



Department of Network Security and Internet Technologies

Head of department:
Ernő Rigo

Phone:
+36 1 279 6266

E-mail:
erno.rigo@sztaki.mta.hu

Address:
H-1111 Budapest, Lágymányosi u. 11.

Web:
hbit.sztaki.mta.hu/en

INTRODUCTION

Our department has a long history of development in the field of computer networking dating back to the 1970s. Over the last four decades, several generations of network architectures as well as software and hardware technologies have emerged, become widespread, some gradually have become obsolete and extinct. The world is preparing to enter an even more connected era with an unprecedented amount of users, devices, and information, all of which must be managed and secured.



MAIN R&D TOPICS

Main R&D topics:

- authentication and authorization infrastructures (Attribute Authorities, Identity Providers)
- management and security of cloud infrastructures (OpenStack, OpenNebula)
- network security supervisory systems, distributed network sensors
- automatic and assisted network monitoring, situation awareness
- special purpose network devices
- methods of IT security management and evaluation (CobIT, ISO27k, OWASP)
- network security incident handling and management

Challenges: While taking an active part in developing and employing new technologies, we have come to the conclusion that several basic problems in the area of systems management and information security seem to prevail. Our team focuses on the key R&D areas related to researching, evaluating, developing, and delivering advanced solutions with the ultimate aim of making Internet technologies more serviceable and networked systems more secure.

Solutions: We take a pragmatic approach to these challenges, researching factors and impacts of different solutions, policies, and processes. We carefully evaluate the alternative technologies, in our own test environments, assessing the integration capabilities of various components, and we carry out precisely planned measurements. This kind of research approach, sometimes called engineering science, leads to a deeper understanding of specific problems, which in turn provides a stable foundation for our planning, development, and service efforts.

Implementation: During implementation activities, benefits from our knowledge of emerging technologies become really effective as we combine them with agile development methodology. This way we achieve an early return on our effort and resources. Our approach is characterized by the continuous evaluation and improvement of our internal processes, products and services. We are keen users of open software, open hardware, and open protocols, but we also have extensive experience with industry leading products, technologies and environments.

HEXAA (www.hexaa.eu) successfully addresses the lack of trustful attribute problems in research and education federations. HEXAA is integrated into the world-wide identity federation of eduGAIN, and also the Hungarian eduID federation. HEXAA is tightly connected to existing collaboration task forces (REFEDs, GN3plus JRA3, GN4-P1, etc.).

Hun-CERT - The department operates Hun-CERT (www.cert.hu), one of the first domestic network incident handling centers for almost a decade. One of our top priorities is to achieve a more robust domestic network and to increase security-awareness of Hungarian Internet users.

- Council of Hungarian Internet Providers
- Metropolitan Ervin Szabó Library
- MATEHETSZ – www.tehetseg.hu
- MVM Paks Nuclear Power Plant
- GEANT
- BOSCH
- NIIFI
- MTMT

On average the staff comprises 15 individuals – most of them are certified IT specialists and engineers – with hands-on experience in current technologies. We take an emphasis on raising and employing new generations of IT professionals as well as relying on the experience of senior colleagues. Many of our colleagues hold relevant industrial certifications such as CCNA, CCNP, CISSP, CISA or CEH.

Data Diode - In the case of critical information infrastructures it is extremely important to prevent unauthorized data traffic. One of the possible methods is making two-way protocols "unidirectional", i.e. disabling data traffic in one direction. For this purpose, we developed a so-called "data diode". The device makes it possible to use common IT services (E-mail, FTP, HTTP, etc.), while on the physical level data flow is proven to be unidirectional.

ASTOR - Adaptive Security Tools for Operational Risk Mitigation. The research project produced a proof of concept toolset that performs automatic investigation of security/risk events occurring in companies and organizations, using adaptive, self-learning methods and resulting in better ratios of erroneous and/or missed alerts than any other methods currently in use.

DBpedia Spotlight Live makes it possible to analyze new articles from Wikipedia on-the-fly, and underlies an UIMA adapter and an OpenLibrary tool that are helping the Apache Stanbol project.

Net-Sensor - in the framework of a research project, an early warning system named "Network Security System for Protecting Critical Infrastructures" has been developed. This system is capable of analyzing data traffic of sub-networks under its supervision in real time, without disturbing normal data-flow. Based on the obtained data it can provide early warnings about the security status of the system.

