
# V2X Cybersecurity

Onn Haran, CTO

onn.haran@auto-talks.com

AdaptiVe Technical Workshop

Athens, Greece

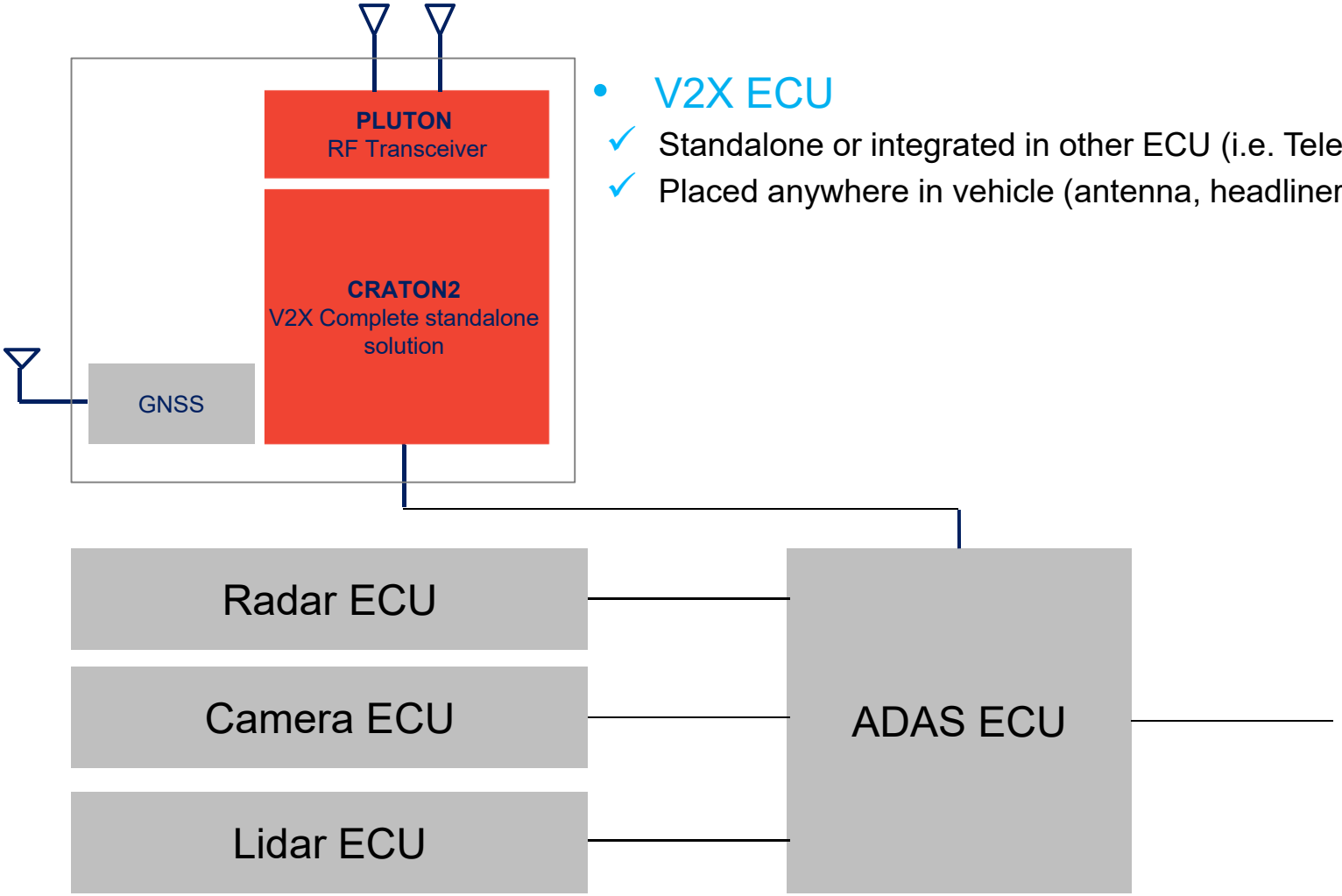
21st April 2016

# V2X and Autonomous Driving

- V2X is a low-cost 360° sensor
  - ✓ Any weather, any visibility, any lighting
  - ✓ Non-line of sight operation: intersection, behind trucks, curves, etc…
- V2X facilitates road usage agreement between vehicles
  - ✓ Lane merge assistance
- V2X is valuable for protecting Vulnerable Road Users (VRUs)
  - ✓ Motorcycles, pedestrians
- V2X can provide accurate information from infrastructure
  - ✓ Traffic light status, signs
- V2X enables Cooperative Adaptive Cruise Control (CACC)

- **V2X will be mandated in every new vehicle in US**

# System Diagram




- V2X ECU
  - ✓ Standalone or integrated in other ECU (i.e. Telematics)
  - ✓ Placed anywhere in vehicle (antenna, headliner, dashboard, …)

# V2X Security Basics

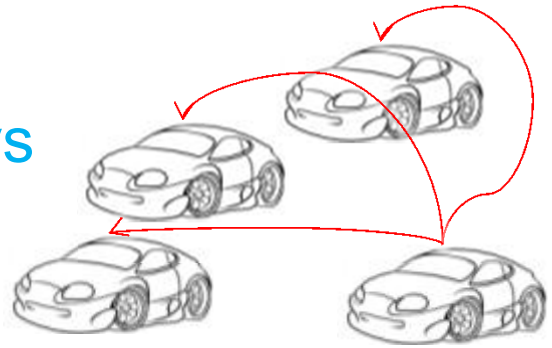
- Main V2X security goals are **Integrity** and **Authenticity**
  - ✓ **Integrity**: Information should be protected against modification or deletion
  - ✓ **Authenticity**: It should not be possible for an unauthorized user to pose as a valid user
- V2X communication is employing public-key cryptography to authenticate over-the-air messages
  - ✓ Signatures are calculated according to Elliptic Curve Digital Signature Algorithm (ECDSA) using 256 bits long keys
  - ✓ Each vehicle has many private-public key pairs
    - ✓ Frequently changed for protecting vehicle user privacy
  - ✓ Each public key is distributed in a certificate
  - ✓ The certificates are signed by a certificate authority (CA)
  - ✓ The same cryptographic solutions can be applied in US and Europe with only minor differences

# V2X Security Functions

- ECDSA signing
  - ✓ Attach a signature generated with a selected private key to an outgoing V2X message
  - ✓ Key requirement: Secure storage
- ECDSA verification
  - ✓ Check the correctness of a received signature based on an already verified public key
  - ✓ Key requirement: Verification performance
- Cybersecurity platform
  - ✓ Prevent harmful operations in V2X unit, other units of vehicle, and V2X units of other vehicles
- Solution certification is essential to validate the security claims

