Exposing New Vulnerabilities of Error Handling Mechanism in CAN

Khaled Serag†, Rohit Bhatia†, Vireshwar Kumar*,
Z. Berkay Celik†, Dongyan Xu†

† Purdue University
*Indian Institute of Technology Delhi

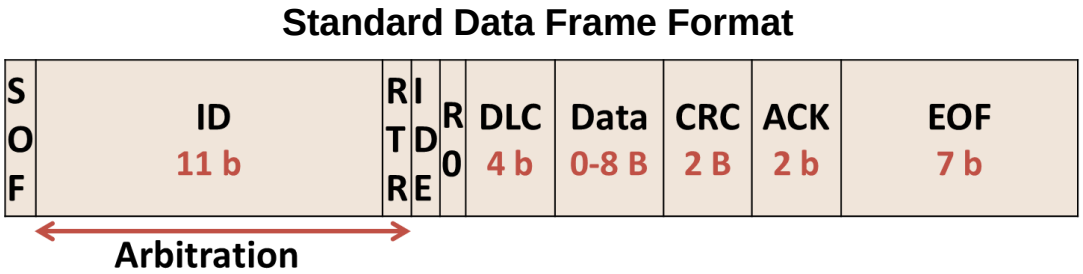
Background and Motivation

- CAN: Communication protocol for automobiles and industrial automation
  - Wiring
  - Decentralization
  - Noise Resistance
  - Effective error handling and fault confinement mechanism
- We investigate CAN's error handling and fault confinement mechanism

Background and Motivation

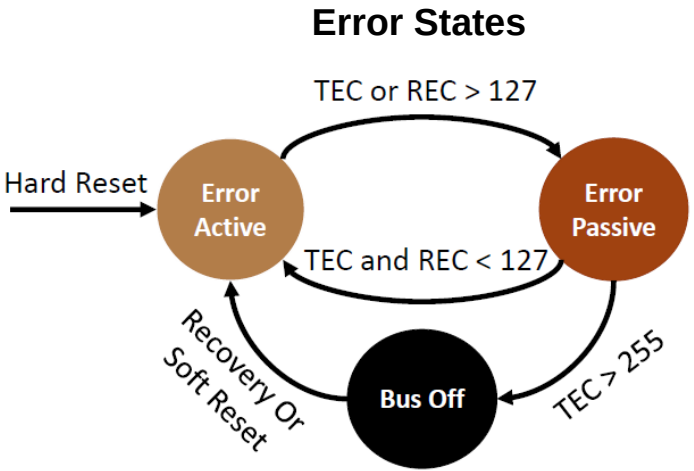
Background and Motivation

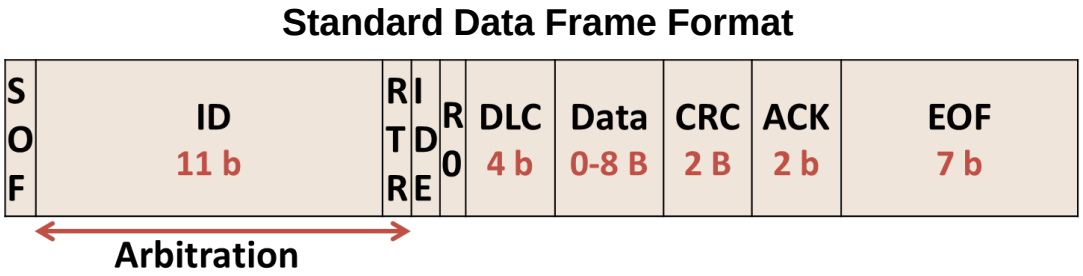
- CAN Operation
  - Format



Background and Motivation

- CAN Operation
  - Format
- CAN error handling and fault confinement mechanism
  - Error Counters: TEC, REC
  - Error States



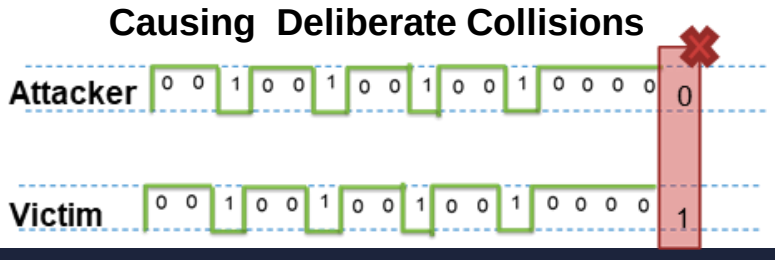


Background and Motivation

- Attacker can remotely compromise certain ECUs (i.e., telematics)
  - Weak security of ECUs has been demonstrated

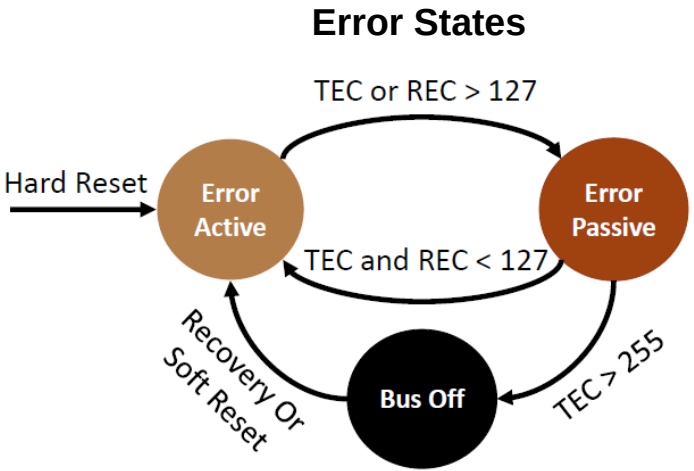
Background and Motivation

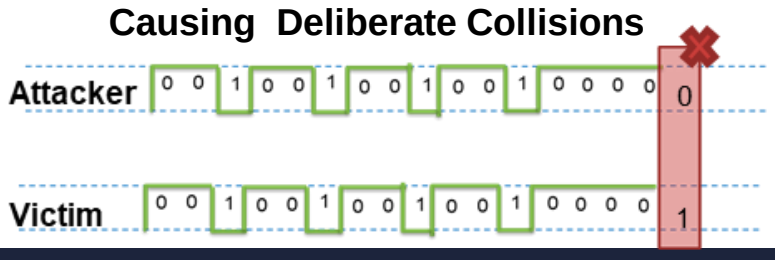
- Attacker can remotely compromise certain ECUs (i.e., telematics)
  - Weak security of ECUs has been demonstrated
- New: Attacks against error handling
  - Simultaneous transmission and collisions
  - Attacker can dictate a victim's error state
  - Security impact of error handling is understudied



