

Ground Vehicle Security Trends, Problems, Solutions, and Future Work

Gedare Bloom, Ph.D.

gbloom@uccs.edu

Computer Science

University of Colorado Colorado Springs

IEEE Pikes Peak Chapter (Region 7 West), Computer Society

February 9, 2023

TECH

Why Car Hacking Is Nearly Impossible

Despite recent claims, your car is not about to get crashed by hackers

By David Pogue on October 23, 2015  6

October 23, 2015

source: <http://goo.gl/6NsB7R>

SCIENTIFIC
AMERICAN™

TECH HACKING

Security Experts Say That Hacking Cars Is Easy

by Jonathan Vanian

@JonathanVanian

JANUARY 26, 2016, 6:47 PM EST

FORTUNE

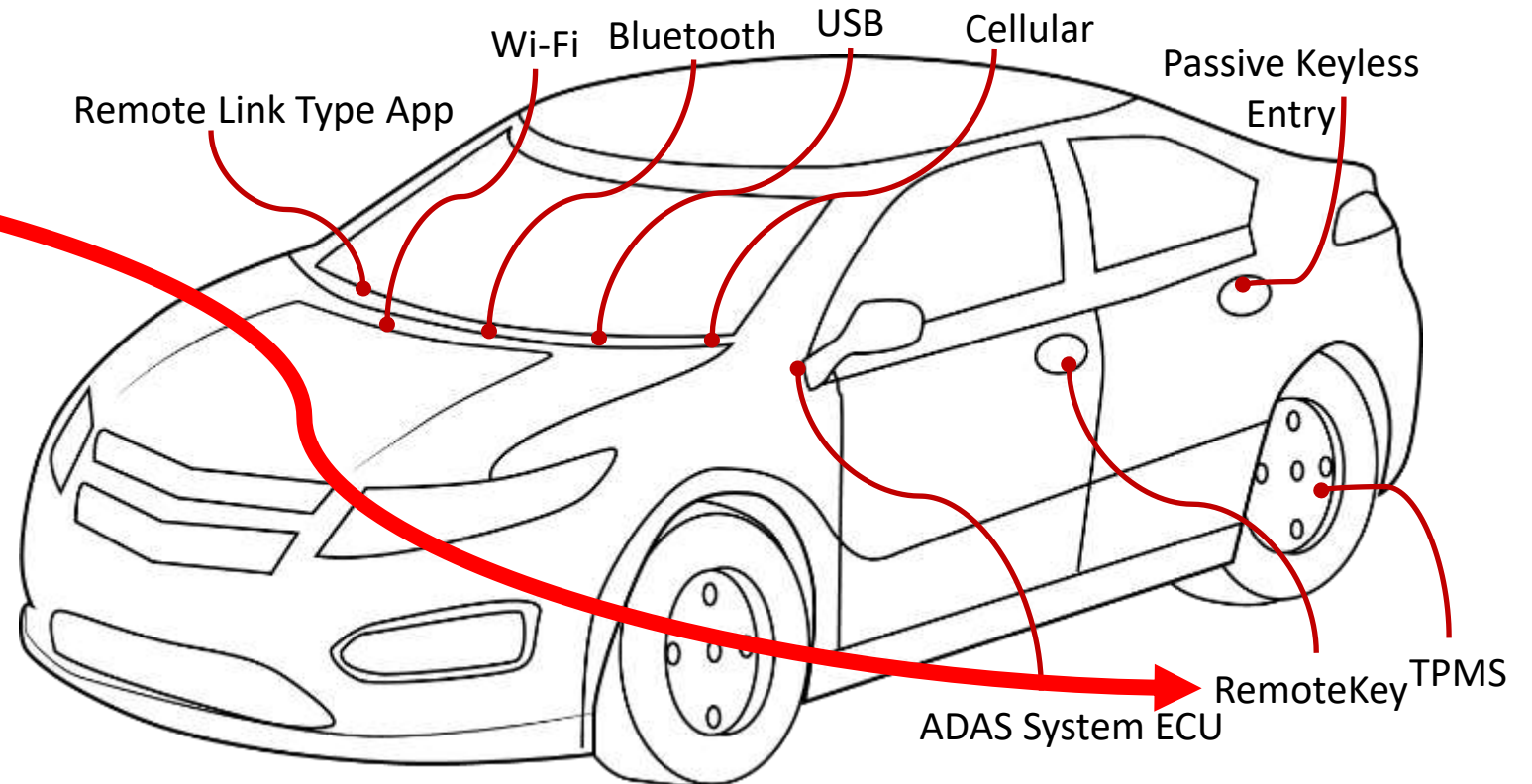
January 26, 2016

source: <http://goo.gl/aGBc9W>

August 6, 2015

This Hacker's Tiny Device Unlocks Cars And Opens Garages

The \$32 radio device, smaller than a cell phone, is designed to defeat the "rolling codes" security used in not only most modern cars and trucks' keyless entry systems, but also in their alarm systems and in modern garage door openers.



ANDY GREENBERG

SECURITY 11.23.2020 07:00 AM

This Bluetooth Attack Can Steal a Tesla Model X in Minutes

The company is rolling out a patch for the vulnerabilities, which allowed one researcher to break into a car in 90 seconds and drive away.

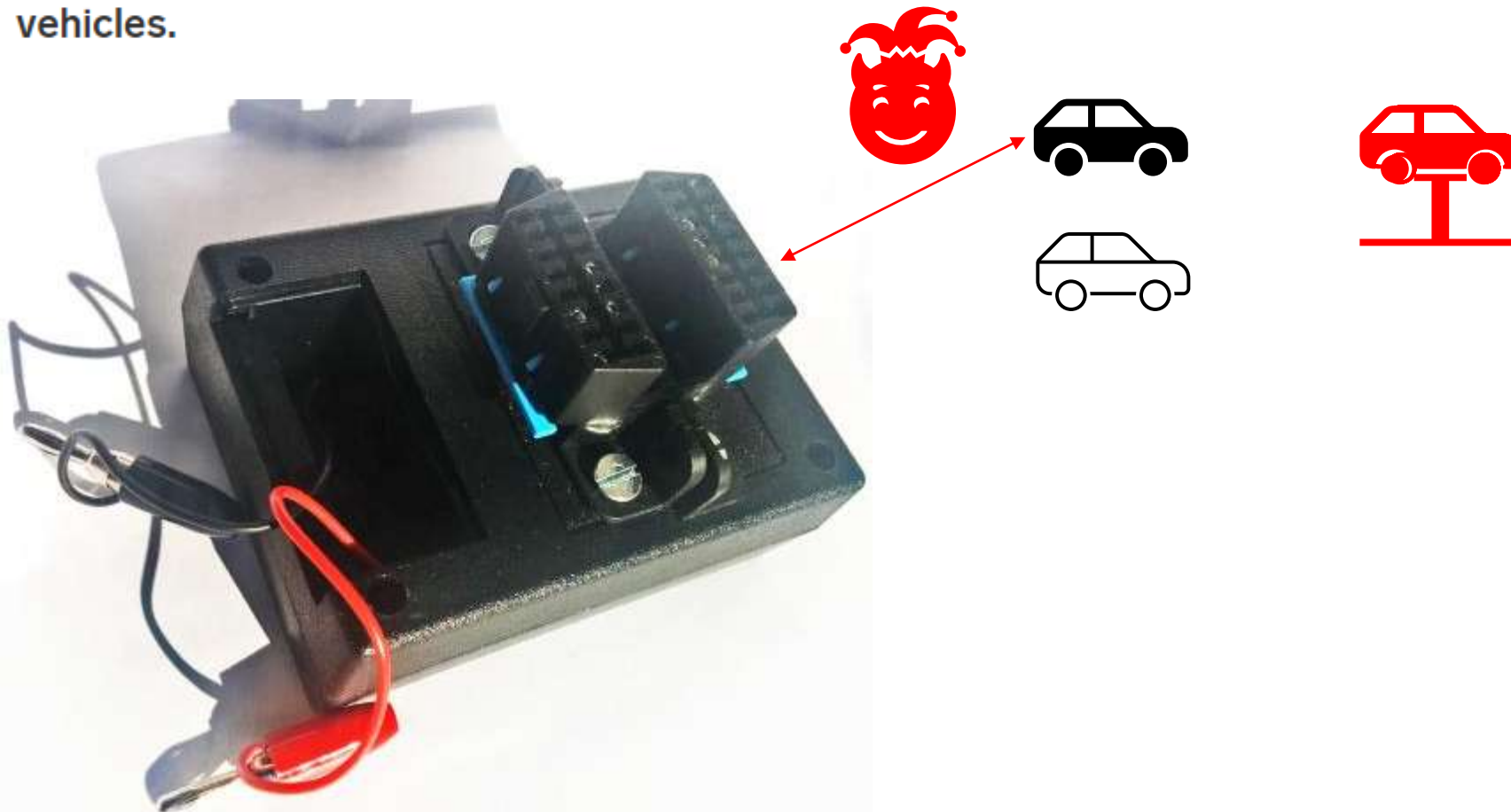
WIRED

November 23, 2020

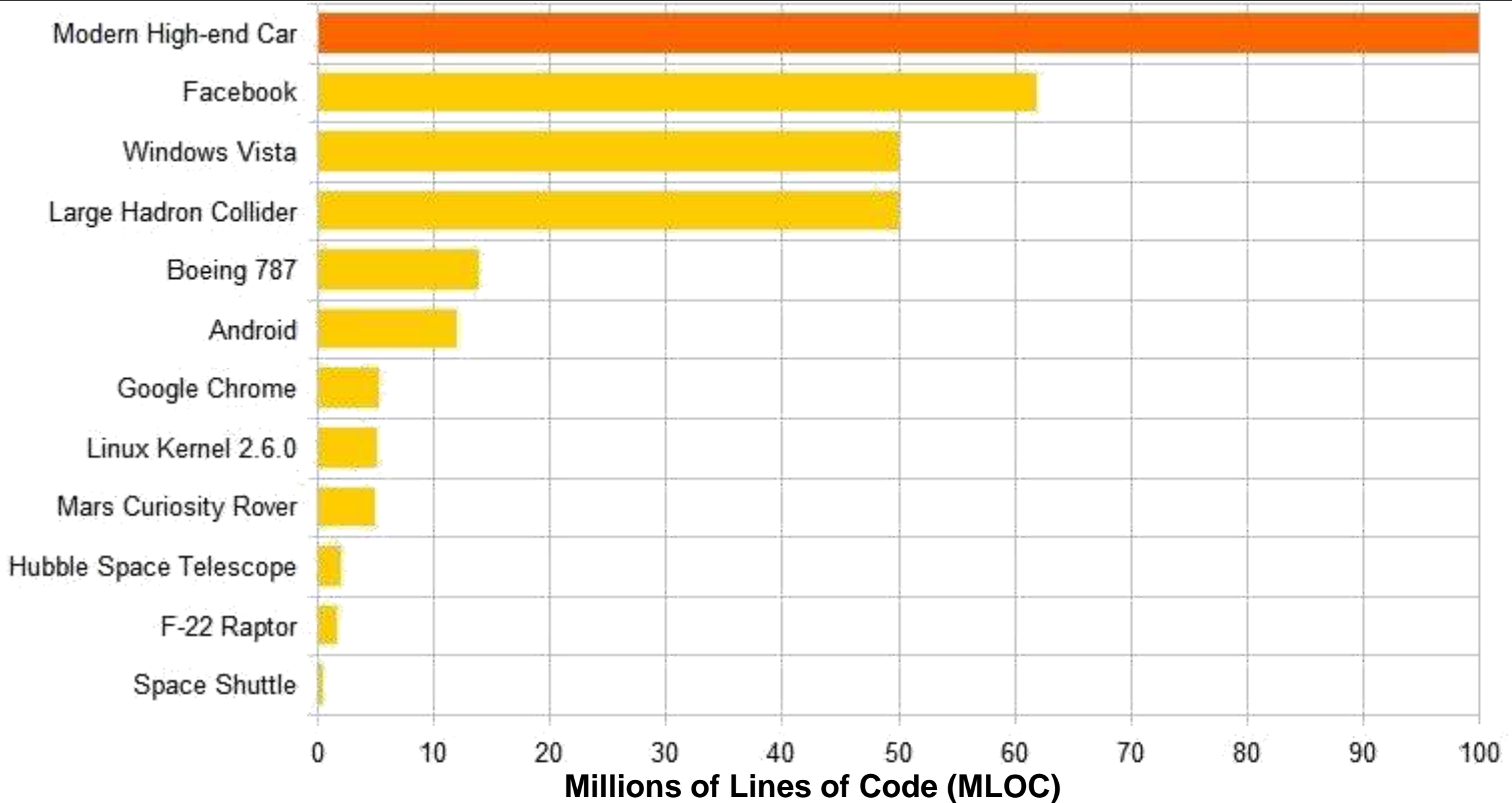
source: <https://www.wired.com/story/tesla-model-x-hack-bluetooth/>

Car Hack Technique Uses Dealerships to Spread Malware

A new hacking device finds vulnerabilities in auto diagnostic tools that could be used to spread malware to thousands of vehicles.



