irdeto

Building a Secure Future.™

Deploying Cybersecurity in Current and Future Vehicles

Return of Experience Sessions

Bevan Watkiss

Manager of Security Assurance and Integrations – Connected Transportation

Chair of GENIVI Security Group

bevan.watkiss@irdeto.com

Trends & Forces

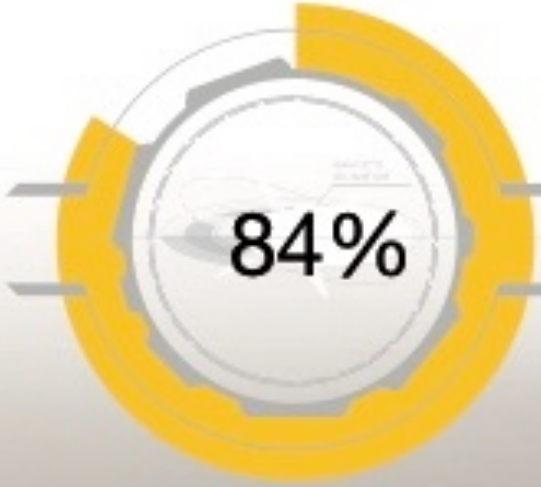
Automation

Mobility

Electrification

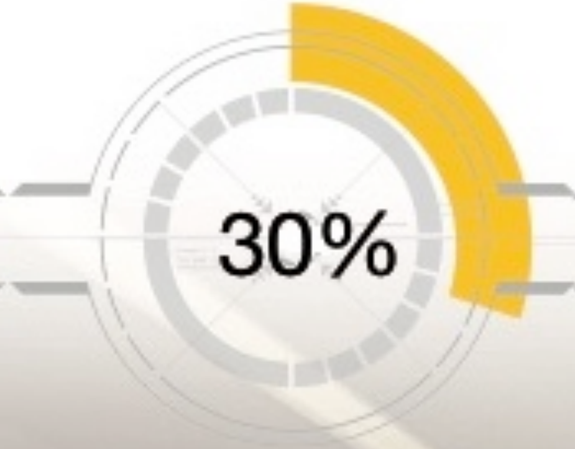
Connectivity

Security



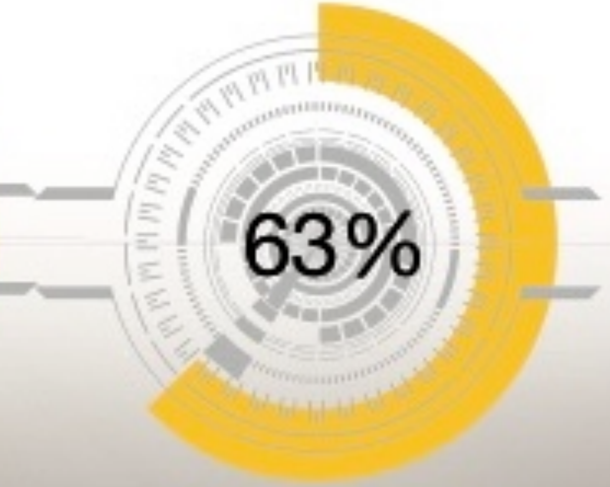
84%

have concerns that cybersecurity practices are not keeping pace with evolving technologies



30%

do not have an established product cybersecurity program or team



63%

test less than half of hardware, software, and other technologies for vulnerabilities

