
Cyber security I Course handbook

Version 2, 19.10.2020

INTRODUCTION

The course runs for 49 days plus a week since it starts. You must pass the first of the three exams within that time. The exams are called Exam 1, 2 and 3 and they are all compulsory. They must be taken in an EXAM classroom at Tampere university premises using credentials from the [Harpo site](https://sec.cs.tut.fi/harpo/) (<https://sec.cs.tut.fi/harpo/>). Harpo provides exercises that are not compulsory, but they are 20% of the final grade. Harpo requires registration with *credentials that are given to the enrolled students only*.

The multiple choice questions (MCQs) in Exam 1 and 2 are drawn from the other course platform [Maso](https://sec.cs.tut.fi/maso/) (sec.cs.tut.fi/maso/). The essential time limits for the course are:

- **8—(15—35)—54** for **Exam 1**
That is: It becomes available on day 8 and is last available on day 54 (*possibly* also during the weekend days 55 and 56). Until day 15 you can gain full points, after 35 none.
- **36—** for **Exam 2**
- **—49** for News, Survey and Essay, which are special exercises in Harpo.
- **51—** for **Exam 3**

The course does not have one text that covers it properly. Conceptually the best coverage is given by the 117 Maso pages with text stubs, that accompany the published MCQs. The pages follow the division mentioned below, and they are also divided to those that provide MCQs for Exam 1 and Exam 2. 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 document "[Maps and lists](#)", linked also from the Harpo main page, may help when you gather knowledge from various sources for the exams.

OBJECTIVES AND CONTENTS

The concise definition of objectives in the official syllabus is given here.

The aim is to learn basic skills about cyber security, needed by everyone who is studying information technology. The student

- identifies security and privacy threats and responsibilities;
- has a wide knowledge of the concepts, principles and mechanisms of information security;
- knows what kind of additional knowledge and skills is needed to perform various information security tasks in different application areas.

The contents as defined in the syllabus are:

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 Maso platform divides the contents into 11 chapters and 32 sections, abbreviated and given in the listing below. Each section has an introductory subsection, and Exam 1 draws from each of them at most one questions until there are 30 questions. Exam 2 similarly draws 50 questions from the remaining 82 subsections. The number at the end of each row tells how many subsections there are for Exam 2. So, for example the section Program-related threats may provide one question to Exam 1 and two questions to Exam 2.

1	Information and threats		Techniques	5
	General	2	7 Secure practices	
	Personal aspects of threats	2	Access	2
	Crypto-related threats	1	On computers	2
	Program-related threats	2	Simplifying computing	2
	Threats in network	2	8 Crypto	
2	Abstract security		Crypto concepts	2
	Core concepts	2	Key matters	2
	Core principles	1	Symmetric algorithms	1
	Auxiliary	1	Public key algorithms	2
3	Lost security		One-way crypto	1
	If things went wrong	2	General ideas on crypto protocols	1
4	Society		9 Tangible security	
	Data protection	2	Physicalities	7
	Identification	2	10 Transporting data	
	Money protection	3	Local network	2
5	Individuals & groups		WAN, Internet	3
	Networked life	2	Remoteness	3
	Soft issues	2	11 Processing and storing	
	Personal specialities	2	Software	8
6	Organizations		Stored data	6
	Management	5		

The section names will probably make more sense when you see the subsection headings. It is not useful to reproduce it here because you will see it in the Maso platform.

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 full 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

To understand the descriptions below you must recall from the introduction that the course does have a schedule although 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 during the study period). 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 in an EXAM classroom (80%) and a set of unsupervised exercises (20%). Any 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 during the same session, 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.
First opportunity on day 8 of the course.
Last opportunity to pass on the last day of the exam week (i.e. day 54, but possibly 55 or 56¹); 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 $d = \text{day}$, $s = \text{exam score}$, $25 < s \leq 30$. Then
if $8 \leq d \leq 15$, points = $2 \cdot (s - 25)$;
if $15 < d < 35$, points = $(s - 25) \cdot (35 - d) / 10$ 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.

¹ The EXAM classrooms may not be available on Saturdays and/or Sundays, due to the Covid-19 pandemic.

First opportunity on day 36.

Can be done in the same session with a successful Exam 1.²

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 number 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 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 3.³

In addition to the essays, Exam 3 includes questions from 9 Harpo exercises, but only from those where you received a near-full score ($\geq 5/6$). 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.

² It is not at all wise and intended to put off the Exam 1 that late, to a time when it contributes 0 points.

³ If there are fewer than 12 essay topics approved to appear in Exam 3, the teacher crafts the missing ones, providing the essay content himself or as a link to external resources.

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 passing limit is 40 points and the grade 1..5 is determined based on this scale:

40 – **1** – 50 – **2** – 60 – **3** – 70 – **4** – 80 – **5** –

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 (**Harjoitusportaali**=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.
NIST SP: Access control models

Have a taste of engineering of security of systems.
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.