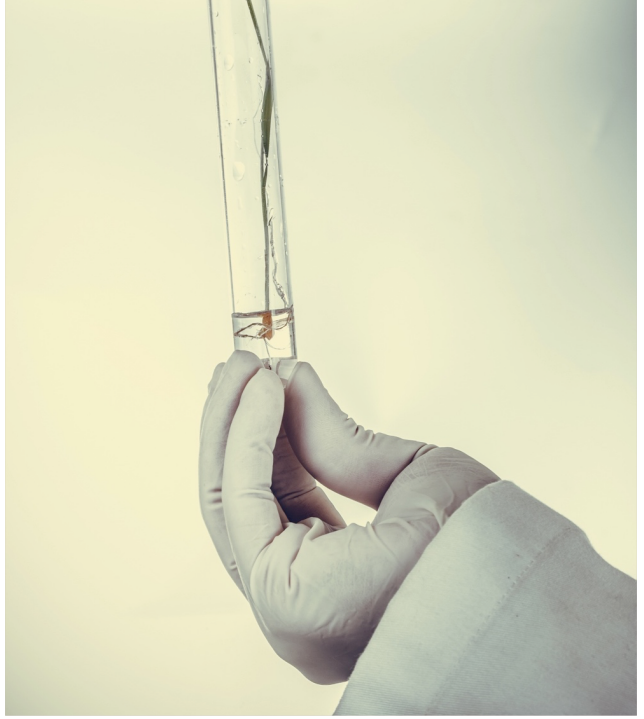
IS IOT A SECURITY NIGHTMARE?

Shahid Raza, PhD
Director, Security Lab

shahid@sics.se

Research Institutes of Sweden
RISE SICS



Three have become one - RISE

The RISE institutes Innventia, SP and Swedish ICT have merged in order to become a stronger research and innovation partner for businesses and society.

THIS IS RISE SICS

SICS → SWEDISH ICT SICS → RI.SE

Turnover 21 Million Euro

Staff 200
76 Ph.D.
32 Professors

+ 30 Years of state of the art computer science

Non-profit research organization

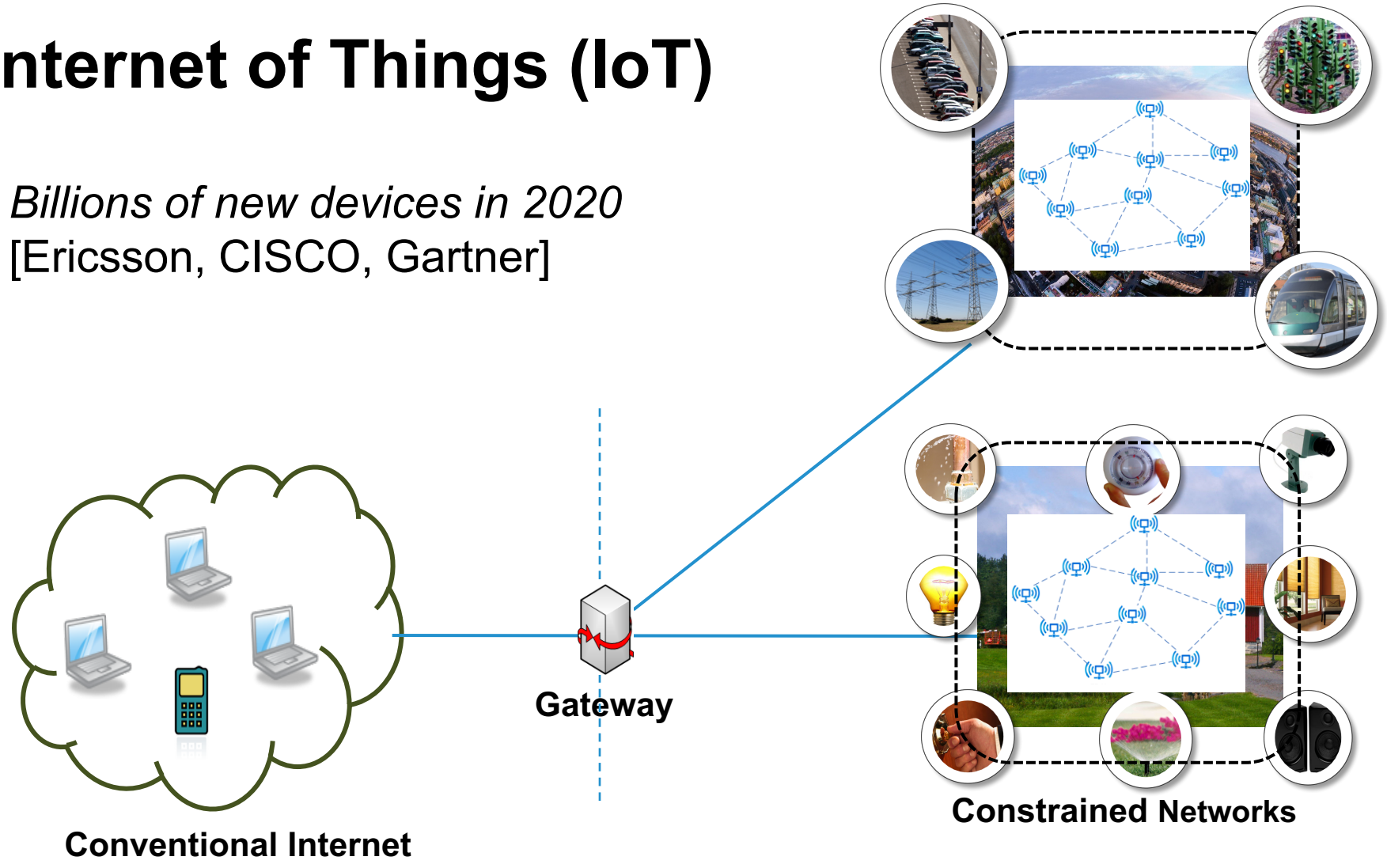
Funded by governmental research programs, industry and the EU

