Zero-trust Supply Chain for Critical Automotive Systems

Sebastian Fischmeister
Dept. of Electrical and Comp. Engineering
University of Waterloo
esg.uwaterloo.ca

Electronics are Everywhere

100+ computers, 10,000+ parts

80 independent computers

...

Commoditization, Race to Cheaper

$75,000 (2010)

$15,000 (2021)

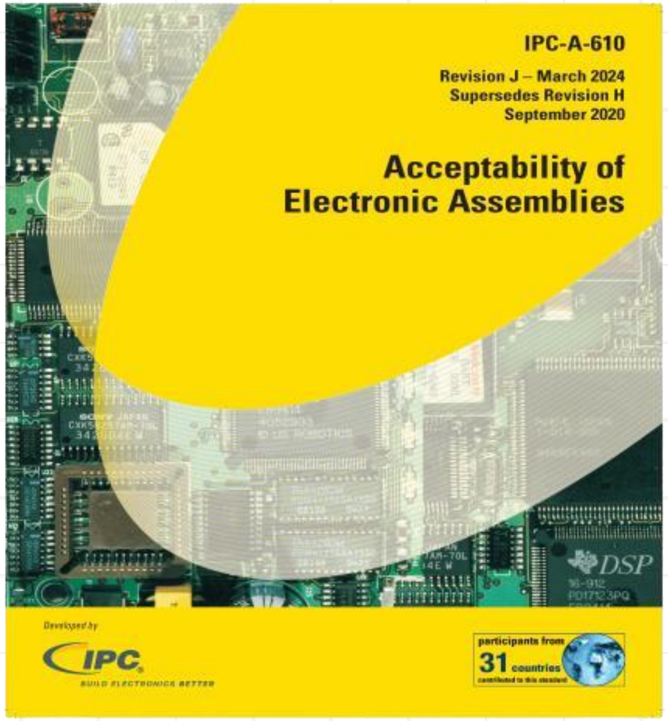
$1,000 (2025+)

Cut-throat competition tempts cutting corners

- **Defects**
- **Oversight**
- **Fraud**

Challenges In the Electronics Supply Chain

Defects


IPC-A-610

Revision J – March 2024
Supersedes Revision H
September 2020

Acceptability of
Electronic Assemblies

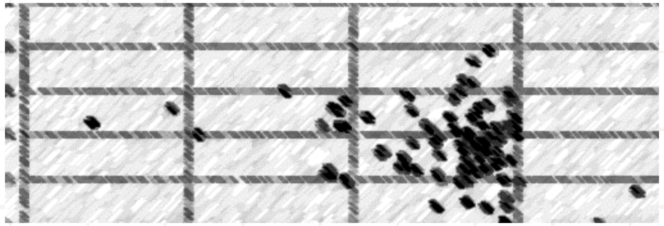
Developed by
IPC
BUILD ELECTRONICS BETTER

participants from
31 countries
contributed to this standard

Oversights

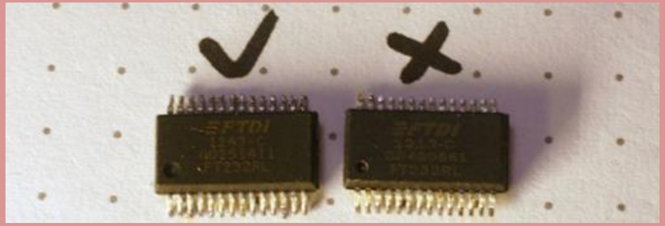
System misconfiguration

Silent substitution

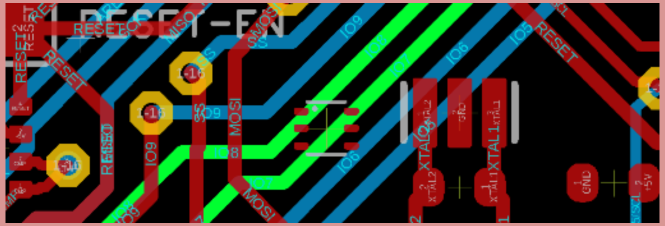

Manufacturing variance

Fraud

Recycled e-waste sold as new



Counterfeit electronics



Hardware implants

Cybersecurity Supply Chain Risk Types

Financial

Goal: make money

- Counterfeit, recycled, swapped parts
- Overproduction redirection
- Sale of implants

Activist

Goal: revenge, …

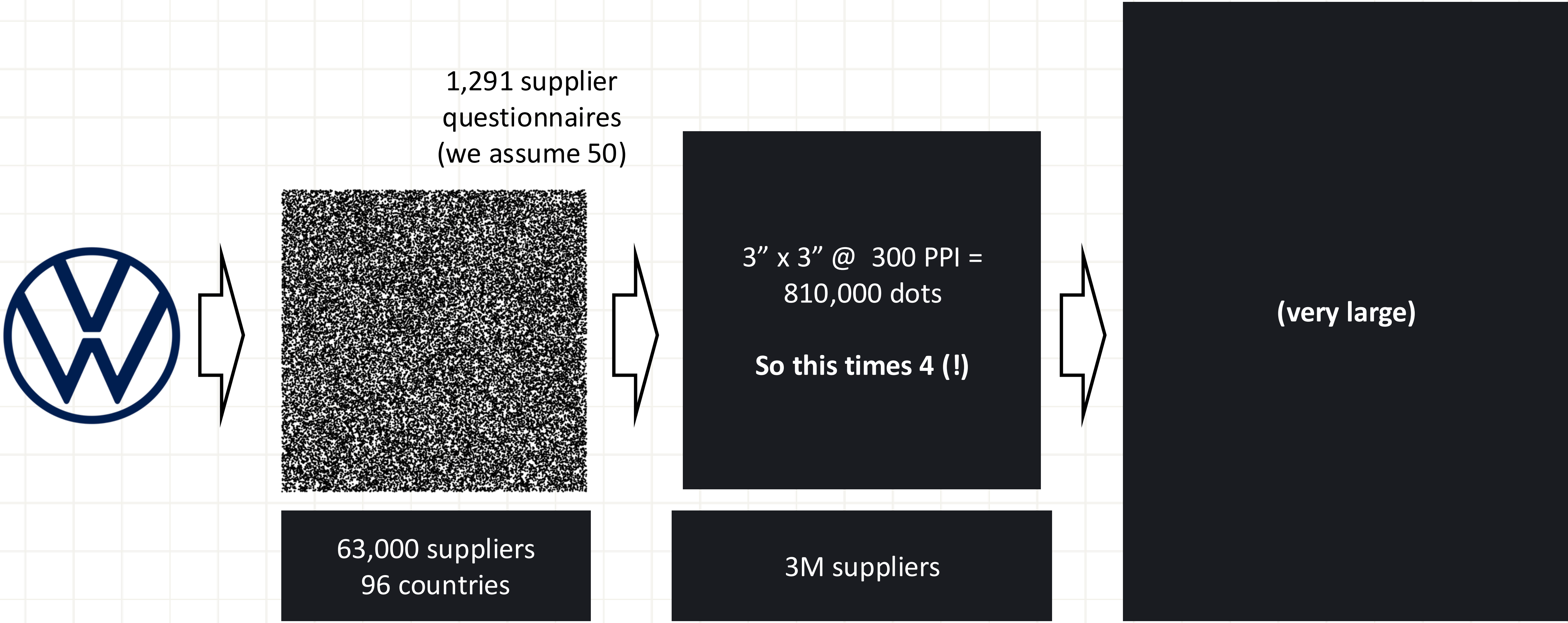
- Deliberate swap of parts
- Data leakage
- Change in design

Nation State

Goal: influence

- Attack staging
- Designed points of failure
- Leverage for geopolitical

Example of Supply Chain Network Effect



1,291 supplier questionnaires (we assume 50)

63,000 suppliers
96 countries

3” x 3” @ 300 PPI =
810,000 dots

So this times 4 (!)

3M suppliers

(very large)

> *“Acquirers **often lack visibility** and understanding ….”*
>
> NIST 800-161: Cybersecurity Supply Chain Risk Management

Trusted-based Supply Chain Risk Management

Step 1

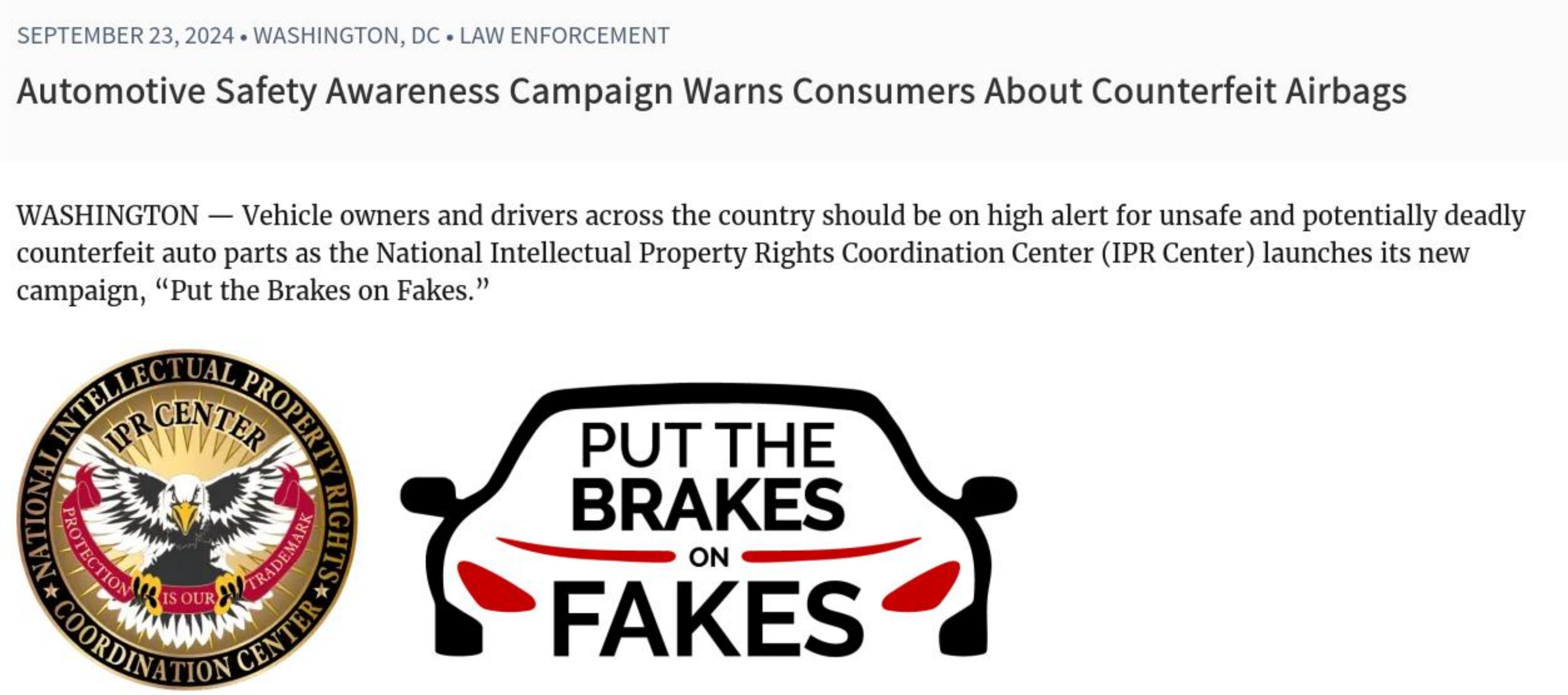
Fill in supplier questionnaire

Step 2

Maybe test a sample

And everything is fine … Until it’s not!