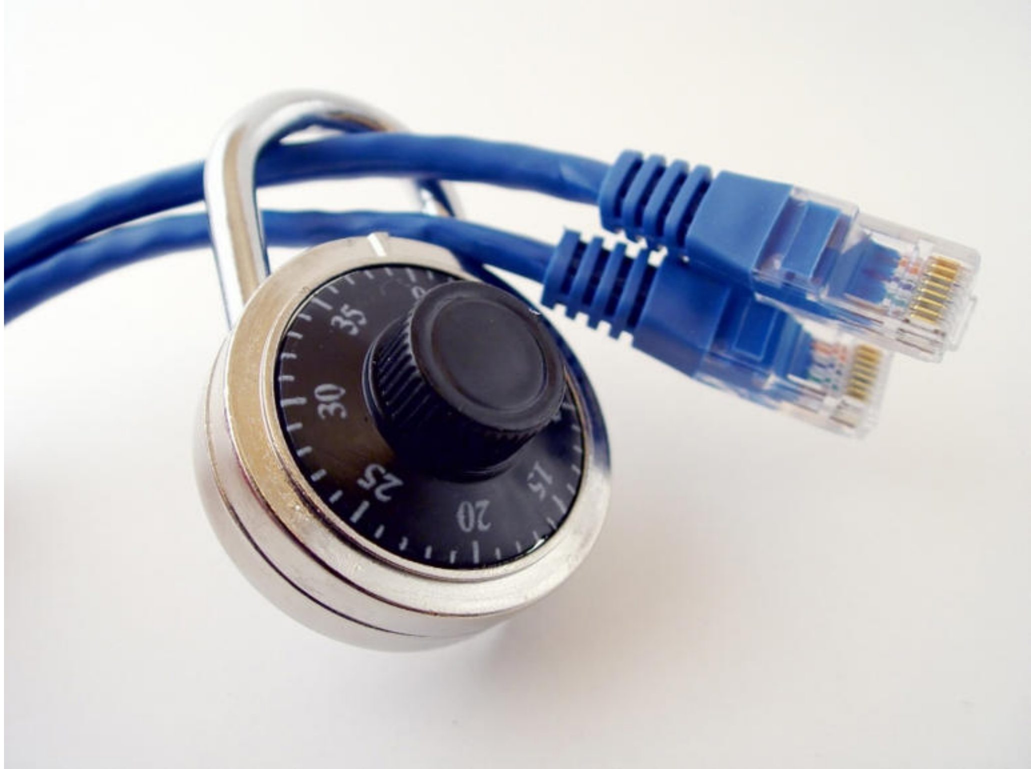
Ponemon INSTITUTE

Single Points of Failure are a Weakness

CAUTION!
Unintended
Consequences
Ahead

UNIT TESTS PASSING
NO INTEGRATION TESTS
imgflip.com

Bolt-On Security has the Same Issues

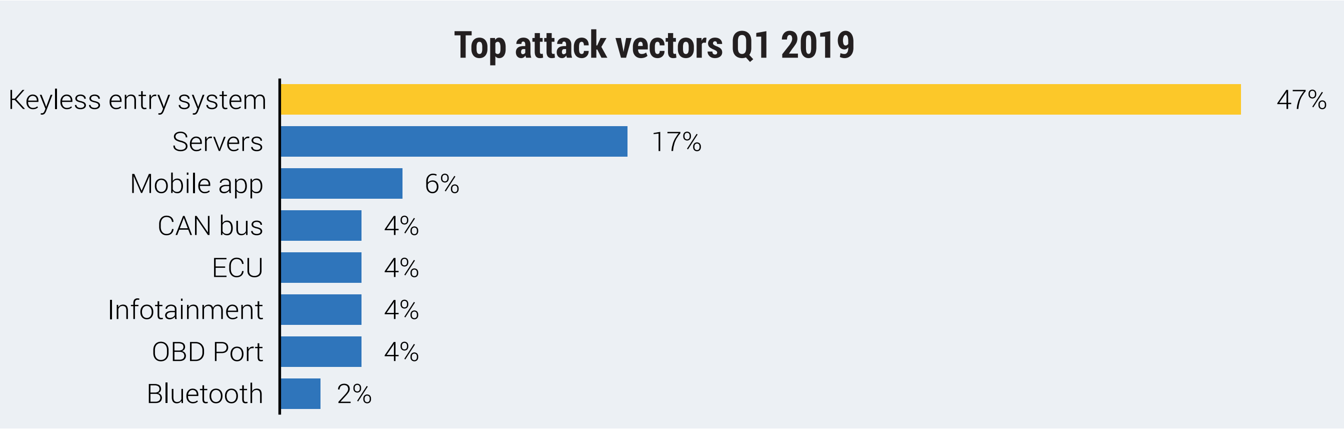


Think like a Hacker

- 2015 - Jeep Hack
- 2016 - Key Fob Hack on 90% of VWs
- 2017 - 150 Jeep Wranglers stolen in San Diego
- 2017 - 11 Teslas Stolen in Netherlands
- 2018 - Keyless entry car theft triples in UK
- 2018 - Keen Labs BMW Hack
- 2019 – BMW stolen in 20 secs in UK

THE TOTAL NUMBER OF INCIDENTS IS ON A SHARP RISE

Q1 2019 sees rapid growth of automotive cyber incidents



How do we Respond?

