ALL MEMBER MEETING '21

Counterfeit Modules, Right to Repair, and Cybersecurity Plans:

Challenges and Opportunities

Chad Childers

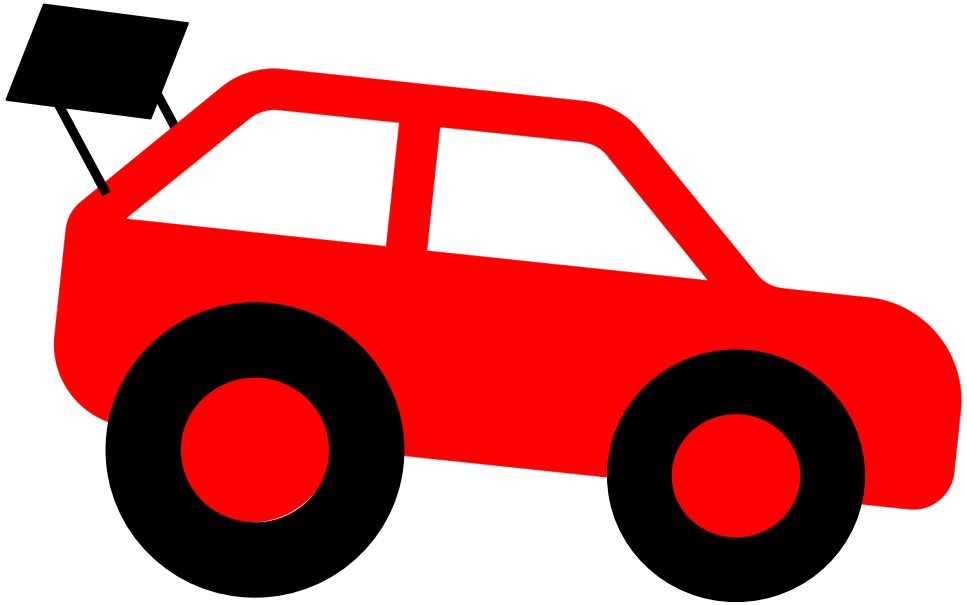
Purpose

- Understand current state of the art, issues, and regulations for automotive modules and diagnostics.
- Explore ways to build a stronger foundation for security, safety, and reliability while sharing the right data and allowing the right R2R!
- Propose expanded built-in test tied to secure boot to detect counterfeit parts at any point in the vehicle life cycle.
- Propose strong auditable authentication requirements for security or safety critical diagnostic access.

Outline

- Background
- Issues
- Current Controls
- Recommendation
- Conclusions
- References

