PROVE & RUN

77, avenue Niel, 75017 Paris, France

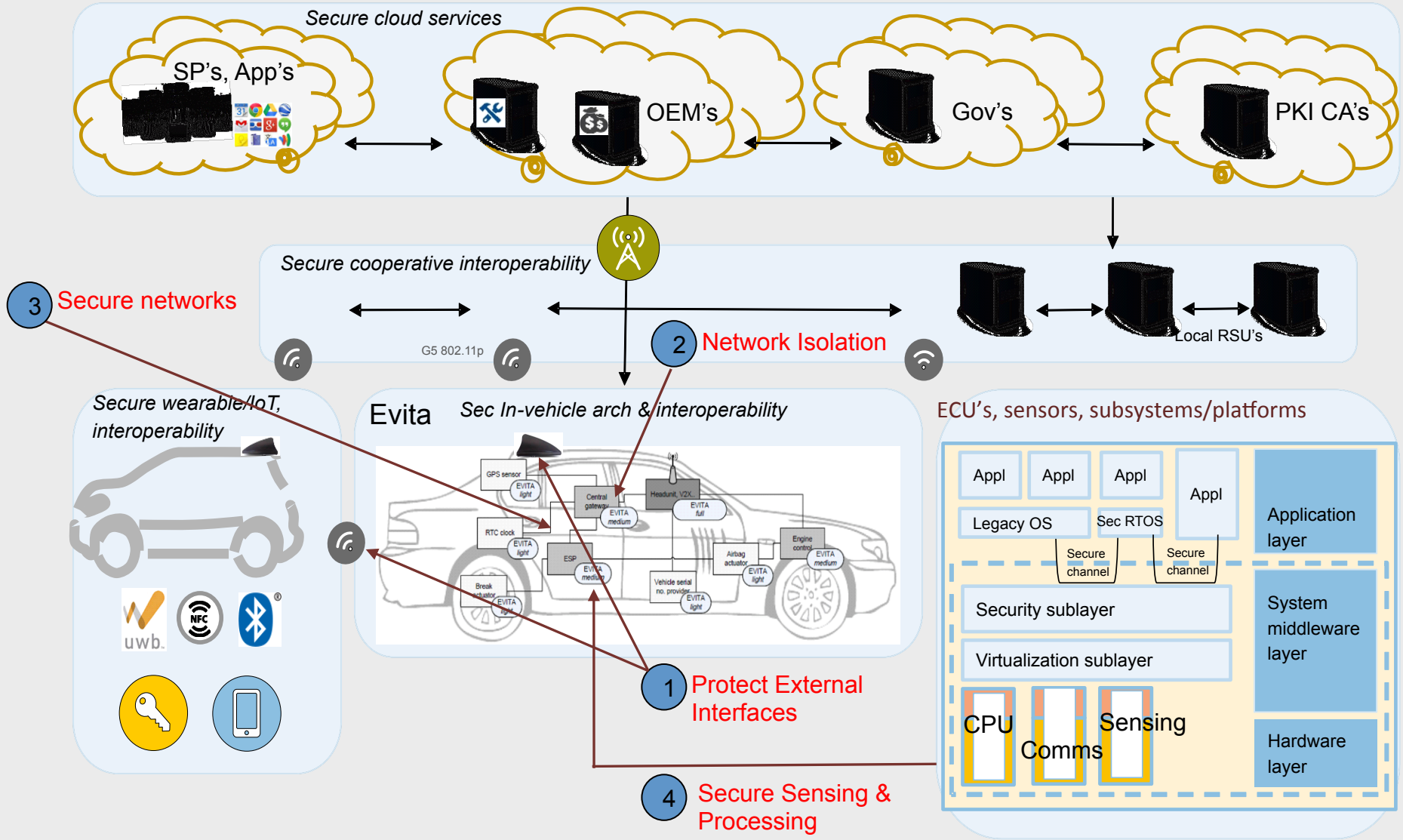
contact@provenrun.com

The 2015 Jeep Hack

- 2015 hack shown to be representative:
  - Remote control of a car
  - Injection of CAN messages
- Not a simple hack
  - Complex attack path
- But not that hard, either
  - Many *bad* vulnerabilities

