Resource-Conscious Network Security for the IP-Based Internet of Things

Von der Fakultät für Mathematik, Informatik und Naturwissenschaften der RWTH Aachen University zur Erlangung des akademischen Grades eines Doktors der Naturwissenschaften genehmigte Dissertation

vorgelegt von

Diplom-Informatiker

René Hummen

aus Aachen, Deutschland

Berichter:

Prof. Dr.-Ing. Klaus Wehrle
Prof., Ph.D. Thiemo Voigt

Tag der mündlichen Prüfung: 02.06.2015

Reports on Communications and Distributed Systems

edited by
Prof. Dr.-Ing. Klaus Wehrle
Communication and Distributed Systems,
RWTH Aachen University

Volume 11

René Hummen

Resource-Conscious Network Security for the IP-Based Internet of Things

Shaker Verlag
Aachen 2015

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Zugl.: D 82 (Diss. RWTH Aachen University, 2015)

Printed in Germany.

ISBN 978-3-8440-3755-5
ISSN 2191-0863

Shaker Verlag GmbH • P.O. BOX 101818 • D-52018 Aachen
Phone: 0049/2407/9596-0 • Telefax: 0049/2407/9596-9
Internet: www.shaker.de • e-mail: info@shaker.de

Abstract

The Internet of Things (IoT) envisions an unprecedented interleaving of the physical with the virtual world to enhance automation and to improve comfort in a variety of application domains ranging from home automation to healthcare and smart cities. Based on recent advances in standardization, many of these application domains are expected to employ IP-enabled embedded devices to realize the envisioned interconnection of the physical world. Such IP connectivity, however, also exposes networked embedded devices to similar network attacks as conventional IP-enabled hosts or services. The severity of these attacks is considerably aggravated in the IoT as attacks in the virtual world suddenly can have detrimental physical impact. Hence, effective network security is a vital precondition for a secure IP-based IoT.

Standard end-to-end security protocols such as TLS have the potential to provide an important building block for interoperable network security in the IoT. The device and network constraints in the embedded domain and the resource asymmetry in the IoT, however, challenge the design of existing security solutions. The resource constraints of embedded devices, e.g., require these solutions to be applicable in the context of only a few MHz of computational power, several kB of RAM, and several tens of kB of ROM. Similarly, energy constraints and low-power wireless communication demand for a high transmission efficiency. Research and standardization, thus, recently started to adapt standard IP security solutions to IoT requirements.

In this thesis, we contribute to these adaptation efforts by addressing emerging protocol design challenges for end-to-end IP security in the context of the IoT. In this, we specifically consider the IoT security protocol adaptations DTLS, HIP DEX, and Minimal IKEv2 that are currently proposed for standardization at the IETF. Notably, while these protocol adaptations should already satisfy IoT requirements, we identify several design-level efficiency and security issues that render the deployment of these protocols in their current state inefficient, infeasible, and even insecure.

First, the high computation overhead of DTLS, HIP DEX, and Minimal IKEv2 significantly hampers the availability and response time of networked embedded devices during the protocol handshake. We present three complementary protocol extensions that account for these computation overheads in the overall protocol design. Second, the extensive message wire-format of these protocol adaptations leads to undesirable transmission overheads in the embedded domain. We devise the Slimfit compression layer that addresses message conciseness issues in the context of HIP DEX. Combined, these two contributions considerably reduce the run-time overheads and improve the security properties of the considered end-to-end security protocols.

Third, extensive RAM and ROM requirements render the use of DTLS, HIP DEX, and Minimal IKEv2 infeasible for a wide range of memory-constrained embedded devices. To still enable these devices to communicate securely, we introduce the handshake delegation architecture that also provides an authorization framework for the embedded domain. Fourth, the 6LoWPAN packet fragmentation of the DTLS, HIP DEX, and Minimal IKEv2 handshake messages is vulnerable to DoS attacks. To protect against these attacks, we present two lightweight defense mechanisms.

Overall, our contributions in this thesis effectively complement each other and, in combination, achieve significant security and efficiency improvements for the considered standard end-to-end security protocols in the context of the IP-based IoT.