Background and Motivation

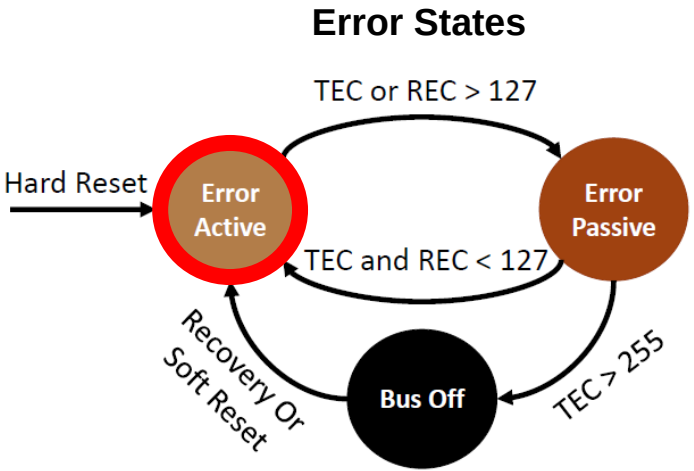
- Attacker can remotely compromise certain ECUs (i.e., telematics)
  - Weak security of ECUs has been demonstrated
- New: Attacks against error handling
  - Simultaneous transmission and collisions
  - Attacker can dictate a victim's error state
  - Security impact of error handling is understudied

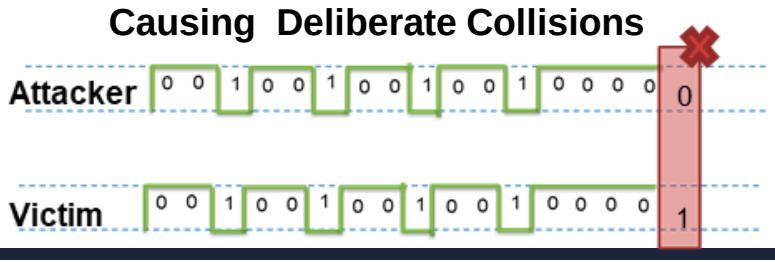




Background and Motivation

- Attacker can remotely compromise certain ECUs (i.e., telematics)
  - Weak security of ECUs has been demonstrated
- New: Attacks against error handling
  - Simultaneous transmission and collisions
  - Attacker can dictate a victim's error state
  - Security impact of error handling is understudied

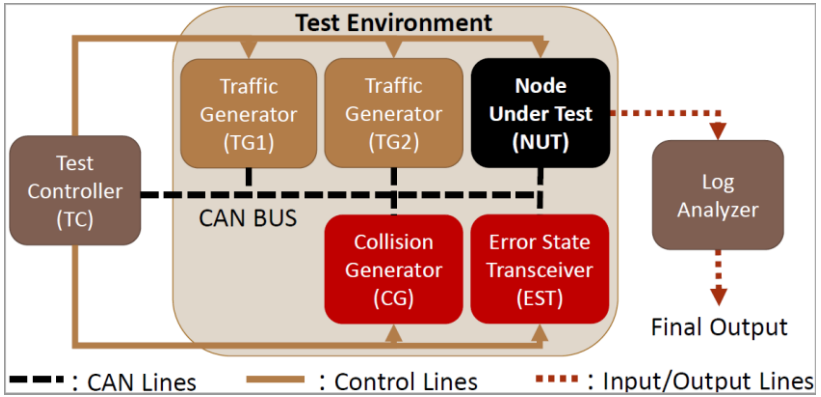




CANOX: A Protocol Testing Tool For CAN

- CAN Operation eXplorer (CANOX)
  - Explores the impact of operating outside of the error active state
  - Reveals possible vulnerabilities

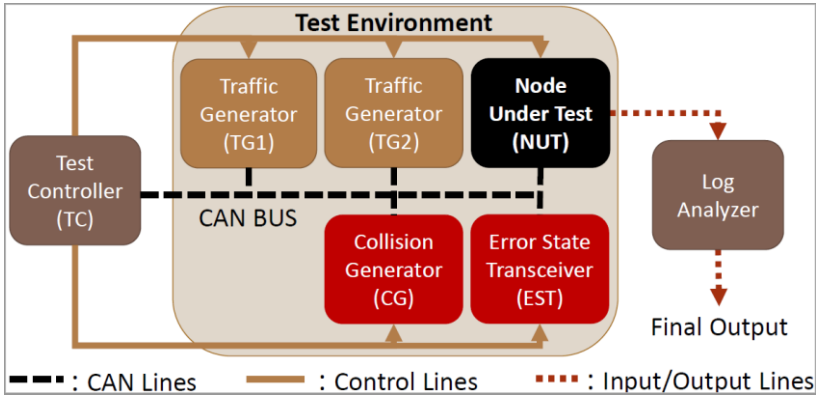
CANOX Architecture



CANOX: A Protocol Testing Tool For CAN

- CAN Operation eXplorer (CANOX)
  - Explores the impact of operating outside of the error active state
  - Reveals possible vulnerabilities
- Node under Test (NUT)
  - logs its metrics throughout the experiment

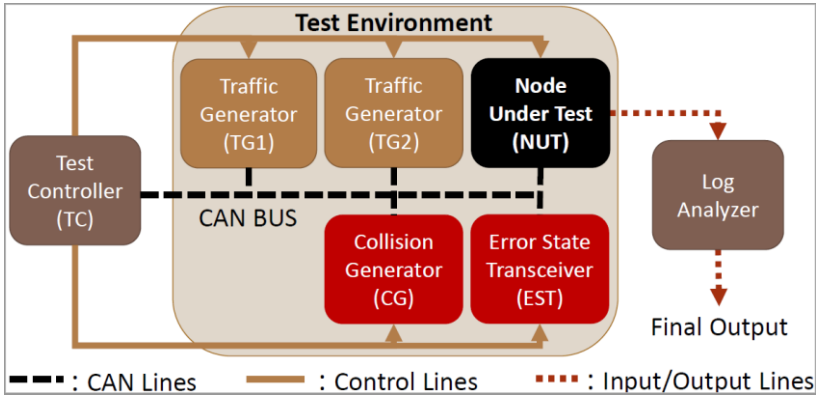
CANOX Architecture



CANOX: A Protocol Testing Tool For CAN

- Scenarios
  - Single Collision Scenario
  - Successive Transmission Scenario
  - Single Transmission Scenario