As-Built vs Real World



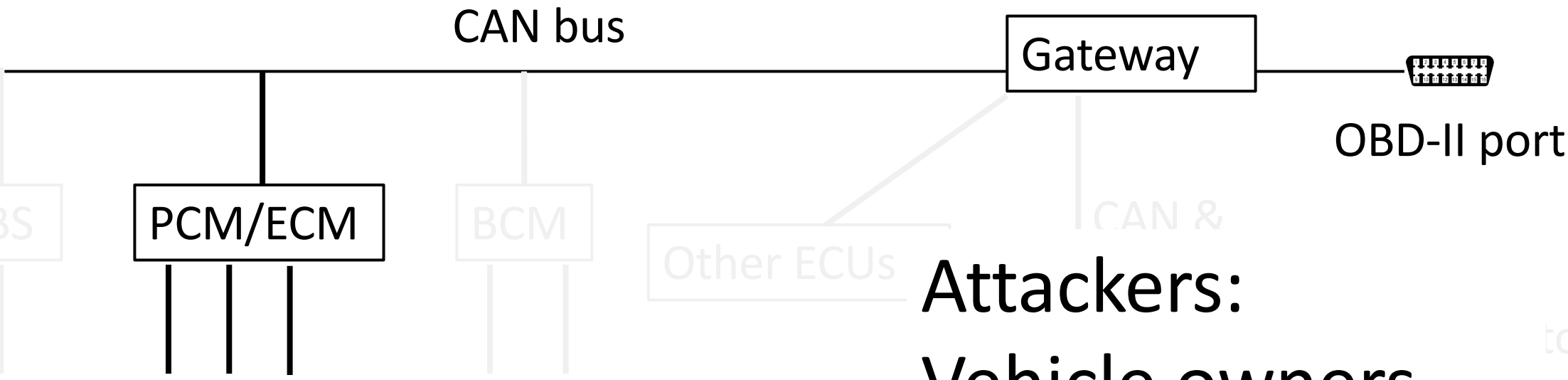
Diagnostic Regulations

- California Air Resources Board (CARB) OBD Regulations
  - 1988 OBD I required manufacturers to monitor emission control components
  - 1994 OBD-II fixed problems, made the system more powerful
- US EPA rules in 1995, 2001, 2003, 2009
  - Makes OBD-II mandatory for all cars sold in US
  - 33 states require OBD for vehicle emission tests
- EU Directives on EOBD (2001 gas, 2004 diesel)
- ISO 15765-4 Diagnostics over CAN (DoCAN)
- ISO 14229-1 UDS

Right to Repair

- EU Motor Vehicle Block Exemption Regulations (BER) since 1995
  - access to technical information for independent shops
  - freedom to source and supply spare parts protects alternatives does not address counterfeits
- Massachusetts Automotive Repair Acts
  - 2013 diagnostic tools & repair information
  - 2020 added open telematics platform

