A Secure Network Architecture for the Internet of Things Based on Local Authorization Entities

Hokeun Kim, Armin Wasicek, Benjamin Mehne and Edward A. Lee (UC Berkeley)

DAC 2016, June 8, 2016

http://terraswarm.org/

Motivation

Main Challenges for IoT Security

- Heterogeneity in security requirements & resource availability

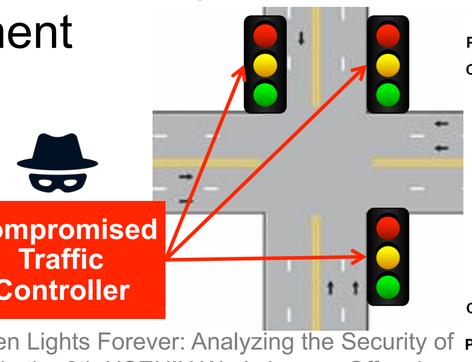
Cardiac monitor and emergency service
- Privacy
- Resource constraints

Drones and ground air traffic control
- Strong and frequent authorization
- Intermittent connectivity

Apple pay
- Confidentiality
- Authentication
- Moderate resource constraints

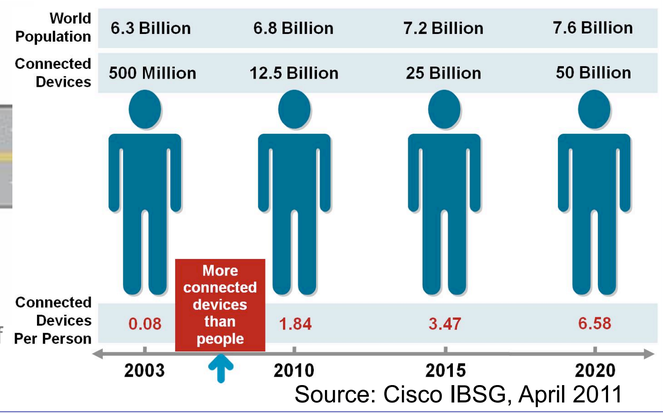
Ambient temperature sensors and receivers
- Data integrity
- Resource constraints

- Operation under open/untrusted environment



B. Ghena, *et al.*, "Green Lights Forever: Analyzing the Security of Traffic Infrastructure," in the 8th USENIX Workshop on Offensive Technologies 2014 (WOOT 14)

- Scalability



Source: Cisco IBSG, April 2011

IoT-related Security Requirements Breakdown

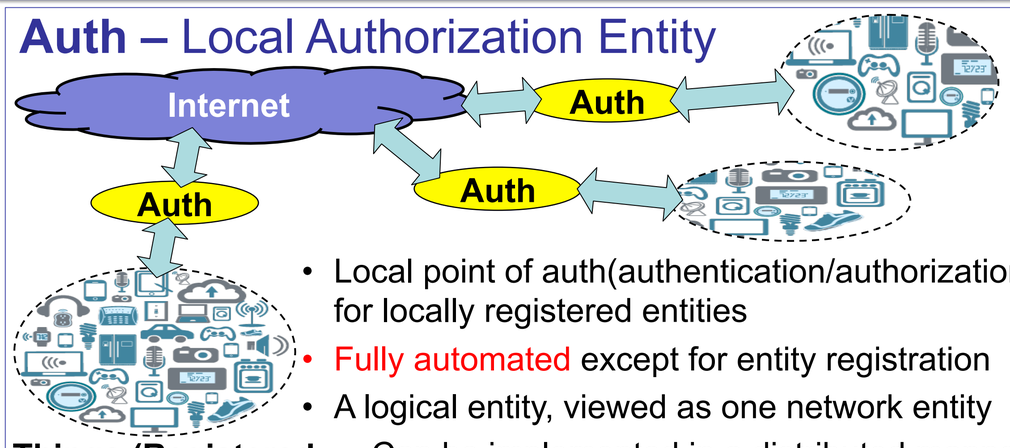
- Strong and frequent authorization & authentication for safety-critical components
- Automated mutual authentication for machine to machine communication
- Dealing with intermittent connectivity
- Support for one-to-many communication (e.g., broadcasting, publish-subscribe) for scalability
- Consideration for resource-constrained devices
- Privacy
- Dynamic entity registration

