used in Exams 1 and 2 are listed in the end of this document.

2. **Basic applications:** One hour, 50 MCQs with correcting and commenting options. Corrections are like in Exam 1. Commenting, or feedback, means giving truly good excuses for two wrong answers as an attempt to get at least their negative impact neutralized. In addition, two points can be obtained by showing good understanding of the meaning of correct answers.

First opportunity on day 36.

PASSING:
25/50

Can be done in the same session with a successful Exam 1.[1]
Three attempts. Increasing intervals between attempts: 4 and 8 days.
If all attempts fail, restart from Exam 1 is possible as long as it is passed during the study period (i.e. before day 57). This unlikely case must be agreed with the teacher.
Passing level 25/50. Brings **25–50 points** toward the final grade.
One practice exam is available before each real attempt.
The exam MCQs are drawn from about 80 pages, at most one from each.
The proportion of hidden variants in Exam 2 is higher than in Exam 1.

3. **Security analysis:** One-hour essay: two topics plus recollections from certain Harpo exercises.

First opportunity on day 51 (i.e. the Tuesday of the exam week).
Can be done together in the same session with exam 2, if its score is at least 30.
Three attempts. If all fail, the only option to pass is to start over next time.
The second and third attempt must wait until the teacher has evaluated the previous attempt. Otherwise no minimum interval between attempts.
Passing level 50%. Brings **10–20 points** toward the final grade.

At your first attempt the essay topics are those that you have submitted in the Harpo Essay exercise, assuming the teacher has approved of them. The teacher also modifies them slightly, firstly to make them suit the exam situation and secondly to force you a *little* toward applying your learning and not repeating what you already wrote in the

[1] It is not at all wise and intended to put off the Exam 1 that late, to a time when it contributes 0 points.

exercise. If you need to take Exam 3 again, you will face two essay questions drawn randomly from the pool of all essay topics submitted by your fellow students. This happens already at the first attempt if you don't have two approved topics of your own. You can see all essays written by other students, and it is of course an intention that you familiarize yourself with them even if you don't need a second attempt at Exam 3.

In addition to the essays, Exam 3 includes questions from 9 Harpo exercises, but only from those where you received a near-full score (≥5/6). Some of these questions repeat a random multiple-choice question from the exercise and ask for its explanation, some are separate questions indicated at the end of the exercise page. To pass, you must give the correct answer and explanation to at least half of these questions. Yes, indeed, if you just get low scores on Harpo exercises, nothing is demanded from you about them in Exam 3. On the other hand, if you get good scores, and do it yourself, you won't spend much time in Exam 3 to pass the threshold.

Exercises on the HARPO platform, mostly automatically graded, will add **0–20 points** to the grade points. Points gathered after an Exam 3 attempt are not counted for the final grade based on that attempt. If you make a new attempt of Exam 3 you can try to improve your Harpo score before that – except on the "specials" that have their deadline before Exam 3 becomes available. The number of attempts is limited in most of the Harpo exercises, but there are about 27,5 points to pursue, out of which maximally 20 are counted.

To summarize, the final grade is based on points collected from:

1. The first successful Exam 1 – after which it cannot be taken any more. The later you do this exam the fewer points are available from it. A zero from a passed Exam 1 is possible.
2. Any successful Exam 2 – taken after the successful Exam 1.
3. Any successful Exam 3 – taken after the first successful Exam 2.
4. Harpo exercises – points valid at the moment of taking the Exam 3 that is used in determining the final grade. Zero points from Harpo is possible, 20 is the maximum.

The grade is determined based on this table:

1	40 –
2	50 –
3	60 –
4	70 –
5	80 –

Once more: You can improve a positive grade by a new attempt on either Exam 2 or Exam 3, or both in any order, but you cannot do it by gathering more Harpo points – unless you pass Exam 3 again.

No points from this course instance remain valid to the next instance, and they are not usable on other courses, not even on the corresponding Finnish course.

HARPO EXERCISES

You will do these exercises on the Harpo platform (**Ha**rjoitus**po**rtaali=exercise portal), which will also let you have the practice exams.

AUTOMATIC EXERCISES

There are 19 exercises that you do without any interaction with the teacher – unless you encounter bugs in the programs or their content. Below is a listing of these exercises under five headings. Cookie will give you just 0,5 points whereas CISSP requires a lot of searching for information and its three sets will give you 2/3 points each, totalling 2 points. All the other exercises are worth 1 point – if you pass them with at most two attempts. After that, the points will decrease to zero, either after 4, 7 or 12 attempts. You will see the exact scoring schedule in Harpo, and you may see multiples of 1/6 points in your listing and your profile. The * in the list below indicates those nine exercises from which a question will be drawn to Exam 3, if the exercise score is at least 5/6.

