Tampere University / ITC Faculty / Computing Sciences / Comp.Sec.100-02 / Jukka Koskinen

Cyber security I Course handbook

Version 12, 20.8.2025 *(from v11: "Uncertainties in Exam 1&2" + "self-evaluation before Exam 1")*
For academic year 2025–2026

INTRODUCTION

This is a self-paced, self-study course that is nearly continuously available to you. The course is organized as *instances* that start in September and end in July, but you typically need not pay much attention to the switch (cf. page 12 for limitations). You will gather grade points from exercises and from one, two or three exams. You will be granted a final grade based on those points, *at most '1' with one exam only and at most '2' or '3' with two exams*. You can "check out" at any point earlier if needed – but you can still improve your grade after that in most cases. You must pass Exam 1 before attempting Exam 2, and Exam 2 before taking Exam 3. Exam 1 can be passed only once. All exams must be taken in an EXAM classroom at Tampere university premises using credentials from the Harpo site (https://tie-sec.rd.tuni.fi/harpo/). Harpo provides the exercises that form part of the grade, maximally 2/3 of grade 1. Harpo requires registration with *credentials that are given to enrolled students only*.

The multiple-choice questions, **MCQ**s, in Exam 1 and 2 are drawn from the other course platform Maso (https://tie-sec.rd.tuni.fi/maso/).

The course does not have one text that covers it accurately. 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 are also grouped into those that provide MCQs for Exam 1 and Exam 2. The Harpo site, with its reading tasks, gives practical coverage for those topics, where you choose to gather some credits for passing the course. The document ***Maps and lists***, linked from the Harpo main page, will help when you gather knowledge from various sources for the exams. Two Harpo exercises are based on that document. The document also introduces and links to two texts as recommended readings for this course (***NIST-Intro*** and ***Cyber-scenarios***), and mentions a third text, which is a large, freely available textbook, ***CyBOK***. The last one has been used as a basis for the Finnish counterpart of this course, but neither course requires the whole of CyBOK.

OBJECTIVES AND CONTENTS

The concise definition of objectives in the official syllabus is given here. Section 1 in *Maps and lists* elaborates on these, and you will need to reflect on these before your Exam 1.

> 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 (*classes* of the course ontology) and 33 sections, abbreviated and given in the listing below. Each section has an introductory subsection, and Exam 1 draws one question from each of them. Exam 2 draws 52 questions from the remaining 84 subsections, at most one from each. 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	
	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
	Basic but more advanced	2
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 section names will make more sense when you see the *sub*section headings on the Maso platform. For the Essay exercise (page 9 below) it is worth noting that **classes** 1, 2, 3 together are the **category** “insecurity & abstractions”, classes 4, 5, 6 are “people”, and 7, 8, 9, 10, 11 are “techniques”.

REQUIREMENTS AND SCHEDULE

The course offers three consecutive exams for the pursuit of different grades. Each exam has its own passing limit.

The first two exams consist of multiple-choice questions, the third one has essay questions. Together with credits from on-line exercises (i.e. Harpo) the first exam suffices to pass the whole course with grade 1. To obtain grade 2 or 3, also the second exam must be passed, and similarly the third exam for grades 4 or 5. With minimal passing scores from all exams the grade will still be 1, if the on-line exercises have only provided a handful of points. Without exercise points it is theoretically possible to reach grade 5. On the other hand, the exercises can form up to 2/3 of grade 1 when done together with the first exam only.

Study methods: You will read materials – given or linked – do on-line (remote) exercises and take on-line non-remote exams. You probably need to find some information on your own to thoroughly understand the sample exam questions, and certainly to be able to compose good essays in one of the exercises. Studying will happen at your own pace but there will be automatically generated reminders of how time is passing, and a display of what others have achieved on exercises and the exams. The teacher is rather promptly available by email, and your (possible) essay exercise always involves interaction with the teacher. Teacher's reactions are needed also for certain other exercises, optional parts of Exam 2 and the whole of Exam 3.