Goal

- **Organization of existing security measures with emphasis on flexibility and usability**
  - **To address IoT-related security requirements above**

Proposed Approach Overview

Auth – Local Authorization Entity



- Local point of auth(authentication/authorization) for locally registered entities
- Fully automated except for entity registration
- A logical entity, viewed as one network entity
  - Can be implemented in a distributed manner to increase availability

Auth DB – Information for Local Authorization

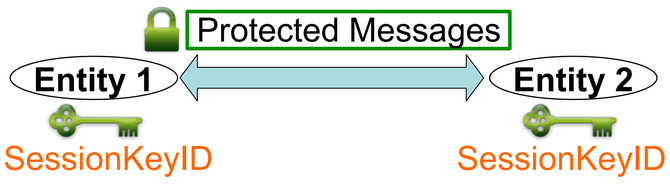
Main Database Tables
- Registered Entity Table
- Communication Policy Table
- Cached Session Key Table

Information for Each Entity
- Unique name, group
- Distribution key, key distribution conditions
- Dynamic entity registration is manageable w/ local Auth

Session Keys Generated by Auth
- Current owner(s)
- Validity periods
- Support for entities with intermittent connectivity (allow caching keys)

Specification of Secure Communication
- Cipher/hash algorithm, crypto key length, validity period
- Different communication policies to support heterogeneous security requirements
- From safety-critical entities under untrusted environment (frequent authorization) to resource-constrained devices

Session Key – For Protecting Communication

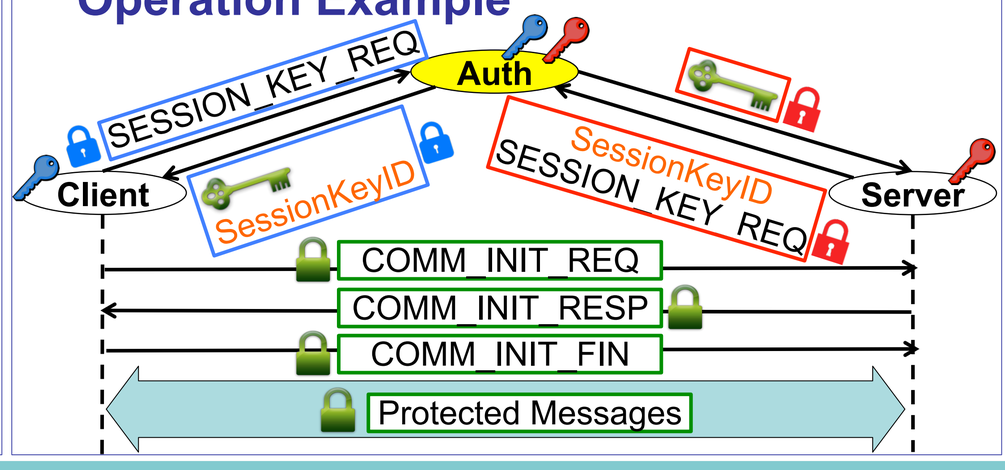


- **Symmetric crypto key for protecting a single session of communication**
  - Generated by Auth, delivered to authorized entities
  - Has a unique session key ID, specified usage conditions (cipher, hash, validity periods)

Distribution Key – For Secure Delivery of Session Keys

- **Pre-shared symmetric key to encrypt session keys**
  - Only known to Auth & entity
  - W/ specified usage conditions (cipher, hash, validity periods)
- **Updating distribution key**
  - W/ public key crypto (keys exchanged during entity registration)
  - If a resource-constrainted entity can't perform public key crypto, it can optionally use permanent distribution key without updates

Operation Example



Experiments and Results

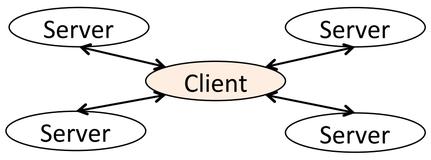
Evaluation of Scalability of Proposed Approach and SSL/TLS for following scenarios