RI.SE

Motivation

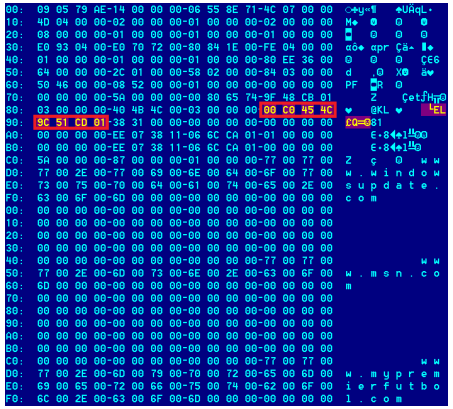
Internet of Things (IoT)

Billions of new devices in 2020
[Ericsson, CISCO, Gartner]



The Reality of IoT

- IoT manufacturers have been ignoring security in the rush to get to market first
- IoT security now is like IT security in the 1990s
- *"There is no Internet of Things, only other people's computers in your house."*
  -- Jacob Hoffman-Andrews



Attack surface increases…

Attackers now have the following options:

1. IoT Backend servers
2. IoT Gateways
3. IoT Devices
4. IoT sensors/actuators
5. The communications links between them all

RI.
SE

An Example IoT attack

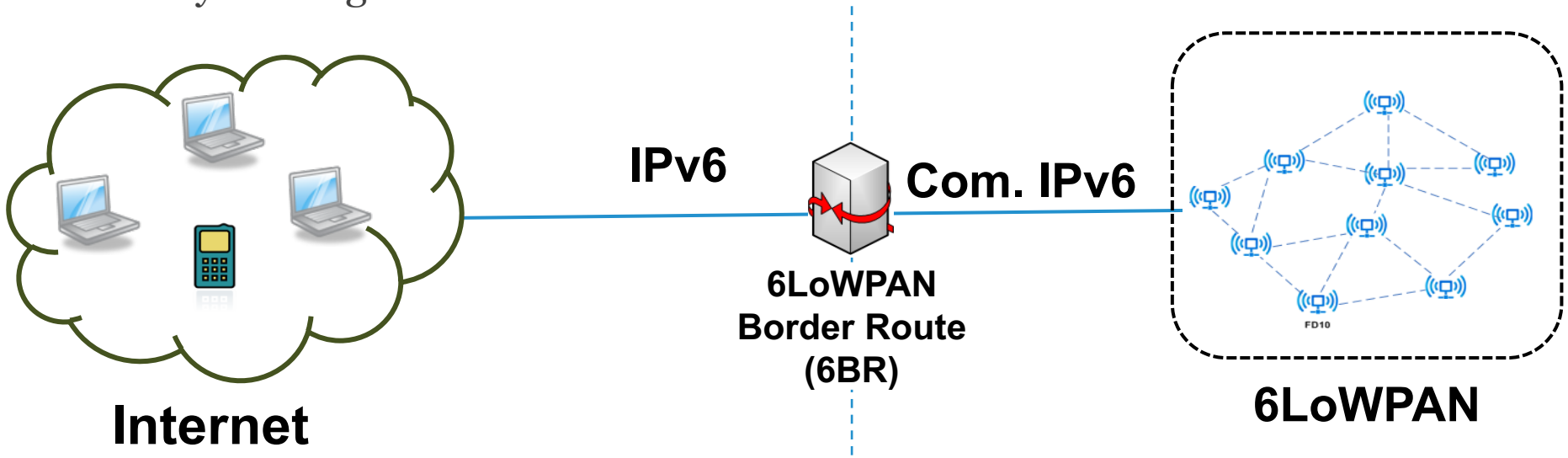
- The Mirai Botnet
  - The most impactful attack by IoT devices [October 21, 2016]
  - DNS attack (Dyn)
    - Amazon, Spotify, Netflix, Twitter, etc. successfully attacks
- An eye-opener for vendors not considering cybersecurity as a built-in component in their systems/solutions.

RI.
SE

Internet of Things (IoT)

- Network of globally identifiable physical objects/things
  - Mostly resource-constrained, lossy wireless networks
  - Multi-hop
  - Unattended deployments
  - Extremely heterogeneous

- IPv6, an IoT enabling technology and integration layer
- IPv6 over Low power Wireless Personal Area Network (6LoWPAN)