Kurzfassung

Die Vision des Internets der Dinge ist eine bisher unerreichte Vernetzung der physischen mit der virtuellen Welt. Hiervon sollen zum Beispiel die Hausautomatisierung aber auch neuartige Anwendungsbereiche wie die intelligente Stadt profitieren. Aktuelle Fortschritte bei der Standardisierung deuten dabei auf einen verstärkten Einsatz von IP-fähigen eingebetteten Systemen hin. Die einhergehende Erreichbarkeit macht vernetzte „Dinge“ jedoch ähnlich wie herkömmliche Rechner und Dienste über das Netzwerk angreifbar. Effektive Sicherheitslösungen sind daher eine wesentliche Voraussetzung für die sichere Vernetzung der physischen mit der virtuellen Welt.

Standardprotokolle für die Ende-zu-Ende-Sicherheit wie TLS haben das Potenzial einen wichtigen Bestandteil für diese sichere Vernetzung zu liefern. Die Geräte- und Netzwerkbeschränkungen im Bereich der eingebetteten Systeme sowie die Ressourcen-Asymmetrie im Internet der Dinge stellen bestehende Sicherheitslösungen jedoch vor enorme Herausforderungen. So setzen die knappen Ressourcen eingebetteter Systeme voraus, dass Lösungen bei stark beschränkter Rechenleistung und begrenztem Speicherplatz einsetzbar sind. Ebenso erfordern Energiebeschränkungen eine hohe Verarbeitungs- und Übertragungseffizienz. Daher müssen existierende Sicherheitslösungen an die speziellen Anforderungen im Internet der Dinge angepasst werden.

Diese Arbeit adressiert grundlegende Herausforderungen beim Entwurf von Ende-zu-Ende-IP-Sicherheitsprotokollen im Internet der Dinge. Hierbei liegt der Fokus auf den Protokollanpassungen DTLS, HIP DEX und Minimal IKEv2. Während diese Lösungen bereits den Anforderungen des Internets der Dinge genügen sollten, identifiziert diese Arbeit diverse Effizienz- und Sicherheitsfragen, die den Einsatz dieser Protokollanpassungen ineffizient, unmöglich, oder gar unsicher machen. Um diesen Problemstellungen zu begegnen, umfasst diese Arbeit insgesamt vier Beiträge.

Die durchgeführten Protokollanalysen zeigen, dass der erhebliche Berechnungsaufwand während der Protokollaushandlung die Verfügbarkeit und die Antwortzeit von eingebetteten Systemen deutlich beeinträchtigt. Der erste Beitrag besteht daher aus Protokollerweiterungen, die eine Berücksichtigung dieser Berechnungskosten ermöglichen. Darüber hinaus deuten die Analyseergebnisse auf umfangreiche Kompressionspotenziale bei den ausgetauschten Nachrichten hin. Zur Umsetzung dieser Potenziale bei HIP DEX führt der zweite Beitrag die Slimfit-Kompressionsschicht ein. Die Kombination dieser beider Beiträge erreicht eine deutliche Reduktion der Laufzeitkosten sowie eine wesentliche Verbesserung der Protokoll-Sicherheitseigenschaften.

Weiterhin decken die vorgenommenen Protokollanalysen umfangreiche Speicheranforderungen im Bezug auf die betrachteten Ende-zu-Ende-Sicherheitsprotokolle auf. Diese Anforderungen machen deren Einsatz auf stark speicherbeschränkten eingebetteten Systemen unmöglich. Der dritte Beitrag stellt eine Delegationsarchitektur vor, um diesen Geräten dennoch eine sichere Ende-zu-Ende-Kommunikation zu ermöglichen. Schließlich identifiziert die Analyse der 6LoWPAN-Anpassungsschicht die Anfälligkeit des dort eingesetzten Fragmentierungsmechanismus für DoS-Angriffe bei der DTLS-, HIP DEX- und Minimal IKEv2-Protokollaushandlung. Zum Schutz vor diesen Angriffen präsentiert der vierte Beitrag leichtgewichtige Abwehrmechanismen.