Software Complexity – Decrease Hardware, Increase Features



Opportunities → Remotely Accessible Attack Surfaces

Much of the exploitable code is not **safety-critical**

Infotainment

Comfort

Exploits lead to **hazards**

Not just cars—All vehicles!

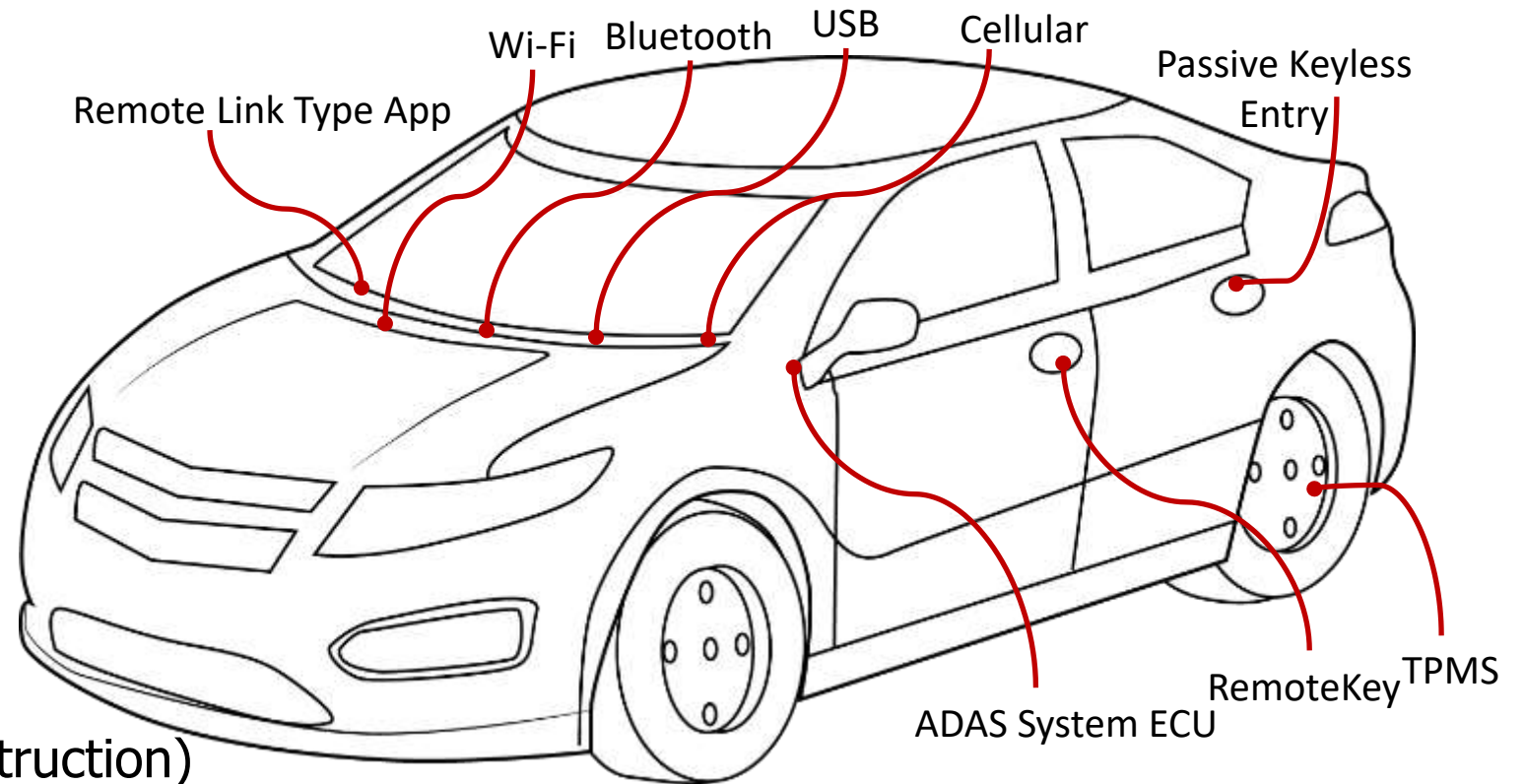
Tractor trailers

Heavy machinery (farming, construction)

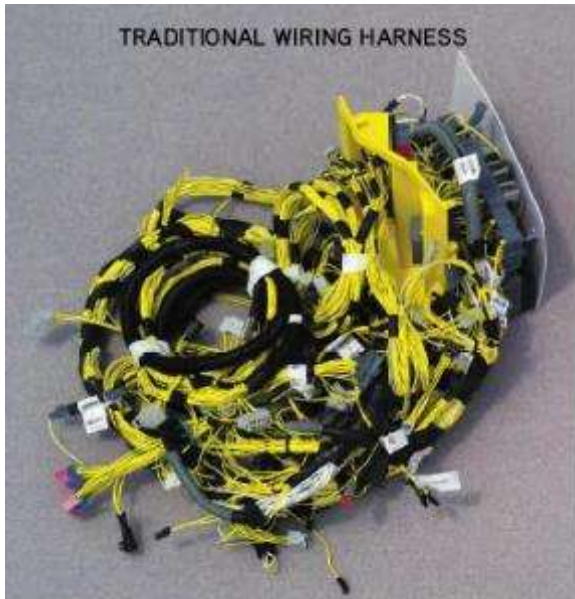
Ground weapon systems

Maritime

Space probes and satellites



Evolution of In-Vehicle Communication



Early 1990s cars used point-to-point wiring

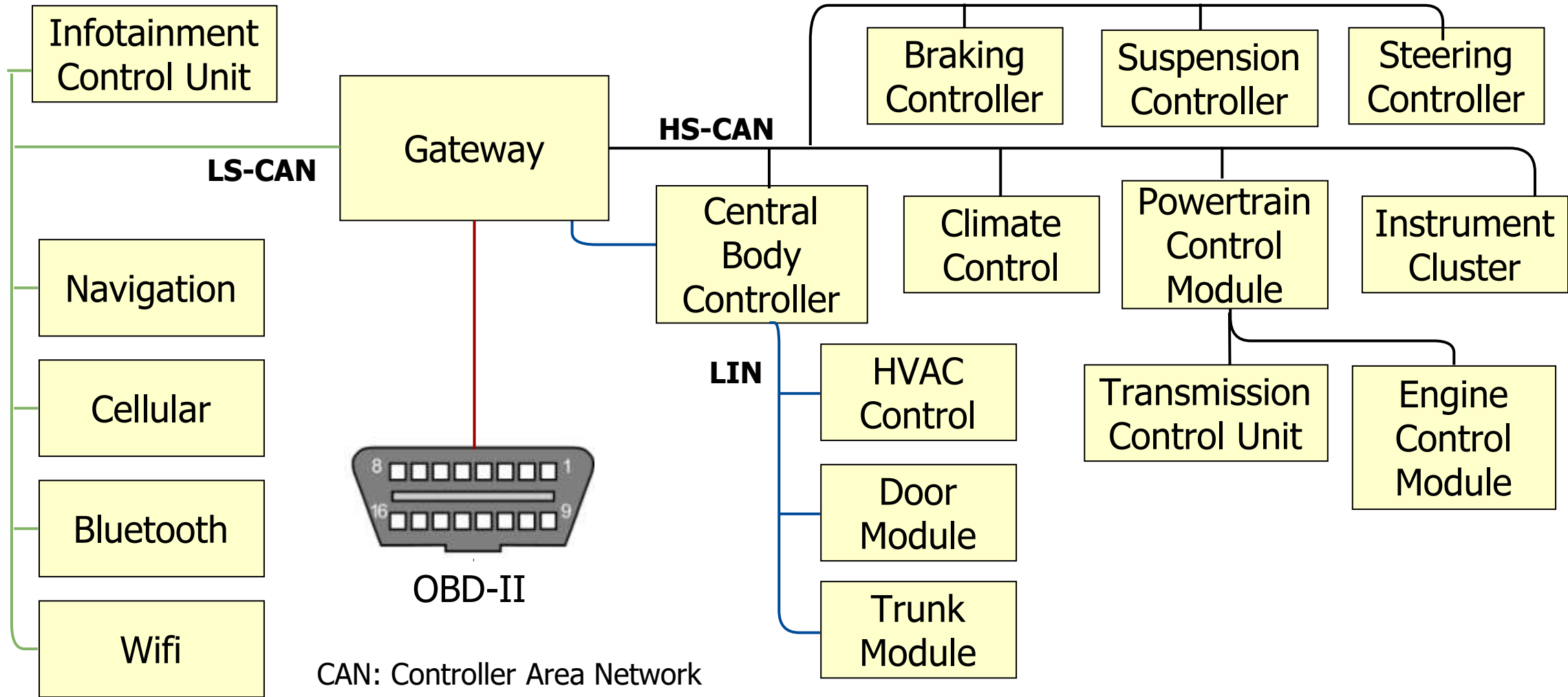
- A typical luxury car had
 - > 1000 yards of copper wire (65 lbs)
 - > 300 connectors, 2000 terminals, 1500 wires
- Expensive to manufacture, install, and maintain
- Unreliable due to very large number of connections



Controller Area Network (CAN)

