Safety and Security in the Automotive Supply Chain

Sebastian Fischmeister
Dept. of Electrical and Comp. Engineering
University of Waterloo

esg.uwaterloo.ca

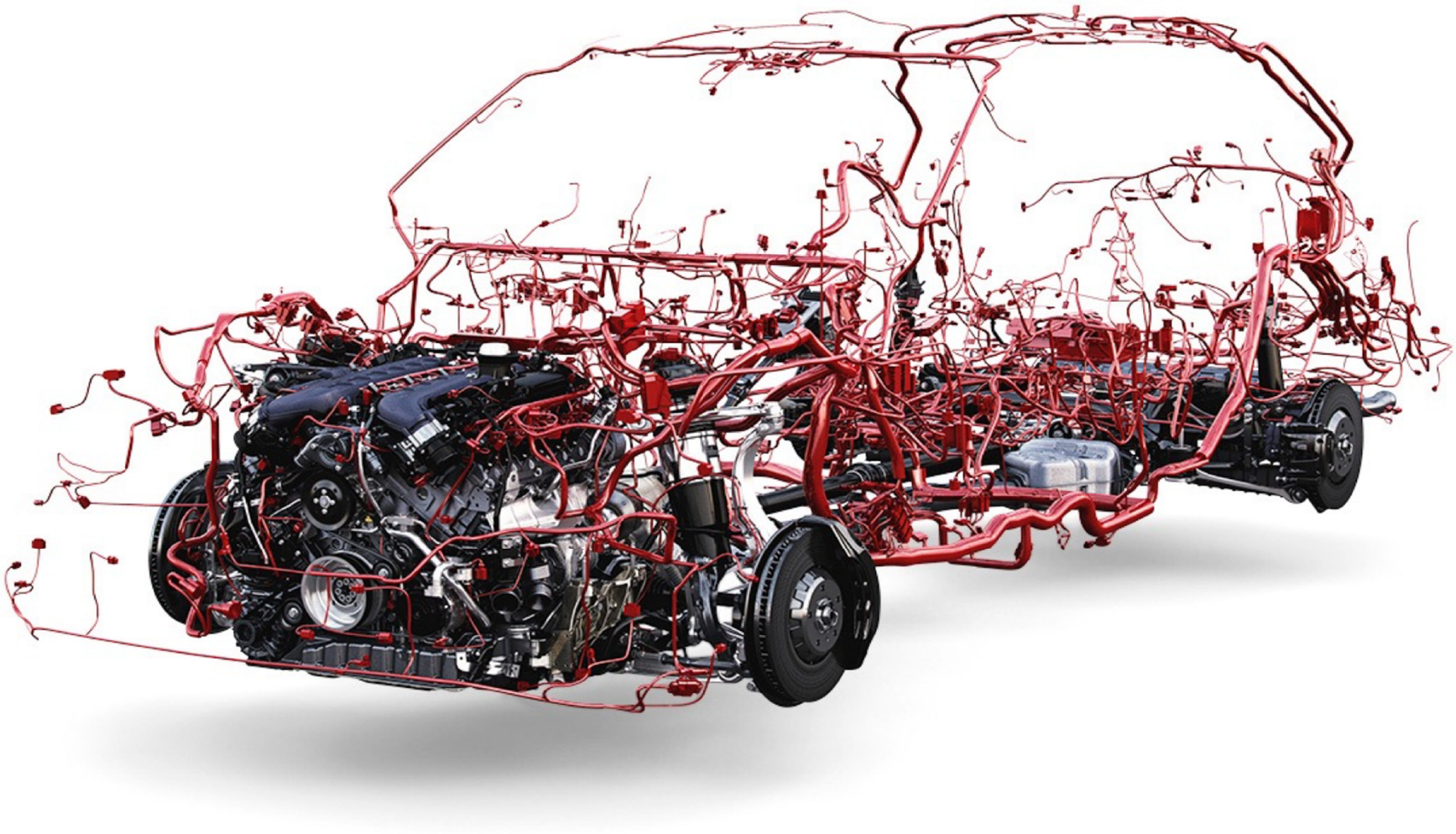
Objectives

(Disclaimer: exaggerated for dramatic effect)