Die vorgestellten Beiträge lassen sich wirkungsvoll miteinander kombinieren und erzielen so erhebliche Sicherheits- und Effizienzsteigerungen für die betrachteten Ende-zu-Ende-IP-Sicherheitsprotokolle im Kontext des Internets der Dinge.

Acknowledgments

A number of people have contributed to my research, which ultimately resulted in this thesis. To all of you, a big and special **thank you**!

First and foremost, I would like to express my gratitude to my advisor Klaus Wehrle for asking me to join his group right after my diploma thesis. Without this initial impulse, I might not have embarked on this intriguing journey called the "PhD". I am especially grateful to you, Klaus, for allowing me to freely pursue my own research interests and – at the same time – cannot thank you enough for your encouragement when finding an attractive research topic proved more challenging than first anticipated. I also thank Thiemo Voigt for welcoming me to SICS for a brief stay, for accepting to review my thesis, and for acting as the second opponent during my PhD defense. The feedback I received from you and your team definitely had a positive impact on my work and the presentation of my research in this thesis.

During my time as a PhD student, I had the pleasure to work with a number of very interested and motivated students. Here, I would like to especially mention Christian Röller, Henrik Ziegeldorf, Hossein Shafagh, Jens Hiller, Maximilian Bogner, and Timo Boetcher. You should all be able to find aspects of your work reflected in this thesis. To all 21, I learned a lot from each of you, professionally as well as personally! I will always remember our fruitful discussions about design improvements, implementation details, and of course also about non-work-related aspects of life. I am particularly proud to see that some of you became PhD students yourself and it is always very exciting to meet you guys in your new jobs after COMSYS.

Over the last couple of years, I also had the chance to closely work with several extremely talented researchers. One of them, Tobias Heer, sparked my interest in scientific research. I owe you my gratitude, Tobi, for encouraging me to start the PhD, for always offering helpful advice, and, equally important, for all the good times as a friend. Miika Komu woke my interest in the HIP protocol in particular and in end-to-end IP security in general. This thesis surely would have an entirely different scope without you, Miika. Moreover, I would like to thank Hanno Wirtz for his painstakingly honest and always spot-on feedback during paper and thesis writing. I could not have wished for better colleagues than Martin Henze and Nicolai Viol regarding all project-related tasks and I am grateful to Georg Kunz for ensuring the necessary creativity and fun in research. Besides these people, I would also like to thank all other PhD students and Postdocs at COMSYS. I am very proud to have worked among you highly talented, motivated, and supportive people. This of course also includes the administrative and technical staff of COMSYS. Thanks, Ulrike May, Petra Zeidler, and Rainer Krogull, for your practical help and patience.

While pursuing my research, I additionally had the opportunity to meet many highly skilled and supportive people at the IETF and beyond. A special “thanks” goes to Robert Moskowitz for his invitation to co-author the HIP DEX Internet-Draft as well as for the conversations on- and off-topic during various IETF meetings. Moreover, I would like to thank Stefanie Gerdes and Shahid Raza for inviting me to contribute to their research papers. A big “thank you” also goes to Johannes Gilger for helping me with the write-up of one of my Internet-Drafts. It was a pleasure to collaborate with all of you. I am glad to have met Ari Keränen and Matthias Kovatsch, who not only helped me network at the IETF but with whom I could also tour the different meeting locations. Finally, I am grateful to Carsten Bormann, Oscar García-Morcón, Klaus Hartke, Sandeep Kumar, Ludwig Seitz, René Struik and many others for all the interesting discussions revolving around network security for IP-enabled embedded devices and the motivation I could draw from these valuable conversations.

Last but certainly not least, my PhD journey was only possible thanks to the unconditional support of my family. Inge, Wilfried, and Torsten, I highly appreciate your constant stream of encouragement and your help when things did not go exactly as planned. Above all, I am deeply grateful to you, Cristina, for standing by my side, for sacrificing many evenings of leisure time, and for always being there for me!

Contents