Secure Federated Authentication in a Constrained Internet of Things

Tobias Markmann

tobias.markmann@haw-hamburg.de

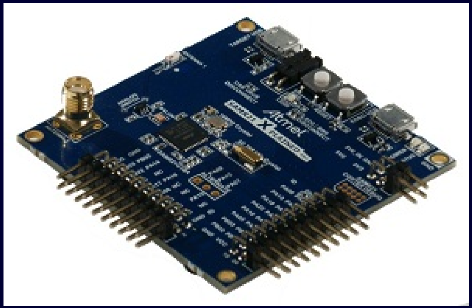
24.06.2015

Outline

1. Motivation and Challenge
2. Related Work
3. Identity-based Crypto Basics
4. IBC-based Federated Authentication for the IoT
5. Discussion

The Internet of Things

- Things:
  - Low CPU power
  - Low memory
  - Low energy
  - Low communication
- Communication:
  - Wired or wireless
  - Global interconnectivity
  - Machine-to-machine
  - Unprotected media
- Billions of connected devices



Motivation

- Security largely neglected in current IoT apps
- *Things* in private areas like home, car or body
- *Things* in business critical environments

Protect communication between constrained IoT devices

Examples: Sensitive data in power metering, smart home communication, ...

Challenge

Lightweight communication security for the IoT

- Lightweight: low memory and CPU requirements, small messages
- End-to-end security
- Security: **authentication** + encryption
- Low management overhead
- No trusted 3rd Party

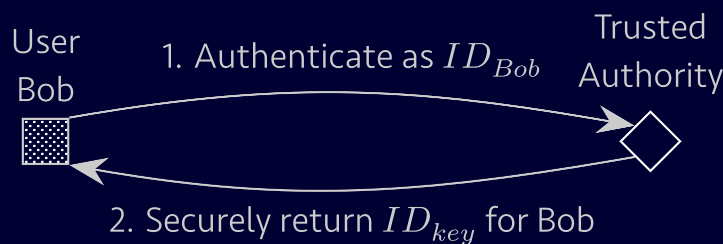
Related Work: Authentication for the IoT with DTLS

Kothmayr et al. [1]

- Comparable to HTTPS, but: HTTP $\longrightarrow$ CoAP, TLS $\longrightarrow$ DTLS
- Design: standard based, end-to-end security over unreliable transports
- DTLS provides authenticity, integrity and confidentially
- Standard X.509 certificates, keys bound to virtual identity (i.e. common name)
- Default data subscribed preconfigured; more delegated by tickets from access server
- RSA via TPM or ECC with 224-bit NIST curve

ID-based Cryptography Workflow

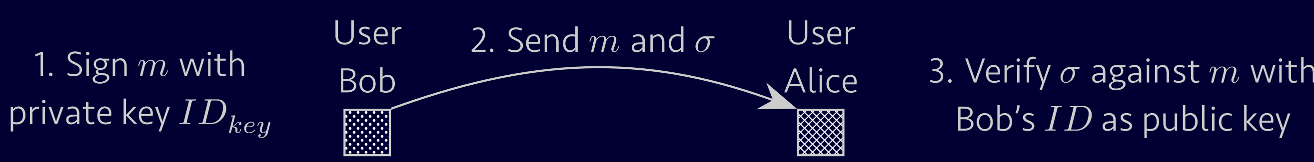
1. Setup $\rightarrow$ system parameters (SP) and master secret key (msk)
2. $\text{KeyExtraction}(SP, msk, ID) \rightarrow$ secret key for ID (ID_{key})