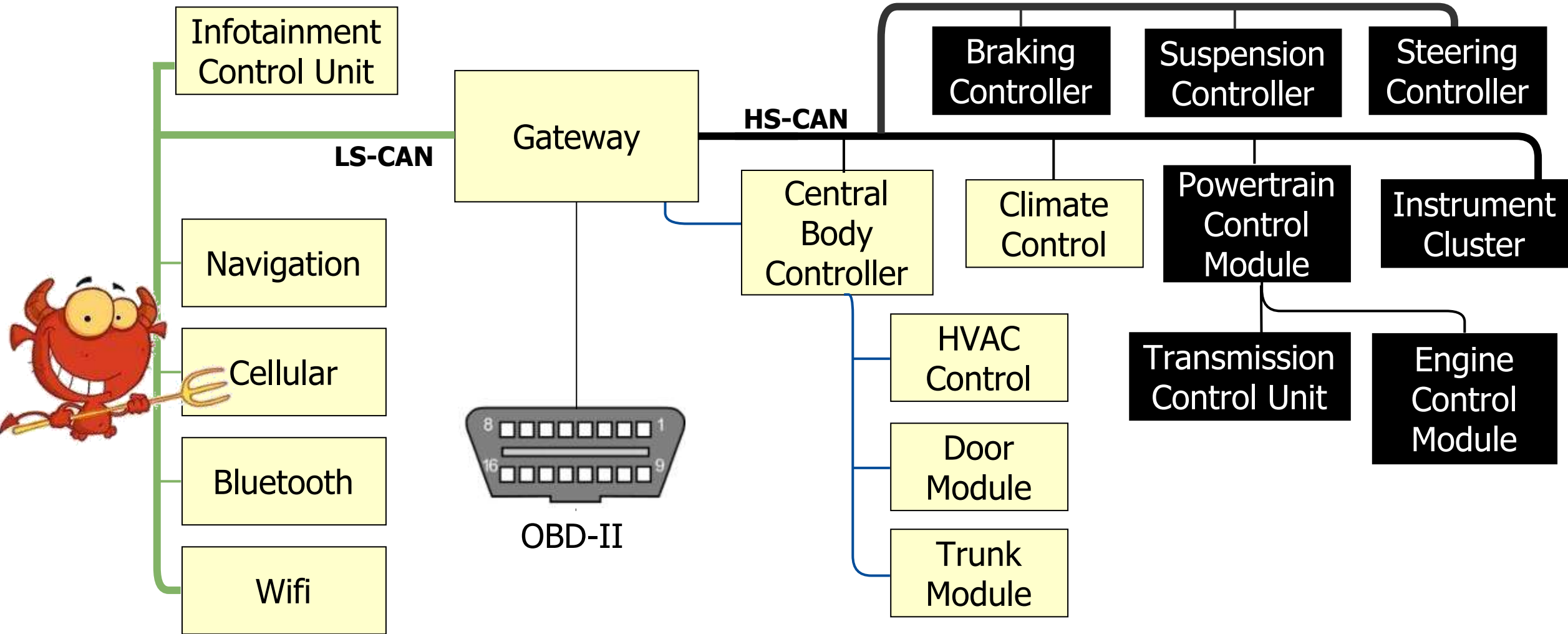
- Simple, robust, reliable in-vehicle network
- Small extra cost of CAN controllers and transceivers offset by massive reduction in wiring costs
- **End-to-end deadline on signals meets real-time message transmission requirements (5ms to 1 sec)**

Primer on Automotive Networking



CAN: Controller Area Network
LIN: Local Interconnect Network
OBD: On-Board Diagnostics

Exploits Lead to Hazards

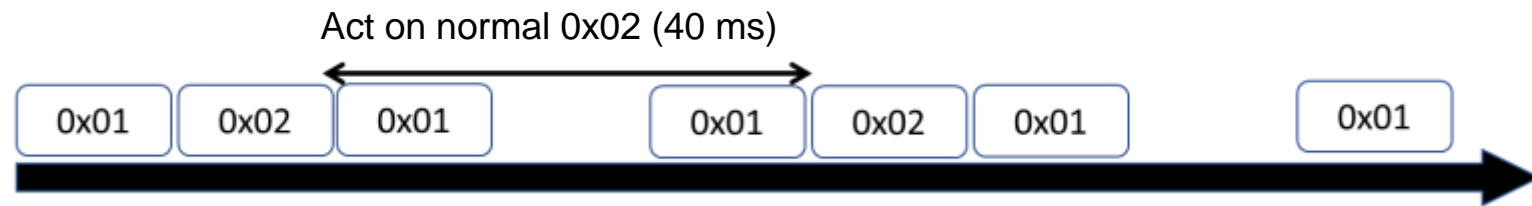


Anatomy of the False Data Injection Attack

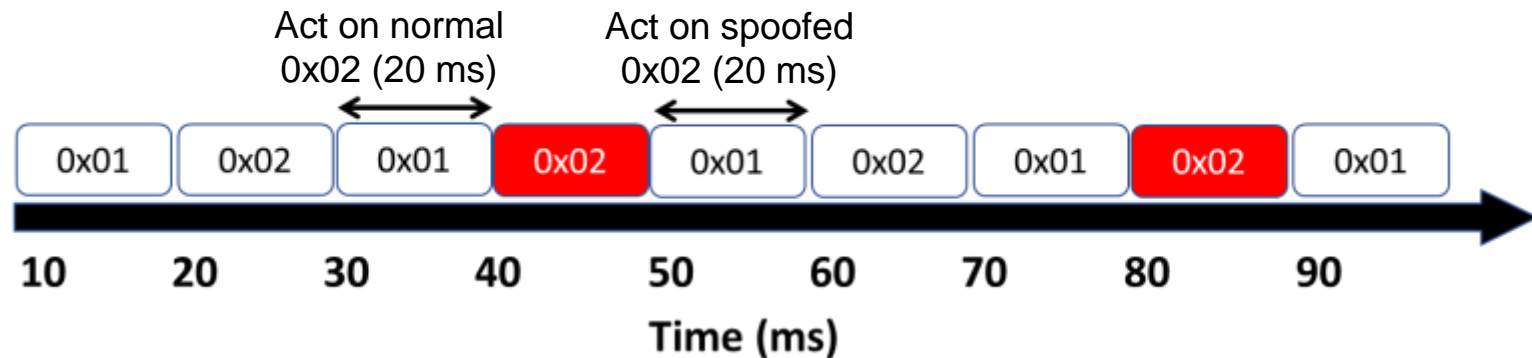
1. Establish foothold by remote exploit
2. Compromise gateway to propagate
3. Spoof messages from foothold to CAN bus

Needs 2x-10x spoof rate to override real messages

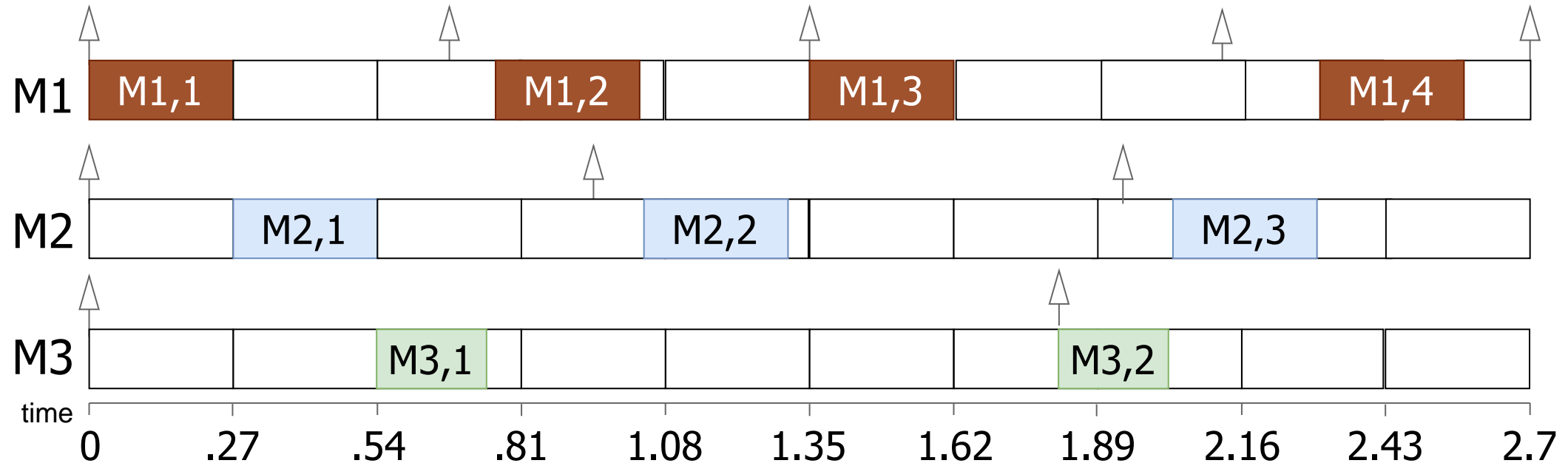
(a) Normal



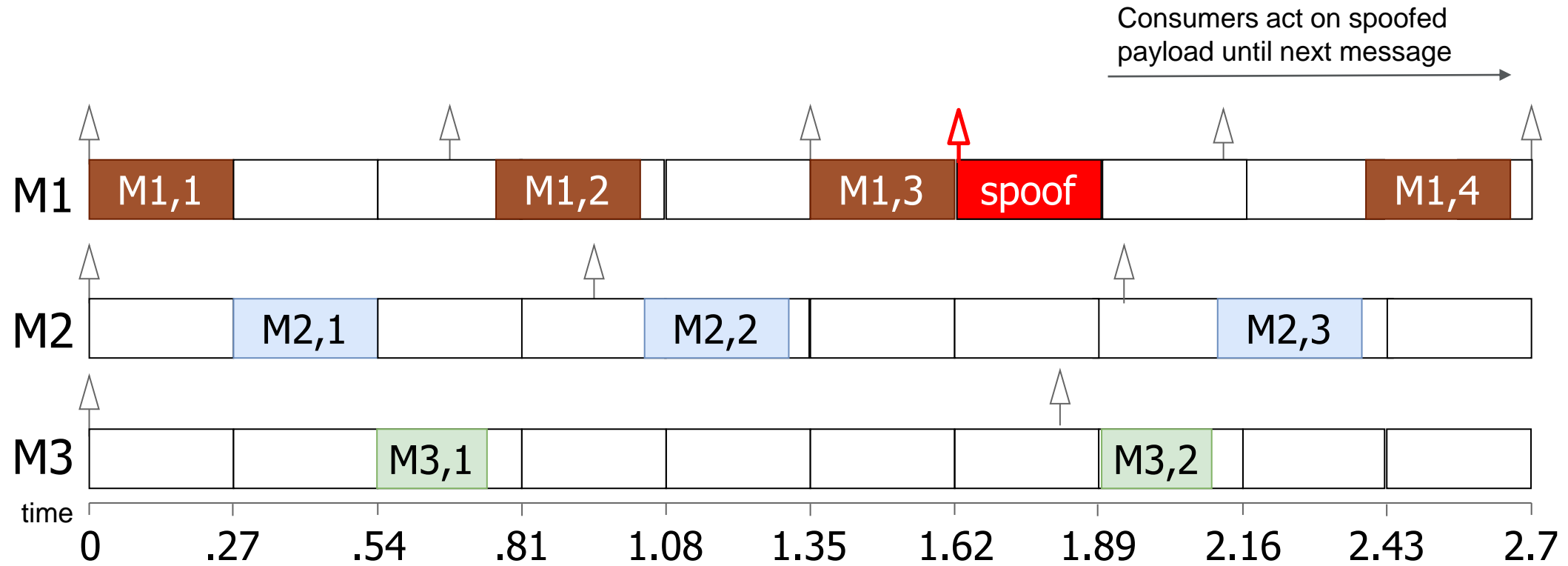
(b) Message Injection



False Data Injection Attack Example – Normal Behavior



False Data Injection Attack Example – Malicious Behavior



Current Approach to Automotive Security

Focus on CAN bus

Ubiquitous interconnect for safety-critical ECUs.

Often generalizable to other wired vehicular bus architectures.

Security Mechanisms

Message authentication – Detect alterations and verify sources.