Elementary or prerequisites

Cookie	Remove the correct cookie. (0,5 points)
Checksum*	Calculate integrity checks.
Calculations	Do modular arithmetic.
Networking*	Review some basic data communications.
Operating systems*	Review what there is between your programs and the hardware.
Programming	Review some programming constructs.

Practical

Certificate	Investigate two certificates.
Encryption	Decrypt a file.
Signature	Verify a signature.
Elementary hacking*	Go where you shouldn't.
Secure email*	Analyze a service.

Cryptic

Cryptoslots 1*	Fill in cryptic concepts ranging from bits to standards.
Cryptoslots 2*	Fill in cryptic concepts around web surfing.
Crypto algorithms 1*	Learn some symmetric crypto.
Crypto algorithms 2*	Learn some asymmetric crypto.

Reading

ENISA: Social media to APT	Study how social media can sting.
NIST SP: Systems Security Eng.	Have a taste of engineering of security of systems.
NIST SP: Access control models	Get close to really theoretical matters.

“Professional”

CISSP	Take first steps toward a professional certificate. (2 points)

SPECIALS

There are three special exercises in Harpo: News, Survey and Essays. They are larger than the automatic exercises and they cannot be accomplished in one session. Full score in News will need a minimum of 16 days, in Survey probably three days, and in Essays about a week. Altogether you can obtain 0–8 points. In Essays the teacher assigns the points, in News and Survey Harpo does automatic scoring but the teacher may modify the points.

All the special exercises have some interaction between the participants. This is the reason why the deadline for these exercises is in the end of the study period, on day 49 of the course, i.e. just before the exam week starts. Recall that in the automatic exercises you can gather more points until you have used up your attempts, reached 20 points, or are using the points to get a final score in exam 3. So, unlike the automatic exercises, your score from the specials will be final before the first possible attempt of exam 3 is due.

NEWS, 0–3 POINTS

Submit **news tweets** on four topic areas and four different kinds of sources (“4&4”) each on a different day, at most one day old, and not repeating what someone else tweeted within six earlier submissions (among a group of about 15 students). When you have 8 fulfilling those conditions you will get 1 point, and each extra 2 will add 0,5 points until 16 gives you 3 points. If you submit more than eight before fulfilling the “4&4”, they will be counted normally as soon as you achieve the “4&4” condition. And the 4 can overlap in the two dimensions.

The idea of not allowing more than one submission per day is to let you learn constant awareness of security matters. If you need to protect an information system, ranging from your own phone with its applications and connections to a corporate network, you need to follow the constantly changing security environment. You only have a little less than 49 days for the tweets, because it is not likely that the tweeting system with student grouping can be accomplished on day 1 of the course.

SURVEY, 0–3 POINTS

Three points are available by taking part in and carrying out a **survey**. You first evaluate your own mobile security and then make evaluations for two people who do not live in Finland, and are not ITC students of TAU. A Finnish respondent is ok, if you are a Finnish student in the Science and Engineering program.

You can choose to do no evaluations at all, or do only your own, or do your own plus one or two others. There will be feedback on these to all course participants. Some automatic statistics can be seen already during the 7 course weeks, but the teacher starts tabulating the data as soon as possible after the deadline.

ESSAYS, 0–2 POINTS

Unlike all the others this exercise is not automatic in any way, but it is carried out in Harpo and scored there. It serves as an exercise toward Exam 3. It will involve the choice of your **essay topics**, but mere choice will not yet give you any points. You will need to write an analysis, receive feedback from the teacher and respond to that in an acceptable way. The teacher feedback may take up to 2 weekdays to arrive, and before it comes you can proceed in this matter only by yourself, not in Harpo. This is the procedure:

1. Invent two topics that belong to different main categories of the ontology, (i.e. insecurity, people and tech.). A good way is to start considering a scenario, ranging from nations, through organizations via your own daily life to development of hardware, software or systems. Then think what can go wrong, who should do something about it, and what security controls would help. Choose one these three aspects (i.e. the main ontology category) and describe the situation with one or two sentences.
2. Receive feedback from the teacher. It may come quickly, or it may take two days depending on the queue of submissions. Before the feedback you can modify your submission but not after. This holds also for points 4 and 6 below.
3. Modify the topics according to the teacher’s advice. Make them problem statements, and write your first draft for a solution, not forgetting to mention sources you have used and intend to use. The draft should be very concise, possibly only listing 5–10 main points. Add in the end a brief evaluation of the process so far, especially in relation to your interests, the feedback, and possible challenges that you may have in learning these topics.
4. Receive feedback from the teacher, including a final decision whether you score 0, 0,5 or 1 points.
5. Modify your solutions to readable but short essays.

