InSecTT Newsletter May 2023

Welcome!

This is the **May 2023 edition** of the InSecTT newsletter, highlighting news & achievements from InSecTT during Q1 2023.

Please distribute this newsletter to all interested parties in your organization. We appreciate your feedback, please send comments or requests to Insectt@v2c2.at.

Enjoy the reading!

Table of Contents

Every digital Moment secured

March 2023

F-Secure’s Threat Intelligence Lead Laura Kankaala joined the InSecTT podcast to discuss the cybersecurity and threat landscape in IoT. Laura shed some light on what are the current threats out there, and what can we do to protect society and end users. Laura also provided some insights on F-Secure’s research focus and the current status of progress.

In InSecTT F-Secure focuses on finding alternative security solutions to protect IoT devices of users, as the common security applications cannot be installed. The research focuses on analyzing the network traffic flow from the IoT devices connected in home and forming and understanding of the normal type of behavior of the IoT device. This forms a baseline towards any potential abnormal behavior or IoT network activity, that may be malicious, can be reflected – and detected.

Check the InSecTT podcast episode here: Project InSecTT: Laura Kankaala from F-Secure on cybersecurity in IoT: what are the threats out there, and what can we do to protect society? on Apple Podcasts https://buff.ly/3zaTzBi

What should you consider when developing secure software?

March 2023

What should the users of IoT take into account when buying and using the IoT devices? Check the tips from InSecTT partner F-Secure's Threat Intelligence Lead Laura Kankaala in the newest InSecTT podcast episode #11 about the cybersecurity and threat landscape in IoT. Project InSecTT: Laura Kankaala from F-Secure on cybersecurity in IoT: what are the threats out there, and what can we do to protect society? on Apple Podcasts: https://buff.ly/3zaTzBi

Advice for developers Developing secure IoT system & devices:
1) Use modern technology stack, i.e. modern programming languages – whenever possible
2) Create channels for updating the IoT and make sure they are updated

Advice for users of IoT and connected devices:
1) Change any default passwords of the devices you have
2) Make sure you update to the newest software available
3) Try to find a product that is not directly connected to internet
4) If possible, don't always buy the cheapest device as the price often reflects the amount of effort put to the security of the device

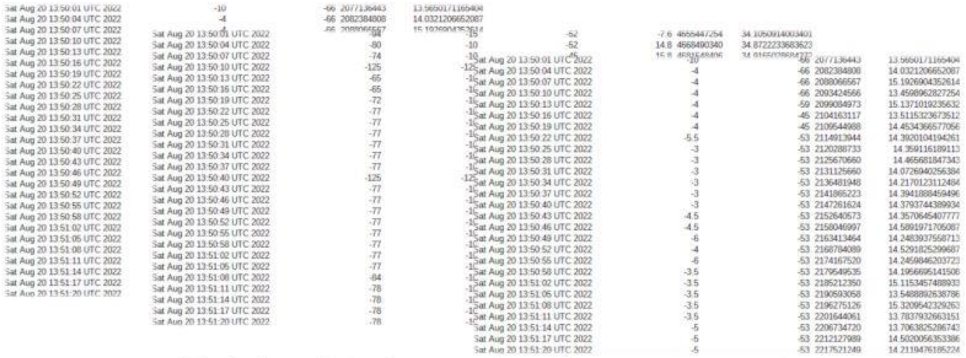
AI assessing uplink quality

March 2023

Onboard systems in vehicles face continuously changing uplink conditions, depending on factors such as coverage, network load, and environmental conditions.