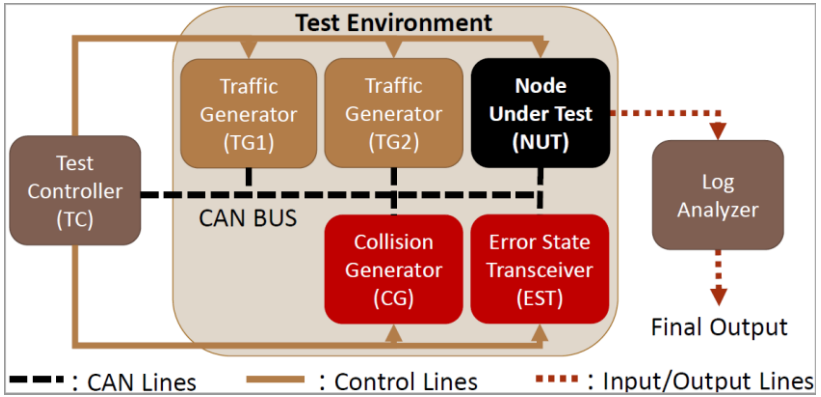
CANOX Architecture



CANOX: A Protocol Testing Tool For CAN

- Scenarios
  - Single Collision Scenario
  - Successive Transmission Scenario
  - Single Transmission Scenario
- Behavioral Metrics
  - Standby Delay (SD)
  - TEC Change (TECC)

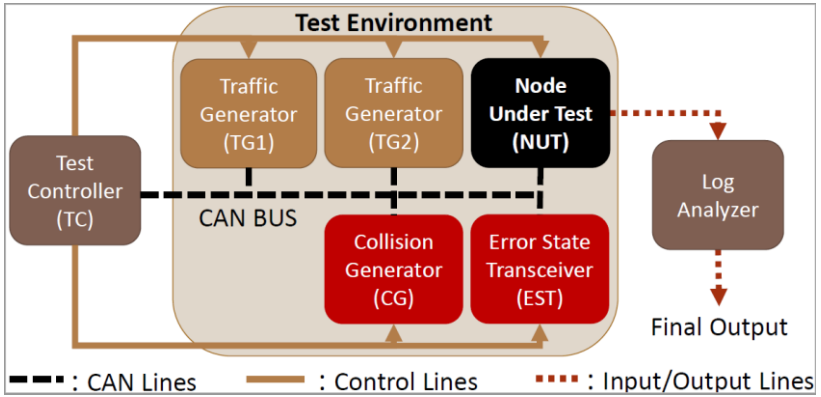
CANOX Architecture



CANOX: A Protocol Testing Tool For CAN

- Scenarios
  - Single Collision Scenario
  - Successive Transmission Scenario
  - Single Transmission Scenario
- Behavioral Metrics
  - Standby Delay (SD)
  - TEC Change (TECC)
- Vary error state and bus traffic

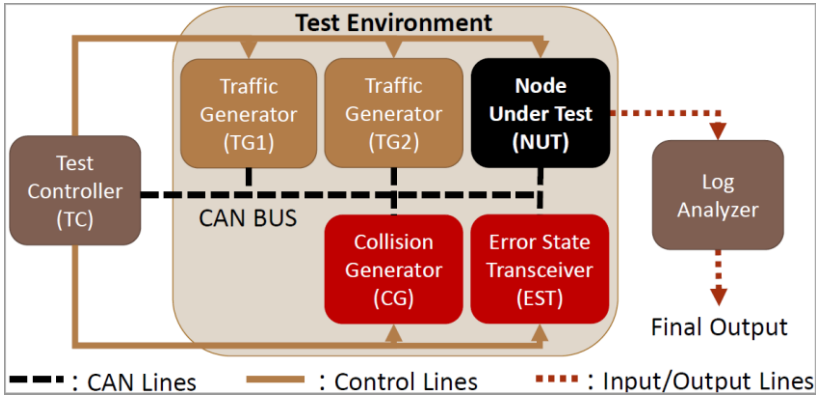
CANOX Architecture



CANOX: A Protocol Testing Tool For CAN

- Scenarios
  - Single Collision Scenario
  - Successive Transmission Scenario
  - Single Transmission Scenario
- Behavioral Metrics
  - Standby Delay (SD)
  - TEC Change (TECC)
- Vary error state and bus traffic
- Log analyzer detects violations

