UMONS
Université de Mons

inforTech
UMONS RESEARCH INSTITUTE
FOR INFORMATION TECHNOLOGY
AND COMPUTER SCIENCE

Infortech Day 2023
Cybersecurity, IoT and HPC

May 24th, 2023, 9:00-17:00
Université de Mons, Belgium
Venue: De Vinci building, room Mirzakhani (1st floor)

9:00 Welcome

9:15 Opening words – Président d'Infortech, *Tom MENS*

9:25 Keynote "IoT Security"

An BRAEKEN (Vrije Universiteit Brussels)

Abstract: *The Internet of Things (IoT) refers to a network of devices (e.g. lamps, smart door locks, vehicles, medical sensors, etc) that are connected to each other to communicate data over the internet. The enormous amount of devices connected to the internet, the constrained nature of these devices with respect to battery, memory, computing resources, as well as the need to be easily accessible and user friendly makes IoT devices easy entry points for hackers to obtain access to privacy sensitive data or disrupt critical systems. In this presentation, we will explain where and how security needs to be integrated during the design process of these devices and their applications.*

10:25 Coffee break

10:40 Technical session 1 – chair: *Bruno QUOITIN*

- **Zero-Touch Mutual Authentication Scheme for 6TiSCH Industrial IoT Networks** (20 min.)
  Ali HAJ-HASSAN (FS/Info)

Abstract: *The rapid growth of the Internet of Things (IoT) has led to an increased number of devices connected to the internet, including industrial devices. However, this growth has also brought about security concerns, particularly in the authentication of new nodes joining IoT networks. Authentication of new nodes is crucial to ensure the legitimacy of the network and the authorization of the new node to the network coordinator. In the case of Industrial IoT (IIoT) networks, which are usually large-scale and dynamic, the process of sharing a pre-shared key (PSK) between the network coordinator and the joining node is impractical. To address these challenges, we propose an autonomous mutual authentication and key establishment protocol for IIoT networks. Our solution involves a certificate-based authentication process for the joining node, followed by a lightweight consensus protocol*

based on Shamir Secret Sharing for authenticating the network coordinator. Once mutual authentication is achieved, a key is established over a public channel. We integrated our solution with the joining phase of 6TiSCH framework and evaluated its performance on a real industrial protocol.

- **Physical Layer Authentication** (20 min.)
  Ewan GENCSEJ (Polytech/TELE)

  Abstract: *Physical layer authentication enables differentiation between legitimate and rogue receivers. Two active schemes, which are better suited for industrial applications, are available: superimposed tag and slope authentication. The former sends an authentication signal simultaneously with the data signal, while the latter scrambles the data symbols using a secret key to authenticate the sender. Currently, I am attempting to retrieve the simulation results of the two papers that present these methods, and here are my findings.*

- **Deep learning based LoRa device identification using Radio frequency fingerprinting** (20 min.)
  Aqeel AHMED (FS/Info)

  Abstract: *LoRa has gained popularity as the de-facto physical platform for the internet of things. Given its ability to allow communication at low power and long range, it is suitable for various IoT applications such as smart homes, smart cities, smart agriculture and environmental monitoring. However, security is still a major threat to low cost IoT devices. One of the main security aspects is the identification of legit and malicious devices in the network. Recently, Radio frequency fingerprinting method has gained the attention of researchers in the area of device identification. Radio frequency fingerprints of a device are specific hardware features that cannot be cloned and altered. In our work, we are exploring the use of deep learning based radio frequency fingerprinting to identify a LoRa device in the network. To this end, an existing dataset is used to reproduce a part of the work already done by the researchers. These results will act as baseline for our future research in this direction.*

- **Secured Federated Learning** (20 min.)
  Xavier LESAGE (Polytech/ILIA)

  Abstract: *Federated Learning is an emerging technology in the field of machine learning that allows deep learning models to be built using data from multiple sources, without the need to centralise the data. Advanced encryption techniques, such as Secure Multiparty Computation (SMPC), homomorphic encryption, and differential privacy, allow for protection from inference and poisoning attacks. In the field of health, federated learning allows several hospitals to contribute to machine learning models without compromising the confidentiality of patient data. In manufacturing, this approach allows a company with globally dispersed production sites to improve product quality while ensuring better data security and privacy.*

12:00 Lunch sandwiches

12:45 Keynote "*Enjeux en HPC, supercalculateur Lucia et scénarios d'utilisation à Cenaero*"

Cécile GOFFAUX (Cenaero)