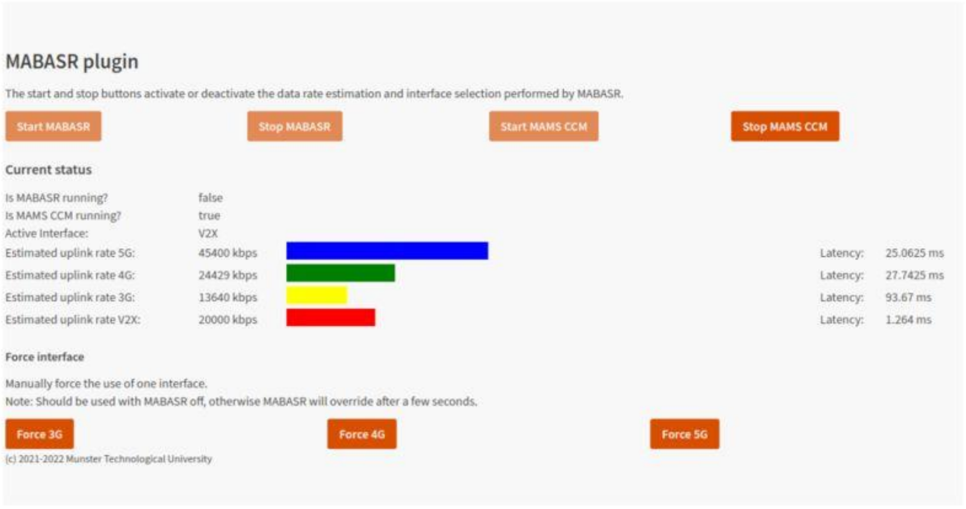
In InSecTT, MTU has developed AI algorithms, trained with real-life mobile network data collected with equipment from project partner Klas, to assess available resources and manage uplink connections efficiently.

#InSecTT #AI #research



Training data from network measurements

Resource estimation and interface decision



MABASR plugin

The start and stop buttons activate or deactivate the data rate estimation and interface selection performed by MABASR.

Current status

Is MABASR running?	false			
Is MAMS CCM running?	true			
Active Interface:	V2X			
Estimated uplink rate 5G:	45400 kbps	🟦	Latency:	25.0625 ms
Estimated uplink rate 4G:	24429 kbps	🟩	Latency:	27.7425 ms
Estimated uplink rate 3G:	13640 kbps	🟨	Latency:	93.67 ms
Estimated uplink rate V2X:	20000 kbps	🟥	Latency:	1.264 ms

Force interface

Manually force the use of one interface.
Note: Should be used with MABASR off, otherwise MABASR will override after a few seconds.

(c) 2021-2022 Munster Technological University

New Podcast: Venkatesha Prasad from TU Delft

March 2023

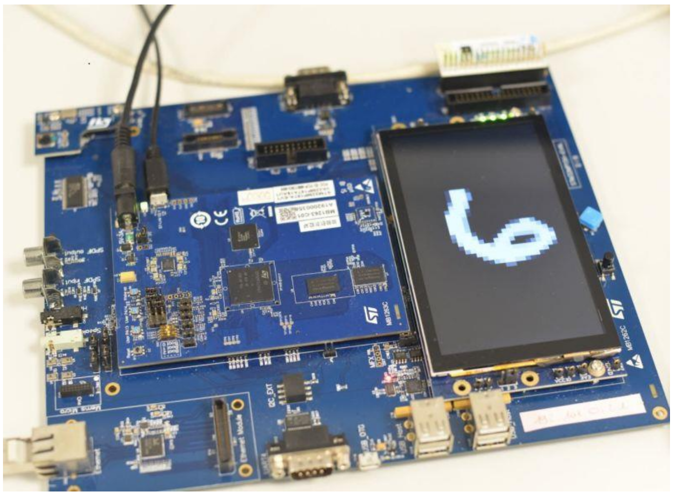
6th March 2023: Today, Venkatesha Prasad (known as 'VP') tells Anamarija about how he came from small-town India to TU Delft in the Netherlands. VP explains the research he and his team at TU Delft do in InSecTT, and what he expects to see in IoT for the near future coming up. So ... is the revolution of the Internet of Things already over, or are we still at the beginning? Tune in to find out

Security: Advanced Threats Analysis

March 2023

One of the most important limitation on the large-scale deployment of machine learning models in a wide variety of hardware platforms is security. That's why security of AI is a hot topic for many partners of InSecTT. The Security of Machine Learning community has demonstrated many attacks at every steps and elements of the traditional ML pipeline. The threats could be algorithmic but also implementation-based, meaning that models are not pure mathematical abstractions but strongly depend on their software or hardware implementations. InSecTT is analyzing advanced threats that aim at directly altering the values of the internal parameters of a model that are stored in memory, for example the Flash memory of a 32-bit microcontroller (a typical platform for IoT). Such attacks can significantly drop the accuracy of a model with only a few bit-flips or even bring enough information to help model reverse engineering.

