Communications Security for Cooperative Intelligent Transportation Systems (C-ITS)

William Whyte
Chief Scientist
Security Innovation

May 2015

Security Innovation®
THE APPLICATION SECURITY COMPANY

Baseline questions

- What is connected vehicle communications security?
- How is it different from other communications security?
- What are specific mechanisms used in Cooperative Intelligent Transportation Systems (C-ITS)?
- Where are security services applied in the protocol stack?

Security challenges

- All the usual ones
  - Confidentiality, integrity, authenticity, authorization, (sometimes) non-repudiation
  - Security and cryptography requirements depend on application setting
- Plus
  - Privacy: don’t want tracking / traffic analysis to be easy
  - Channel congestion: 3-6Mbps channels
  - Constrained devices due to cost of automotive quality equipment – affects connectivity, hardware security, …
- Plus!
  - Security management: distributing security management information to devices that have intermittent Internet connectivity

Links with IETF projects

- IP over multihop in VANET
  - BOF efforts in ITS (its wg)
- New certificate format
  - Proposal to use in TLS (tls wg)
- Automated certificate issuance
  - Close in spirit to acme wg
- Certificate management
  - Similar topics to those addressed by PKIX
- … links are tenuous but C-ITS would benefit from using technology that’s already been invented

Outline

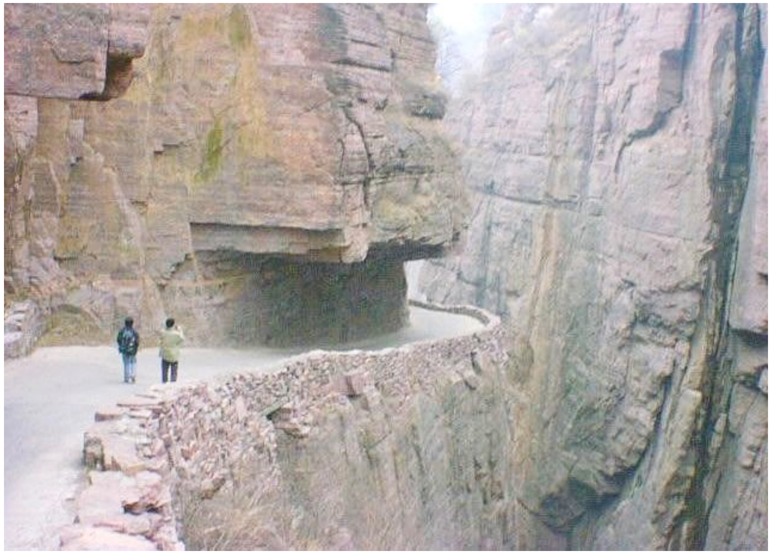
- Trust model
  - IEEE 1609.2 / ETSI TS 103 097 certificates
  - Broadcast single-hop messages
- Privacy: protections against an eavesdropper who is not in all places at once
- Advertised services
  - Simple service discovery mechanism, risk of unauthorized use of spectrum
- Geonetworking
  - Want to allow VANETs, i.e. vehicles can forward application messages without having to understand the application payload
  - Risk: channel flooding

Trust Model: IEEE 1609.2 / ETSI TS 103 097

- Application Identifiers, Service Specific Permissions, and CA responsibilities

Threat model for collision avoidance

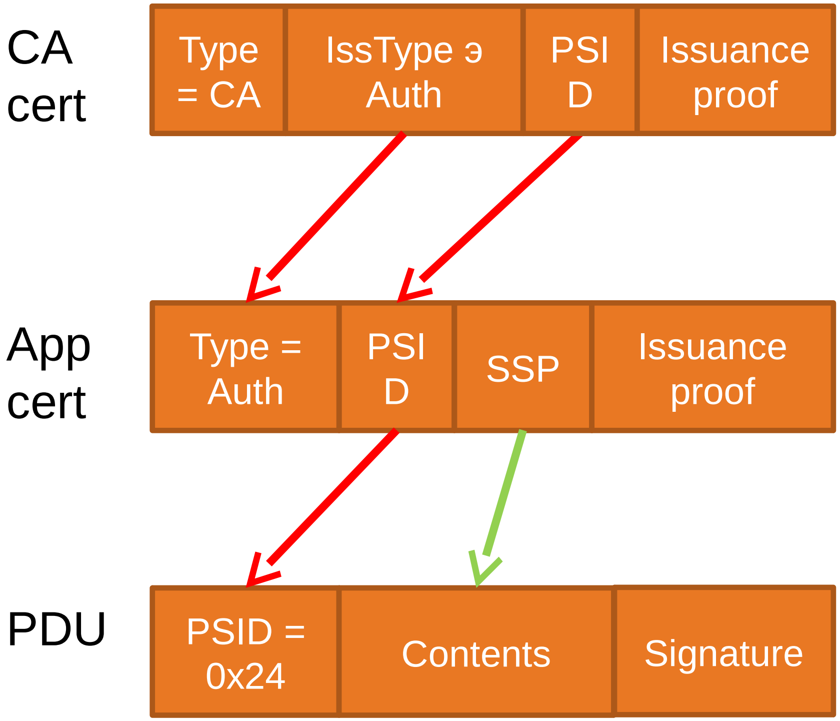
- False positives
  - Unlikely to cause physical harm
  - “Something bad round the corner! swerve now!”
  - But invalid alerts reduce driver faith in system
  - Appropriate security approach: Authentication + misbehavior detection