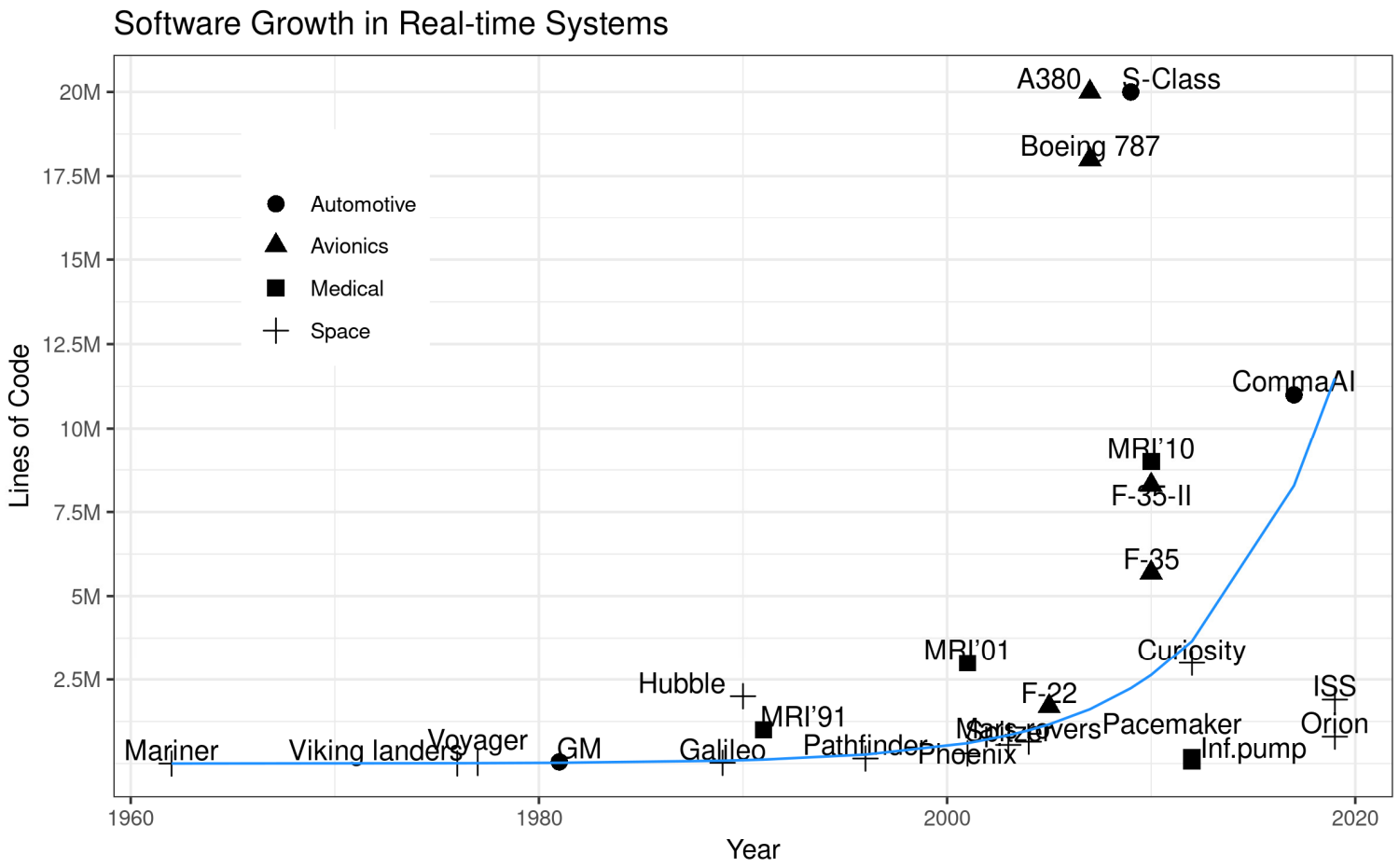
- Show that we have no clue what's going on in modern systems
- Show that attackers (=business people) leverage this today
- Show that Canadians are at risk, because of it
- Show a silver lining and a call to action

