Authentication and key management in Internet of Things domain

Department of Computer, Control, and
Management Engineering Antonio Ruberti

Sapienza
Università di Roma

Stefano Milani

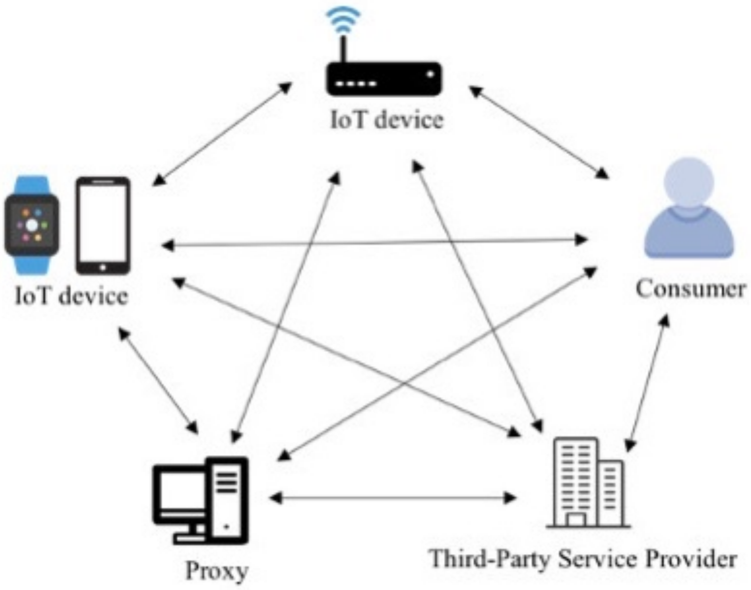
Why key management is needed

- IoT enables a constant transfer and sharing of data among users and things
- Authentication, authorization, access control and non-repudiation are essential to ensure secure communication
- How the approaches used in the Internet changes when applied in the IoT world

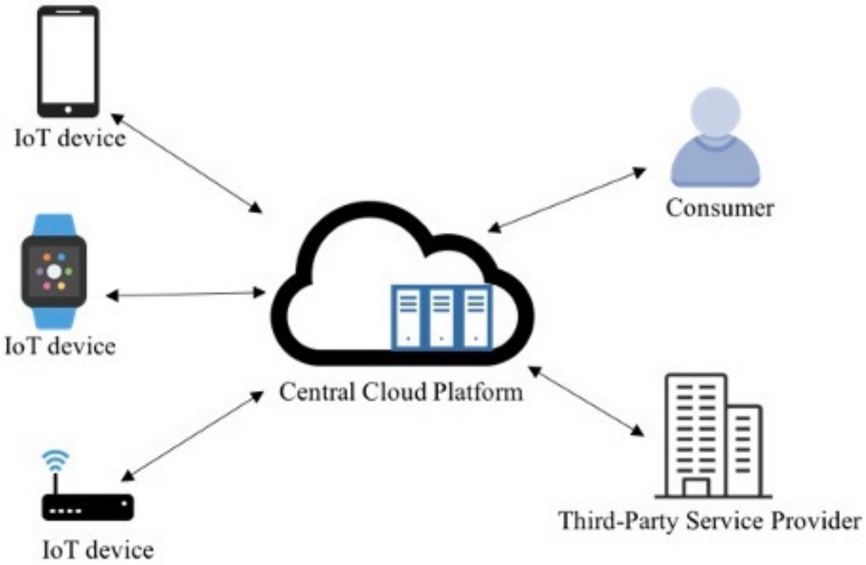
Problems in IoT domain

- Devices with limited resources such as CPU, memory and energy budget
- Lossy network with low bandwidth
- Existing IP-based protocols are feasible?

Two main approaches



Distributed IoT System



Centralized IoT System

Distributed approach

Need some sort of handshake between entities

- Certificate
- Asymmetric encryption/decryption
- Agreement of a key

Internet Key Exchange (IKEv2)

- Allows to establish a SA between two entities
- Certificate-based authentication, agreement of a common encryption model
- Supports a lot of cipher (AES)
- Based on UDP

Host Identity Protocol (HIP)

- Introduce Host Identity (HI) name space
- Based on public key infrastructure
- IP address replace with HI
- Resistant to DoS and MitM attacks

Elliptic Curve Cryptography

- Alternative to DH and RSA key exchange
- Require less computation power
- Smaller key size for equivalent security level
- Largely used in wireless scenarios
- Adapts to Identity-based encryption

Centralized approach

- Single entity manages the devices and keying material
- Preconfigured keys or certificate
- Single point of failure
- Now the most used approach

PANA

- **Pac** PANA Client
- **PAA** Authentication agent
- **AS** Authentication Server
- **EP** Enforcement Point

LoRaWAN

- AES-128 in counter mode (CTR)
- Pre-shared keys
- Two authentication methods

Activation by Personalization

- Authentication data hard-coded into the device
- No join procedure required
- LoRaWAN Network Identifier, Network Address
- Cryptographic session key

Over-The-Air Activation

- End-Device Identifier, Application identifier and Application Key needed to be hard-coded
- Used to derive two keys: NwkSKey and AppSKey
- No mechanism to update the session keys
- Need to restart to whole process

References

- Security Challenges in the IP-Based Internet of Things
- Security, privacy and trust in Internet of Things: The road ahead
- Enhancing LoRaWAN Security through a Lightweight and Authenticated Key Management Approach
- The advantages of Elliptic Curve Cryptography for wireless security