Application layer security for IoT

Joel Höglund and Shahid Raza

An overall trend for internet security is to offer solutions which allows more fine grained content protection. With application layer security built on top of the for IoT widely used CoAP standard, messages can traverse proxies while still offering true end-to-end security.
We are investigating how to bring application layer key establishment to IoT, and how to best combine it with mechanisms for key enrollment. Together with previous work with lightweight certificates, this has potential to further reduce the overhead needed for IoT devices to be part of a Public Key Infrastructure, and to become true first class citizens of the Internet.
The proposed solutions are developed in close alignment with ongoing standardisation efforts in the area, to improve the potential for industrial impact.
This work is partly funded by the SFS PhD program for Research Institutes.