Intrusion detection – Monitor messages, metadata for anomalies.

Challenges:

Accommodating legacy and after-market systems/components.

Solutions need to meet resource and economic constraints.

Security mechanisms must be reconciled with safety requirements!

Exploring the State-of-the-Art

- Collaborative arrangement with ORNL
 - Data set collected in 2017.
 - Logging CAN traffic through the OBD-II of a real sedan on a dynamometer.
- Message injection attacks
 - Injected at high rate to override normal vehicle operations.



Oak Ridge National Laboratory
Vehicle Security Center

Vehicle	Detection Type	Detection Accuracy	False Positive
1	Interval	75%	0%
	Frequency	100%	0.7%
2	Interval	96.9%	30%
	Frequency	100%	1.4%

60 false positives per second

My Vehicular Security Publications

- [AutoSec] **G. Bloom.** WeepingCAN: A Stealthy CAN Bus-off Attack. 3rd International Workshop on Automotive and Autonomous Vehicle Security, 2021.
- [CEM] U. Ezeobi, H. Olufowobi, C. Young, J. Zambreno, and **G. Bloom.** Reverse Engineering Controller Area Network Messages using Unsupervised Machine Learning. IEEE Consumer Electronics Magazine, 2020.
- [TVT] H. Olufowobi, C. Young, J. Zambreno, and **G. Bloom.** SAIDuCANT: Specification-Based Automotive Intrusion Detection Using Controller Area Network (CAN) Timing. IEEE Transactions on Vehicular Technology, 2020.
- [CPS-SPC] H. Olufowobi, S. Hounsinou, and **G. Bloom.** Controller Area Network Intrusion Prevention System Leveraging Fault Recovery. ACM Workshop on Cyber-Physical Systems Security & Privacy, 2019.
- [TII] **G. Bloom,** G. Cena, I. Cibrario Bertolotti, T. Hu, and A. Valenzano. *Event Notification in CAN-based Sensor Networks.* IEEE Transactions on Industrial Informatics, 2019.
- [D&T] C. Young, H. Olufowobi, J. Zambreno, **G. Bloom.** *Survey of Automotive Controller Area Network Intrusion Detection Systems.* IEEE Design & Test, 2019.
- [AutoSec] H. Olufowobi, U. Ezeobi, E. Muhati, G. Robinson, C. Young, J. Zambreno, and **G. Bloom.** *Anomaly Detection Approach Using Adaptive Cumulative Sum Algorithm for Controller Area Network.* AutoSec, ACM Workshop on Automotive Cybersecurity, 2019.
- [AutoSec] C. Young, H. Olufowobi, **G. Bloom,** and J. Zambreno. *Automotive Intrusion Detection Based on Constant CAN Message Frequencies Across Vehicle Driving Modes.* ACM Workshop on Automotive Cybersecurity, 2019.
- [RTSS-WIP] H. Olufowobi, **G. Bloom,** C. Young, and J. Zambreno. *Work-in-Progress: Real-Time Modeling for Intrusion Detection in Automotive Controller Area Network.* IEEE Real-Time Systems Symposium, 2018.
- [ICIT] **G. Bloom,** G. Cena, I. Cibrario Bertolotti, T. Hu, and A. Valenzano. *Supporting Security Protocols on CAN-Based Networks.* 18th Annual IEEE International Conference on Industrial Technology, 2017.

My Vehicular Security Publications

- [AutoSec] **G. Bloom.** WeepingCAN: A Stealthy CAN Bus-off Attack. 3rd International Workshop on Automotive and Autonomous Vehicle Security, 2021.
- This talk**
- U. Ezeobi, H. Olufowobi, C. Young, J. Zambreno, and **G. Bloom.** Reverse Engineering Controller Area Network Messages using Unsupervised Machine Learning. IEEE Consumer Electronics Magazine, 2020.
- [TVT] H. Olufowobi, C. Young, J. Zambreno, and **G. Bloom.** SAIDuCANT: Specification-Based Automotive Intrusion Detection Using Controller Area Network (CAN) Timing. IEEE Transactions on Vehicular Technology, 2020.
- [CPS-SPC] H. Olufowobi, S. Hounsinou, and **G. Bloom.** Controller Area Network Intrusion Prevention System Leveraging Fault Recovery. ACM Workshop on Cyber-Physical Systems Security & Privacy, 2019.
- [TII] **G. Bloom,** G. Cena, I. Cibrario Bertolotti, T. Hu, and A. Valenzano. *Event Notification in CAN-based Sensor Networks.* IEEE Transactions on Industrial Informatics, 2019.
- [D&T] C. Young, H. Olufowobi, J. Zambreno, **G. Bloom.** *Survey of Automotive Controller Area Network Intrusion Detection Systems.* IEEE Design & Test, 2019.
- [AutoSec] H. Olufowobi, U. Ezeobi, E. Muhati, G. Robinson, C. Young, J. Zambreno, and **G. Bloom.** *Anomaly Detection Approach Using Adaptive Cumulative Sum Algorithm for Controller Area Network.* AutoSec, ACM Workshop on Automotive Cybersecurity, 2019.
- [AutoSec] C. Young, H. Olufowobi, **G. Bloom,** and J. Zambreno. *Automotive Intrusion Detection Based on Constant CAN Message Frequencies Across Vehicle Driving Modes.* ACM Workshop on Automotive Cybersecurity, 2019.
- [RTSS-WIP] H. Olufowobi, **G. Bloom,** C. Young, and J. Zambreno. *Work-in-Progress: Real-Time Modeling for Intrusion Detection in Automotive Controller Area Network.* IEEE Real-Time Systems Symposium, 2018.
- [ICIT] **G. Bloom,** G. Cena, I. Cibrario Bertolotti, T. Hu, and A. Valenzano. *Supporting Security Protocols on CAN-Based Networks.* 18th Annual IEEE International Conference on Industrial Technology, 2017.

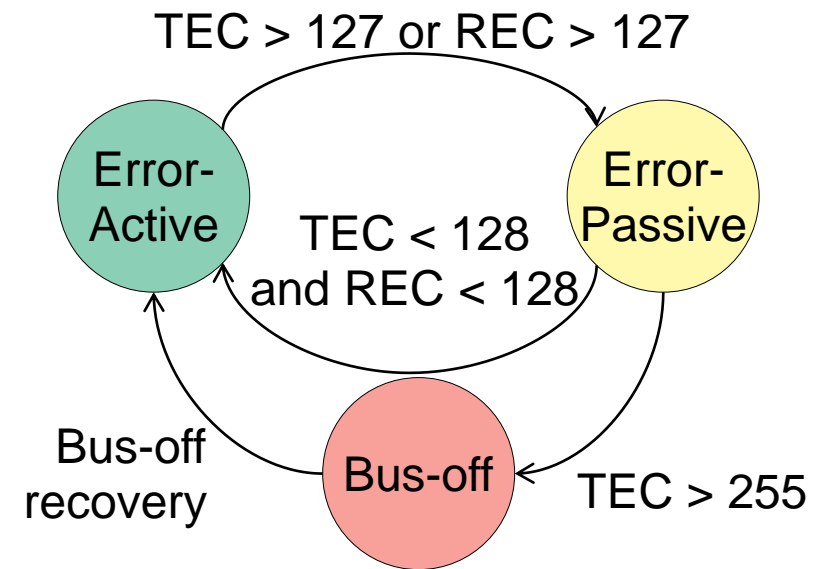


WeepingCAN

A Stealthy CAN Bus-off Attack

CAN Error Handling

- CAN protocol implements error handling feature for nodes transmitting on the bus to monitor bus health.
- Each node implements two error counters, called transmit error counter (TEC) and the receive error counter (REC).

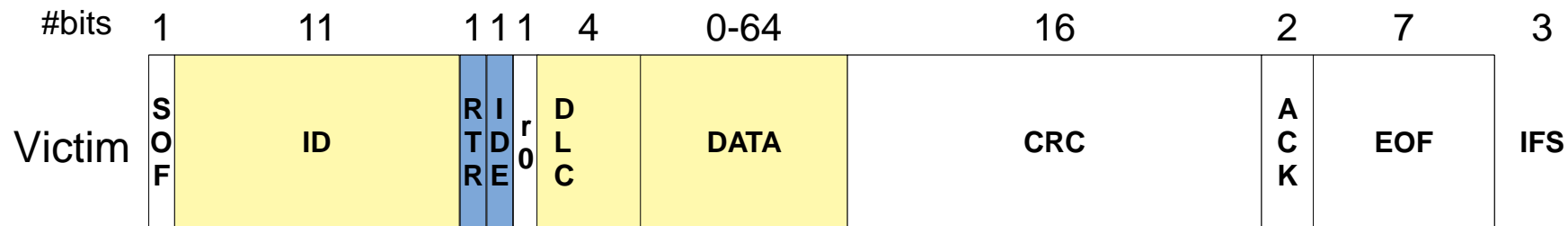


Anatomy of Original CAN Bus-Off Attack

1. Establish foothold by remote exploit.
2. Move laterally if necessary.
3. Inject **specialty-crafted attack messages** to CAN bus

Attack message format

Identical bit prefix as victim message frame until a **dominant (0)** bit error

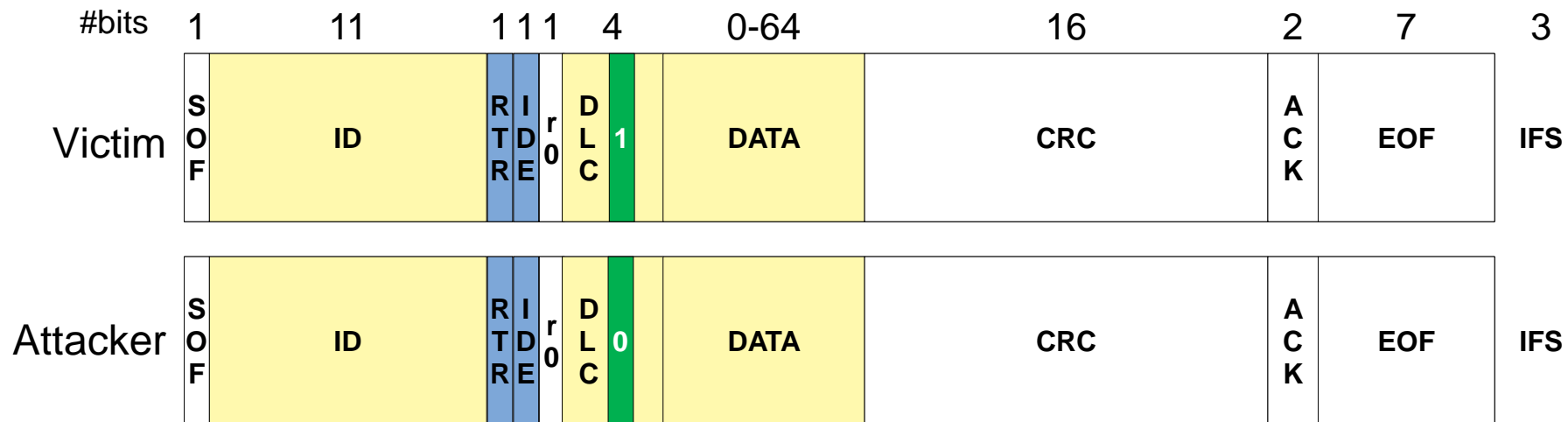


Anatomy of Original CAN Bus-Off Attack

1. Establish foothold by remote exploit.
2. Move laterally if necessary.
3. Inject **specialty-crafted attack messages** to CAN bus