6. Receive feedback from the teacher, including a final decision whether you gain additional 0, 0,5 or 1 points.

After this procedure you will see almost the same problems in your Exam 3, and you should try to score the maximal 10+10 points on them, not only by memorizing but by showing understanding. If you don't score at least 10 points you must take the Exam 3 again, and then the two questions are drawn from those that the teacher has modified from other students' essays. Note that you can fail Exam 3 also by not passing the threshold of answering correctly to some questions from your successful automatic exercises.

You can go to Exam 3 with zero score from the essays and even without doing them. In that case you will get randomly chosen essay topics, probably from those the others have written. If you have a full score of 20 from other Harpo exercises, you can still do this exercise, and take the benefit of practicing for the exam. Remember that this opportunity will end before the exam week starts.

MATERIALS

COURSE TEXTS

"NO TEXTS"

The course does not have one text that covers it properly. After this document that you are reading right now, conceptually the best coverage is given by the 117 web pages with text stubs, that accompany the published MCQs. These reside on the Maso site http://sec.cs.tut.fi/maso/. The pages follow the ontology mentioned above, and they are divided to those that provide MCQs for Exam 1 and Exam 2.

Naturally, the Harpo site with its reading tasks gives a practical coverage for those topics, where you choose to gather some credits for passing the course. The site is at https://sec.cs.tut.fi/harpo/. It requires registration with credentials that are given to the enrolled students.

NIST-INTRO

For the student to get a concise and holistic view of the course topics, *NIST Special Publication 800-12, Revision 1*, (2017) is recommended[2]. It bears the title *An Introduction to Information Security*. It suffices to study the main body of the document, pages 7–70 plus section 1.4. There are several topics that will not appear in the exams. The rest of this section gives advice on reading this document, the *NIST-Intro*.

The NIST-Intro is a brief text written in a comprehensive handbook style. The course is not dependent on it or even its vocabulary. For instance, the course does not use the terms adversary and adversarial, but instead attacker and malicious. More notably, the course does not include authenticity and non-repudiation under the concept of *integrity* (cf. sections 1.4, 10.20 and Glossary). The term *authorization* is used in the course mainly in the narrow meaning of granting access rights, while the NIST-Intro deploys the term in more complicated managerial contexts (cf. 6.5 and 7.1).

From chapter 1 only section *1.4 Important Terminology* is needed now, but it is good to be aware of the U.S. context given in the rest of chapter 1. Similar legislation and documents exist in other

[2] NIST=National Institute of Standards and Technology (USA)

countries. The rest of the NIST-Intro makes frequent referrals to the documents outlined in chapter 1, mainly from the NIST or FIPS[3] publications. They are of course not the topic of this course.

The roles described in chapter 3 are not to be taken too “seriously” (i.e. learned verbatim), but each of them shows something that needs to be done with respect to information security. This also includes the supporting roles in section 3.17.

Note that the insider threat is much more than explained in the example of 4.1.2. It is almost common sense that it is more often related to some gain to the insider than just retaliation through sabotage when being terminated. Section 10.16 Personnel Security helps complementing the view.

Chapter 5 Information Security Policy is administrative but very important also for an engineer.

A SIDESTEP TO ISO 270**

It is worth noting here that ISO has published a whole set of standards concerning various administrative aspects, together specifying an *information security management system*, ISMS, for an organization. The standard series spans 19 documents in the numbering range 27000–27021 whereby it is called the ISO 27000 series. It is outlined in the freely available introduction ISO 27000 (Overview and vocabulary). You must learn from what you are reading just now that **ISO 27001** is the most important among these, because organizations can (and sometimes must) get their ISMS certified against it. That is, they get audited, pay, and are given a “badge”: ‘We are managing our IS well enough.’

This sidestep is worthy also because the NIST-Intro does not mention ISO 27000 series at all. This little fact is worth learning also as such because it shows how different standard bodies and different nations can see things differently and do things in their own way. The ISO 27000 document does not, of course, refer to any NIST publication. As a final detail the vocabulary in it defines *integrity* simply as “property of accuracy and completeness”, i.e. without requiring authenticity and non-repudiation.

BACK TO NIST-INTRO

The brief introduction to the NIST *Risk Management Framework* in chapter 6 is good to read, but as a framework (among many others) it will make more sense on later courses that delve deeper into risk management.

Chapter 7 *Assurance* provides more insight into its topic than is required in the exams. Assurance does not appear on the course in one place but dispersed into various places and usually without being named but just linked to issues that need assurance. (Note also that *assurance* does not appear as a term in the ISO 27000 vocabulary.)

The title of chapter 8, *Security Considerations in System Support and Operations* reminds concisely that there are many activities needed to run an information system and most of these activities are not focused on security. And still security needs and opportunities must be considered in everything. The needs are easy to understand for instance in software support or media control (sections 8.2 and 8.5), but spotting opportunities for improvement may require more insight. Examples are shown for instance in sections 8.1 and 8.6 on user support and documentation.

