Security for Battery Efficient IoT

ETSI Challenging IoT Security & Privacy Workshop

Steve Kohalmi, October 22, 2018
The Power Problem: 10 Years on Two AA Batteries

- IoT use cases are different
  - Widely distributed monitors and sensors
  - Mobile asset tracking
  - Industrial automation and fleet management
- Constrained devices
  - Low everything: power, cost, data rate, complexity
  - But not low security
- Cannot sustain the old model
  - Radio
  - Control
  - Security
Addressing IoT in Cellular Networks

- Radio and signaling
  - Enhanced Coverage GSM (EC-GSM)
  - LTE-M (Cat-M)
  - Narrow Band IoT (NB-IoT)
- Cellular IoT EPS optimizations
  - Small, non-IP data transport via control plane (DoNAS)
  - Reduced signaling
- BEST – Battery Efficient Security for very low Throughput IoT
  - TS33.163 release-15
- 5G phase 2: studies of IoT features are just starting
  - Evolution of Cellular IoT security
  - Authentication and key management for applications based on 3GPP credentials
The Goals for BEST

• Work seamlessly with NB-IoT and LTE-M
• Power efficiency: over-the-air & compute cycles
• Support both IP and non-IP data
• Secure roaming
• End-to-middle and end-to-end security models
• Operator controlled IoT middle-platform
BEST – Data over User Plane

- Pre-Shared Key authentication and session keys
- End-to-Middle Secure Data Protocol (EMSDP)
  - Efficient, optimized, minimalist protocol
  - Agnostic to the Payload data type, supporting both IP and non-IP data
BEST – Data over NAS via the SCEF
BEST – Enterprise Application Service (EAS)

- End-to-end data security
- With device authentication under operator control

IoT Devices

RAN

Mobile Core Network

- MME
- HSS
- S-GW
- P-GW

IoT Application Service Providers

HPLMN Security Endpoint (HSE)

3GPP standard Control Plane
3GPP standard Data Plane
Not standardized (SGi)
BEST – Roaming

Mobile Core Network

IoT Application Service Providers

HPLMN Security Endpoint (HSE)

3GPP standard Control Plane
3GPP standard Data Plane
Not standardized (SGi)
The Case for BEST

• Untrusted data is worthless, unsecured is dangerous
• Good security is simple, but strong and thorough
• Security doesn’t have to be power hungry
• Roaming device communication doesn’t have to be insecure
• Secure the IoT; secure IoT devices communication
Thank You
BEST – Data over NAS via the User Plane
BEST – Access and Core Agnostic