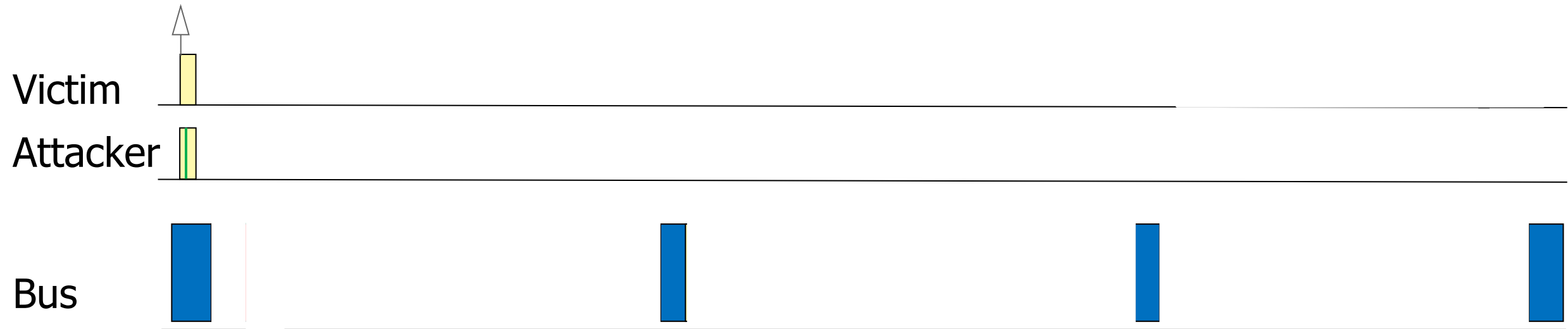
Attack message format




Identical bit prefix as victim message frame until a **dominant (0)** bit error
Software attacker can only inject errors in the DLC and Data fields



Original CAN Bus-Off Attack: Phase 1

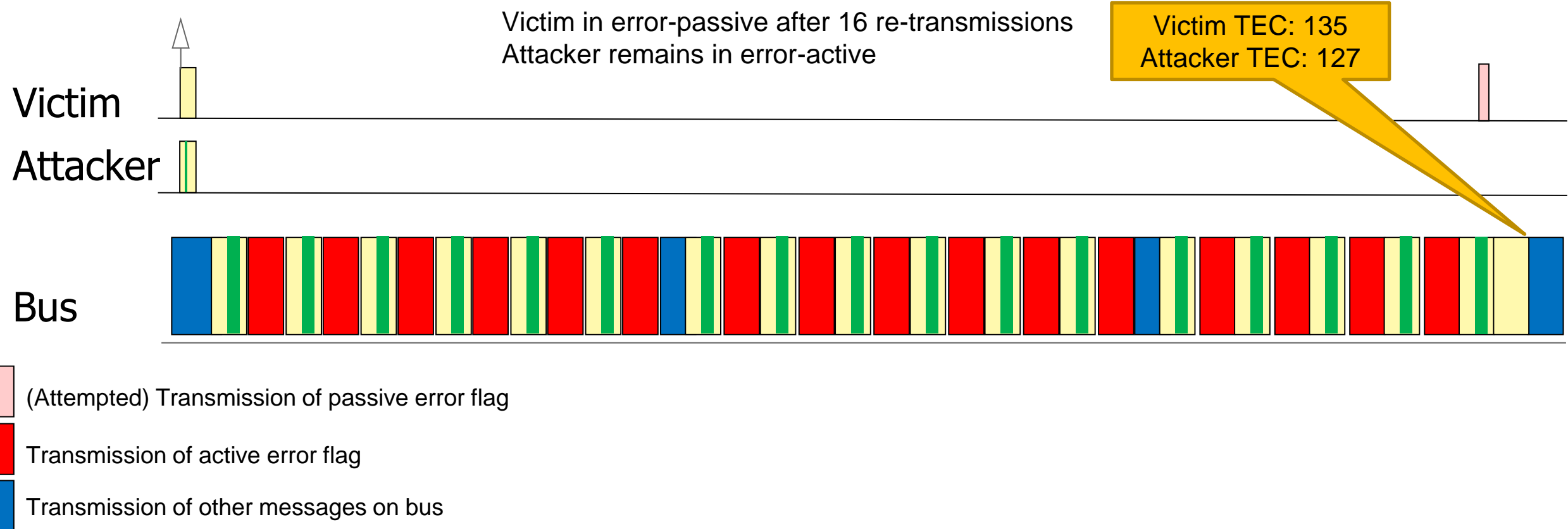
- Synchronize attack message injection with victim transmission
 - Enqueue attack during transmission of message **preceding** the victim
- Collision causes cascade of bit error, retransmissions of both messages



-  (Attempted) Transmission of passive error flag
-  Transmission of active error flag
-  Transmission of other messages on bus

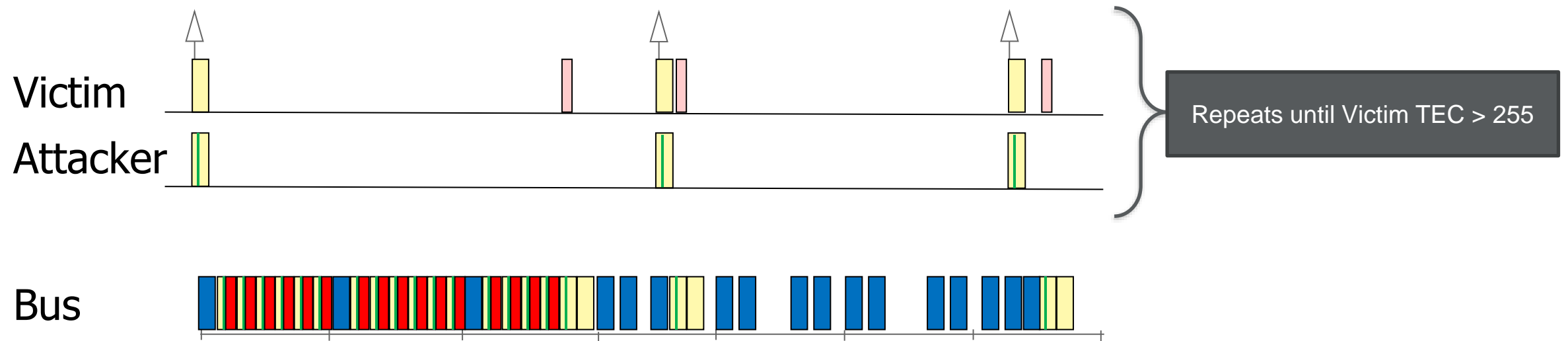
Original CAN Bus-Off Attack: Phase 1




- Synchronize attack message injection with victim transmission
 - Enqueue attack during transmission of message **preceding** the victim
- Collision causes cascade of bit error, retransmissions of both messages



Original CAN Bus-Off Attack: Phase 2

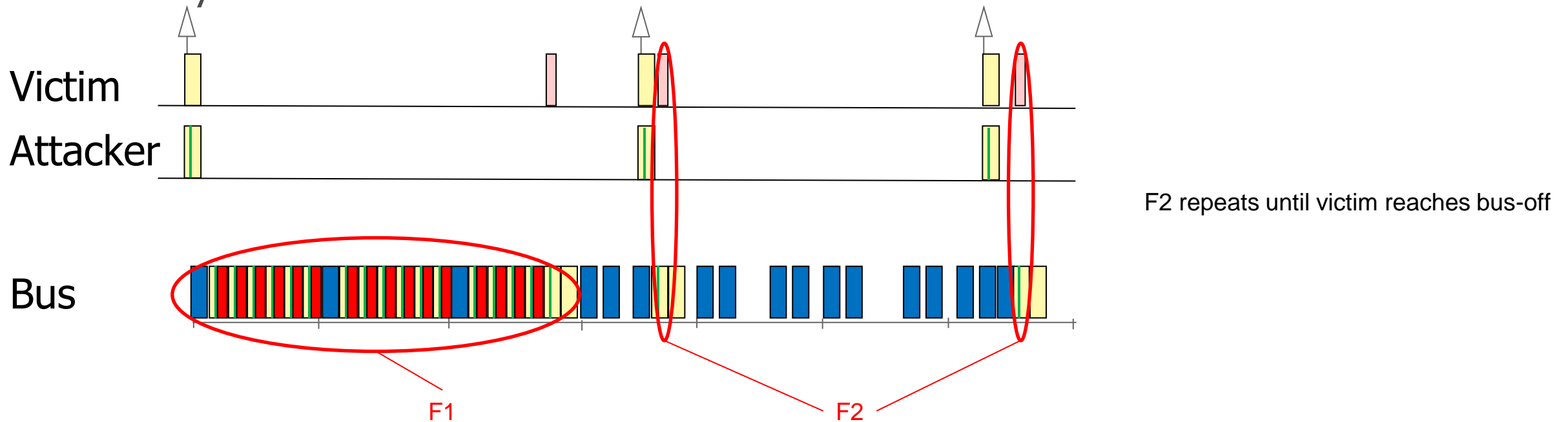
- Synchronize attack message injection with victim transmission
 - Enqueue attack during transmission of message **preceding** the victim
- Collision causes **passive error flag**, retransmission of victim message



-  (Attempted) Transmission of passive error flag
-  Transmission of active error flag
-  Transmission of other messages on bus

Two Detectable Features of Original CAN Bus-off

- F1: Cascade of repeated active error/retransmission
 - Observable by any node on bus
- F2: Transmission of attack message during victim's passive error flag
 - Only visible to the victim



Bus-off mitigation techniques rely on these features

WeepingCAN Attack

1. Disable retransmission of the attack message
 - Avoids feature F1
2. Inject attack message with *randomly-located* **recessive (1)** bit error
 - Flips role of attacker and victim
 - Avoids feature F2
 - Also avoid fixed-position bit errors

Two Approaches for Disabling Retransmissions

1. Disable automatic retransmissions for all messages

- Supported by most CAN Controllers for Time-Triggered CAN (TTCAN*)
- Requires re-enabling retransmissions after each injection
 - Or the attacker ECU can't win arbitration for its regular messages

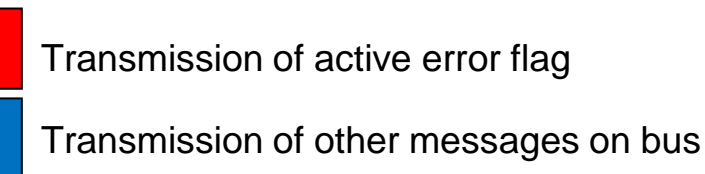
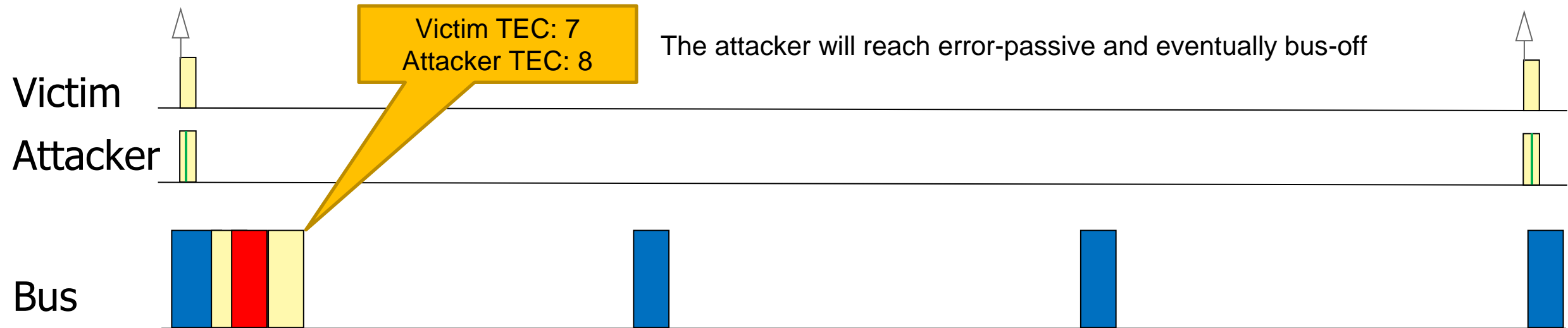
2. Abort transmission on Transmit Error

- CAN controllers can raise an interrupt on a transmit error
- Interrupt handler can abort the retransmission

* WeepingCAN is named for the first approach, which led to discovery of the attack, because TT is a crying emote.

