**Reliable control of peripheral clock**

**Targeting and shutting down a victim**

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

**CANnon: Stealthy Remote Shutdown Attacks via Automotive MCUs**

**Sekar Kulandaivel, Automotive Security PhD Candidate**

**Background**

- **ECU**
  - Application Layer
    - SW App.
  - Data Link Layer
    - CAN HW
  - Physical Layer
    - CAN Bus

**CANnon Design**

- **Reliable control of peripheral clock**
  - A B C C C A B
  - Actual attacker output
  - Timer ISR
    - Interrupts every CAN bit time
  - ISR will either:
    - A. Enable clock
    - B. Disable clock
    - C. Do nothing

**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)

**Attack Insight**

Modern ECU design with peripherals

- Oscillator
- Clock
- Power
- SW App.
- CAN Hardware
- CAN Peripheral
- CAN Transceiver
- CAN TX
- CAN RX

**Clock control is now possible**

Remote adversary disables clock

- Logical attack output
  - 1 0 1 0 1 0 0 1 0 1 0 1 1 1 0 1 1 1 0
  - Dominant state held
- Actual attack output
  - 1 0 1 0 1 0 0 1 0 1 0 0 0 0 0 0 0 0

**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 CANvases network mapper to identify highest-priority frame

**Attacks on two real vehicles**

- Powertrain ECU of ‘17 Ford Focus
  - Shutdown in 2ms but auto-recover
- 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