Users are central in several sections in chapter 10 that describes categories of security controls. Section 10.8 *Individual Participation* may seem surprising as a security mechanism or control, but this may not be so if you come from the U.S. or somewhere else where GDPR is not in power; General Data Protection Regulation of the European Union, since 2018, has 99 articles dealing with many aspects of “PII”, personally identifying information.

There are considerably more technical details on cryptography on the course, especially in Harpo, than in the NIST-Intro, but chapter 9 gives a very good context for the techniques. Together with a certain amount of details such contextual understanding is likely to become of lasting value for most

[3] Federal Information Processing Standard (USA).

professions in cyber security. And at the infosec program at TAU it is definitely useful, because the advanced courses have a strong emphasis in cryptography engineering.

Chapter 10 *Control Families* gives a breakdown of security controls into 20 families. As you become more familiar with information security, and partly on this course already, you may find this division interesting by comparing it to other points of view. One influential viewpoint is the Common Criteria standard that firstly divides security into functions and assurance. The functions (given as *functional requirements* in part 2 of the CC) mainly correspond to what is meant by controls in the NIST-Intro. There are 66 families of functional requirements in the CC standard. So, it is better for you to stick to the NIST-Intro. But you must know the existence of CC and its purpose of facilitating assessment of information security – and its idea of doing this by checking various *assurance* requirements to know that the security *functions* (required by the type of system) are effective. The same idea is of course present in the NIST-Intro.

Pay attention to the cost considerations at the end of various chapters. If you enter the profession you need to cause expenses that your employer might think are not justified because they do not bring any income.

CYBER

It is time for a final word on NIST-Intro, ISO 27000, and CC, the three documents treated above. The word is *cyber*. It does not appear at all in the latter two (except in a name of an institute in CC). In the NIST-Intro it appears 8 times on pages 7–70. Only one of the occurrences is *cyber security*, the name of this course, and even that mention comes from a referred document. The other mentions are mainly about cyber attacks and criminals. The name of the previous versions of this course was still *information security* in 2018. The terminological change is anticipated in the Glossary of NIST-Intro on page 79: “Note: DoDI 8500.01[4] has transitioned from the term information assurance (IA) to the term cybersecurity. This could potentially impact IA related terms.”

Why is this course called cyber security? It is trendy, one could say, but it is true that no information security professional should any more ignore the security landscape outside his or her own organization. Any attack can also be part of something more serious that affects or is outright targeted at the critical infrastructure. This matter is not emphasized in the course contents which is rather traditional “InfoSec”. You may wish to take up this sort of topic as one of your Exam 3 essays.

To mitigate the lack of *cyber* in Exams 1 and 2, a quote follows introducing the critical sectors and the way forward with learning “real” cybersecurity, including ENISA’s role in it. ENISA is the European Union Agency for Network and Information Security. It has conducted a study, Stock taking of information security training needs in critical sectors (Dec 2017). This is the executive summary of that document:

> The European Union’s Directive on security of network and information systems (NIS Directive[5]) asserts that “network and information systems and services play a vital role in society”, and that the “magnitude, frequency and impact of security incidents are increasing, and represent a major threat”. Given that urgency, the NIS Directive goes on to argue that “operators of essential services” need to identify “which services have to be considered as essential for the maintenance of critical societal and economic activities”. This is in fact referring to the operators in the so-called critical sectors […]:
>
> - energy,
> - transport,
> - banking,

[4] The DoDI reference is to a Department of Defense Instruction from 2014.

[5] Adopted in 2016. This official ENISA page on NIS refers in future tense to the national actions due in 2018. (Link checked in July 2020)

- financial market infrastructures,
- health sector,
- drinking water supply and distribution, and
- digital infrastructure.

The protection of these seven critical sectors should have the highest priority, because when they are under threat, the functioning of society itself and the well-being of its citizens are at stake. As part of this effort, it is extremely important to increase the competences of cyber security personnel. This requires the availability of high quality trainings across the board, available to all critical sectors.

Within the critical sectors, there are significant differences regarding the maturity level of cyber security. Therefore, some of the critical infrastructure operators will not be as ready as others, to counter the risks resulting from new cyber security threats in a timely and adequate manner.

With the emphasis that the NIS Directive places on the importance of the seven critical sectors, this study aims to identify the current situation in these sectors in regard to the available cyber security trainings, and if there are any training needs specific to each of the sectors, beyond the generic needs for such trainings.

Over the past years, ENISA has developed a wide range of cyber security trainings, and also delivered the training content to several national and governmental CSIRTs (Computer Security Incident Response Teams) as well as their constituents. The next important question that this study set out to answer is if and how the ENISA training portfolio actually is useful for the seven critical sectors – and what could be done to improve the suitability of that portfolio to the existing training needs.

