Integrity for Car-Computing

A cryptographic vision for integrity in vehicle networks

Eran Tromer

CPIIS

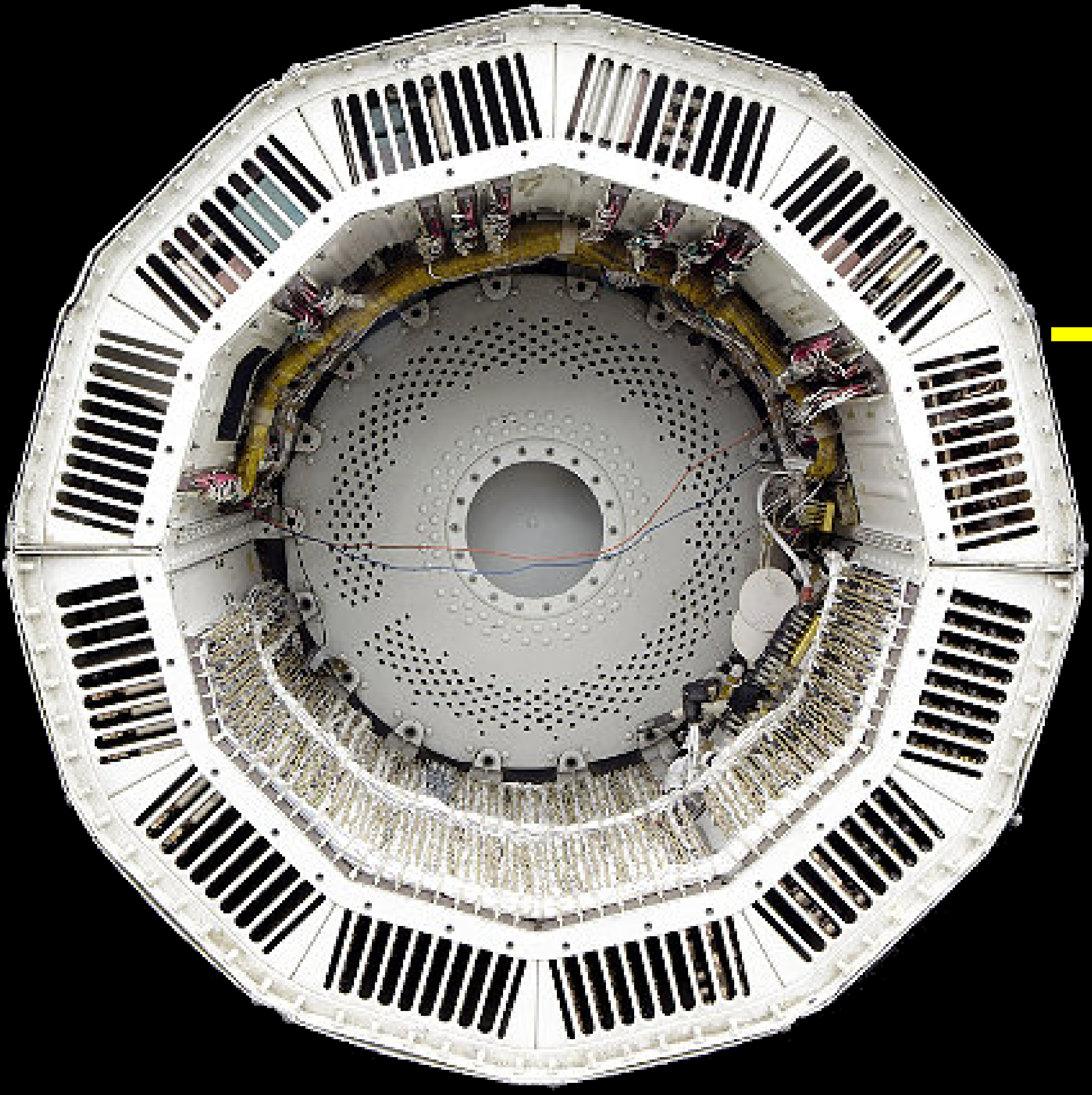
Check Point Institute for Information Security