Abstract: *Lucia est un calculateur haute performance inauguré en Novembre 2022, opéré par Cenaero et hébergé par A6K à Charleroi. La puissance de calcul agrégée de Lucia se monte à 4 Pflops, ce qui le place parmi le top 500 mondial des supercalculateurs. Cet outil supporte la demande croissante des entreprises et centres de recherche pour le calcul HPC et la simulation numérique, avec des applications dans des domaines très divers tels que l'automobile, l'aéronautique, les télécommunications, la santé, la chimie ou encore l'étude du climat.*

13:45 Coffee break

14:00 Technical session – chair: *Véronique MOEYAERT*

- **Best Approaches for Customs Fraud Detection** (20 min.)
  Sedrick STASSIN et Otmane AMEL (Polytech/ILIA)

  Abstract: *The rapid growth of e-commerce has placed considerable pressure on customs representatives. Artificial intelligence (AI) systems have emerged as a promising approach to minimize the risks faced in the customs domain. In this presentation, we introduce various approaches that perform well for customs fraud detection: first, unsupervised approaches to predict a fraud label, and second, approaches to predict Harmonized System (HS) codes, a crucial element for an accurate customs declaration. Finally, we investigate the performance of such models with the multimodal information at our disposal.*

- **Verification of computer systems thanks to state machines** (20 min.)
  Gaetan STAQUET (FS/Info)

  Abstract: *Due to the roles computer systems play in our society, it is of paramount importance to verify that these systems behave as expected. Performing "classical" testing methods (unit, integration, and so on) can be a cumbersome task. Moreover, they do not guarantee that the system is bug-free. On the other hand, there exists a branch of the formal methods where systems are abstracted into finite state machines. Since these machines are easier to manipulate and understand than the original systems, they can be used to verify that a problematic behavior does not occur. In this talk, we introduce these finite state machines, how to construct them from a system, and, finally, we give a concrete example, based on the verification of JSON documents against a set of constraints.*

- **A Preliminary Study of GitHub Actions Dependencies** (20 min.)
  Hassan ONSORI DELICHEH (FS/Info)

  Abstract: *GitHub Actions was introduced in 2019 as a software development workflow automation tool, allowing to automate a wide range of social and technical activities in GitHub repositories. These Actions are developed in GitHub repositories and can be distributed through the GitHub Marketplace. GitHub Actions forms an ecosystem because workflows can rely on reusable Actions, that themselves may depend on other components such as NodeJS packages, Docker images, or other Actions. Just as packages in software*

library ecosystems have been shown to suffer from a multitude of maintainability issues due to their complex dependency networks, we posit that the same is true for Actions. Therefore, this paper presents preliminary insights in the dependencies of Actions. Based on a dataset of 2,817 Actions, we report on the characteristics of these Actions and we explore to which extent they are developed using JavaScript, Docker or as composite Actions, and to which extent they depend on other components. We show that most Actions are developed using JavaScript, and that composite Actions are gradually replacing Docker Actions. We also show that Actions have many dependencies, especially towards JavaScript packages, resulting in a large number of deeply nested transitive dependencies. This justifies the need for further maintainability studies of the GitHub Actions ecosystem.

15:00 coffee break

15:15 Technical session – chair: *Saïd MAHMOUDI*

- **Multipath Transport Protocols for Now and Beyond** (20 min)
  Quentin DE CONINCK (UCLouvain)

  Abstract: *This presentation gives a quick introduction of the recent advances at the transport layer during the last few years, notably through the introduction of the QUIC protocol and the multipath extensions in both TCP and QUIC. It then describes existing deployments of multipath solutions and discusses the importance of matching the multipath algorithms to their serving use case. It finally concludes with potential new use cases opened by (Multipath) QUIC.*

- **Product Quality Optimization through Production Line Analysis using AI in Industry** (20 min)
  Tojo Valisoa ANDRIANANDRIANINA JOHANESA (Polytech/ILIA)

  Abstract: *IoT sensors enable real-time data collection on production lines that can be used to control the quality of output products. Some parameters of the production process have a direct impact on product quality, making their monitoring crucial. We propose to use AI to predict critical control parameter values based on other input process parameters, in order to adjust input parameters in case of predicted value deviation. This approach will help to optimize product quality and reduce manufacturing defects.*

- **Artificial Intelligence and Deep Learning for 2D/3D object detection with the presence of occlusion** (20 min)
  Zainab OUARDIRHI (Polytech/ILIA)

