Standards-based End-to-End IP Security for the Internet of Things

René Hummen, Klaus Wehrle
Communication and Distributed Systems, RWTH Aachen University, Germany
Email: {hummen, wehrle}@comsys.rwth-aachen.de

***Abstract*—Peer authentication and secure data transmission are vital aspects for many scenarios in the IP-based Internet of Things (IoT). To enable end-to-end security, recent research and standardization efforts focus on a number of IP security protocol variants for the IoT, most notably Datagram TLS (DTLS), the HIP Diet EXchange (DEX), and minimal IKEv2. In this dissertation outline, we present the main motivation for employing these protocol variants in constrained network environments and discuss the need to surpass the status quo. Most importantly, we highlight our identified challenges when employing these protocol variants in constrained network environments and provide a high-level overview of our previously proposed approaches to counteract the identified design-level protocol issues.**

I. Introduction

Organizations such as ETSI, the IETF, and the ZigBee Alliance undertake tremendous efforts towards standardizing IP technology and application layer protocols for the interconnection of constrained devices and services in the Internet of Things (IoT). Notably, these standardization efforts enable end-to-end addressability, abstraction from device and network constraints, and universal interoperability at the protocol level. Network scenarios destined to benefit from the resulting standards range from small-scale home automation solutions to large-scale industrial control systems and smart cities.

In many of these scenarios, sensed information and actuation commands traverse untrusted networks, e.g., when exchanging information between constrained devices and Cloud services via the Internet. The protection of sensitive information thereby cannot only rely on network-specific security measures within the individual constrained network domains. Instead, sensitive information must be protected in an interoperable end-to-end manner to prevent information leakage or the execution of harmful actuation tasks. To this end, IP technology on constrained devices allows to reuse standard security solutions of traditional IP networks. However, these solutions do not specifically consider the limited computation, memory, and energy resources of constrained devices as well as the small packet size and lossy link characteristics of constrained networks in their protocol design. Thus, research and standardization recently shifted their focus to more lightweight variants of existing IP security protocols. These most notably include DTLS [1], the HIP DEX [2], and minimal IKEv2 [3].

Although the proposed protocol variants aim at adapting existing IP security solutions to the special requirements of constrained network environments, most efforts are currently limited to specifying minimal protocol profiles [3], [4]. These profiles define a reduced set of required protocol functionality and give recommendations for the selection of cryptographic primitives. However, while profiles allow to minimize protocol complexity and thus code size as an important applicability metric for constrained devices, the current approaches are still conservative in nature. In fact, HIP DEX proposes the most radical adjustments by introducing an aggressive retransmission mechanism for the increased packet loss in constrained network environments compared to traditional IP networks. This retransmission mechanism requires one communication end-point to continually send a handshake packet at short time intervals until it receives the corresponding response from its peer. We believe there is the need to go beyond mere protocol profiling and the use of blunt force to achieve standards-based end-to-end IP security that is suitable for the IoT.

978-1-4799-1270-4/13/$31.00

In our dissertation work, we therefore ask ourselves the following three high-level research questions regarding the *applicability of the proposed security protocol variants for constrained network environments*:

1) The adaptations of these protocols are currently restricted to a limited set of measures. Hence, can we identify necessary refinements that further tailor these protocols to the new requirements of constrained network environments?
2) IoT scenarios often involve economies of scale and downscaling of hardware resources to reduce cost. Still, can we enable the full potential of the proposed protocol variants for *tightly* constrained devices that have insufficient resources for a complete protocol implementation?
3) Layer separation and fragmentation allow to abstract from specific network characteristics at the security protocol layer. Thus, do adverse side-effects exist when deploying the protocol variants in constrained environments?

In this dissertation outline, we highlight the main results of our research and provide answers to the above questions.

II. Prerequisites

We now present the main assumptions for the abstract network scenario that is in focus of our work and briefly outline the methodology along which we conduct our research.