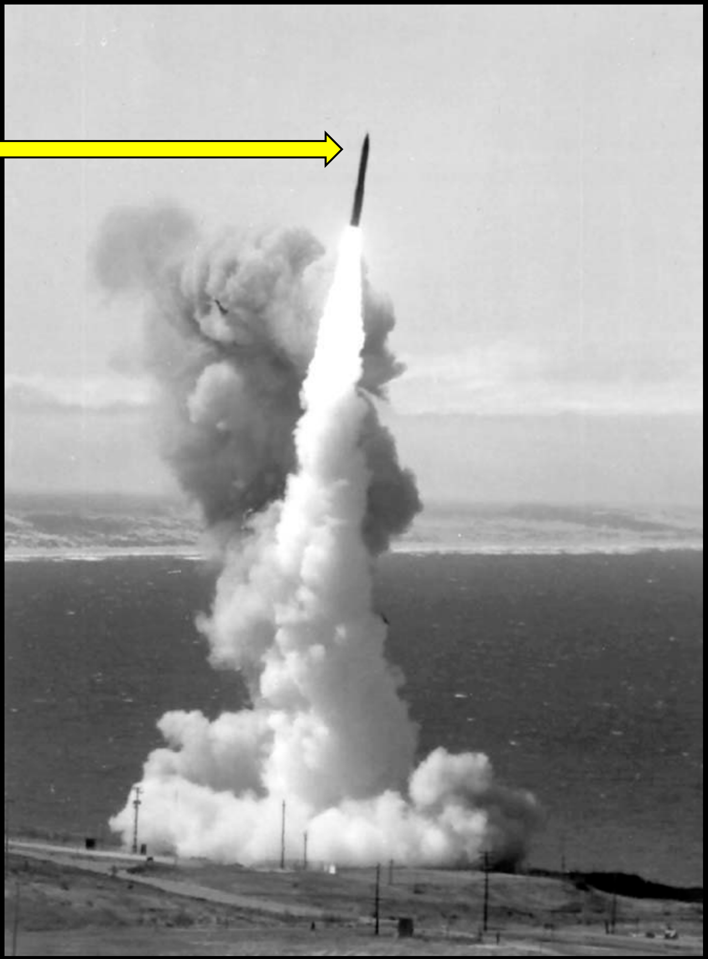
בית הספר למדעי המחשב על שם בלבטניק

The Blavatnik School of **Computer Science**

The first vehicle computer

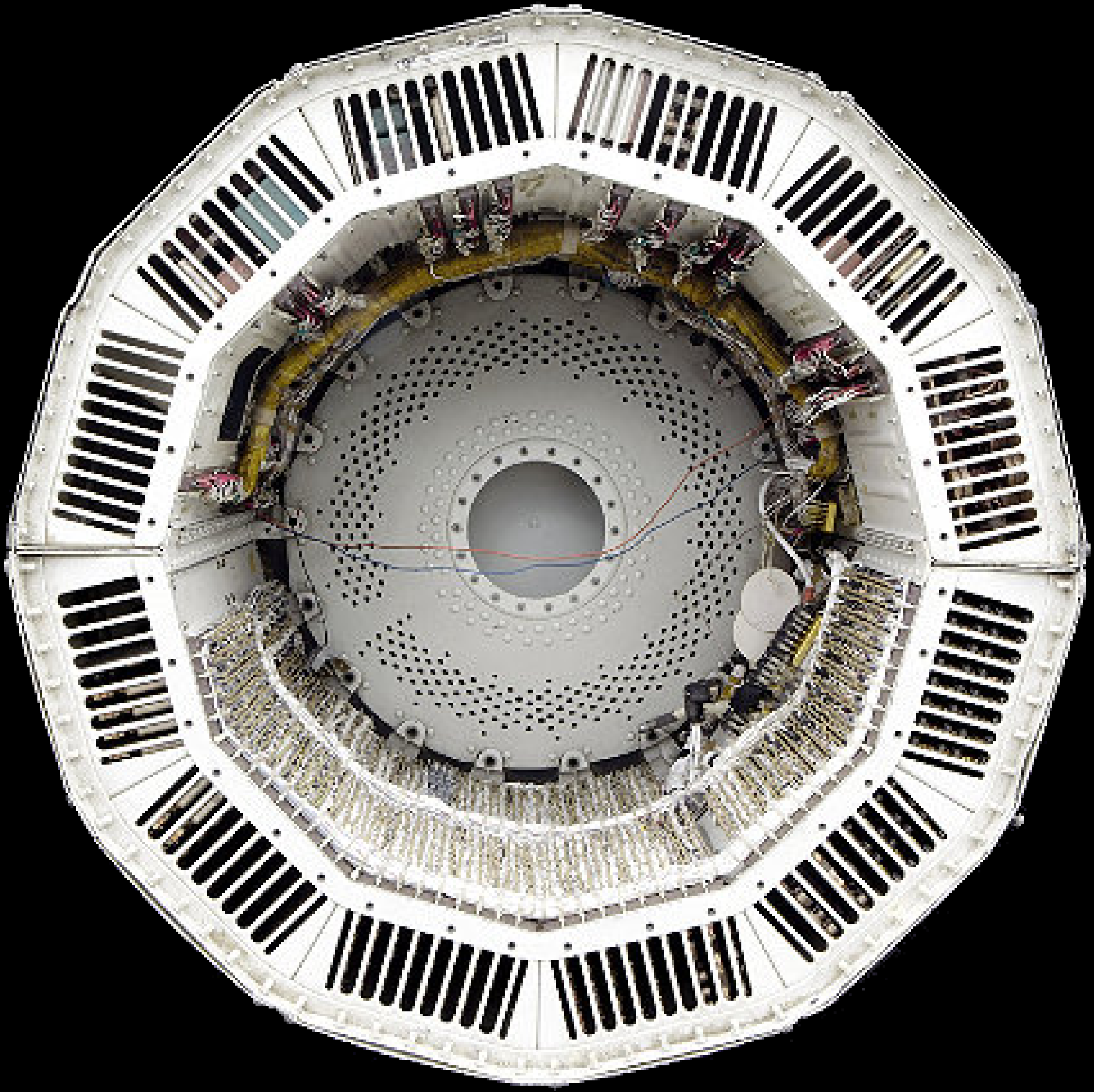
D-17B *Minuteman I* guidance system





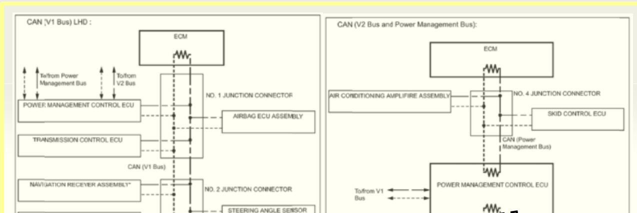
