
The chair of IT security conducts research of new concepts, methods and technologies to increase security and trustworthiness of IT-based systems and applications. Research highlights encompass the development and testing of trustworthy and embedded platforms, the development of enhanced malware detection techniques with machine learning methods, the design and verification of new security protocols and security engineering.

Description
An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity. The most common classification is either in network (NIDS) or host-based (HIDS) intrusion detection systems, in reference to what is monitored by the IDS. Network based intrusion detection attempts to identify unauthorized, illicit, and anomalous behavior based solely on network traffic. A network IDS, using either a network tap, span port, or hub collects packets that traverse a given network. Using the captured data, the IDS system processes and flags any suspicious traffic. One approach to classify attacks is using anomaly detection method based on machine learning algorithms. The task given to student involves developing a platform/service by using existing machine learning algorithms to detect abnormal activities. Tasks include:

- Developing a benchmark service applying different ML algorithms for different datasets
- Detect anomalies specially in ICS (Industrial Control System) networks
- Analyze and deal with different NIDS datasets

Requirements
The student should have all mentioned requirements in his/her resume.

- Solid experience in Python programming language
- Familiar with machine learning
- Basic knowledge in network security

Contact
Mohammad Reza Norouzian
Technische Universität München
Chair for IT Security (I20)
Boltzmannstraße 3, 85748 Garching
Tel. + 49 89 289 18584
norouzian@sec.in.tum.de
www.sec.in.tum.de

Apostolis Zarras
Technische Universität München
Chair for IT Security (I20)
Boltzmannstraße 3, 85748 Garching
Tel. + 49 89 289 18567
zarras@sec.in.tum.de
www.sec.in.tum.de

Bruno Bierbaumer
Technische Universität München
Chair for IT Security (I20)
Boltzmannstraße 3, 85748 Garching
Tel. + 49 89 289 18580
bierbaumer@sec.in.tum.de
www.sec.in.tum.de