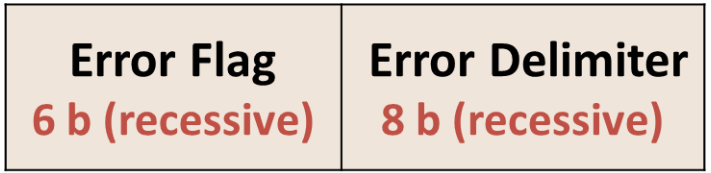
CANOX Architecture



Vulnerability 1: Passive Error Regeneration

- Failure to send a passive error frame generates a new error

Passive Error Frame

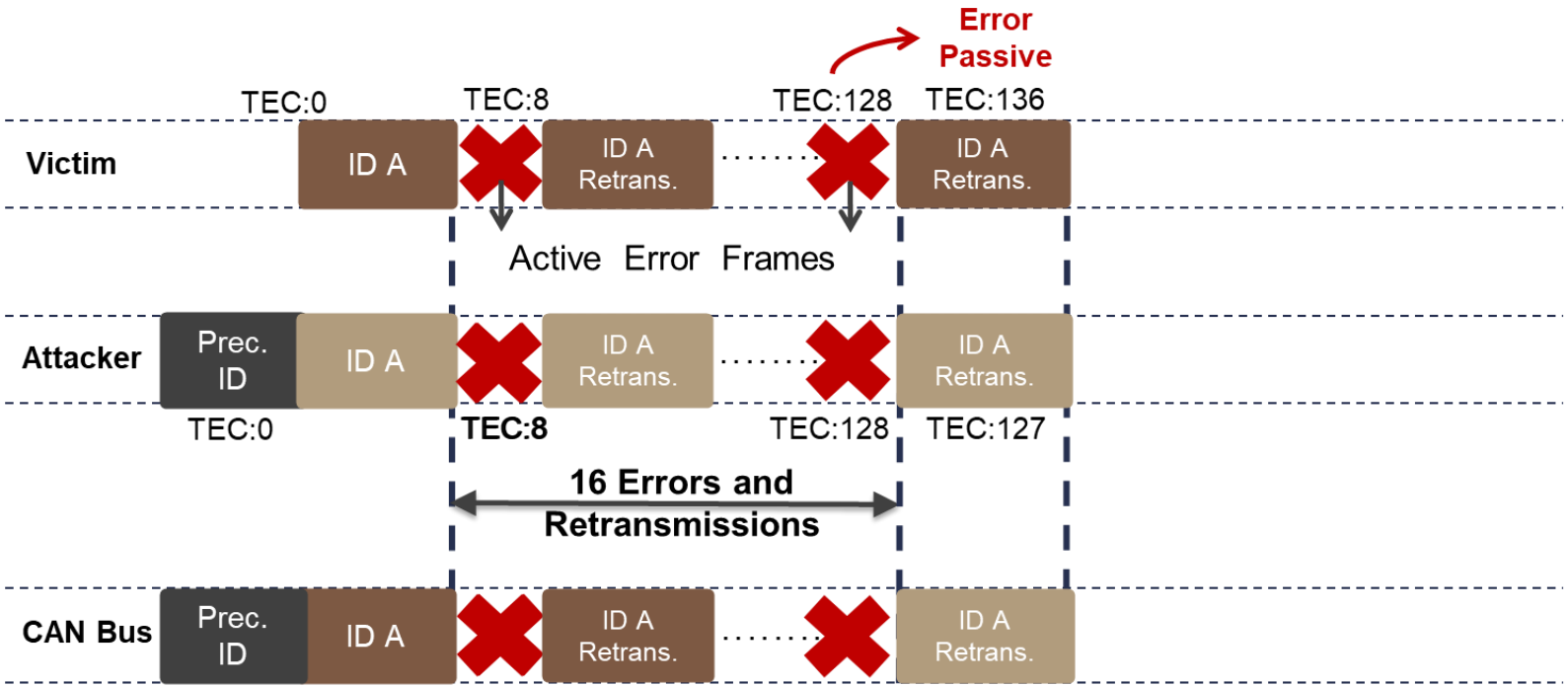


Vulnerability 1: Passive Error Regeneration

- Failure to send a passive error frame generates a new error

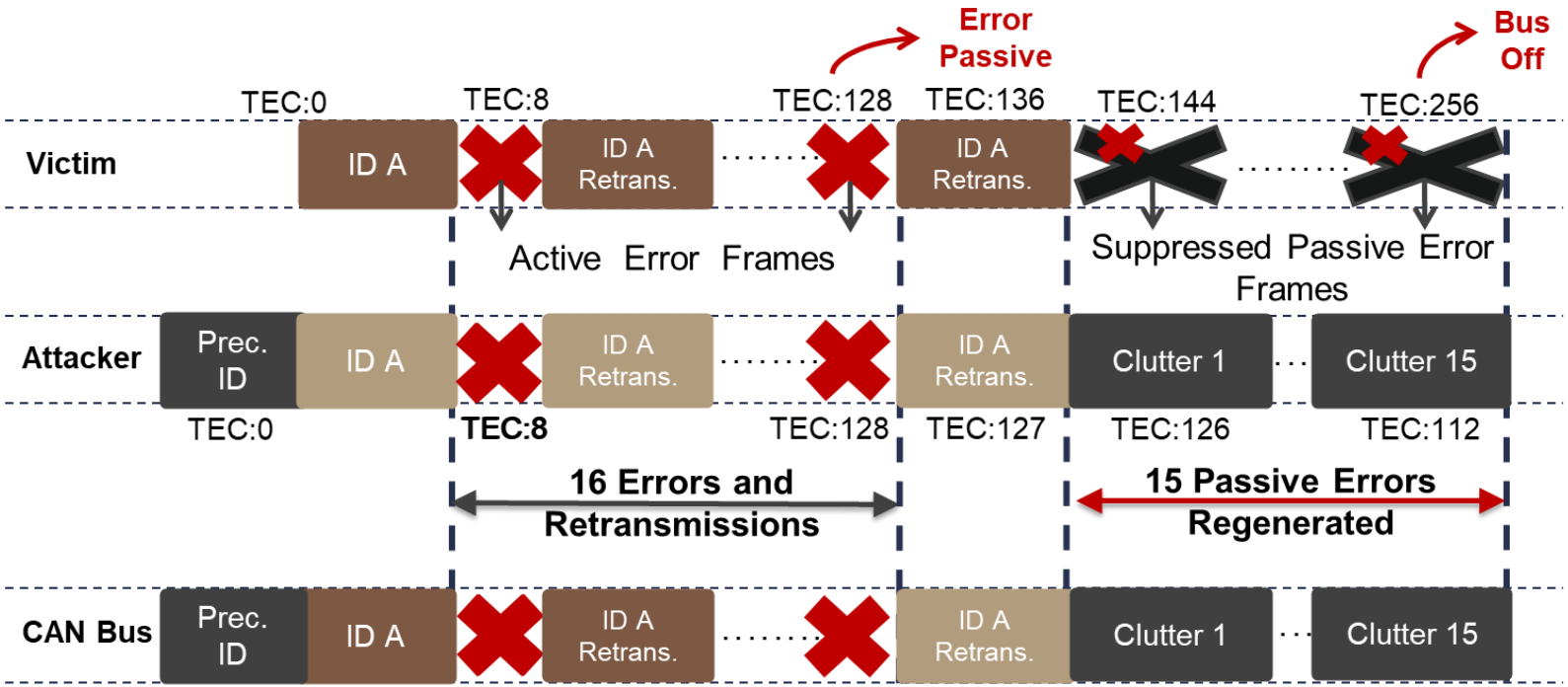
Vulnerability 1: Passive Error Regeneration