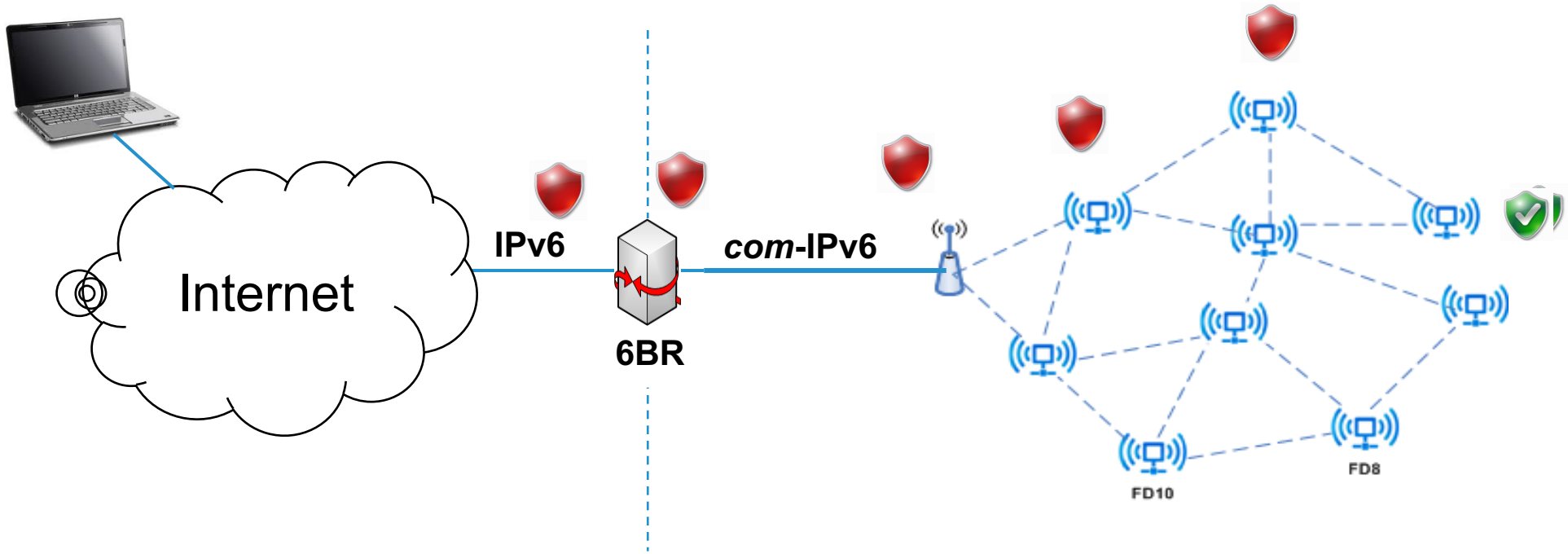


Communication Security in the IoT

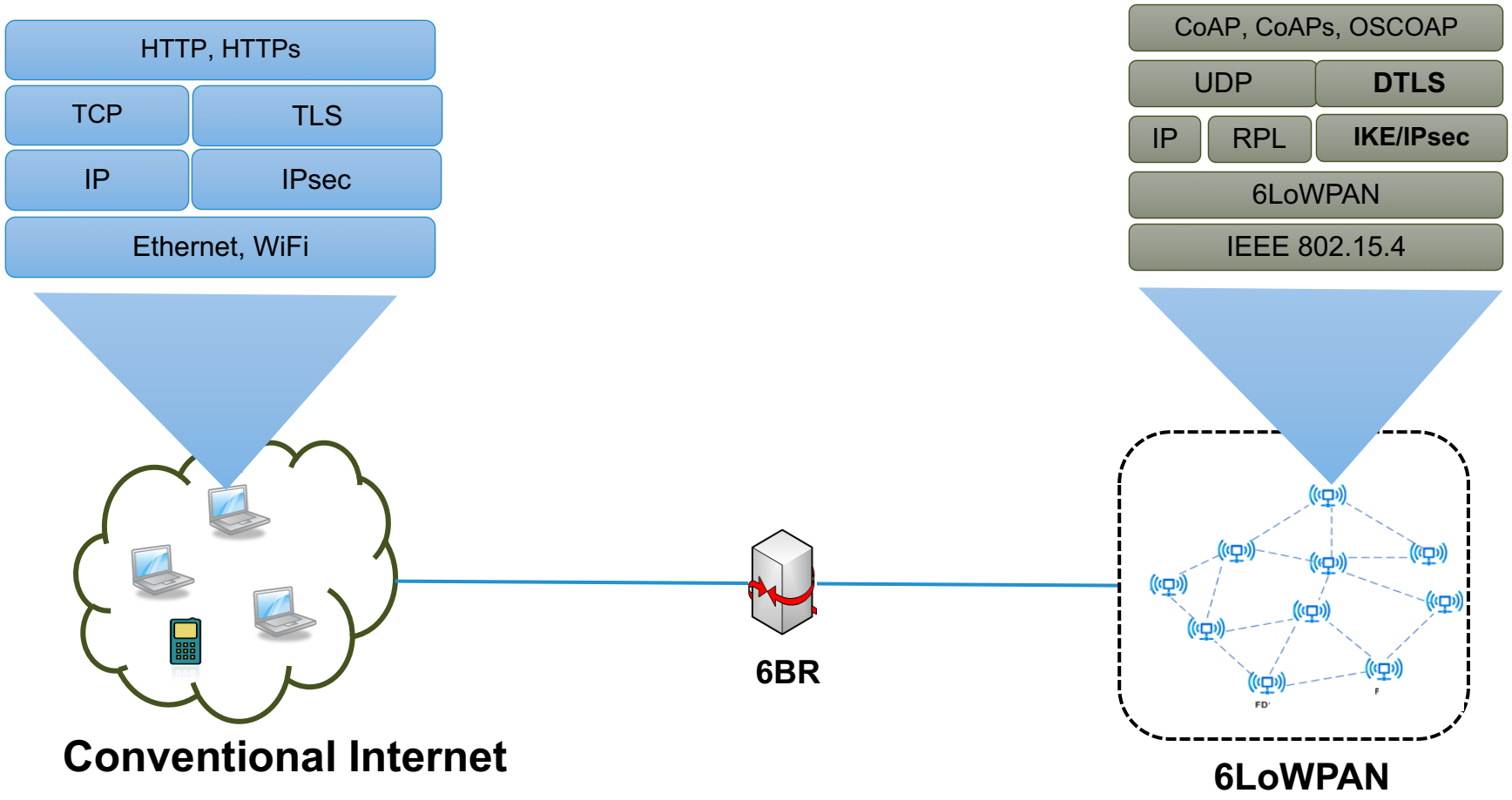
RI.
SE

Communication Security in the IoT

- Per hop security
- End-to-End (E2E) security



IoT Protocols



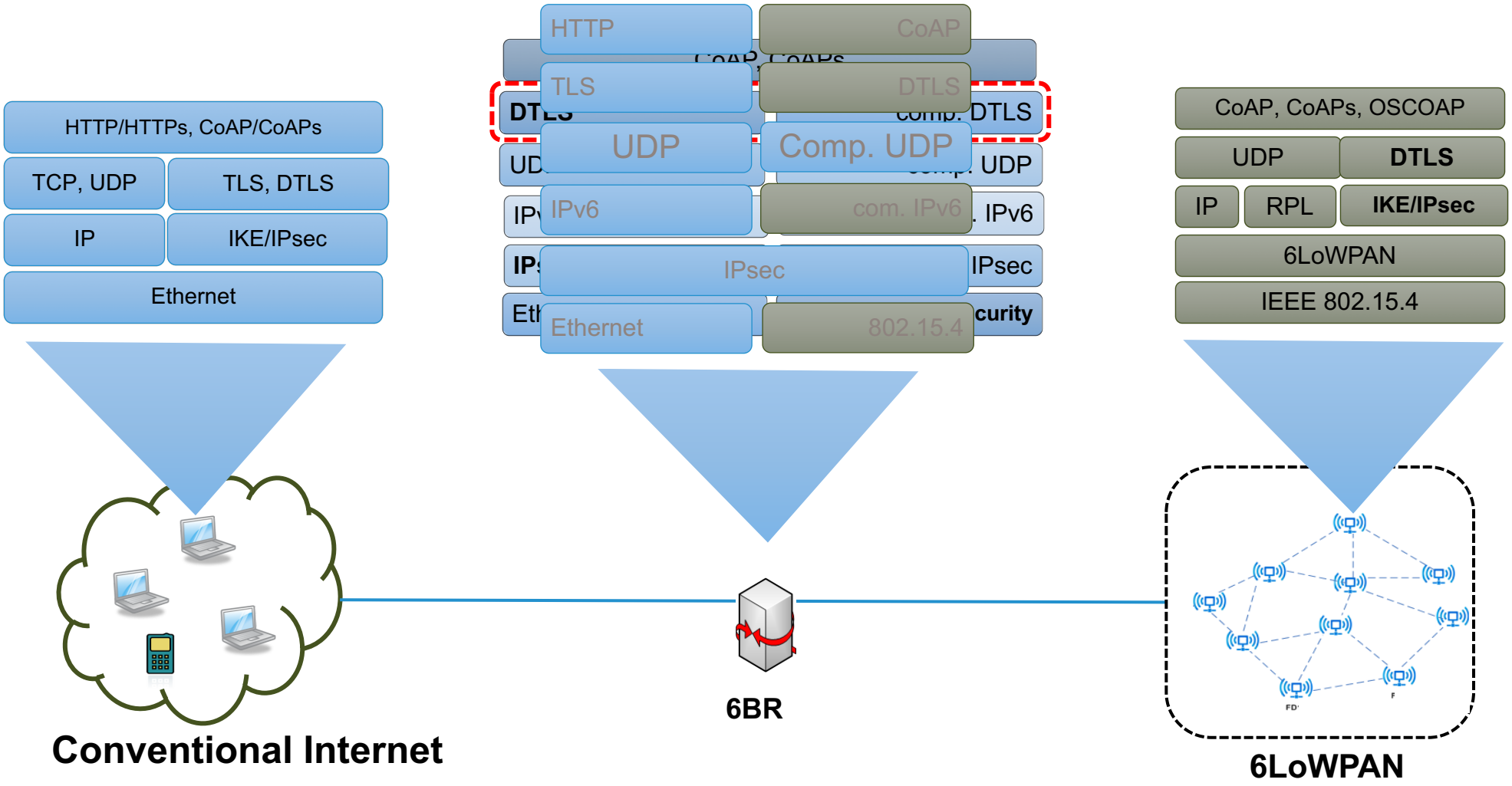
IEEE 802.15.4-based IoT Application Layer Size

- Total IEEE 802.15.4 Maximum Transmission Unit (MTU) size: 127 bytes
  - After IEEE 802.15.4 header (25 bytes): 102 bytes
  - After IEEE 802.15.4 security (21 bytes): 81 bytes
  - After IPv6 header (40 bytes): 41 bytes
  - After UDP header (8 bytes): 33 bytes
  - *Therefore, we only have **33** bytes for the UDP payload.*

- **After 6LoWPAN compression**
  - The 48 bytes IPv6 + UDP header, in the best cases, becomes 6 bytes
    - IPv6 link-local with UDP
  - *In the best case, we have **75** bytes for the UDP payload*

RI.SE

IoT and Security Protocols



Secure CoAP (CoAPs)