Modern Vehicles are Beyond Deep Comprehension of Human Minds

Cars are Complicated



Code Complexity is Increasing



- Ford F150: **150M**

- Between 30-100 ECUs in cars (across 6 citable sources)

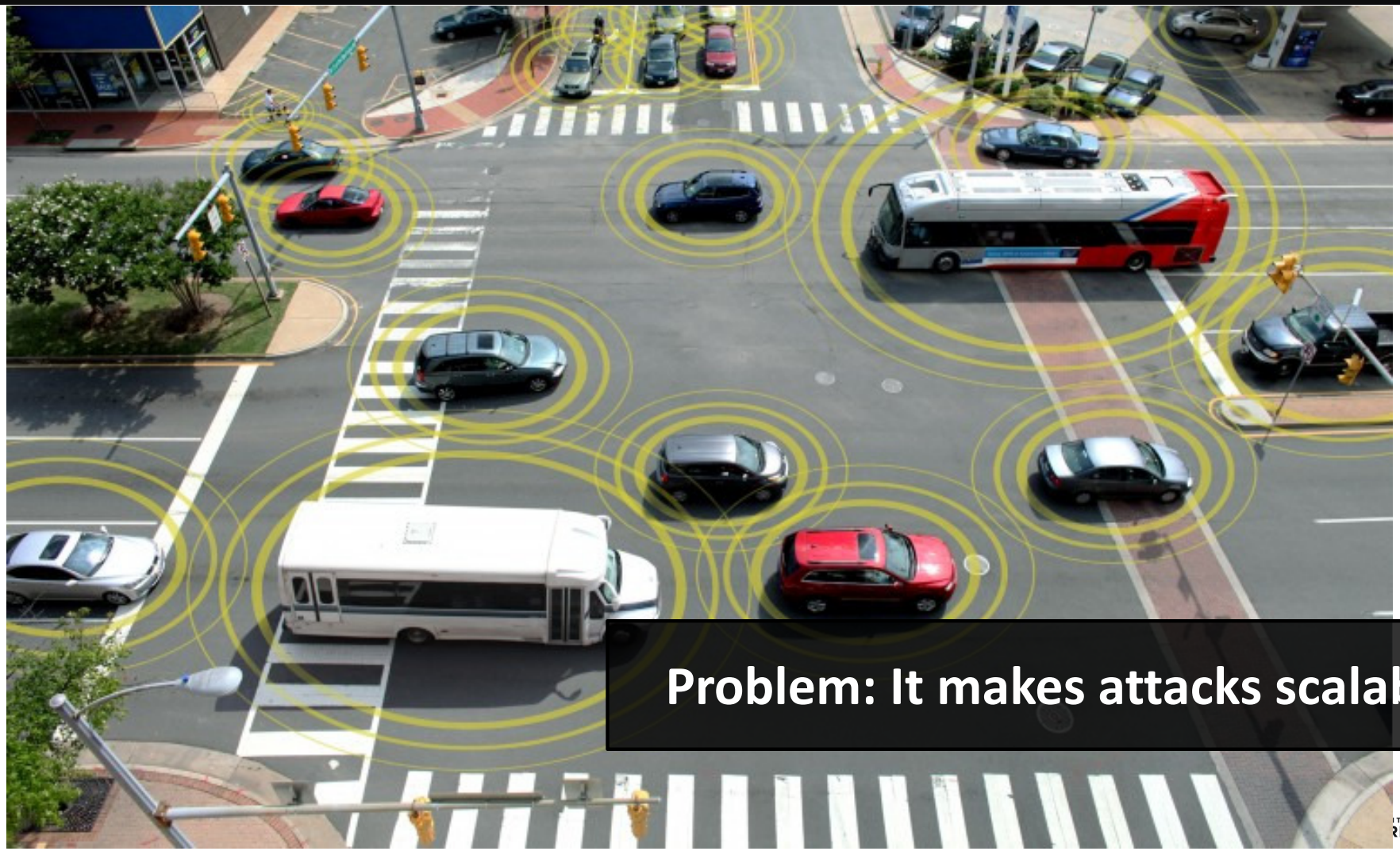
We Cannot Comprehend Digital Systems