Automotive Industry has Counterfeit Problems



SEPTEMBER 23, 2024 • WASHINGTON, DC • LAW ENFORCEMENT

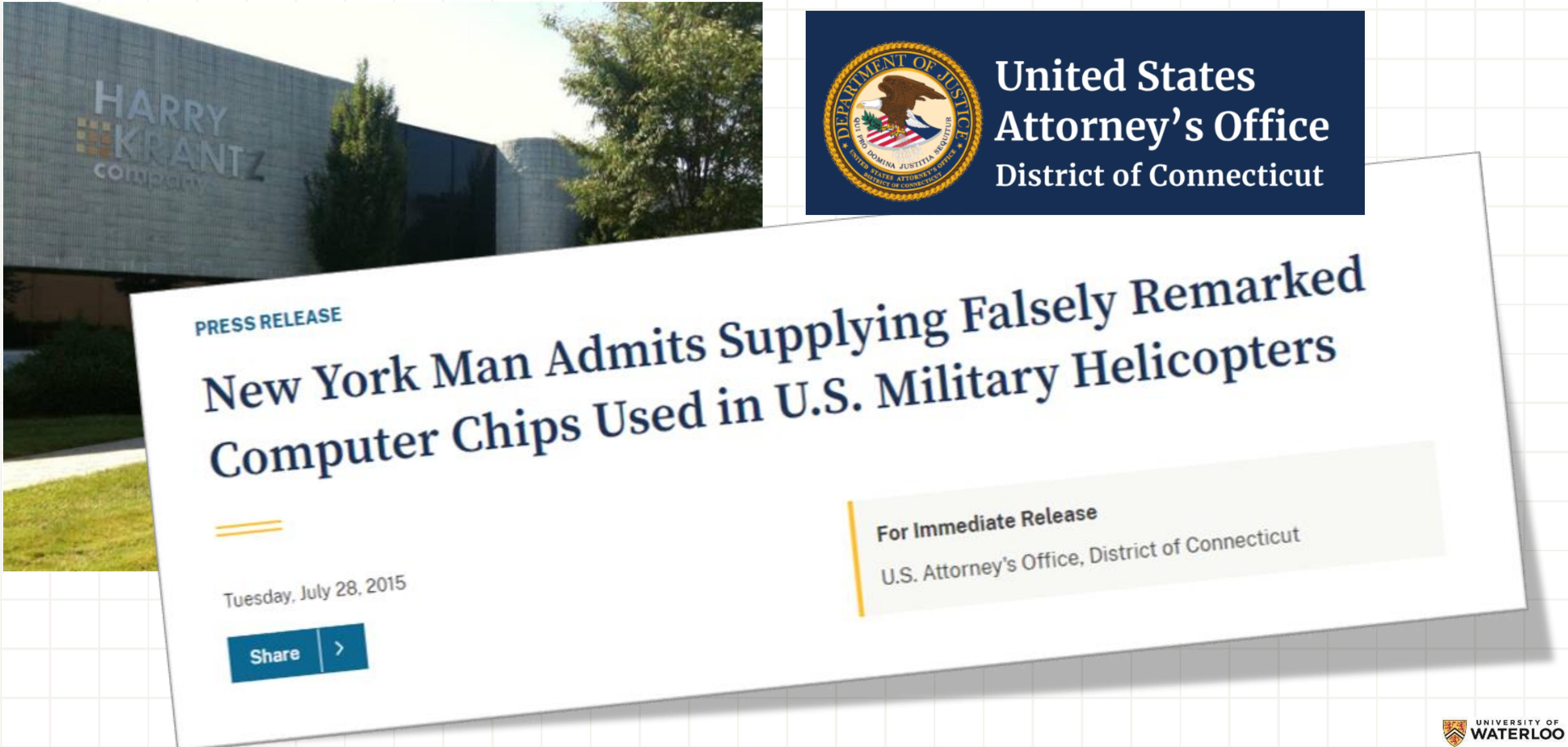
Automotive Safety Awareness Campaign Warns Consumers About Counterfeit Airbags

WASHINGTON — Vehicle owners and drivers across the country should be on high alert for unsafe and potentially deadly counterfeit auto parts as the National Intellectual Property Rights Coordination Center (IPR Center) launches its new campaign, “Put the Brakes on Fakes.”

NATIONAL INTELLECTUAL PROPERTY RIGHTS
COORDINATION CENTER
IPR CENTER
PROTECTION IS OUR TRADEMARK
PUT THE
BRAKES
ON
FAKES

Incorrectly Marked Electronics

United States Attorney's Office
District of Connecticut



PRESS RELEASE

New York Man Admits Supplying Falsely Remarked Computer Chips Used in U.S. Military Helicopters