Criteria for grading: Because of the three-tier structure, grading may seem complicated. Most importantly at this stage, the first exam has the highest passing limit, almost 70% after minus points from wrong answers, but the questions are from the core content only. The exercises can improve the grade with two steps – assuming the appropriate exams have been passed. Exams 1 and 2 are graded automatically, but Exam 2 can have a small input by the teacher. Exam 3 is evaluated by the teacher. The criteria are given below. It is worth noting that each exam has a passing limit, at which the points affecting the grade jump from 0 to 10. Two exceptional and rarely needed paths of passing the course are explained on page 14, a low one and a high one.

MAIN PROCEDURE IN DETAIL

This section adds details to what has been outlined above. The course structure and grading are also visualized with a graph available on Harpo main page. (Start from the orange textbox at the top.)

The grade of this course is determined by scores collected from four components: three supervised exams in an EXAM classroom (in Tampere) and a set of unsupervised exercises. 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:

Exam 1, basic concepts

- You must get your self-evaluation at Maso approved shortly before your first attempt.
- One hour, 32 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 total score.
- If you are uncertain of an answer you can tick a box, resulting in 1/2, 0, or −1/6 points.
- Once you pass this, you cannot take it again. You can discard an attempt *during* the exam if you are not satisfied with your score (by correcting answers to empty). Even the lowest score in Exam 1 does not prevent you from getting the highest grade from the course.
- A minimum of two days (i.e. 48 hours) between attempts.
- Passing level 22/32. Brings **10–20 points** toward the final grade.

- A list of about 90 concepts is given in advance. Each has a related MCQ.
- The MCQs are shown on 33 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 *Maps and lists*.

Exam 2, basic applications

- One hour, 52 MCQs with correcting and commenting options. Uncertainties and 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 four correct answers.
- 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. This unlikely case must be agreed with the teacher.
- Passing level 22/52. Brings **10–40 points** toward the final grade.
- One practice exam is available before each real attempt.
- The exam MCQs are drawn from 84 pages, at most one from each.
- The number of hidden variants in Exam 2 is higher than in Exam 1.

Exam 3, security analysis

- One-hour essay: one big topic (30% of score) and seven small topics (10% each, so, not *very* small), the latter including recollections from certain Harpo exercises.
- Can be done together in the same session with exam 2, if its score is at least 30.
- Three attempts. If all fail and passing of Exam 3 is needed, the only option is to start over from Exam 1. It is very unlikely and not intended either that anyone reaches Exam 3 without having already effectively passed the course.
- The second and third attempt must wait until the teacher has evaluated the previous attempt. Otherwise, there is no minimum interval between attempts.
- Passing level 50%. Brings **10–20 points** toward the final grade.

The big essay question is chosen by yourself in advance from a pool of given topics below. The purpose of the big essay is to let you show your skill of analytic, maybe even critical, thinking, and you should indeed be very careful when composing your answer. Length is not an essential attribute and exact memorizing is not necessary, but the goal is concise expression, good organization and full understanding of what you write. You must remember the essential of your chosen question, though, because your answer will be evaluated against it even if you need not write it down verbatim in the exam.

Here is the **pool of questions for the big essay**. Any changes to this listing during the current academic year will be announced here and on the Harpo main page.[2] The number in parentheses shows what class they belong to.

[1] … but it is not intended to put off the Exam 1 to that late stage of your learning.

[2] These questions are all derived from earlier essay *exercises*, which means you can find fairly good drafts in Harpo. Improve on them using your best skills, more recent sources (references are not needed in the exam, of course), and pay attention to matching the question. See also the teacher's feedback on the essays, at least in their final stage. Note that these essays were written in an earlier setting, without the connection to AI.