The first vehicle computer

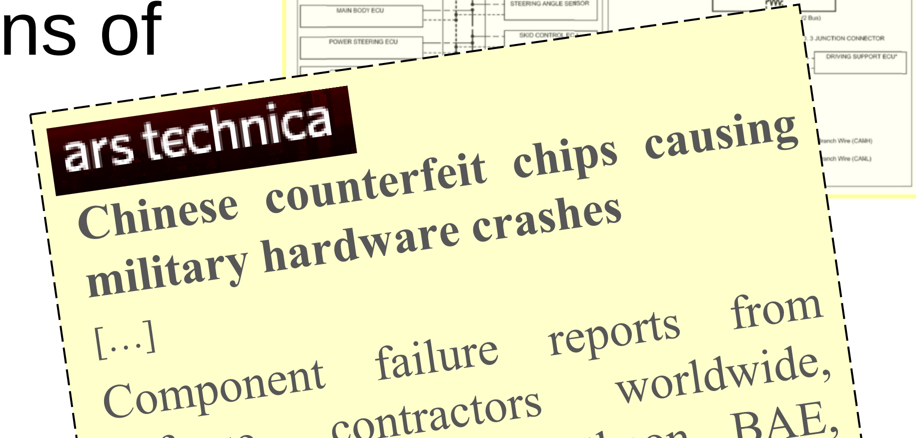
D-17B *Minuteman I* guidance system



In-car integrity

- Modern cars contain dozens of Electronic Control Units
- Can you trust them?
  - Hardware supply chain
  - Bad software
  - Errors
  - Bad updates
  - Attacks



