TalTech Cyber Security Engineering bachelor's program IVSB

Valdo Praust

IVSB program manager

August 27th, 2026

Why is cyber security such a critical issue?

Unlike a mechanical device, the actual functionality of a digital chip cannot be fully checked or verified - it is extremely expensive and practically infeasible to perform a detailed reverse engineering of a hardware and a simultaneous detailed software audit

- **Usually we don't really know down to the smallest details what's going on inside the digital device (leakage of confidential data, distortion of important information, undocumented hardly noticable behaviour etc)**
- Because it's possible to hide the actual content of the information (steganography), the traditional net traffic monitoring doesn't often help

In order to prevent this it's generally necessary to implement a set of specified steps (which can be considered as security measures) in order to ensure correct and secure operation of any IT-embedded (digital-embedded) device

Example 1 - Mafia group X wants to assassinate a politician Y

Description. the central computer of Politician Y's car; is hijacked by a mafia group X.

When politician Y drives on a mountain road, the Group X takes control of the car. The brakes will be deactivated, the speed will be fixed at 140 km/h, the car's engine stopping capability will be disabled and gear shifting will also be disabled. **Politician Y is no longer able to control the car and the result is a fatal crash**

Note. Most modern cars are almost fully controlled by the central computer rather than directly by the driver– only exceptions are the steering wheel and partly the brakes

Example 2 - Country A intelligence wants to obtain Country B secret military plans

Description. **Country A's intelligence service replaces the jacket button of Commander C of Country B's Defence Forces with an identical-looking one, which also includes a hidden digital interception microphone, a GPS device and a radio transmitter**

The new jacket button will record all secret conversations and will transmit these via radio signals in an area where there are no shield and radio waves detection devices. At all other times, the button remains completely radio silent

Result. Country A will know all about Country B's secret military plans. It will happen because there is a radio shield and a ban on the introduction of a electronic devices in the critical rooms of Country A. But there is no ban for a jacket (with buttons) as it's falsely supposed to be a rigid non-IT device

Example 3 - Vote buying in traditional paper-based elections

Description. **Voters are asked to photograph their ballot in the voting booth using mobile phone after writing candidates' number and before placing the ballot in the ballot box**

After leaving the polling station voters will show a photo of ballot. **If it shows the "correct" candidate number, they receive the permitted amount of money**

Note. In ordinary elections from ordinary citizens it's clearly overkill to be required to abandon a mobile phone when entering the voting boot (and there's no guarantee that they have another phone yet, people cannot be searched)

Classical model of cyber security (information security) – CIA triad

Cyber security is classically a simultaneous assurance of three main goals or **three main components** (which are usually considered to be independent of one another):

- **Availability** – information, that we possess and process, must be available to the parties designated by the business (main) process and at the time, form and other terms specified by the business (main) process
- **Integrity** – concerned parties (designated by business/main process) must know where the information originates and are convinced of its accuracy (i.e. the information has not been falsified or changed in any other way)
- **Confidentiality** – information, carried by the data, must only be available to persons/entities designated by the business/main process and must be inaccessible for all others

From cyber security to Cyber Security Engineering

Ensuring cyber security (simultaneous availability, integrity and confidentiality) it's typical necessary to use and involve **different types of measures/techniques**:

- IT (hardware, software, networks)
- human
- legal
- mathematical/cryptographical
- technical/physical (buildings, facilities, doors, windows etc)

As security is the property of all processes (including IT which support these processes), security needs to be addressed in all phases of a system's life cycle
Therefore, cyber security technologies cover all aspects of IT and much more than IT (human / legal / mathematical and cryptographic / technical and physical etc.)

