Security for Practical CoAP Applications: Issues and Solution Approaches

Martina Brachmann and Oscar Garcia-Morchon
Philips Research
Distributed Sensor Systems
Eindhoven, Netherlands
eMail: {martina.brachmann, oscar.garcia}@philips.com

Michael Kirsche
Brandenburg University of Technology Cottbus
Computer Networks and Communication Systems Group
Cottbus, Germany
eMail: michael.kirsche@tu-cottbus.de

***Abstract*—Protocols like 6LoWPAN and CoAP allow for an integration of smart objects into an IP-driven *Internet of Things*, thus enabling new applications such as pervasive health care or intelligent building control automation. Enabling security services (e.g. confidentiality, authentication, authorization) for these applications is essential, as they affect our personal daily life. However, established standard protocols and solutions cannot be directly used in 6LoWPAN/CoAP networks, due to the resource constrained nature of smart objects and new operation challenges in practical deployments. This work presents a compact overview of the current state-of-the-art in the IP-based Internet of Things; details practical security issues that need to be solved, namely end-to-end security and secure multicast based on (D)TLS; and discusses further work.**

I. Introduction

The expression 'The Internet of Things' (IoT) was first mentioned by Kevin Ashton in 1999 [1]. It combines the general meaning of the term 'Internet' with (smart) objects, such as sensors, localization systems or RFID tags, called 'Things', and denotes a network of objects, identifiable by a unique address [2], [3].
The intention is, that such objects are able to gather information in a more accurate and efficient way than humans can do. The captured information can be used to improve peoples lifestyle and well-being [1], as well as to protect the environment, or to automate designated processes (industrial automation). One possible usage scenario for IoT, described in [4], is pervasive healthcare, where wireless medical sensors can be associated to different personal area networks and used for health monitoring independent of location or time. Another widely discussed example is building control automation in order to directly control lighting, heating or security settings in a building through a mobile phone [5]. There are also efforts to use wireless sensor nodes to monitor tunnels [6] and dikes [7], to observe birds [8] or control freight during transportation in cargo containers [9].

Devices behind these use cases are typically battery powered and equipped with slow micro-controllers and small RAMs and ROMs. The data transfer is performed over wireless links with low bandwidth and high packet error rates [3]. Unlike the Internet, there are high scalability requirements with trillions of nodes [10] and the communication is either Human-to-Machine (H2M) or Machine-to-Machine(s) (M2M) [2].

The Internet Engineering Task Force (IETF) is currently defining and standardizing an IP-based Internet of Things. Several working groups (WG) are involved in this task [3]:
(i) The *IPv6 over Low-Power Wireless Personal Area Networks* (6LoWPAN) WG is concerned with the adaptation of IPv6 to IEEE 802.15.4 since IPv6 addressing is envisioned for the enormous amount of nodes that might be interconnected in the IoT [3]. Goals of the WG are the inclusion of neighbor discovery methodologies and the compression of IPv6 packets [11]. The latter is relevant since the Maximum Transfer Unit (MTU) of an IPv6 packet is minimum 1280 Bytes while IEEE 802.15.4's maximum packet size is 127 Bytes [12]. (ii) The *Routing Over Low power and Lossy networks* (ROLL) WG focuses on the design of routing approaches for networks with resource constrained devices, slow links and a high packet drop rate [13]. (iii) The *Constrained RESTful Environment* (CoRE) WG defines an application layer protocol for resource constrained devices, called Constrained Application Protocol (CoAP) [14]. CoAP is related to HTTP since both depend on the fundamental Representational State Transfer (REST) architecture of the web. Thus, CoAP allows, for example, accessing the resources of a CoAP server from the Internet (refer to Figure 1) by using certain HTTP methods and a similar URI scheme to identify resources. To prevent message overhead, the non-reliable UDP is used. Reliability is added again by CoAP through mechanisms like Message ID's, for duplicate detection, or confirmable messages that require an acknowledgment at application layer [15].

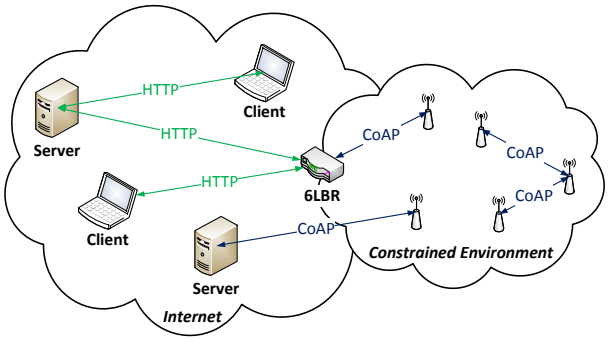


Figure 1. The CoRE architecture (cf. ([16])