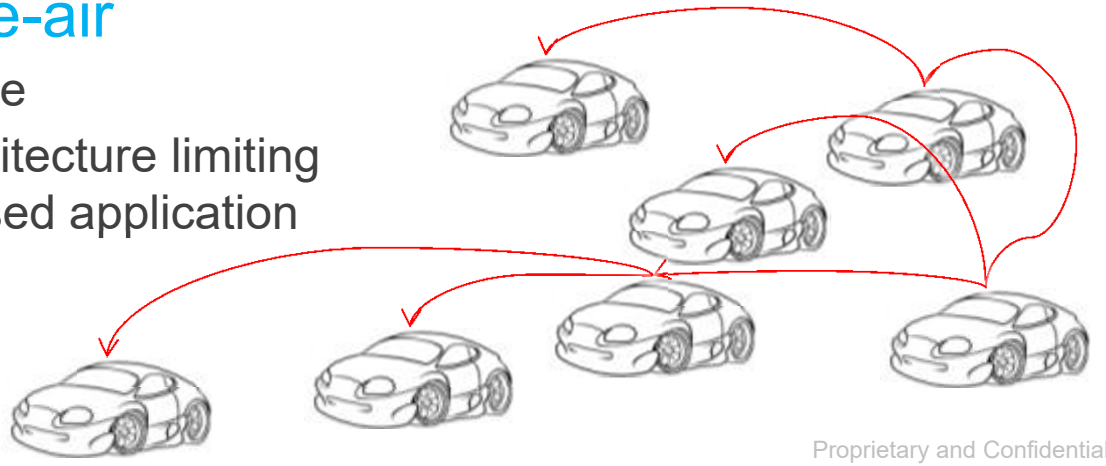
# Potential Attacks

- Attacking other ECUs in the vehicle via IVN (e.g. CAN)
  - ✓ Remedy: IVN transmission is only possible from a secure execution domain
- Sending fake messages to generate false alerts
  - ✓ Remedy: Line-rate verification blocks all fake messages
- Sending messages using stolen private keys
  - ✓ Remedy: Private keys are securely stored



---

- Worm spreading over-the-air
  - ✓ Remedy: Minimal attack surface
  - ✓ Remedy: Secure gateway architecture limiting the capabilities of a compromised application



# Tamper Resistant HSM

- Tamper-resistant HSMs will prevent a flood of stolen V2X private keys, potentially putting vehicle users at risk
  - ✓ As opposed to a tamper-evident HSM, a tamper-resistant HSM destroys secret keys when it detects a physical attempt to read them
  - ✓ Tamper-resistant HSM blocks cheap physical methods for copying private keys from a V2X device
- Side-channel protection prevents key extraction by monitoring time and static and dynamic power consumption
- A large amount of V2X certificate revocations will overwhelm the capacity of CRL distribution and storage systems
- Tamper-resistant HSM is best practice in industries where private keys are stored outside of a secure environment (e.g. credit cards)

# Verify-All

- ECDSA verification of all incoming V2X messages
- Unverified V2X messages can never affect the vehicle
- No received message, including emergency, is ever missed
- Not requiring applications to decide whether a message should be verified
  - ✓ Simplifies application security design and testing

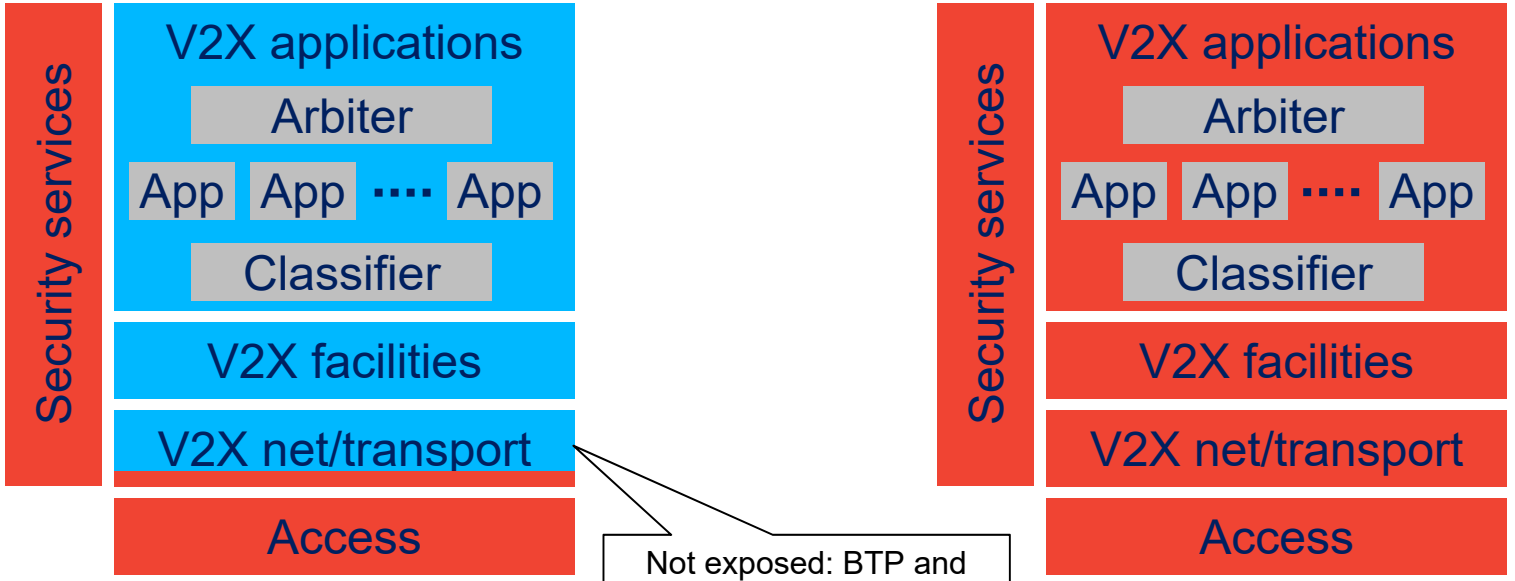
- Assumptions about incoming message rate fail when it matters
- 

