A Security Protocol Adaptation Layer for the IP-based Internet of Things

René Hummen, Tobias Heer, and Klaus Wehrle
Communication and Distributed Systems
RWTH Aachen University
Germany
{hummen,heer,wehrle}@cs.rwth-aachen.de

1 Introduction

The vision of the "Internet of Things" (IoT) is an opportunity to connect previously unconnected devices and currently isolated networks to today's Internet infrastructure. Recent efforts at the IETF and related standardization bodies aim at making IPv6 available to embedded, networked devices and corresponding networks [1] [2] [3]. These efforts are in parts driven by the goal of achieving a homogeneous interconnection between IoT networks among each other as well as with the Internet domain.

However, fundamental differences between the IoT domain and the Internet domain prevent an immediate deployment of existing IP-based protocols from a conceptual perspective. This is also true for existing IP-based security protocol suites [4] [5] [6] [7], where design decisions regarding the employed security mechanisms commonly depend on assumptions about network topology as well as device and network capabilities. Likewise, security protocols proposed for the wireless sensor network (WSN) domain are tailored to the respective use case and cater for specific computation, memory, and bandwidth limitations [8] [9] [10]. Thus, neither standard IP security solutions nor WSN security protocols fulfill the requirements of both domains and, therefore, do not lend themselves to establishing secure communication between the IoT domain and the Internet per se.

In this work, we outline where today's IP-based security protocols do not suffice to meet the requirements in the IoT domain. Furthermore, we present our conceptual ideas on how to enable secure communication between the IoT domain and the Internet by means of a security protocol adaptation layer.

2 Secure Interconnection between the IoT and Internet domains

The fundamental differences between the IoT domain and the Internet domain can be classified by the host and network capabilities as well as the respective network topology. Each dimension thereby shows challenges for standard IP security protocols to perform in the IoT domain:

1. *Device capabilities:* Internet hosts and IoT devices differ strongly regarding their available hardware resources. While Internet hosts are typically equipped with CPUs in the GHz range and several GBs of memory, embedded devices in the IoT domain are limited to CPUs in the MHz range and several KBs of memory. Recent IP security protocols cater for these differences of host capabilities by means of cryptographic agility concepts allowing for various ciphers for peer authentication. However, as the capabilities of a single Internet host compare to the capabilities of multiple IoT hosts, Internet hosts can mount attacks against IoT devices that are similarly effective to today's distributed Denial of Service attacks. DoS protection mechanisms built into standard IP security protocols do not mitigate this type of attack, as they often assume that individual hosts are equally powerful.

2. *Network capabilities:* The lossy communication channel, small packet sizes, and throughput in the order of tens of Kbit/sec for the IoT domain compare to a relatively reliable channel and high throughput the Internet. The lossy channel in the IoT scenario thereby demands for optimized protocol flows. Fate sharing of packet flights as implemented by (d)TLS is problematic, as the complete flights would need to be retransmitted in the likely event of packet loss. Additionally,

different MTU sizes make fragmentation likely for packets originating from the Internet domain. 6LowPAN compensates for this fact by handling packet fragmentation at its adaption layer. However, IP packet fragmentation enables malicious Internet hosts to fill up the limited buffer space of IoT hosts with invalid IP fragments by sending merely a few large packets. This is due to the fact that IP security protocols commonly calculate integrity checksums and signatures over whole packets instead of over intermediate fragments. Hence, the validity of fragmented packets cannot be verified before packet re-assembly.

3. *Network topology:* IoT networks denote wireless multi-hop routing structures, whereas the Internet backbone is wired and ISP-centered. The cooperative routing topology of IoT networks in combination with the higher bandwidth available to Internet host allows to not only target single IoT devices, but whole IoT networks with DoS attacks. As today's IP security protocols focus on end-to-end mechanisms, they do not defend against this type of attack that would need to stopped at the IoT ingress point.

The above issues show that IP security solutions do not cater immediately to a secure interconnection of IoT networks and the Internet. We now present an adaptation layer-based approach to enabling security bootstrapping between the IoT domain and the Internet with existing IP security protocols.

2.1 A security protocol adaptation layer

To overcome the resulting security issues when connecting IoT networks to the Internet, we argue that an adaptation layer for IP security protocols is necessary. This adaptation layer follows a concept similar to the 6LowPAN adaptation layer for IPv6 by allowing for domain-specific protocol variants. Furthermore, gateways that connect different domains can translate between a standard IP security protocol and its domain-specific protocol variants.

In its simplest form, the adaptation layer consists of a security offloading functionality at the gateway that terminates security associations with Internet peers. This either allows to use unprotected packet delivery within a trusted IoT network or it enables using specific security mechanisms and protocols in the IoT domain that are tailored to the capabilities and network topology. However, in cases where communicating peers do not trust the gateway, it is essential that end-to-end security associations between the peers are not terminated at the gateway. Thus, the adaptation layer must preserve end-to-end security mechanisms at the gateway as it translates between protocol variants of the interconnected domains.