So far, the 6LoWPAN, ROLL, and CoRE WGs have defined a number of protocols. Some of them are already RFCs while others are still Internet Drafts at a very advanced state (e.g. CoAP [15], 6LoWPAN-HC [17], RPL [18]). Rolling out the protocols developed by the three WGs offer many application areas. For example, it will be possible to setup light configurations in large-scale systems [19]. Another use case is requesting temperature or humidity in cargo containers via Internet during transportation [9]. This enables an advanced monitoring of the cooling chain for vendors and transportation operators. However, these scenarios require high security needs [20]. For instance, an entity (e.g. a person, a device, or an application) requiring access to specific resources in a thing needs to be authenticated first. To prevent attacks, the users identity should be protected and the exchanged information must be secured. In case the protection measures fails, changes should be traceable and reparable. Another important demand is system availability to ensure that authorized subjects can use their access privileges at any time. Thus, these networks should be resilient to Denial-of-Service (DoS) attacks.

II. Problem Statement

Despite the work performed by the involved IETF working groups, adequate solutions for a secure IP-based Internet of Things are still not available.

The authors of [21] and [22] describe existing security solutions for the Internet and give reasons why these solutions do not suit the needs of constrained networks. The required security mechanisms for the IoT can be grouped into five categories [21]. The first one, *network security*, refers to the defense of the lower layers in the OSI model, namely physical layer, data link layer and network layer. The second category, *application security*, aims at protecting applications and the exchange of data between two or more entities. The third refers to the *secure bootstrapping* [21] of the network while the other two aim at the security model of the 'object' itself and the security architecture behind the object and its interconnection with other objects and the Internet. Regarding application security, CoAP [15] describes four security modes to accomplish different security requirements for varying goals: (i) *NoSec*, no security, (ii) *SharedKey*, one key for all communication partners of a node, (iii) *MultiKey*, one key per communication partner, and (iv) *Certificate*, when a certificate is used. In the following, we discuss two security issues related to the use of the security modes 'SharedKey' and 'MultiKey' when targeting end-to-end security and secure group communication, respectively.

a) End-to-End Security: Devices relying on CoAP's 'SharedKey' or 'MultiKey' mode after bootstrapping can secure their communication using a pre-shared key (PSK) and DTLS [15], which is the datagram oriented version of TLS (Transport Layer Security) [23]. CoAP runs over UDP, which is the reason why DTLS [24] is used. It provides mechanisms for a reliable negotiation of a session secret and additional measures to verify exchanged packages. For that reason DTLS packets cannot be directly translated to TLS and vice versa. In this context, a first issue concerns the fact that a proxy is needed to translate packets when, for instance, an HTTP client wants to access the resources from a CoAP server in the back-end. The proxy can be a 6LoWPAN Border Router (6LBR), as Figure 2 illustrates it. In addition, a mapping between HTTP and CoAP in the application layer is required. To ensure that no malicious code will be added, the proxy/6LBR has to be a trusted instance. Until now, there is no solution to ensure end-to-end security for this use case.

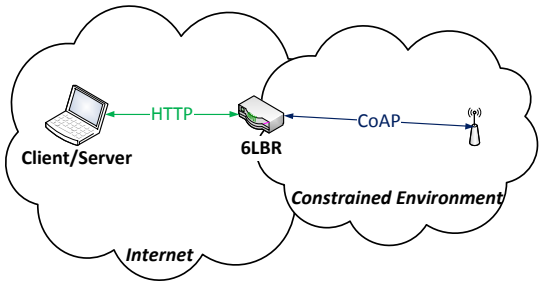


Figure 2. Possible scenario for end-to-end security

However, a couple of related security methods from other use cases outside the IoT scope are available for adaptation and inclusion into IoT security. For instance, one approach is a TLS-DTLS tunnel [25], where DTLS packets are encapsulated in TLS packets and vice versa. Another strategy was chosen for ITLS (Integrated Transport Layer Security) [26]. The sender encrypts a packet with two keys. The proxy owns the first key, decrypts with it the packet and forwards it to the receiver. This method can be used in case the proxy is not trustworthy. Both TLS-DTLS tunnel and ITLS require additional source code on sender and receiver side. This can be a disadvantage in constrained networks and, especially, for devices with scarce memory. A different approach that could be adapted for the problem is the method chosen for dynamic tunneling over either TCP/TLS or UDP/DTLS based on network conditions, described in [27]. Nevertheless, further analyses and comparisons of this and other approaches are needed. Examples for further analyses concern the memory consumption or the induced message overhead for negotiation of the session secrets.

b) Secure group communication: Multicast messages are used in CoAP to manipulate resources in a group of devices at the same time (e.g., turning off all light bulbs in a certain building floor). As already pointed out, unicast messages can be secured using DTLS with PSK. Regarding this, a second issue relates to the fact, that DTLS does not support multicast. A solution is necessary to ensure secure multicast within a group of nodes and to fulfill the multicast (security) requirements for CoAP, listed in [19]. Similar to unicast, when using the Internet for manipulating a resource in a group, no end-to-end security can be provided. In addition, TCP does not support multicast. Like in the end-to-end security problem, a proxy/6LoBR has to make a translation from HTTP to CoAP, TLS to DTLS, and in this case a mapping from the unicast address in the destination field of the UDP header to

a multicast address. Here, the proxy has to decide whether a message's destination address is multi- or unicast. To our keen knowledge, there is no possibility to mark a message as a multicast message in HTTP and the underlying protocols.