Nobody would build the bridge, but people would try to build digital systems of equal complexity.

=> Humans are terrible at judging logical complexity

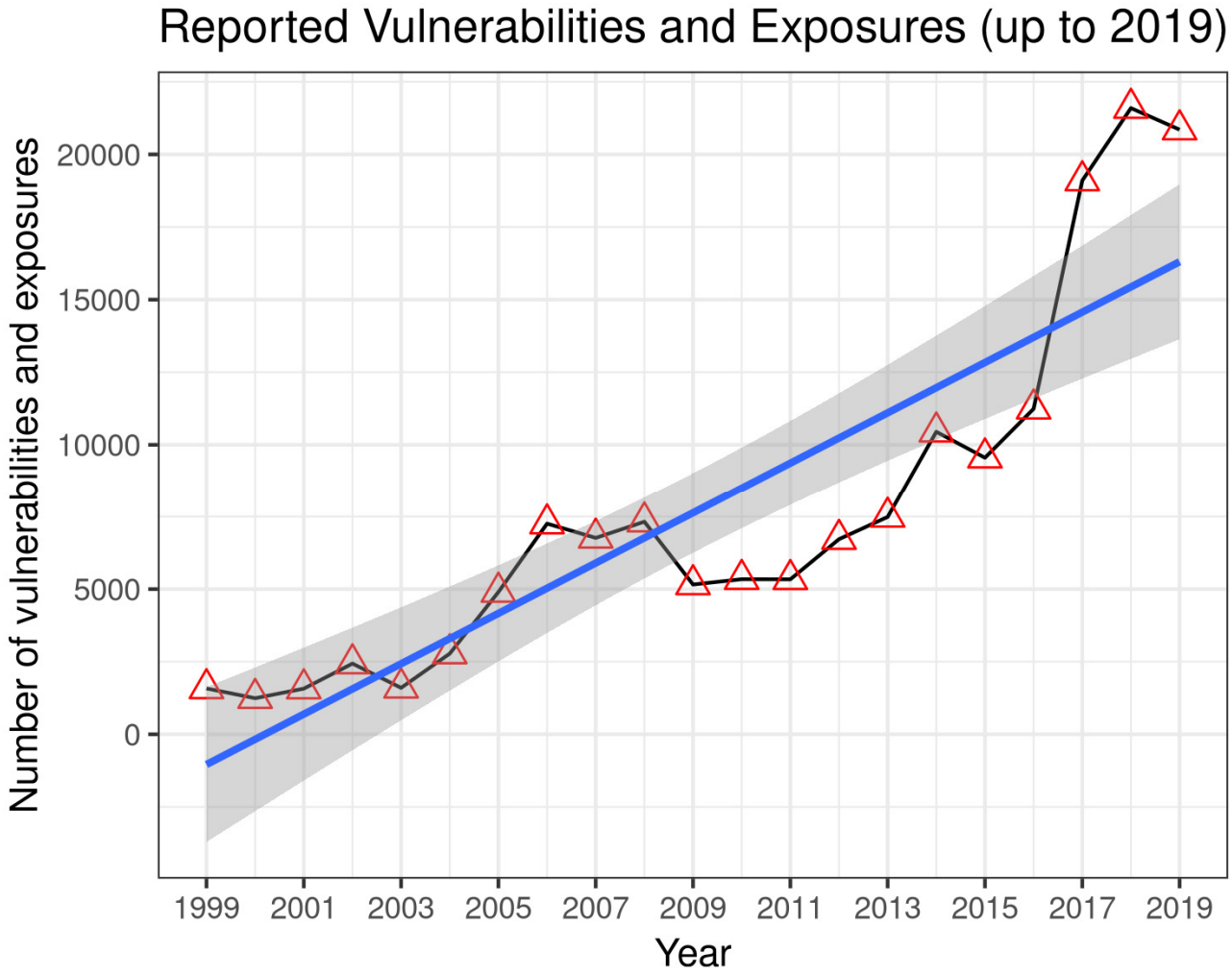
Illustrating one root cause:
Bridge from Tokyo
to Vancouver

