Axiom: DTLS-Based Secure IoT Group Communication

MARCO TILOCA, KIRILL NIKITIN, and SHAHID RAZA, SICS Swedish ICT AB

This article presents Axiom, a DTLS-based approach to efficiently secure multicast group communication among IoT-constrained devices. Axiom provides an adaptation of the DTLS record layer, relies on key material commonly shared among the group members, and does not require one to perform any DTLS handshake. We made a proof-of-concept implementation of Axiom based on the tinyDTLS library for the Contiki OS and used it to experimentally evaluate performance of our approach on real IoT hardware. Results show that Axiom is affordable on resource-constrained platforms and performs significantly better than related alternative approaches.

CCS Concepts: • **Security and privacy** → **Security protocols**; • **Computer systems organization** → *Embedded and cyber-physical systems;*

Additional Key Words and Phrases: Security, DTLS, multicast, group communication, Internet of Things

ACM Reference Format:
Marco Tiloca, Kirill Nikitin, and Shahid Raza. 2017. Axiom: DTLS-based secure IoT group communication. ACM Trans. Embed. Comput. Syst. 16, 3, Article 66 (April 2017), 29 pages.
DOI: http://dx.doi.org/10.1145/3047413

1. INTRODUCTION

We have been rapidly moving toward a pervasive networked society where all devices that can benefit from a connection will be connected with one another. This technology trend is commonly referred to as the *Internet of Things* (*IoT*) [Atzori et al. 2010; Kortuem et al. 2010], and it aims at connecting the physical and cyber world by means of tiny resource-constrained devices, embedded in everyday physical objects. To this end, different protocols have been standardized to enable interaction in the IoT. For instance, *6LoWPAN* [Hui and Thubert 2011] enables IP capabilities, *RPL* [Winter et al. 2012] enables routing capabilities, and *CoAP* [Shelby et al. 2014] enables web capabilities.

Several IoT application scenarios such as smart lighting applications, collective building control, and emergency broadcast services can benefit from the adoption of a group communication model, regardless of the specific application-level protocol. According to this communication model, a device becomes a member of a group by

This project was funded by the EU's FP7 program for research, technological development, and demonstration under grant agreement no. 607109; the EU H2020 project NobelGrid under grant no. 646184; VINNOVA, the EIT Digital HII project ACTIVE; and a Swedish Institute scholarship. This work was carried out during the tenure of an ERCIM "Alain Bensoussan" Fellowship Programme. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 246016.
Authors' addresses: M. Tiloca and S. Raza, RISE SICS AB, Isafjordsgatan 22, Kista, Sweden; emails: {marco.tiloca, shahid.raza}@ri.se; K. Nikitin, School of Computer and Communication Sciences, EPFL, EDOC-IC INN 134 (Bâtiment INN) Station 14, Lausanne, Switzerland; email: kirill.nikitin@epfl.ch.

DOI: http://dx.doi.org/10.1145/3047413