- Failure to send a passive error frame generates a new error



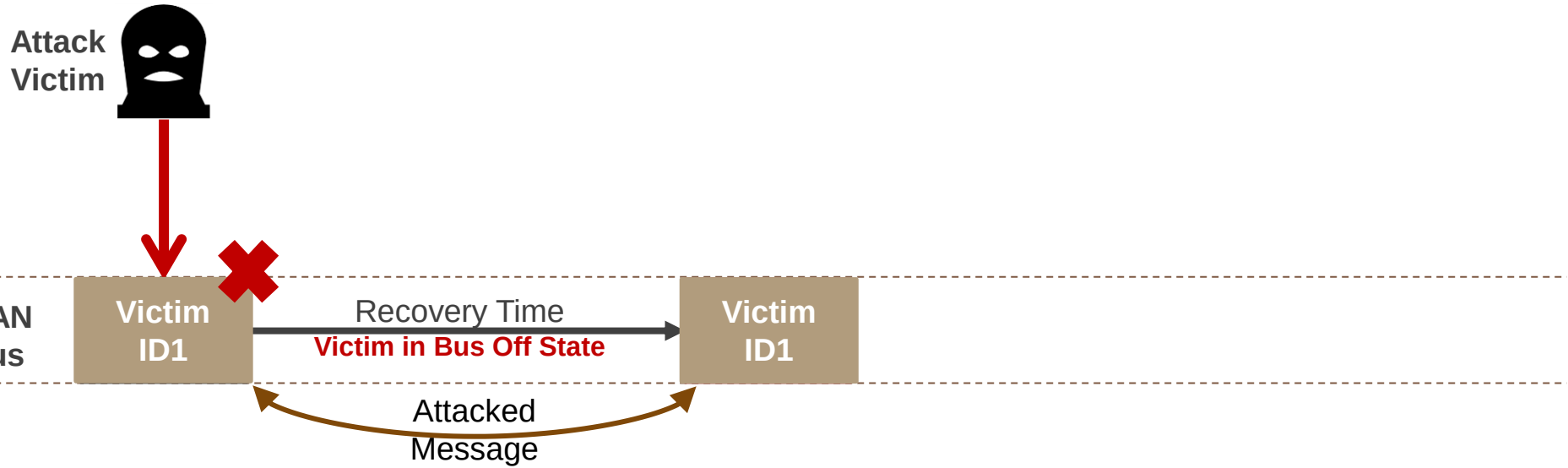
Vulnerability 1: Passive Error Regeneration

- Failure to send a passive error frame generates a new error



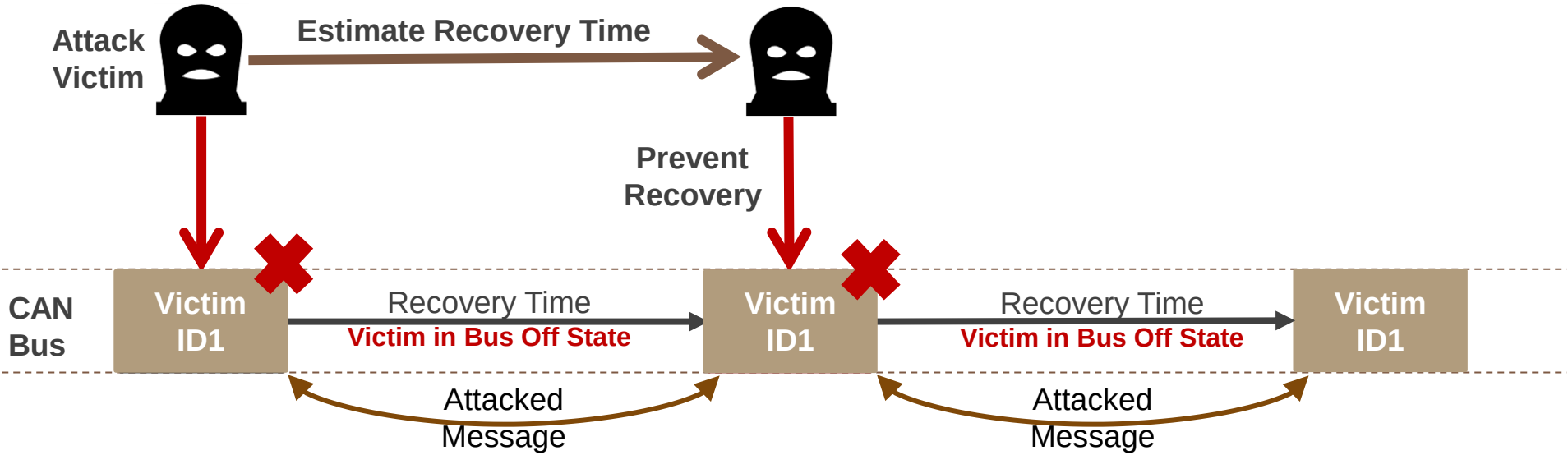
Vulnerability 2: Deterministic Recovery Behavior

- At recovery, an ECU will send the same message that failed to transmit



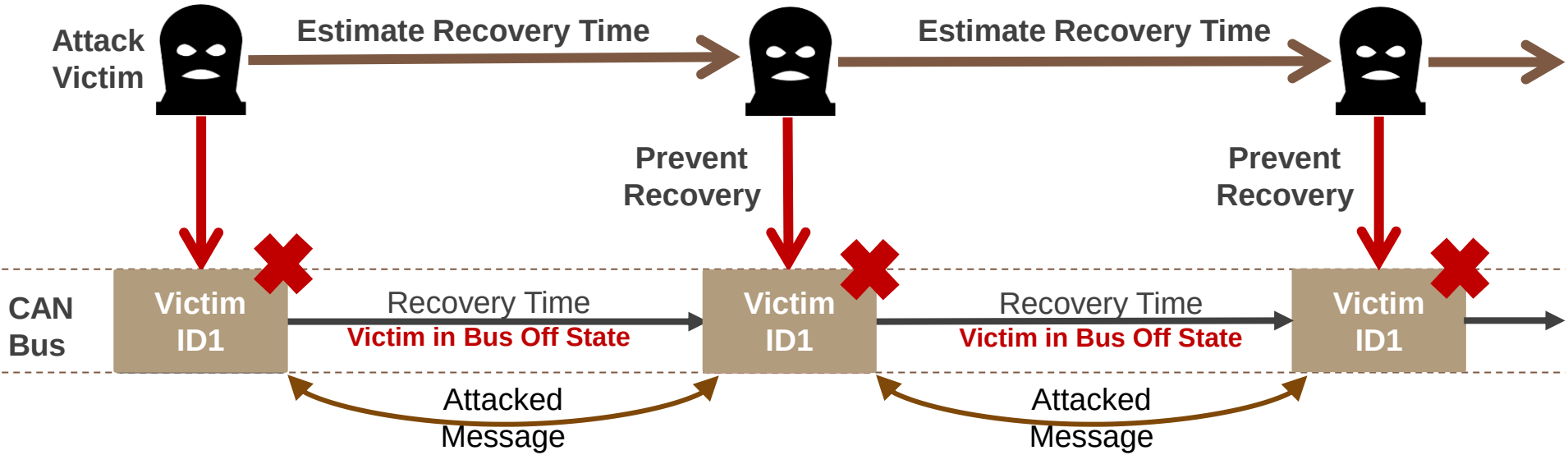
Vulnerability 2: Deterministic Recovery Behavior

