IoT Security

Strong Security for Constrained Devices

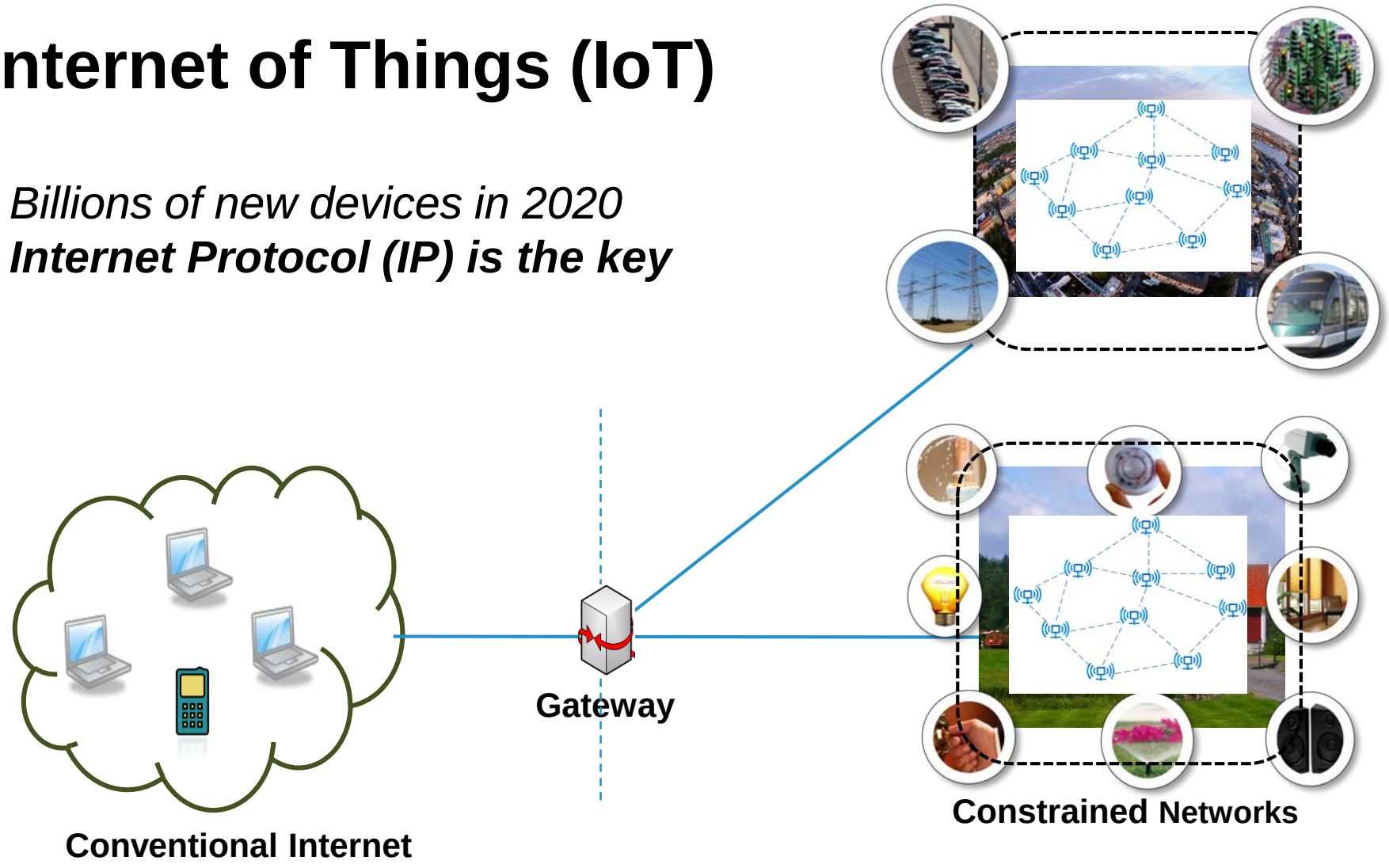
Shahid Raza
Director of Security Lab @ RISE SICS