- Describe the threat landscape of using an unprotected wireless network. Explain first what it means that a wireless network is unprotected. (1)
- Protecting an information system (IS) against threats directly requires some security measures. Besides such requirements a cyber security professional (CybSecP) must consider requirements that come from outside the system itself. What kinds of requirements can there be? (2)
- What kinds of jobs are there for cyber security professionals? In other words, how are security activities divided among various occupations that have security as their main task? (2)
- How can cyber security be tested, and what are the benefits and challenges of doing so? (2)
- Cities are getting smarter, and the enabling technology is IoT, Internet of Things. How should different stakeholders of smart cities deal with cyber security? (2)
- Ransomware: what makes it possible, how does it operate, how to prevent it, how to recover from it? (3)
- What are the "original" seven critical sectors of a society that cyber security should protect (original in the sense of the *first* version of the NIS directive)? Give real or invented examples of cyber attacks, concentrating on the attack vectors and not the consequences. (4)
- What makes elderly people risky with respect to cyber security? What ways are there to improve the situation? (5)
- How and why should an organization's password policy take into account human factors? (5)
- First describe motivations of cyber criminals. Then describe the opportunities and difficulties they have in reaching their goals. (5)
- What are special requirements that should be expressed in organizational security policies with respect to remote work in contrast to on-site work? (6)
- Humans can be authenticated more strongly to information systems than with passwords, but there are weaknesses also in strong methods. What are the stronger methods and their weaknesses? (7)
- Describe requirements, opportunities and challenges of online voting. (8)
- What are the physical threats to information security? (9)
- How can voice recognition be used for security purposes, and what can go wrong? (9)
- Describe secure networking solutions for remote work. (10)

In addition to the big question, Exam 3 includes seven randomly drawn **small questions**. They come from two sources, mainly:

1. Firstly, there are 10 Harpo exercises that will contribute a question, if you have received a near-full score (≥5/6) on them. 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. If you get more than 7 questions in this way to your Exam 3, the best 7 answers will be evaluated.

2. If you receive fewer than seven questions from Harpo exercises in the above way, the question set is filled to seven by drawing from those questions in your last Exam 2, that you did not get right. Only publicly available questions are involved in this. You can see the set of your non-successful questions after each Exam 2, that is, afterwards and not only at the end of the exam.

3. There is a small chance that these two sources don't make 7 questions. Even 0 is possible in principle. For such cases, a small set of extra questions is given, from where the missing ones will be drawn. This set is available through the Harpo main page.

Exercises on the HARPO platform, mostly automatically graded, will add **0–25 points** to the grade points. Points gathered after an Exam 2 or 3 attempt are not counted for the final grade based on that attempt. If you make a new attempt of Exam 2 or 3 you can try to improve your Harpo score before that. The number of attempts is limited in most of the Harpo exercises, but there are 38 points to pursue, out of which maximally 25 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.
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 Exam 2 or 3 which is used in determining the final grade. For grade 1 based on Exam 1 only, you can gather sufficient Harpo points also after the exam. In general, zero points from Harpo is possible, 25 is the maximum.

You can skip item 3, or items 2 & 3, or item 4, or items 3 & 4.

The passing limit is 30 points and the grade 1..5 is determined based on this scale:

30 – **1** – 40 – **2** – 50 – **3** – 60 – **4** – 70 – **5** –

You can try to improve a positive grade by retaking your last passed exam (except Exam 1) or going for the next level exam, but you must gather any new Harpo points before the new exam attempt.

Transfer of points from one course instance is subject to the Expiry and Update rules stipulated in the end of this document. The points are not usable on other courses, not even on the corresponding Finnish course.

Obtaining the grade. If you earn grade 5 with Exam 3, it will be registered within a few days. Registering a lower positive grade will wait until your request or the Expiry. Registration will not affect your possibility of improving the grade if it is otherwise possible.

Example. There is an Excel sheet available on the Harpo site for you to calculate the effect of various points. Below you can see how it looks like after filling in good but not excellent scores. Points from Harpo and Exam 3 transform directly to grade points, while 12 is subtracted from the Exam 1 and 2 points for that purpose. Pay attention also to the effect of empty and wrong answers in the MCQ exams (the halved "uncertainty" points are not included in the sheet). The example shows the numbers of answers at Exam 1 (25, 5 and 2) but more likely you will use this sheet directly with exam points.

Cyber security 1 exam scoring

Write your results or estimates in green cells to see how grading works.