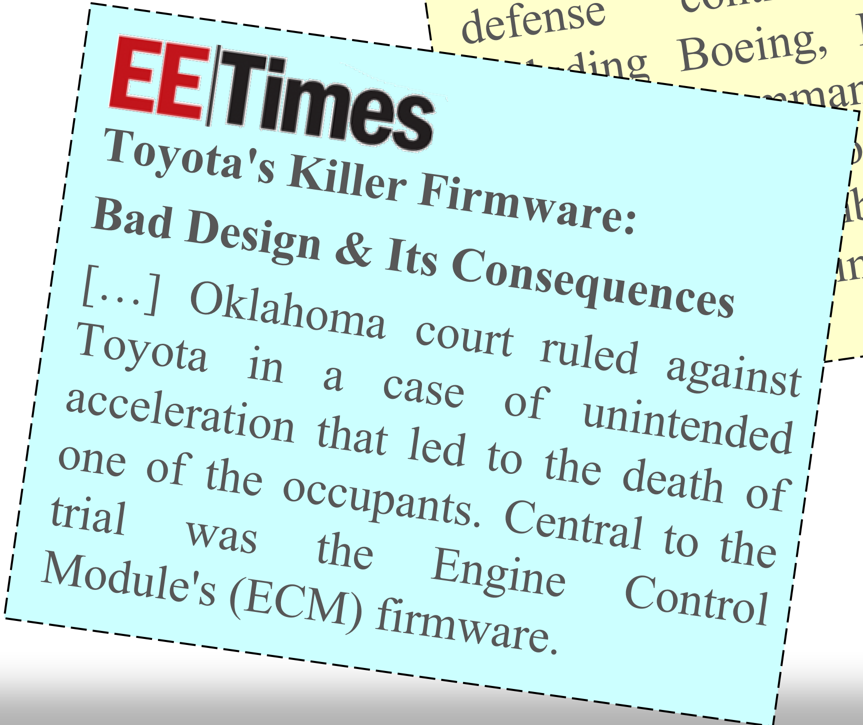


ars technica

Chinese counterfeit chips causing military hardware crashes

[…]

Component failure reports from defense contractors worldwide, ding Boeing, Raytheon, BAE, man, and Lockheed ns have turned up ber of counterfeit nstalled in mission-