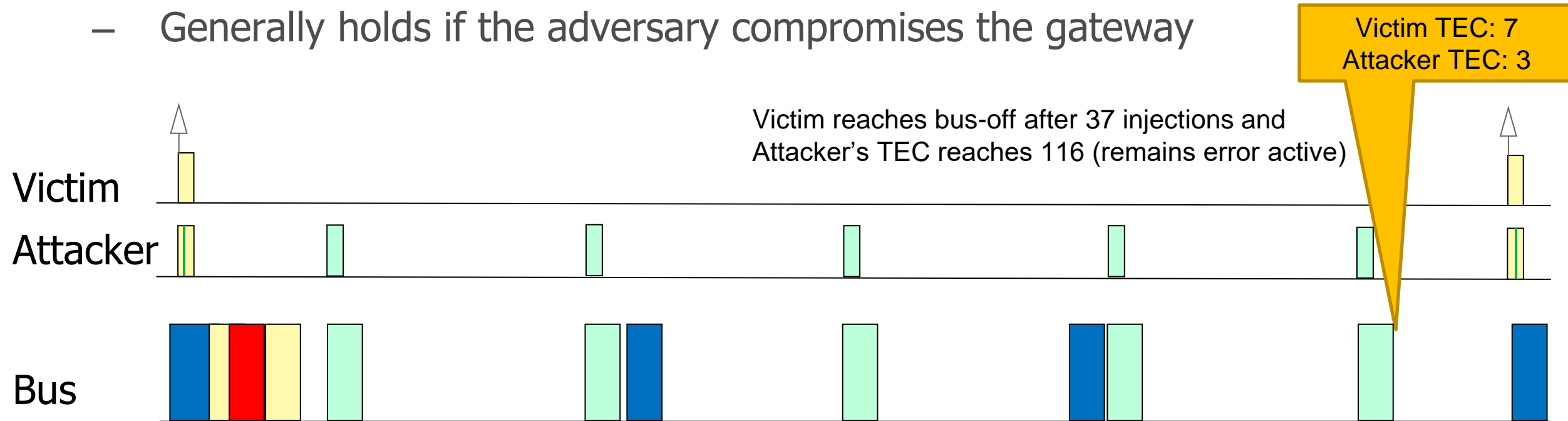
WeepingCAN Attack: Take 1

- Synchronize attack message injection with victim transmission
 - Enqueue attack during transmission of message **preceding** the victim
- Collision causes attacker to transmit error flag, retransmission of victim



WeepingCAN Attack: Take 2

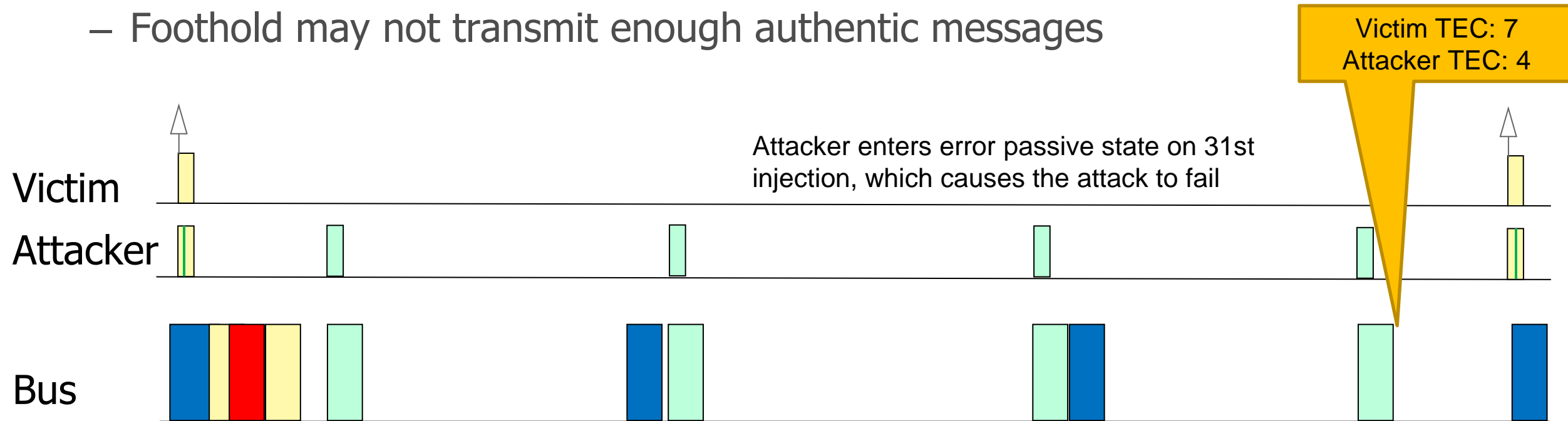
- Exploit an ECU that transmits more authentic messages than the victim
 - Possible if adversary can send/fabricates authentic messages of the foothold
 - Generally holds if the adversary compromises the gateway



- Transmission of active error flag
- Transmission of other messages on bus

WeepingCAN Attack: Take 3

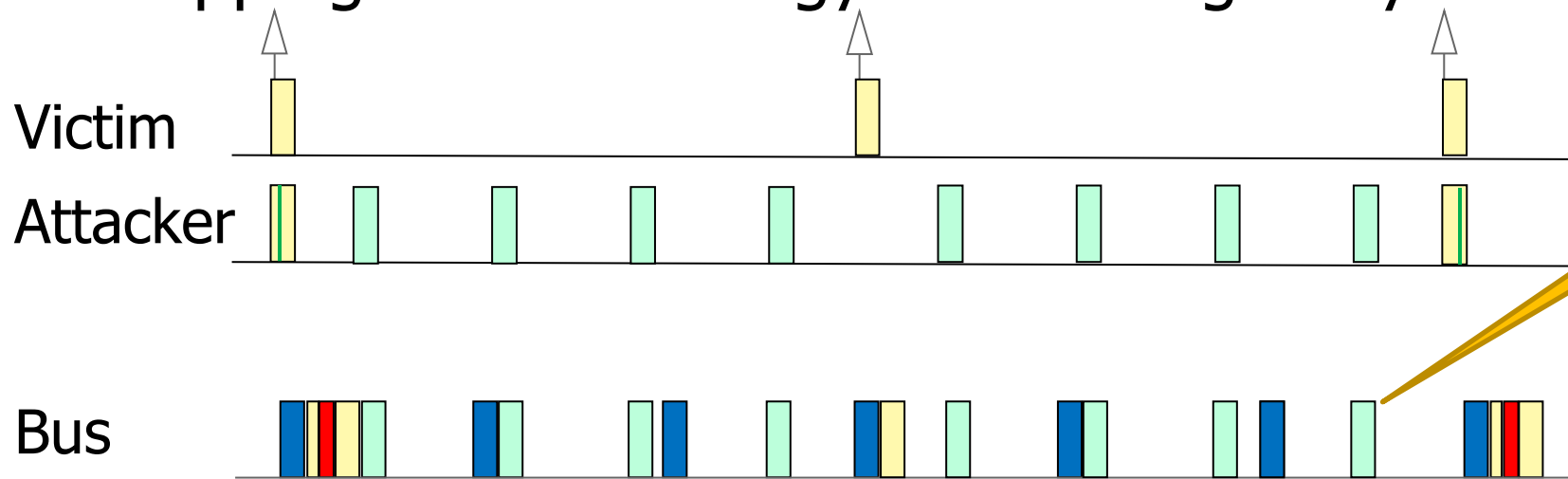
- Transmission of extra messages may be detectable
 - Only transmit authentic messages with expected inter-arrival times (and data)
 - Foothold may not transmit enough authentic messages



- Transmission of active error flag
- Transmission of other messages on bus

WeepingCAN Attack: Take 3

- Transmission of extra messages may be detectable
 - Only transmit authentic messages with expected inter-arrival times (and data)
 - Foothold may not transmit enough authentic messages
- **Skipping Attack Strategy: Don't be greedy**



Victim TEC: 6
Attacker TEC: 0

Attacker fully recovers
TEC between injections

Transmission of active error flag
Transmission of other messages on bus

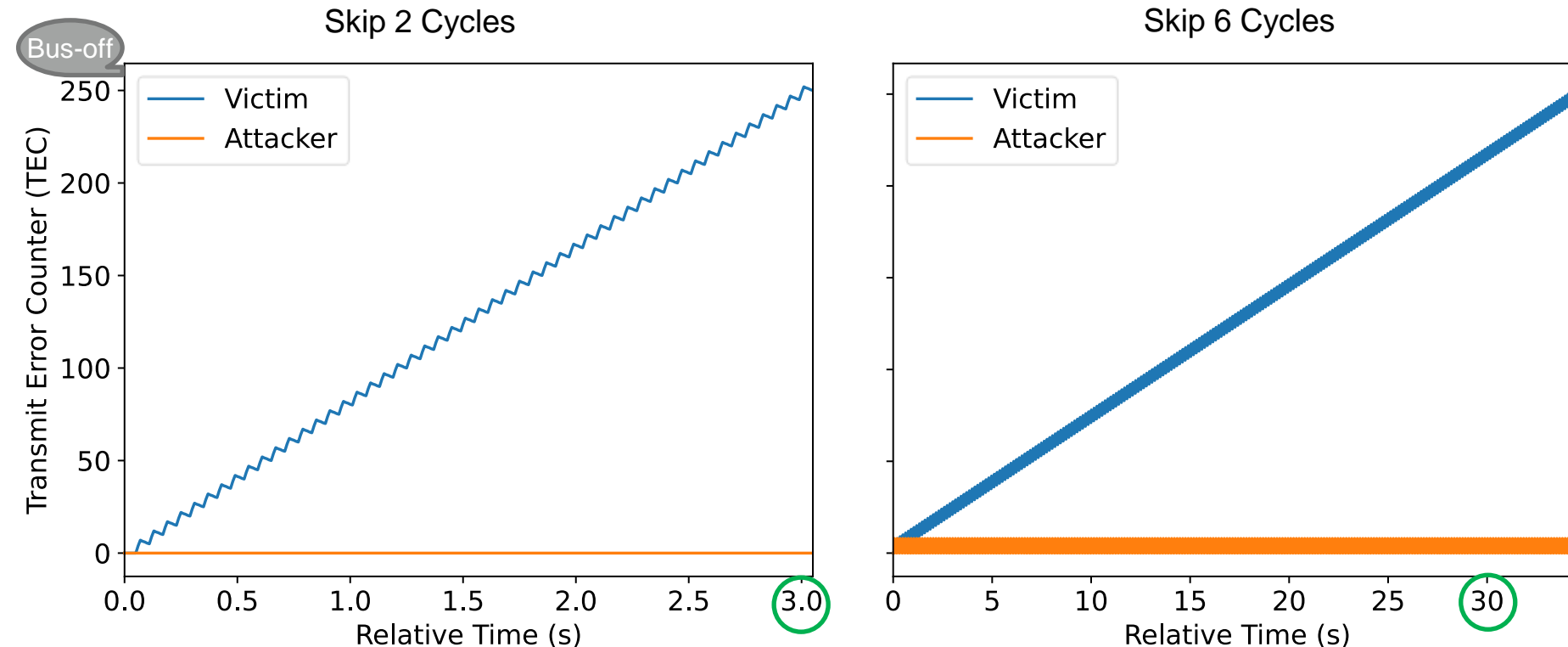
Experimental Validation

- CAN Benchtop Setup
 - Two BeagleBone Black (BBB)
 - Three TM4C129EXL (TM4C)
 - 3.3v CAN in a breadboard
 - Saleae Logic Pro to snoop bus
- Synthetic Benchmark
 - Slightly modified from original bus-off attack paper by Cho and Shin
- Modified SAE Benchmark
 - Reproduced from other prior work