# of tasks		Give Harpo and **exam** points in these dark green cells.					**Grade** points (gp)
30	**Harpo**	15	Or, clear Ex 1 and 2 cells, and write				**15**
	max=	25	# of answers here.			**Exam**	
			correct	empty	wrong	points	
32	**Exam 1**		25	5	2	24 1/3	**12 1/3**
		22	=min				
52	**Exam 2**	25				25	**13**
		22	=min				
1+7	**Exam 3**	12					**12**
		10	=min	Grade point sum			**52 1/3**
						Grade	**3**

HARPO EXERCISES

You will do exercises on the Harpo platform (**Har**joitus**po**rtaali=exercise portal), which will also let you have the practice exams. The sum of all available Harpo points is 38. This allows you to pursue the highest effective score of 25 points without getting full scores from all exercises.

AUTOMATIC EXERCISES

There are 25 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. *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.[3] 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 ten exercises from which a question will be drawn to Exam 3, if the exercise score is at least 5/6.

Elementary or prerequisites

Cookie & VPN	Connect via VPN and remove the correct cookie.
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

Password *	Classify attacks against passwords.
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.
Spek	Calculate manually a simple cryptotext and a MAC.

Reading

Mindmaps 1	Study *Maps and lists* superficially.
Mindmaps 2	Study *Maps and lists* more thoughtfully.
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"

"Jewels"	Crystallized infosec from van Oorschot's book
Principles and problems	Learn some long-lasting wisdom.
CISSP	Take first steps toward a professional certificate. (2 points)

[3] As an exception, *Cookie & VPN* allows you to try as many times as you like (you will need only one, anyway).

SPECIALS

There are five special exercises in Harpo: Availability, Contributions, News, Survey and Essays. Availability is no more complicated than the automatic exercises, but it cannot be automated. The other specials are larger than the automatic exercises and they cannot be accomplished in one session. A full score in News will need a minimum of 16 days, in Survey probably three days, and in Essays usually more than a week. Contributions can last as long as you study the topics. Altogether you can obtain 0–12 points. Availability and Contributions are approved by the teacher, and 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 produce results that are visible to other participants on the course. Because of the free timing, there is not much interaction, though. Contributions are visible to the world, and they might turn out somewhat interactive. Starting in 2024, there is an ‘extra special’ exercise defined at the end of this section. It is intended to encourage the learning of cybersecurity concepts in Finnish. It will provide 1 point outside the ordinary range of Harpo points.

AVAILABILITY, 0–1 POINTS

Obtain and set up a password management system and a cloud storage system on your computers and write a report on their properties, based on a questionnaire. Submit the report via a file transfer application to the teacher. The names and basic settings of the systems can be shown to others.

CONTRIBUTIONS, 0–2 POINTS

You can earn grade points by writing your learning notes into Maso pages. From the fourth one onwards each note brings you 1/6 grade points until you have 2. The notes are supposed to be contributions to the learning materials for everyone. That determines the criteria for approval of the notes by the teacher. You can contribute more than 15 notes. The extras do not give you points but they will be evaluated. They may also increase your chances of excelling as a receiver of positive votes for your contributions. At the same place where you write these point-aspiring notes you can also submit questions or comments. They do not bring points or reduce your opportunity for contributions, but they may lead to answers by others in their notes of either kind.

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. 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.

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 each course instance, but the teacher will tabulate the data only afterwards.

ESSAYS, 0–3 POINTS

Essays are conceptually related to what you do in Exam 3. This is why you must not start them before you have passed Exam 1.

This exercise is "automatic" in a very special way, and it is likely to be challenging for you and very difficult for the teacher who is supposed to evaluate not only your work but its relation to the work of an AI service. The three stages of the exercise can be summarized in this way:

> **Stage 1:** Pick two topic areas from a list. Develop them into two sufficiently different problem statements and submit them as prompts to an AI, that is, as questions to a large-language model, like ChatGPT. Edit the problems until the AI responses are fully relevant. Submit to Harpo the problem statements and their classification – but *not* the AI responses.
>
> **Stage 2:** Do as the teacher's feedback suggests. Submit to Harpo your modified problem descriptions *and* the AI responses. This stage can bring you up to 1 point.
>
> **Stage 3:** Edit the texts according to the teacher's new feedback, including one scientific reference to support certain claims in each text, as requested by the teacher. Submit the edited texts and the references to Harpo. This stage can bring up to 2 points.