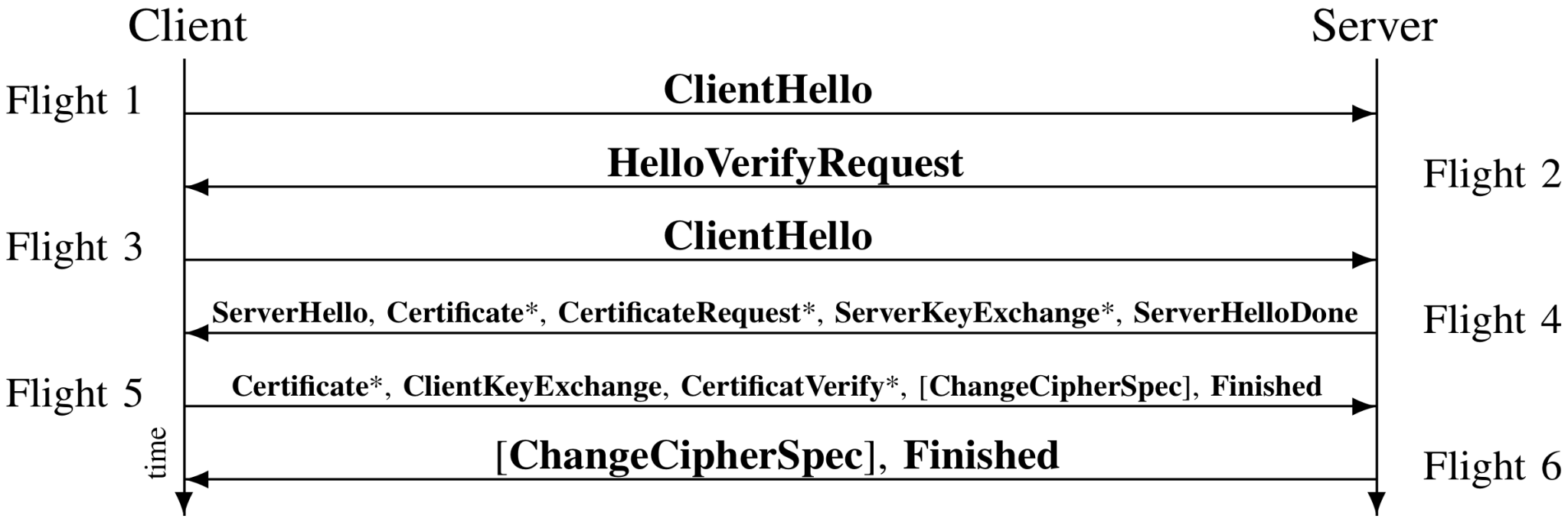
- CoAP enables secure web in the IoT
  - HTTP + TLS = HTTPS
    - Reliable and synchronous transport (TCP)
  - CoAP + DTLS = CoAPs
    - Unreliable and asynchronous transport (UDP)