A. Network Scenario

As depicted in Fig. 1, the network scenario consists of constrained devices in an IoT domain, services that are located in a local network or the Internet, and gateways that interconnect these network domains. Constrained devices are assumed to communicate over constrained network links, e.g., based on IEEE 802.15.4. Moreover, we assume that constrained devices

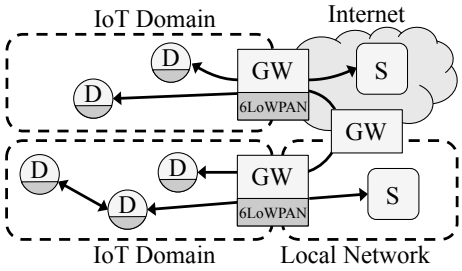

Fig. 1: Constrained devices (D) communicate with each other and with local or Internet-based services (S) via a gateway (GW). Entities belonging to an IoT domain are equipped with the 6LoWPAN layer. Arrows indicate forwarding paths for specific protocol handshakes.

are IP-enabled and equipped with 6LoWPAN [5], an IETF-standardized IPv6 adaptation layer for constrained network environments. The gateway is connected to the local network or the Internet via a commodity broadband connection.

Concerning device resources, we assume that constrained devices are equipped with only a few MHz of computation power, several kilobytes of RAM and several *tens* of kilobytes of ROM. Furthermore, these devices may be battery-powered. Gateways and services, on the contrary, run on common wall-powered network and server hardware, respectively.

B. Research Methodology

Regarding our research methodology, we started with a theoretical protocol analysis for each of our three high-level research questions. We then formulated hypotheses for ourselves about the protocol behavior in constrained network environments, i.e., with device and network constraints in mind. We confirmed these hypotheses with real-world experiments, thus substantiating the identified protocol design issues. Based on these results, we then proposed approaches to counteract the identified design-level protocol issues. One of the main goals in developing our proposed approaches thereby was to remain interoperable and standard-compliant.

III. Identified Challenges and Proposed Approaches

We now outline the main results of our dissertation work. Specifically, we briefly present our identified protocol issues and highlight the central ideas of our proposed approaches. We conclude the presentation of each approach with an indication of our chief evaluation results. Sections III-A and III-B thereby target our first research question, whereas Section III-C and Section III-D give answers to our second and third research question, respectively. For detailed information and a comprehensive discussion of related work, we refer the interested reader to our corresponding publications [6]–[9].

A. Tailoring Protocol Mechanisms

DTLS, HIP DEX, and minimal IKEv2 consider public-key cryptography in their protocol design for peer authentication and key agreement. More precisely, while DTLS optionally defines a symmetric key-based handshake, HIP DEX and minimal IKEv2 mandate the use of public-key-based primitives.

We identified three main challenges that directly stem from the use of public-key cryptography. First, public-key operations involve a considerable amount of transmissions and computation time. As a result, constrained devices are unable to perform other tasks, e.g., packet forwarding, while the CPU is busy computing cryptographic operations. Second, already a *single* adversary can exploit these expensive operations on a constrained device, e.g., with multiple handshakes in short succession. Existing DoS protection mechanisms of IP security protocols do not suffice to defend against such attacks [10]. Third, retransmissions of handshake packets are commonly based on fixed timeouts. Consequently, these approaches do not account for the varying packet processing times and cause spurious retransmissions or delayed handshake conclusion. To thwart these issues, we proposed three lightweight protocol extensions. We thereby focused on HIP DEX, but also showed that our extensions generalize to DTLS and minimal IKEv2.

Specifically, we presented a novel *session resumption mechanism* for HIP DEX that is inspired by similar mechanisms for TLS [11] and IKEv2 [12]. Notably, our mechanism functionally extends on related work and focuses on the reduction of the memory requirements for inactive sessions and of radio transmissions during session resumption.

