

# Security and Privacy in ITS

## *ITS WG5*

### Status and a Look Ahead

Scott W. Cadzow<sup>1</sup> & Siv Hilde Houmb<sup>2</sup>

<sup>1</sup>Cadzow Communications Consulting Ltd.

ITS WG5 Chair

[scott@cadzow.com](mailto:scott@cadzow.com)

<sup>2</sup>Telenor GBD&R, Arena for Service Innovation

[Siv-Hilde.Houmb@telenor.com](mailto:Siv-Hilde.Houmb@telenor.com)

## Outline

- ❑ **ITS – from the security point of view**
  - A look at ITS from a security perspective
- ❑ **Security and Privacy**
  - Definitions – what does it concern
  - The role of security and privacy for the ITS mandate
  - Security and privacy in a standardisation context
- ❑ **Security in ITS**
  - What are WG5 worried about and how do we address these concerns?
- ❑ **Privacy in ITS**
  - What is the impact of ITS on privacy?
- ❑ **Security work in TC ITS**
  - WG5 – Results and status of work
  - WG5 - Look ahead

## ITS from a Security Viewpoint

### □ Intelligent Transport Systems

- Intelligent – able to modify its behaviour based on information received both reactively and predicatively
- Transport – anything able to move along some recognizable “way”
- System – an integration of components that offers added functionality than any of the components in isolation

### □ What is ITS meant to achieve?

- Real-time information to drivers/road users
  - Supplement road signs with real time information gained from analysis of the behaviour of other transport users and road conditions etc.
- Driving planning information
  - Ad-hoc information
  - Interactive information

## Security and Privacy

- ❑ **Security: the ability of the ITS to keep the information transmitted secure from non-intended recipients**
- ❑ **Privacy: the ability of the ITS to keep the meaning of the information transmitted secure from non-intended recipients**
- ❑ **Both are important in building trust in ITS from the involved stakeholders and the end-users**
- ❑ **Both are important in meeting the needs outlined in the ITS mandate**
- ❑ **Security and Privacy have very different repercussions and different solutions**
  - **ITS is an excellent technology for vehicle tracking – Privacy**
  - **Information might be manipulated resulting in an accident - Security**

## Security in ITS (1)

- **The role of the security work in ITS is to ensure that:**
  - **Information which should be kept secret is kept secret**
  - **Information which should not be manipulated en route is not**
  - **Critical information is not lost or distorted**
  - **ITS applications and services are accessible upon request if permitted**
  - **ITS application and services does not or cannot be used to manipulate information**
  - **.....**

## Security in ITS (2)

- ❑ **What we want to do is to prevent unwanted incidents:**
  - **Assuming we model ITS as a system containing assets where the assets may be physical, human or logical, then these assets may have weaknesses that may be attacked by threats.**
  - **The threat itself is enacted by a Threat Agent, and its invocation may lead to an Unwanted Incident, breaking certain pre-defined security objectives.**
  - **A Vulnerability is modelled as the combination of a Weakness that can be exploited by one or more Threats.**
  - **When applied, Countermeasures protect against Threats to Vulnerabilities and reduce the Risk.**

## Security-Functionality Trade-Offs

- Message manipulation**
  - **E.g. Modify traffic light signals in favour of the criminal**
    - At the same time this may be a desirable blue light service
- Message masquerade**
  - **E.g. The traffic authority has raised the speed limit**
    - But the message is from a rogue transmitter
- Traffic analysis**
  - **E.g. Knowledge of where you are may give a burglar accurate knowledge of the time a police car will arrive on scene**
    - At the same time it can be used to assist in planning time of arrival for blue light services
- And so on ...**

