TalTech Cyber Security Engineering bachelor’s program IVSB

Valdo Praust

IVSB program manager

August 27th, 2025

Why cyber security is an extremly critical issue?

Unlike a mechanical device, the actual functionality of any digital chip is unchekcable and **unverifyable** - 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 up to minor 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 does not often help

In order to prevent this it's generally necessary 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. **Politician Y's car central computer is hijacked by a mafia group X.**

When politician Y drives on a mountain road, the group X overtakes the car driving. The brakes will be deactivated, the speed will be fixed at 140 km/h, the car's engine stopping capability will be disabled and the possibility of gears swiching will bealso disabled. **Politician Y is no more able to control the car and the result is a fatal crash**

Note. Most of contemporary cars are almost fully controlled by the central computer not directly by 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. **The intelligence service of State A replaces the jacket button of Commander C state B Defense Forces with an analog 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. On other times button keeps rigid radio silence

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 electronical 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 - Purchasing of votes for a traditional paper-based ballot elections

Description. From voters there are asked to take a picture from the ballot in cabinusing mobile phone after writing candidates’ number and before entering the ballot info the box

After leaving the polling station voters will show a photo of ballot. **For a case it bears a "right" 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 cab (and there’s no guarantee that they have another phone yet, people cannot be searched)

Classical model of cyber security (information security)

Cyber security is classically a simultaneous ensurance of three main goals or **three main components** (which are usually considered to be independent of each others):

- **Availability** – information, what 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, beared 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 type of techniques**:

- IT (hardware, software, networks)
- human
- legal
- mathematical/cryptographical
- tehnical/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 system
Therefore, cyber security technologies cover all aspects of IT and much more than IT (human factor, legal factor, physical security, etc.)

Security IT system/data *versus* securing main or business process

In contemporary world instead of securing data and IT systems there are often secured main or business processes

- 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 (processes where IT is used) itself 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 in case if we are able to **properly explain its principles and rules** to AI
- In critical systems we need to be able to control **EVERYTHING** AI does at a conceptual level. Often AI doesn't understand what we want it to do because we don't explain all the background and context
- **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 the AI) **need to understand that all the security requirements are met**.

IVSB bachelor’s program – main principles

- **We do not assume that students have a previous systematic experience and/or knowledge in IT – we cover during 3 years all main topic of IT in certain (a little bit more than basic) level**

- **But we assume that students have a deep interest in IT from a security point of view (together with a deep interest of application of IT in various main processes)**

- **We heavily assume that students have an ability to think logically and algorithmically** – this is the important basis for understanding both IT and IT-controlled and IT-embedded systems. We have tested it in admission test

- **We assume that students have a math knowledge on a general international high-school level** – we have tested it (together) with algorithmical thinking in admission test

IVSB bachelor’s program – learning outcomes

- Understanding the concept of the IT systems life cycle
- Ability to code, test, and distribute of an infosystem with the focus on security
- Ability to perform information system security testing basing on best international standards and practices
- Basic skills to administrate, develop end test secure information systems
- Adhering ethical norms of the cyber (data) security

IVSB bachelor’s program – duration and amount

Duration - three years or six semesters

Total amount - 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 previous demand

- Experience in the field of IT – 40 years
- Experience in the field of data security (cyber security) – 34 years (since restoring Estonian independence 1991)
- During last 34 years I have involved in a bulk of Estonian national security-related IT projects – Estonian ID card, Estonian digital signature project, Estonian national data security standard etc
- Contemporarly I spend physically a lot of time 100 km's from Tallinn (developing Estonian Bicycle Museum). In Tallinn and in TTU campus I am physically available usually some days in week

Thank you!