Securing IT systems and data *versus* securing the main business process

In today's world, the ultimate goal is often to secure the main business process, rather than merely the underlying data and IT systems

- A typical **main or business process** is any area where IT is used - and to which IT usually provides significant additional value
- But IT is used absolutely everywhere!
- Consequently, in addition to IT, **you must in your future life familiarize yourself also with the field where IT is specifically applied** - an attack or security breach is very often field-specific, as a lot of security measures are typically field-specific.
- However, IT systems are often more complex than the business processes they support

IT *versus* Cyber Security *versus* AI

The misconception is that AI does everything instead of us - designs systems, writes software, constructs chips - and we don't have to delve deep into the content

- Yes, AI can do a lot of routine work instead of us – but only if we are able to **properly explain its all principles and rules** to AI
- In critical systems (main processes) **we need to be able to control EVERYTHING that AI does at a conceptual level**. AI may fail to infer what we actually want if the necessary background and context are not provided
- **We need to be able to make it clear to the AI what level of security we want.** Since there are usually hundreds of ways (vectors) for a practical system to compromise security, we need to make this clear to the AI and somehow make sure it understands it correctly. This can be also done with AI, but this activity can only be automated to a certain extent - **we (not AI) need to be able to verify that all security requirements have been met.**

IVSB bachelor's program – main principles

- **We do not assume that students have a prior systematic experience and/or knowledge in IT – we cover during 3 years he main areas of IT at a solid foundational level**
- **But we assume that students have a strong interest in applying IT from a security point of view (together with interest of application of IT in various main processes)**
- **We heavily assume that students have an ability to think logically and algorithmically and have math knowledge on a general international high-school level** – this is the important basis for understanding both IT and IT-controlled and IT-embedded systems. This is assessed in the admission test

IVSB bachelor's program – learning outcomes

1. Understanding the concept of the IT systems life cycle
2. Ability to code, test, and develop, test and deploy an information system with the focus on security
3. Ability to perform information system security testing based on best international standards and practices
4. Basic skills to administer, develop and test secure information systems
5. Adherence to ethical principles in cyber security

IVSB bachelor's program – duration and workload

Duration - three years or six semesters

Total workload - 180 ECTS, including:

- general studies - 30 ECTS
- core studies - 66 ECTS
- special studies - 72 ECTS (incl internship 24 ECTS)
- free choice courses - 6 ECTS
- graduation thesis - 6 ECTS

Valdo Praust, IVSB program manager

- valdo.praust@taltech.ee
- +372 514 3262
- In Teams – available by prior arrangement

- **Experience in the field of IT – 40 years**
- **Experience in the field of data security (cyber security) – 35 years** (since the restoration of Estonian independence in 1991)
- **During last 35 years I have been involved in many Estonian national security-related IT projects** – Estonian ID card, Estonian digital signature project, Estonian national data security standard etc
- **Currently I spend physically a lot of time about 100 km from Tallinn** (developing Estonian Bicycle Museum). **In Tallinn and in TalTech I am usually on the TalTech campus few days a week**

Teaching features at the university (including TalTech Cyber Security Engineering curriculum), I

1. **A university curriculum consists of different courses (compulsory and elective courses). The organisation of studies and the detailed rules may vary considerably across different courses, depending on course nature** (physical attendance requirements, the specific format of lectures/seminars/practices, continuous assessment, etc.)
2. **Each lecturer is actually the „king" or „prince" of his/her own course and decides solely all detailed course rules and teaching organization** - in order to ensure that **course learning outcomes** are actually and effectively achieved

Teaching features at the university (including TalTech Cyber Security Engineering curriculum), II

3. **Courses' learning outcomes, together with the detailed rules, are described in detail in course extended syllabus available in the Study Information System (ÕIS).** The lecturer will certainly also explain these on more detail at the first lecture/contact session

4. **Make sure you attend the very first class in person of every course which you have selected for the current semester!** Some lecturers may decide not to admit a student to the course later if the student has missed the first few weeks — this is at the lecturer's discretion