RISE Research Institutes of Sweden
ICT
SICS

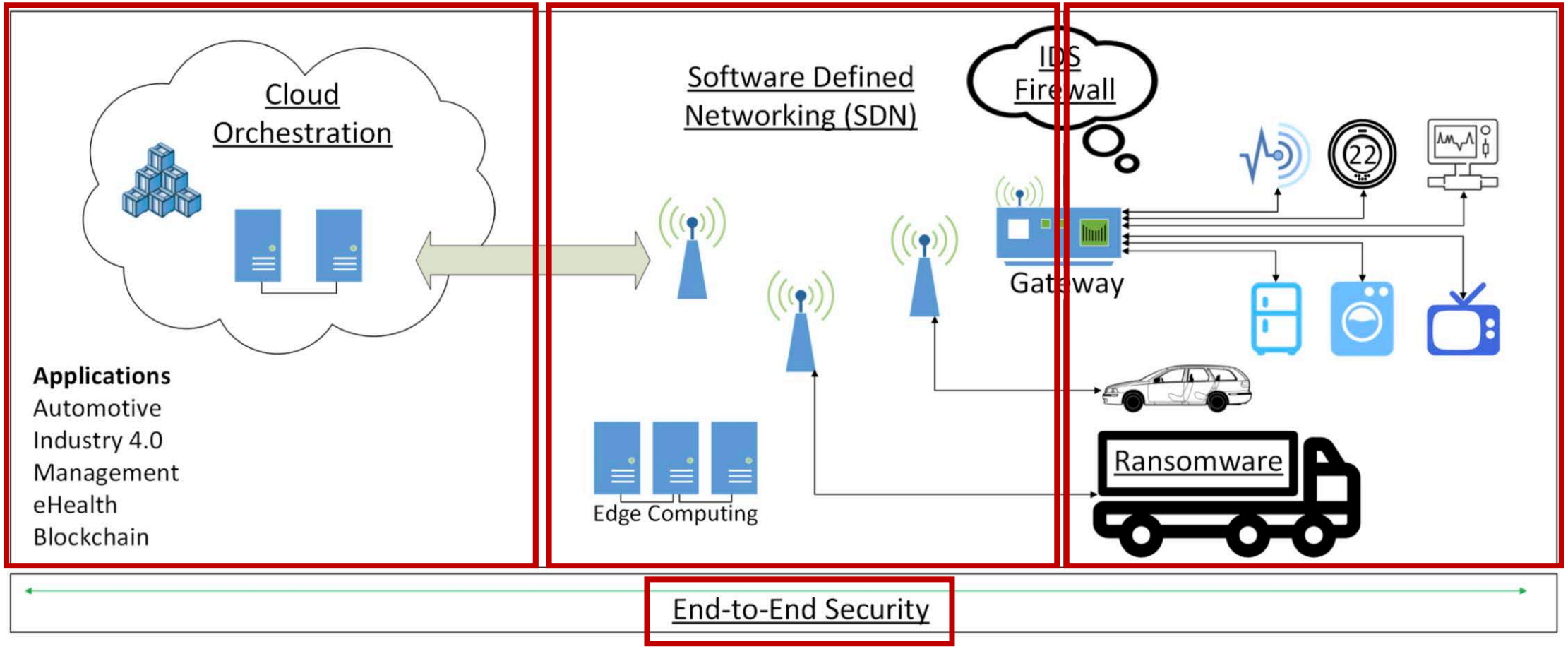
Internet of Things (IoT)