Tuesday, July 28, 2015

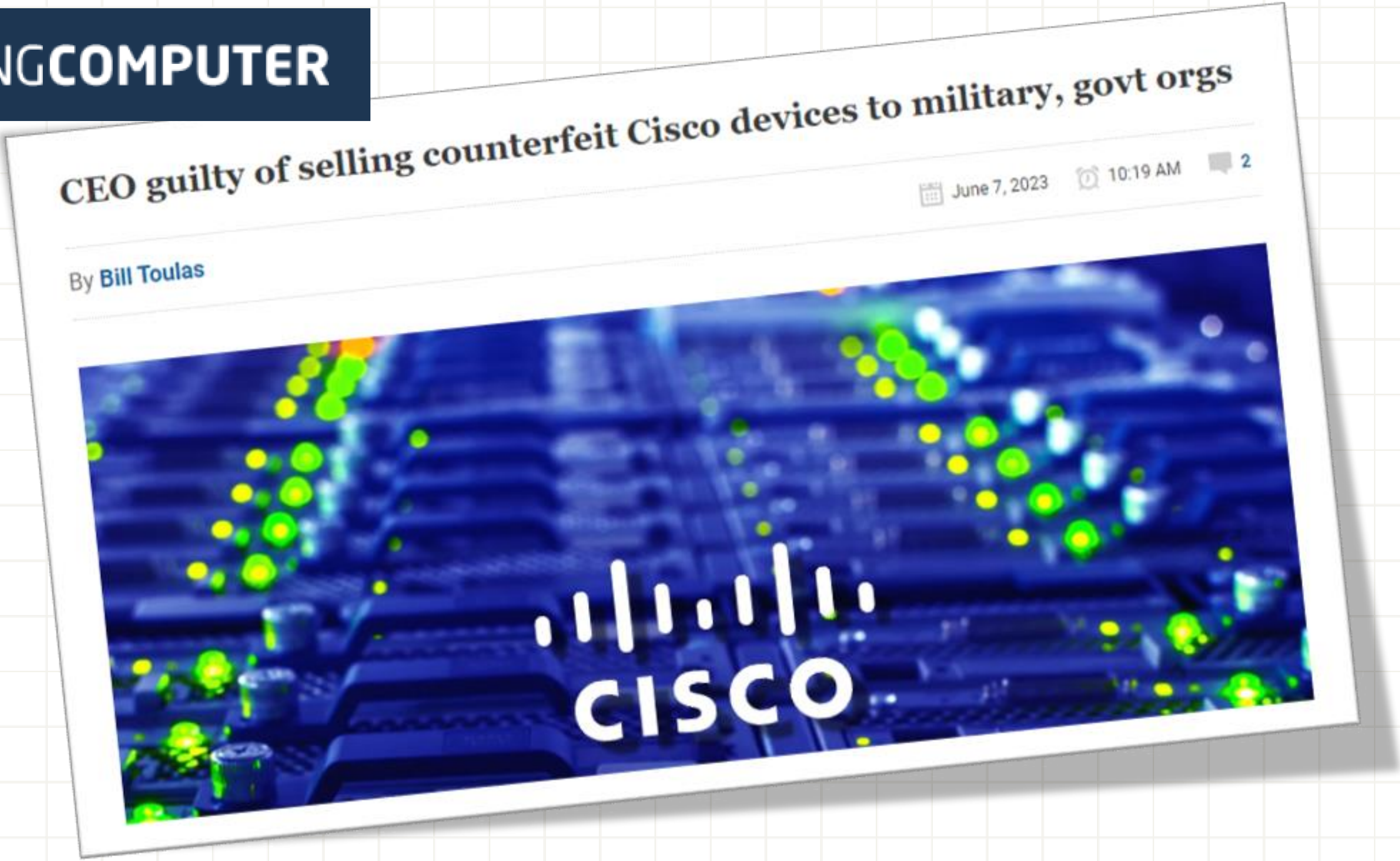
Share >

For Immediate Release

U.S. Attorney's Office, District of Connecticut

Tampered Electronics

BLEEPINGCOMPUTER

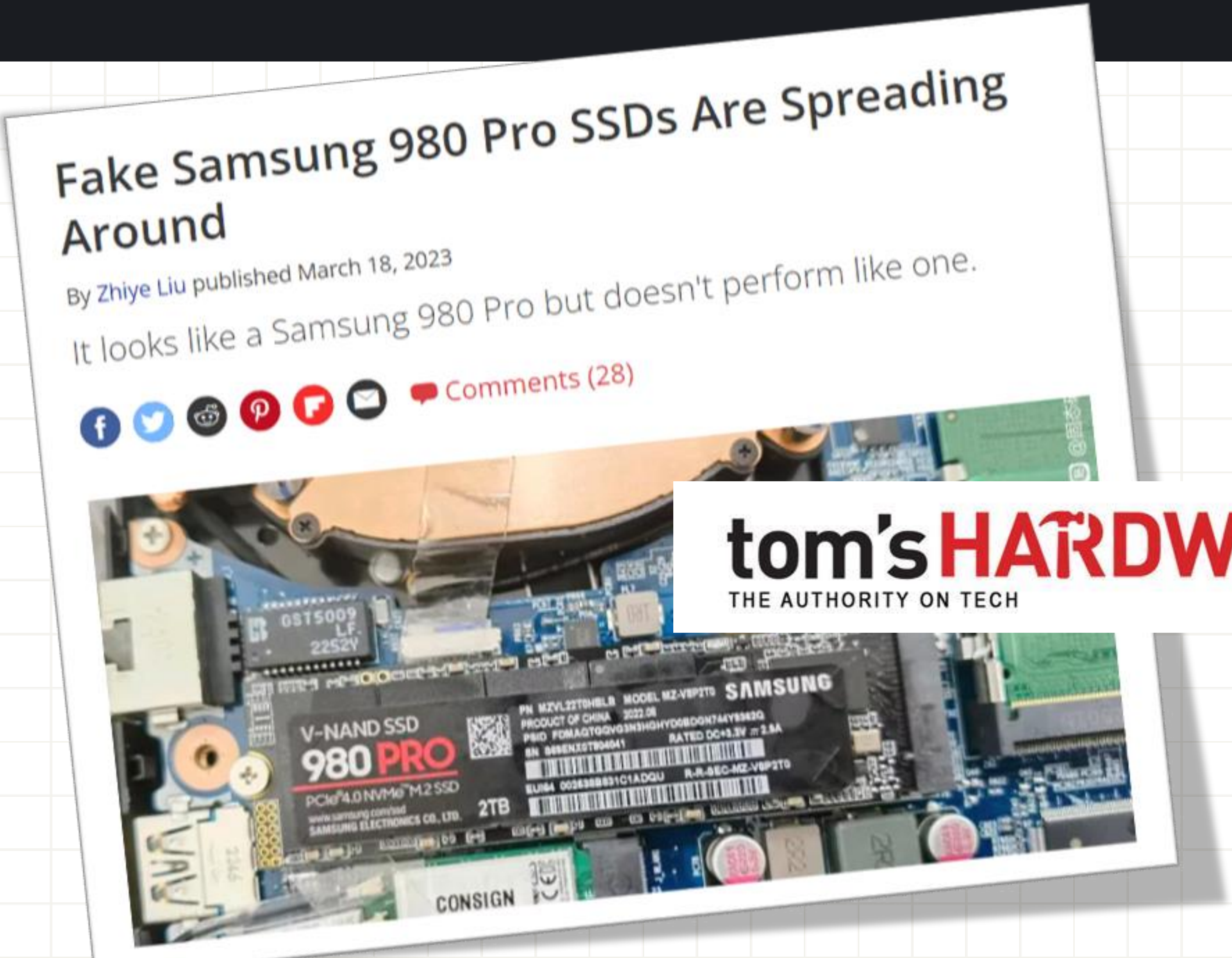


CEO guilty of selling counterfeit Cisco devices to military, govt orgs

June 7, 2023 10:19 AM 2

By Bill Toulas

COTS



Fake Samsung 980 Pro SSDs Are Spreading Around

By Zhiye Liu published March 18, 2023

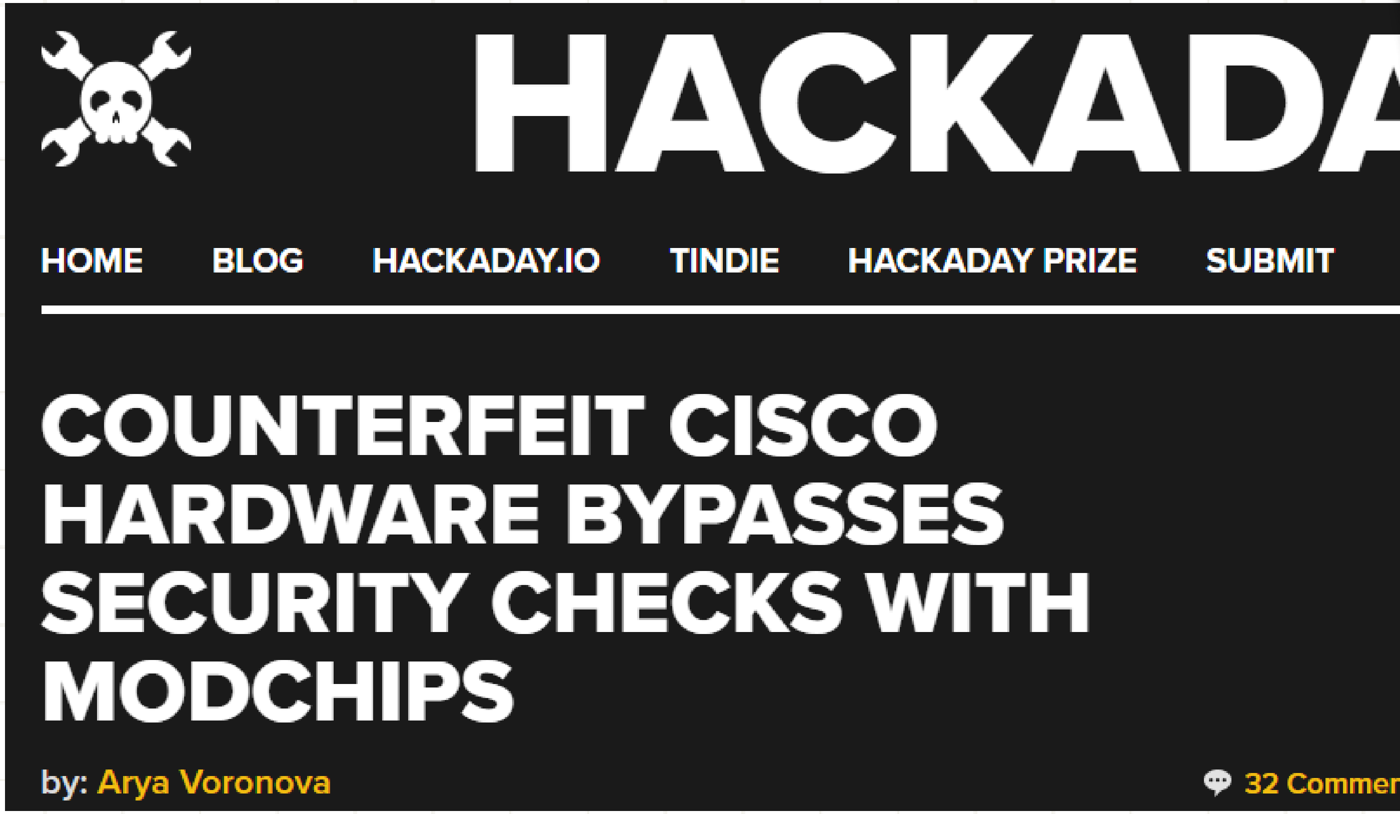
It looks like a Samsung 980 Pro but doesn't perform like one.

Comments (28)

tom's HARDWARE

THE AUTHORITY ON TECH

Cisco Modchip (TOCTOU)