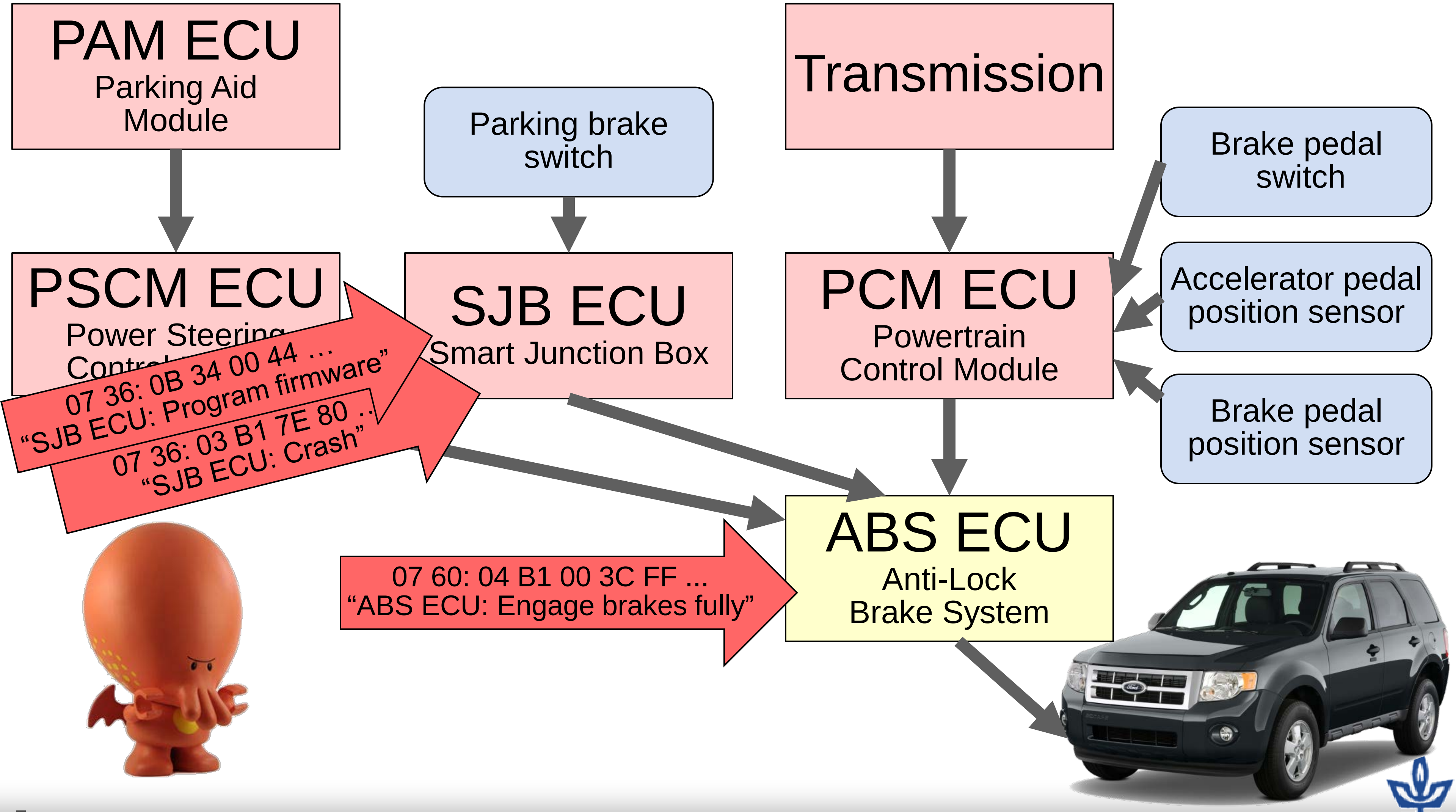
EETimes

Toyota's Killer Firmware: Bad Design & Its Consequences

[…] Oklahoma court ruled against Toyota in a case of unintended acceleration that led to the death of one of the occupants. Central to the trial was the Engine Control Module's (ECM) firmware.

Example: engaging ABS

See [Miller Valasek 2013]



PAM ECU
Parking Aid Module

Parking brake switch

Transmission

Brake pedal switch

PSCM ECU
Power Steering Contr

SJB ECU
Smart Junction Box

PCM ECU
Powertrain Control Module

Accelerator pedal position sensor

Brake pedal position sensor

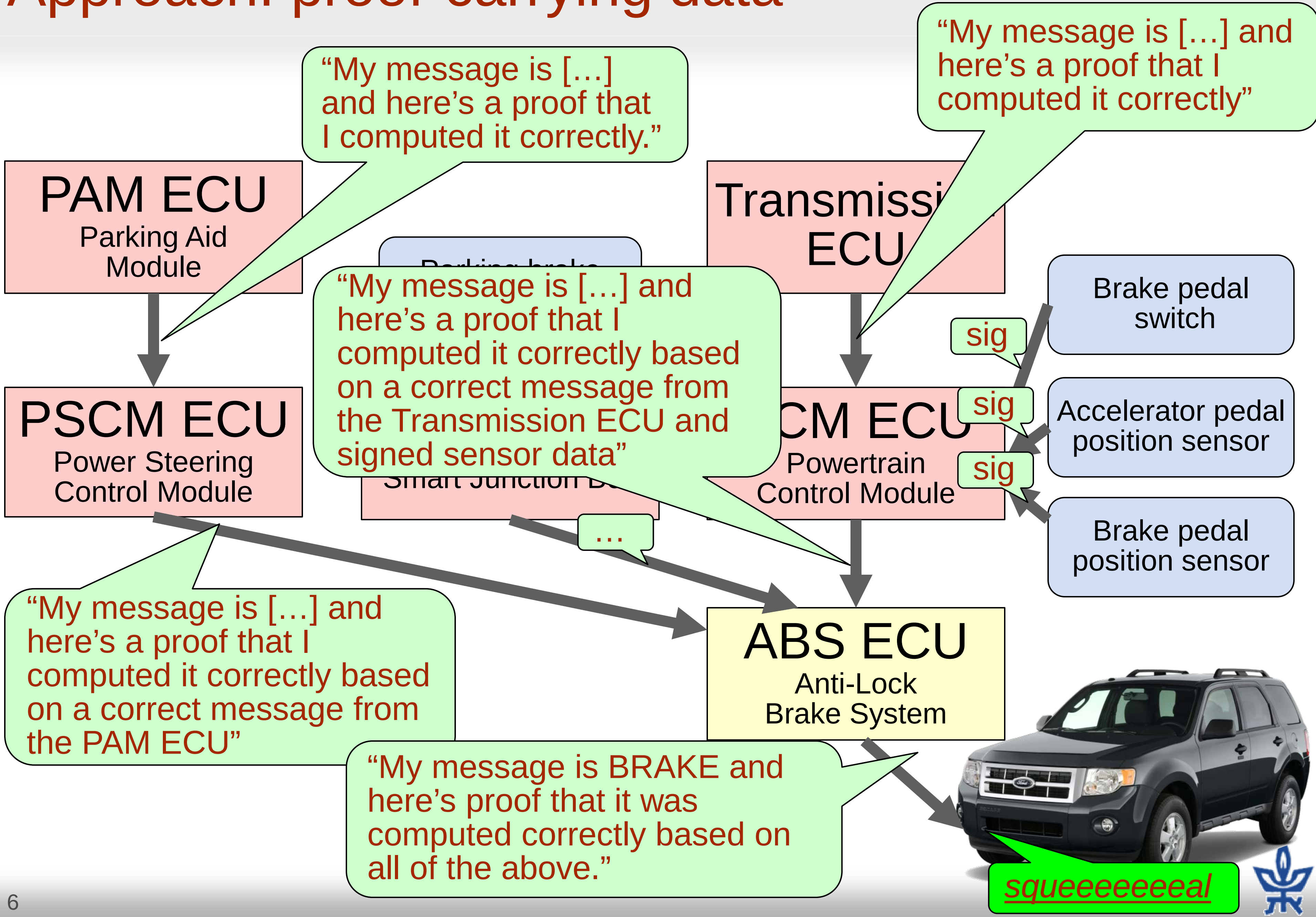
07 36: 0B 34 00 44 …
“SJB ECU: Program firmware”