Systems Are Safety-Critical and Networked



Problem: It makes attacks scalable!

More Vulnerabilities Every Year



160,274 (Dec '19)

In last 10 years:

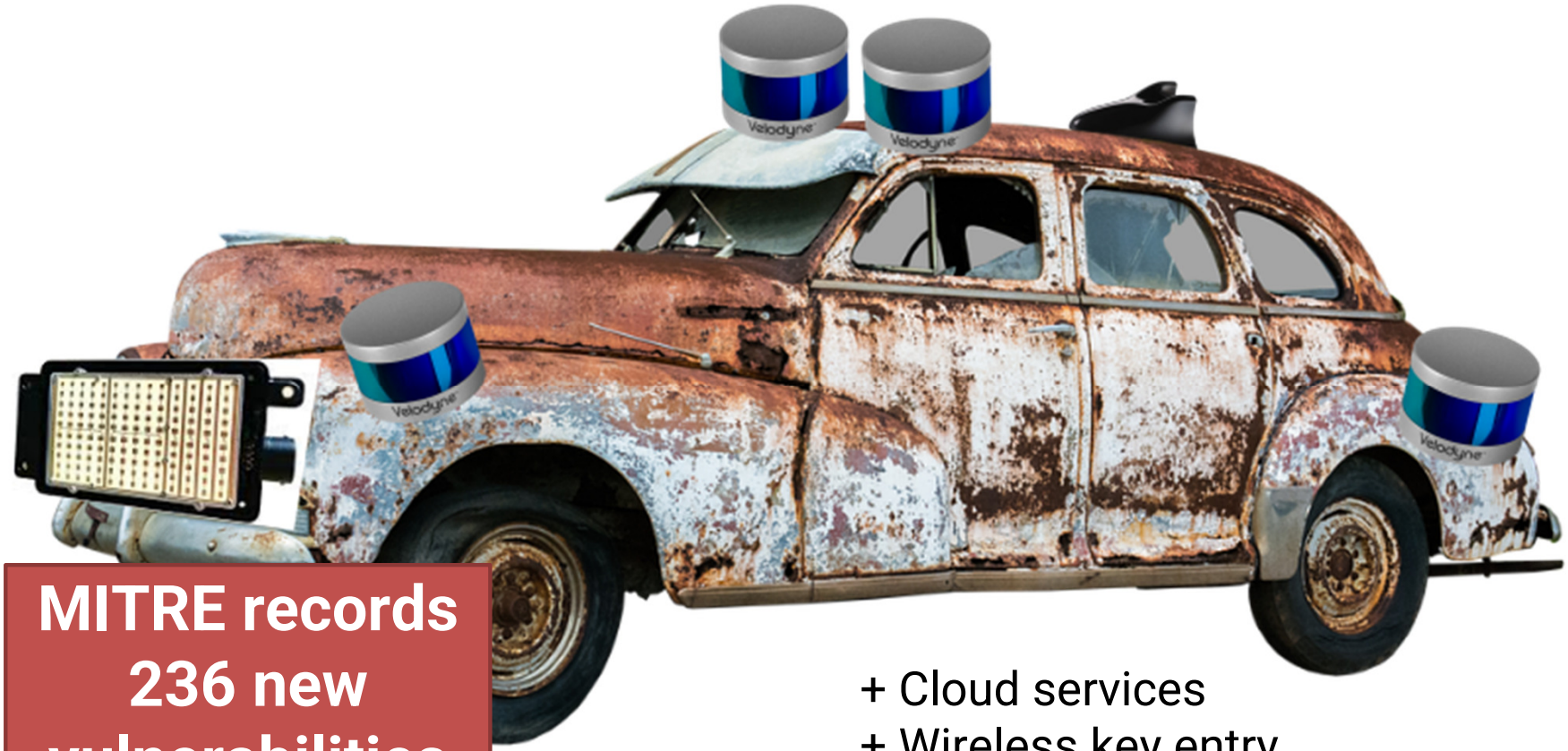
- **236 per week**
- **1.4 per hour (!)**