- At recovery, an ECU will send the same message that failed to transmit



Vulnerability 2: Deterministic Recovery Behavior

- At recovery, an ECU will send the same message that failed to transmit

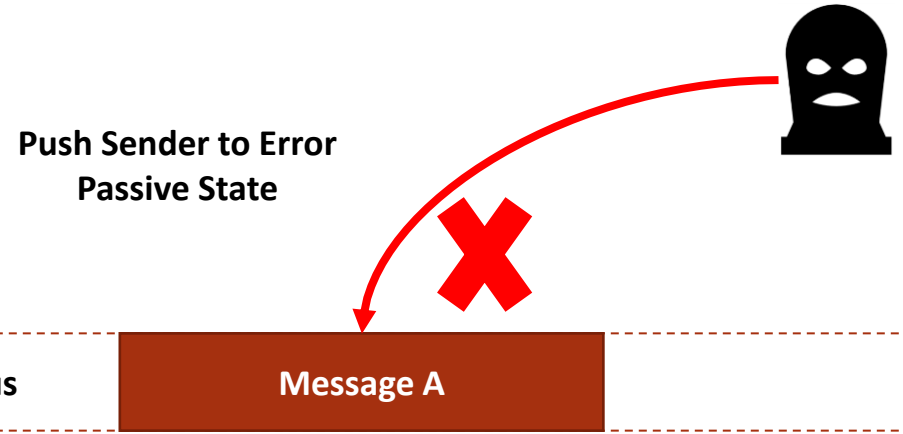


Vulnerability 3: Error State Outspokenness

- The error state of a message sender is detectable by any node on the bus
- This could be exploited to map the network

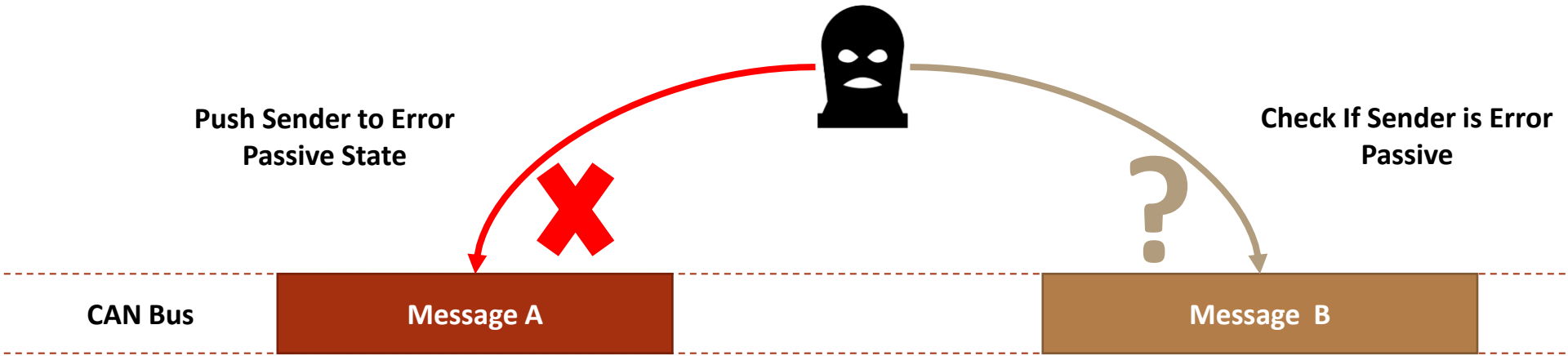
Vulnerability 3: Error State Outspokenness

- The error state of a message sender is detectable by any node on the bus
- This could be exploited to map the network



Vulnerability 3: Error State Outspokenness

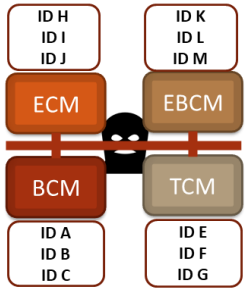
- The error state of a message sender is detectable by any node on the bus
- This could be exploited to map the network



“Scan-Then-Strike” (STS) Attack

- **Threat Model:**
  - Remotely compromised ECU able to execute arbitrary code
  - No physical access or previous knowledge of the vehicle

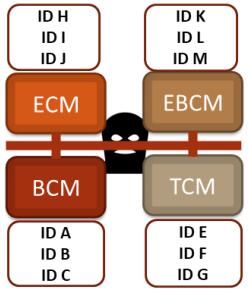
Attacker observing a vehicular CAN bus

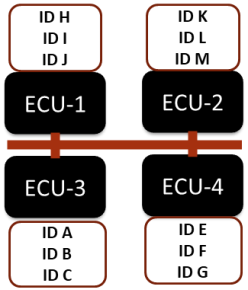


“Scan-Then-Strike” (STS) Attack

- **Threat Model:**
  - Remotely compromised ECU able to execute arbitrary code
  - No physical access or previous knowledge of the vehicle

Attacker observing a vehicular CAN bus



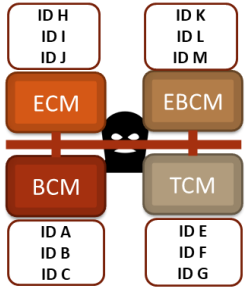


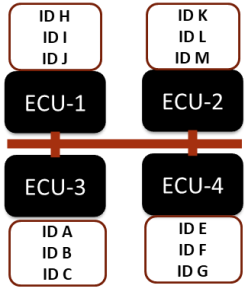
1-Network Mapping

“Scan-Then-Strike” (STS) Attack

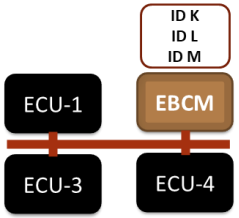
- **Threat Model:**
  - Remotely compromised ECU able to execute arbitrary code
  - No physical access or previous knowledge of the vehicle

