ETSI ITS Security Assessment

Alexandru C. Serban\textsuperscript{1,2}
Erik Poll\textsuperscript{1}
Joost Visser\textsuperscript{2}

\textsuperscript{1}Digital Security - Radboud University, Nijmegen

\textsuperscript{2}Research Team - Software Improvement Group, Amsterdam
Contents

Outline of ETSI ITS

Security in ETSI ITS

Security Issues

Conclusions
A word about ETSI ITS

▶ ETSI ITS standardises V2V & V2X in Europe

“Does your car have any idea why my car pulled it over?”
A word about ETSI ITS

- ETSI ITS standardises V2V & V2X in Europe
- Defines C-ITS and its evolution to support full autonomous driving (including wireless communications dedicated to automotive ITS and road transport and traffic telematics)

“Does your car have any idea why my car pulled it over?”
A word about ETSI ITS

- ETSI ITS standardises V2V & V2X in Europe
- Defines C-ITS and its evolution to support full autonomous driving (including wireless communications dedicated to automotive ITS and road transport and traffic telematics)
- Defines 'Automotive Security'

"Does your car have any idea why my car pulled it over?"
ETSI ITS Reference Model
PKI Infrastructure in ETSI ITS
ETSI vs OSI
Authentication and Authorisation Flow

1. ITSS requests enrolment from the Enrolment Authority (EA).
2. EA provides pseudonym certificates to ITSS.
3. ITSS requests service permissions from the Authorisation Authority (AA).
4. AA grants service permission to ITSS.
5. ITSS and AA exchange service independent certificates.
6. ITSS requests service consumption from the Service.
7. Service requests service consumption from ITSS.

The flow illustrates the process of authentication and authorisation in a secure system, involving multiple parties for enhanced security.
ITSS - EA

Requests:

▶ Create
▶ Update
▶ Remove enrolment certificates.

issues:

▶ Update & Remove requests can be replayed.

Attack economic factors:

▶ hard to mount because these requests are not frequent
ITSS - EA

Requests:
▶ Create
▶ Update
▶ Remove enrolment certificates.

Issues:
▶ Update & Remove requests can be replayed.
ITSS - EA

Requests:
- Create
- Update
- Remove enrolment certificates.

Issues:
- Update & Remove requests can be replayed.

Attack economic factors:
ITSS - EA

Requests:
▶ Create
▶ Update
▶ Remove enrolment certificates.

Issues:
▶ Update & Remove requests can be replayed.

Attack economic factors:
▶ hard to mount because these requests are not frequent
Requests:
  ▶ Create
  ▶ Update
  ▶ Remove pseudonim certificates.
ITSS - AA

Requests:
- Create
- Update
- Remove pseudonym certificates.

Issues:
- all requests can be replayed
ITSS - AA

Requests:
- Create
- Update
- Remove pseudonim certificates.

Issues:
- all requests can be replayed

Attack economic factors:
ITSS - AA

Requests:
- Create
- Update
- Remove pseudonim certificates.

Issues:
- all requests can be replayed

Attack economic factors:
- easier to mount because these requests are frequent
ITSS - Service

What do you think about TLS?

I don't use it *all* the time...

We're not meant to be together.
Take aways

- 1st versions of all security protocols will be broken (see TLS)
Take aways

- 1st versions of all security protocols will be broken (see TLS)
- ETSI ITS makes no exception
Take aways

▶ 1st versions of all security protocols will be broken (see TLS)
▶ ETSI ITS makes no exception
▶ Since security specs. are huge, first implementations will also be broken (see TLS)
Take aways

▶ 1st versions of all security protocols will be broken (see TLS)
▶ ETSI ITS makes no exception
▶ Since security specs. are huge, first implementations will also be broken (see TLS)
▶ Future research ranges from formal verification to conformance verifications (e.g. through SAT solvers, model learning, etc)