Durability of Vehicles Challenges Business Assumptions Compromising Safety & Security

Outdated in 1 year.

Operating since 1950s.

Your New Car will become a Highly-automated Oldtimer



MITRE records 236 new vulnerabilities per week

+ Cloud services
+ Wireless key entry
+ Android/Apple in Car
+ old V2V

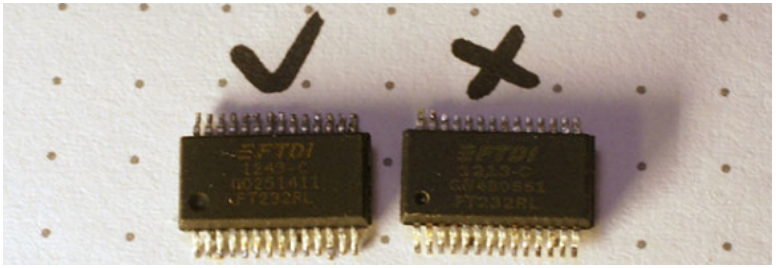
An Additional Frontier

SUPPLY CHAIN CYBERSECURITY

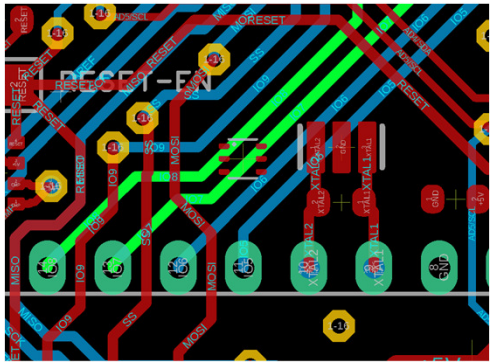
Problem: Trusting the Hardware

- Integrity of the underlying hardware?
- Did I get what I ordered?

Problem 1: Recycled e-waste sold as new.



