Fingerprinting ECUs for Vehicle Intrusion Detection

Kyong-Tak Cho, Kang G. Shin, *University of Michigan*

~~Fingerprinting ECUs for Vehicle Intrusion Detection~~

Kyong-Tak Cho, Kang G. Shin, *University of Michigan*

How To Tell if Your Car is h4xd

Kyong-Tak Cho, Kang G. Shin, *University of Michigan*

What we know

- Cars introduce a number of attack vectors in 2016
  - Bluetooth, Cellular, etc.
- ECUs can be compromised by remote attacks
  - UCSD + UW work presented by Surya
- In 2014, Miller et. al compromised a Jeep Cherokee remotely, triggering a recall of 1.4M vehicles
- **tl;dr: Cars are computers in 2016, and computers have security problems**

35,092

“GM Took 5 Years to Fix Full Takeover Hack”

https://www.wired.com/2015/09/gm-took-5-years-fix-full-takeover-hack-millions-onstar-cars/

Problem

- Security solutions in cars are *limited*
  - Message Authentication Systems
  - IDS systems
- Modern IDS systems are *not perfect*
  - Quantifiable failure scenarios where no guarantees are kept

Solution

- *Clock based IDS, CIDS, which uses ECU fingerprinting to detect Vehicle Intrusion*

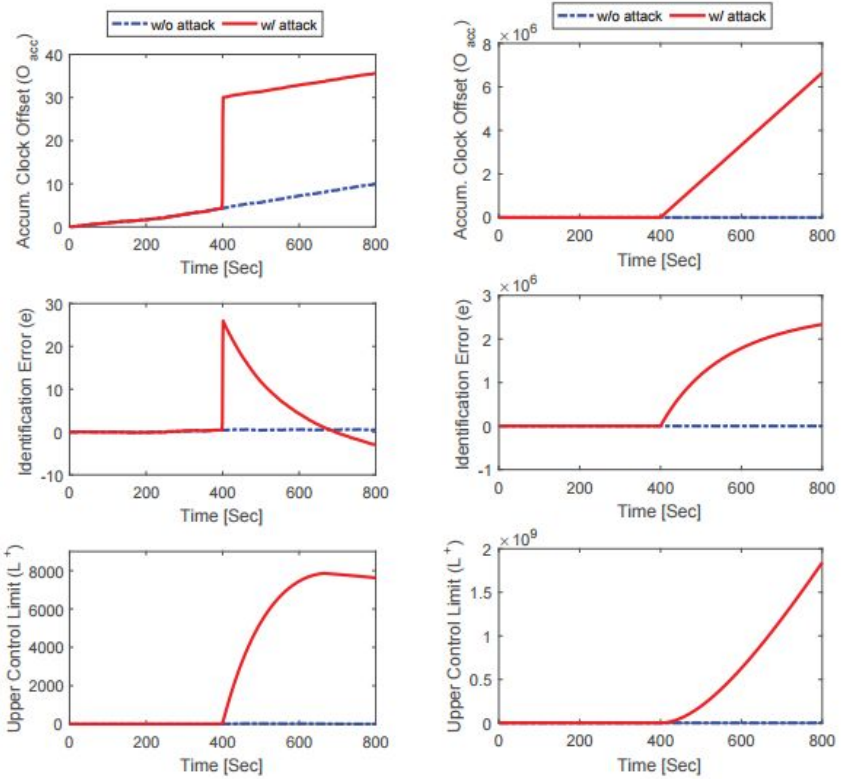
Attack Model

- Fabrication
  - Strong attacker injects packets onto the in-vehicle network via compromised ECU
  - DoS, Malicious Packets, etc.
- Suspension
  - Weak attacker stops/suspends compromised ECU communication with CAN bus
    - Attacks both the ECU and related ECUs
- Masquerade
  - Two compromised ECUs, one strongly and one weakly compromised
  - Mask the fact that one ECU is down by using another ECU to ping messages

Clock Skew Fingerprints

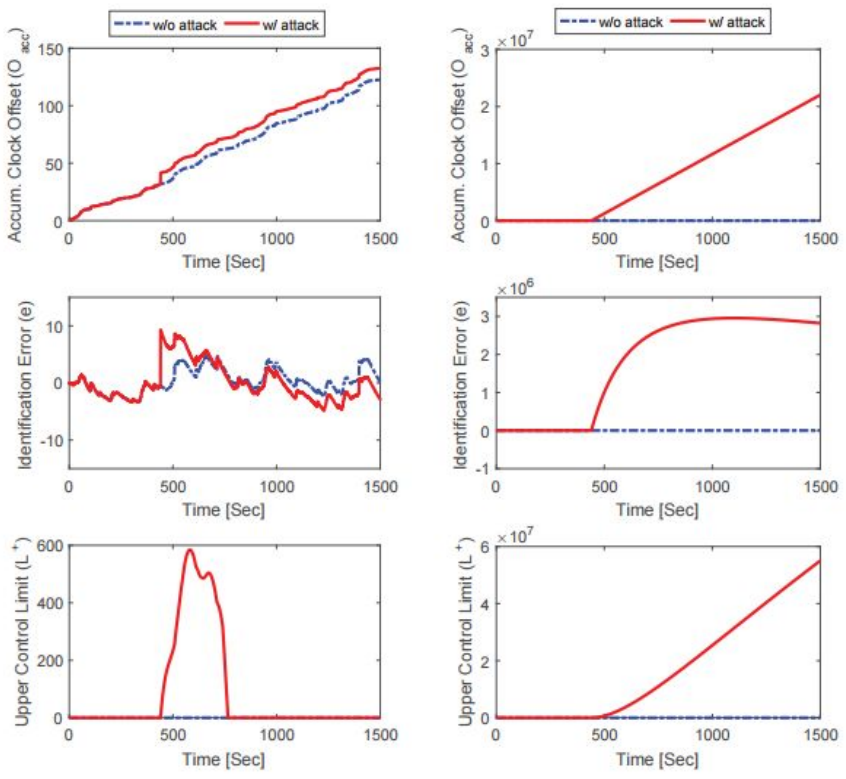
- Clock Skew: *The difference between the frequencies of clock* C_i and the true clock C_{true}
- We can use *skew* to uniquely fingerprint different ECUs in the vehicle, thus enabling *verification of where the message came from*
- **How does this prevent masquerade attacks?**