As a TAU student with your account, you can access Microsoft Copilot at bing.com/chat. Copilot can access fresh data because it is also a search engine. There are anonymous services that use an API provided by Chat GPT-4, the best-known public AI in 2024. They limit the quantity and frequency of exchange with the API more than Copilot. As the task is more on you than on the AI, you can do fine for instance with gptchatly.com, even with its prompts and answers limited to 4096 characters, ChatGPT-3.5, and data from 2021. (Prefer to *paste* your question, not to lose your writing when an error occurs.) Also anonchatgpt.com works, but it seems to restrict each question to so short sentences (~244 chars) that you hardly can specify a problem properly. You are allowed to use your @tuni.fi email to register to an AI service for this learning task. For privacy reasons it is better to act without registering, especially in case you do other things besides this task. In any case, do not submit any personal data to these services.

While this exercise is directing you to learn smart AI usage and there certainly are other occasions where AI fits well, *you cannot refer* to this exercise as a justification to use AI in coursework where it hinders your learning or where it is not supposed to be used.

There is a separate document about challenges with essay writing using AI[4], but here is a simple example of how AI can waste your time. The teacher asked ChatGPT to improve the language in the sentence "you cannot refer to…" above. This was the response: "Please do not interpret this exercise as a justification to employ AI in coursework that hinders your learning or is not intended for such use." A nice start and fluent text, but the latter part speaks about *coursework hindering* your learning!

The Harpo page for essay submissions will give you some instructions but this is the main guidance:

> **Stage 1**
> There is a long list of topic areas below, more and less detailed. Pick two that interest you most[5]. Or, if you have experience or interest in something different, propose it to the teacher by email and

[4] See also Maps & Lists section 28.

[5] and such that are **not** yet treated by others *in the way* you intend to do. There is a list of existing essays with short descriptions and links to the texts in Harpo. Use it.

proceed after reaching an agreement. In any case, develop each of your topic areas into a narrower topic that you can classify into one of the 11 *classes* of the course ontology (see page 2 above and more closely Section 7 in Maps & Lists). Then make sure your point of view on the two topics belong to two different main *categories* of the ontology (i.e. insecurity (+abstractions), or people, or techniques).

Each class lies in one main category only (property of an ontology), but the point of view may seem to give variation within a class. For instance, you could think of ransomware as "insecurity", but you probably investigate it in the technologies category, most likely in class 11 (software), or 8 (crypto), or perhaps in 10 if you are focusing on filtering it in the network. However, if you study how laymen should understand the threat posed by ransomware, you are in the category "people". So, understand the ontology before proceeding, and first choose the category, as explained next.

You may start developing each topic by imagining a cyber-interesting scenario within the chosen topic area. In general, the scenario can range *from* nations, through organizations *via* your own daily life *to* development of hardware, software or systems. Continue by thinking what can go wrong, who should do something about it, and how security techniques would help. Choose one of these three aspects. That will correspond to the category. Then find a suitable class in that category. Security problems are often quite wide, and this sort of classification will help you make yours narrower. Describe your topic according to its class *as a problem* with a few sentences.

Submit your problem to AI and see if the answer is relevant to your question from the chosen point of view. Modify[6] the problem description to reach that, and when you are ready, submit your problem description to Harpo (the same you submitted to AI). The teacher will submit it to Copilot and give feedback to you in Harpo – most likely about still limiting the scope and going to certain kinds of details.

Stage 2

Follow the feedback and adjust your question to the AI. Submit the question and the answer, that is, your prompt to the AI and its response. But edit the response not to repeat the prompt.

The teacher will now award you a score 0, 0,5 or 1, depending on how well you managed to direct the AI towards "a correct track". The AI response need not be perfect.