07 36: 03 B1 7E 80 …
“SJB ECU: Crash”

07 60: 04 B1 00 3C FF ...
“ABS ECU: Engage brakes fully”

ABS ECU
Anti-Lock Brake System

Approach: proof-carrying data



“My message is […] and here’s a proof that I computed it correctly.”

“My message is […] and here’s a proof that I computed it correctly”

PAM ECU
Parking Aid Module

Transmissi
ECU

Parking brake

“My message is […] and here’s a proof that I computed it correctly based on a correct message from the Transmission ECU and signed sensor data”

Brake pedal switch

sig

sig

sig

Accelerator pedal position sensor

Brake pedal position sensor

PSCM ECU
Power Steering Control Module

Smart Junction Bo

CM ECU
Powertrain Control Module

…

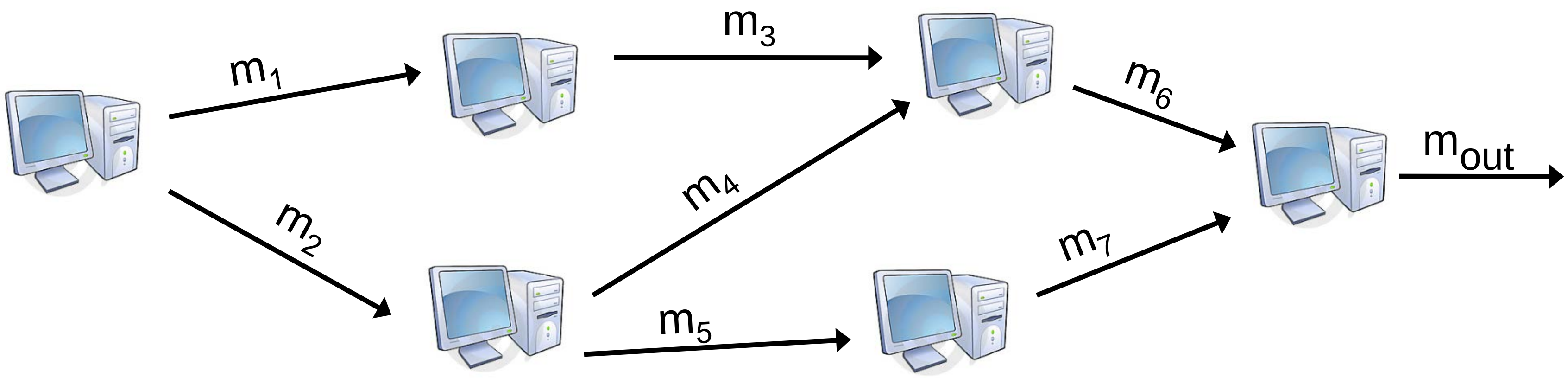
“My message is […] and here’s a proof that I computed it correctly based on a correct message from the PAM ECU”

ABS ECU
Anti-Lock Brake System

“My message is BRAKE and here’s proof that it was computed correctly based on all of the above.”