A solution approach for the described problems could be the use of IPsec ESP [28] as an alternative to DTLS. As mentioned in the Internet Draft of CoAP [15], IPsec is not recommended by the CoRE WG, because it is not supported for all IP stacks. However, there is a multicast extension for this protocol [29] available. [21] suggests to consider the MIKEY architecture [30] as a solution for negotiating a group key in the IoT.

III. Conclusion and Outlook

Solving the problems described in Section II, namely end-to-end security and secure group communication, is the key to ensure a secure IP-based Internet of Things. In this section, we hence introduce preliminary ideas to overcome them. The first one concentrates on the problem when using both HTTP and CoAP and hence, TLS and DTLS for a connection. The second part is to find solutions for exchanging messages in a group of CoAP nodes by using DTLS.

The goal for the first problem is to achieve a fully secure communication between an HTTP and a CoAP entity. Due to the resource-constrained nature of the nodes, the usage of (D)TLS-PSK is assumed [15]. Figure 3 illustrates the involved protocols for achieving end-to-end security. It contains one HTTP and CoAP entity each and a 6LoWPAN Border Router (6LBR), which acts as a proxy. A translation of the message headers created by the (D)TLS record layer and the protocols laying on top of it (handshake, alert, cipher suite, application data), depicted in Figure 4, must be implemented.

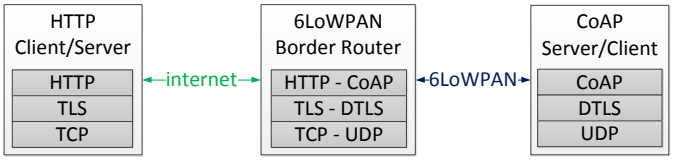


Figure 3. Architecture to achieve end-to-end security

For the development of a good solution, a number of factors need to be analyzed. For instance, whether the HTTP or CoAP client starts the communication, whether the proxy is within the CoAP network or if it is trusted.

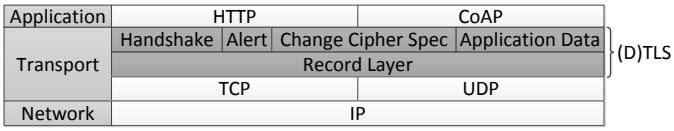
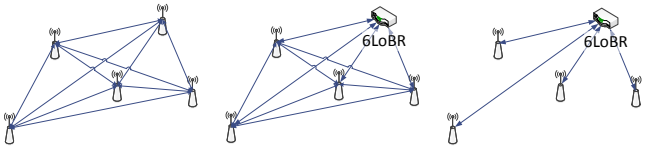


Figure 4. (D)TLS in protocol stack

Further, the steps to extend DTLS support to secure multicast are to be analyzed. Two entities using DTLS negotiate a session key for the communication. This key is determined by a PSK and a pair of nonces created by both client and server. That is why only two entities can negotiate one unique session key. For the second issue, a solution has to be found, implemented and evaluated, to establish a secure connection by means of DTLS within a group of devices with a single session key.

For group communication different approaches are available that have to be analyzed. The first one concerns the possible communication topologies, illustrated in Figure 5. There are distributed, centralized and hybrid topologies. Several use cases, advantages and disadvantages are described in [21]. This leads to a number of open issues including: when to build a group, how to determine group members and when to close it. For example, a membership in a group can be defined and fixed during device bootstrapping. Another aspect is when and how to refresh session keys.



(a) Distributed (b) Hybrid (c) Centralized

Figure 5. Different communication topologies for group communication

In conclusion, this paper presented an short outline of the current state-of-the-art in the IP-based Internet of Things. With main focus on security, we have identified and discussed two issues that need to be solved to ensure secure communication links. In our future research, we will further study these and other security gaps and we will develop adequate solutions solving them.

References

[1] K. Ashton, "That 'Internet of Things' Thing," online, http://www.rfidjournal.com/article/view/4986, 2009.

[2] "Internet of Things in 2020: Roadmap for the Future," online, http://www.iot-visitthefuture.eu/index.php?id=57, 2008.