  - I-94 road, Galesburg, MI
  - January 9th 2015
  - 193 vehicles involved

# Verification Cyber Attack Surface
## Verify-All vs. Verify-on-Demand

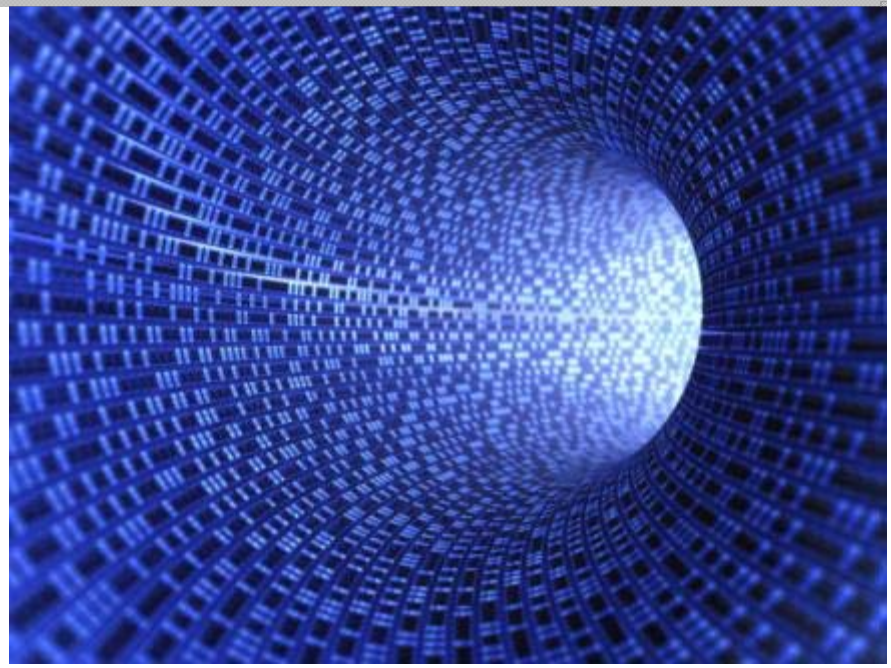
- **Verify-All**
  - ✓ V2X facilities and apps are never exposed to untrusted data
  - ✓ Minimal potential contamination

- **Verify-on-Demand**
  - All layers are exposed to untrusted data
  - Any database can be contaminated
  - Imposing unquantifiable risk