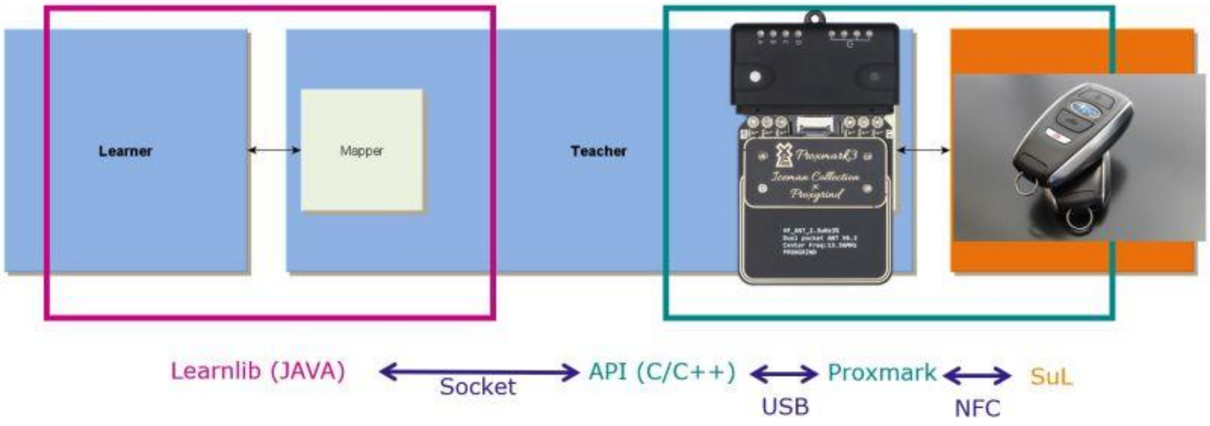
Check our paper published at IEEE IOLTS 2022 on the evaluation of the Bit-Flip Attack (https://buff.ly/3IzxtNd)



Cybersecurity Testing of car access systems

February 2023

#AVL and #NXP develop cutting edge learning-based #cybersecurity #testing approaches for #automotive car access systems.
We try to infer a model of the system-under-test and subsequently use model checking and fuzzing techniques to derive security test cases.
This allows for deriving intelligent automated security testing for these systems, ultimately leading towards more secure vehicles.



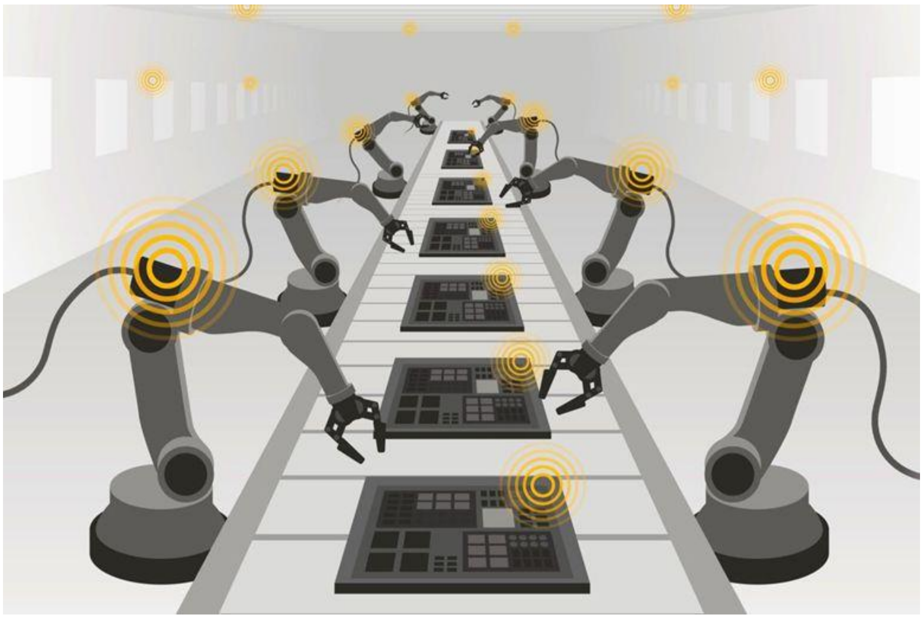
AI-enhanced secure and reliable communication