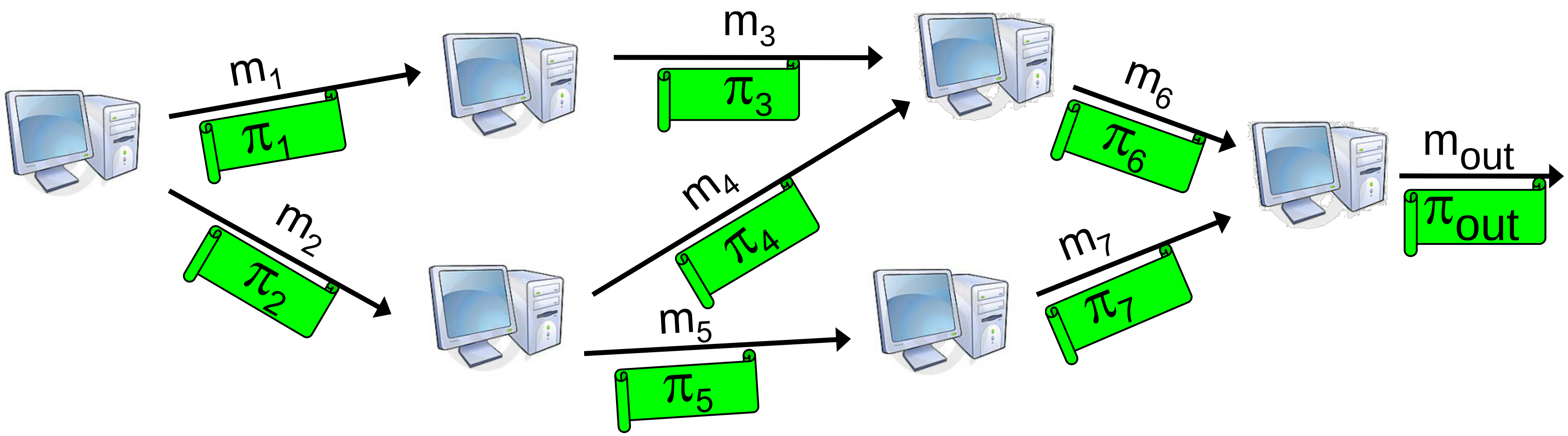
squeeeeeeeeal

Integrity via Proof-Carrying Data



- Diverse network, containing untrustworthy parties and unreliable components.
- Enforce correctness of the messages and ultimate results.

Integrity via Proof-Carrying Data (cont.)



- Every message is augmented with a proof attesting to its compliance” with a prescribed policy.
- Compliance can express any property that can be verified by locally checking every node.
- Proofs can be verified efficiently and retroactively.
- If the final proof is OK, we can trust the result.

The road to Proof-Carrying Data

Feasibility			Network		C program size		Program running time		P
Theory	Proto-type	Fast	1 hop	Any	Small	Any	Short	Any	
✓			✓						[Micali 94] [Groth 2010]
✓			✓	✓					[Chiesa Tromer 2010]
✓	✓		✓		✓		✓		[Ben-Sasson Chiesa Genkin Tromer Virza 2013] [Parno Gentry Howell Raykova 2013]
✓	✓		✓		✓	✓	✓		[Ben-Sasson Chiesa Tromer Virza 2014]
✓	✓	?	✓	✓	✓	✓	✓	✓	upcoming

Used in Zerocash: anonymous Bitcoin
[Ben-Sasson Chiesa Garman Green Miers Tromer Virza 2013]

The correct execution of arbitrary C programs can be verified in 5 milliseconds using 230-byte proofs.

SCIPR Lab

The road to Proof-Carrying Data on the road

- More efficient PCD: cost, latency
- Formally defining the critical security properties within a vehicle, and then applying PCD to enforce them
- Extending to V2V and V2I
  - Trusting other cars
    (that trust other cars
      (that trust other cars
        (that trust infrastructure (and other cars))))
  - Protecting privacy using zero-knowledge proofs

SCIPR Lab **scipr-lab.org**