M2M Security Standards: ETSI contributions

Presented by Francois Ennesser (Gemalto), ETSI TC M2M WG4 (Security WG) chair

Thanks to Contributors: M2M WG4 (Alper Yegin, Phil Hawkes, Ioannis Broustis, Yi Cheng, Phil Brown), Mireille Pauliac (3GPP), Colin Blanchard (TC TISPAN), Denis Praca (TC SCP)
Examples of M2M attacks

  - Can be identified and tracked by non-authorized persons
  - Can even be impersonated!

- Car stolen in 3 minutes using security loophole: [http://www.networkworld.com/community/node/80983](http://www.networkworld.com/community/node/80983)
  - No authentication required to duplicate electronic key!
  - Other attacks target car alarm systems and can even start cars automatically.
  - Similar attacks also performed e.g. to open automatic garage doors!

  - Transmitting meter readings (up to every 2 seconds) via HTTP, unencrypted, without authentication

  - Uses unencrypted local radio link
  - Could deliver fatal dosage!

- Heart monitor hacking: [http://www.theregister.co.uk/2008/03/12/heart_monitor_hacking/](http://www.theregister.co.uk/2008/03/12/heart_monitor_hacking/)
  - Can be turned off or forced to deliver impulse!
Securing every link in the chain

- Physical device security (e.g. tamper-resistance)
- Communication security on application level (e.g. IP encryption end-to-end)
- Modem security
- SIM / MIM / embedded Secure Element security
- Network security
- Application backend server security

> ETSI security work from 3GPP, TC TISPAN, TC SCP and TC M2M are relevant
M2M-related 3GPP SA3 activities

3GPP « Machine Type Communications » (MTC)
- SA3 is responsible for security aspects of MTC.

Deliverable: 3GPP TR 33.868 on “Security aspects of Machine-Type Communications”
- Security solutions for SIMTC (Security Improvements for Machine-Type Communications) Device Triggering included in 3GPP SA2 Rel-11 specifications.
- TR 33.868 to be completed in R12 with wider scope “Security aspects of Machine-Type and other Mobile Data Applications Communications Enhancements”
- TR completion will result in SA3 MTC-related Specification

Work Item initiated on Security Assurance / Certification
M2M Security features in 3GPP

- Secure Connection between MTC Device and MTC Server
  - Privacy
  - Security of small data transmission
  - Reject message without integrity protection
- Device Triggering enhancements
- Group based features, Congestion Control, Time Control, Low mobility, Power optimization, Monitoring
- External Interface Security
- Security of UE configuration
- Restricting the USIM to specific MTC User Equipments
Formal Threat Analysis methodology: TVRA

- Used for M2M Threat analysis
- M2M specific of detectability and recoverability added to account for multitude of unattended devices in remote locations

RFID in M2M applications: Privacy aspects

- Many M2M devices could be simple RFID chips
- Data derived may imply the identity of a person
- New notions: (un)linkability and (un)observability
ETSI TR 187 020 outlines a standardization roadmap for privacy and security of RFID.

The development of the roadmap involved analyses of RFID from a number of perspectives:

- Role of Privacy Enhancing Technologies for RFID and analysis of security threats to RFID
- Analysis of privacy and its link to behaviour
- OECD guidelines and relevant data protection
- EU directives on data protection and privacy
ETS1 TC SCP and M2M

- **TS 102 671** introduces M2M Form Factors
  - Physical or logical binding to host device
  - Hardened operating characteristics (lifetime...)
- **“eUICC”: Change of subscriptions on the field**
  - Completing Requirements stage (SCP REQ)
  - No technical limitation, but ecosystem considerations
- **Extend and management of UICCC “profiles”**
  - Main contentious point between stakeholders
  - Need to consider non Network Access Applications on UICC, e.g. for access to M2M Service Layer
ETSI TC M2M Release 1: End 2011, Rel. 2: End 2012

- Specification of an M2M Service Capability Layer (SCL) servicing M2M applications (independently of verticals) through RESTful APIs

M2M Service Layer security

- Part of TS 102 690 (Stage 2) and TS 102 921 (Stage 3)
- Support for credential bootstrapping and mutual authentication, integrity and confidentiality on M2M Gateway-to-Infrastructure Interface (mld reference point) in Release 1 and 2

The future: Migration to worldwide OneM2M Partnership

- End-to-end security & privacy service for M2M applications?
M2M Framework

M2M Device/Gateway

M2M Applications

M2M Service Capabilities Layer

Communication modules

M2M Network

M2M Applications

M2M Service Capabilities Layer

Core Network Connection

Core Network A

Core Network B

Security is out-of-scope in Release 1
M2M Service Layer Procedures

Network Bootstrap
- Provisions: names, service levels, security keys, etc...
- Can be based on 3GPP, 3GPP2, ETSI TISPAN, etc.
- Can be independent or related