The main general conclusions are:

- the cyber security training field is extensive and diversified, but does not sufficiently address the issue of raising the cyber security resilience of critical infrastructure: CIP-related trainings are still a niche
- there is a shortage of specialised trainings in the field of ICS/SCADA[6] systems cyber security – which is an essential element in countering operational threats (e.g. in the energy sector)
- there are very few trainings specialising in the specific threats encountered in the different (sub)sectors
- cyber security awareness raising trainings are lagging behind
- there is a shortage of trainings in regard to decision making as a result of data leakages or privacy incidents
- there is a pressing need for trainings related to GDPR, since this will affect every sector, and could have an operational impact on the organization.

(EXAMPLE) TRUSTING A PROGRAM CAN BE COMPLICATED

Assume your laptop is running Microsoft Windows and you are editing some files that you need to copy over the internet to a computer at the university. How can you make such file transfers securely?

What you are reading now is an exercise that presents the solution in the third paragraph and then spends 2,5 pages making questions – and hardly providing answers. The intention is to familiarize you with all sorts of issues that are related to trusting a program. There are no other exercises of this kind

[6] ICS = Industrial control system, SCADA = Supervisory control and data acquisition.

on the course, but this example may lead you to think of some other situation as a possible topic for your essay in Exam 3.

Start by finding the correct site to download WinSCP. Is it winscp.net?

Download the program file, and start investigating it. You can do this even if you don't use Windows. The file is less than 11 megabytes and doesn't do any harm.

There are three checksums given on the download page:
MD5: 1dd9535e9f9ee30679b14a6fc16c87b9
SHA-1: b93eb228de3293f74b54974296c72eb6e4fab046
SHA-256: 79de2d5cba143cba220ecf6c76d9e07407243e554ba524a78365ccd881b80214

What coding is this, with abcdef?

You may guess that SHA-256 has 256 bits. How many have SHA-1 and MD5?

The site indeed calls these checksums, but their calculation is much more complicated than mere summation. What is a more precise term for these “fingerprints”?

How can you calculate the fingerprint of the downloaded file? In Windows the keyword can be FCIV. Find the fingerprint of the file and compare it with the one given.

What does a successful comparison prove?

If the file were not ok, why would the page give a correct fingerprint?

So, a matching fingerprint only proves that the file is the same as on the page.

Could you find support elsewhere for the fingerprint, and what would it help?

Now see more closely into the file, but not into its contents but its metadata. In MS-Windows go to >Properties >Digital signatures. Or find a certificate decoder in the web, like https://www.sslshopper.com/certificate-decoder.html to decode this

```
-----BEGIN CERTIFICATE-----
MIIFeTCCBGGgAwIBAgIQAjJGbclbQOydIdkymr/NXTANBgkqhkiG9w0BAQsFADBs
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSswKQYDVQQDEyJEaWdpQ2VydCBFViBDb2RlIFNpZ25p
bmcgQ0EgKFNIQTIpMB4XDTIwMDIxMDAwMDAwMFoXDTIzMDIxNzEyMDAwMFowgZcx
EzARBgsrBgEEAYI3PAIBAxMCQ1oxHTAbBgNVBA8MFFByaXZhdGUgT3JnYW5pemF0
aW9uMREwDwYDVQQFEwg4NzMzMTUxOTELMAkGA1UEBhMCQ1oxDzANBgNVBAcTBlBy
YWd1ZTEXMBUGA1UEChMOTWFydGluIFByaWtyeWwxFzAVBgNVBAMTDk1hcnRpbiBQ
cmlrcnlsMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArjgofJe/Yqm1
CDbY+bsHzq51KVtLZiHMP4vf6u9wNfdsZ93Zr4Z7BS85U/cac0ab7v+zfQSb9SAp
v8K9heu/s02D/5u1St2NFrW9uztFfZeE9L5Vy7IHhqFAdk1ZDTgM5zkuu1DsK/g8
1vjYHFulKdCM/4DVO8dXNQiQfU1o1mMMTIh+ygudKvZtRwQdpJUTkKu26Y4HSDYw
GTtB/BwzTX1T3TCCCOmGSXaqBNrXgQgfgjAs9Zfa5GCoaQOUo8SlH8emNiVuHzJ4
yDixNeiTOLQvJNfLGHAPZShXnrf2BSbYrpBxKCDmucuhMQfgI3VUboR1ohPzZUQ6
eRYSLltk7wIDAQABo4IB6TCCAeUwHwYDVR0jBBgwFoAUj+h+8G0yagAFI8dwl2o6
kP9r6tQwHQYDVR0OBBYEFB6VJN3DGK95aOAEc/7thaBFoj6lMCYGA1UdEQQfMB2g
GwYIKwYBBQUHCAOgDzANDAtDWi04NzMzMTUxOTAOBgNVHQ8BAf8EBAMCB4AwEwYD
VR0lBAwwCgYIKwYBBQUHAwMwewYDVR0fBHQwcjA3oDWgM4YxaHR0cDovL2NybDMu
ZGlnaWNlcnQuY29tL0VWQ29kZVNpZ25pbmdTSEEyLWcxLmNybDA3oDWgM4YxaHR0
cDovL2NybDQuZGlnaWNlcnQuY29tL0VWQ29kZVNpZ25pbmdTSEEyLWcxLmNybDBL
BgNVHSAERDBCMDcGCWCGSAGG/WwDAjAqMCgGCCsGAQUFBwIBFhxodHRwczovL3d3
dy5kaWdpY2VydC5jb20vQ1BTMAcGBWeBDAEDMH4GCCsGAQUFBwEBBHIwcDAkBggr
BgEFBQcwAYYYaHR0cDovL29jc3AuZGlnaWNlcnQuY29tMEgGCCsGAQUFBzAChjxo
dHRwOi8vY2FjZXJ0cy5kaWdpY2VydC5jb20vRGlnaUNlcnRFVkNvZGVTaWduaW5n
Q0EtU0hBMi5jcnQwDAYDVR0TAQH/BAIwADANBgkqhkiG9w0BAQsFAAOCAQEAkACN
0vCCRLPCJfpMyMIXIIYysXez4+ODX4xvUQfWZIrCqzvs+d15rK+KrD2YYyQUdf+i
sBkVGX0jtTT3jP6KQXRZFPo+esnHKv2NPGh3feDRP7w8iSc//PHMD9uuUuGndvIl
YaRgqVNlZ4Ne11PKXL8szR1b/6MbkpdK1cbx/zTnG5UY4/oeAIz1CBUqFh6OIVLP
O3KrJO5afSjnP0KH5Vq4ha9JzwIWMKgJY22CI8OFgRLMpajNbriLdoXCLWkiM4tv
oM/jzrqIOSATO6+cXRF1x0abIGl3mVCL1XfIqdYmrtuHx1m5FOG7uhBdE1sWer7y
EGdvHzDGZOCZFPW7Uw==
-----END CERTIFICATE-----
```