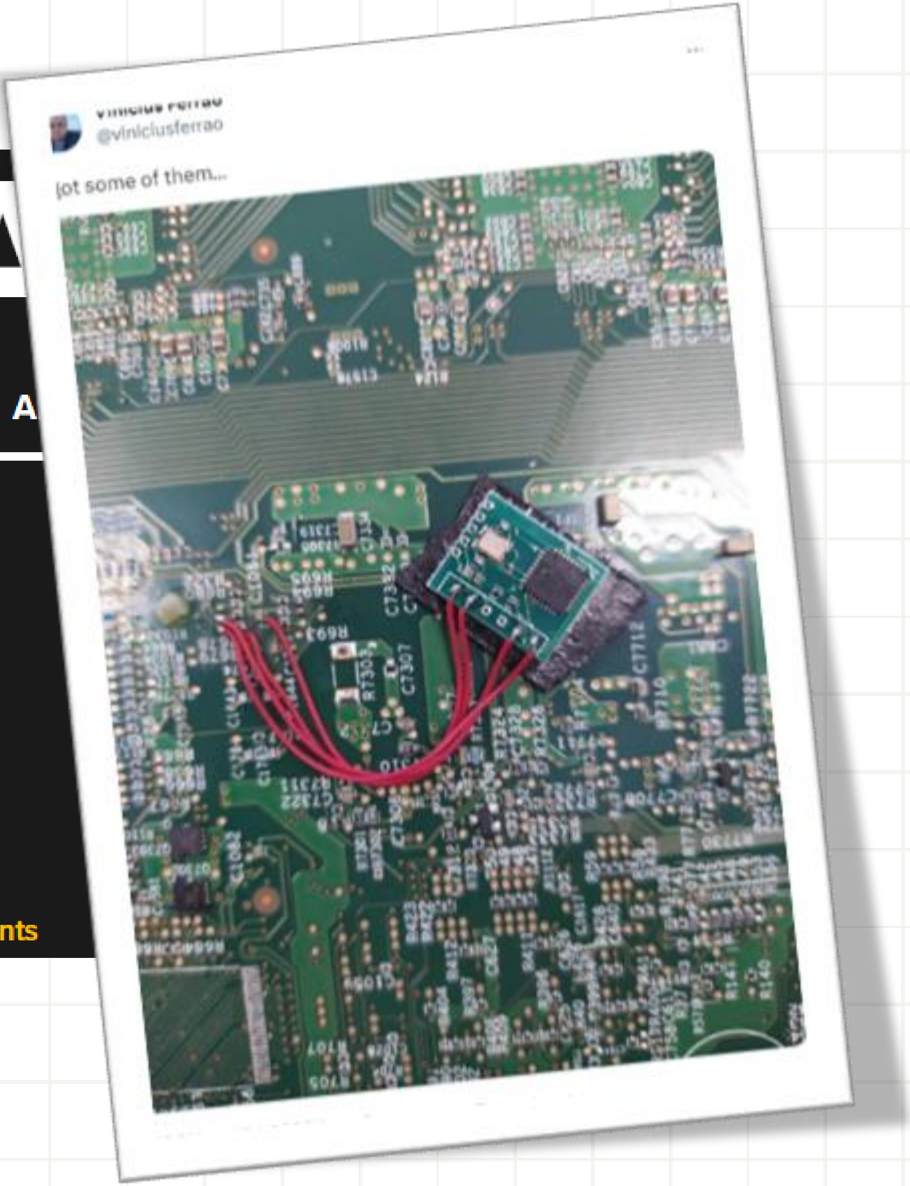
HACKADA

HOME BLOG HACKADAY.IO TINDIE HACKADAY PRIZE SUBMIT A

COUNTERFEIT CISCO HARDWARE BYPASSES SECURITY CHECKS WITH MODCHIPS

by: Arya Voronova

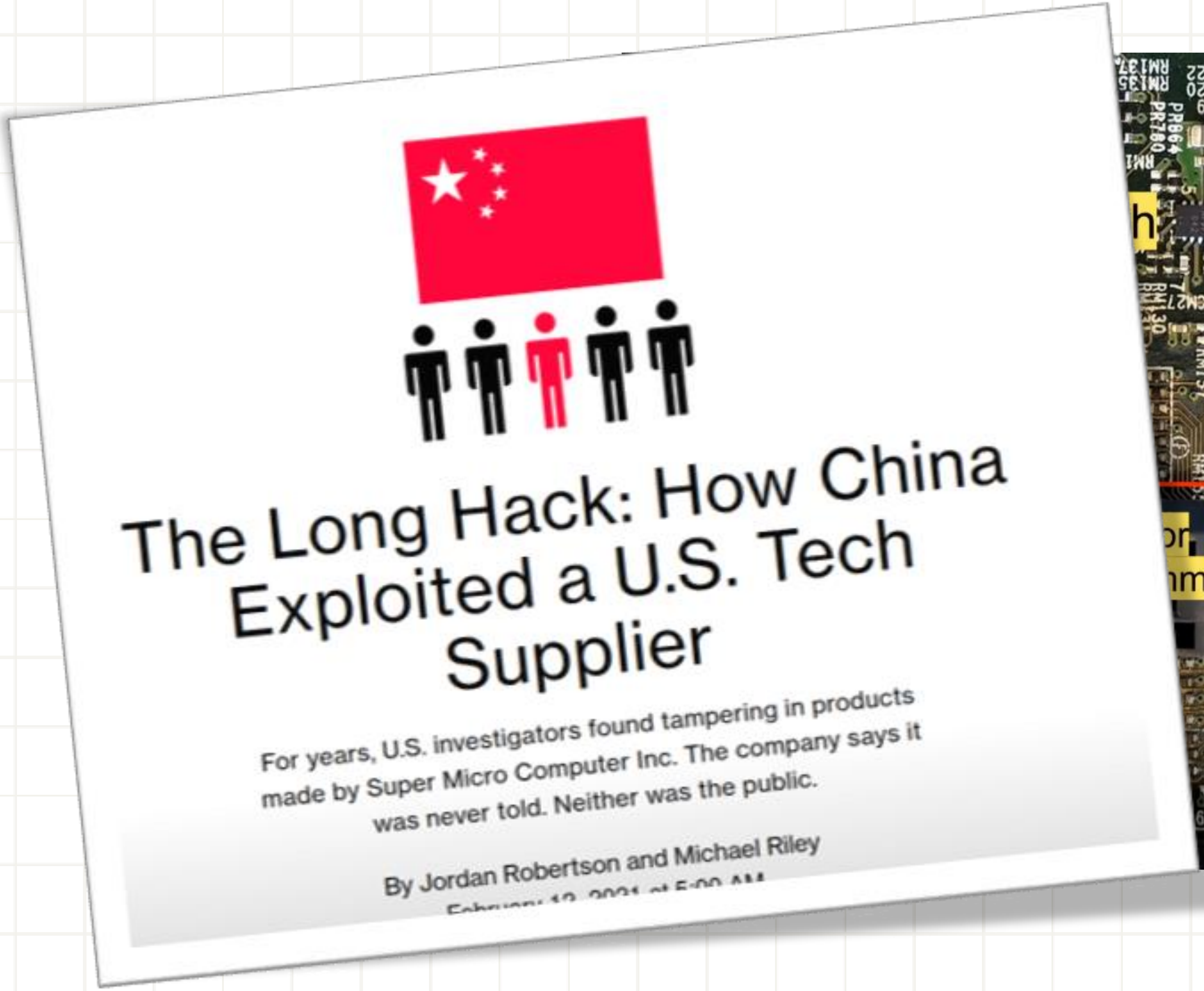
32 Comments



Vinicius Ferrao
@viniciusferrao

jot some of them...

Trammell Hudson: Super Micro Attack Prototype Implementation

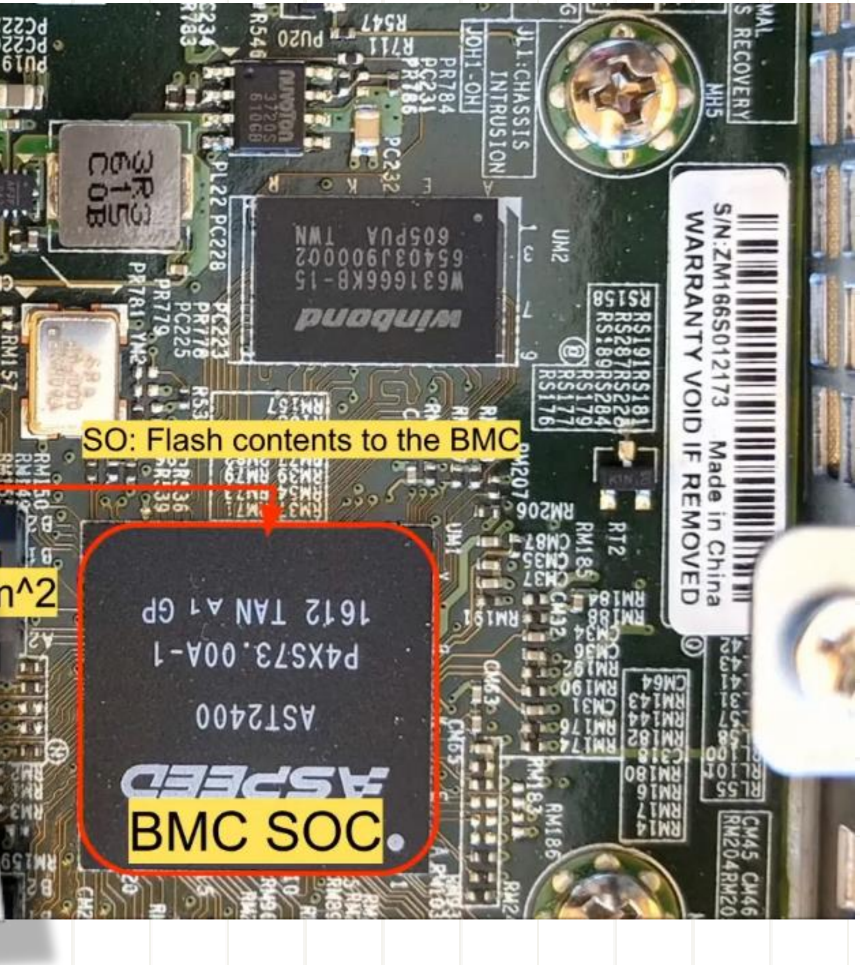


The Long Hack: How China Exploited a U.S. Tech Supplier

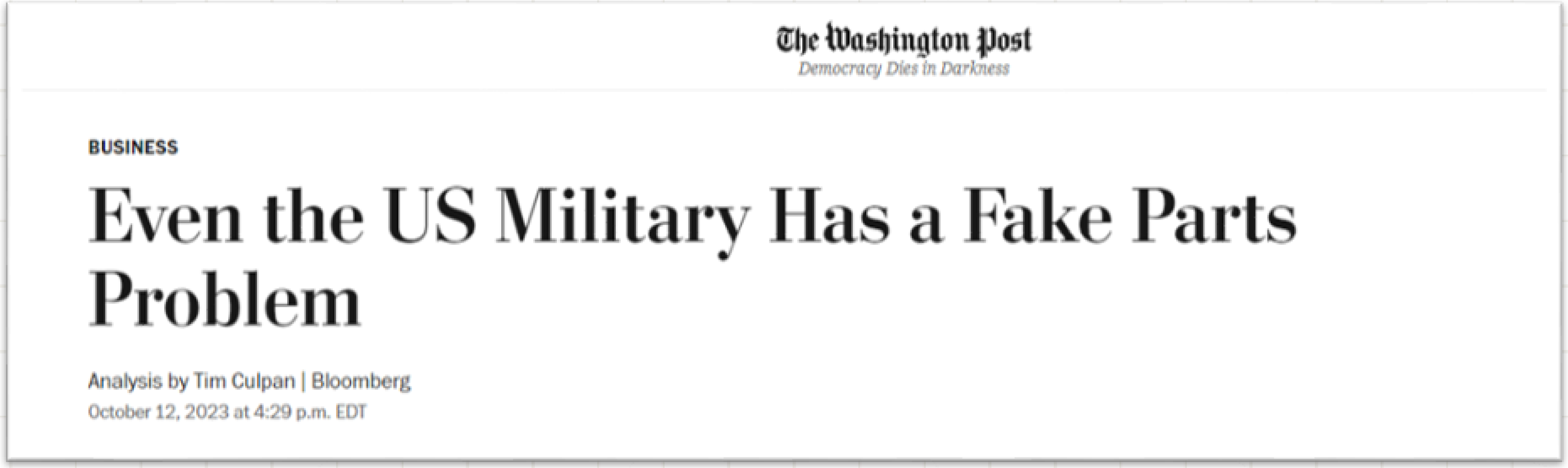
For years, U.S. investigators found tampering in products made by Super Micro Computer Inc. The company says it was never told. Neither was the public.

