Security in the Internet of Things - Experiences from Use Cases

Dirk Stegemann (Bosch Sicherheitssysteme GmbH, Germany)
Jamshid Shokrollahi (Robert Bosch GmbH, Germany)

Internet of Things

The idea of the Internet of Things is to extend the Internet from a network of computers to a network of *things*, i.e., general smart objects with enhanced communication abilities. Or put another way, the Internet of Things enables embedded devices to behave and offer similar services as conventional internet nodes.
Among the many example applications that are being discussed for the Internet of Things, we choose to consider two particular use cases: Car-to-Car communication and building automation.

Car-to-Car Communication

Car-to-Car communication means to have moving vehicles exchange information among each other, e.g., in order to reduce energy consumption and to increase safety.
Similarly to truck drivers who exchange traffic information over CB radio, cars could submit traffic profiles for where they come from and request this information for where they are about to go, only with seamless integration into on-board systems and without any explicit driver interaction. But also real-time information about the brake assistant being triggered could be forwarded over short-range communication to successive vehicles to indicate a potential danger.

Building Automation

Building automation is commonly used as general term for systems that provide services to building users and its owners. Example domains include fire alarm systems, intrusion detection systems, heating / ventilation / air conditioning (HVAC) systems, as well as voice evacuation and public address systems. Devices in current building automation systems communicate mostly in wire-based closed circuits using proprietary protocols, and cross-domain interoperation has to be implemented with complex application layer gateways. Hence, introducing Internet of Things ideas to building automation would mean that each *thing* - be it an HVAC temperature controller, a smoke detector, or a loudspeaker - would be attached to an IP network and could interact with the systems that use it (and potentially the rest of the world) over standard protocols.

Security Implications

As the two use case examples already imply, the arrival of the Internet of Things means that systems will become more open to the potentially hostile outside, and purely communicating to *things*, which was hard or even impossible in conventional systems, will be almost trivial and difficult to prevent especially with standardized wireless communication. The attack surface will therefore inevitably become larger and increase the possibility of malicious attackers manipulating the system.
Moreover, the standardized IP-based communication between *things* makes it easier to move system logic, e.g., processing of sensor data, from the devices to external, potentially cloud-based computing resources. This shift will cause a lot more - ultimately personal - information to be floating around in and across systems. Hence, in addition to the general demand in distributed systems for confidential communication, authentication of communication partners and message integrity, the Internet of Things will require a suitable way of defining and establishing trust in the system, since personal information should not be revealed without the acknowledgement of the owners.

Limitations and possible Solutions

For interoperability as well as security reasons, it is good practice to rely on widely used security solutions like the AES block cipher and the SSL/TLS protocol whenever possible. However, several constraints for embedded *things* like little processing power, small memory, and long-term battery-powered operation prevent many standard mechanisms from being directly applicable. Therefore, costs and interoperability versus security trade-offs are needed, e.g., by resorting to special protocol options, hardware accelerators for specific cryptographic primitives, security proxies, and out-of-band mechanisms like tamper switches and application-layer plausibility checks.