DTLS In Constrained Environments (DICE) BOF

Wed 15:10-16:10, Potsdam 3

BOF Chairs: Zach Shelby, Carsten Bormann

Responsible AD: Stephen Farrell

Mailing List: dtls-iot@ietf.org

Note Well

This summary is only meant to point you in the right direction, and doesn't have all the nuances. The IETF's IPR Policy is set forth in BCP 79; please read it carefully.

The brief summary:

- **By participating with the IETF, you agree to follow IETF processes.**
- **If you are aware that a contribution of yours (something you write, say, or discuss in any IETF context) is covered by patents or patent applications, you need to disclose that fact.**
- **You understand that meetings might be recorded, broadcast, and publicly archived.**

For further information, talk to a chair, ask an Area Director, or review the following:

BCP 9 (on the Internet Standards Process)

BCP 25 (on the Working Group processes)

BCP 78 (on the IETF Trust)

BCP 79 (on Intellectual Property Rights in the IETF)

Agenda

- Problem space (overview)
- Solution space (2 slots)
- Discussion
- Charter
- Key Questions

The Problem

- CoAP is moving towards mass deployment
  - DTLS 1.2 is the chosen security mechanism
  - Suitable range of security modes & ciphers are available
  - This was exactly the right choice!
- However, DTLS has several drawbacks
  - Not clear what DTLS protocols, extensions and modes are needed
  - No support for IP multicast, which CoAP is often used with
  - Handshake overhead can be unnecessarily high
  - DTLS handshake state-machine is complex
- What if we just do nothing?
  - Proprietary, likely broken, security mechanisms will be invented
  - Or worse, deployments without security, e.g. for multicast

The Scope

- The DICE working group would initially:
  - Define a constrained DTLS profile
    - For a specific use case in IoT
  - Define DTLS record layer group communications
    - With minimal record layer impact

- Explicitly out of scope:
  - Changing DTLS in the profiling work
  - Key management (of any kind)
  - Specification of new cipher suites

Related Work

- Profiling Work Item Strawman
  http://tools.ietf.org/html/draft-keoh-dtls-profile-iot-00

- Group Communication Work Item Strawman
  http://www.ietf.org/id/draft-keoh-dtls-multicast-security-00.txt

- Other Existing work
  http://www.ietf.org/id/draft-keoh-lwig-dtls-iot-01.txt
  http://www.ietf.org/id/draft-hartke-core-codtls-02.txt
  http://www.ietf.org/id/draft-tschofenig-lwig-tls-minimal-03.txt

Relation to other WGs

- CORE
  - Has defined CoAP binding to DTLS 1.2 and “must implement” Cipher suites
  - May work on AA issues around CoRE for use with DTLS
  - Main source of application requirement expertise for DICE work
- LWIG
  - Has provided implementation guidance related to DTLS as input
  - DICE focuses on standards track profile and group support
- TLS
  - Maintenance of core TLS specifications
  - Main source of security expertise and reviews for DICE work

Possible Future Work

- New transports for TLS, e.g. CoAP
  - We need practical experience in the mean time
  - Not clear if benefits are sufficient
- Use of more efficient cipher suites, e.g. hash-only
  - Requirements possibly from DICE, suite definition to be done in the TLS WG
- Revocation, ACL management
  - But this probably belongs in its own WG

Work Item Presentations

- DTLS Profiling (5 min) - Hannes Tschofenig
  - http://tools.ietf.org/html/draft-keoh-dtls-profile-iot-00
  - http://www.ietf.org/id/draft-keoh-lwig-dtls-iot-01.txt
  - http://www.ietf.org/id/draft-hartke-core-codtls-02.txt
  - http://www.ietf.org/id/draft-tschofenig-lwig-tls-minimal-03.txt

- Record Layer Group Communications (10 min) - Sandeep Kumar
  - http://www.ietf.org/id/draft-keoh-dtls-multicast-security-00.txt