- False negatives
  - People may come to rely on warnings
  - Need to warn about denial of service once system is widely deployed

Trust model

- IEEE 1609.2 / ETSI TS 103 097
  - Secure messages and certificates, targeted at MANET setting
- Signed PDUs are authorized by certificates
  - PSID: Identifies “application”
  - Service Specific Permissions (SSP): permissions within application
- CA ensures that sender is entitled to these permissions
  - Implications for hardware and software security, data quality
- Receiver checks PDU is consistent with permissions



CA cert

Type = CA | IssType ∍ Auth | PSID | Issuance proof

App cert

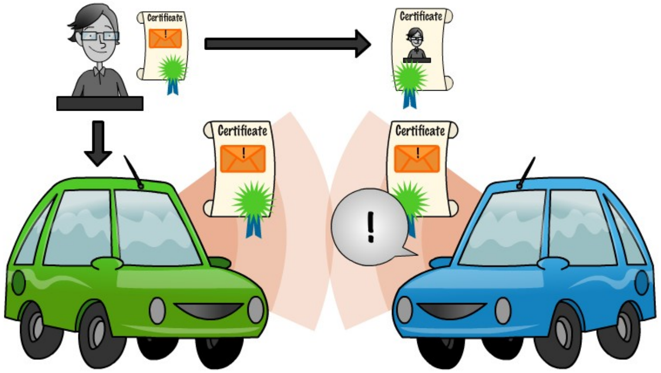
Type = Auth | PSID | SSP | Issuance proof

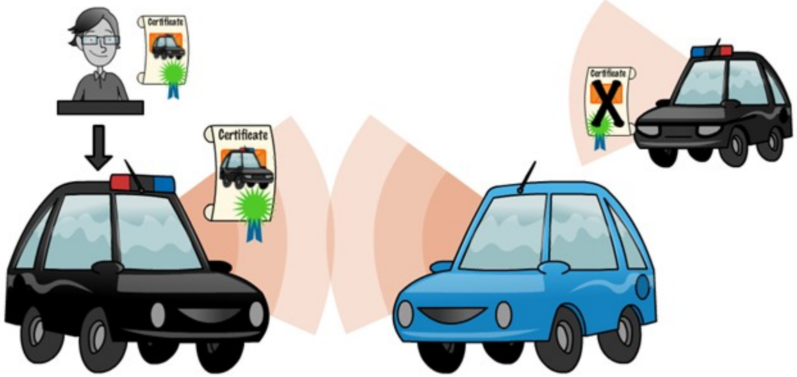
PDU

PSID = 0x24 | Contents | Signature

Trust model example and implementation

- Cooperative Awareness Message (EU): “Here I am”
  - Identified by ITS-AID 0x24
- Default (NULL) SSP: cert owner can send “here I am” message only
- SSP 00 00 40: cert owner can claim to be emergency vehicle, request right of way
- Receiver of a CAM checks that CAM payload is consistent with both CAM PSID and sender-specific SSP
  - This must be carried out by CAM processing logic
  - Cannot be carried out by the security services



