Outline

1) Motivation and goals
2) Proposed framework
3) Proposed system architecture
4) Delegated ECC public-key authentication
5) Experimental evaluation
6) Conclusions
Outline

1) Motivation and goals
2) Proposed framework
3) Proposed system architecture
4) Delegated ECC public-key authentication
5) Experimental evaluation
6) Conclusions
Motivation and goals

We may currently observe that:

- Sensing applications on the IoT will require appropriate security mechanisms, including to protect end-to-end communications.
- Security should be quantifiable and adaptable.

Main goals:

- Propose a framework supporting adaptable end-to-end security in the context of Internet-interconnected WSN.
- Address end-to-end transport-layer security with delegated ECC public-key authentication.
- Evaluate experimentally the proposed mechanisms in the context of the proposed framework.
Outline

1) Motivation and goals
2) Proposed framework
3) Proposed system architecture
4) Delegated ECC public-key authentication
5) Experimental evaluation
6) Conclusions
Proposed framework

- A framework for the usage of secure end-to-end transport-layer communications with Internet-integrated sensing applications:

- Access control information
- Device capabilities
- Certification information
- Compute end-to-end security mode
- Application functional profile
- Application security profile
- Authentication and key agreement delegation
- Full end-to-end security support
- Full end-to-end security delegation

Information required for the usage of new security mechanisms

Security and functional requirements of applications

Security may adapt and reconfigure during the lifetime of the application
Outline

1) Motivation and goals
2) Proposed framework
3) **Proposed system architecture**
4) Delegated ECC public-key authentication
5) Experimental evaluation
6) Conclusions
Proposed system architecture

Main goals:

- Support of end-to-end transport-layer security in three usage modes: full DTLS security, DTLS with delegated handshake, DTLS with fully delegated handshake.

- Support of future security mechanisms in the context of Internet-integrated WSN.

- Full compatibility with application-layer CoAP and 6LoWPAN security
Proposed system architecture

Sensing device

TLS_PSK_WITH_AES_128_CCM_8

Access control server

DTLS delegated authentication, other security suites may be supported

An application may support multiple LoWPAN domains

A device may move between domains

Access control information related with LoWPAN devices

6LBR

Certification authority

Internet/external host

WSN1

End-to-end security

WSNn

Sensing device

Access control server

6LBR
Outine

1) Motivation and goals
2) Proposed framework
3) Proposed system architecture
4) Delegated ECC public-key authentication
5) Experimental evaluation
6) Conclusions
Delegated ECC public-key authentication

Regarding CoAP security:

- CoAP supports three security modes:
  - PreSharedKey (TLS_PSK_WITH_AES_128_CCM_8)
  - RawPublicKey and Certificates (TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8)

- Encryption may use AES (CCM,CBC)

- AES/CCM is available in sensing platforms such as the TelosB implementing IEEE 802.15.4
Delegated ECC public-key authentication

- A secure DTLS session requires the two parties to agree on:
  - The cipher suite
  - The encryption keys

- The DTLS handshake transports the information required for both parties to obtain encryption keys:
  - A shared master key is obtained from a pair of client and server random values plus a pre-shared master secret key (PMSK)
  - Final encryption keys are obtained from the shared master secret.

- PMSK generation depends on the cipher employed:
  - With public-key suites the client generates the PMSK and sends it to the server
  - Pre-shared keys suites don’t support this, but we may modify TLS_PSK_WITH_AES_128_CCM_8 as long as we maintain appropriate security on the LoWPAN
Delegated ECC public-key authentication

- Trust and security between 6LBR and 6LoWPAN devices
- Intercepts and forwards packets at the transport-layer
- Public-key certification of communicating entities

CoAP security mode

PreSharedKey CoAP security mode (modified)

Certificates CoAP security mode

ERCIM Workshop 2013
Mediated DTLS handshake

Controls the handshake and supports ECC on behalf of sensing device

Requests information about device
Request PSK auth
Server random
Mutual auth between 6LBR and device via the AC

Requests public-key auth
ACK public-key auth
Client random and PMSK
AES/CCM

DTLS protected communications

ER CIM Workshop 2013
6LBR and CoAP server mutual authentication

Trusted entity. For each device stores: ID, certificate, supported ciphers and compression methods

Obtain security-related information about the destination CoAP device

Authentication token

Mutual authentication between the 6LBR and the CoAP device

PMSK exchange in the context of the DTLS handshake
Outline

1) Motivation and goals
2) Proposed framework
3) Proposed system architecture
4) Delegated ECC public-key authentication
5) Experimental evaluation
6) Conclusions
Experimental evaluation

- Experimental evaluation setup using Linux and TelosB devices
- TelosB: 16-bit MSP430, 48KB ROM, 10KB RAM, IEEE 802.15.4
- Support of TinyOS, BLIP, CoAP, DTLS (ECDSA, ECDHE), SHA-256 and LoWPAN authentication
- Standalone AES/CCM hardware encryption
- LibCoAP with DTLS support
Experimental evaluation

- Two application profiles:
  - Moderate number of DTLS sessions/hour (1 to 400) and of CoAP requests per DTLS session (2).
  - Higher number of DTLS sessions/hour (14 to 7200) and of CoAP requests per DTLS session (10).

- Evaluate end-to-end security in two usage modes:
  - Support of full end-to-end DTLS security.
  - Delegated DTLS authentication using the proposed mediated handshake.
Experimental evaluation

- Impact on the lifetime of sensing applications (moderate usage profile):

Clear advantage of delegated DTLS authentication, particularly for a lower number of DTLS sessions per hour.

Advantage is less expressive for higher values, due to the higher impact of AES/CCM encryption in comparison with the DTLS handshake.
Experimental evaluation

- Impact on the lifetime of sensing applications (higher usage profile):

![Graph showing lifetime (hours) vs. Number of DTLS sessions per hour]

Similar conclusions regarding the advantages of delegated DTLS authentication.
Outline

1) Motivation and goals
2) Proposed framework
3) Proposed system architecture
4) Delegated ECC public-key authentication
5) Experimental evaluation
6) Conclusions
Conclusions

- Efficient support of end-to-end security using delegated mutual authentication.
- Compatibility with standardized CoAP security.
- Other security mechanisms based on a security gateway may be adopted in the future (application-layer message analysis and filtering, 6LoWPAN security).

Future work:
- Transparent end-to-end security for mobile devices.
- Mechanisms to configure security according to application profiles and characteristics of devices.
- Adoption of other security suites on the LoWPAN domain.