  Abstract: *The popularity of smart video surveillance (SVS) systems has increased due to its autonomous monitoring capabilities, which include the environment and infrastructure's automatic detection, tracking, analysis, and follow-up activities with little to no human intervention. Particularly in this field, object detection tasks are frequently used. The capacity to train models using big datasets within high performance infrastructures allowed deep learning algorithms to provide excellent efficiency. Object detection and recognition are made more challenging by the fact that a majority of existing learning strategies are limited by a range of data availability and network performance issues. These methods, in particular, handle every object independently and do not account for the relative occlusion of surrounding objects, which causes SVS systems to experience a variety of occlusion*

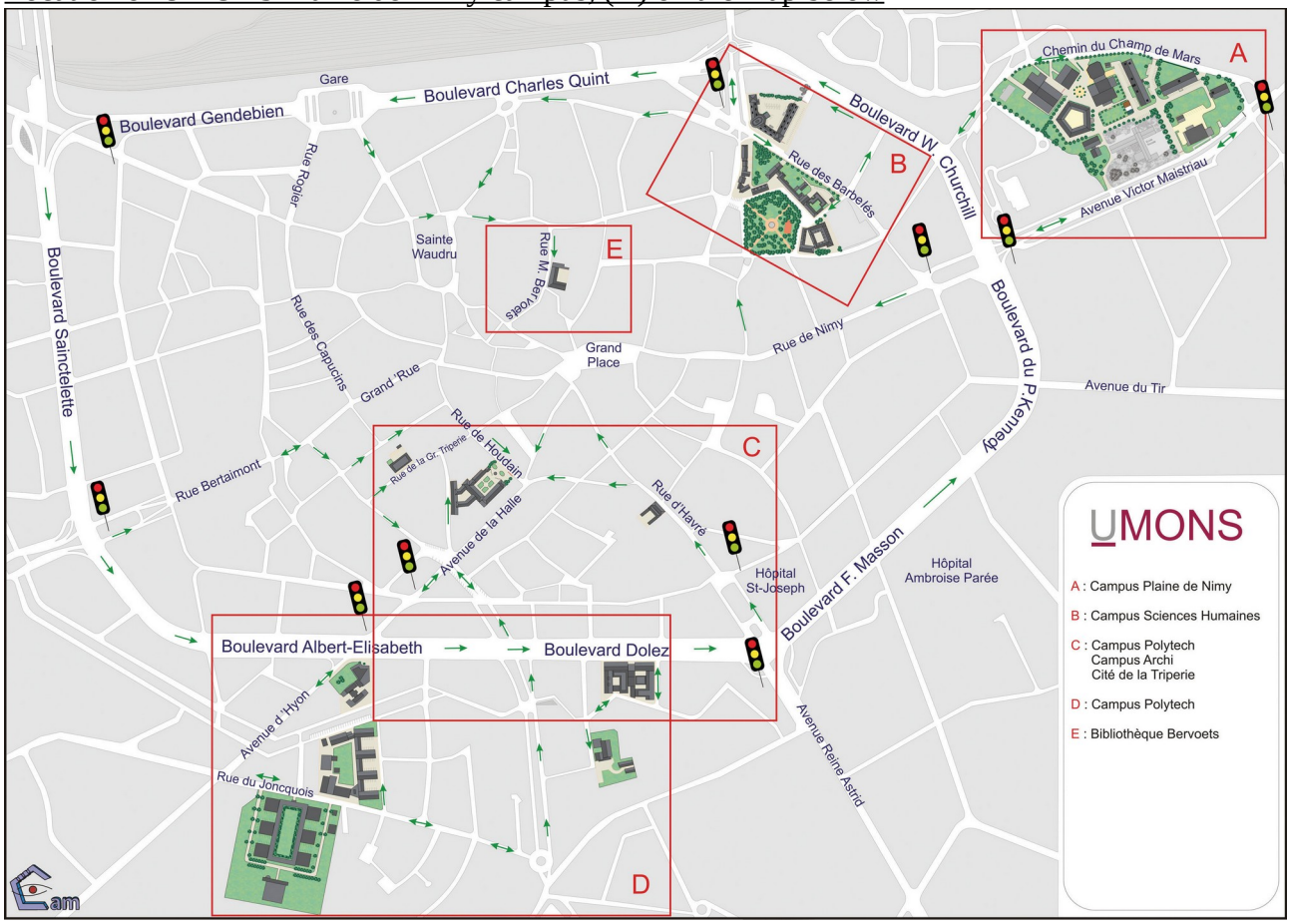
problems in real-world scenarios. Indeed, the goal of this thesis is to create a revolutionary SVS system that can process data from the camera sensor in real time while requiring the least amount of data and providing high precision when processing data that has occlusion issues.

