

PhD Student: Samuel Lindemer, RISE Cybersecurity Lab, Kista Stockholm <samuel.lindemer@ri.se>

Main Supervisor: Shahid Raza, RISE Cybersecurity

Title: Digital Certificate Revocation for the Internet of Things

Abstract:

Digital certificates have long been used for traditional Internet applications, and have now entered into widespread use for the Internet of Things. However, constrained devices currently have no means to verify the revocation status of certificates. Without the ability to revoke certificates, network administrators have no recourse in the event of a private key compromise. Our research in this area is part of our larger mission to enable fully featured public key infrastructures in the IoT. We aim to standardize a new protocol to solve this problem. Later, our research focus will shift to secure software updates for the IoT, which depend on digital certificates for code signing.

This work is done in collaboration with Uppsala University and is funded by the EU Horizon 2020 COCNCORDIA, a project that is building an EU cybersecurity center of excellence.