Billions of new devices in 2020

Internet Protocol (IP) is the key



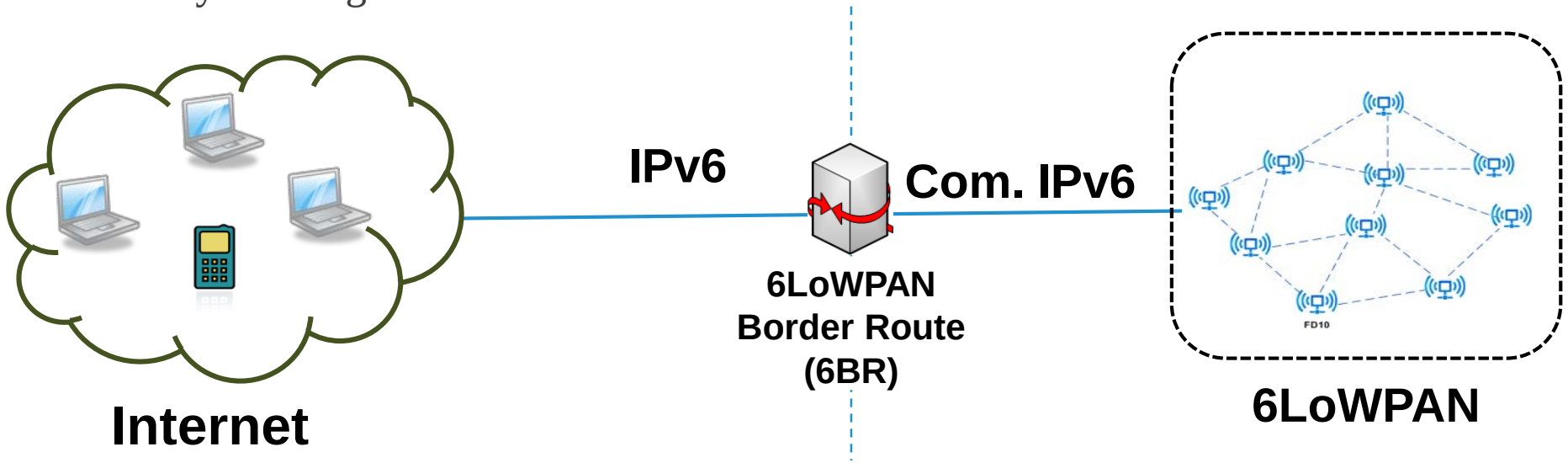
An typical IoT Architecture



Internet of Things (IoT)

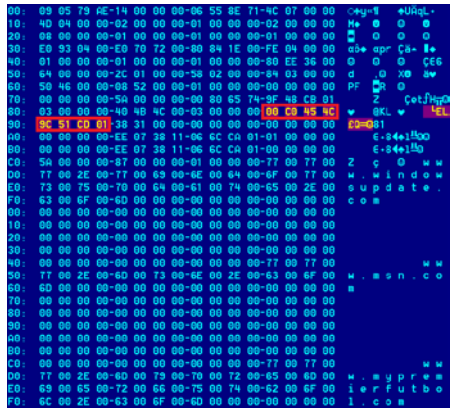
- Network of globally identifiable physical objects/things
  - Mostly resource-constrained, unreliable wireless links
  - Multi-hop
  - Unattended deployments
  - Extremely heterogeneous

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



The Reality of *deployed* IoT Security

- IoT security now is like IT security in the 1990s
- IoT manufacturers have been ignoring security in the rush to get to market first
- *"There is no Internet of Things, only other people's computers in your house."*
  -- Jacob Hoffman-Andrews
- Recent attacks are changing the mindset (*security is not an add-on*)