## Privacy in ITS (1)

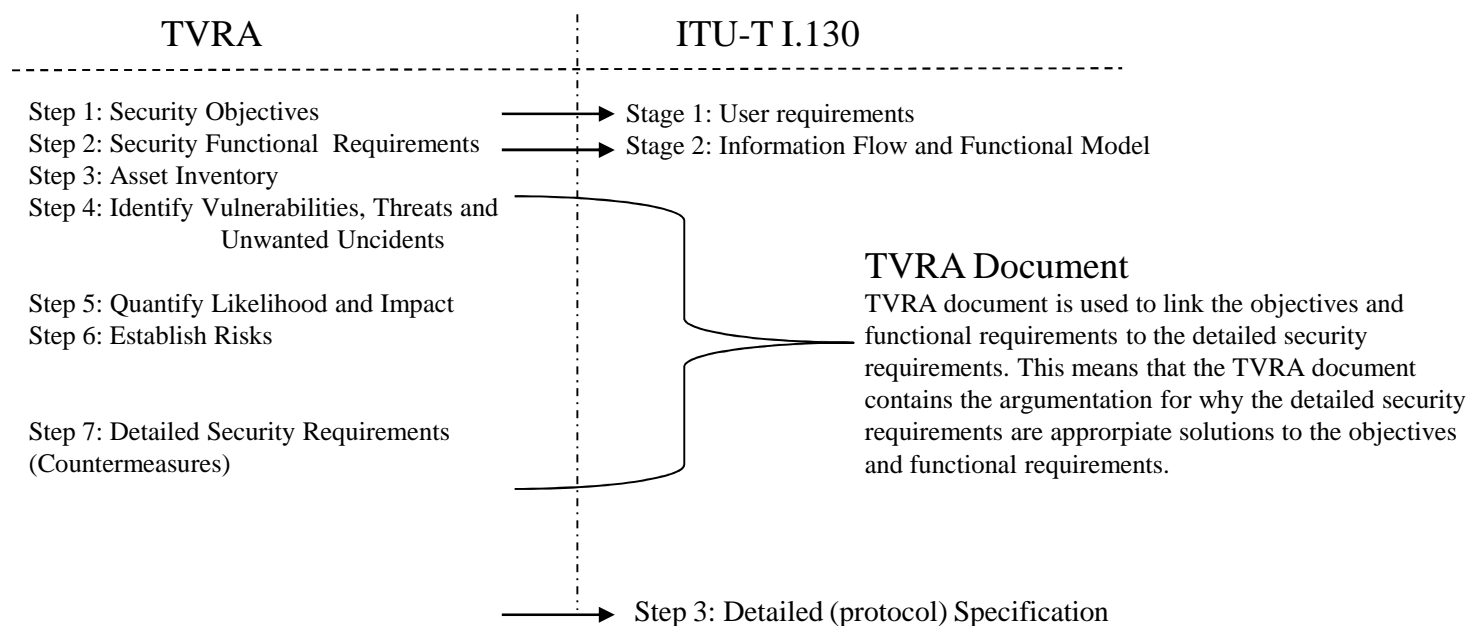
- ❑ Overall guidelines comes from the OECD and enshrined in EU law:
  - Data gathering has to follow a number of principles
    - Collection limitation, Data quality, Purpose specification
    - Etc.
- ❑ Article 12 of the Universal Declaration of Human Rights:
  - *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".*
- ❑ Article 12 is embodied in the EC directives on privacy (2002/58/EC) and on data protection (EU Directive 95/46/EC) with exceptions consistent with protection under law given by the directive on data retention (2006/24/EC) and by the provisions for lawful interception given in COM 96/C329/01

## Privacy in ITS (2)

- ❑ Privacy implications on ITS are many
- ❑ Maintaining Privacy is crucial in building trust among ITS players (infrastructure operators, manufactures, etc.) and towards the end-users
- ❑ The Privacy Challenge
  - Privacy implies a right for you to be protected but also a right for others to be protected against you
- ❑ Example of a privacy challenge:
  - The LDM is intended to assist the driver, but can also be used as a tracking device
- ❑ The goal of the privacy work in WG5 is to contribute to removing fear, uncertainty and doubt from the diverse infrastructure operators and by that help to reach the required critical mass

## Security Work in TC ITS

- **WG5 security work follows the three stages approach (ITU-T I.130)**



- **The stages approach and TVRA is part of Making Better Standards in ETSI**
  - **Overview on the stages approach can be found at:**  
<http://portal.etsi.org/mbs/protocolStandards/stagedApproach.htm>
  - **Overview on TVRA can be found at:**  
<http://portal.etsi.org/mbs/Security/writing/TVRA.htm>



## WG5 – Results Thus Far

- ❑ **Identify and catalogue the risks**
  - Sufficiently to identify where standardised countermeasures need to be applied
- ❑ **Build a verifiable objectives-requirements-test model**
  - Need to answer how an objective is met (i.e. by which requirements)
  - Need to test that a requirement can be implemented

DTR/ITS-0050005 - ETSI TR 102 893 (TVRA)

- ❑ **Build (in standards) a countermeasure framework**
  - For Authentication, Authorisation, Integrity and Confidentiality
  - For key management where crypto devices are deployed
  - For failsafe behaviour

DTR/ITS-0050001 - ETSI TS 102 731  
(Security Services and Architecture)

## WG5 – Look Ahead (1)

### □ Security

- **Continuous update of TVRA**
- **Objectives catalogue and verification**
- **Requirements catalogue and verification**
- **Security architecture framework**
  - Integration to station architecture
  - Integration to roadside unit architecture
  - Integration to CSP architecture
- **Security mechanism development**
  - Protocols (authentication, key management)
  - Mechanisms (integrity, confidentiality)
- **Cryptographic development**
  - If needed
  - SAGE to lead

## WG5 – Look Ahead (2)

### □ Privacy

- Analyse relevant laws and regulations
- Privacy-focused TVRA
- Privacy specific countermeasures
- Develop privacy framework
- Lawful Interception and Data Retention
  - If there is a CSP in the ITS loop these apply
- Investigate and eventually specify how security countermeasures (mechanisms) can assist in ITS compliance to privacy regulations



## Other Considerations

### Other SDOs

#### ➤ Integrating to ISO TC204

- With WG16 for CALM
- With WG17 for nomadic devices
- With WG9 for command and control
- With WG4 for public transport

### ITS is not just about the 5GHz band