[3] C. Bormann, J. Vasseur, and Z. Shelby, "The Internet of Things," online, http://isoc.org/wp/ietfjournal/?p=2066, 2010.

[4] O. Garcia-Morchon, T. Falck, T. Heer, and K. Wehrle, "Security for Pervasive Medical Sensor Networks," in *6th Int. Conference on Mobile and Ubiquitous Systems (MobiQuitous 2009)*, July 2009.

[5] G. Derene, "How to Control Your Home with your Cell Phone," online, http://www.popularmechanics.com/home/improvement/4301977, 2009.

[6] Tunnel Sensors Ltd., "Tunnel Sensors - Monitors for the Tunnel Environment," online, http://www.tunnelsensors.com/, 2011.

[7] URBANFLOOD CONSORTIUM, "About UrbanFlood," online, http://urbanflood.eu/aboutus.aspx, 2010.

[8] T. Bari, "BirdTracking: A Wireless Sensor Network to Observe Bird Life," M.Sc. Thesis, Embedded Software Group, Delft University of Technology, The Netherlands, August 2010.

[9] K. Kuladinithi, O. Bergmann, T. Poetsch, M. Becker, and C. Goerg, "Implementation of CoAP and its Application in Transport Logistics," in *Extending the Internet to Low power and Lossy Networks*, 2011.

[10] N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals," IETF 6LoWPAN, RFC 4919, 2007.

[11] 6LoWPAN WG, "Description of Working Group," online, https://datatracker.ietf.org/wg/6lowpan/charter/, 2011.

[12] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks," IETF 6LoWPAN, RFC 4944, 2007.

[13] ROLL WG, "Description of Working Group," online, https://datatracker.ietf.org/wg/roll/charter/, 2011.
[14] CoRE WG, "Description of Working Group," online, https://datatracker.ietf.org/wg/core/charter/, 2011.
[15] Z. Shelby, K. Hartke, C. Bormann, and B. Frank, "Constrained Application Protocol (CoAP)," IETF CoRE, draft-ietf-core-coap-05 (work in progress), 2011.
[16] Z. Shelby, "Introduction to Resource-Oriented Applications in Constrained Networks," 2011.
[17] J. Hui and P. Thubert, "Compression Format for IPv6 Datagrams in Low Power and Lossy Networks (6LoWPAN)," IETF 6LoWPAN, draft-ietf-6lowpan-hc-15 (work in progress), 2011.
[18] P. Thubert, A. Brandt, T. Clausen, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, and J. Vasseur, "RPL: IPv6 Routing Protocol for Low power and Lossy Networks," IETF ROLL, draft-ietf-roll-rpl-19 (work in progress), 2011.
[19] A. Rahman and E. Dijk, "Group Communication for CoAP," IETF CoRE, draft-rahman-core-groupcomm-05 (work in progress), 2011.
[20] R. H. Weber, "Internet of things - new security and privacy challenges," in *Legal discourse in cyberlaw and trade*, S. M. Kierkegaard, Ed., 2009, pp. 1–15, proceedings from the 4th International Conference on Legal, Security and Privacy issues in IT.
[21] O. Garcia-Morchon, S. Keoh, S. Kumar, R. Hummen, and R. Struik, "Security Considerations for the IoT," IETF CoRE, draft-garcia-core-security-01 (work in progress), 2011.
[22] R. Hummen, T. Heer, and K. Wehrle, "A security protocol adaptation layer for the ip-based internet of things," *Interconnecting Smart Objects with the Internet Workshop*, 3 2011, without peer-review.
[23] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," IETF TLS, RFC 5246, 2008.
[24] E. Rescorla and N. Modadugu, "Datagram Transport Layer Security," IETF TLS, RFC 4347, 2006.
[25] J. Reardon, "Improving Tor using a TCP-over-DTLS Tunnel," M.Sc. Thesis, University of Waterloo, Canada, 2008.
[26] E.-K. Kwon, Y.-G. Cho, and K.-J. Chae, "Integrated transport layer security: End-to-end security model between wtls and tls," in *Proceedings of the The 15th International Conference on Information Networking*, ser. ICOIN '01. IEEE Computer Society, 2001.
[27] T. Short, H.-C. Chen, V. Parla, and M. Tardif, "Method for dynamically tunneling over an unreliable protocol or a reliable protocol, based on network conditions," April 2007.
[28] S. Kent, "IP Encapsulating Security Payload (ESP)," IETF IPsec, RFC 4303, 2005.
[29] B. Weis, G. Gross, and D. Ignjatic, "Multicast Extension to the Security Architecture for the Internet Protocol," IETF MSEC, RFC 5374, 2008.
[30] J. Arkko, E. Carrara, F. Lindholm, M. Naslund, and K. Norrman, "MIKEY: Multimedia Internet KEYing," IETF MSEC, RFC 3830, 2004.