Moreover, we promoted the *puzzle-based DoS protection mechanism* of HIP DEX for all proposed protocol variants and tailored this mechanism to constrained network environments. Particularly, we proposed a simple attack detection and puzzle difficulty selection strategy based on a sliding window. We further introduced a protocol extension that enables an on-path gateway to collaborate in the puzzle difficulty selection to account for device and network heterogeneity.

To take the varying processing times of handshake packets into account, we proposed an *adaptive retransmission mechanism* that employs multiple worst-case estimates for the retransmission timeout. More precisely, retransmissions of packets triggering only inexpensive operations at the peer are based on a network delay-based timeout, whereas expensive handshake packets also employ a processing-based timeout.

Our evaluation confirmed that our proposed session resumption mechanism substantially reduces the computation, memory, and transmission overhead of the standard protocol. Moreover, our collaborative puzzle-based DoS protection mechanism accounts for device and network heterogeneity and successfully defends constrained devices against unconstrained adversaries. Likewise, our refined retransmission mechanism affords a timely handshake conclusion despite packet loss.

B. Adapting the Packet Format

Minimal IKEv2 and HIP DEX feature a concise four-way protocol handshake. This stands in stark contrast to the DTLS handshake that requires 6 round-trips and up to 15 packets. Still, minimal IKEv2 and HIP DEX achieve their conciseness at the cost of larger packet sizes, thus commonly causing packet fragmentation. Packet fragmentation in turn leads to an increased loss probability for the entire packet as the loss of a single fragment results in the loss of the complete packet.

We focused our protocol analysis on HIP DEX and identified expendable information in its packet structure. While often useful in the scope of Internet-based communication, the transmission of this information is undesirable in constrained network environments. To remove the identified redundancies

in the packet before transmission, we proposed the *Slimfit compression layer* for HIP DEX. As its main building blocks, Slimfit i) removes static packet content defined in the protocol specification, ii) modifies the packet structure to increase the compression efficiency, and iii) introduces an evolvable compression scheme for cipher suite negotiation parameters.

Our evaluation showed that Slimfit perceivably decreases retransmissions and even slightly *reduces* the HIP DEX handshake processing overhead. Notably, the 2.5kB ROM overhead is the only tradeoff for the transmission and computation gains.

C. Delegating the Session Establishment

The proposed protocol variants often exceed the available memory resources of tightly constrained devices such as Tmote Sky motes that are equipped with 48 kB of ROM and 10 kB of RAM. The total overhead of Contiki OS including our public-key-enabled DTLS implementation, for example, amounts to about 75 kB of ROM and to just below 12 kB of RAM.

To still enable public-key-based peer authentication in inter-domain scenarios, we proposed a *handshake delegation architecture*. Our delegation architecture is based on the fact that peers store session state across connections for session resumption. This enables a trusted entity such as the device owner to perform a public-key-based handshake on behalf of the constrained device. Subsequently, the trusted entity securely transfers the session resumption state that was established during the initial handshake to the constrained device via a secure channel. The constrained device then utilizes this session state in an abbreviated session resumption handshake that does not require public-key operations.

Our delegation architecture unburdens the constrained device from all public-key-related overheads and most DTLS handshake complexities. Still, as a tradeoff, the transitive security of our approach is weaker than the security properties of DTLS without our architecture. A detailed evaluation and overhead analysis remain as the last open item of our work.

D. Securing Packet Fragmentation

When deploying DTLS, HIP DEX, or minimal IKEv2 in constrained network environments, handshake packets belonging to these protocols commonly exceed the maximum frame size of the employed link layer technologies. In case of link layer-protected IEEE 802.15.4 frames, e.g., handshake packets larger than 42 byte at the security protocol level typically trigger fragmentation at the 6LoWPAN [5] layer.