coaps://mySite:port/myResource

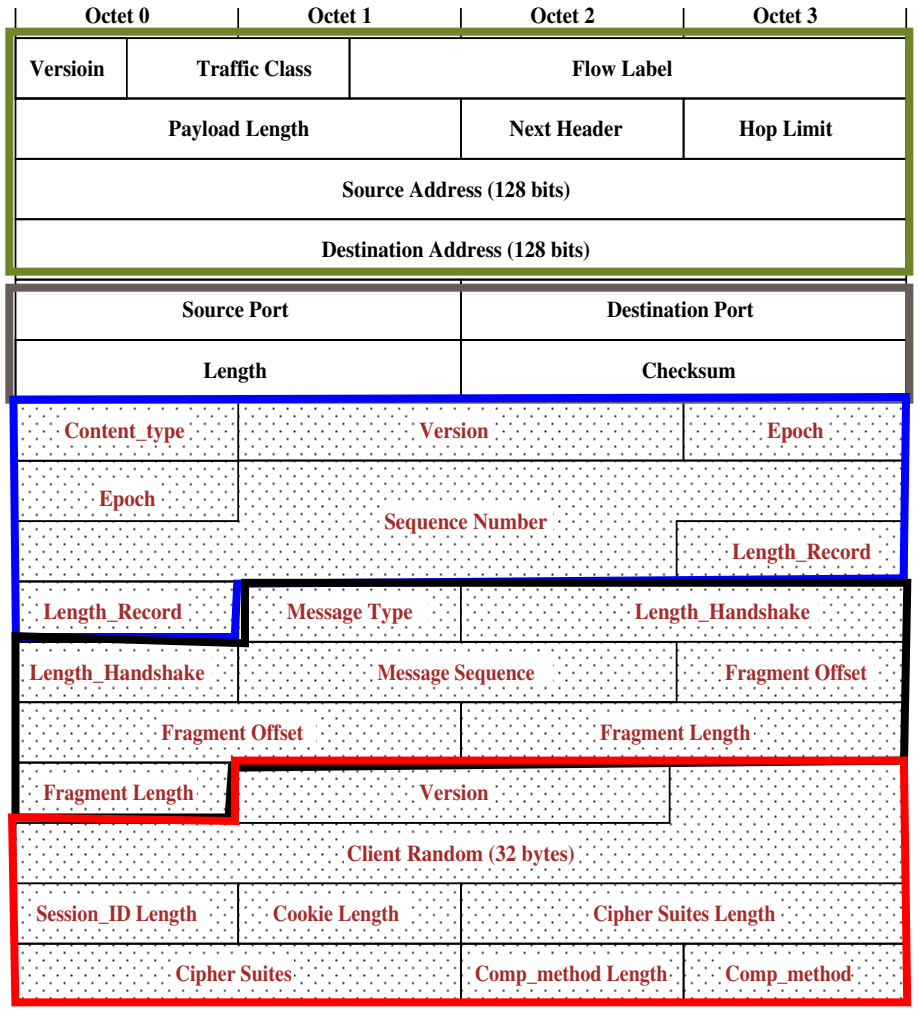
https://mySite:port/myResource

RI.
SE

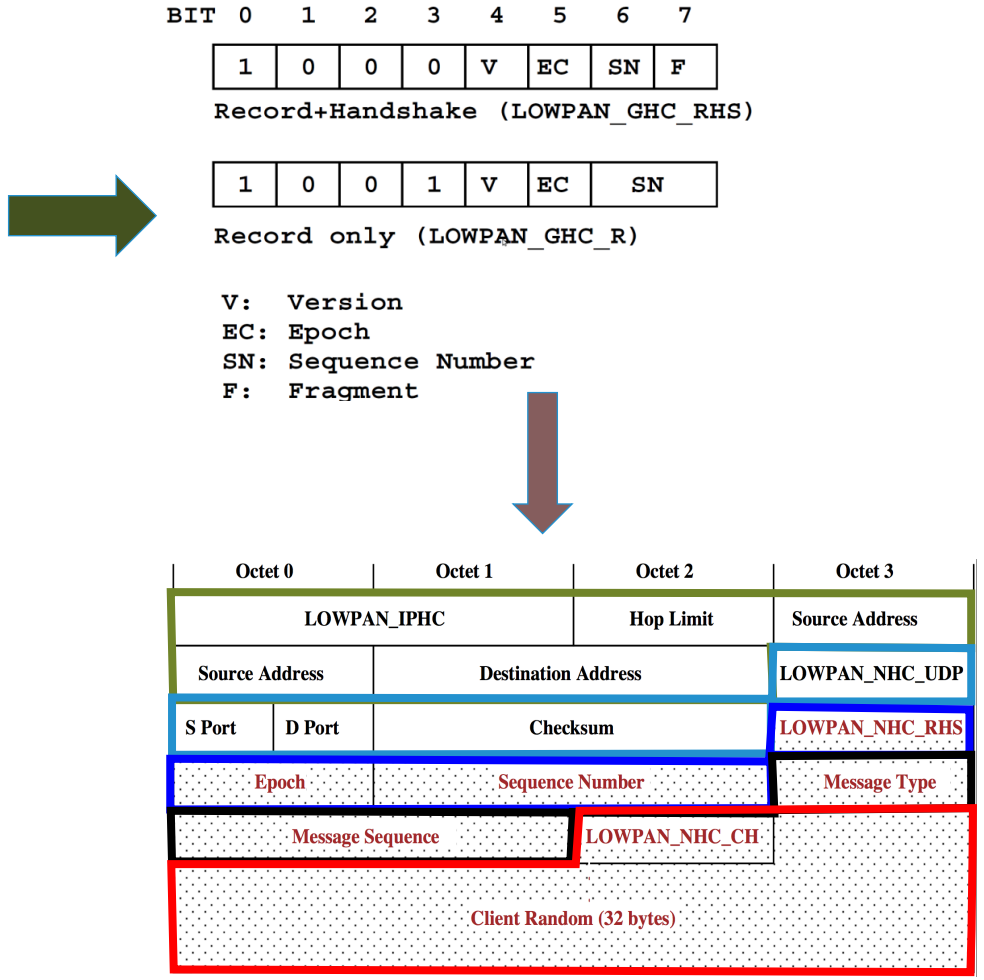
The DTLS Handshake



Extending 6LoWPAN-compression to DTLS



IP Datagram with ClientHello



Compressed ClientHello

Lightweight DTLS

- Example: *IP datagram with ClientHello*

Protocol	Uncompressed [bytes]	Compressed [bytes]
IP	40	7
UDP	8	4
DTLS Record	13	7
DTLS Handshake	12	
ClientHello (Minimal)	42	17
Total	**115**	**35**

Shahid Raza, et al., *Lithe: Lightweight Secure CoAP for the Internet of Things*. IEEE Sensors Journal, 13(10), 3711-3720, October 2013.

RI. SE

Lightweight DTLS

- Header size comparison

DTLS Header	Without Compression [bit]	With Compression [bit]	%Saving
Record	104	40	62%
Handshake	96	24	75%
ClientHello	336	264	23%
ServerHello	304	264	14%

IP security (IPsec)

- *End-to-End security at the network layer*

- Authentication Header (AH)
  - Integrity and authentication
- Encapsulated Security Payload (ESP)
  - Confidentiality and optionally integrity and authentication
  - Transport and Tunnel modes
  - Manually shared keys or use Internet Key Exchange (IKE)
  - Recommended for IPv6

https://tools.ietf.org/html/draft-raza-6lo-ipsec-04

RI. SE

IEEE 802.15.4 Security

- *Per-hop security at the link layer*

- The application controls the security required
- By default – "NO Security"
- Four types of packets
  - Beacon, Data, ACK, Control packets for MAC Layer
- NO Security for ACK packets

Shahid Raza, et al., *Secure Communication for the Internet of Things - A Comparison of Link-Layer Security and IPsec for 6LoWPAN.* Journal of Security and Communication Networks, 7(12), 2014

