CANnon: Stealthy Remote Shutdown Attacks via Automotive MCUs

Sekar Kulandaivel, *Automotive Security PhD Candidate*

Motivation

Against evolving threat landscape

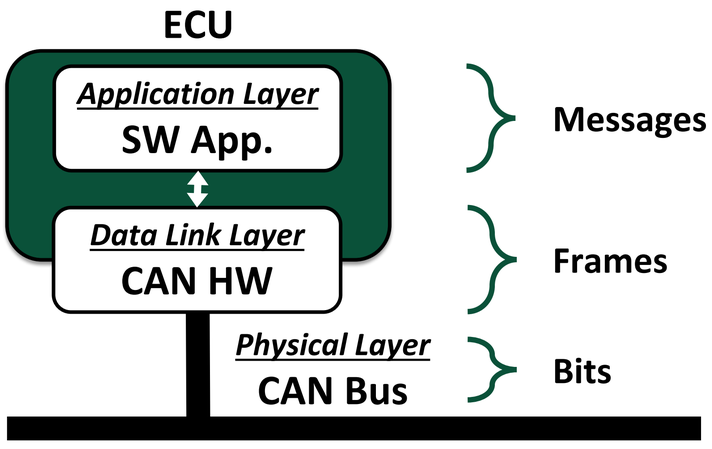
- Message authentication
- Intrusion detection systems
- Secure hardware solutions

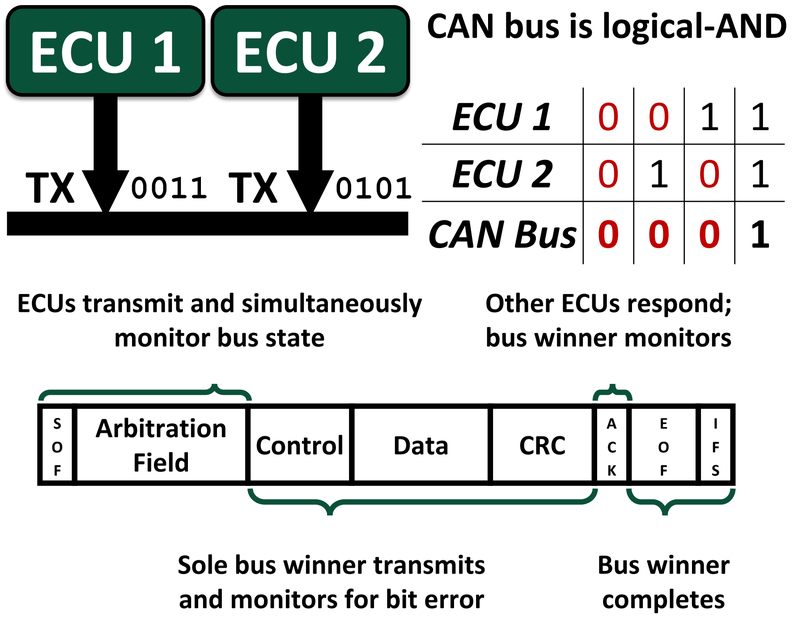
Limitation of current attacks

Existing attacks cannot simultaneously be:

1. Remote (software-based attack)
2. Stealthy (against modern defenses)
3. Reliable (practical in real scenario)

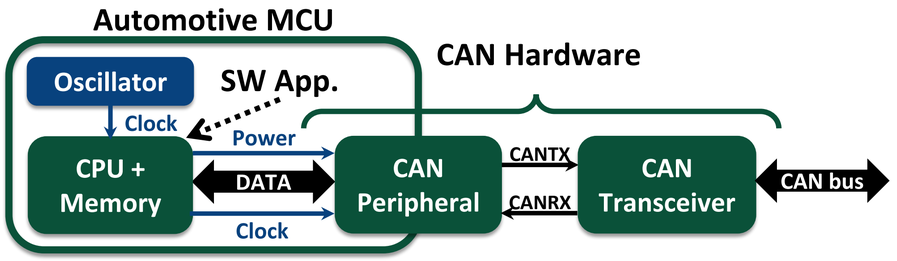
Background



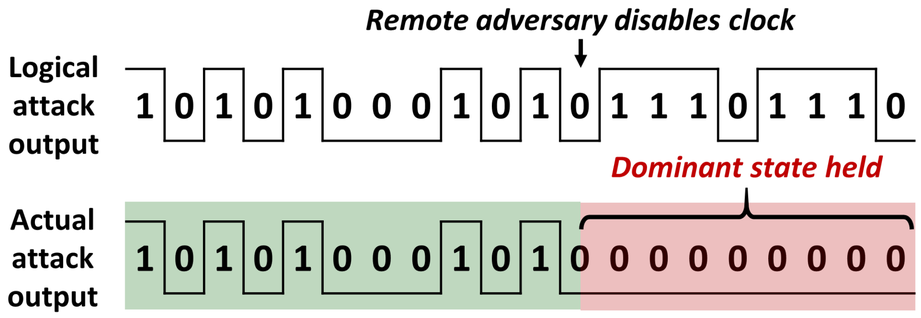


Attack Insight

Modern ECU design with peripherals

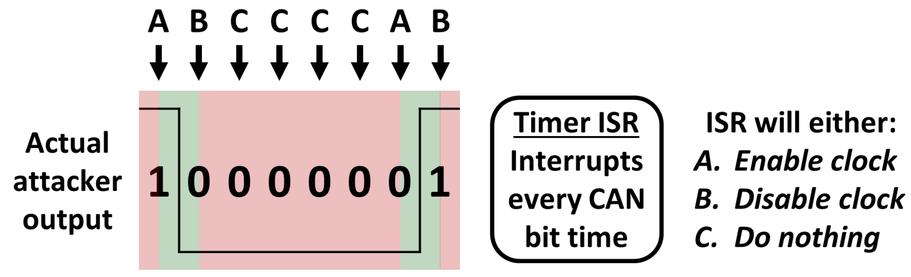


Clock control is now possible

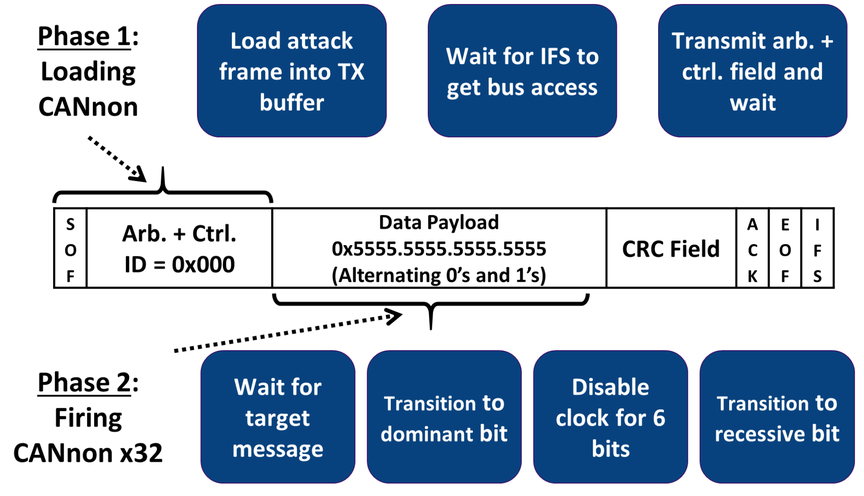


CANnon Design

Reliable control of peripheral clock



Targeting and shutting down a victim



Key Results

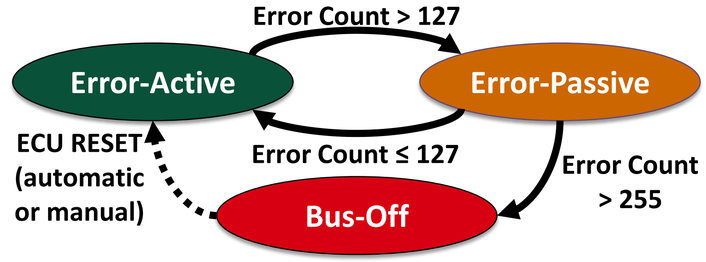
CANnon attack alternatives

- Firing with SOF bit
- Firing with ACKs

Practical challenges

- Period deviation in victim frames
  - Guarantee victim frame time by forcing ordered queuing of frames
- Interruptions by higher-priority frames
  - Use CANvas network mapper to identify highest-priority frame

Attacks on two real vehicles



- Powertrain ECU of `17 Ford Focus
  - Shutdown in 2ms but auto-recovers
- Power steering ECU of `09 Toyota Prius
  - Permanent shutdown in 700ms

Countermeasures

Prevention

- Forced clear of transmit buffers
- Removal of clock gating for CAN

Detection

- Detecting bit-wise voltage spikes
- On-chip power analysis

Carnegie Mellon University
CyLab