Trust Mechanisms for IoT Cybersecurity



The Internet of Things connects a large number of devices ranging from sensors and smart home devices to industrial systems. Many IoT devices operate with limited computational resources and therefore cannot support complex security mechanisms. As a result, compromised or malicious devices can threaten the security of the entire system.

Current approaches to IoT security rely on mechanisms such as authentication protocols, cryptographic protection, or centralized monitoring systems. However, these solutions are often difficult to deploy on resource-constrained devices or in highly distributed environments. Recent research has therefore explored trust management approaches that evaluate device behavior, reliability, and identity over time.

The goal of this thesis is to investigate mechanisms for establishing trust in IoT ecosystems composed of resource-constrained edge devices. Possible approaches include trust scoring, behavioral monitoring, lightweight identity management, or other techniques that help evaluate the reliability of devices. The student will study existing solutions and develop a prototype approach to demonstrate how trust can be established in constrained IoT environments.

Practicalities

Promotor:	Bart Preneel		
Daily supervisor:	Farhad Aghili	farhad.aghili@sirris.be	office Sirris-Heverlee
	Laurens Le Jeune	laurens.lejeune@sirris.be	office Sirris-Heverlee
	Roozbeh Sarenche	roozbeh.sarenche@kuleuven.be	office B01.13
Nature of the work:	30% literature, 35% theoretical work, 35% implementation		
Number of students:	1		

 © 2026 – 2027 COSIC