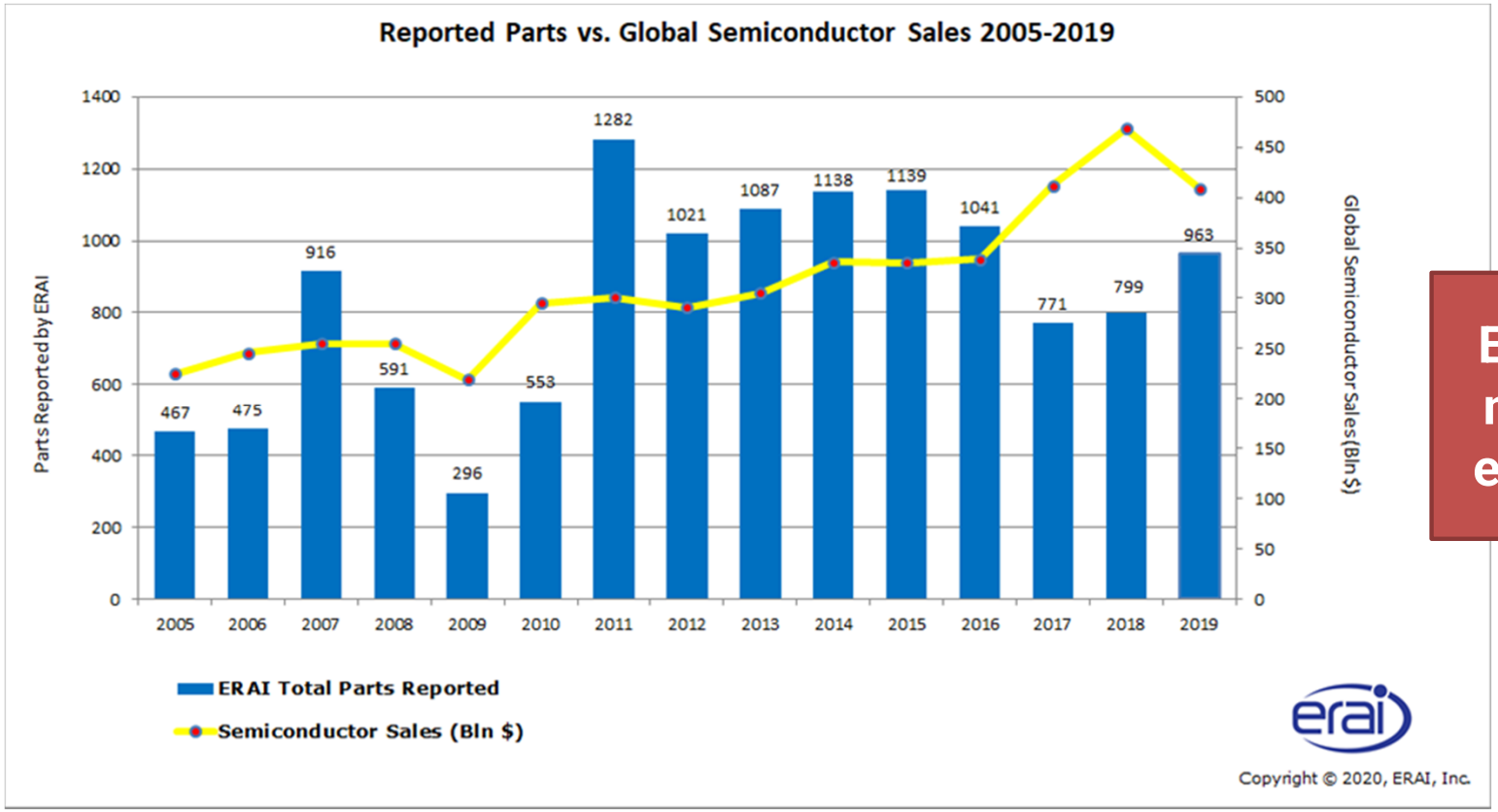
Problem 2: Counterfeit chips



Problem 3: Hardware implants

This decade will be about attacks through the supply chain.

How Big is the Problem?

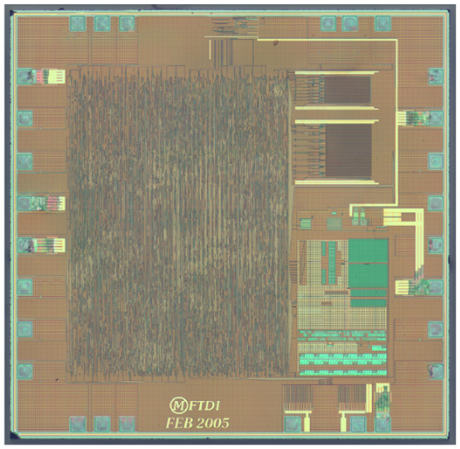


ERAI records 18 new counterfeit entries per week

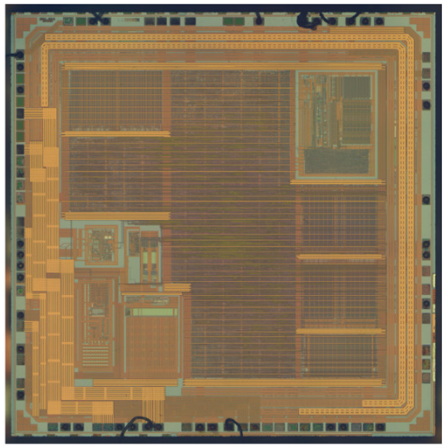
Taken from: https://www.erai.com/erai_blog/3167/_2019_erai_reported_parts_statistics