My (curriculum manager) role in different courses, I

1. **To ensure that the overall combination of courses (compulsory + elective courses) provides a up-to-date, comprehensive and coherent up-to-date practitioner-oriented education without significant gaps.** In the case of our curriculum - a comprehensive practitioner-oriented education in cyber security engineering

2. **For our curriculum-specific courses - to define the course workload (ECTSs) and more detailed learning outcomes together with the lecturer** – in the way that actual course effectively supports the overall goals of cyber security engineering curriculum

My (curriculum manager) role in different courses, II

3. **As a rule, I generally don't interfere the nuances and details of teaching methods inside courses.** These areas are left to the lecturers to decide and to choose a suitable teaching form (I only monitor that **learning outcomes will be actually met**)

4. **In general, I expect that all compulsory courses to be completed. Some exceptions are possible (transfer of credits, recognition of prior work experience), but these remain exceptions and all of these require detailed discussion with me.** The goal remains also in these cases the same: the courses you complete must provide together a comprehensive and coherent education

My role as a curriculum leader across courses, I

1. **I decide all exceptions where the student's curriculum deviates from the set of compulsory courses for some reason** (transfer of previously completed courses, transfer of previous work experience, etc.). **This generally requires detailed discussion with me**. My criteria are simple - in addition to the overall volume (ECTS) being completed, **your overall education must remain comprehensive and must be essentially equivalent to the missed mandatory courses**, and there must be a **serious and important reason for the actual change**

2. **I decide the suitability of the internship** - the **internship activities must have a substantive connection to cyber security** (in details – with some aspects of security)

My role as a curriculum leader across courses, II

3. **I chair internship defence committees**
4. **If a student has a a clear intention to write a final thesis related to a specific topic, I try to help find top specialists in the relevant field as a supervisor or co-supervisor**. I have quite a comprehensive overview of the professional experiences of our different lecturers and also experiences of potential external supervisors
5. **I chair thesis defence committees at all three defending levels** (draft defense, pre-defense, final defense)

My general recommendations for studying (incl. cyber security) at University, I

1. **To graduate (get a higher education) you need to work hard and make a sustained effort.** A university is not a drive-inn or a roadside tavern, where forev everyone is given wisdom and skills like in a food hall. Skills and knowledge are typically acquired through hard work, but in addition, this activities should be **purposeful and wisely organized**

2. **The efforts you will make during the study will be many times greater than the efforts for admission** (a difficult test). This can prepare you for **interesting, demanded and well-paid (preferrably life-long) work in cyber security**

My general recommendations for studying (incl. cyber security) at University, II

3. **You have a lot of freedom at university in comparison with high school, but this certainly requires the ability to properly plan your time.** You must plan your different activities in the long-term perspective in order to avoid "overruns" and/or long periods where you have to live in a regime of 20 hours of work and 4 hours of sleep in order to „survive“.

   No one else will manage your time for you. In high school, much of this planning was effectively done for you through a tightly structured timetable - at university, it’s all **your own responsibility**

My general recommendations for studying (incl. cyber security) at University, III

4. **I don't guarantee that you can absolutely avoid situations when you will be obliged to live in a regime of 20 hours work + 4 hours of sleep and/or 48-72 hours of continuous work.** However, **while planning your time in wise way and for long-term perspective, you can certainly and essentially shorten these periods** (sometimes even avoid)

   Your young organisms certainly tolerate such short strong effort periods as well as fully skipping 1-2 nights in exceptional cases. **Cyber security may occasionally require short periods of intense work during unexpected incidents, but good planning and sustainable working habits should very heavily minimize such situations**

My general recommendations for studying (incl. cyber security) at University, IV

5. **Generally, I assume that you'll devote the next three years primarily to your studies.** This does not mean that you will not be able to work part-time alongside your studies. At the same time, having a responsible and serious full-time job alongside your studies usually **requires compromises** in either your work or your studies

I sincerely hope that you will successfully complete the cyber security studies you are starting today and graduate in three years!

Thank you and good luck!