



Jan Richter: Analysis of security mechanisms for resource constraint web enabled devices

Description

This Thesis deals with the Security of web enabled Sensor networks. The trend of ever shrinking computer devices enables engineers to equip household sensors and actuators like thermostats, smoke detectors and other household objects with communication capabilities. In this way the now interconnected devices can communicate with each other and even with the outside world. This also means that they are vulnerable to attacks and hence need a concept of security.

The thesis introduces a method, device profile for web services (DPWS), which defines how the communication between connected devices can be established. It will show how the standard methods of securing communication channels are leveraged in the DPWS communication scenario. The first part focuses on how capable very low power devices that implement these communication scenarios are. To show this an evaluation of a particular platform (the G2 from Microsystems) is done. The G2 is a very low power platform running on a SPARC V8 clocked at 44 MHz. The performance of this system is compared with other lower power platforms. While these evaluations yield the result that low power systems are capable to implement secure communication it also became obvious that in real time scenarios problems arise. The time which it will take to establish a secure channel is not practicable. The second focus point of the thesis is identifying improvement possibilities for the introduced security scheme and evaluating their potential. These improvement possibilities must be with the standard protocol framework the security scheme is implemented in. To fully understand, the protocols are broken down to their integral pieces. In that way the optimal configuration for interconnected devices is found and analyzed to draw conclusions on the potential of resource constrained devices.

Advisor

Univ.-Prof. Bernhard Rinner