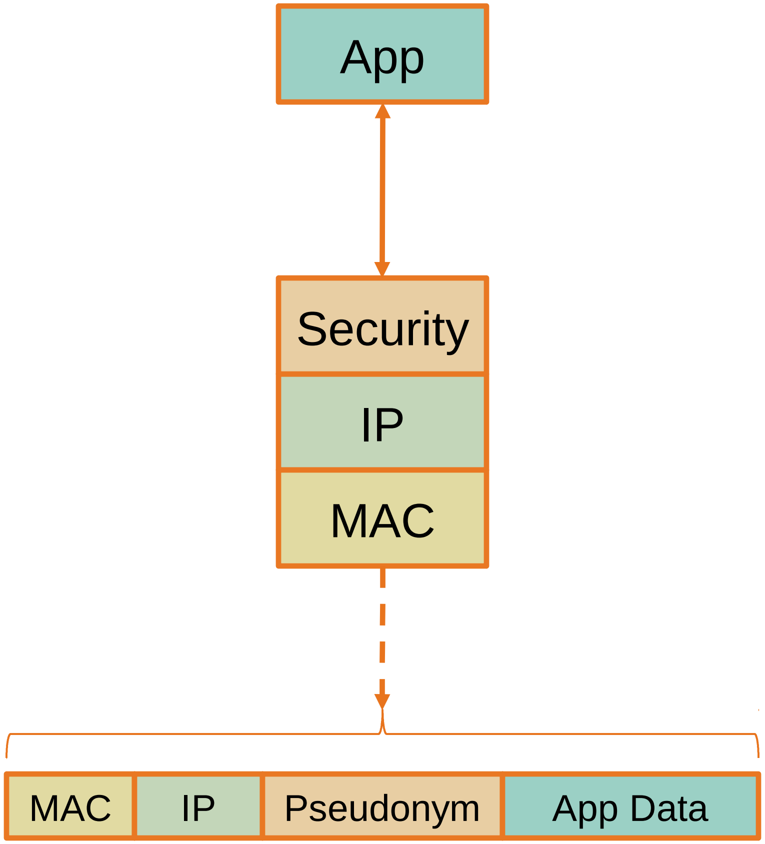


Performance

- Signed messages
  - ECDSA over 256-bit NIST or Brainpool curves
  - IEEE permits “implicit” certificates (no explicit signatures, smaller certs, faster verify than two ECDSA verifications)
  - ETSI uses only explicit certificates
- Up to 600 incoming messages per second
  - Impractical to verify all in software even on full-featured PC platforms
  - Option 1: Use hardware acceleration (EU)
  - Option 2: Prioritize verifying messages that will result in an action (US)
- Butterfly keys (US): one-time request allows CA to generate arbitrary number of distinct, unlinkable device certificates
  - CA pregenerates certs, device downloads them at its leisure
  - Multiple certs supports privacy, pregeneration reduces peak load
  - (CRYPTO! Takes advantage of properties of discrete log)

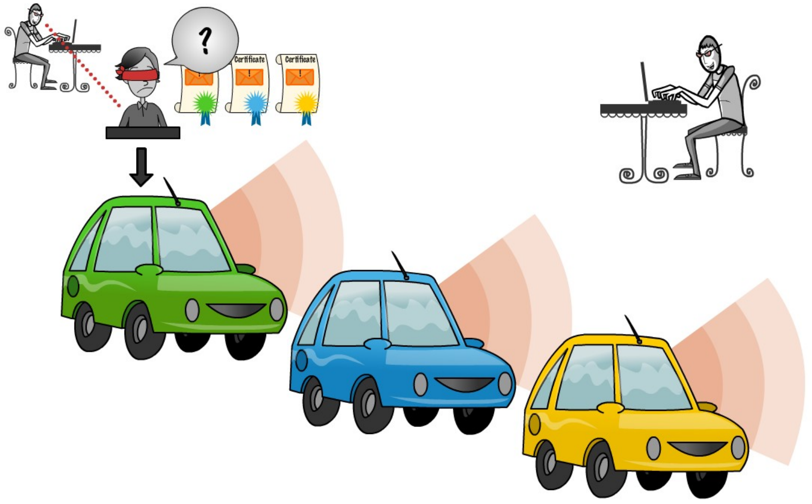
Privacy

- A listener who records all Basic Safety Messages (BSMs) can track a vehicle
  - By design!
- System design provides privacy protection against a "mid-size" attacker
  - Multiple certificates for an application (20+ per week)
  - Change all identifiers in the stack simultaneously
- Need policy measures to prevent automatic speeding tickets etc



Privacy against CA

- A CA could track if it knows which certificates go to which device
  - … so the (US) system “blinds” the CA
- Devices can be revoked and their certificates linked
  - Under specific circumstances
  - Requires cooperation between different organizations
  - (CRYPTO! Identifiers generated by XORing independent hash chains)
  - No information revealed about previous movement