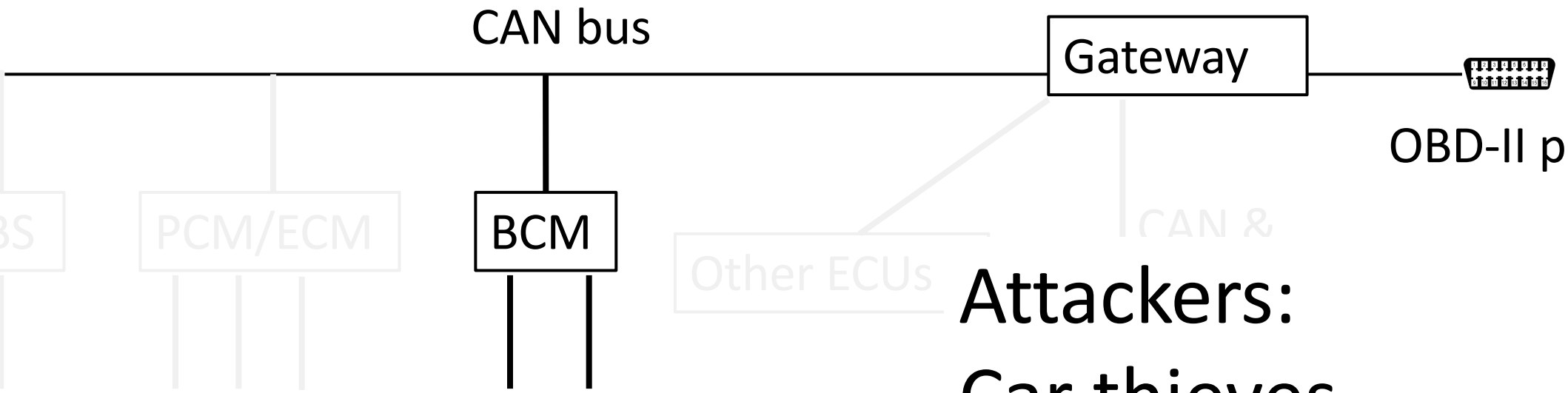
Issues - Chip Tuning



More power / fuel economy
Higher emissions
Regulatory issues
Warranty issues

Attackers:
Vehicle owners
Custom shops
OEM

Issues - Anti-Theft



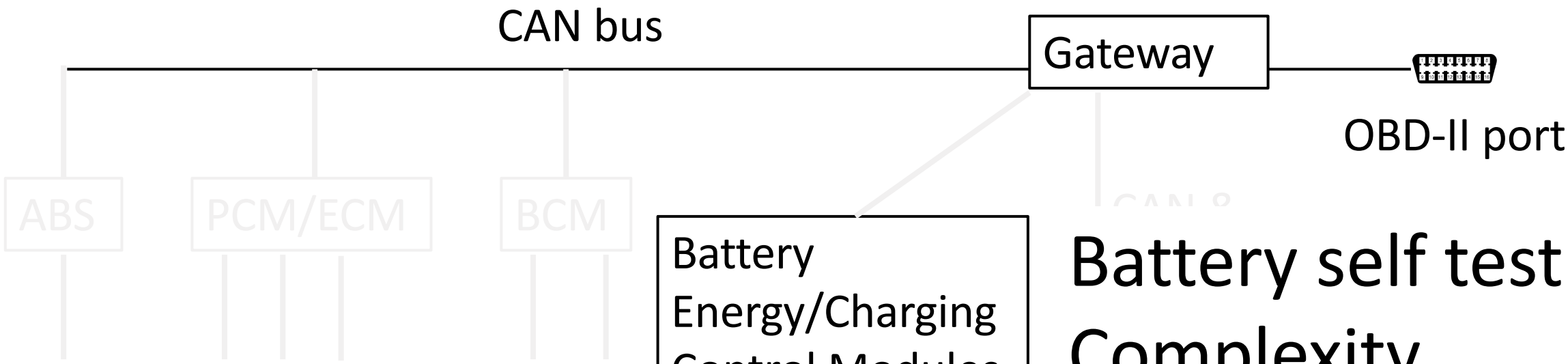
Body enclosures locking
Key fob programming
Immobilizer
Module reprogramming
UDS service 0x27 security access

Attackers:
Car thieves
Counterfeiters
Nation State

Issues – Counterfeit Modules

- Accidental purchase from untrusted supply chain
- Intentional dealer / shop malfeasance
- Modules from approved supplier may contain counterfeit components
- Aftermarket parts are allowed but will need to pass DV test and be authenticated for future vehicles

Issues - Electric Vehicle



Off board charge controller
Smart Grid Charge points
Plug and Charge payments

Battery self test
Complexity
Counterfeit
charge points

Current Controls

- Security access for reprogramming
  - Dealer / shop employees sharing / selling credentials
  - UDS service 0x27 security access seed/key
  - Backend challenge/response
- Secure boot
  - Only for a few modules
- Diagnostic self test
  - Only for emissions or safety critical modules
  - Diagnostic Trouble Code (DTC) developed for emissions

Recommendations

1204 - Siege of Chateau Galliard

Most advanced castle of its day, defense in depth

Toilet chute was not Outbound Only

Do not allow any writable DID or config without strong authentication or over inbound Internet or wireless communications