February 2023

The high number of interconnected devices, provided by wired and wireless communication infrastructure within factory network and with the outside world generates a severe vulnerability against either intentional cyber attacks from external sources or unintentional disruptions caused by the devices themselves utilised in manufacturing sites. One of the usecases in the project InSecTT, Cybersecurity in Manufacturing, aims to develop a reliable and secure communication layer for both wired and wireless manufacturing infrastructure. This use case is provided by Arçelik Global which is a partner of InSecTT from the manufacturing domain.

The use case will focus on how to leverage AI-enhanced secure and reliable communication technologies to improve manufacturing and production plants' security, safety, and reliability. The use of communication technologies with AI integration will increase security and reliability, achieving the two main objectives of preventing interruptions and widespread harm from cyberattacks and offering a reliable system with high-quality output.

#ECSELJU #H2020 #research #manufacturing #IoT #AI #wirelesssystems #robot #robotics



InSecTT

5G wireless communications for Intelligent transport systems

February 2023

Capgemini Engineering is an integral part of the Capgemini Group, a global leader in partnering with companies to transform and manage their business by harnessing the power of technology and innovation. Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering, and platforms. For the InSecTT project, Capgemini is researching 5G wireless communications for Intelligent transport systems mainly, platoon use cases, bringing a system level simulator together with a network and management platform.

Biometric and sensing tecnologies at airport passenger terminals

January 2023

Within the #Insectt project, Aeroporti di Puglia works on the application of biometric and sensing tecnologies at airport passenger terminals, in order to provide a faster and effective recognition system, to detect dangerous situations and to track anomalies on the move.

Moreover, Aeroporti di Puglia also works on the application of an electromagnetic sensing network suitable for the monitoring of drainage channels crossing the airport grounds.

InSecTT

AI and IoT for security systems at airports

January 2023

Aeroporti di Puglia SpA is one of 50+ partners in #InsecTT, a pan-European project oriented to provide smart solutions into the domain of Artificial Intelligence of Things.

In terms of airport security, the InsecTT project exploits #AI and #IoT to integrate existing security systems at airports, allowing the analysis of structured and unstructured flow of people in airport terminals and the monitoring of critical access points to the airport grounds.

https://buff.ly/3IW5edl

AEROPORTI DI PUGLIA

BARI BRINDISI FOGGIA TARANTO

InSecTT

Process control in large construction projects

January 2023

One of the main challenges faced by large civil infrastructure construction projects (e.g., construction of highways, railways, tunnels, etc.) is to provide stakeholders with up-to-date information about the actual progress of construction tasks. This is needed to measure productivity and for early detection of deviations from original project planning.

The complexity of such challenge derives from the large areas where these projects are executed, the large number and variety of machinery and workers involved, and the difficulty of deploying monitoring technologies in these environments.

Within the InSecTT project, ACCIONA is addressing this challenge for a specific scenario of automated productivity measurement in the construction of tunnels through conventional methods (drill & blast). This is achieved through advanced processing of data collected by IoT-based workers and machinery tracking systems, and electricity consumption monitoring. Thus, it is possible to detect and automatically measure the different tasks within each tunnel excavation cycle, and to quantify the resources used for each task.