- **MLOps for Edge deployment of a Real Time Danger Detection AI** (20 min)
  Mohamed BENKEDADRA (Polytech/ILIA)

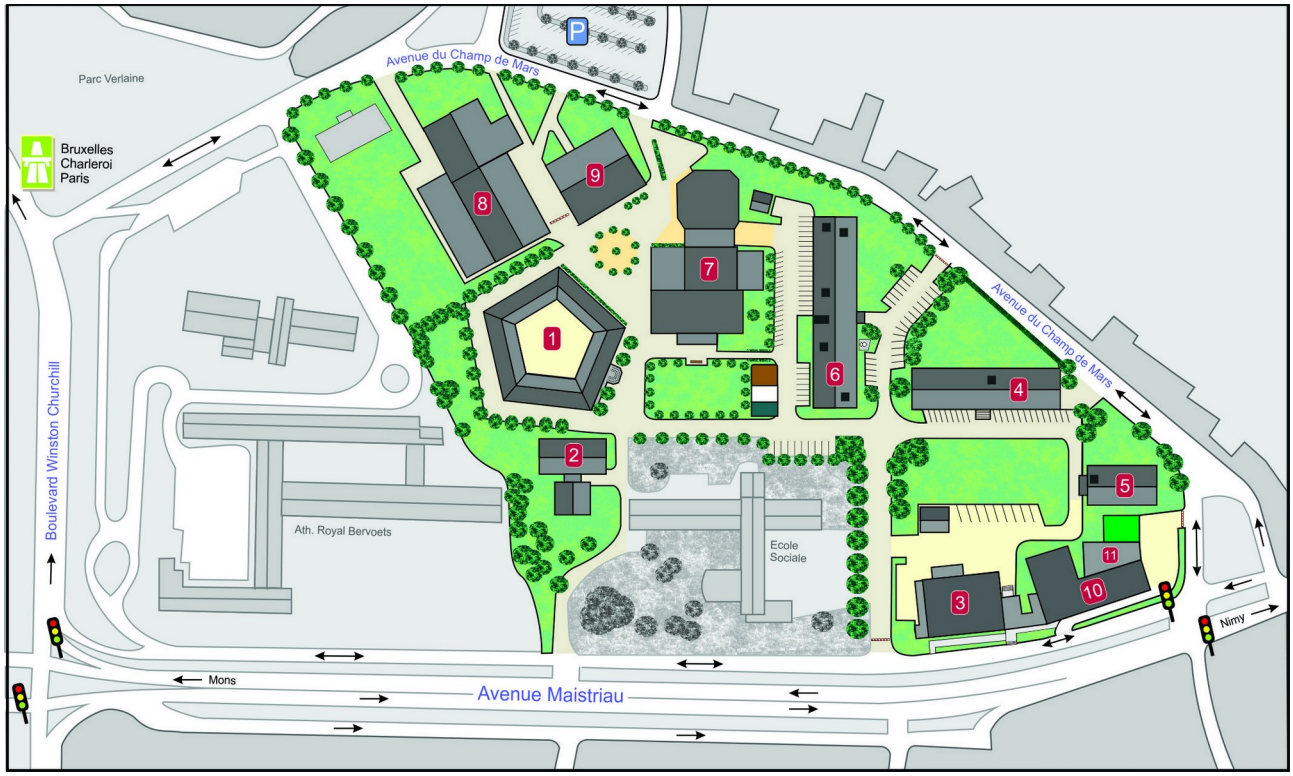
  Abstract: *Falls, Collisions, Electrocution, and other similar dangers are prominent in construction sites. Through a deep learning based computer vision system, we were able to detect some of these dangers in a real construction site. Through this presentation, we focus on the object detection/localization part of this system. For production environments, the development of a deployment solution is necessary. Hence, we go in depth into the MLOps pipeline that we developed to train, test, and deploy these object detection models. In addition, we present a recent study that we've done to optimize data acquisition, for the retraining of these models, to have auto adaptability and continuous improvement of the system through continuous learning. Finally, We will propose some future work that could lead to semi-auto generalization of the solution to other use cases through domain adaptation with Self-KD.*

16:35 Drink

Location of UMONS Plaine de Nimy campus, (A) on the map below



Location of the meeting room, **Mendeleïev/De Vinci** building, room Mirzakhani, (10) on the map below



Contact : Bruno Quoitin (bruno.quoitin@umons.ac.be, +32 65 373448)