In the latter case, the adaptation layer needs to i) allow for domain-specific on-the-wire packet structures and packet flows, ii) enable intermediate gateways to efficiently translate between different wire formats, and iii) afford the extension of selected security mechanisms (i.e., for adequate DoS protection). As an example, such an adaptation layer can partly be realized by defining a canonical packet format that is used by the communicating end-hosts to apply end-to-end security mechanisms (e.g., integrity checksums and signatures). End-hosts may afterwards compress the canonical format, e.g., by applying statefull or stateless compression techniques in order to translate the canonical format into an optimized on-the-wire format and packet flow for a given network (see Figure 1). As translation operations must keep

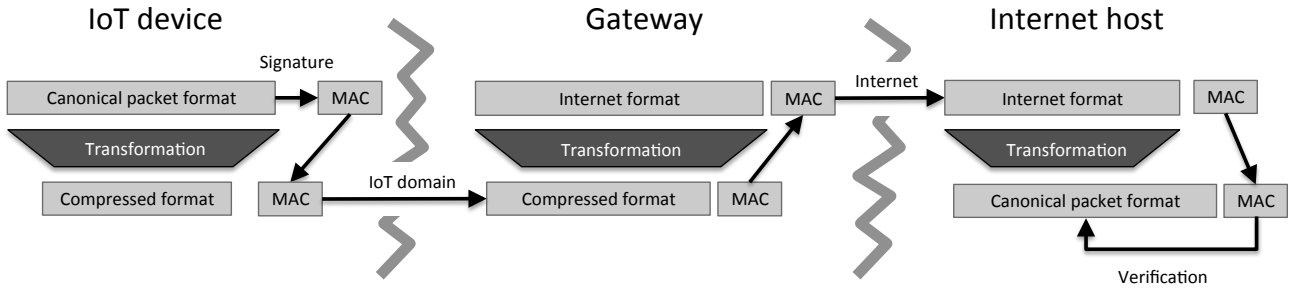

Figure 1: Translation between the canonical packet format and the respective wire formats.

the canonical format intact, a gateway can then re-build the original packet content from a received optimized packet flow and translate it to the wire format of the neighboring domain. Furthermore, end-hosts and gateways may opt for adding or remove additional information during the translation step facilitating domain-specific security mechanisms such as DoS protection. Likewise, gateways may support IoT devices by carrying over computationally expensive tasks in the canonical format and adding the computed information to the translated packet flow.

3 Conclusion

In this work, we outlined that the differences between the IoT and the Internet create new attack vectors against IoT hosts that are not mitigated by employing today's standard IP security solutions. Specifically, we argue that IP security suites do not meet the exact security requirements in the dimensions host capabilities, network capabilities, and network topology. We think that a security protocol adaptation layer is a viable approach for enabling IP-based security protocols within the IoT domain as well as for the interconnection between the IoT and the Internet domain. As briefly indicated, this adaptation layer may come in different shapes and may be implemented in a variety of ways. Hence, we strongly believe that research in this area is essential to further improve bridging the gap between the IoT and the Internet.

References

[1] T. Winter, P. Thubert, A. Brandt, T. Clausen, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, and JP. Vasseur. RPL: IPv6 Routing Protocol for Low power and Lossy Networks. draft-ietf-roll-rpl-18 (Internet Draft), February 2011.

[2] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC 4944 (Proposed Standard), September 2007.

[3] Z. Shelby, K. Hartke, C. Bormann, and B. Frank. Constrained Application Protocol (CoAP). draft-ietf-core-coap-04 (Internet Draft), January 2011.

[4] C. Kaufman. Internet Key Exchange (IKEv2) Protocol. RFC 4306 (Proposed Standard), December 2005.

[5] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246 (Proposed Standard), August 2008.

[6] E. Rescorla and N. Modadugu. Datagram Transport Layer Security. RFC 4347 (Proposed Standard), April 2006.

[7] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson. Host Identity Protocol. RFC 5201 (Experimental), April 2008.

[8] Perrig A, R. Szewczyk, J. Tygar, V. Wen, and D. Culler. SPINS: Security Protocols for Sensor Networks. *Wireless Networks*, September 2002.

[9] L. Eschenauer and V. Gligor. A key-management scheme for distributed sensor networks. In *CCS '02: Proceedings of the 9th ACM conference on Computer and communications security*, 2002.

[10] C. Karlof, N. Sastry, and D. Wagner. TinySec: A link layer security architecture for wireless sensor networks. In *SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems*, 2004.