Geonetworking / multi-hop / advertised services

- Security to control congestion

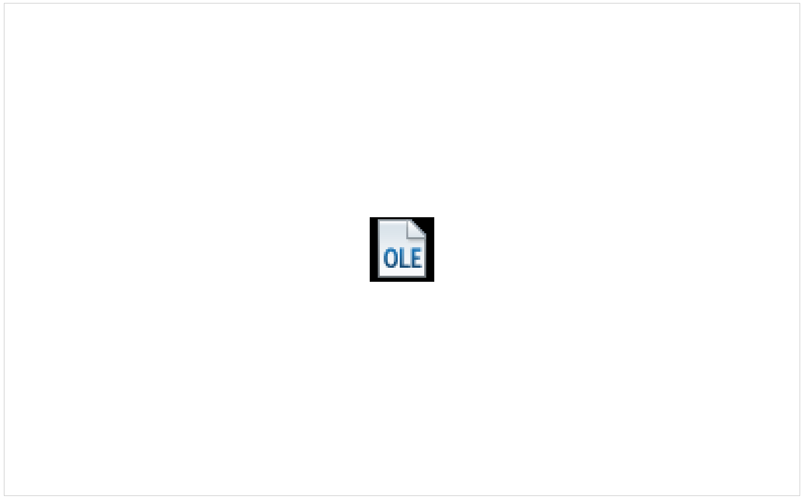
Geonetworking within VANET

- ETSI model
  - All packets sent over geonetworking are signed at the geonetworking layer
  - Indicates that the sender has permissions to ask that a packet is forwarded
  - Packets are verified before forwarding
  - Prevents unauthorized requests for forwarding, reduces congestion
- Packet size optimization: application messages signed at the geonetworking layer do not need to also be signed at the application layer
  - So long as they are not forwarded over a different medium

Architectural comparison: OBE

EU

US

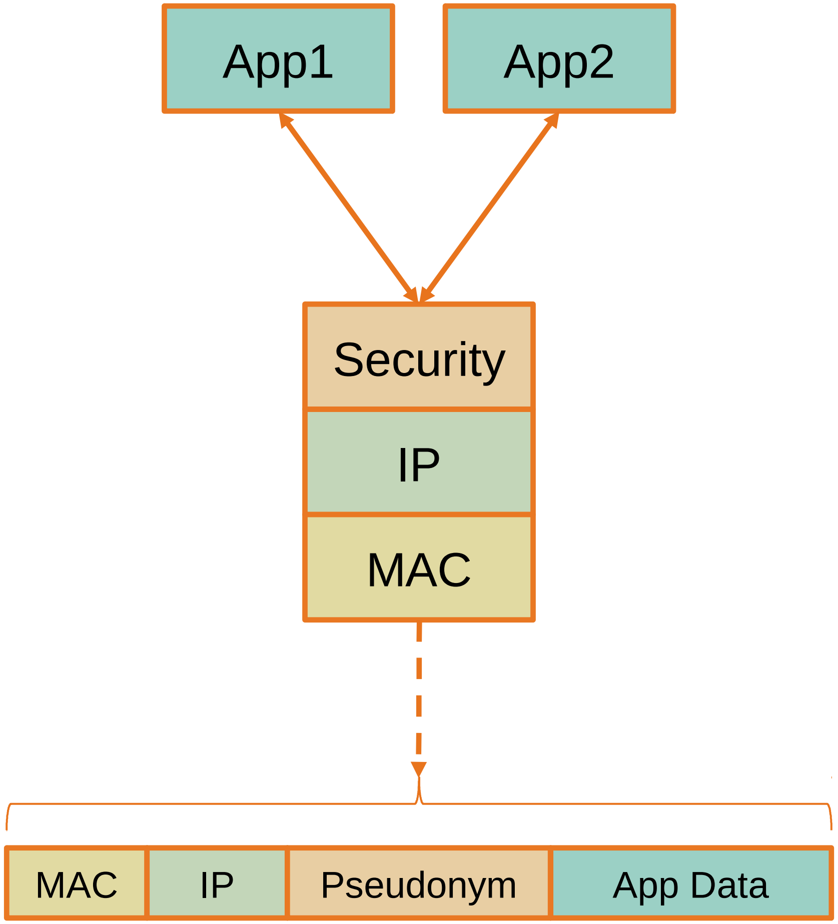


Service advertisements

- Indicate:
  - Service (identified by PSID) is available on a particular service channel
    - Tolling, Point of Interest Notification, Electric Vehicle Charging…
  - Particular access parameters (Enhanced Distributed Channel Access (EDCA) parameter set from IEEE 802.11e) to be used to access
- Possible threats:
  - Service advertised, spoof service provided
    - Out of scope of security for advertisements
  - Advertised bad service causes QoS issues for valid service
    - E.g. tolling on safety channel
    - To be addressed by policy
  - Response to service compromises privacy
    - Users are assumed to give consent to service by opting in

Privacy: Multi-application

- If a private user interacts with separate services A and B, services A and B should not be able to tell it was the same user.
  - A transaction with a user should not be linkable with the user's vehicle
  - An eavesdropper should not be able to use a device's collection of applications to identify it
- Possible solution:
  - Different virtual device for each service?
- Early stage research



Conclusions and future challenges

- Security systems designed to meet the requirements of day-1 applications
  - Work within channel capacity and processing constraints
  - Support different trust “levels”, revocation, privacy against reasonable attackers
- Future challenges
  - Integrate into general IoT security framework
  - Manage congestion in an adversarial setting
  - Definition and harmonization of policy re which applications may use which channels
  - Support more sophisticated communications models
  - Short signatures that remain secure if a quantum computer is invented

Thank you!

SecurityInnovation
THE SOFTWARE SECURITY COMPANY

Aerolink

William Whyte

wwhyte@securityinnovation.com