STANDARDS FOR
COOPERATIVE ITS

Steve Randall and Siv Hilde Houmb
Personal Data Protection &
ITS Workshop
Brussels, 12\textsuperscript{th} June 2012
Speakers

Steve RANDALL & Siv Hilde HOUMB

- Members of the expert team developing core ITS security and privacy standards and active participants in ETSI TC-ITS.
Outline

- ETSI’s role in ITS Standardization
- Cooperative ITS Communications
- Privacy Challenges in ITS
- ITS Privacy Concerns and Mechanisms
- Using Standards in the Protection of Identity and Privacy
- Short-term certificates as a privacy measure
- Status of ITS Privacy Standardization
ETSI

- European standards organisation specifying globally-applicable standards in ICT including fixed, mobile, radio, converged, broadcast and Internet technologies
- Independent, not-for-profit, created in 1988
- Direct member participation
- 750+ member companies and organisations from 63 countries and five continents
- Over 23,000 publications
ITS is often classified into a number of different categories, including:

- Advanced Traveller Information Systems (ATIS)
- Vehicle-to-Infrastructure Integration (VII)
- Vehicle-to-Vehicle Integration (V2V)

ETSI focuses on:

- V2V and V2I (VII) cooperative awareness in support of safer transport
- ITS-S as source of data and as processor of data
Primary role of ETSI TC ITS WG5

- Provide standardisation such that ITS is:
  - Legal, Interoperable and interworkable
  - Low risk to the user, the OEM and the “ITS Operator”
- Standardize ITS security on behalf of the ESOs
- Provide guidance on the risks involved in ITS
- Identify security mechanisms to meet operational requirements
Basic ITS Messages

- **Cooperative Awareness Messages (CAM)**
  - 5.9GHz broadcast every 100ms
  - Single hop
  - Current vehicle/device status

- **Decentralized Environment Messages (DENM)**
  - 5.9GHz broadcast, one-time only
  - Multi-hop, relayed
  - Reporting an event (e.g. accident) of interest to other vehicles/devices
Simple Collision Avoidance Scenario
Simple Collision Avoidance Scenario
Both vehicles are aware of each other’s presence and position and are able to avoid a collision.
Vehicles travelling in the opposite direction on a segregated carriageway can be ignored.
The vehicles do not need to know each other’s identity.

The vehicles need enough information to track each other in order to:
  • avoid collision (heading, size, position...)
  • distinguish one vehicle from another close by
Privacy Challenges in ITS

○ CAM payload includes privacy-revealing information
  - Identifiers across the stack (pseudonym)
  - Vehicle attributes, location, time and speed
  - Information broadcasted frequently
  - No control over the receivers

○ Need to balance details in ITS messages (specifically CAM) with privacy requirements
  - Delicate balance between safety and privacy
Privacy Concerns in ITS

- Misuse of data
- Malpractice

- Message content (e.g. vehicle length)
- Security and communication identifiers (e.g. certificate and MAC address)

- Communication overhead (e.g. sender and receiver IP address)
- Rogue RSE
Many road safety applications depend on the tracking of other vehicles.

The information necessary for collision avoidance can be used by an attacker.

It is impossible to distinguish between legitimate and illicit tracking.

ETSI’s standards provide identity protection mechanisms but cannot totally protect privacy.
ITS Privacy Objectives

- **Anonymity (pseudonymity)**
  - There should be no pointer to any real-world identity (e.g. VIN, license plate number, owner name, static IP address, etc.).

- **Long-term unlinkability**
  - It shall not be possible to link transmissions from the same vehicle over a long time period (e.g. link two transmissions broadcast on different days).
ITS Privacy Mechanisms

- Real identity never used in ITS messages
- Separation between identification and authorization
- Pseudonimity across the stack when sending ITS messages
- Authenticity of ITS messages

Short-term certificates
Short-Term Certificates

- ITS must respect and comply with the European Data Protection Directive
- However, it is unclear how to apply European Data Protection Directive to ITS stations in V2V mode
  - E.g., how often do we need to change certificates to satisfy the directive?
  - The US solution is to change certificate every five minutes
Revocation and Privacy

- It is useful to have a service to revoke certificates as devices may become compromised.
- There is an unfortunate relationship between revocation and privacy:
  - The ability to revoke certificates is a contradicting objective to privacy.
    - Example: a scheme that has perfect privacy makes it impossible to pinpoint a single device, thus there is no way to detect and revoke that device.
Anonymity is difficult as safety applications need to track and distinguish between vehicles.

Status of ETSI ITS Standardization:
- Pseudonymity across the stack
- Separation between identification and authorization
- Protection of the real identity
- Supports revocation by CRL and infrastructure-based revocation, but does not specify how
- Does not specify the frequency of certificate change
Long-term unlinkability is challenging because safety applications need to track and distinguish between vehicles.

**Status ETSI ITS Standardization:**

- Separation between identification and authorization
- Pseudonymity of sender of ITS messages
- Short-term certificates
Challenges not yet addressed by ETSI ITS Standards:

- Revocation of authorizations (long-term certificate, short-term certificates, authorities)
- Misbehaviour reporting
- Authority hierarchy and roles
- Frequency of pseudonym change
- Pseudonym change across the ITS stack
- Granularity of ITS messages contents is too fine
ITS Authorities - Overview

Authorization Authority

Enrolment Authority

Vehicle

Vehicle

ITS CAM/DENM

Authorization

Enrolment

PDA

Roadside Unit
Conclusions (1)

- ITS messages (CAM) broadcast details about vehicles (identifiers, speed, length, width, etc.)
- Safety messages need to distinguish between vehicles and track vehicles
- Perfect privacy is not possible
- Need a reasonable privacy-by-design
- Privacy concerns can be found in most network layers
ETSI ITS standards support revocation by CRL and infrastructure-based revocation, but does not specify how.

ETSI ITS standards do not specify the frequency of certificate change.
The work and analysis incorporated in this presentation has received funding from:

• EU support to ETSI’s standardisation work programme under EC/EFTA Contract reference SA/ETSI/ENTR/453/2010-09.

The authors are solely responsible for it, it does not represent the opinion of the Commission, and the Commission is not responsible for any use that might be made of information contained therein.
Thank you for your attention