By Jordan Robertson and Michael Riley

February 12, 2021 at 5:00 AM



There’s Your “Trusted Supplier”



The Washington Post
Democracy Dies in Darkness

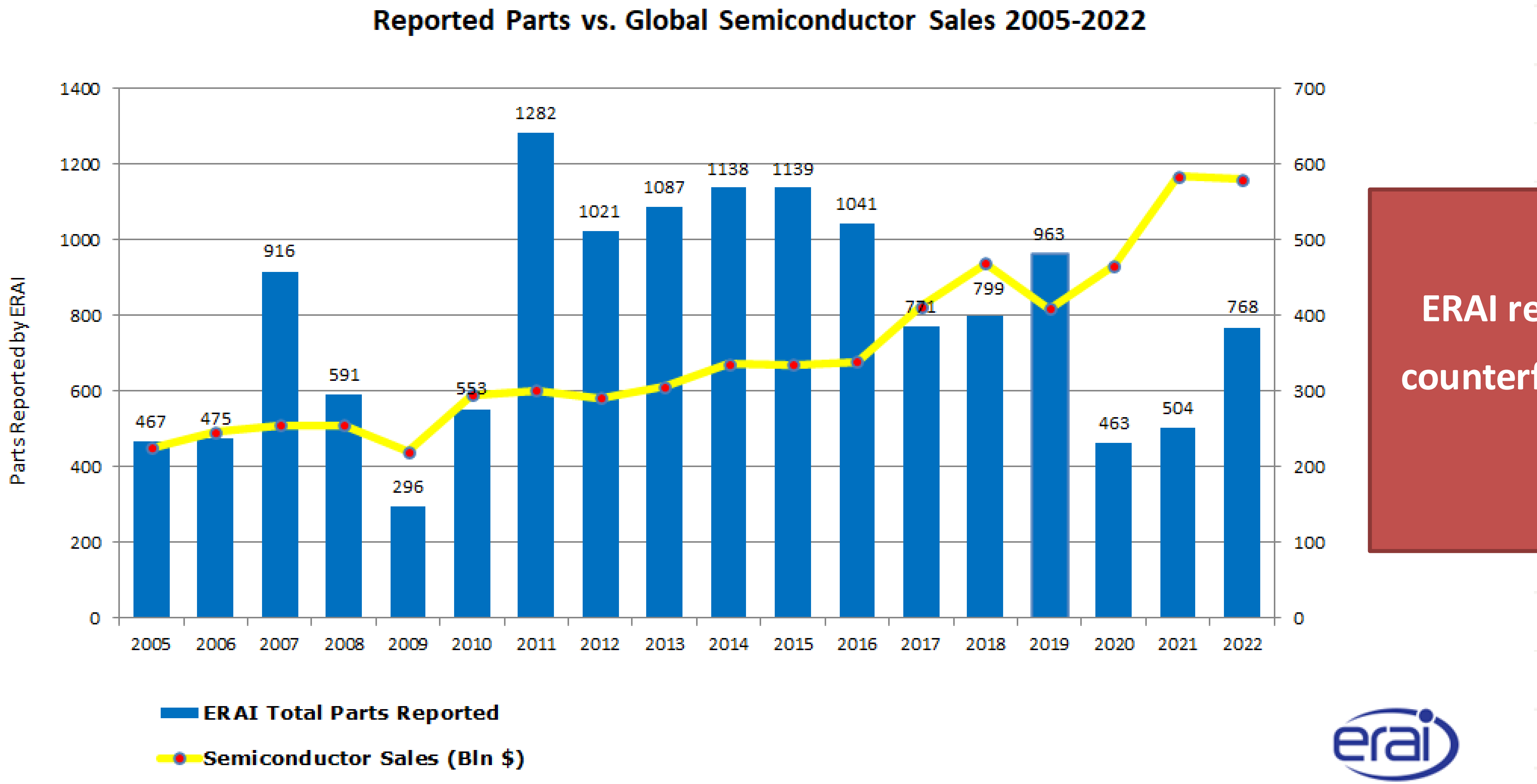
BUSINESS

Even the US Military Has a Fake Parts Problem

Analysis by Tim Culpan | Bloomberg
October 12, 2023 at 4:29 p.m. EDT

- 400 displays installed **in US C-130J and C-27J military aircraft**
- […] 1/3 failure rate including one incident […] in use
- L-3 Communication Display Systems placed an order […] (demanded) sample pieces (for testing) […]
- Not a problem: The Chinese vendor handpicked 18 genuine chips […]
- another 6,000 was placed. The chips were fakes.

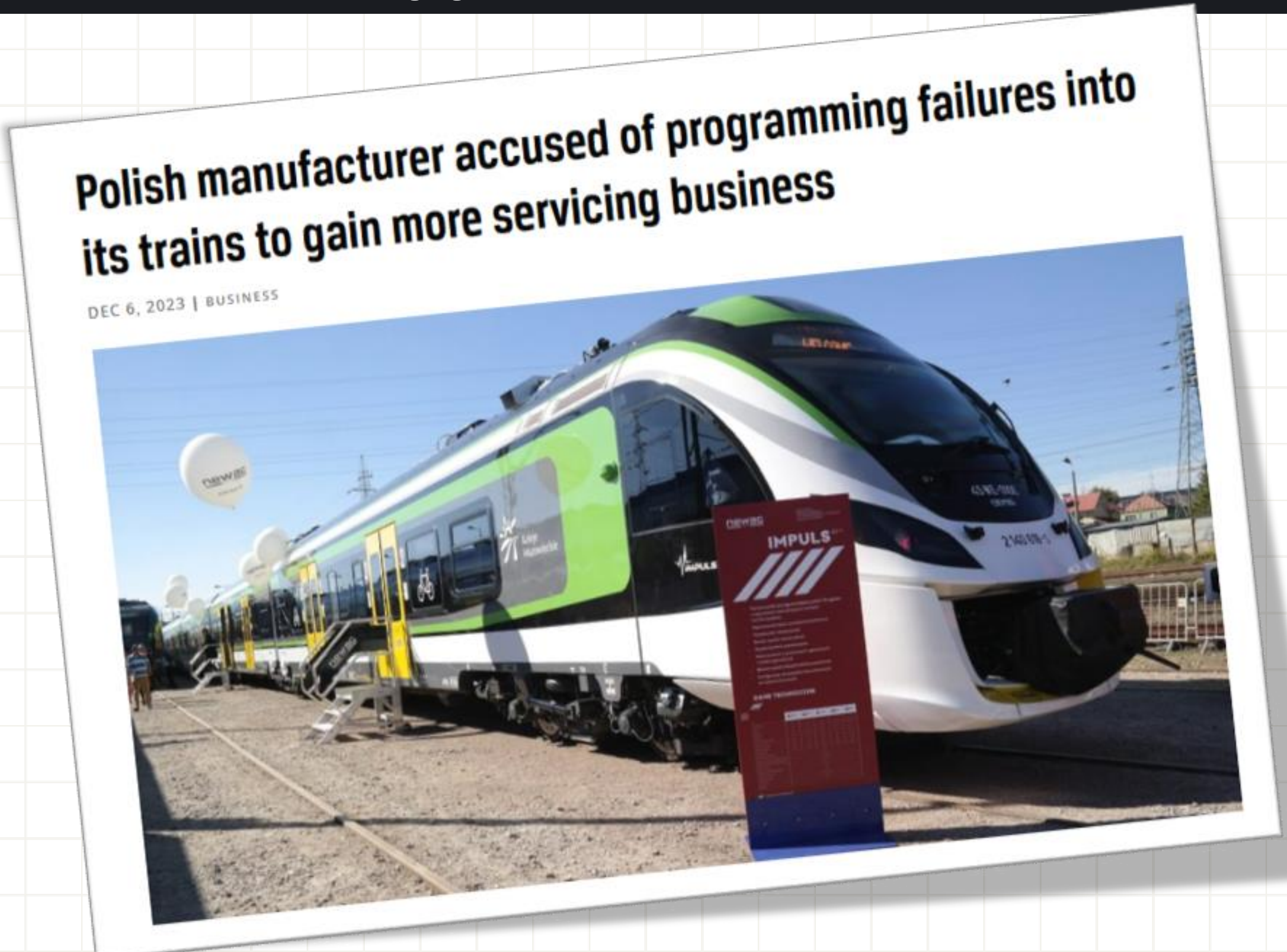
How Big is the Problem?