Stage 3

Depending on how good the AI response was, your task at this stage will be to improve it or augment it – based on the new feedback from the teacher. In any case, a specific task will be to find one scientific article to support certain claims in the text and explain how that support shows in the reference. A real essay written by you, not to speak about a thesis, would naturally have all claims supported by references or your own experiments, but this is just a small exercise toward such.

Stage 3 submission will be the result of *your* editing the AI responses from stage 2, and it will bring you 0–2 points, probably with some other feedback. The evaluation criterion is the quality of your work on the two texts, with respect to teacher's feedback after stage 2.

The teacher's feedback may come quickly, or it may take a couple of days. Before the feedback you can modify your submission but not after. One "method" of feedback for both stages 1 and 2 is to redirect or focus you a little as an attempt to give you an opportunity for some analytical or even critical thinking of your own.

[6] Keep a log of your prompts and the responses for yourself. Learn how small changes in the AI prompt can change the response a lot. Try to find a "stable point", which is likely to produce similar response to the teacher, too.

One goal of the essays is to create readable, not very long texts that your fellow students would benefit from. Assume the reader already knows cyber security concepts at least on the level of Exam 1[7].

The maximal two points at stage 3 requires that both texts are thoroughly processed by you, especially they must be free from smooth-looking sharp corners or twists stemming from the AI (cf. the example above) or yourself, and from linguistic errors (easily created by you during the edit work). Naturally, the texts must also be free from coarse errors or omissions regarding their topic. The space (and time of course) is restricted, and something can be missing, hopefully later augmented by the teacher's feedback. Besides providing information to other readers, the criteria for a good essay are quite like those of the "big essay" in Exam 3: concise expression, good organization and full understanding of what you write.

Here is a list of topic *areas* for the essays in the exercise. A good way to ***develop*** these toward *essay topics* (titles & problem statements) is to take an *analytical* point of view. In that way you can achieve more than you could do by only compiling *descriptive* information that the AI has found.

These are for the essay *exercise*, **not** for Exam 3. Its big essay questions start on p. 4.

1. Components of current-day spreading malware.
2. Current state of macro viruses.
3. How can malware be detected if it was never seen before?
4. Reverse engineering of malware code.
5. Evasion techniques used by malware.
6. How does the digital immune system work among a large user base of antivirus software?
7. Money ecosystem of cyber criminals.
8. How can an intruder get into an information system *without* credentials?
9. How can an intruder stay "safe" inside an information system?
10. Psychological explanation of "hacker's ethics".
11. Opportunities for an identity thief.
12. How has social engineering developed over time (since, say, year 2000)?
13. Effect of training and awareness against social engineering.
14. Recent development in user experience (a.k.a. usability) in cyber security.
15. A summary of legal code in a chosen area of cyber security in your country.
16. Forensics and the possibilities of attribution in case of malicious information operations.
17. A chosen type of failures to comply with GDPR, explained with examples of penalties.
18. Sanitization in sociological research.
19. Does AI help more the internet trolls or those who fight against misinformation?
20. How can settings on mobile apps be automated to match the user's security preferences?
21. Preventing data leakage from an organization by filters.
22. The costs and benefits of an information security management system (ISMS).
23. Guidelines or standards for secure information processing practices in your home country.
24. End-to-end encryption for mobile phone calls.
25. Identity-based encryption, idea, practicality, and applications.
26. Homomorphic encryption, idea, practicality, and applications.
27. How is the NTRU cryptosystem doing in the market? What are its benefits and drawbacks?
28. Contract signing – when the parties are remote.
29. How does technology help in digital rights management (DRM)?
30. Parameters for TLS setup (i.e. not for a handshake but for an installation).
31. What can go wrong at different parts of the life cycle of symmetric cryptographic keys?
32. Various levels of PKI certification policies.
33. Blockchain in other uses than cryptocurrency.
34. Properties of parental control software.

[7] and it is not a bad idea for yourself to be aware of Exam 2 level matters before finalizing your essays.