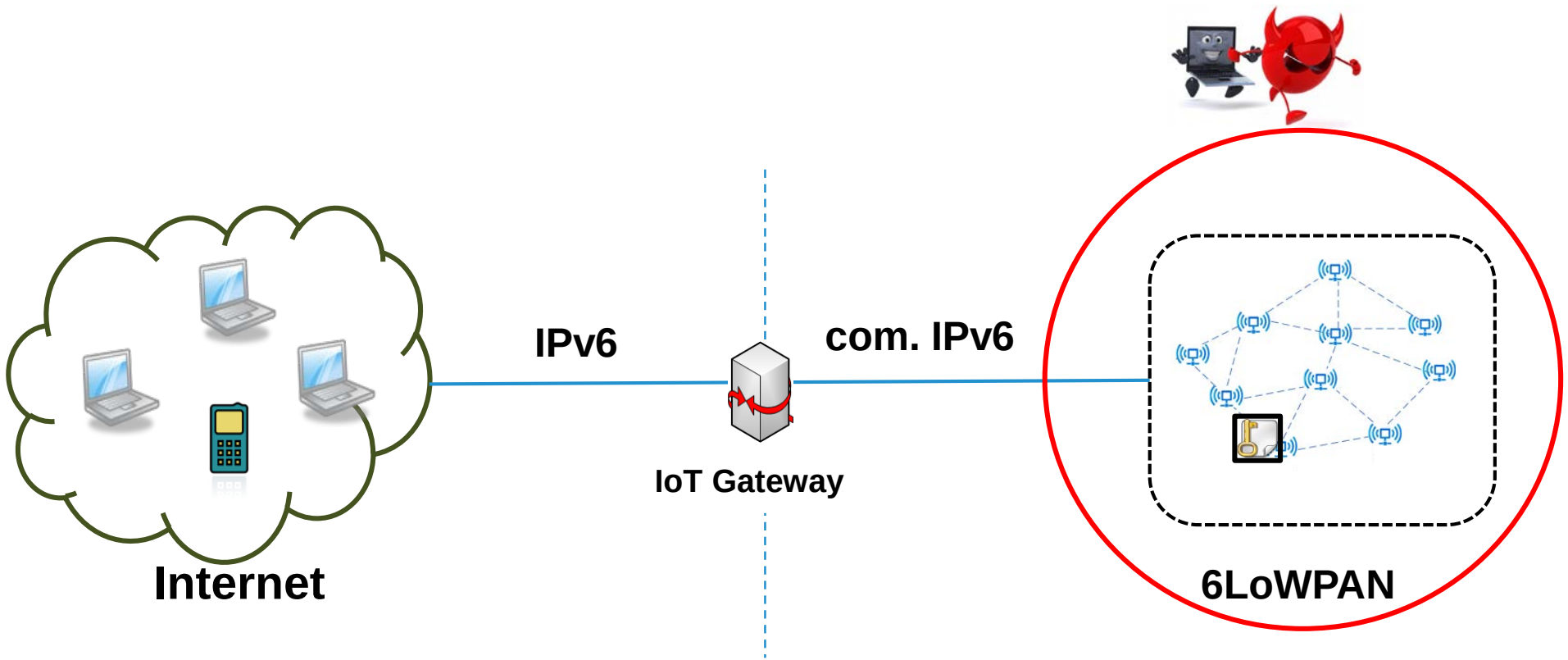
An Example IoT attack

- 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

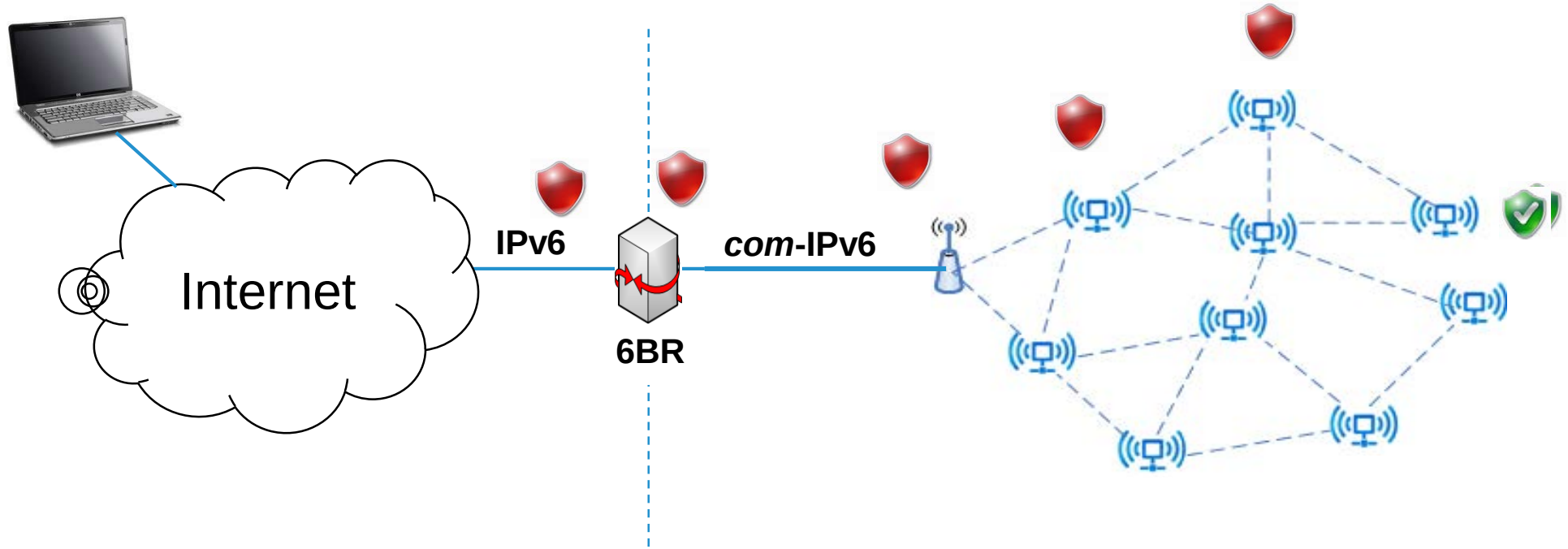
IoT Security

- **Communication Security**
  - Confidentiality
  - Integrity
  - Authentication
- **Network Security**
  - Availability
- **Data-at-rest Security**
  - Confidentiality
  - Integrity
  - Access Control