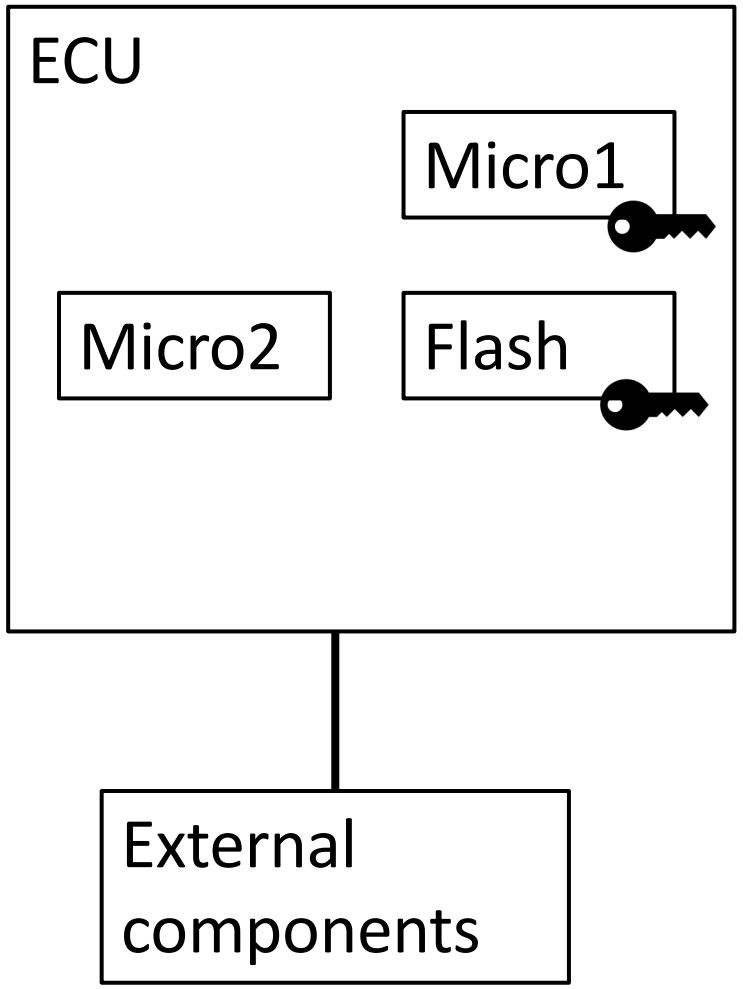
Granular Authentication

- UDS service 0x27 is not secure, even level 3
- Backend logging and response to unusual activity is the first step
- Any weak auth writable DID is a vulnerability
- Signing of firmware, configs, critical commands
- UDS service 0x29 PKI from a trusted backend server
- Authenticated secure tunnel initiated by the module
- Authentication of service technician requires factors that cannot be shared or sold and strong identity proofing, trust accountability

Right to Repair vs Right to Anonymity

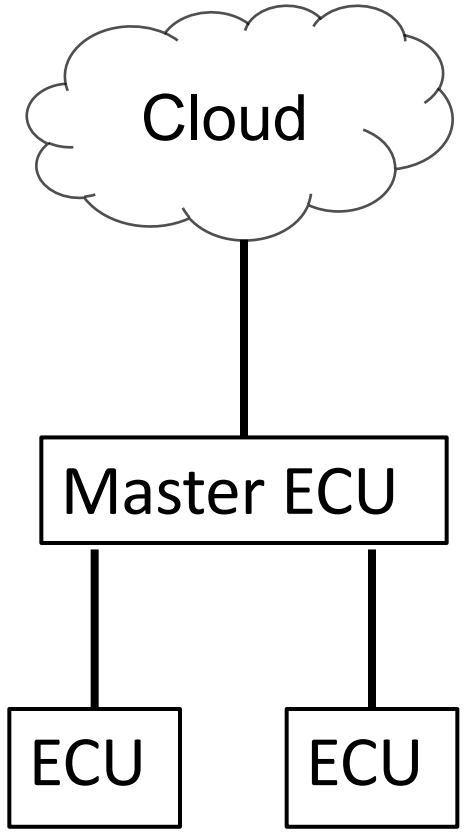
- For safety, security, and warranty, allow changes only when traceable to an accountable person
- Physical access beats encryption or technical controls
- Secure boot validation of firmware, config, and components
- Built-in self test of components can help detect counterfeits
- System secure boot needs standard PKI based communication, not putting requirement on ASIL-D module
- Need ability to validate in the vehicle, V2V, V2I, and to the OEM

System Secure Boot Part 1



- Secure boot requires SHE or HSM or hardware root of trust like Micron Authenta Flash (counterfeit-proof)
- Logic / memory BIST, memory measurements, built-in test of other components within the ECU
- Test of external components on LIN, h/w, query other modules

System Secure Boot Part 2



- Use DICE key tied to secure boot to sign attestation, versions, measurements
- Report signed boot attestation to master ECU. Signature validation does not require ASIL rated module and could be gateway
- Validate golden list against signed lists, locally and in cloud

Conclusions

- We propose a unified, distributed solution that can be implemented on a variety of modules
- Using signatures solves the problems of transport authentication and trusted module validation
- Identity proof of a person who takes repair responsibility is the hardest problem

References

- Privafy MicroEdge™ end-to-end secure connectivity, device onboarding and lifecycle management

  www.privafy.com/privafy-microedge
- Micron Authenta™ hardware root of trust
  www.micron.com/products/advanced-solutions/authenta

Questions?

chad@privafy.com