Civil Security for Society, Increased Cybersecurity HORIZON-CL3-2023-CS-01-01: Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces), an Innovation Action.

About Óbuda University (https://bit.ly/ou-at-funding-and-tenders)

Óbuda University is an active player in the international scientific community, providing outstanding results in the fields of machine intelligence, cybersecurity, security of critical infrastructure, robotics, medical systems, intelligent systems, materials, and green technologies. ÓU has relations with more than 90 countries and has also signed 185 educational cooperation agreements. Moreover, ÓU is involved in 71 domestic and international research projects (more than 20 are EU-funded) and participates in 300 bilateral international programs. Besides nearly all EU Member States and countries associated to the Horizon programme, our international research partners include: Vietnam, Hong Kong, the UK and Australia. Furthermore, Óbuda University organizes and co-organizes around 15 international scientific conferences a year. It offers an exciting, up-to-date, student-friendly, creative and supportive environment for learning and research, with an emphasis on both basic and applied research, internationalization, green and sustainable development, research, innovation, lifelong learning and networking and cooperation with industry partners.

About our mission in cybersecurity

One of our major goals is to promote and support different aspects of cybersecurity at university level, as sooner or later companies, businesses and other institutions will need experienced and well-trained professionals, engineers and researchers in this field. In addition to teaching and establishing a theoretical background, we attach particular importance on cybersecurity research, development and innovation to provide practical techniques and methods for our students and partners. In the practice of teaching, we focus on developing a project approach, nurturing talent and encouraging research. To this end, we set up research groups with students, where they learn the challenges of research and development in a practical approach and experience teamwork.

In order to support cyber defence research, a "core" real/virtualised hybrid test network is continuously being developed within the university network, including a Security Operation Centre (SOC) and a Honeypot segment, complemented by additional intrusion detection, prevention and analysis solutions. The SOC is operated in a largely virtualised environment using open-source building blocks. Since cyber defence research (Honeypot and SOC optimization, attacker profiling, ditigal forensic, active deterrence, incident management) requires a large amount of log and traffic samples, we organize various cyber defence challenges and competitions (Capture the flag (CTF) and Attack/Defence competitions), which on the one hand provide excellent motivation and orientation of students towards cyber security, and on the other hand provide sufficient "realistic looking" simulated attack data for analysis and optimization.

About our laboratory

SOC R&D

One of our main research directions is the expansion and continuous development of our Security Operations Center (SOC), which is currently operating on campus and built with open-source tools. This will primarily involve optimisation based on log and monitoring data from SOC-connected devices, but we are also working on broader solutions for attack detection. In a general network, we will fine-tune devices used on the defence side, such as firewalls, intrusion prevention/intrusion detection, antivirus and others, by analysing data coming into the SOC, where appropriate using machine learning assisted methods. The result of the research is applied in

various research, development and consultancy projects to prepare the systems and human resource of our partners to be cyber resilient.

VSOC R&D

The rapid development of vehicle electronics in the last decades has led to the emergence of an increasing number of new electronically supported functions. The various control units no longer operate as autonomous devices, but together, using different communication protocols, have made it possible to build a vehicle electronics network. This continuous evolution also requires an increase in the reliability, data transfer rate and data volume of communication technologies. In addition, the connection of cars to the Internet places new demands on the protocols and networks used in the automotive industry. Our research aims at the security analysis of automotive electronic networks. We work together with large automotive companies in this direction to be sure that their products are cyber safe.

Honeypot R&D

In order to protect an organization's network infrastructure, a so-called Honeypot mechanism is often used to detect, prevent or in some way counteract attempts to unauthorized use of information systems. To this end, systems incorporating several honeypot functions and services are often used, rather than just a single honeypot server. These systems trap attackers, trying to attract attention by simulating real services and environments. The aim is to attract and divert the attacker's attention from the real network. The main goal of our research is to build a framework for measuring the effectiveness of honeypots and to optimize honeypots based on the metrics. The honeypot system built in our SOC-supported network is tested by means of Capture the Flag (CtF) contests advertised among students. Here we have embedded CtF challenges in honeypot services that students have to find in a given time interval.