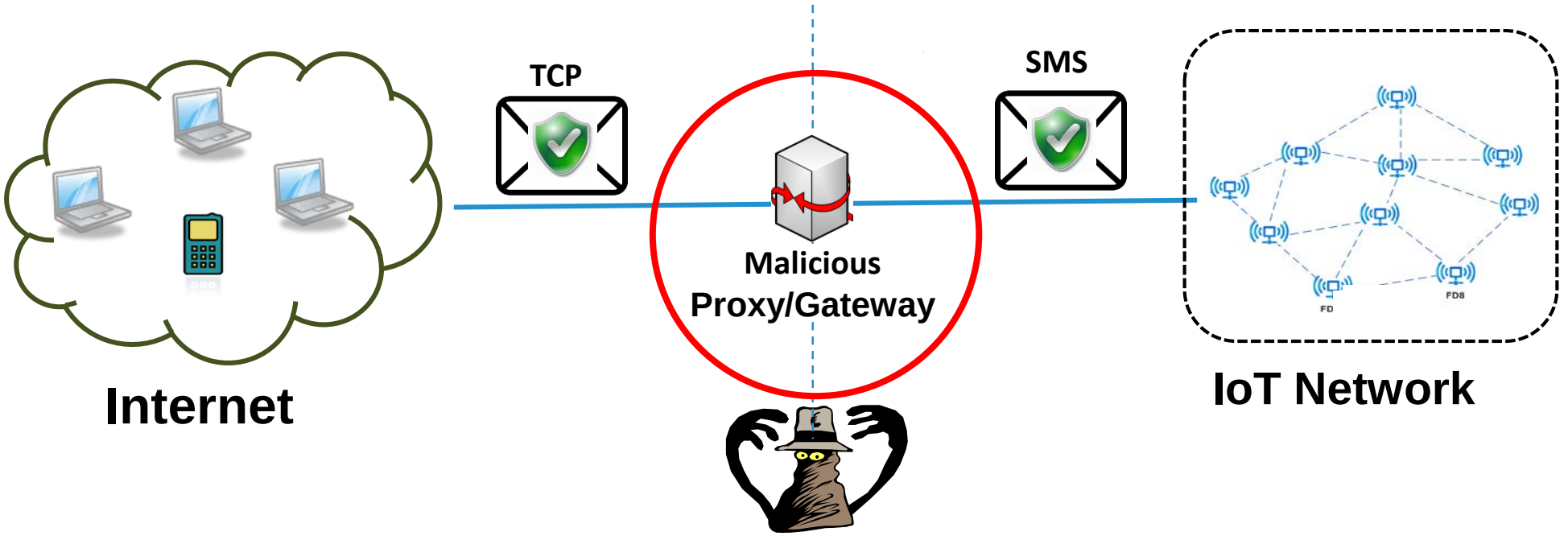


Communication Security in the IoT

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



IoT Security – **OSCORE**
E2E security with malicious gateways



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

IoT Security – what is really missing or being done?

- **Identity/Key Management**
  - IoT security is hard NOT because there exists no cryptographic protocols that meet communication security requirements, BUT because *management of secure identities/credentials (symmetric keys, passwords, PINs, certificates) using available solutions is simply not suitable for billions of heterogeneous devices.*
- **Personal data protection – e-privacy and GDPR**
- **DDoS protection**
  - IDS and firewalls
  - To/From IoT devices
- **Software Updates for IoT**
  - IETF SUIT WG

RI. SE

Key Management in IoT

- **Security Modes**
  - Pre-shared key (PSK) – *State-of-the-art in sensor network*
  - Certificate-based - *State-of-the-art in Internet*

