Federated End-to-End Authentication for the Constrained Internet of Things Using IBC and ECC

Tobias Markmann
HAW Hamburg
tmarkmann@acm.org

Thomas C. Schmidt
HAW Hamburg
t.schmidt@acm.org

Matthias Wählisch
Freie Universität Berlin
waehlisch@ieee.org

ABSTRACT

Authentication of smart objects is a major challenge for the Internet of Things (IoT), and has been left open in DTLS. Leveraging locally managed IPv6 addresses with identity-based cryptography (IBC), we propose an efficient end-to-end authentication that (a) assigns a robust and deployment-friendly federation scheme to gateways of IoT subnetworks, and (b) has been evaluated with a modern twisted Edwards elliptic curve cryptography (ECC). Our early results demonstrate feasibility and promise efficiency after ongoing optimisations.

Keywords

Smart objects, ID-based cryptography, end-to-end security, authentication, federation

1. INTRODUCTION

Security and privacy of critical applications in the IoT require a protection layer that provides end-to-end security over open and uncontrollable media channels. Typical deployment scenarios of highly constrained devices in low power lossy wireless networks make certificate-base public-key infrastructures (e.g, SSL) infeasible. The Internet standard DTLS introduces UDP-based encryption, but assumes authentication in place. This leaves the major challenge of authenticating huge numbers of smart objects using highly efficient algorithms, low communication overhead, and still providing a flexible, automated trust management.

End-to-end authentication is a critical requirement for many IoT scenarios as they interact with the real world in private areas, or in a security sensitive manner which needs to be protected and controlled. End-to-end security protocols do not depend on link-layer security and do not require control of all devices en route. In this work, we assume the common deployment of gateways that (a) interconnect IoT domains with the global Internet, (b) are under the same administrative control as the IoT subnet, and (c) have sufficient resources to serve as a trusted authority (TA).

We propose identity-based cryptography (IBC) [1] for improving on the status quo—end-to-end authentication using traditional PKI with DTLS [2]. In IBC, an arbitrary bit string can be used as the public key. Keys that are addresses, for example, abandon the need for key distribution and all management overhead associated with certificates. IBC comes at the price of enhanced complexity, in particular for signature verification, and the problem of revoking identities. The size of the Internet (oT) will pose additional high scalability requirements on any IBC-type architecture.

We will address these challenges and concerns in the following approach (§ 2), and the evaluation in § 3. Here we also discuss the future steps in our ongoing work.

2. APPROACH

We consider the scenario of constrained IoT devices in subnetworks that are connected with the Internet using more powerful border gateways. Each owner of such IoT subnet is also entitled to assign the subnet-ID (IPv6 SLA) and maintains a trusted authority (TA) on the local gateway[1].

The TA is bound to IPv6 prefix (incl. subnet-ID) and assigns IP addresses to its local devices. By assigning private keys to these IPv6 addresses and distributing its public key locally, the TA enables IBC-bound authentication of the local nodes. Strictly local responsibility further assures (a) a simple, realistic management model, and (b) scalability. However, end-to-end authentication between nodes from different domains requires a federation between TAs that is protected against man-in-the-middle attacks and allows for a scalable localization of globally distributed TAs.

Our approach to a globally robust federation is based on cryptographically generated subnet-IDs. Under the common assumption of 48 bit globally routable prefix ('a /48'), we assign the subsequent (e.g., 64) bits for use as the subnet-ID, leaving a sufficient address space for assigning interface identifiers within the subnet. This subnet-ID is set to a truncated hash of the TA public key and thereby binds the responsible TA cryptographically to its subnet, while remaining resistant against accidental hash collisions. Being aware of this addressing logic and by using the full prefix with a conventional node-ID (e.g., ::001), any Internet device can request the public key from a remote TA. This allows for a scalable, fully distributed trust management, while the cryptographic binding prevents any unobserved modification along the path.

[1] A TA is comparable to a certificate authority (CA),but issues and has access to all private keys for this TA.

SIGCOMM '15 August 17-21, 2015, London, United Kingdom

ACM ISBN 978-1-4503-3542-3/15/08.
DOI: http://dx.doi.org/10.1145/2785956.2790021

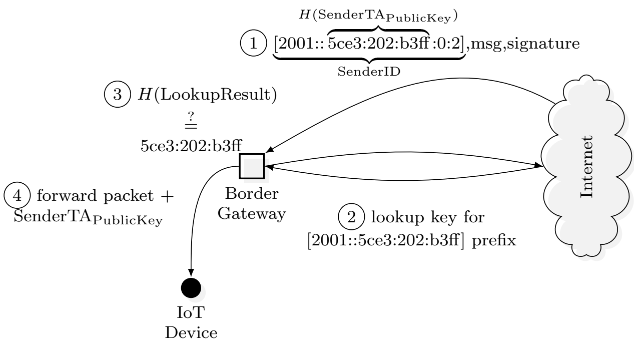

Figure 1: IBC message verification process

The detailed verification process can be seen in Figure 1. A packet that arrives at the border gateway includes the IPv6 header plus message and signature from the sender ①.