ERAI records **14** new counterfeit entries **per week**

https://www.erai.com/erai_blog/3181/_2022_annual_report

Your “Trusted Supplier” is Not Your Friend



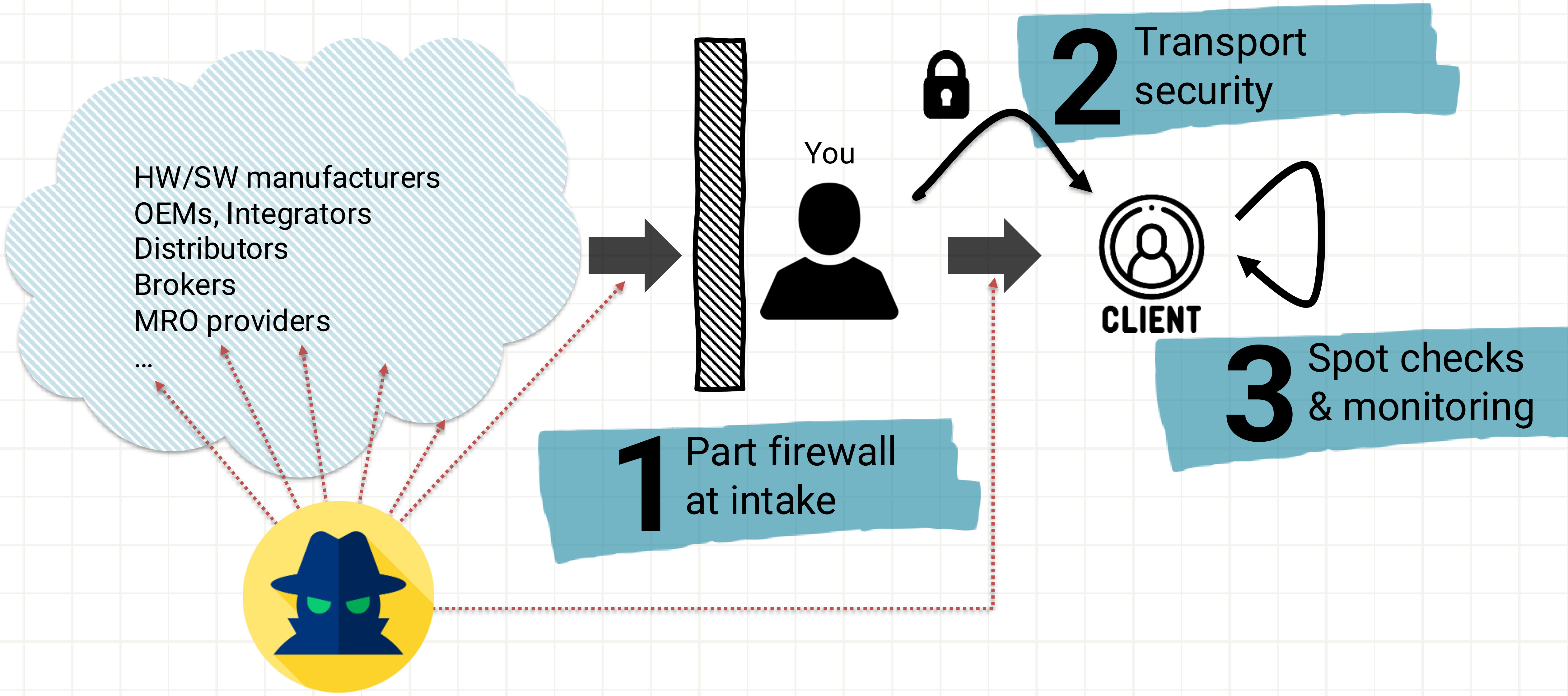
Polish manufacturer accused of programming failures into its trains to gain more servicing business

DEC 6, 2023 | BUSINESS

Supplier was a secret competitor

ZERO-TRUST FOR THE AUTOMOTIVE SUPPLY CHAIN

Supply Chain Risk Monitoring Model



HW/SW manufacturers
OEMs, Integrators
Distributors
Brokers
MRO providers
…

You

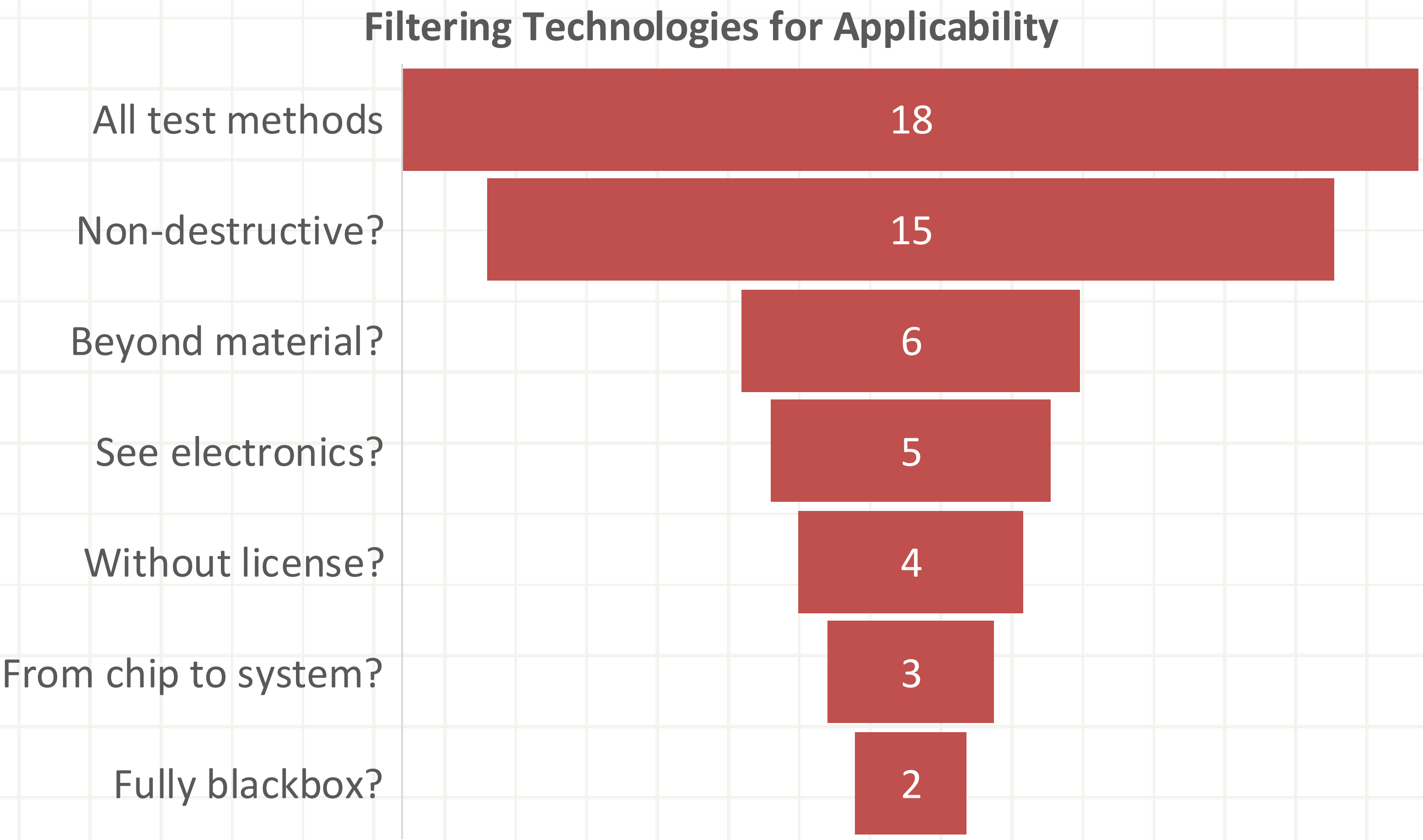
CLIENT

1 Part firewall at intake

2 Transport security

3 Spot checks & monitoring

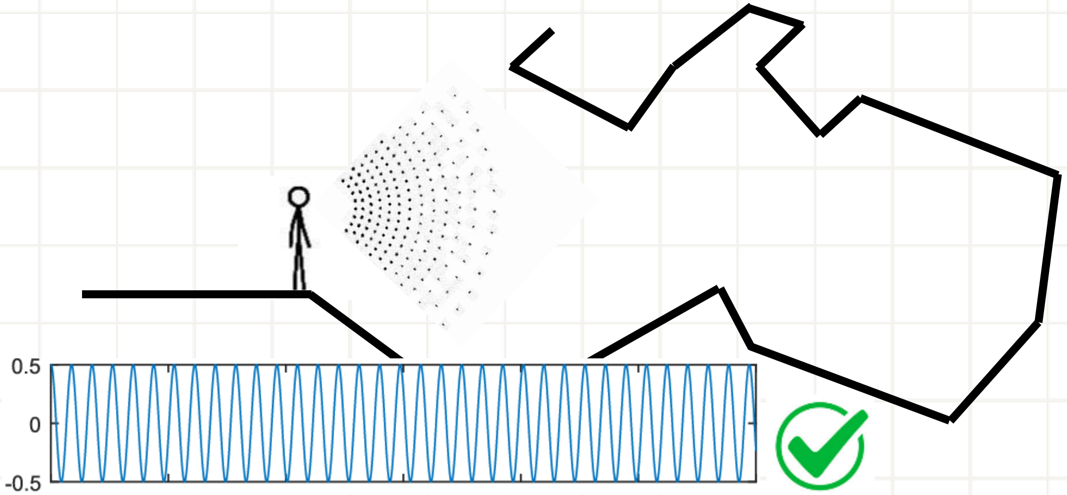
Test Methods (AS6171A)