Evaluation



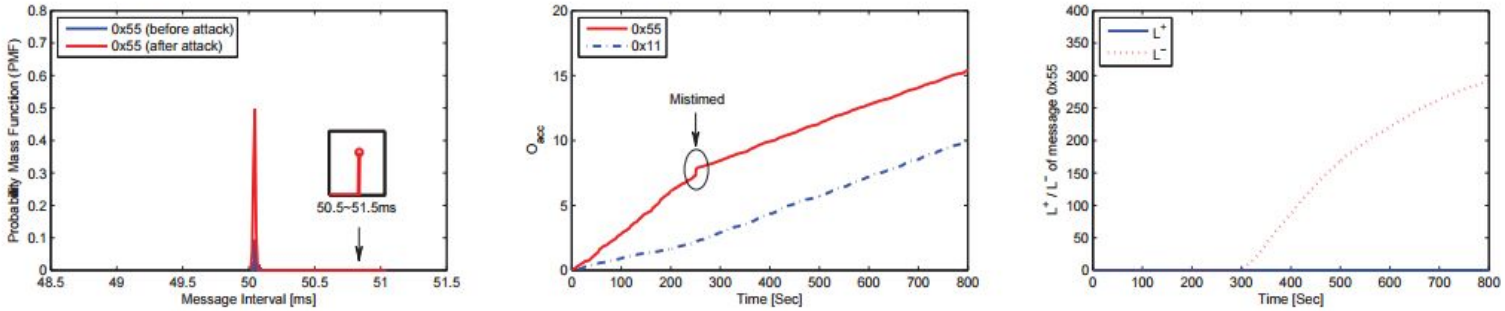
(a) Fabrication attack. (b) Suspension attack.

Figure 6: CIDS defending fabrication attack (left) and suspension attack (right) in a CAN bus prototype.

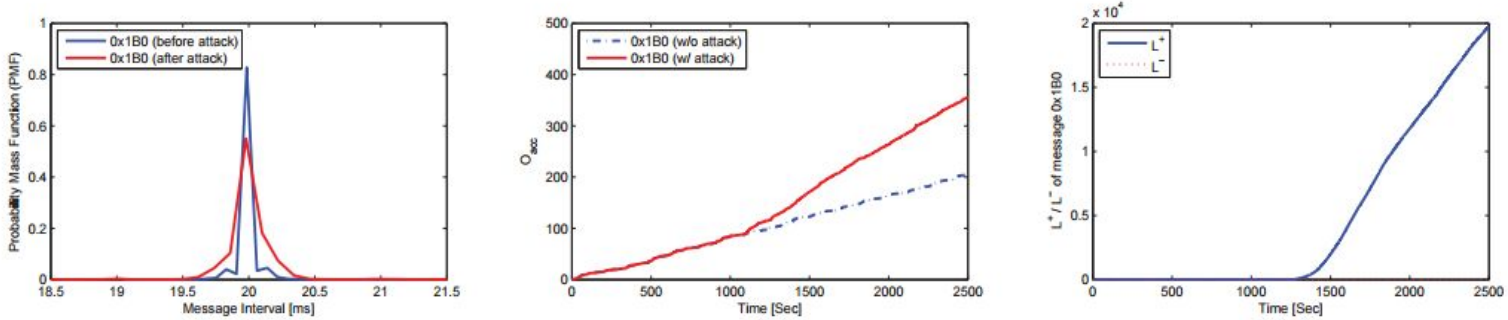


(a) Fabrication attack. (b) Suspension attack.

Figure 7: CIDS defending fabrication attack (left) and suspension attack (right) in a Honda Accord 2013.



(a) CAN bus prototype.



(b) Real vehicle.

Figure 8: Masquerade attack — Probability mass function of message intervals (left), changes in accumulated clock offsets (middle), and control limits (right) derived in CIDS.

Limitations

- The algorithm for estimating clock skew can be tweaked for more accurate results, and thus more accurate fingerprinting
- Spoofing clock skew by heating up ECU components
- CANnot extract clock skew without periodic messages, and ECUs are not homogenous

Discussion