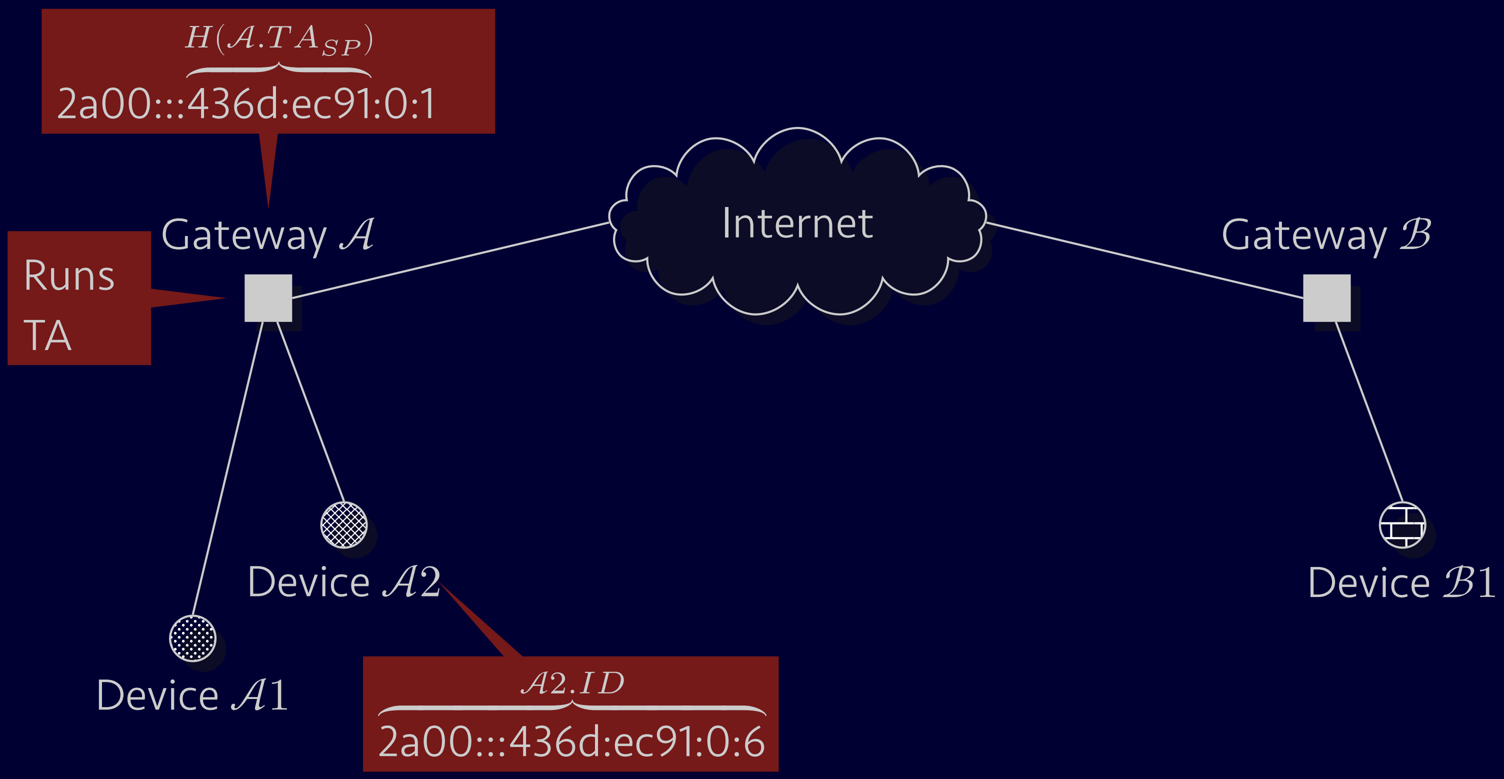
3. Authentication and Verification

   $\text{Sign}(SP, ID_{key}, m) \rightarrow (\sigma)$

   $\text{Verify}(SP, ID, m, \sigma) \rightarrow 1/0$



Proposal: Federated Authentication using IBC [2]



System Phases

1. System initialisation
2. Device setup
3. Authentication
4. TA public key lookup
5. Revocation
6. Key renewal

1. System Initialisation

1. Initialise IBC trusted authority
2. Generate ID_{key} for gateway
3. Configure network of gateway
4. Load secret keys for online device configuration

2. Device Setup

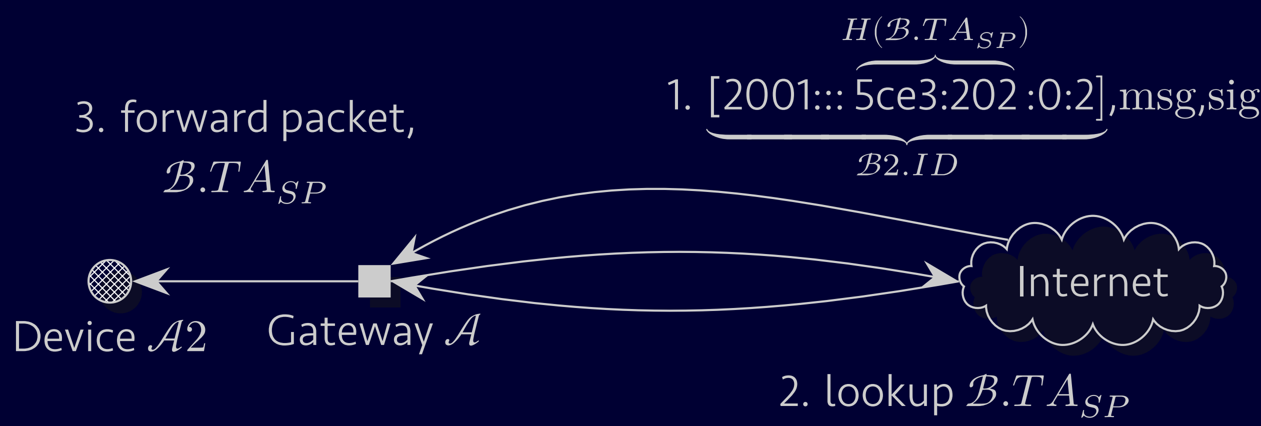
A. Static / Offline

- Generate ID_{key} and network config before deployment

B. Dynamic / Online

- Set of pre-shared keys (PSK), stored on device and gateway
- Device sends authenticated encrypted (AE) request to gateway
- TA generates ID (new IP), ID_{key} and sends it securely via AE
- Device verifies and decrypts
- Device finalises network configuration