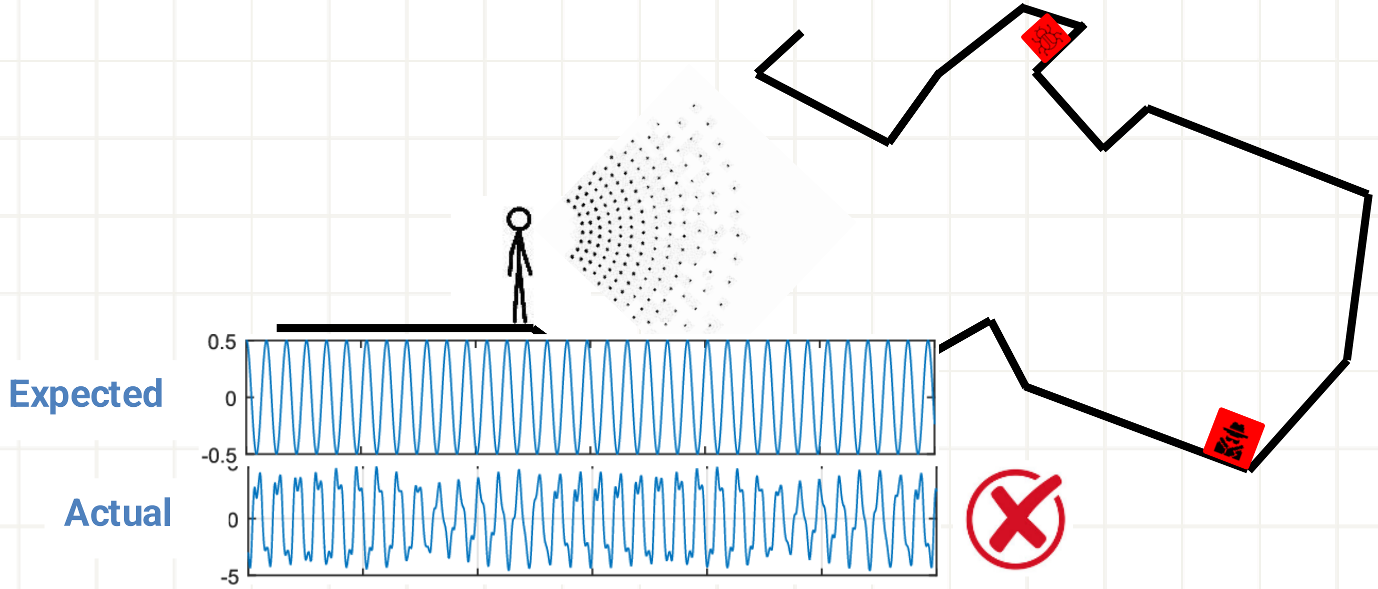
Started with all and filtered down

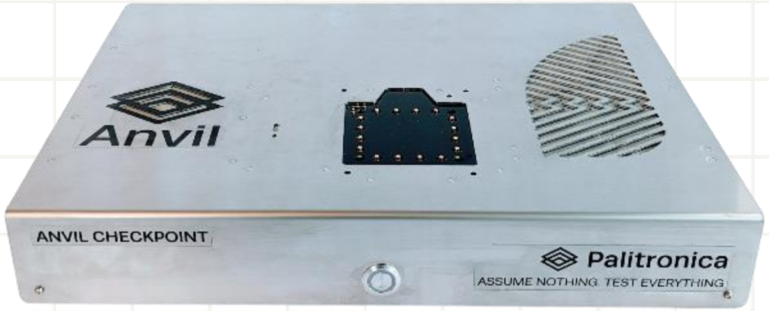
- **What is left are side-channel-based methods**
  - Radiated Electromagnetic (EM) Emissions
  - RF Domain Analysis
  - Power consumption, temperature, acoustics, etc

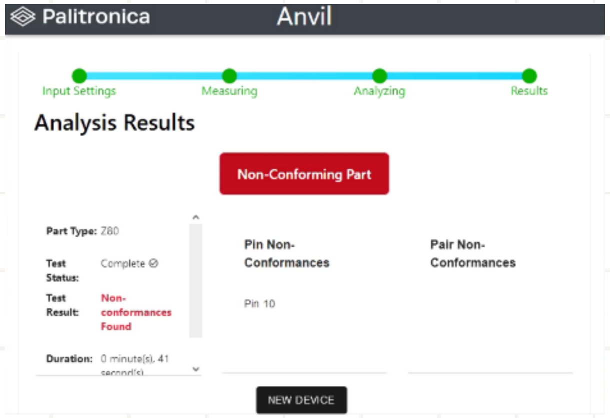
Detection Based on RF Reflectometry



Echo Response Signal







Analysis Results

Non-Conforming Part

Part Type: Z80

Test Status: Complete

Test Result: Non-conformances Found

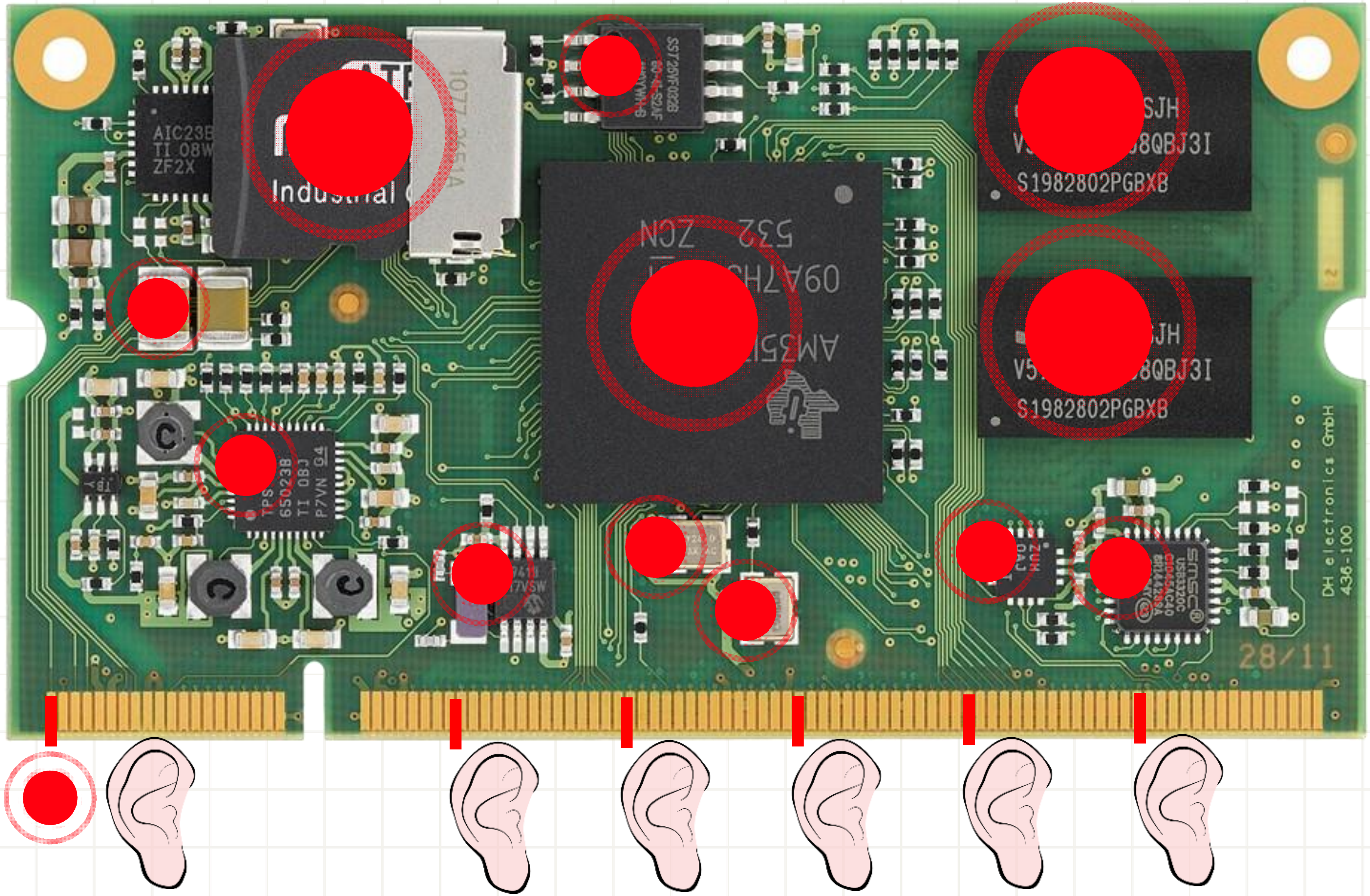
Duration: 0 minute(s), 41 second(s)

Pin Non-Conformances

Pin 10

Pair Non-Conformances

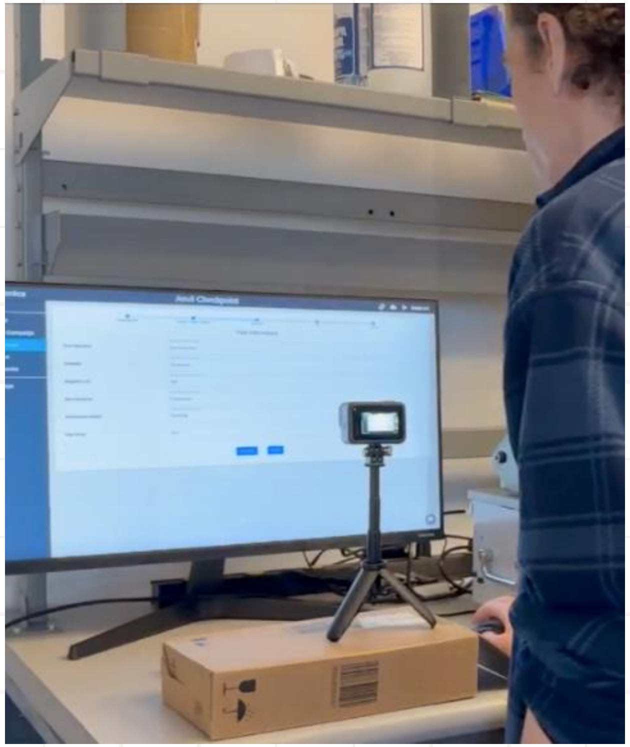
Visualization



A Simple Incoming Inspection

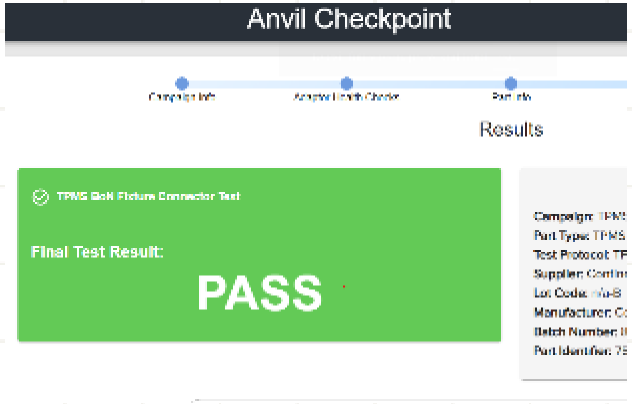
1.

Plug in the part



2.