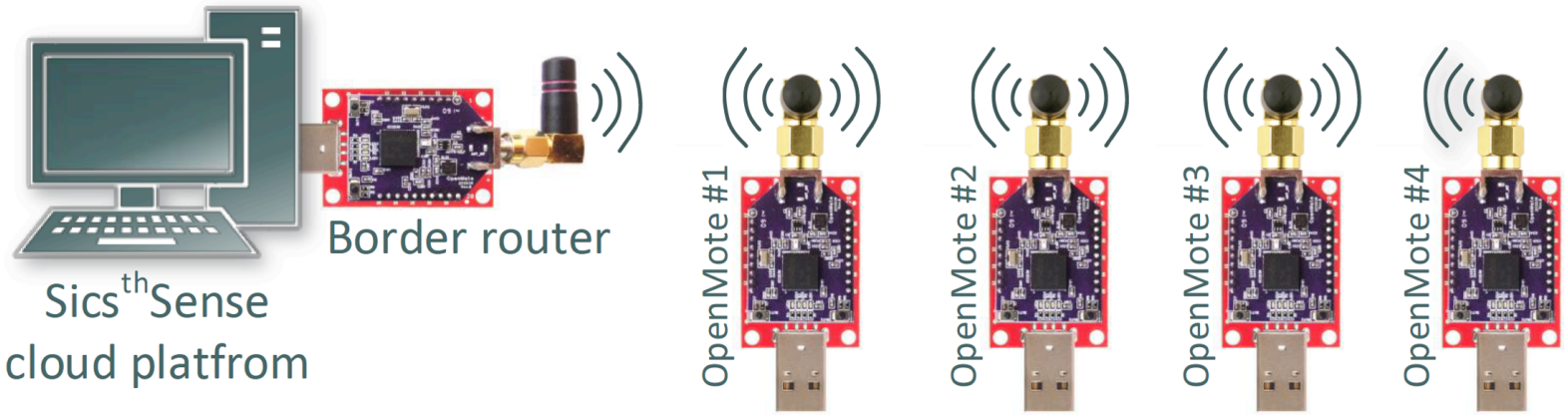
RI. SE

Lets use them

- Contiki OS
  - Open source open license operating system for IoT
  - Implementations of most IoT protocols
    - IPv6
    - 6LoWPAN
    - CoAP, RPL
    - IEEE 802.15.4
    - **IPsec**
    - **IKEv2**
    - **DTLS**
    - **Object security**
    - OAuth 2.0 (Coming…)
- SICSthSense
  - An open source and open license cloud platform for IoT

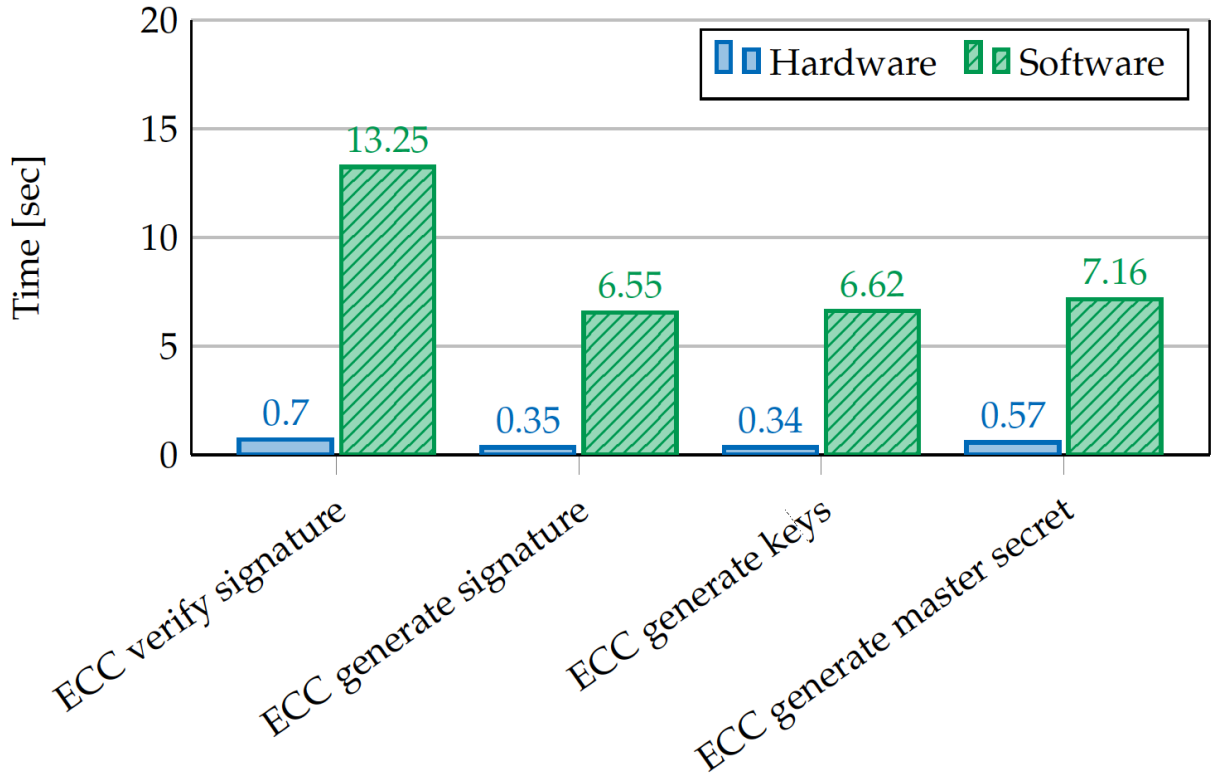
RI.
SE

Performance Evaluation



IKEv2 Vs. DTLS Handshake (Cont.)