InSecTT

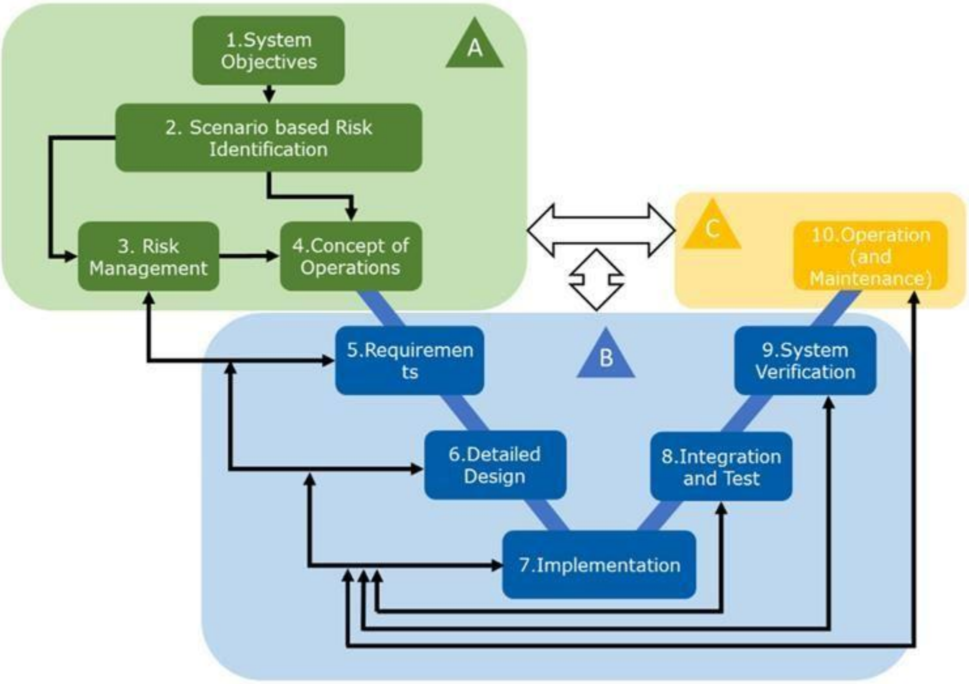
Trustworthy AI

January 2023

Throughout the last two years, Virtual Vehicle conducted a series of workshops to explore how to develop AI applications that are perceived as trustworthy from the user´s perspective. These workshops led to a model for how to integrate humans with systems to achieve trustworthiness.

Early on, we analyzed existing recommendations in EU Ethics Guidelines and ISO specifications, as well as the proposed legislation in the EU AI Act. These recommendations were discussed in a sequence of workshops to identify trustworthiness risks in individual InSecTT use cases and to find approaches to mitigate them in development. The resulting human systems integration model for trustworthy AI is intended to enable the potential of AI applications toward accepted use and uptake within the consortium and beyond.

Human Systems Integration Process Model for the Orchestration of Trustworthy systems

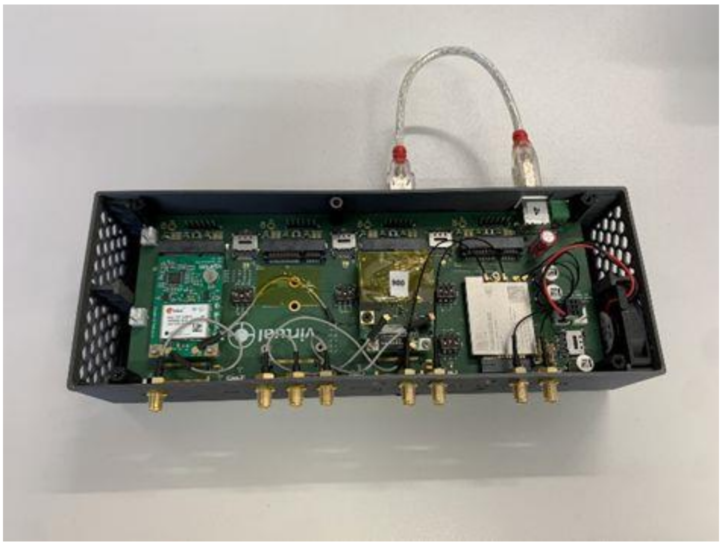


InSecTT

InSecTT is contributing to Open Software

January 2023

InSecTT is powering the vehicle communication systems in our automated vehicles. Project results, such as the vehicleCAPTAIN foster the basis for the technologies of tomorrow. Our 52 partners provide highly valuable input for our research and development.We are proud that we can soon give something back, by releasing core software as free and open source.



