Ad Hoc Networks 32 (2015) 3–16

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

OSCAR: Object security architecture for the Internet of Things

Mališa Vučinić [a,b,*], Bernard Tourancheau [a], Franck Rousseau [a], Andrzej Duda [a], Laurent Damon [b], Roberto Guizzetti [b]

[a] Grenoble Alps University, CNRS Grenoble Informatics Laboratory, UMR 5217, 38400 Saint-Martin-d'Hères, France
[b] STMicroelectronics, 850 Rue Jean Monnet, 38920 Crolles, France

ARTICLE INFO

Article history:
Received 9 June 2014
Received in revised form 10 October 2014
Accepted 22 December 2014
Available online 30 December 2014

Keywords:
Communication security
Internet of Things
Object security
DTLS
Authorization
End-to-end security

ABSTRACT

In this paper, we propose OSCAR, an architecture for end-to-end security in the Internet of Things. It is based on the concept of *object security* that relates security with the application payload. The architecture includes Authorization Servers that provide clients with Access Secrets that enable them to request resources from constrained CoAP nodes. The nodes reply with the requested resources that are signed and encrypted. The scheme intrinsically supports multicast, asynchronous traffic, and caching.

We have evaluated OSCAR in two cases: 802.15.4 Low Power and Lossy Networks (LLN) and Machine-to-Machine (M2M) communication on two different hardware platforms and MAC layers on a real testbed and using the Cooja emulator. The results show that OSCAR outperforms a security scheme based on DTLS when the number of nodes increases. OSCAR also results in low energy consumption and latency.

1. Introduction

The long awaited Internet of Things (IoT) has never been closer, but security remains an important concern. Although constrained nodes of IoT may benefit from the existing IP security protocols, their core design assumptions build upon the connection-oriented security model that poorly fits IoT requirements. Research efforts towards the secure IoT have mostly concerned designing lightweight variants of security protocols and porting them to constrained nodes [1–4]. However, they do not pervade sufficiently, which led to a situation in which the recently standardized Constrained Application Protocol (CoAP) [5] fully supports the application requirements, but security does not keep up.

Smart devices, due to their severe energy and memory constraints, heavily rely on group communication, asynchronous traffic, and caching. Supporting a variety of existing security protocols/mechanisms to specifically target these requirements is practically impossible due to memory limitations. IETF has thus taken a position [5] to reuse Datagram Transport Layer Security (DTLS), the all-round point-to-point security protocol, to secure the communication channel between a constrained device running CoAP, in further text denoted as constrained CoAP node, and a client.

Apart from its current incompatibility with caching and multicast traffic, the DTLS approach has an important impact on scalability: Memory limitations of constrained nodes restrict the number of DTLS sessions. In IoT scenarios such as Smart Cities in which a large number of clients may communicate with constrained CoAP nodes, the limitations lead to a considerable load that translates to an increased energy consumption and a shortened lifetime.

In this paper, we address the problem of IoT security from a networking perspective and follow the Representational State Transfer (REST) architecture model [6] to remove the notion of state between server and client. We achieve this goal by leveraging the concept of *object*

[*] Corresponding author at: Grenoble Alps University, CNRS Grenoble Informatics Laboratory, UMR 5217, 38400 Saint-Martin-d'Hères, France.

http://dx.doi.org/10.1016/j.adhoc.2014.12.005
1570-8705/© 2014 Elsevier B.V. All rights reserved.

security that concerns data instead of communication end-points. In the proposed OSCAR architecture, we offload some expensive operations from constrained CoAP nodes to more powerful servers. Initially, constrained CoAP nodes publish their certificates to Authorization Servers and clients contact them to obtain Access Secrets that enable clients to request resources from constrained CoAP nodes. They reply with the requested resources that are signed and encrypted. The scheme couples the object security principle with the capability-based access control to provide communication confidentiality and protect nodes from replay attacks. Yet, we fully leverage a vast amount of work behind the (D)TLS protocol and use secure channels for authenticated certificate and Access Secret distribution.