3. Authentication



Sending authenticated messages

a. $\mathcal{B}2$ signs message: $sig = \text{Sign}(\mathcal{B}.TA_{SP}, \mathcal{B}2.ID_{key}, msg)$

b. Send msg and sig to $\mathcal{A}2$

Verifying authenticated messages

a. $\mathcal{A}2$ verifies message: $\text{Verify}(\mathcal{B}.TA_{SP}, \mathcal{B}2.ID, msg, sig)$

3. Authentication

More protocols:

a. Elliptic-curve Diffie–Hellman key exchange, signed by IBS

b. ID-based key exchange

c. Establish DTLS association from above

4. Trusted Authority Lookup

1. $\mathcal{A}$ requests TA system parameters from $(\mathcal{B})$
   - Gateways conventionally located at …:0:1
2. $\mathcal{B}$ sends signed $B.TA_{SP}$ back
3. $\mathcal{A}$ verifies response against hash in address
4. On match, $\mathcal{A}$ stores trust association $(\mathrm{Prefix}(\mathcal{B}), B.TA_{SP})$

leap of faith or *trust on first use* (TOFU) based trust

5. Revocation (Related Work)

1. Revocation by expiration, by Boneh and Franklin [3]
   - ID format: $real\ ID \parallel week$
   - **No** explicit revocation

5. Revocation (Related Work)

2. Explicit revocation before expiration, by Hoeper and Gong [4]

- ID format: $real\ ID \parallel time\ period \parallel version$
- Designed for MANETs
- Each node monitors traffic for malicious behavior
  - ⋆ Bad behavior (traffic, logic)
  - ⋆ Explicit self-revocation
- Propagate observations to m-hop nodes
- Revoked if $> \delta$ neighbors accused a node
- Revoked devices obtain new key with $version++$

5. Revocation

- Detect malicious devices and report to TA
- The TA records malicious devices
- Devices with $\#reports > threshold$
  - No new key on TA rollover
  - Possibly block traffic
- Start TA rollover

6. Key Renewal (TA rollover)

1. Generate new TA and gateway address
2. Add new address to network interface
3. Notify other known TAs about new TA
   - Enable trust continuation
4. TA locally broadcasts signed rollover notification
5. Devices securely (ECDH, AE) request new ID and key
6. Remove old TA and network routing after grace period

Implementation & Evaluation

- Project II (Done)
  - Elliptic curve crypto based on twisted Edwards curve Curve25519 [5]
  - vBNN-IBS [6] as ID-based signature algorithm
  - Implementation in C using RELIC [7]
- Upcoming
  - Implement basic features of architecture
  - Evaluate on SAM R21, low-power simple ARM Cortex-M0+
  - Constant time prime field implementation

Discussion

- IBC reduces the key management problem
- Explicit revocation of devices
- TA identity bound to network address

Current issues:

- IDs change on TA rollover
  $\longrightarrow$ securely propagate rollover to other parties
- Gateway running TA is a high-value target
  $\longrightarrow$ semi-online TA (complicates online device setup)

Thanks

- Questions?
- Feedback?
- Suggestions?

References

[1] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig and G. Carle, "A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication", In *2012 IEEE 37th Conference on Local Computer Networks Workshops (LCN Workshops)*, pages 956–963, Piscataway, NJ, USA, 2012. IEEE.

[2] T. Markmann, T. C. Schmidt and M. Wählisch, "Federated End-to-End Authentication for the Constrained Internet of Things using IBC and ECC", In *Proc. of ACM SIGCOMM, Poster Session*, 2015. ACM. Accepted for publication.

[3] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing", In J. Kilian, editor, *"Advances in Cryptology — CRYPTO 2001"* , number 2139 in Lecture Notes in Computer Science, pages 213–229. Springer, Berlin, Heidelberg, Germany, 2001.

[4] K. Hoeper and G. Gong, "Key Revocation for Identity-Based Schemes in Mobile Ad Hoc Networks", In T. Kunz and S. Ravi, editors, *"Ad-Hoc, Mobile, and Wireless Networks"* , number 4104 in Lecture Notes in Computer Science, pages 224–237. Springer, Berlin, Heidelberg, Germany, 2006.

[5] A. Langley and R. Salz, "Elliptic Curves for Security" , Internet-Draft – work in progress 02, IETF, 2015.

[6] X. Cao, W. Kou, L. Dang and B. Zhao, "IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks", *Computer Communications*, 31(4):659–667, 2008.

[7] D. F. Aranha and C. P. L. Gouvêa. "RELIC is an Efficient LIbrary for Cryptography" , https://github.com/relic-toolkit/relic.

Image Sources

- http://www.atmel.com/tools/ATSAMR21-XPRO.aspx
- https://www.pinterest.com/mikkohypponen/hackers-with-hoodies/