Digital Certificates for IoT

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

PKI4IoT: Public Key Infrastructure (PKI) for IoT

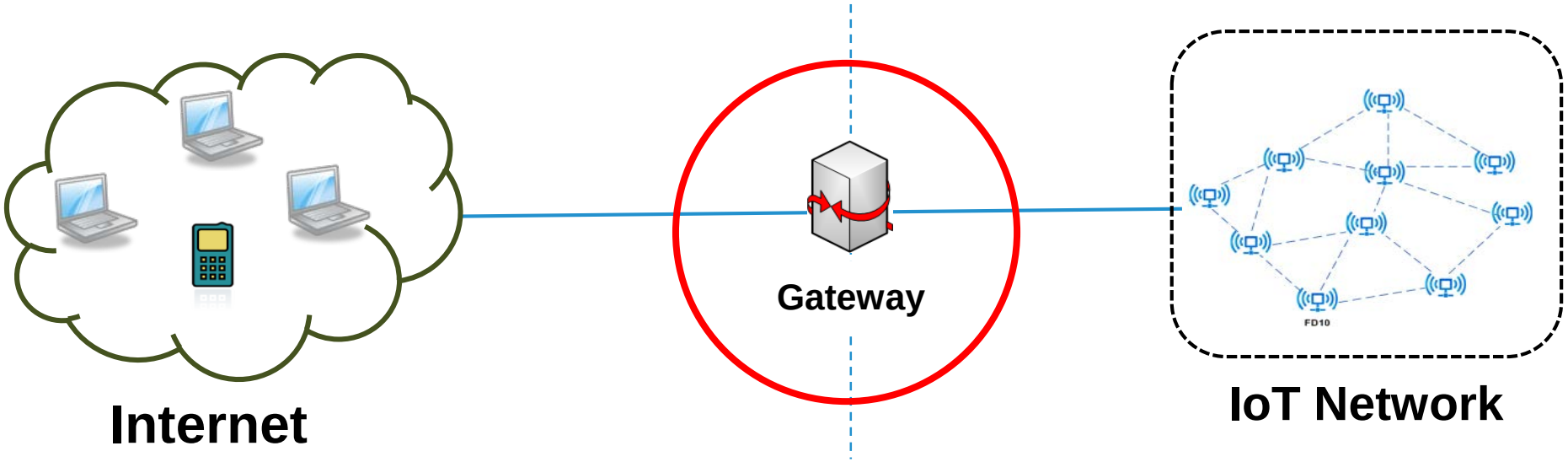
- Lightweight X.509 certificates for IoT
  - *The digital certificate size is a bottleneck*

- Certificate Enrolments for IoT
  - *Existing process of getting a certificate from CAs is not feasible for IoT*