35. Technical properties of password managers.
36. Properties of a chosen class of security software for end-users.
37. Breaking anonymity in TOR.
38. Approaches to censoring the citizens' internet usage.
39. Ability of authorities to access mobile phone traffic data.
40. Tracking internet users.
41. A variety of unlock mechanisms for mobile phones.
42. Body implants / prosthesis that communicate.
43. Low-level IoT gadgets.
44. Anti-tampering technologies on users' devices.
45. Examples of successful product certifications against Common Criteria or a similar standard.
46. Long-term storage of digital archives.
47. Protecting against disturbance or data leakage by electromagnetic radiation.
48. Web browser as a substitute for an operating system.
49. Hardware-assisted protections in modern operating systems.
50. APP-ification in the sense of web transactions being moved to mobile apps.
51. API-fication in the sense of non-professional software developers.
52. Security techniques at various layers of a database management system.
53. What properties in software development environments help in preventing insecure code?
54. How is software tested against security vulnerabilities?
55. Gamification of learning environments (either: cheating in such a system, or: learning security topics).
56. Virtual economies inside games or apps, new vistas for criminals?
57. Misinformation as a tool for far-reaching purposes.
58. Any topic area of the "big essay" questions of Exam 3 (see p. 4) from a clearly different perspective – for instance, a particular e-voting system in a country, or a particular type of physical cyber security.

These are for the essay *exercise*, **not** for Exam 3. Its big essay questions start on p. 4.

EXTRA SPECIAL: *SANO SE SUOMEKSI*, 0–1 POINTS

You can pass your exercises and exams without knowing much more Finnish than "Tampere". Even if you become fluent in Finnish, your foreign nationality may prevent you from entering certain cybersecurity jobs in Finland. However, knowing Finnish is a good asset in the labour market and life in this country, and most cybersecurity jobs here are open to good experts from any country.

On this background, you will be rewarded with one Harpo point for learning some basic concepts in Finnish – under the assumption that this is part of your *learning* this language *in general* – that is, not *only* these concepts and not *only* being a Finnish speaker in an international study program. These assumptions will be checked lightly, and the eventual point will be outside the maximum quota of 25 Harpo points.

Your task is to translate into Finnish one of the concept maps from the Maps & Lists, more precisely, one from sections 2, 3, 4, 6, 19, 20, or 28. Note that the teacher has translated some maps for the Finnish course, and you can find them with these links: section 23, section 26, section 27 (both). Section 29 is *missing* a concept map on privacy. You can also create one for it (still in Finnish). Be sure to include essential details of GDPR in it.

To carry out this task, you can use the same program, CmapTools, or a different one, or you can just draw the map on paper and scan it. In either case, send the product to the teacher by email – with your phone number. The teacher will give you feedback by a call, where he will check that you can explain something from your map in Finnish. For instance: *Miksi luvun 2 kartassa "Informaatio \ data" solmusta "vaihe" on linkki solmuun "Jakelu"?* And as you are still learning, this means: *Why in the map "Information \ data" in section 2 there is a link from node "phase" to node "Distribution"?* Don't take that too seriously. You may be able to answer another question if not just this – and your map may be different. And furthermore, the whole thing can be done in Swedish as well.

TIME LIMITS

The course is continuous but not without an end. If you study actively in the same way as on traditional courses of this size, you need not read this section. Otherwise, please pay attention to the limits on how much time you can use to pursue your grade on this course. The limits consist of a 2-part **expiry** rule and an **update** rule.

Firstly, there is an obvious **unreachability rule:** If you are no more a TAU student, usually noticed by the teacher seeing that your @tuni.fi email doesn't work anymore, then also the rest of your data will be removed from Harpo.

Expiry rule: You must re-register and restart collecting points from zero,

(1) if there are 150 days or more since your last login to Harpo or the Exams, regardless of what you achieved before that.

Naturally if you passed the course, you have obtained your due credits at that time, or they will be registered for you at the expiry time. Note, however, that *improving* a grade that is 5 months old also starts from the scratch.

or

(2) if 300 days or more elapsed since you *passed* an Exam OR accomplished an *automatic* exercise with *more* than 0,5 points (i.e., with at least 2/3 points)

Note that doing only Special exercises does not count here. Of course, they may help you pass the course if you have passed Exam 1, but in that case do not procrastinate beyond those 10 months!