Source: http://icitech.org/icit-brief-whos-behind-the-wheel-exposing-the-vulnerabilities-and-risks-of-high-tech-vehicles/

Connected Cars – The Global View



What is the security challenge

- Security by Design: build security in your architecture
  - *Protect the most sensitive ECUs (typically the Infotainment system, the TCU and the Gateway)*
  - *Provide secure execution environment for security critical applications (*(FOTA, Firewall, Logging Events, Intrusion Detection, etc.)
- The main issue is with the software
  - *Hackers will exploit bugs, weaknesses and errors that exist in thousands in the software of embedded systems, in particular Operating Systems*
  - *Existing OSes such as Android, Linux, large RTOS cannot be technically secured and used as such. They need to be sandboxed :*

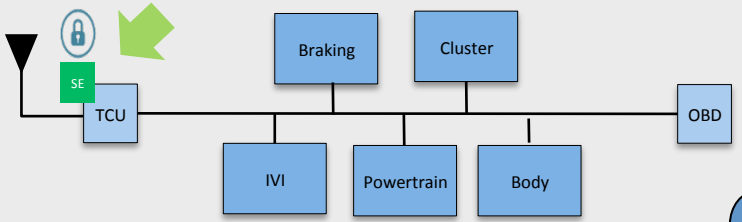
Security Toolbox

- Security architectures have converged towards a **security architecture based on three pillars**:
  - Secure elements or hardware coprocessors for the Root of Trust, cryptography, and transactions
  - **TEE** (Trusted Execution Environments)/**Secure OS**
  - Hardware or Software **Hypervisors**
- The last two first **need to be significantly reinforced** for connected cars (to secure Gateway, TCU, Infotainment, e-Cluster,…).

Connected Cars – Security Layers

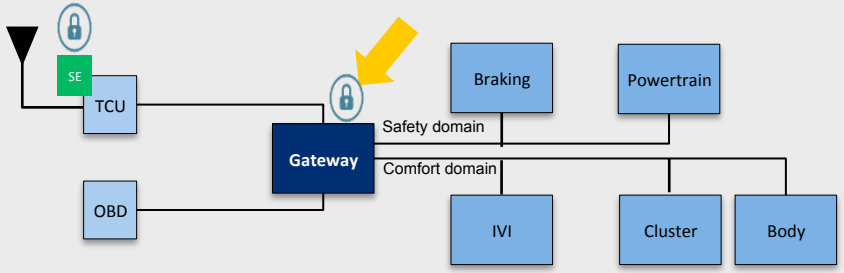
Layer 1: **Protect External Interface**

Secure M2M authentication, secure key storage



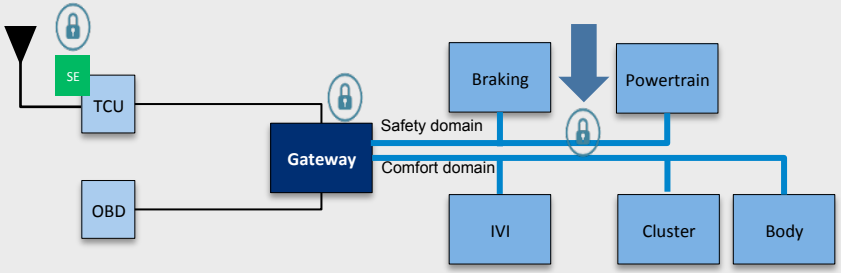
Layer 2: **Isolate Network**

Domain isolation, firewall/filter, centralized intrusion detection (IDS)



Layer 3: **Secure Network**

CAN ID Killer, message authentication, distributed intrusion detection (IDS)



Layer 4: **Secure Processing**

Secure boot, run time integrity, OTA updates