RI. SE

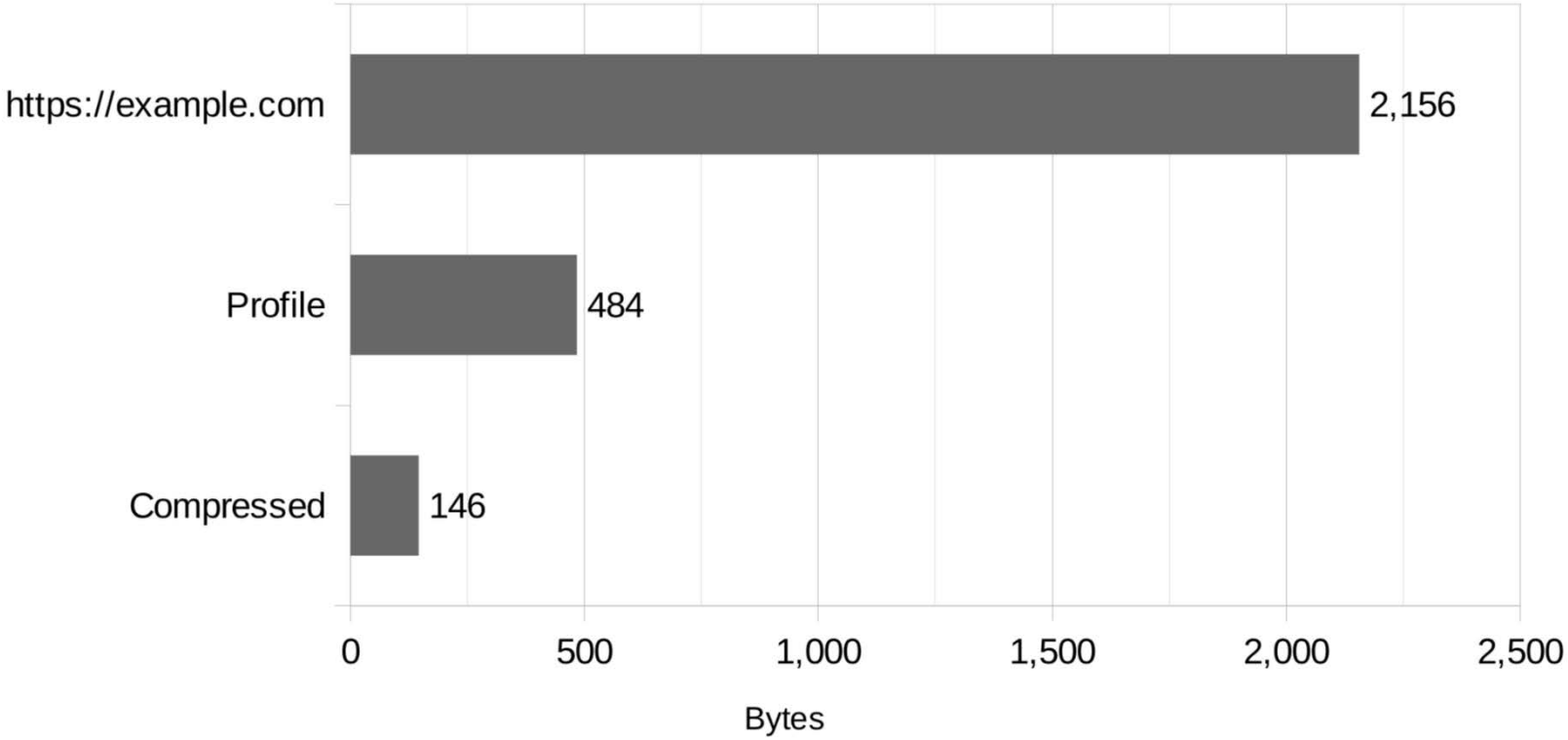
Current PKI offerings for IoT

- Delegated to a more powerful node, such as an IoT gateway
- Do not support IoT protocols



PKI4IOT - X.509 Certificates for IoT

- Lightweight but standard-compliant certificates



Filip Forsby et al.. *Lightweight X.509 Digital Certificates for the Internet of Things*. 4th International Conference on Safety and Security in Internet of Things, November 6, 2017, Valencia, Spain

PKI4IOT - Certificate Enrollment

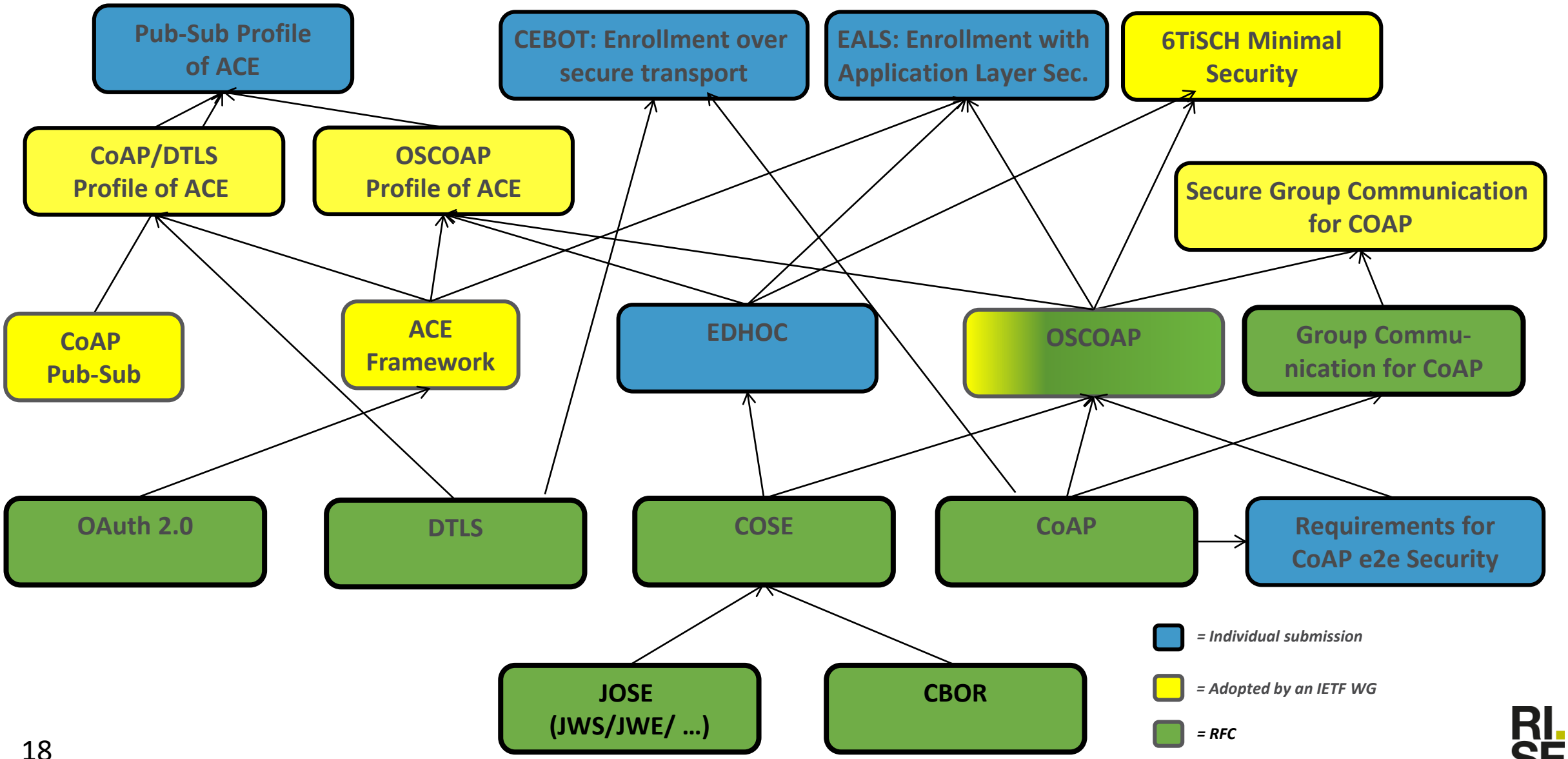
It equips IoT devices with capabilities that enables them to obtain digital certificate(s) in a secure and automated way and by using the communication protocols that these devices speak.