In other words, 10 months' very low activity causes expiry which means that your data is removed from Harpo, and this will already happen after 5 months' complete absence. You will receive automatic email reminders well before either kind of expiry. These emails may also trigger the unreachability observation.

Update rule: Each course instance closes in the end of July, and a new one starts in the beginning of September (at the latest). The Harpo and Exam system are out of use between the instances. The new instance may or may not have a different syllabus and set of requirements. The changes are most likely small. All your earlier achievements will be carried over to the new instance in a fair way, even if there were changes in the scoring or grading arrangements. Also, possible new Expiry and Update rules will not violate your earlier rights.

Issues with the information systems

You must be enrolled to SISU for the study period during which you will earn your grade from this course. This means two things: Firstly, you must have a study right for this course and be attending at the moment when the teacher sets your data into Harpo based on SISU data. Secondly, if your status has changed to insufficient and you reach a grade after that, you cannot get a credit for it. The second point needs your own attention and responsibility, because Harpo does not know about your status, but SISU will not accept credits outside the time of sufficient status.

The registration code for Harpo will change between instances. This will not affect you if you are already registered and have not triggered the Expiry rule. If your data have been removed and you want to restart, you must contact the teacher, also within the same instance.

LOW AND HIGH EXCEPTIONAL PATHS

The course is very flexible from the student's point of view. The most rigid thing is the requirement to visit an EXAM class in Tampere. There is no real exception on this, but in some cases it will be justified for the student to take a slightly different path. The first case is when MCQs seem to cause extra difficulty. The second one relates to high-achieving students who for some reason cannot take Exam 3. This can be the case for exchange students who have a very limited time in Tampere.

Low path

If you pass Exam 1 but with such a low score that you have difficulty in obtaining exercise points to reach 30 – maybe having failed too many exercises – you can try Exam 2. If you pass it, things are fine, but if you do not, you will earn some points for the grade 1, hopefully enough: The rule is this:

> Assume your passed Exam 1 and your Harpo make together x grade points, and $20 < x < 30$. Then prepare and go to Exam 2. It requires 22 exam points to pass. If you only score y exam points and $12 \leq y < 22$, calculate $z = x + 2\times(y-12)$. This will fall in the range 20..50. If z is at least 30, you will pass the course with grade 1. As always, inform the teacher if you want to check out that grade.

High path

Hard-working students often obtain high scores already before their Exam 3, sometimes above 60, in principle even 70. These do not yield the grade 4 or 5 yet without a passed Exam 3. This has a good reason. Exam 3 is the only compulsory check of your learning to *analyse* and possibly even to *evaluate*[8], while the MCQs and most exercises can be passed with lower levels of learning: remembering–comprehending–applying (also needed, of course, and as such not of lower value).

As noted above, Exam 3 might not be possible in some cases. Then the rule to obtain grade 4 is this:

> If you have obtained grade points like this, during the valid time of your study right:
>
> - Exam1 + Exam2 ≥ 40 and
> - Exam1 + Exam2 + Harpo ≥ 60,
>
> then do these extra pieces of work in Harpo:
>
> 1. Do the Essay exercise, successfully. It will be alright, if you already earlier obtained a positive evaluation from the final version of both essays. (Note that the score is single but the verbal evaluation is given individually.)
> 2. Interview two extra respondents in the Survey exercise, representing a "minority", which currently means female and/or aged above 40. You may have done this already and it will be alright, albeit with the young male bias. It did not increase your score anyway.
> 3. Do the Availability exercise. It is alright, if you did this already.

[8] The level of *synthesis* from the well-known Bloom's taxonomy may not be testable with the current methods and it is not among the course objectives either.

All these exercises involve interaction with the teacher (1&3) or some other non-student (2), and this serves as the justification for granting the grade 4 without Exam 3. Especially the essays are quite similar to what you would write in part of Exam 3. The difference is of course that they are not supervised.

It does not matter if your study right expires during these extra bits of work. Harpo does not know about it and your grade will be registered to the date of your last ordinary achievement. However, the course expiry rules apply in the normal way.