What sort of decoding happened? In other words what coding is it that starts like this `MIIFeTCCBGGgAwIBAgIQAjJGbclbQOydIdkymr/NXTANBgkqhkiG9w0BAQsFADBs` ?

You will see also a person's name. Whose? Is he the attacker who modified the program and digitally signed it? Who gave him the certificate for the code signing key?

(Go to >Details and >View Certificate.) What evidence is given to support the validity of the signature?

(Go to >Issuer Statement.) Which CP and CPS are valid for the certificate in question? See how these documents look like and what they tell about. (CP=Certificate Policy, CPS=Certification Practices Statement)

So, if you trust the certificate and the signature on the program, what evidence do you have that the signer has authority to sign the code?

You apparently get to evaluate the download site. There you get to a similar chain of investigation that first leads to a certificate authority. Then it leads to evaluating the trustworthiness of the site itself. Did they write the code or are they just distributing it? How would you trust that the site is not spreading malware?

Can you find support through some kinds of reputation checks – on the publisher and on the program itself? Does the publisher provide evidence that code was made securely?

Can you see the software license somewhere before starting to install the program? Yes, but can you find the page, without this direct link? When you see it is a GNU GPL, are you relieved that you don't need to read more? Did you notice that there are some picture elements that are not under the GPL, and there are a few extra paragraphs in the license concerning them? And in the end there is also a note on privacy.

You need not install the program, but what is your conclusion, aided with your antimalware software, whether it is safe to install it?

Because the WinSCP file is digitally signed the operating system automatically attempts to verify the signature during installation. Most likely it accepts the signature because it regards the certificate as valid. So, you may think you did the above pondering in vain. Not really, the operating system is no wiser than you, but it just has the CA certificate preinstalled. And it probably still asked you to accept the installation. And furthermore, it probably asked you to provide admin credentials before proceeding.

This is just one example – and quite high in the hierarchy between hardware and humans – of the security tasks of an operating system. This is essential in the modern networked computing, but the more profound security services are lower in the hierarchy. Some of them are almost as old as operating systems themselves, for instance keeping user's code from poking or even peeking into the OS code. Some of the low-level controls are newer, like ASLR, about which you may find out yourself now, or when facing the MCQ on the Maso pages.

Let us get back to WinSCP. If you install and start using it, some important questions still remain.

The program does file transfer between hosts over the internet. How do you know what protection is needed and whether that protection is given? Firstly, how is the destination host authenticated? Secondly how is your transmission encrypted?