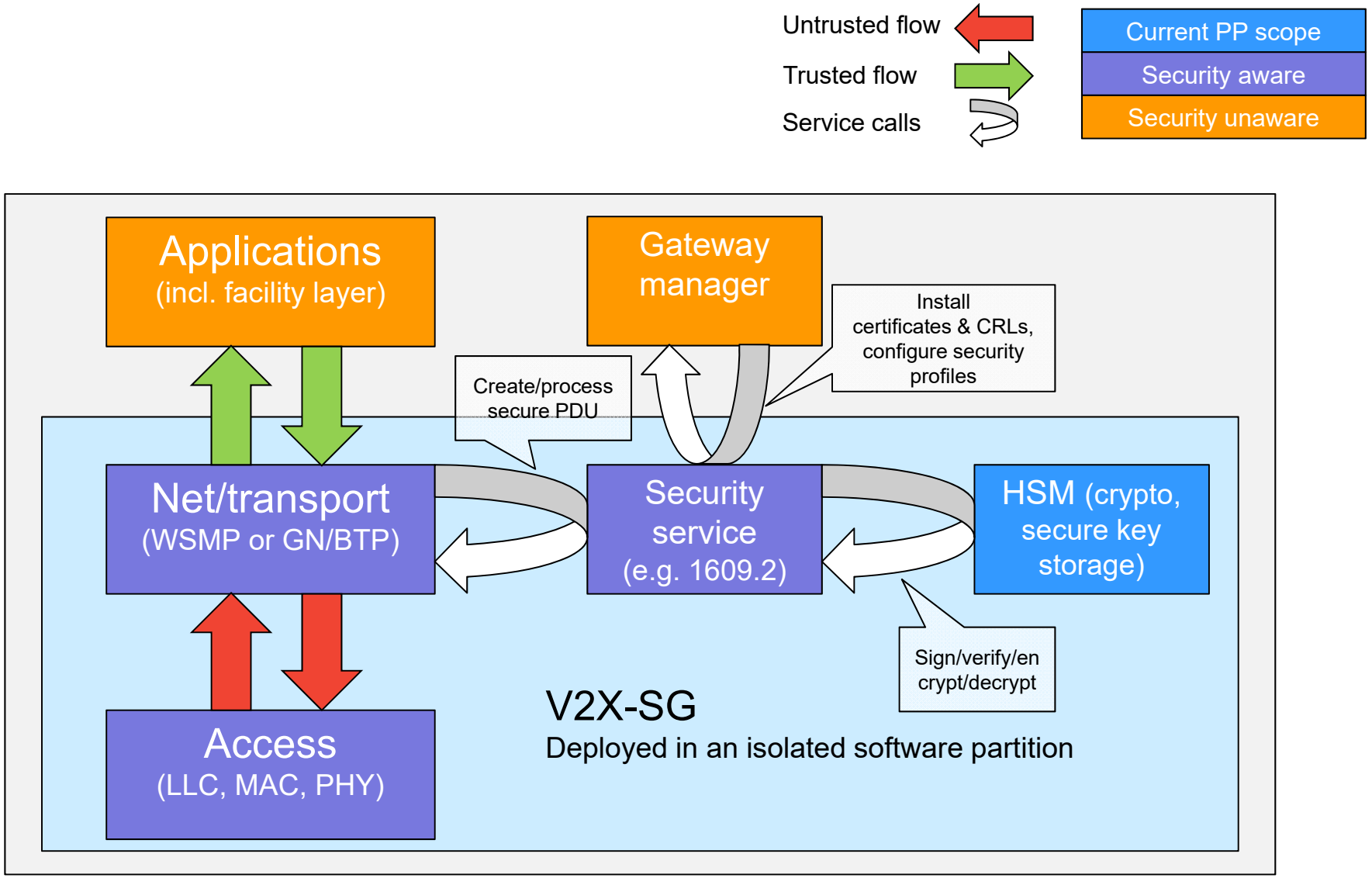


# Cryptographic Agility

- Existing curves might be upgraded in the future
- Cryptographic agility is required
  - ✓ Users will not agree to disable V2X after enjoying the benefits
  - ✓ OEMs will have to replace equipment if not upgradable
- Design requirements
  - ✓ Field update of curves
  - ✓ Verification performance should be maintained at long curves
  - ✓ Signing latency should be low at long curves



# V2X Secure Gateway (V2X-SG)




# Thank you!

## Contact us at:

E-mail: info@auto-talks.com; Website: www.auto-talks.com