Network Registration

Application Registration of D/GA on D/GSCL
- Establishes context of D/GA in D/GSCL

M2M Service Connection
- M2M Service Bootstrap
- Provisions M2M SP assigned ID and Kmr
- Mutual authentication of mId end points
- generation of Kmc
- Optional establishment of secure communication over mId based on Kmc and sub-keys of Kmc
- Establishes context of DGSC in NSCL and vice versa

SCL Registration of D/GSCL with NSCL

mId Security (Optional) secure communication over mId

Application Registration of D/GA on D/GSCL
- D/GA interaction with local D/GSCL

AND

SCL Registration of D/GSCL with NSCL
- D/GSCL interaction with NSCL
- D/GA interaction with local D/GSCL
- NA interaction with local NSCL

M2M Communication via DGSCL and NSCL

Provisions M2M SP assigned ID and Kmr
- Can be independent or related
M2M Service Bootstrap Procedures

- Optional bootstrap of M2M Service Layer Credentials on the field
  - Establishment of shared secret Kmr in Device and Network, adequately protected
  - Alternative: Pre-provisioning, e.g. on UICC

- Access network (AN) dependent vs. access-agnostic
  - May derive credentials from existing AN credentials, or create independent ones

- Bootstrap procedures
  - TLS/TCP
    - Uses X.509 certificates pre-provisioned on the device/gateway
    - Access-agnostic
  - GBA
    - Uses Access Network credentials in UICC (e.g. USIM, CSIM or ISIM application)
    - Access-dependent
  - EAP/PANA
    - Uses any type of credentials (SIM, AKA, PSK, certificates, IBE, OTP, etc.)
    - Access-agnostic, unless using network access credentials (e.g., UICC with EAP-AKA)
Optional derivation of an M2M Service Connection (session) Key
- Not needed when relying on access network security (i.e., Kmc not needed)
- Interoperable UICC supporting framework elaborated in Release 2

Access Network dependent vs. access-agnostic
- Direct derivation from existing AN credentials is possible

Connection procedures
- TLS/TCP
  - Uses Kmr as PSK
  - Access-agnostic
- GBA
  - Uses Access Network credentials in UICC (e.g. USIM, CSIM or ISIM application)
  - Access-dependent
- EAP/PANA
  - Uses Kmr as PSK with EAP-GPSK (access-agnostic), or
  - Uses xSIM/UICC with EAP-SIM/EAP-AKA (access-dependent)
Securing the mIId Interface

One or more of the following methods used

- Relying on access network (i.e., lower-layer) security
- Using channel security
  - TLS (TCP) or DTLS (UDP), using M2M Connection Key (Kmc) as PSK
- Using object security
  - XML-DSIG and XML-ENC, using Kmc
Various Scenarios - Baseline

- Pre-provisioned device/gateway credential types
  - SIM/AKA credential
  - Certificates
  - Any type of credentials

M2M Bootstrap Procedures
- GBA
- TLS/TCP
- EAP/PANA

M2M Service Connection Procedures
- GBA
- TLS/TCP
- EAP/PANA

mId security methods
- TLS/DTLS (Channel Security)
- XML-DSIG/ENC (Object Security)
- Relying on Access Network Security

© ETSI 2011. All rights reserved
Support of Integrity Validation

Integrity Validation (IVal)
- optional feature enabling e.g. to detect tampering of device
- enables fine grained access control for both M2M Device/Gateways and M2M Service Providers.

Rel-1 supports IVal prior to Bootstrap and during Service Registration procedures
- Code Integrity checks performed/stored in Secured Environment
- IVal result (4 bytes):
  - Mapping device software image to standard M2M services
  - Sent to M2M Service Provider during service registration.
  - Signed with IVal key to ensure integrity and authenticity of reported results.
- The M2M Service Provider can grant or deny service access based on the reported IVal results and provider policy
Integrity Validation Call Flow

M2M Device/Gateway

- Perform IVal for Bootstrap / Connection
  - Device IVal: Bootstrap/Connection Security Policy gates whether bootstrap continues or halts

Bootstrap Procedure

Service Connection Procedure

- Perform IVal for Service Registration
  - Device IVal: Service Registration Security Policy gates whether registration continues or halts

Service Registration Request

- IVal results: 32-bit signed mapping of standard service capabilities

Service Registration Result

- Access Control based on IVal results and policies

Initiate M2M Services

M2M Service Provider

MAS/MSBF

Access granted or denied based on service provider policy

© ETSI 2011. All rights reserved
Contact Details:

francois.ennesser@gemalto.com

Thank you!