Counterfeit, Implant, Hardware Trojan Detection

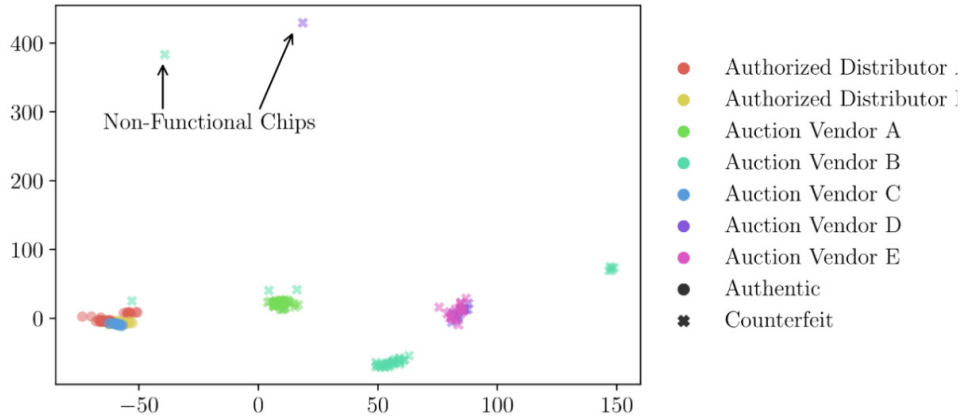
We purchased 220 FTDI Microcontroller chips on the open market from 7 different vendors
= Found 120 (54%) counterfeit chips in total



(a) Authentic Die [5]



(b) Counterfeit Die [5]



Bruce Power | Natural Resources Canada | National Defence

University of Waterloo | WatCAR driving innovation

Silver Lining: Hardware Integrity Assessment

- ✓ Non-destructive
- ✓ Blackbox
- ✓ Vendor Agnostic
- ✓ In-Situ

DETECT SUPPLY CHAIN ATTACKS

Detect implants, alterations, and weaknesses maliciously inserted into the firmware.

REVEAL COUNTERFEIT PARTS

Determine system integrity and detect counterfeit parts without requiring an internal inspection.

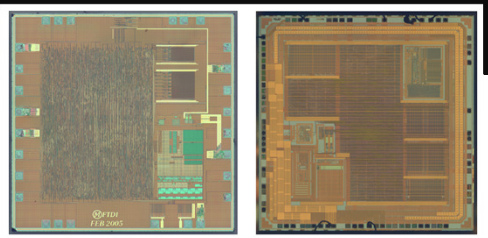
PROTECT AGAINST BACKDOORS

Identify undisclosed functionality through malicious firmware and hardware tampering.

Ensure that you got is actually what you ordered!

Developed at UWaterloo, commercialized through: Palitronica

Conclusions



(a) Authentic Die [5] (b) Counterfeit Die [5]

54% counterfeit!

- Vehicles are beyond deep comprehension of an individual
- Supply chain cybersecurity is important today
- Almost all companies blindly trust their suppliers
- Canadians accepts an unknown safety risk through the supply chain
- Technology for comprehensive the supply chain cybersecurity exists today

Call to action

- Urgent and important to nudge investment in supply chain cybersecurity
- Support POCs to understand what you can ask for

Contact info:

Sebastian Fischmeister
sfischme@uwaterloo.ca
Dept. of Electrical and Computer Eng.
University of Waterloo
200 University Ave West
Waterloo, ON N2L 3G1

This work was supported in part by industrial partners and the Canadian tax payer, so thank you very much to everyone who pays taxes.