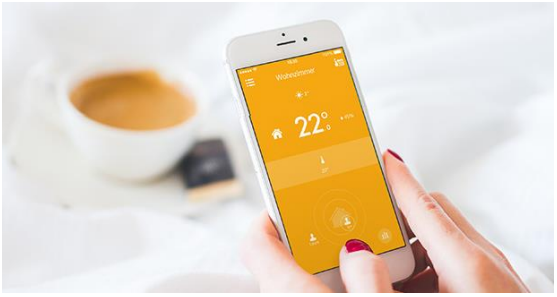
Intrusion Detection and Response in the Internet of Things

Background

Interconnecting embedded devices with the Internet leads to the so-called Internet of things. The Internet of things has many applications, such as smart homes, smart cities, precision agriculture, and Industrie 4.0. These applications will involve large numbers of wireless embedded devices that communicate with each other and remote hosts using IPv6.



Ad for the tado° thermostat

The security challenges in this area are diverse. On the one hand, IoT devices can be attacked from the Internet. On the other hand, IoT devices are often deployed outdoors in hostile environments and communicate wirelessly. Consequently, IoT devices require protection from both remote and local attackers. That said, many security issues persist.

Scope

In this project, we aim at exploring the possibility of validating Constrained Application Protocol (CoAP) traffic “en-route”. CoAP is an energy-efficient application layer protocol for the Internet of things. It recently reached RFC status and is becoming increasingly popular. Yet, current means of securing CoAP traffic, such as IPsec and DTLS, are insufficient. For example, a remote attacker can still send plenty of CoAP requests and thereby expend the limited energy reserves of IoT devices. A compromised IoT device, on the other hand, can, e.g., send private information to an attacker’s host on the Internet without any encryption. We conjecture that a trusted CoAP proxy can detect and prevent many of such attacks by validating CoAP traffic en-route.

Contact

Konrad-Felix Krentz, Dr. Feng Cheng, Prof. Dr. Christoph Meinel

Internet Technologies and Systems Group

Reading

http://coap.technology/