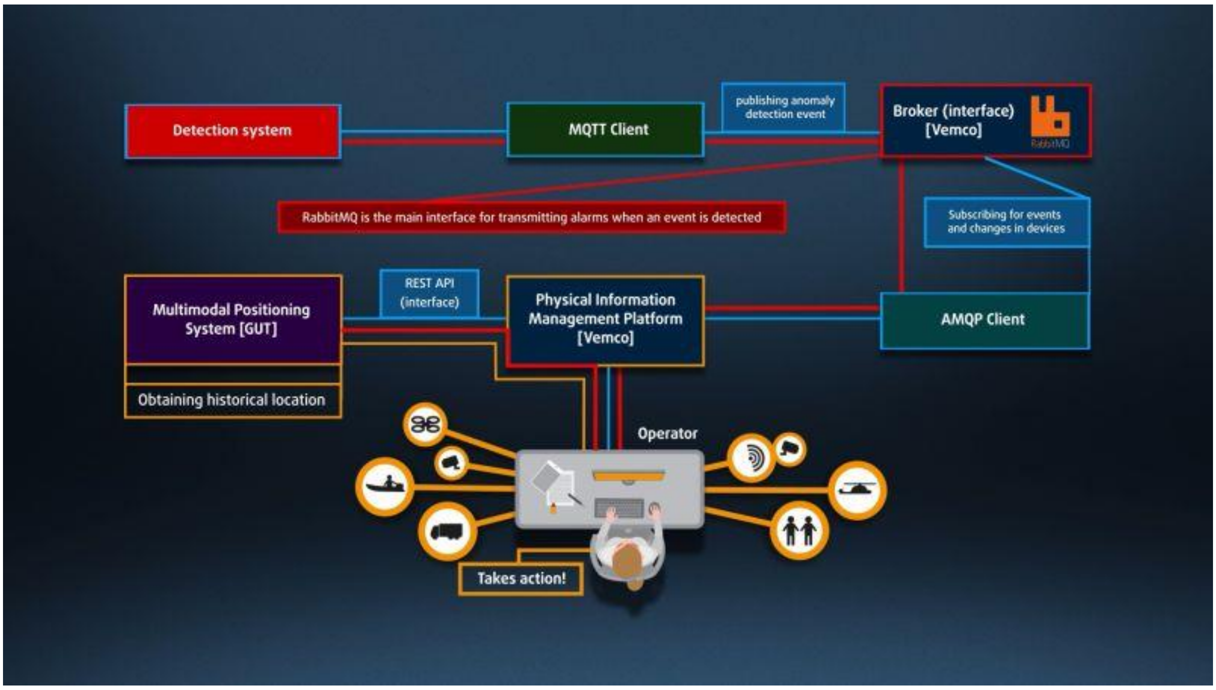
A Physical Security Management Platform

January 2023

In InSecTT Vemco is mainly focused on building Physical Security Management Platform (PSIM). PSIM allows to integrate multiple systems used by single company in one platform. Integrated systems maybe developed for security and safety purposes, localization-based, detection, etc.

The very important functionality of PSIM is allowing operator / administrative user to observe improper on-facility behaviors / deivces functioning, by receiving alarms and reacting to them.

On the graphic below we present a common situation in which integrated system is used in PSIM interface. In the beginning integrated system detects an anomaly which is then transported via MQTT / AMQP protocol to RabbitMQ message broker. From there PSIM subscribing service receives detection message and informs the operator about potential threat. The operator is able to raise an alarm and observe the whole situation from the point of view of other integrated systems during detection time.


Detection system
MQTT Client
publishing anomaly detection event
Broker (interface) [Vemco]
RabbitMQ
RabbitMQ is the main interface for transmitting alarms when an event is detected
Subscribing for events and changes in devices
Multimodal Positioning System [GUT]
REST API (interface)
Physical Information Management Platform [Vemco]
AMQP Client
Obtaining historical location
Operator
Takes action!