Knowing that WinSCP, or some similar program on your own machine, handles the security task properly is largely based on trust and the observation that many others have trusted without any problems. But crowds are not always right. And if you are one the early adopters, you might need to do your own testing by seeing what sort of traffic the program generates. A packet sniffer will help in this, but probably you would need several other tools, also such that are designed to do cryptanalysis or other sorts of attacks.

New programs to be installed would start this story over, and go beyond the course objectives. It is obvious though that you must not see any cleartext in the traffic, and you must not see repeating patterns when you modify the input, i.e. the file to transport. And of course, you should see an SSH handshake. SSH, the Secure SHell, originally a Finnish design from 1995 by Tatu Ylönen, will appear as a basis of WinSCP in what follows.

The main reason to trust the operation of WinSCP is that it provides support for SFTP and SCP and not just FTP. What does this mean? In other words, what are these protocols?

It is apparent that the authors and publishers of WinSCP are honest and try to do their work well. Although WinSCP can be considered a secure program, it has also had bugs, such as an integer overflow. It is described on https://www.cvedetails.com/cve/CVE-2013-4852/ in a single sentence, which can be structured as follows:

Integer overflow
in PuTTY 0.62 and earlier,
WinSCP before 5.1.6,
and other products that use PuTTY
allows remote SSH servers to
cause a denial of service (crash) and
possibly execute arbitrary code in certain applications that use PuTTY
via a negative size value
in an RSA key signature
during the SSH handshake,
which triggers a heap-based buffer overflow.

Here PuTTY is the SSH client program on which WinSCP is based, that is, WinSCP talks to the SSH server at the remote machine through PuTTY.

What stage does the vulnerability described above affect when using WinSCP:

a) Verification of the installation file signature discussed at the beginning of this text,
b) server program authentication to the client program,
c) authentication of the client user to the server or
d) the stage at which the program checks the integrity of the file transferred between machines?

How did you reach this conclusion?

CONCEPTS AND WORDS APPEARING IN EXAMS 1 AND 2

The MCQs for Exam 1 have been made around these 90 concepts.

- 2FA
- Access control
- Accountability
- AES
- Anonymity
- Attack vector
- Authentication
- Availability
- Backdoor
- Backup
- Block cipher
- Botnet
- Buffer overflow
- CAPTCHA
- Certificate authority
- Challenge-response
- Checksum
- Copyright
- Credentials
- Crypto primitive
- Crypto protocol
- Crypto algorithm
- Cryptography
- Cyber attack
- Data protection
- Defence in depth
- Denial of service
- DES
- Dictionary attack
- Distributed denial of service
- DMZ
- DRM
- Eavesdropper
- Encryption
- Entropy
- Exposure
- Firewall
- GDPR
- Hash
- Hoax
- Identity theft
- Impersonation
- Integrity
- Intellectual property
- IPsec
- KEX
- Key
- Log in
- Malware
- Man in the middle
- Non-disclosure agreement, NDA
- Non-repudiation
- One-time pad
- Overwriting
- packet filter
- Passive attack
- Password
- Password salt
- PCI-DSS
- Phishing
- PKI
- Plaintext
- Policy
- Privacy
- Pseudonym
- Public key -- private key
- Ransomware
- Risk
- Risk analysis
- Risk management
- Sandbox
- Script kiddie
- Security control, mechanism, ….
- Separation of duties
- Shared secret
- Signature
- Single-sign-on
- Social engineering
- Spam
- SSH
- Steganography
- Stream cipher
- TLS
- TOR
- Trojan horse
- Virus
- VPN
- WPA
- X.509 certificate
- Zero-day

Here is a list of names and acronyms appearing in both exams, partly repeating the above list, but fairly complete in that matter.

.cmd
.com
.pif
.scr
.tar
.txt
A5
ACID
AES
AH
AI
Amazon
API
ARP
ASCII
Blowfish
Bluetooth
CA
CAPTCHA
CBC
CBC-MAC
CPU
CRL
CSRF
ctrl-Z
CVE
DAC
DDoS
DEP
DES
DH
DLL
DMZ
DNS
DNSSEC
DoS
DRM
DVV
ECB
ESP
ESP
EU
Excel
FICORA
GDPR
HLR
HMAC
HR
HTML
HTTP
HVAC
IaaS
IAM
IEEE
IKE
IMAP
IMEI
IMSI
IoT
IP
IPR
IPsec
IPv6
ISO
Java
JPEG
Kerberos
Kerckhoffs
LAN
Linux
MAC
MAC
MD5
MDC
MFI
Microsoft
MobilePay
NFC
Nigeria
NTP
OS
OS
OSI
Oulu
OWASP
PaaS
PayPal
PC
PCI-DSS
PGP
PICS
PIN
PIN
PKI
PPP
PUK
Rabin
RAM
RBAC
RC4
RDF
ROM
RSA
SaaS
SCADA
sgid
SHA
SHA1
SHA-256
SIEM
SIEM
Siirto
Siirto
SIM
SMS
Smurf
SQL
SSH
suid
SYN
TCB
TCP
TCP/IP
TLS
TOCTOU
TOR
Trojan
Turing
UDP
UN
Unix
URL
USB
USIM
VLAN
VLR
VPN
Wifi
Wikipedia
WLAN
WPA
X.509
XOR
XSS