Security analysis of 5G networks - 5G SOC development

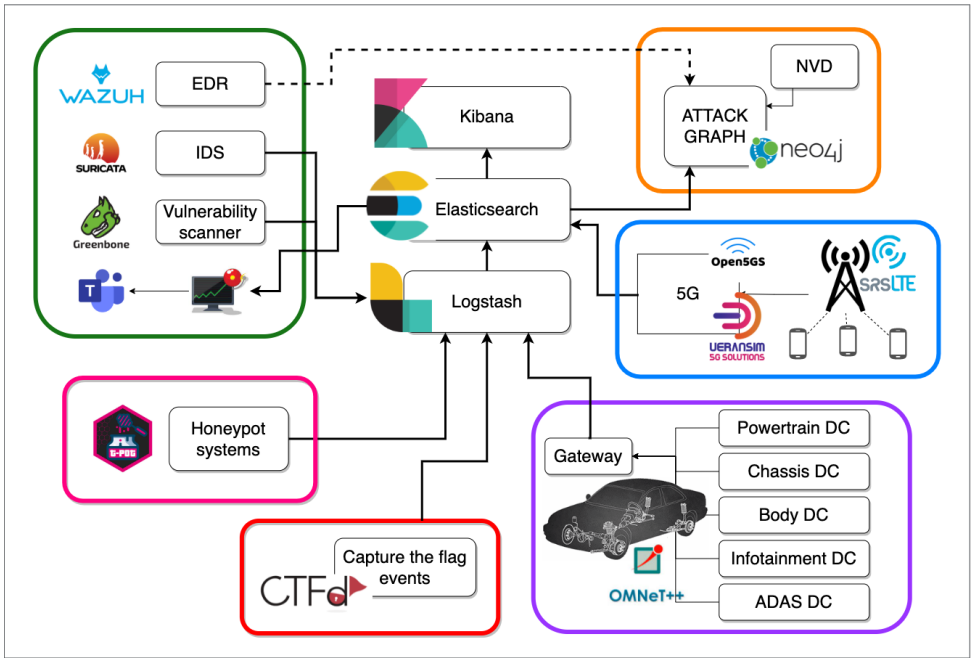
The new 5th generation of mobile communications offers us a lot of new opportunities. However, new technological achievements naturally bring with them many new security threats. The main objective of our research is the security analysis of the RAN interface of 5G networks in a dedicated 5G lab. The research will investigate potential vulnerabilities from both the offensive and defensive sides and will also aim at enabling network monitoring by setting up a dedicated Security Operations Centre (SOC) for 5G networks. A state-of-the art physical infrastructures are established in our university working together with operators and technology suppliers.

Investigating the applicability of attack graphs in SOC environments

Identification of vulnerabilities, security analysis and risk assessment, which are essential to identify and improve the security level of a network. It is also important for risk assessment to visualise the correlations between the attack actions that attackers can take. Tree structure-based or graph-based models are commonly used to represent attack paths. However, the use of these methods poses scalability problems and existing graph and tree generating applications usually have a very limited toolbox. The main thrust of our research is to implement an attack graph generator stored in a graph database that meets our own requirements, which will help to further optimize the functions supported by the SOC by scanning, analyzing and evaluating the data stored in our other research topics.

Our R&D references

We do work by using open-source toolkits to build up our SOC environment. The following figure shows the built up core architecture and the processes we operate on it.



Óbuda University SOC researches

Besides the computational infrastructure we do have two 5G research laboratories. One closed laboratory is dedicated to technology development. Here all tools can be found that are necessary for a modern communication laboratory. In our open laboratory, we use public frequencies of an operator in our research where the access points are installed on and in our building. In the open lab, the focus is on the applications.

Our proposed project aims to contribute to the achievement of some or all of the following outcomes as specified in the topic:

1. Tools to support cybersecurity resilience, preparedness, awareness, and detection within critical infrastructures and across supply chains;
2. Cloud infrastructures vulnerabilities mitigation;
3. Secure integration of untrusted IoT in trusted environments;
4. Use of Zero-Trust architectures;
5. Trust & Security for massive connected IoT ecosystems & lifecycle management;
6. Secure interoperability and integration of systems;
7. AI-based automation tools for cyber threat intelligence;
8. Secure infrastructure, secure Identities and usability for a security chain covering

We propose the following key areas of focus for our project:

1. Research and development of advanced cybersecurity technologies and tools especially using SOC environment.
2. Implementation of robust cybersecurity measures for critical digital infrastructures.
3. Promotion of cybersecurity awareness and best practices through training and education initiatives.
4. Collaboration with relevant stakeholders, including public authorities, industry partners, and academic institutions.
5. Integration of privacy and fundamental rights considerations into all project activities.

We are seeking partners with expertise in the following areas (but not limited to):

1. Cybersecurity research and development.
2. Digital infrastructure protection.
3. Privacy and fundamental rights in digital technologies.
4. Software and hardware security.
5. Certification and assurance frameworks.
6. Cybersecurity awareness and culture building.
7. Identification and analysis of regulatory aspects