Certificates for constrained IoT devices (CEBOT)

- EST designed for CoAP using DTLS and IPv6

  https://www.ietf.org/id/draft-ietf-ace-coap-est-00.txt

IoT Security Standardization at IETF

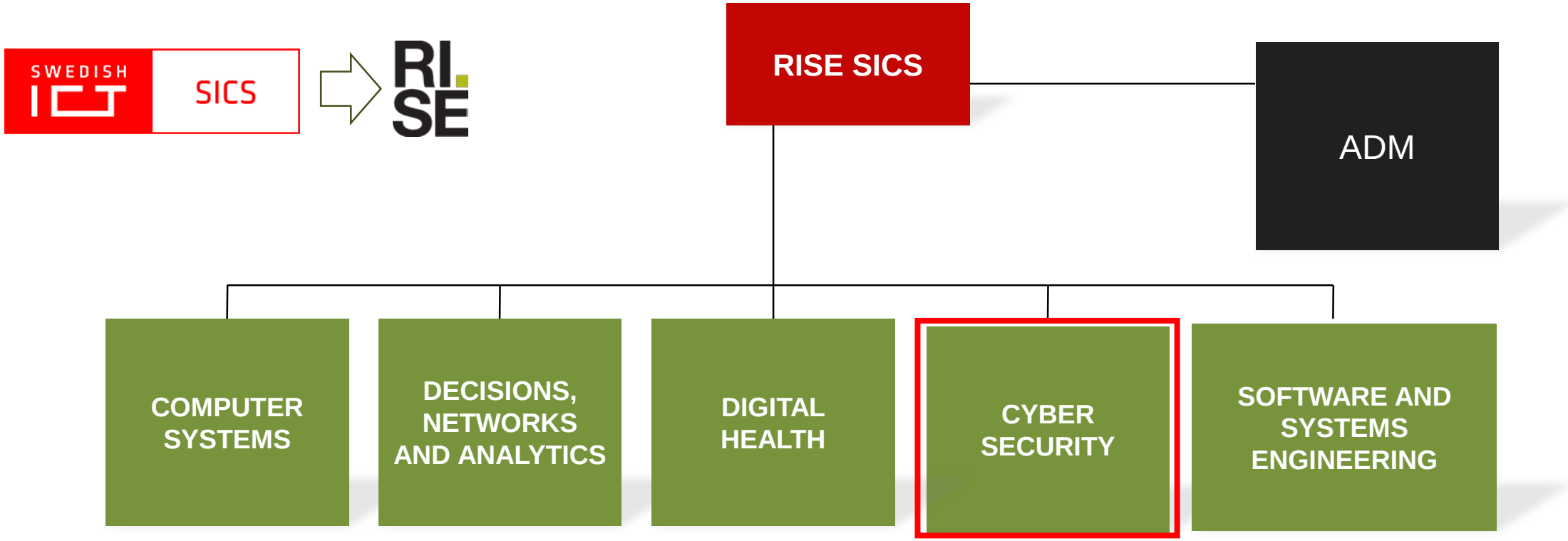


THANKS…

RISE Research Institutes of Sweden

RISE SICS

RISE SICS



Among the largest security groups in Sweden

- 16 members
- Two locations (Stockholm, Lund)

Featured security research areas and projects