An adversary, who is located inside the IoT domain, can exploit this fragmentation mechanism by sending a duplicate fragment with altered payload in reaction to an overheard legitimate fragment. The fragment recipient then is unable to distinguish the forged fragment from the legitimate one due to the lack of per-fragment authentication. As a result, an eavesdropping adversary can prevent the successful reassembly of handshake packets at the cost of a single duplicate fragment.

Moreover, a reassembling node has to optimistically store packet fragments and rely on a timeout mechanism to discard incomplete packets. As a result, an adversary can occupy the scarce buffer memory of a target node by sending an incomplete fragmented packet. This malicious buffer reservation enables the adversary to block the processing of fragmented handshake packets by periodically sending a single fragment.

To defend against these fragmentation attacks, we proposed lightweight security mechanisms at the 6LoWPAN layer. Our *content-chaining scheme* provides efficient per-fragment authentication by cryptographically binding the content of a packet to its first fragment via a hash chain construction. Our *split buffer approach* segments the reassembly buffer into fragment-sized buffer slots. This segmentation enables the processing of fragmented packets despite an adversary who partially occupies the reassembly buffer at a target node. We extended this split buffer with a *packet discard strategy* that disposes of packets with suspicious sending behavior.

Our evaluation confirmed the existence of the identified attacks and showed that our proposed mechanisms mitigate these at moderate computation, memory, and transmission cost.

IV. Conclusion

In this dissertation outline[1], we motivated the need for standards-based IP security in the IoT. During our research, we uncovered important design-level protocol issues when employing the currently considered IP security protocol variants in constrained network environments. Our proposed approaches counteract these issues in an efficient and protocol-compliant manner, and thus significantly improve the applicability of these protocol variants for constrained environments. We are currently in the process of disseminating our proposed approaches at the IETF and hope that our research results have a positive impact on future standards in our research domain.

References

[1] E. Rescorla and N. Modadugu, "Datagram Transport Layer Security Version 1.2," RFC 6347, IETF, IETF, 2012.

[2] R. Moskowitz, "HIP Diet EXchange (DEX)," draft-moskowitz-hip-dex-00 (WiP), IETF, 2012.

[3] T. Kivinen, "Minimal IKEv2," draft-kivinen-ipsecme-ikev2-minimal-01 (WiP), IETF, 2012.

[4] S. Keoh, S. Kumar, and Z. Shelby, "Profiling of DTLS for CoAP-based IoT Applications," draft-keoh-dtls-profile-iot-00 (WiP), IETF, 2013.

[5] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks," RFC 4944, IETF, 2007.

[6] R. Hummen, H. Wirtz, J. H. Ziegeldorf, J. Hiller, and K. Wehrle, "Tailoring End-to-End IP Security Protocols to the Internet of Things," in *Proc. of IEEE ICNP*, 2013.

[7] R. Hummen, J. Hiller, M. Henze, and K. Wehrle, "Slimfit - A HIP DEX Compression Layer for the IP-based Internet of Things," in *Proc. of IEEE WiMob 2013 Workshop IoT*, 2013.

[8] R. Hummen, J. H. Ziegeldorf, H. Shafagh, S. Raza, and K. Wehrle, "Towards Viable Certificate-based Authentication for the Web of Things," in *Proc. of ACM HotWiSec*, 2013.

[9] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, and K. Wehrle, "6LoWPAN Fragmentation Attacks and Mitigation Mechanisms," in *Proc. of ACM WiSec*, 2013.

[10] K. Hartke and O. Bergmann, "Datagram Transport Layer Security in Constrained Environments," draft-hartke-core-codtls-02 (WiP), IETF, 2012.

[11] J. Salowey et. al., "Transport Layer Security (TLS) Session Resumption without Server-Side State," RFC 5077, IETF, 2008.

[12] Y. Sheffer and H. Tschofenig, "Internet Key Exchange Protocol Version 2 (IKEv2) Session Resumption," RFC 5723, IETF, 2010.

[1]This research is funded by the DFG Cluster of Excellence on Ultra High-Speed Mobile Information and Communication (UMIC).