- Using the Contiki OS and with
  - ECC
    - *With* and *without* CC2538 crypto hardware
  - Certificate-based mode



Key Management in IoT

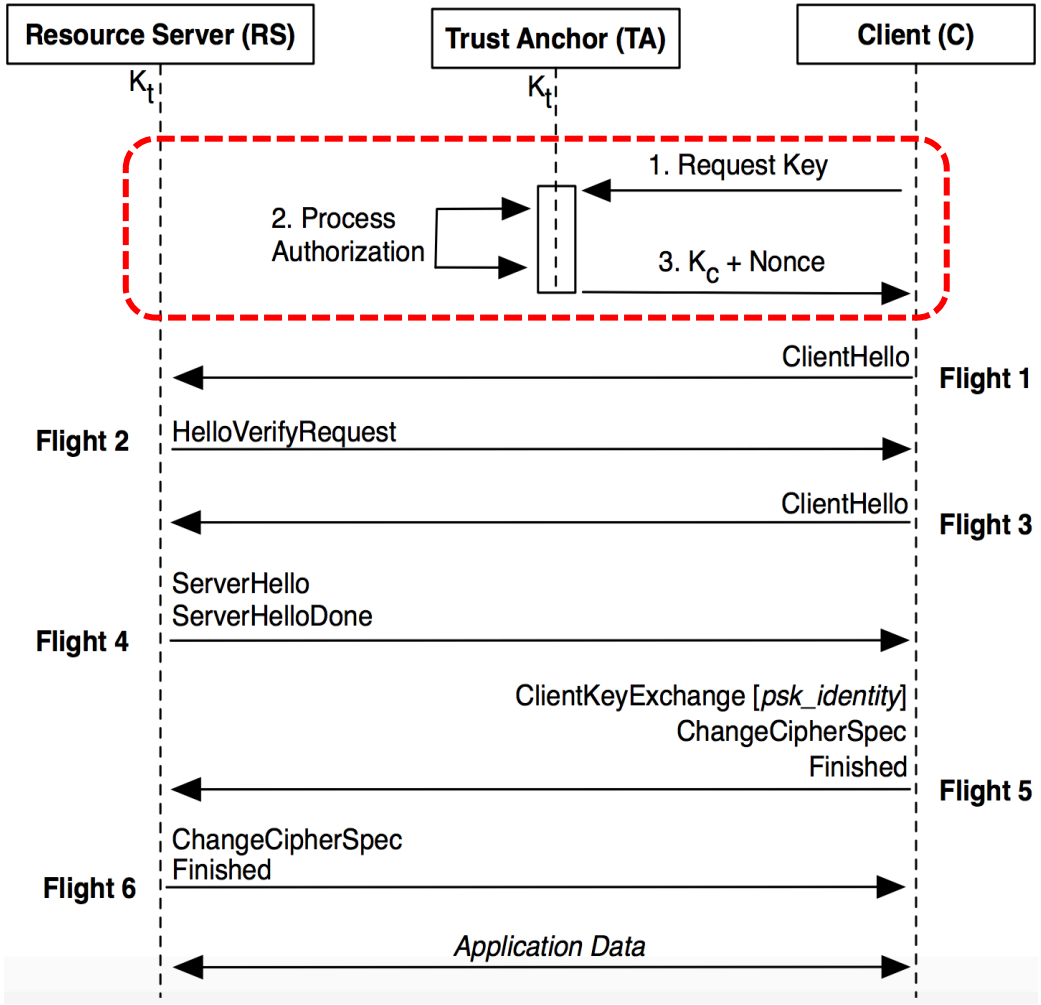
Security Modes

- Pre-shared key (PSK) – *State-of-the-art in sensor network*
- Raw-public key (RPK)
- Certificate-based - *State-of-the-art in Internet*

RI.
SE

DTLS with Scalable Symmetric Keys

- An IoT node needs to recognize and remember only one device, the Trust Anchor (TA)
- DTLS Standard compliant



Shahid Raza, et al., *S3K: Scalable Security with Symmetric Keys - DTLS Key Establishment for the Internet of Things.* IEEE Transactions on Automation Science and Engineering, 2016

Digital Certificates in the IoT

- **Certificate based cyber security protocols**
  - Datagram TLS (DTLS)
  - IKEv2/IPsec
  - Object security
- **IoT Standards specifying digital certificates**
  - CoAP
  - LwM2M
  - IPSO Objects
  - ETSI
- **Enrollment**
  - Process of certifying digital keys/certificates

A Current Research Project

- The CEBOT project: *It aims to equip IoT devices with capabilities that will enable them to obtain digital certificate(s) in a secure and automated way and by using the communication protocols that these devices speak.*

- **Partners**
  - SICS Swedish ICT, Stockholm
  - Technology Nexus (neXus)
- **Endorsers**

Husqvarna Group, Ericsson, intel, SAAB, Sustainable Innovation, yanzi networks, scypho Join the evolution

Cyber security at RISE SICS

- **IoT security**
  - VINNOVA SIP-IoT **CEBOT**
  - Eurostars **SecureIoT**
  - H2020 **NobelGrid**
  - EIT **ACTIVE**
  - Celtic-Plus **CyberWI**
- **5G Security**
  - H2020 **5G-ENSURE**
  - H2020 **5G-ENSURE-II** (in-submission)
- **Cloud security**
  - H2020 **COLA**
  - H2020 **PaaSword**
- **Software security / Virtualization**
  - VINNOVA UDI **SECONDS**
  - ARTEMIS **EMC²**
  - SSF **PROSPE**
  - SICS Internal **Ransomware**
- **Blockchain**
  - Funding by a SICS internal project
  - A couple of proposals in-submission

Network and Data Security in the IoT

- **Secure Storage in the IoT**
  - *Fusion: Coalesced Confidential Storage and Communication Framework for the IoT.*
    Journal of Security and Communication Networks (Wiley), March 2015.

- **Network Security in the IoT**
  - *SVELTE: Real-time Intrusion Detection in the Internet of Things.*
    Ad Hoc Networks (Elsevier), 11(8), 2661-2674, November, 2013

RI.
SE

THANKS…

Shahid Raza, PhD
Director, Security Lab

shahid@sics.se

Research Institutes of Sweden
RISE SICS

Med stöd från:

VINNOVA

Energimyndigheten

formas

STRATEGISKA INNOVATIONS-PROGRAM