ISE Project – PKI Scalability & Embedded Security Experimentations

Brigitte LONC, RENAULT
Workshop V-SEC 2017
Toronto, 24 September 2017
ISE PROJECT: SECURED INTELLIGENT TRANSPORT SYSTEMS

Start: July 2014 - 3 Years

Cooperative safety and mobility applications depend upon data from other vehicles and the infrastructure

**Context**

- Vehicles Broadcast/Geocast information to neighbors
  - vehicle dynamics info (position, speed, heading ...)
  - perception of dynamic environment for active safety and future autonomous cars
- Security and privacy are paramount in cooperative ITS (G5)

**Challenges**

- Build security infrastructure (PKI)
- Ensure scalability
- Validation in large scale scenario
- Methods and process for security assurance/evaluation

Financial support:

Academic support:
ISE Key results and follow-up

- **ISE project Timeline:**
    - List of publications
    - Transfer to industry and to standardization (ETSI)

- **Next steps:**
  - follow on project on Secured Cooperative Autonomous systems (SCA)
  - Started July 2017 – end July 2020
  - focus on interoperability, scalability and dynamic sizing in the context of EU C-ITS Certificate Policy
  - hybrid communications (ITS G5, cellular)
  - crypto-agility and security updates OTA for future C-ITS evolution
  - detection of misbehaving systems in operational C-ITS system and revocation of trust.
Architecture Overview
ETSI TS 103 097, TS 102 940/941

- Embedded: ITS G5 (DSRC) performances VTC 2017
- Cloud: PKI scalability VNC 2016
ISE Embedded Security Platform & experimentations
Implementation and validation of the ITS security mechanisms based on ETSI standards

Performance evaluation of the security architecture

Contributions to the security standard development

Effective transfer of research results to industry

✓ Vehicle’s embedded security
✓ Penetration tests tools
✓ ISE PKI protocol

✓ Security stack performance
✓ PKI responsiveness
On-Board Communication Architecture

FACILITY
- CAM
- DENM
- SAM
- SPAT
- MAP
- LDM

NETWORKING
- BTP
- TCP/UDP
- GN
- IPv6

ACCESS
- 802.11p

SECURITY
- Enrl./Auth.
- TSL req.
- Signed mes.

Legend
- Layer
- Module
- API

Legend
- Crypto.
- Storage

Operator

RCA

Distribution Center

EA

AA

ITSA-S

CRL

TSL
Vehicular Security Modules

 Implemented Modules
- Signature
- Verification
- Pseudonym change
- ITS-S identifier change
- Enrolment request
- Pseudonym (AT) reload
- TSL/CRL Request
- HSM integration
**ISE Experimental Platform**

**Implementation and integration**

- **Hardware platform**
  - RENESAS OBU: 802.11p, HSM, GPS

- **Software platform**
  - YOGOKO Communication Stack
  - ISE Security modules
  - Applications: Authorization Ticket reloading, EEBL, SVW,

**ITS-S architecture**
(ETSI EN 302 665)
Vehicular Platform

SystemX vehicle

On-Bord Unit

HMI

Raspberry PI 3

Satory track tests

SystemX surrounding area
PKI Scalability & performance results
• Communications between ITS and the infrastructures are fundamental to improve traffic management, road safety, mobility and comfort services.

• EU and US standards define the Public Key Infrastructure (PKI) as the base of trust for vehicular communication.

• No one has investigated the **PKI scalability** in large scale deployment.

• We assess PKI performance and scalability **replicating the system** on hundreds of machines.

• We evaluate different replication strategies in terms of **performance and consistency implications**.

**Reference:**
Vehicular PKI Scalability-Consistency Trade-Offs in Large Scale Distributed Scenarios, Pierpaolo Cincilla, Omar Hicham, and Benoit Charles
IEEE Vehicular Networking Conference (VNC 2016)
ISE PKI Architecture

**EA**: Enrolment Authority  
**AA**: Authorization Authority  
**RCA**: Root Certificate Authority

**Backbone Network**

- **3G/4G**
- **Roadside ITS-S gateway**
- **RSU**
- **AT 1**
- **AT 2**
- **AT n**
- **Distribution Center**
- **PKI**
- **TSL**
- **CRL**

**Workshop V - SEC 2017**

**Toronto, 24 September 2017**
EC and AT request protocol
• Why is it important to study VPKI Scalability?

Millions of ITSs, billions of (pseudonyms) identities
Experiments Setup

- Amazon EC2 instances
- EU Ireland Data Center
- US Northern California Data Center
- C4.large (2 vCPU, 3.75GB RAM)
- C4.xlarge (4 vCPU, 7.5GB RAM)
- C4.2xlarge (8 vCPU, 15GB RAM)
1. Centralized Deployment

- System saturation!
We need to distribute the system
2. Replicated PKI Deployment

- AT delivery throughput scales well (representing majority of requests)
- EC delivery throughput degrades augmenting the number of replicas.

![Graph showing AT and EC throughput](image)
2. Replicated PKI Deployment

To boost the writes... Trade consistency!

- Synchronous vs asynchronous updates propagation (Local vs Global)
- Database operation’s execution order (FIFO vs ABCAST)
To **boost** EC delivery performance we must **relax** the storage consistency properties.
3. Geographic Replication

10 AA in US and 10 EA in Europe

10 AA and 10 replicated EA in US
3. Geographic Replication

Autorisation Tickets all settings
Conclusion

- Centralized deployment doesn’t scale and has saturation points
- Replication scales well for AT, for EC we need to relax the consistency to gain scalability
- Geo-replication gives better performance for AT, and for EC as long as we relax the consistency constraint
ISE European PKI - United State PKI

**US PKI (CAMP)**

- First year of deployment:
  - 20 certificates per car/week
  - ~17 million new cars per year
  - ~53 billion certificates per year
  - ~134,069 certificates per minute
  - ~5,045 batch downloads per minute

**EU PKI (ISE)**

- Variable
- Similar
- Variable
- ~270,000
- Real time

Workshop V-SEC 2017
Next challenges: PKI dynamic dimensioning

- PKI load is not static and changes over time
- Need to adapt the resources (number of machines) for the current load
- Minimize the cost while meeting the SLA with the minimum number of resources
Thank you For your attention

brigitte.lonc@renault.com

www.irt-systemx.fr