DTLS Profiling for IoT

Hannes Tschofenig, Sye Loong Keoh, Sandeep Kumar, Klaus Hartke

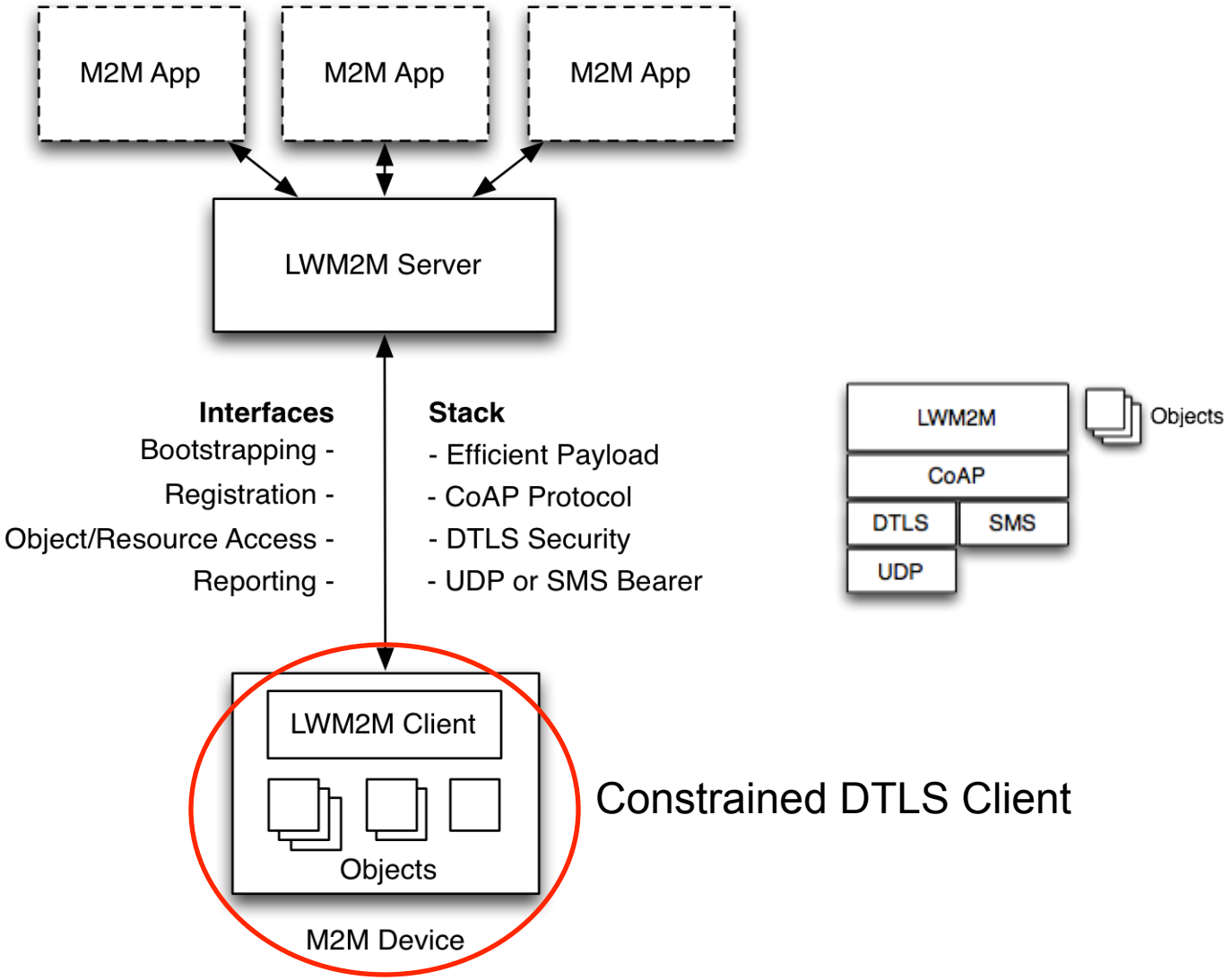
http://tools.ietf.org/html/draft-keoh-dtls-profile-iot-00
http://www.ietf.org/id/draft-keoh-lwig-dtls-iot-01.txt
http://www.ietf.org/id/draft-hartke-core-codtls-02.txt
http://www.ietf.org/id/draft-tschofenig-lwig-tls-minimal-03.txt