- Good security starts with good security architecture and design.
- High availability and high confidence with the assurance that any possible attacks are anticipated
- The system needs to self-defend. Self-repair, self-healing, and fault-tolerant systems can deal with the immediate threat of malicious faults; while telemetry monitoring, policy updates, and system updates (OTA) can address recovery of unanticipated compromises, reducing even the remote possibility of widespread problems in a fleet.

Current Guidelines and Recommendations may be Insufficient

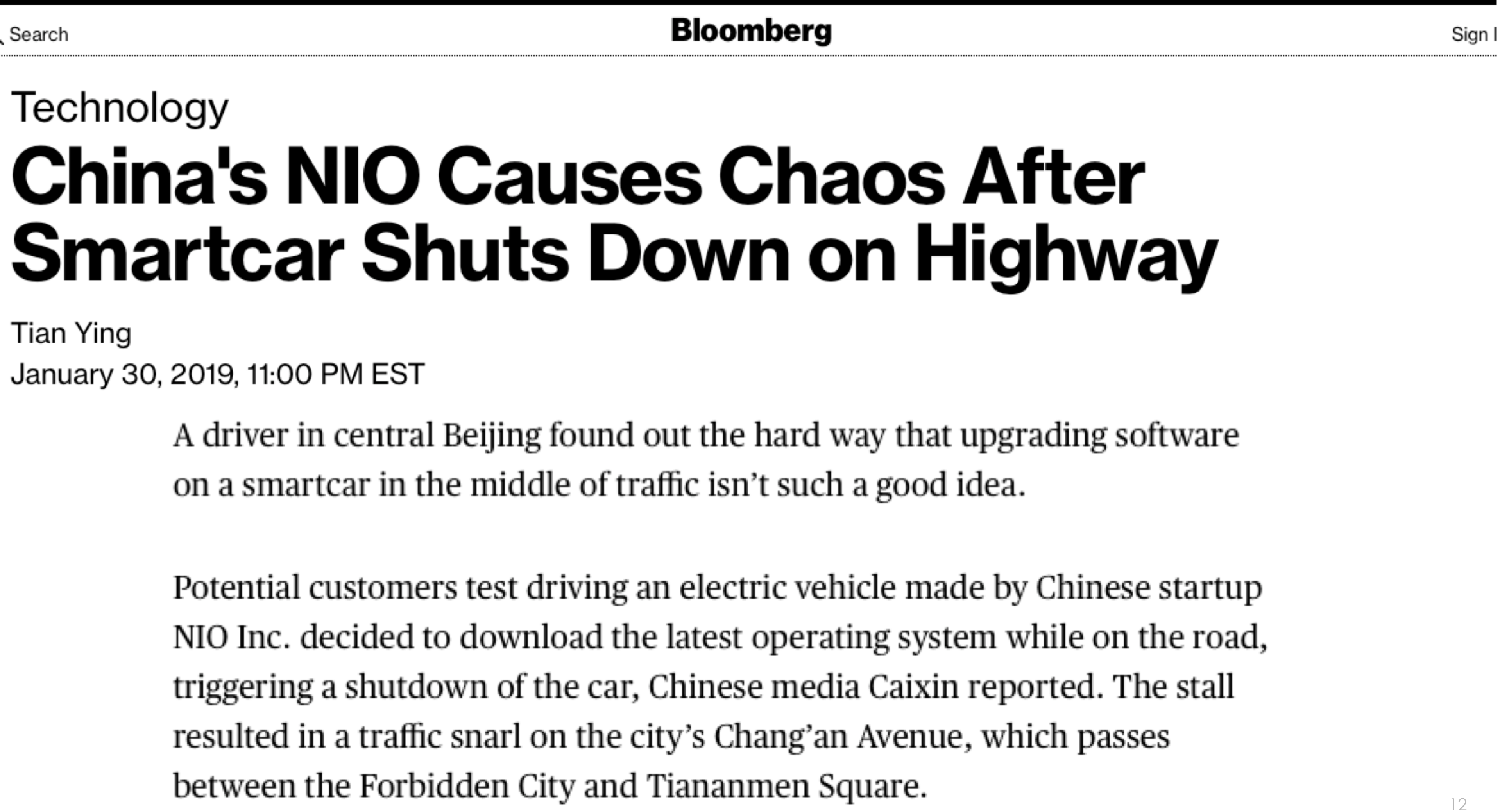
- The National Highway Traffic Safety Administration (NHTSA) report on Cybersecurity Best Practices for Modern Vehicles recommends, “Identify, Protect, Detect, Respond, and Recover”.
- Well, when you’re driving down the highway, it could be a long time between Identify and Recover, if is all happening in the cloud (“Please wait while the countermeasure to your cybersecurity threat downloads”)