Attacker observing a vehicular CAN bus





1-Network Mapping

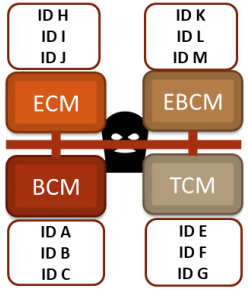


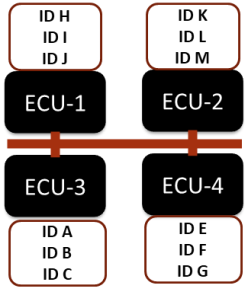
2-Victim Identification

“Scan-Then-Strike” (STS) Attack

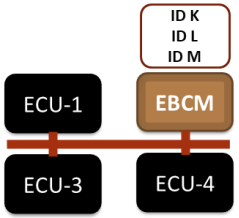
- **Threat Model:**
  - Remotely compromised ECU able to execute arbitrary code
  - No physical access or previous knowledge of the vehicle

Attacker observing a vehicular CAN bus

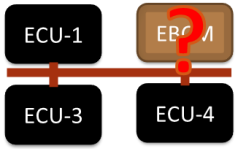




1-Network Mapping



2-Victim Identification

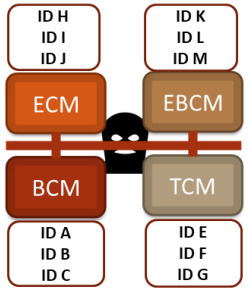


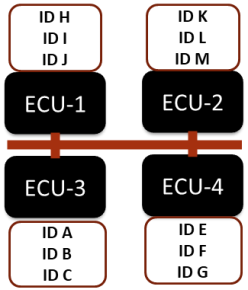
3-Learning Recovery Behavior

“Scan-Then-Strike” (STS) Attack

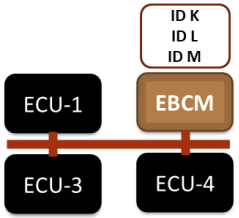
- **Threat Model:**
  - Remotely compromised ECU able to execute arbitrary code
  - No physical access or previous knowledge of the vehicle

Attacker observing a vehicular CAN bus

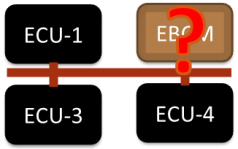




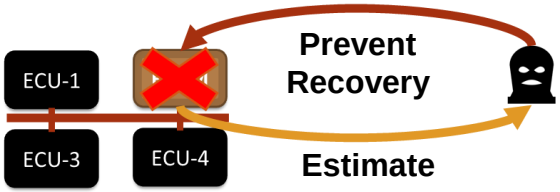
1-Network Mapping



2-Victim Identification



3-Learning Recovery Behavior



4-Suppression and Recovery Prevention

Results

Testbed Results

ECU #	Suppression Rate
ECU-1	99.9%
ECU-2	99.9%
ECU-3	99.9%
ECU-4	99.9%

Results

Testbed Results

ECU #	Suppression Rate
ECU-1	99.9%
ECU-2	99.9%
ECU-3	99.9%
ECU-4	99.9%

$$Srate = \frac{Bus\ Off\ Time}{Total\ Time}$$

Results

Testbed Results

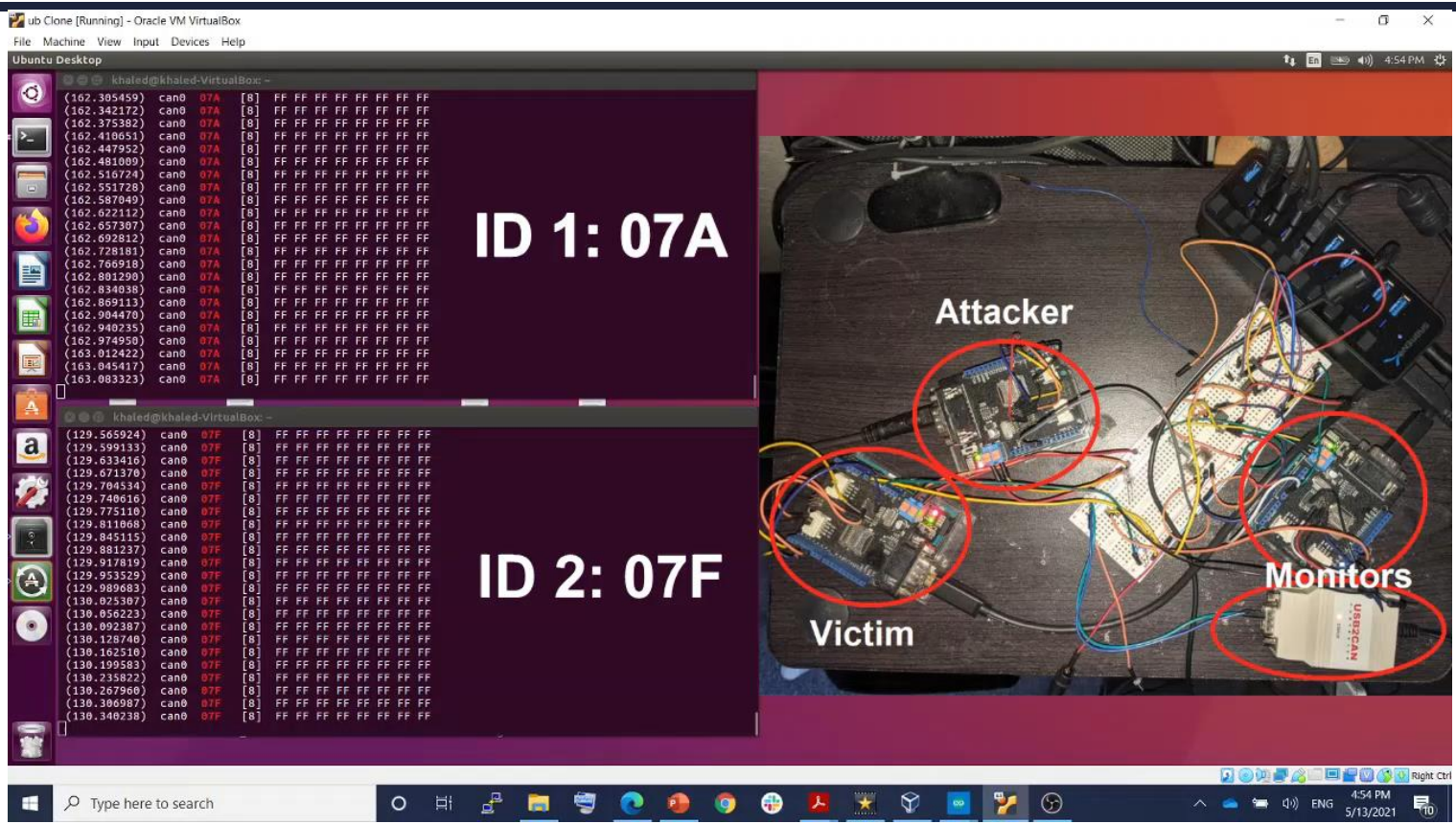
ECU #	Suppression Rate
ECU-1	99.9%
ECU-2	99.9%
ECU-3	99.9%
ECU-4	99.9%