The main contributions of our article are the following:

- A new scalable security architecture for IoT that jointly provides end-to-end security (E2E) and access control, decouples confidentiality and authenticity trust domains, and intrinsically supports multicast, asynchronous traffic, and caching.
- An evaluation of the architecture in a constrained Machine-to-Machine (M2M) scenario for two hardware platforms and MAC layers, on a real testbed and on the instruction level emulator of Cooja, demonstrating performance benefits with an increasing number of clients.

The article is organized as follows. We discuss the current Internet security model and the requirements of IoT applications in Section 2. We provide a detailed description of the proposed architecture in Section 3. In Section 4, we elaborate on how traditional Cloud services can integrate our architecture. We analyze and discuss security considerations in Sections 5 and 6, and present evaluation results in Section 7. Section 8 summarizes the related work. We conclude in Section 9.

2. Internet security model and IoT requirements

As the Internet relies on the communication model involving end-points, the security design followed by placing the trust on end-points and securing the communication channel. With evolving applications, the Internet has become a content distribution network leveraging the legacy client–server architecture. This paradigm has led to substantial research efforts on future Internet architectures, such as information centric networks, like DONA [7] and Content-Centric Networking [8]. Our work leverages their contributions and applies the general concepts with the goal to provide a robust, but flexible security approach to IoT and its traffic requirements.

As discussed by Smetters and Jacobson [9], the host oriented paradigm has a direct consequence on trust – its transitivity: Once a logical connection between the hosts is closed, the trust in the information is gone. The model serves very well typical e-commerce, e-banking, or IP telephony applications, because the trust in the information is implicitly dependent on the trust of the communicating entities *during the connection time*. However, considerable issues arise when the notion of a connection disappears. As stressed by Modadugu and Rescorla [10], DNS is purposely secured with the application level extension DNSSEC and not with a connection-oriented protocol such as DTLS. Content oriented security schemes such as S/MIME or PGP secure electronic mails that pass multiple application level gateways without a clear connection between end-points. IoT applications behave similarly:

- *Application traffic is asynchronous.* Constrained CoAP nodes (event detectors, monitoring sensors, smart meters) notify their clients (subscribers) of measured values or physical state changes as they happen. Clients send commands to actuating devices asynchronously in reaction to the changes in the environment. DNS traffic is a good parallel as asynchronous human actions trigger name resolution.
- *Caching is a must.* Severe energy constraints of sensor nodes lead to long sleep periods with less than 1% of the duty cycles. In this case, caching sensed data at untrusted intermediaries appears as an important means for keeping applications running independently. Electronic mails face a similar problem as they may go through untrusted servers until delivery.
- *Group communication is frequent.* In common IoT applications, clients may want to send messages to a subset of sensor/actuator nodes to perform an action, for example to turn off all lights on n^{th} floor or to update the firmware. IPv6 multicast and UDP provide support for this type of traffic bearing no connection state between end-points.

Typical Web applications involve a single server and multiple clients [6]. As a consequence, the server side application may control access after client authentication. IoT reverses this paradigm by having many nodes serving as servers and possibly many clients taking part in the same application. More importantly, CoAP nodes may need to reduce their functionalities due to resource constraints. Subsequently, access control becomes a distributed problem, especially when taking into account the recent efforts for decoupling the sensor network infrastructure from applications [11,12]. Furthermore, new applications have emerged that use local databases to store parts of collected data. For example, in Antelope [13] each constrained node in a network runs a database management system.

For these reasons, the connection-oriented security model does not fit well the actual IoT needs. Connection time tweaking and keep-alive messages could probably squeeze in connection-oriented security protocols, such as DTLS or IPsec, and work around the asynchronous traffic requirement. Aside the overhead, this approach would still provide us only with the communication channel security. To support caching, we would need to trust the intermediate nodes/proxies to store the data in clear. Note that we may deal with devices physically accessible to anyone. To support group communications, we would need to open separate secure connections among group members and/or add additional protocols on top of them, which effectively provides redundant security services necessary for use cases. Such a solution is not a long term approach.