Finally here is a list of about 400 slightly less common words that appear in the MCQs of Exam 1 and 2. It is here to help you be proactive against possible language problems and not to teach you any infosec. Still, some ordinary words were kept here because of their importance in infosec, or at least in the MCQs.

abstraction
accredited
acquire
adequate
adjacent
admissibility
affiliate
aggregation
airborne
alleged
analogue
apprentice
argon
array
artefact
assessment
atomicity
attest
audit
augment
avalanche
awareness
bait
bastion
beacon
blackmail
bloat
boost
byte
bytecode
callback
cascade
certify
clearance
collation
collude
commission
compatible
compile
comprehensive
condense
conduct
confiscate
conform
conscious
consent
consort
constraint
convinced
correlate
counterfeit
court
credential
custody
dashboard
database
decay
decommission
deduce
deface
defend
degrade
delegate
deliberate
denote
deploy
deprecate
deputy
desktop
deteriorate
deterrence
detrimental
digit
directive
directory
disadvantage
discern
disclaim
disclose
discrete
discretionary
discriminate
dismantle
dispersed
disposal
disrupt
disseminate
distinguish
divulged
dongle
duration
elevated
embarrass
embed
emoji
encapsulate
encode
endanger
enforce
ensuing
ensure
enterprise
entity
entropy
entry
escrow
espionage
establish
estimate
ethics
evade
exclude
explicit
exploit
expose
extinguish
extract
facilitate
fake
falsify
fate
federated
fine-grained
flash-memory
flux
forensic
forge
fragile
fraudulent
fundament
fuse
fuzz
genuine
goods
grant
guarantee
halon
hazard
heuristic
hijack
hoax
hostile
identical
identifier
ignore
illicit
immature
impair
impersonate
implanted
implicit
inadequate
inaudible
incidence
incompatible
incremental
indifference
indirection
inference
infrastructure
infringement
inherent
inheritance
insurance
intact
intangible
intercept
intimidate
intrude
intrusion
iris
irrelevant
iterate
jamming
jargon
kernel
laborious
lack
lagging
launder
layout
leak
legislation
liable
likelihood
load-balancing
log
logarithm
macro
mainframe
malfunction
malice
malicious
mandatory
masquerade
matrix
meme

merchant
metadata
metaphor
microchip
mindset
misspell
misuse
mitigate
modem
modular
morality
mule
mutual
neglect
negligible
neuroimplant
non-mutable
notary
notify
notorious
obfuscate
obligation
obscene
obscure
obsolete
offense
offsite
omit
onion
optimal
outage
outsource
overlap
overly
override
padding
padlock
paradox
parameter
parlance
patch
patent
path
pattern
payee
payer
payload
payroll
perimeter
peripheral
permission
permutation
perpetrator
persist
persuasive
perturbing
phenomenon
plumber
policy
potential
practitioner
pre-assigned
premises
preserve
pretend
prevalence
priority
privilege
prohibit
prone
protocol
provisioning
proxy
prying
quantum
query
quotient
rainbow
random
ransom
real-time
recruit
recursion
redirect
redundant
regulation
relay
rely
remainder
remediation
remedy
render
replay
replicate
reply
reputation
requisite
reside
residual
resilience
resolution
resolve
restore
resume
retrieve
revelation
revenue
reverse
revocation
revoke
roam
rollback
root
rooting
rot
router
rudimentary
runtime
safeguard
safety
salami
sanction
sandbox
sanitize
scalar
scan
scatter
scope
script
scrutinize
secrecy
secret
segment
segregation
semantic
sensitive
server-side
session
shadow
shred
signatory
signature
significance
simulate
skew
smuggle
sniffer
socket
solicit
sophisticated
spam
span
spoof
spreadsheet
stack
stateful
stipulate
stream
subcontractor
subnet
subroutine
subscriber
subsequently
subset
substitute
substring
succession
superuser
supervisor
suppression
surveillance
swap
swipe
syndrome
synonym
syntactic
tag
tamper
tap
tariff
teleworker
tenure
testify
threat
token
transaction
transposition
trapdoor
triad
troll
trustworthy
tunneling
underage
unduly
unforeseen
uninterruptible
unveiling
upheld
utility
validate
vault
vendor
verify
versatile
virtual
watermark
webcrawling
withdraw
wrapper
zombie
zone

There may be more interesting words in the Harpo exercises but there you have better chances of checking their meaning.