Push a button



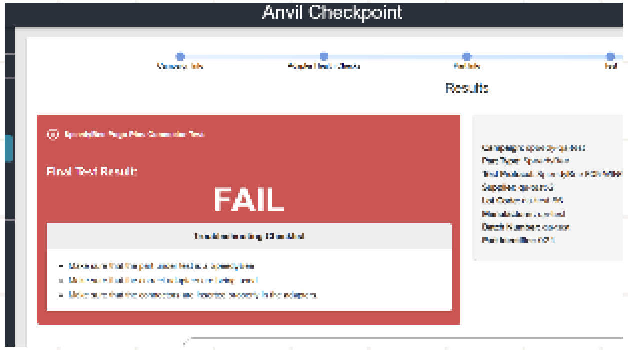
Results

TPMS BoN Fixture Connector Test

Final Test Result:

PASS

Campaign: TPMS
Part Type: TPMS
Test Protocol: TP
Supplier: Contin
Lot Code: n/a-B
Manufacturer: C
Batch Number: I
Part Identifier: 75



Results

[illegible] Connector Test

Final Test Result:

FAIL

Troubleshooting Checklist

- Make sure that the part under test is a [illegible]
- Make sure that [illegible]
- Make sure that the connectors are inserted securely in the adapters.

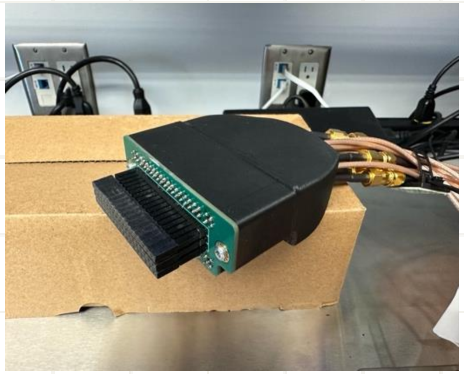
Campaign: [illegible]
Part Type: [illegible]
Test Protocol: [illegible]
Supplier: [illegible]
Lot Code: [illegible]
Manufacturer: [illegible]
Batch Number: [illegible]
Part Identifier: [illegible]

3.

Get a PASS or FAIL

Example: Telematics Control Unit

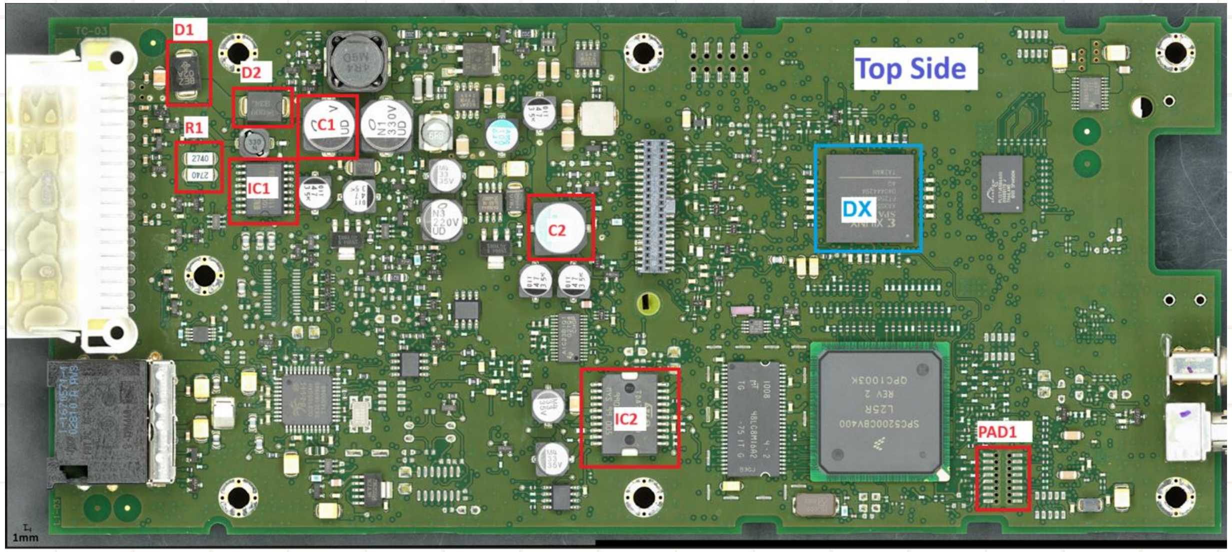
>60 TCUs
Various sources

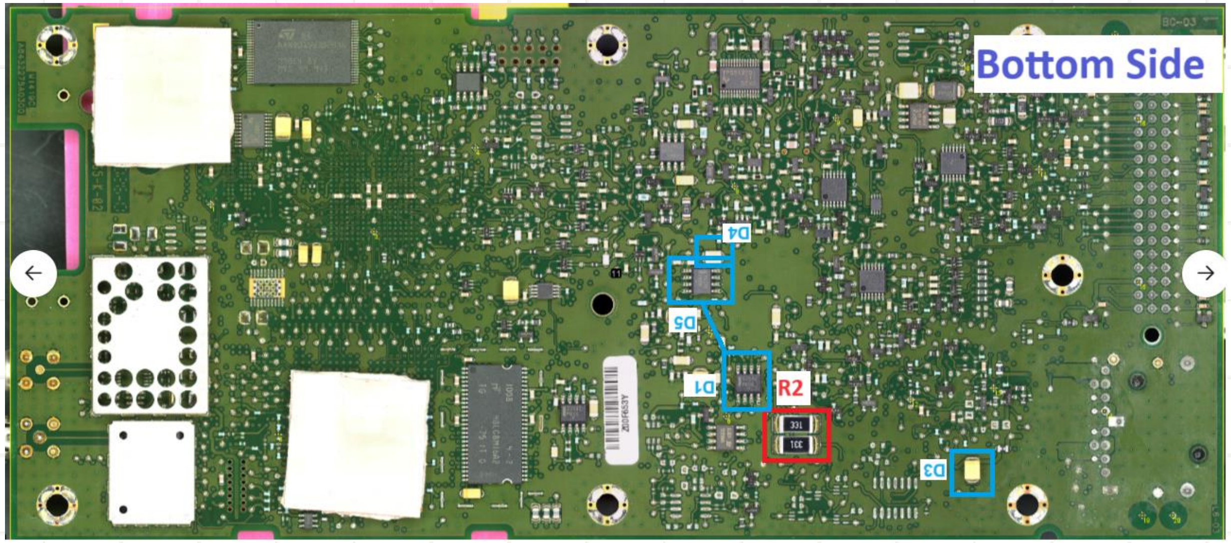


Tested through connector and BoN

Identified:

- Short
- Removal
- Swap
- Age/recycle
- Refurbished





STEPPING STONES TO
ZERO TRUST SUPPLY CHAIN

Relevant Standards

- Cybersecurity
  - NIST SP 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
  - NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations (especially the SR portion)
  - Other sectors have specific ones (defense, energy, etc.)

- Management and Testing Compliance
  - AS5553D Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition
  - AS6171A Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts
  - EIA933 Requirements for a COTS Assembly Management Plan
  - …

Assemblies are the next frontier (e.g., AS6171A/23 Assemblies, AS9970 COTS)

Cybersecurity Supply Chain Risk Management

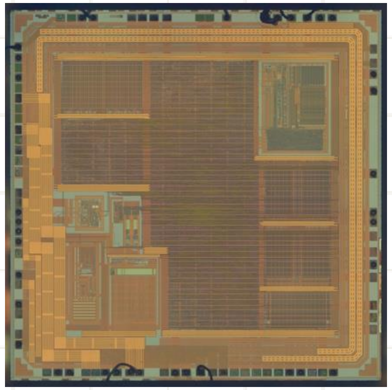
- **Strategic decisions:** risk profile, risk appetite, risk tolerance, ownership
- **Fact finding:** identify suppliers, criticality, prioritization
- **Governance structures:** risk management council
- **Documents:** Strategy, plan, policy, mission, ...
- **Awareness:** Training, gap analysis, training, …

Are you C-SCRM ready?

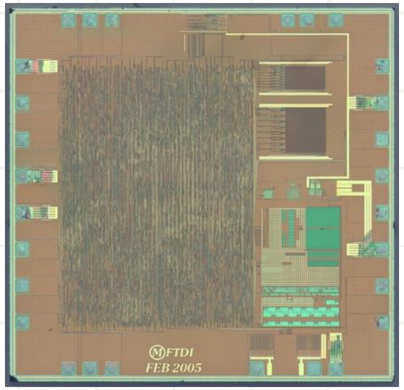
Supply Chain Cyber Tabletop Exercise

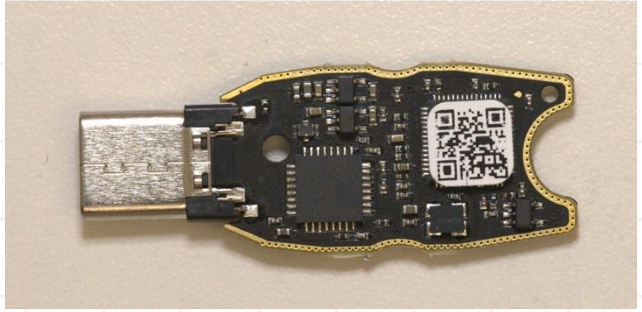
- Done at the VP & executive level
- Simulate 4 supply chain incidents (fraud, attacks, etc.)
- Learn about risk mitigation
- Duration: 3h + policy review
- Workflow:
  - Hold the TTX
  - Address findings
  - Repeat TTX

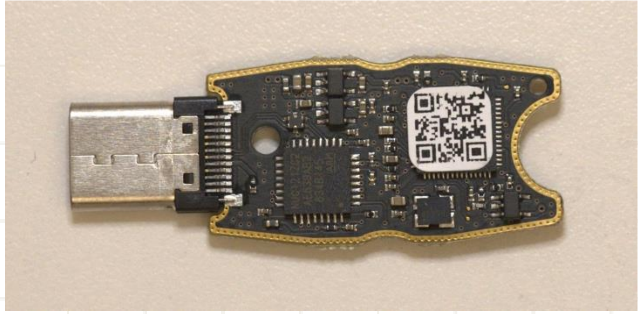
Conclusions



- Risk in the supply chain is often overlooked (especially fraud)
- New technology for incoming inspection is becoming available
  (blackbox, unpowered, non-destructive)
- Prepare your organization for new requirements and improve your posture







Q&A

UNIVERSITY OF WATERLOO

Contact info:

Sebastian Fischmeister

sfischme@uwaterloo.ca

Dept. of Electrical and Computer Eng.
University of Waterloo
200 University Ave West
Waterloo, ON N2L 3G1