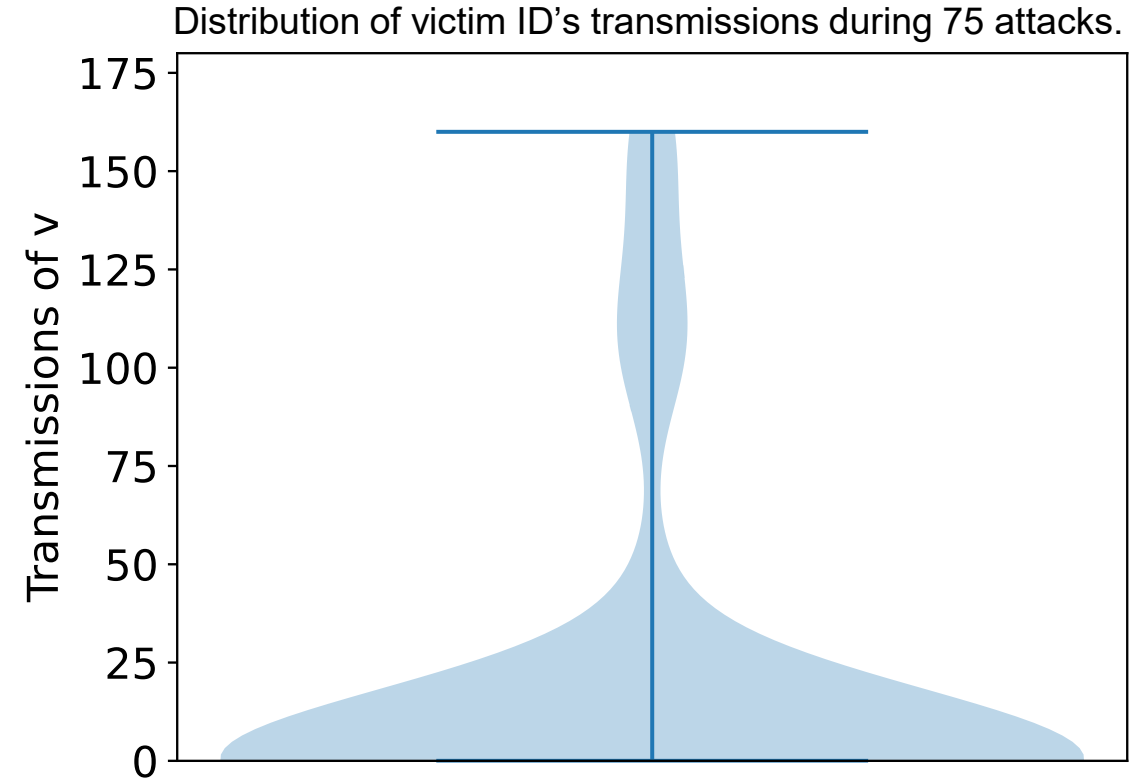
Skipping Attack Strategy with Synthetic Benchmark

- Conducted 100 attacks skipping from 2 to 6 cycles per injection
 - All 500 attacks were successful
- 0% of attacks triggered F1 detection
 - Zero transmissions of victim ID by the attacking ECU prior to bus-off



Evaluation of Stealthiness with Modified SAE Benchmark

- Conducted 74 attacks skipping 5 cycles per injection
 - 78% attack success (58 end in bus-off)
- Failure implies victim ID transmitted
 - Distribution of transmissions shown →
- Median number of transmissions is 0
 - Most attacks succeed without victim ID transmission prior to bus-off
- Feature F1 was detected in 2.7% (two) of the attacks



Real Vehicle Verification

- Conducted WeepingCAN on a 2016 Kia Optima in a safe environment
 - Identified a low priority message in accessory mode
 - Attached a TM4C board configured to attack it with abort on transmit
 - Snooped bus and captured log file
- Attempted 3 attacks with one success
 - Victim is not observed on bus for 3 seconds
 - Attacker doesn't transmit for 7 seconds from start of attack
 - Loses synchronization with victim



Current Approach to Ground Vehicle Security

Focus on CAN bus

Ubiquitous interconnect for safety-critical ECUs.

Often generalizable to other wired vehicular bus architectures.

Security Mechanisms

Message authentication – Detect alterations and verify sources.

Intrusion detection – Monitor messages, metadata for anomalies.

Challenges:

Accommodating legacy and after-market systems/components.

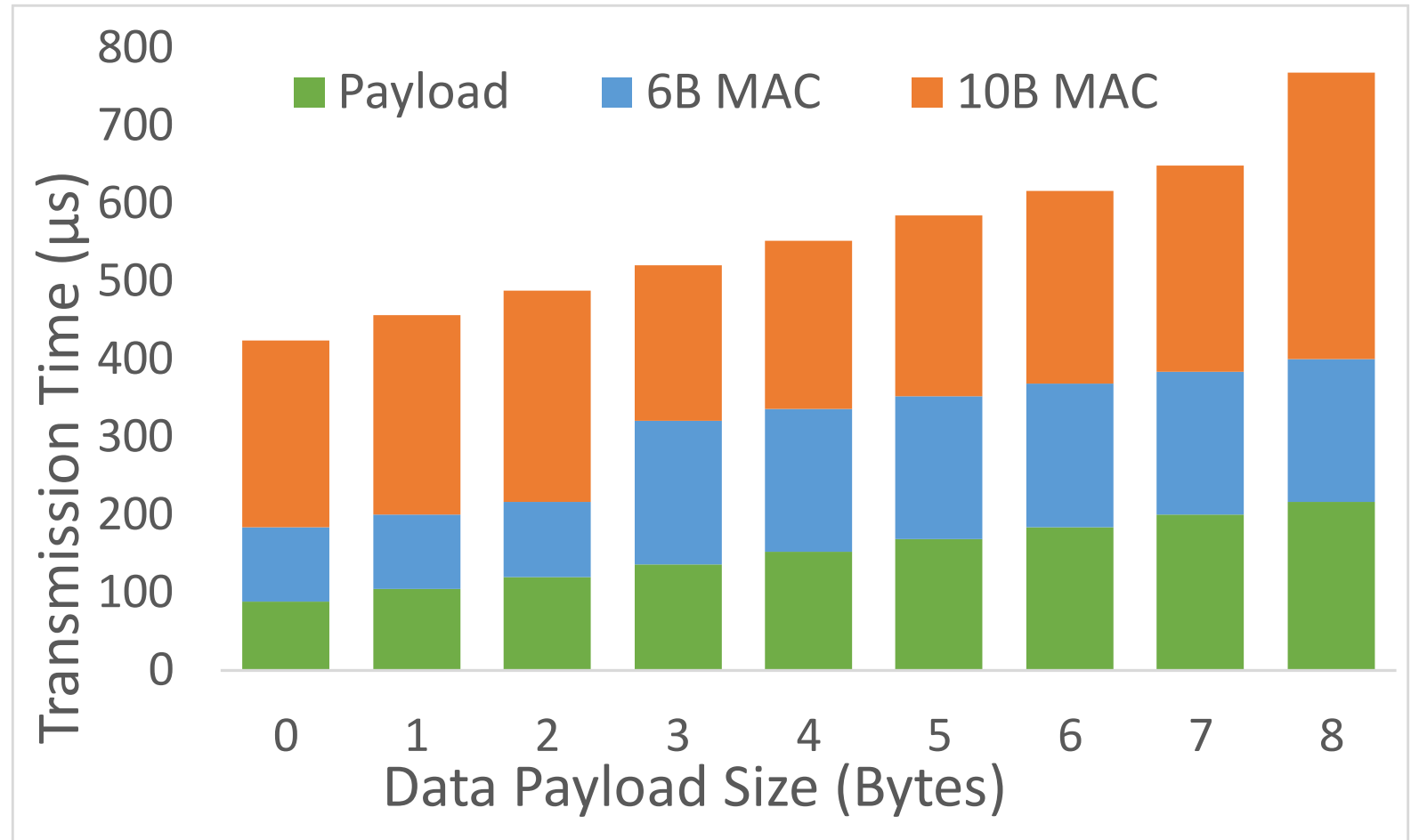
Solutions need to meet resource and economic constraints.

Security mechanisms must be reconciled with safety requirements!

Cryptographic Authentication in CAN has a massive overhead

Full MACs and Freshness Values (nonces) more than double message transmission times and bus utilization

Best methods to incorporate Crypto in real-time busses is under-explored



O. Ikumapayi et al., "CANASTA: Controller Area Network Authentication Schedulability Timing Analysis"
under review in IEEE Transactions on Vehicular Technology

CAN Bus Intrusion Detection with Anomalies or Signatures?

- Signature-based
 - What rules and how to update them?
- Anomaly-based
 - What features and classifiers? How to deal with false positives?

SoTA: Message Timing Anomalies

- Message Frequencies
- Message Intervals
- Other Statistical Features

Wildly Varying Published Results

Disparate training dataset

- Inconsistencies in the training datasets
- Assumptions used by the algorithms

Disparate evaluation dataset

- Differences in the test datasets

Disparate evaluation metrics

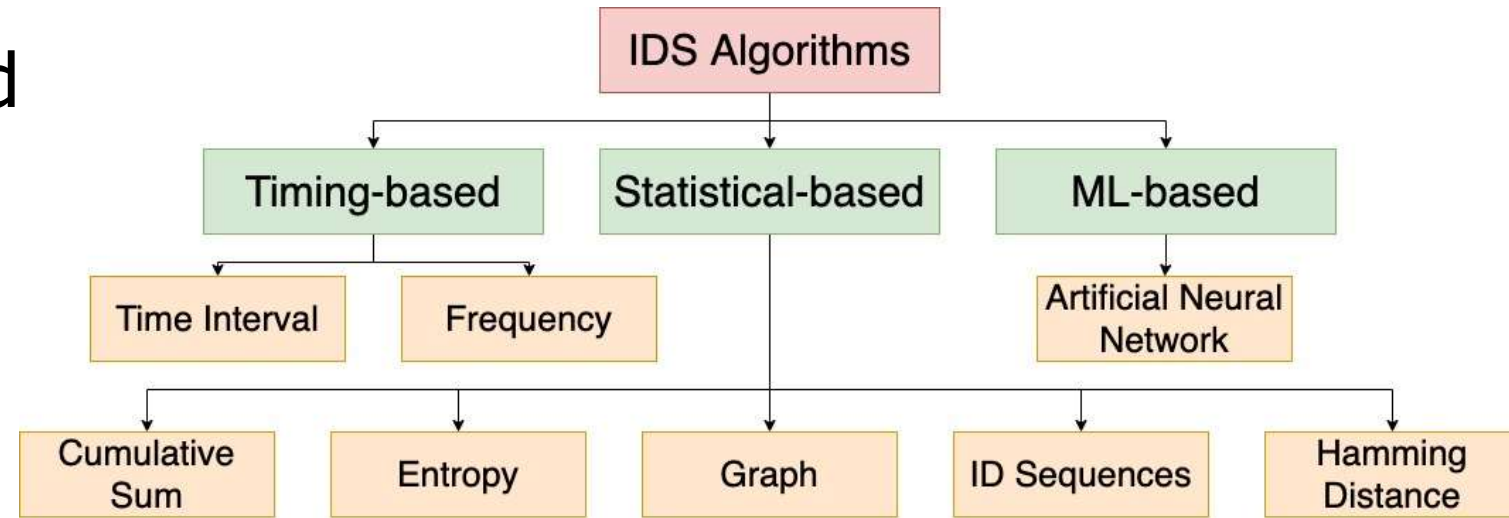
- Inconsistencies among the chosen metrics

Consistent IDS Evaluations are Challenging

We re-implemented IDSs and observed performance varies by the basis of the attack.