DICE BOF, IETF-87 Berlin

DTLS Profiling

- Our protocols are generic, often not tailored to specific deployment environments.
- With smart objects there are constraints about what features to implement with an impact for interoperability.
- Profiles of DTLS require information about the expected use case.

Simple Use Case – OMA Lightweight



Potential Profiling Examples

- Constrained node to implement DTLS Client only
- Limit to the security modes defined in CoAP
  - PSK, RPK, X.509
- Require mutual authentication
- Clarify needed protocols & extensions
  - Sub-set of Alert and ChangeCipherSuite
  - Determine if session resumption needed
- (Maintain cipher negotiation)

Enabling Secure Group Communication reusing DTLS Record layer

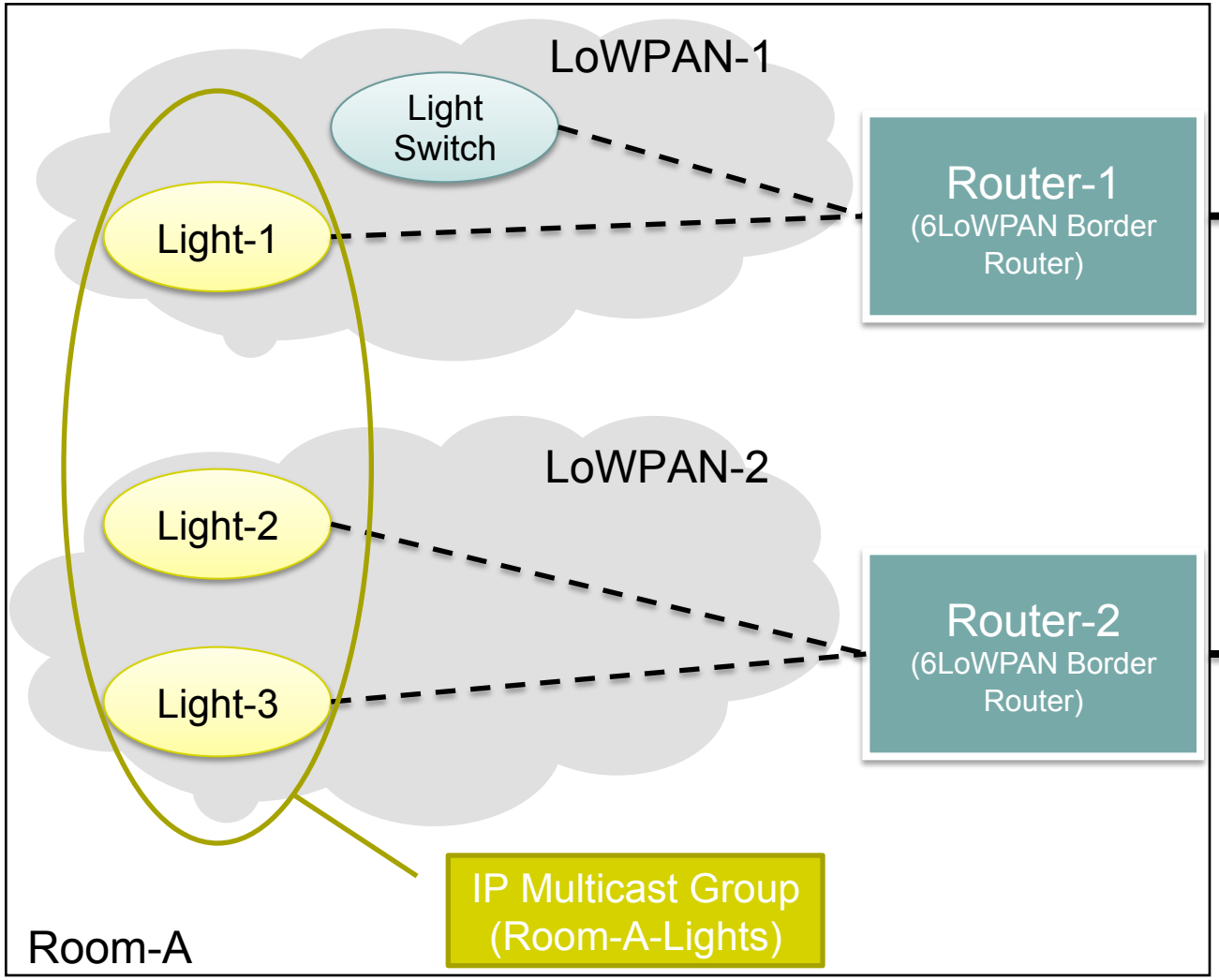
draft-keoh-dtls-multicast-security

Sye Loong Keoh, Oscar Garcia-Morchon, ***Sandeep S. Kumar****, Esko Dijk*

IETF87 Jul 28 – 2, 2013, Berlin

Email: sandeep.kumar AT philips.com

Group Communication Use Cases



Source: Group Communication for CoAP (draft-ietf-core-groupcomm)

Use-cases

- Group light control