$$Srate = \frac{Bus\ Off\ Time}{Total\ Time}$$

Vehicle Results

ECU #	Function	Suppression Rate
ECU-1	EBCM (Brake)	97.5%
ECU-2	BCM (Body)	91.4%
ECU-3	TCM (Transmission)	85%
ECU-4	ECM (Engine)	83%

Demo


ub Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Ubuntu Desktop
4:54 PM
khaled@khaled-VirtualBox: ~
(162.305459) can0 07A [8] FF FF FF FF FF FF FF FF
(162.342172) can0 07A [8] FF FF FF FF FF FF FF FF
(162.375382) can0 07A [8] FF FF FF FF FF FF FF FF
(162.410651) can0 07A [8] FF FF FF FF FF FF FF FF
(162.447952) can0 07A [8] FF FF FF FF FF FF FF FF
(162.481009) can0 07A [8] FF FF FF FF FF FF FF FF
(162.516724) can0 07A [8] FF FF FF FF FF FF FF FF
(162.551728) can0 07A [8] FF FF FF FF FF FF FF FF
(162.587049) can0 07A [8] FF FF FF FF FF FF FF FF
(162.622112) can0 07A [8] FF FF FF FF FF FF FF FF
(162.657307) can0 07A [8] FF FF FF FF FF FF FF FF
(162.692812) can0 07A [8] FF FF FF FF FF FF FF FF
(162.728181) can0 07A [8] FF FF FF FF FF FF FF FF
(162.766918) can0 07A [8] FF FF FF FF FF FF FF FF
(162.801290) can0 07A [8] FF FF FF FF FF FF FF FF
(162.834038) can0 07A [8] FF FF FF FF FF FF FF FF
(162.869113) can0 07A [8] FF FF FF FF FF FF FF FF
(162.904470) can0 07A [8] FF FF FF FF FF FF FF FF
(162.940235) can0 07A [8] FF FF FF FF FF FF FF FF
(162.974950) can0 07A [8] FF FF FF FF FF FF FF FF
(163.012422) can0 07A [8] FF FF FF FF FF FF FF FF
(163.045417) can0 07A [8] FF FF FF FF FF FF FF FF
(163.083323) can0 07A [8] FF FF FF FF FF FF FF FF
ID 1: 07A
khaled@khaled-VirtualBox: ~
(129.565924) can0 07F [8] FF FF FF FF FF FF FF FF
(129.599133) can0 07F [8] FF FF FF FF FF FF FF FF
(129.633416) can0 07F [8] FF FF FF FF FF FF FF FF
(129.671370) can0 07F [8] FF FF FF FF FF FF FF FF
(129.704534) can0 07F [8] FF FF FF FF FF FF FF FF
(129.740616) can0 07F [8] FF FF FF FF FF FF FF FF
(129.775110) can0 07F [8] FF FF FF FF FF FF FF FF
(129.811068) can0 07F [8] FF FF FF FF FF FF FF FF
(129.845115) can0 07F [8] FF FF FF FF FF FF FF FF
(129.881237) can0 07F [8] FF FF FF FF FF FF FF FF
(129.917819) can0 07F [8] FF FF FF FF FF FF FF FF
(129.953529) can0 07F [8] FF FF FF FF FF FF FF FF
(129.989683) can0 07F [8] FF FF FF FF FF FF FF FF
(130.025307) can0 07F [8] FF FF FF FF FF FF FF FF
(130.056223) can0 07F [8] FF FF FF FF FF FF FF FF
(130.092387) can0 07F [8] FF FF FF FF FF FF FF FF
(130.128740) can0 07F [8] FF FF FF FF FF FF FF FF
(130.162510) can0 07F [8] FF FF FF FF FF FF FF FF
(130.199583) can0 07F [8] FF FF FF FF FF FF FF FF
(130.235822) can0 07F [8] FF FF FF FF FF FF FF FF
(130.267960) can0 07F [8] FF FF FF FF FF FF FF FF
(130.306987) can0 07F [8] FF FF FF FF FF FF FF FF
(130.340238) can0 07F [8] FF FF FF FF FF FF FF FF
ID 2: 07F
Attacker
Monitors
Victim
USB2CAN
Type here to search
ENG
4:54 PM
5/13/2021

Responsible Disclosure

- Reported vulnerabilities to:
  - Bosch Product Security Incident Response Team (PSIRT).
  - Cybersecurity and Infrastructure Security Agency (CISA)
    - Case opened
  - Society of Automotive Engineers (SAE)
    - Committee review for next standard revision
- Proposed mitigations to each of the discovered vulnerabilities

Conclusion

- CAN's error handling mechanism – a security weakness
- We introduced CANOX
  - A protocol testing tool to identify possible vulnerabilities
- Three new error-handling vulnerabilities revealed by CANOX
  - Each could be exploited separately
  - STS: an end-to-end attack via exploiting all three vulnerabilities
- Attack Implementation on a testbed and a real vehicle
  - Mapping Accuracy: 100%
  - Single Frame Bus Off Effectiveness: 100%
  - Persistent Bus Off Suppression Rate: 83-100%

Thank You!
Questions?

Khaled Serag: kserag@purdue.edu

This work was supported in part by the Office of Naval Research (ONR) under Grant N00014-18-1-2674.