Experimental Setup

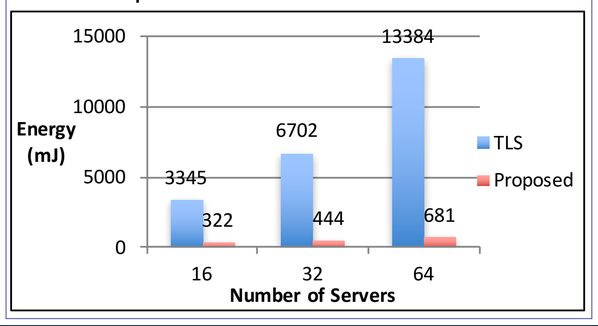
- Assume that there is a resource-constrained client/publisher which communicates with multiple servers/subscribers
- Measure security overhead of the resource-constrained client/publisher
- Convert the security overhead (network packets, cyprto operations) into energy consumption using numbers in [1],[2]

[1] Feeney and Nilsson. "Investigating the energy consumption of a wireless network interface in an ad hoc networking environment", IEEE INFOCOM 2001
[2] Rifa-Pous and Herrera-Joancomarti. "Computational and Energy Costs of Cryptographic Algorithms on Handheld Devices", Future Internet, Feb. 2011.

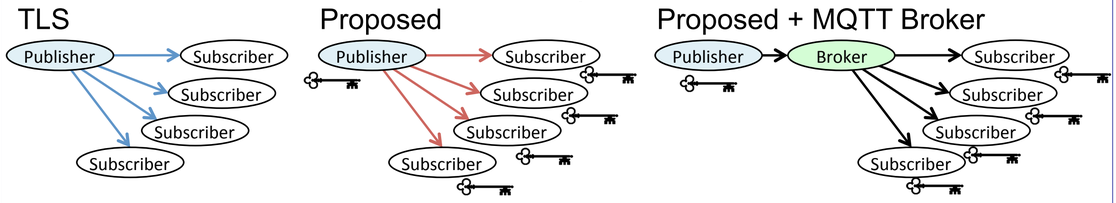
Scenario 1: A resource-constrained client and servers



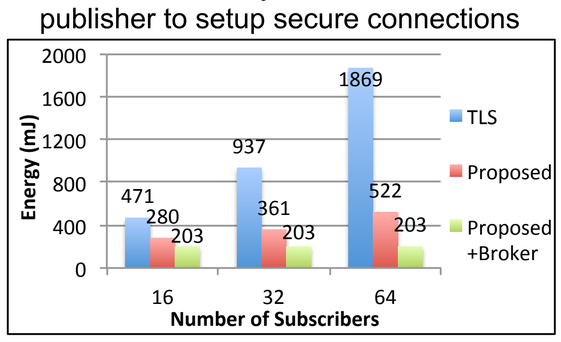
- Estimated security overhead for the client to setup secure connections with servers



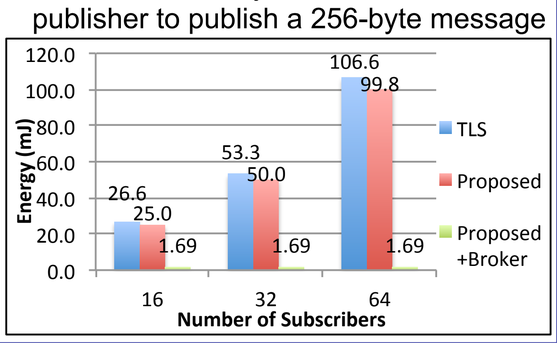
Scenario 2: A resource-constrained publisher and subscribers



- Estimated security overhead for the publisher to setup secure connections



- Estimated security overhead for the publisher to publish a 256-byte message



Sponsored by the TerraSwarm Research Center, one of six centers administered by the STARnet phase of the Focus Center Research Program (FCRP) a Semiconductor Research Corporation program sponsored by MARCO and DARPA.