- Firmware updates
- Parameter distribution

Motivation & Requirements

Group communication (in LLNs): also vulnerable to eavesdropping, tampering, message forgery, replay, etc.

Limited resources and memory: reduce the number of cryptographic protocols on device.

DTLS is chosen security solution for unicast CoAP: beneficial for constrained devices if it can be used also for COAP group communication.

Requirements

Immediate goals

- Group level data integrity and authentication
- Data confidentiality (optional)
- Replay protection

To extend later (out-of-scope for now)

- Data source authentication: *application level*, e.g., object security
- A Group Security Association (GSA): *distribute keying materials*, *specify the ciphersuite for encryption and authentication*
- Multicast key management: *update/renew group keys periodically.*

Reuse of DTLS Record Layer

In scope: Transport of COAP group messages over the DTLS record layer secured with group key.

Out of scope: Changes to DTLS state-machine, Group session Key management.

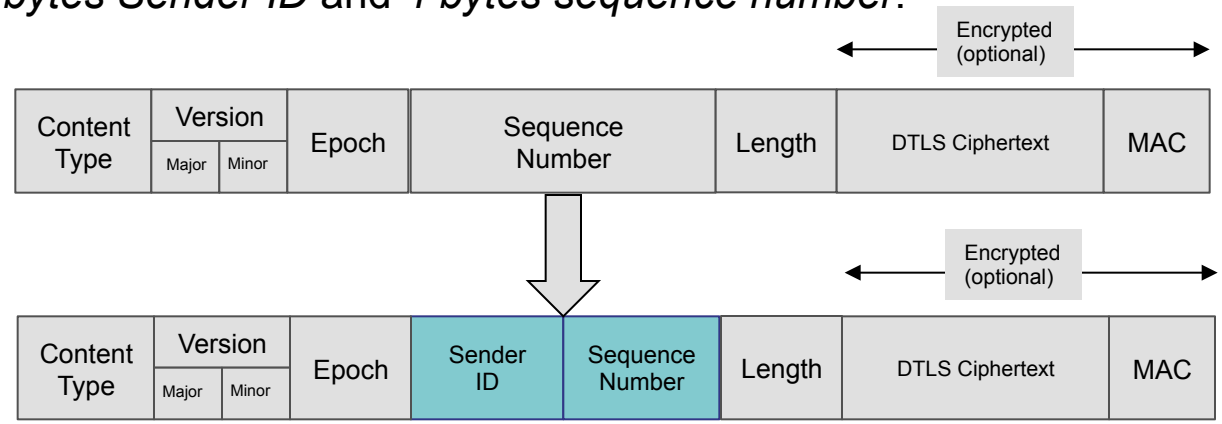
Assumptions:

- Group session key and cipher for authentication & encryption to use are known to all group members **out-of-band**.
- Support for few senders and multiple receivers in the secure group communication.
- *A (2-byte) Sender-ID derived from the IPv6 address is unique among senders.*

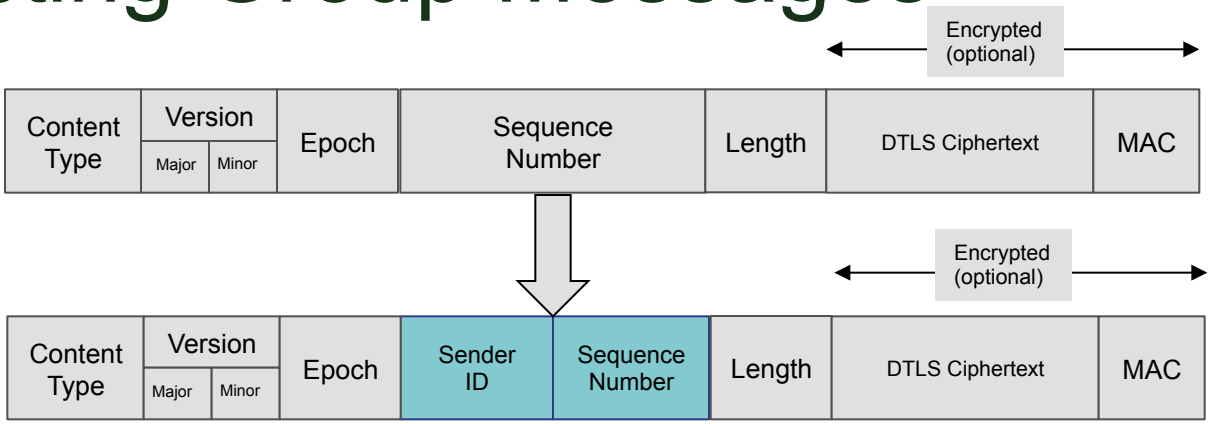
Proposal:

- Without changing the DTLS Record Layer, the *6-byte sequence number* field is split into:

  2 bytes Sender ID and *4 bytes sequence number*.



Protecting Group Messages



Senders

- The sender must include its *Sender ID* in the DTLS Record Layer header and increment the sequence number when sending a group message.
- Each sender manages its own *epoch* and *sequence number,* no synchronization is needed with other senders in the group.
- The *epoch* will be increased, and the *sequence number* will be reset once the group session key is renewed or updated (**out-of-scope**)

Receivers

- All receivers first perform a group key lookup by using the multicast destination IP address of the packet.
- Using the *Sender ID* field, receivers retrieve the last used *epoch* and *sequence number* to detect replay.
- Message is decrypted and the MAC of the message is checked

Summary

- Group communication is often used in machine-to-machine (M2M) applications.
- Group communication is equally vulnerable and requires security.
- Preferably re-use existing security protocols on constrained devices in LLNs.
- Propose to reuse DTLS Record layer to support secure group communication, with key management **out-of-scope**.

Summary of DICE Objectives

- The DICE working group would initially:
  - Define a constrained DTLS profile
    - For a specific use case in IoT
  - Define DTLS record layer group communications
    - With minimal record layer impact
- Explicitly out of scope:
  - Changing DTLS in the profiling work
  - Key management (of any kind)
  - Specification of new cipher suites

An Important Question

a) Is this a topic the IETF **should** try to address?

b) Is this a topic the IETF **should not** try to address?

c) Do you not understand the problem well enough?

