Root of Trust in the Physical Internet

Keywords: *Root of Trust, Secure Firmware Update, Physical Internet, Internet of Things*

Contribution Form: Research Paper

Word count: 999

1. Building Trust in Physical Internet

Analogous to the Internet of computers whereas digital content is routed in a highly efficient way the Physical Internet (PI) aims to increase the efficiency of transportation of physical objects. Likewise a global system PI is „based on the interconnection of logistics networks by a standardized set of collaboration protocols, modular containers and smart interfaces" (Ballot et al., 2014, p. 23). The high order of collaboration requires a solid foundation of trust. This raises the question ‚How trust can be built in the Physical Internet?'.

Regarding the rapid expansion of the Internet to objects of our everyday life, the Internet-of-Things (IoT) closes the gap between the physical and the digital world (Mattern, 2010). Hence, the IoT is not only an enabling technology but an integral part of the PI (Montreuil, 2015). Breaking down to the smallest unit, smart tags, tiny, battery operated computers equipped with sensing, communication, data storage and processing capabilities connect the physical and the digital world.

The more capable the more vulnerable to attacks smart tags become. Once compromised a single smart tag can open criminals not only container padlocks but also grant them access to the higher level systems e.g. logistics information systems. In order to build trust in the PI, we propose a model to protect the ‚root tip' of IoT and PI, the smart tag firmware.

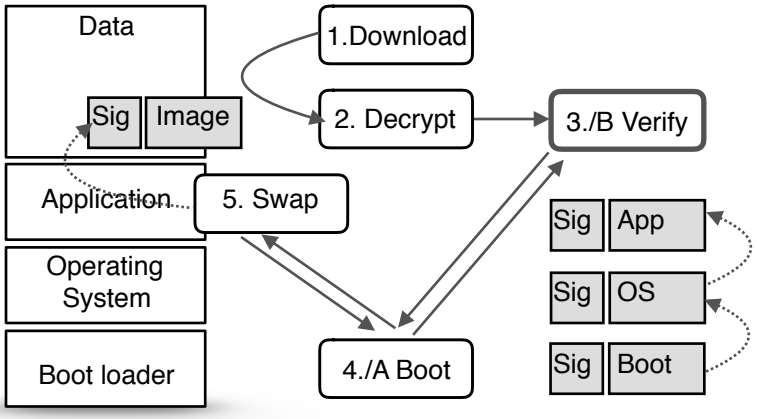
2. Root of trust and Secure Firmware Update

Root of Trust refers to a „system element that provides services, including verification of system, software and data integrity and confidentiality, and data (software and information) integrity attestation between other trusted devices in a system or network." (Casper, 2011). Computer systems are built of different levels of abstraction. Exemplarily shown in Figure 1 the boot loader in our model represents the lowest level a micro kernel booting the system and applying basic integrity checks. To enable a „chain of trust" the next higher level i.e. the operating system is verified (B) after powering and booting (A) the device. At the operating system level the integrity of the application is in turn verified (B) etc.

To keep smart tags up-to-date remote reprogramming or Over-The-Air firmware update is necessary. We propose a basic concept for a secure firmware update: The firmware image is

downloaded (1) and (2) decrypted before it is stored in the ‚update area', a predefined memory region reserved for firmware images or shared with temporary application data to save memory. The downloaded package includes the signature of the firmware image. The signature is verified (3) by the public key stored in a protected memory area. A boot flag is set. After the re-boot (4) the new and old firmware image is swapped (5) and the boot flag is cleared.

Figure 1: Memory Model and Basic Concept of Secure Firmware Update



Given the constraints in energy consumption, processing power and memory space, implementing secure firmware update is challenging. To investigate the performance of the proposed model we measured memory usage, run-time and power consumption of a prototype. We chose a typical processor core, i.e. ARM Cortex-M0+ processor with 256kB Flash and 32 kB RAM bonded to a IEEE 802.15.4 radio chip into a system on chip (SoC). Regarding the cryptographic signature verification we focus on Ecliptic Curve Digital Signature Algorithm (ECDSA).

3. Expected performance results

The evaluation setup is composed of typical smart tag nodes attached to mockups of PI container. To demonstrate the Internet Protocol based wireless connectivity the tags are connected to a 6LoWPAN standard router. Embedded into a real-life scenario the smart tag is programmed to continuously measure the temperature and humidity and reports significant changes to a device management server. As can be seen in Figure 1, the secure firmware update process relies on checking the integrity and authenticity of the (new) software. The cryptographic signature verification introduces not only a larger memory footprint but affect also the run-time as well as the power consumption consequently. Hence, we focus on the optimization of the ECDSA. We hypothesize that our model results only in a minor increase in resource usage.

Our findings will demonstrate the proof-of-concept of a lightweight concept of the RoT principle for the PI and the additional resources e.g. memory, power consumption needed. Furthermore we will clarify the additional life-cycle-costs of a prototypical smart tag comparing to a currently available smart tag without RoT and remote firmware update capabilities.

4. Contribution

Lack of trust and security is one of the biggest barrier for the global adoption of the PI and the IoT likewise. Only few references on how to build trust in the Physical Internet can be found. Building trust requires the safeguarding the integrity of data and software, especially on the smallest computational units of the PI; the smart tags. This research project focuses on a lightweight Root-of-Trust model. Furthermore the model takes the dynamic nature of the IoT and the PI into account and proposes a secure firmware update for smart tags. By measuring the performance on a low-cost hardware we proof the applicability and pave the way for trust in the Physical Internet.

References

Ballot, E., Montreuil, B., and Meller, R.D. (2014) The Physical Internet. Paris: Predit.

Montreuil, B., and Louchez, A. (2015) The Physical Internet Will Rest On The Internet Of Things. Manufacturing.Net

Mattern, F., and Floerkemeier, C. (2010) „From the internet of computers to the internet of things“, *From active data management to event-based systems and more:* pp. 242-259

Casper, W. D., and Papa, S. M. (2011) „Root of Trust“ *Encyclopedia of Cryptography and Security*, pp. 1057-1060