We have also observed that dataset quality can have a biasing impact.

Hard to do good engineering without good measurements.

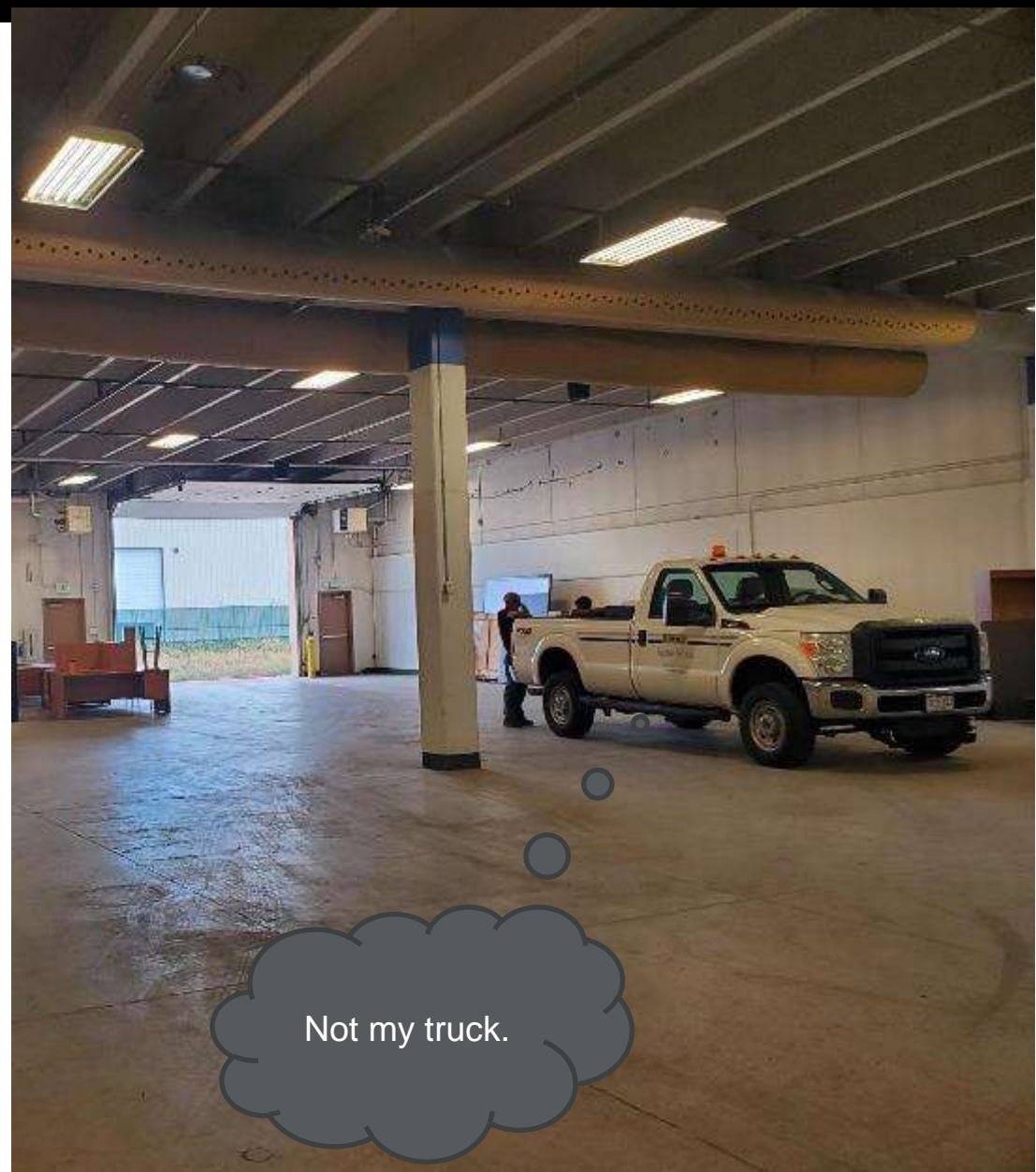
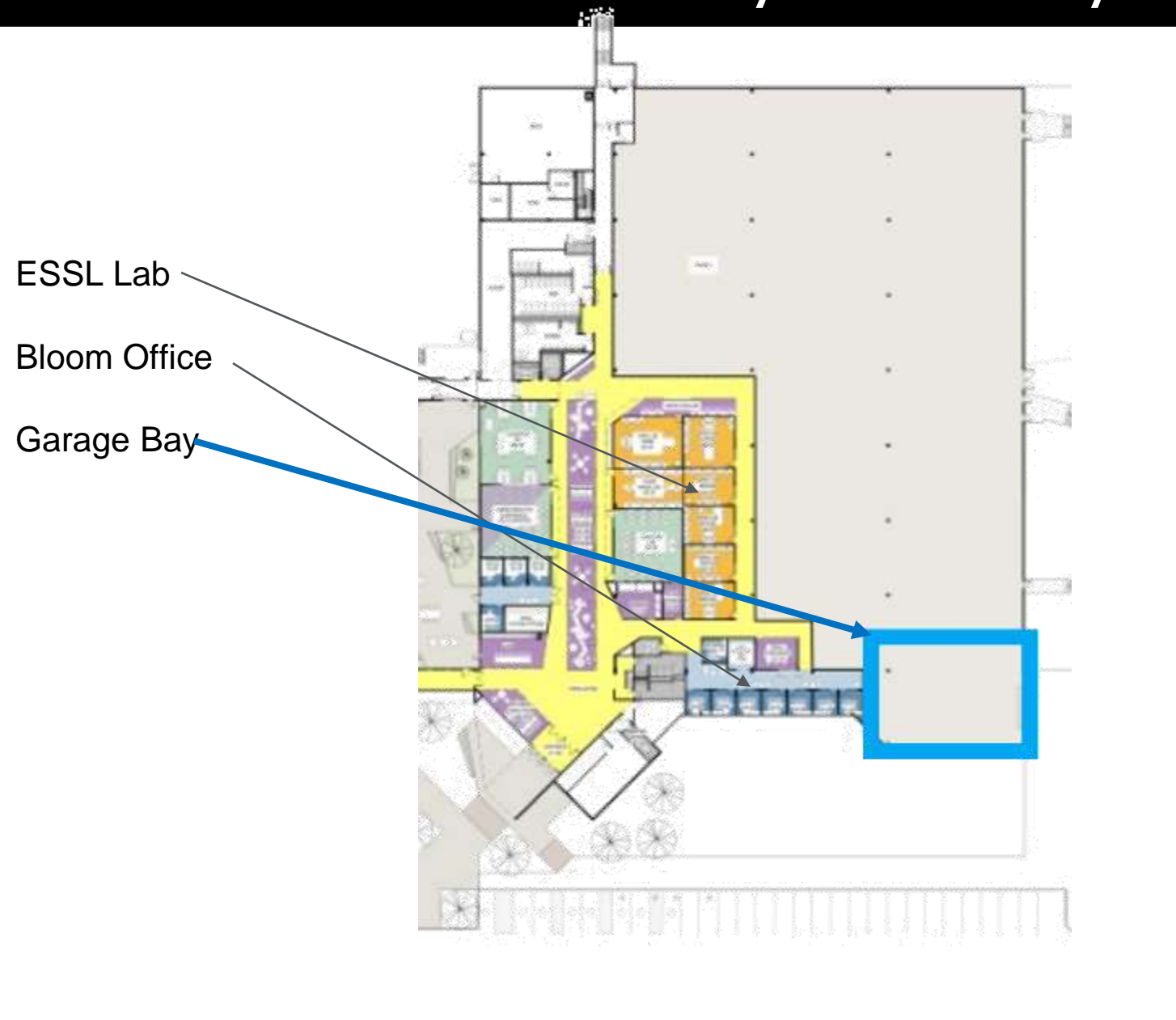


	Timing-based		Statistical-based				ML	
Attacks	Interval	Freq	CUSUM	Entropy	Graph	ID Seq.	Hamming	ANN
DoS	0.70	0.30	1.0	0.03	0.80	0.87	0.99	0.99
Fuzzy	0.67	0.99	0.65	0.05	0.99	0.92	0.99	0.98
RPM Spoof	0.00	0.1	1.0	0.08	0.82	0.83	0.85	0.86
Gear Spoof	0.00	0.12	1.0	0.10	0.67	0.87	0.86	0.87

Future Work in Vehicular Security

- **Real-Time Security**
 - Using principles of real-time theory to enhance security of real-time systems
 - Generalize to other cyber-physical system (CPS) domains
- **Connected and Autonomous Vehicles**
 - Cars, Robots, Planes, Satellites, Heavy Trucks
 - Transportation Infrastructure
 - Automotive Ethernet and V2V-V2I Protocols
- **Electric Vehicles**
 - Charging Stations and Electric Grid
- **Education, Training, and Outreach**
 - SAE CyberAuto, CyberTruck, CyberTractor, CyberBoat
 - Vehicle Cybersecurity Testbeds, Labs, and Curriculum

Facilities in the O'Neil Cybersecurity Education & Research Center



Embedded Systems Security Lab (ESSL @ UCCS)



Lab Director

Gedare Bloom, Ph.D.
Associate Professor

Lab Supervisor

Sena Hounsinou, Ph.D.
On the Job Market!



Affiliated Alumni

Habeeb Olufowobi, Ph.D.
Assistant Professor
University of Texas Arlington



Ebelechukwu Nwafor, Ph.D.
Assistant Professor
Villanova University



Ph.D. Students



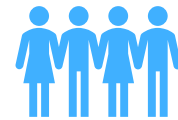
Vijay Banerjee



Uchenna Ezeobi



Doug Healy



Bobby Eimer
Rodney Jones
Farhad Mofidi
Zainab Olalekan*
Minhajul Alam Rahat*
Jordan Scott
Joshua Seaton*



Omolade Ikumapayi



Constance Hendrix



Katrina Rosemond



This work is supported by NSF CNS-2011620, NSF OAC-2001789, NSF-2046705, NSA H98230-21-1-0155 and Colorado State Bill 18-086. The opinions, findings, and conclusions or recommendations expressed are those of the author(s) and do not necessarily reflect the views of any other person or organization.