If the sender originates in the same subnet, the border gateway and a final receiver can authenticate using the same TA public key. In the case of an unknown subnet, the receiver first needs to obtain the TA public key corresponding to the sender's subnet, before it can authenticate the message in the packet ②. When verifying a signature of a device from a subnet, the subnet prefix includes a truncated hash of the corresponding TA public key. This prevents a replacement of public keys without change of the identity as part of a man-in-the-middle attack. After the verification of the received TA public key ③ the original packet and the TA public key are forwarded to the final IoT device ④.

An essential part of this *federated* end-to-end authentication is the lookup and verification of other TA public keys. There can be independent TA lookup methods that are used by more powerful devices and lookup methods that externalize the potentially complex lookup procedure from the IoT device to commonly present IoT gateways. IoT border gateways serve the connection of the IoT network to the worldwide Internet and are usually more powerful.

The border gateway can manage authentication and trust of TA key material and efficiently piggyback new and trusted TA keys to the constrained IoT device during communication, thereby avoiding additional communication load and latency. In this way verification of TA key material can be provided to highly diverse devices in the IoT.

The revocation of public keys in IBC is a non-trivial issue due to the implicit binding of public key and identity. A revocation of a public key in IBC also revokes the identity. However, identities in our approach are locally assigned IPv6 addresses, which can be renewed whenever trust to a local device requires revocation. Legitimate devices remain able to request new keys for their new identities from the TA and obtain a new IPv6 address with private identity key.

This architecture is implemented using elliptic curve cryptography based IBC to allow efficient implementation on the constrained devices of the IoT. We evaluated the use of ECC, specifically twisted Edwards curves, for constrained devices by writing an open implementation of [3] for the open-source RELIC [2] cryptographic library.

In addition, we plan to add a slight modification to the DTLS protocol, to allow two-way authentication based on IBC. This will allow end-to-end secured use of application protocols like the Constrained Application Protocol (CoAP).

3. EVALUATION AND FUTURE WORK

We now evaluate the performance of the ID-based cryptographic load by using the existing short Weierstrass ECC implementation in RELIC, as well as our twisted Edwards curve implementation using extended coordinates. A comparison between the short Weierstrass implementation and our code using Curve25519 [3] can be see in Figure 2, showing the performance of the ECC implementations under application with vBNN-IBS [4]. Using the twisted Edwards curve with extended coordinates gives a performance boost of roughly 20% on a constrained IoT platform. Without optimization, this already indicates feasibility, since the ID-based signature verification is compatible in performance to an RSA-2048 verification.

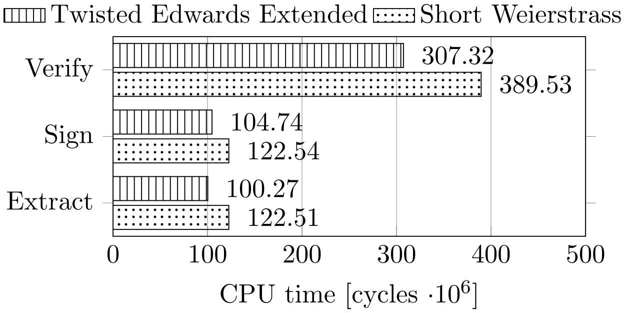

Figure 2: Performance of vBNN-IBS on a 32-bit ARM Cortex-M4 with 168 MHz clock speed.

Our next steps are further implementations of the described authentication architecture and to improve the ECC performance. There is room for a substantial performance boost that lifts the performance of RELIC in a competitive, efficient range.

We plan to evaluate the proposed system design with an open implementation using RELIC and RIOT [5], our free and open-source operating system for the IoT. Additionally, we will develop further measures to protect the local TAs.

4. REFERENCES

[1] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," in *Advances in Cryptology — CRYPTO 1984*, LNCS Springer, Aug. 1985, vol. 196, pp. 47–53.

[2] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "DTLS based security and two-way authentication for the Internet of Things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2710–2723, 2013.

[3] D. J. Bernstein, "Curve25519: New Diffie-Hellman Speed Records," in *Public Key Cryptography - PKC 2006*, LNCS Springer, 2006, vol. 3958, pp. 207–228.

[4] X. Cao, W. Kou, L. Dang, and B. Zhao, "IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks," *Comp. Comm.*, 31 (4), 2008.

[5] E. Baccelli, O. Hahm, M. Günes, M. Wählisch, and T. C. Schmidt, "RIOT OS: Towards an OS for the Internet of Things," in *Proc. of INFOCOM*, 2013.

[2] https://github.com/relic-toolkit/relic