Charter Question

- The draft charter has been posted to the DICE mailing list:
  - http://www.ietf.org/mail-archive/web/dtls-iot/current/msg00102.html

a) Is the scope of the charter **clear** enough?

b) Is the scope of the charter **not clear** enough?

Proposed Charter

Over the past few years, there have been many efforts to implement DTLS on embedded systems in order to support Internet of Things (IoT) applications. In fact, Transport Layer Security (TLS) and its datagram variant were both invented for use in the Internet-based web applications, and implementers face many challenges to deploy (D)TLS on IoT devices that are limited in memory resources (RAM, Flash), CPU and power. In particular, (D)TLS supports a wide range of security features and functionalities, some of these features are not necessarily required for IoT applications. One of the goals of DICE working group is to document the immediate problems that hinder the deployment of DTLS on embedded systems and proposes a DTLS profile for CoAP-based IoT applications based on well understood application use cases.

Proposed Charter

Group communication is an important feature in IoT applications as it can be effectively used to convey messages to a group of devices without requiring the sender to perform multiple time- and energy-consuming unicast transmissions, one for each group member. For example, in a building control management system, Heating, Ventilation and Air-Conditioning (HVAC) and lighting devices can be grouped according to the layout of the building, and control commands can be issued to a group of devices. Unsecured group communication for CNNs is enabled by using CoAP on top of IP-multicast. However, it must be secured as it is vulnerable to the usual attacks (eavesdropping, tampering, message forgery, replay, etc). DTLS has been chosen by CoRE to protect CoAP unicast communications, and it would be beneficial if the same security protocol, i.e., DTLS Record Layer can be used to protect CoAP group communication as well without changing the existing DTLS state machine. The goal of the DICE working group is to ensure that DTLS is the obvious choice for protecting CoAP and other UDP based protocols for the Internet of Things. Key management of group keys is however out of scope of this working group.

Proposed Charter

The current design of DTLS leads to fragmentation of DTLS handshake messages over the wireless link, in particular when Raw Public-key and Certificate modes are used. From the various implementation experiences reported in the LWIG working group, the complexity of re-transmission and re-ordering of DTLS handshake messages in constrained networks has resulted in a significantly increased code size and RAM. Additional reliability mechanisms for transporting DTLS handshake messages are required as they will ensure that handling of re-ordered messages needs to be done only once in a single place in the stack. This working group may also look at alternative TLS transports in cooperation with the TLS WG.

This WG combines expertise from both the IETF Application and Security areas in order to work out the appropriate use of DTLS for the Internet of Things. DICE will work closely with LWIG to understand the complexity and overhead issues of DTLS, and to investigate the performance issues of the DTLS handshake. Cooperation with the TLS WG will be necessary for all activities in DICE.

Proposed Charter

The scope of this WG is to define the following:

- Document the problems with the DTLS handshake for IoT, and define a suitable profile of DTLS for an IoT architecture and use case that minimizes the complexity and overhead of DTLS for constrained devices. The set of DTLS extensions and modes to be supported will be defined.

- Define the reuse of DTLS Record Layer for secure CoAP group communication in combination with a (out-of-band delivered) group key for select cipher suites. The DTLS state machine should not be modified/altered and key management is outside the scope.

Goals and Milestones

Oct 2013 WG document for DTLS for Constrained Environments profile

Nov 2013 WG document for secure COAP group communication for IoT

Feb 2014 DTLS for IoT profile specification submitted to the IESG for publication as standards track

Mar 2014 Secure COAP group communication specification submitted to the IESG for publication as standards track

Another Important Question

a) Do you think this charter **makes sense** to propose?

b) Do you think this charter **does not make sense** to propose?

c) Do you not know enough to make a conclusion?

And Finally

a) How many people are willing to edit, comment or implement documents?