Cybersecurity Best Practices for Modern Vehicles

U.S. Department of Transportation

National Highway Traffic Safety Administration

NHTSA



Technology

China's NIO Causes Chaos After Smartcar Shuts Down on Highway

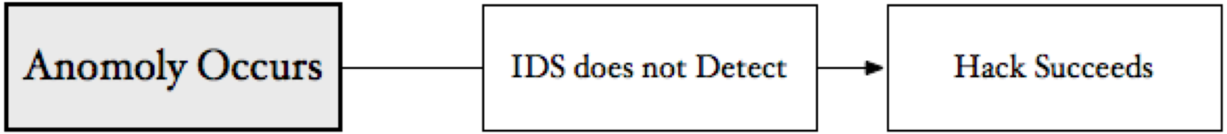
Tian Ying

January 30, 2019, 11:00 PM EST

A driver in central Beijing found out the hard way that upgrading software on a smartcar in the middle of traffic isn’t such a good idea.

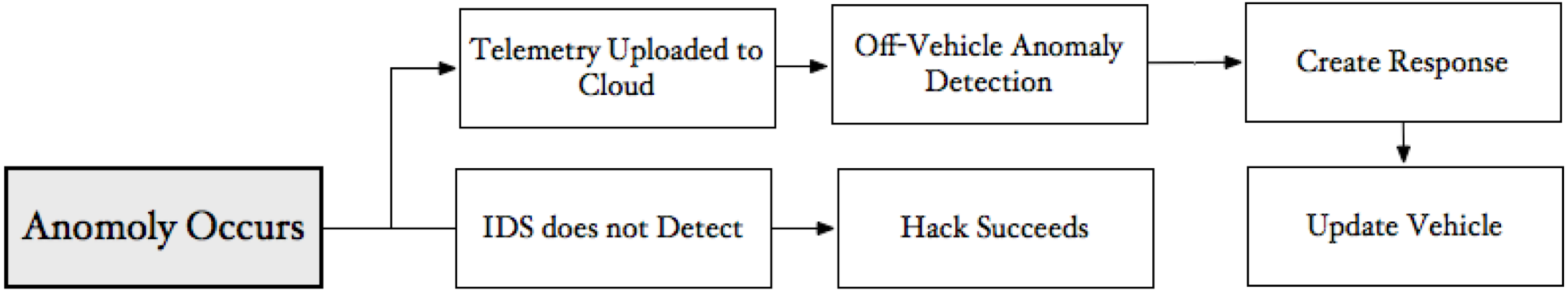
Potential customers test driving an electric vehicle made by Chinese startup NIO Inc. decided to download the latest operating system while on the road, triggering a shutdown of the car, Chinese media Caixin reported. The stall resulted in a traffic snarl on the city’s Chang’an Avenue, which passes between the Forbidden City and Tiananmen Square.

Off-Vehicle Process is Important



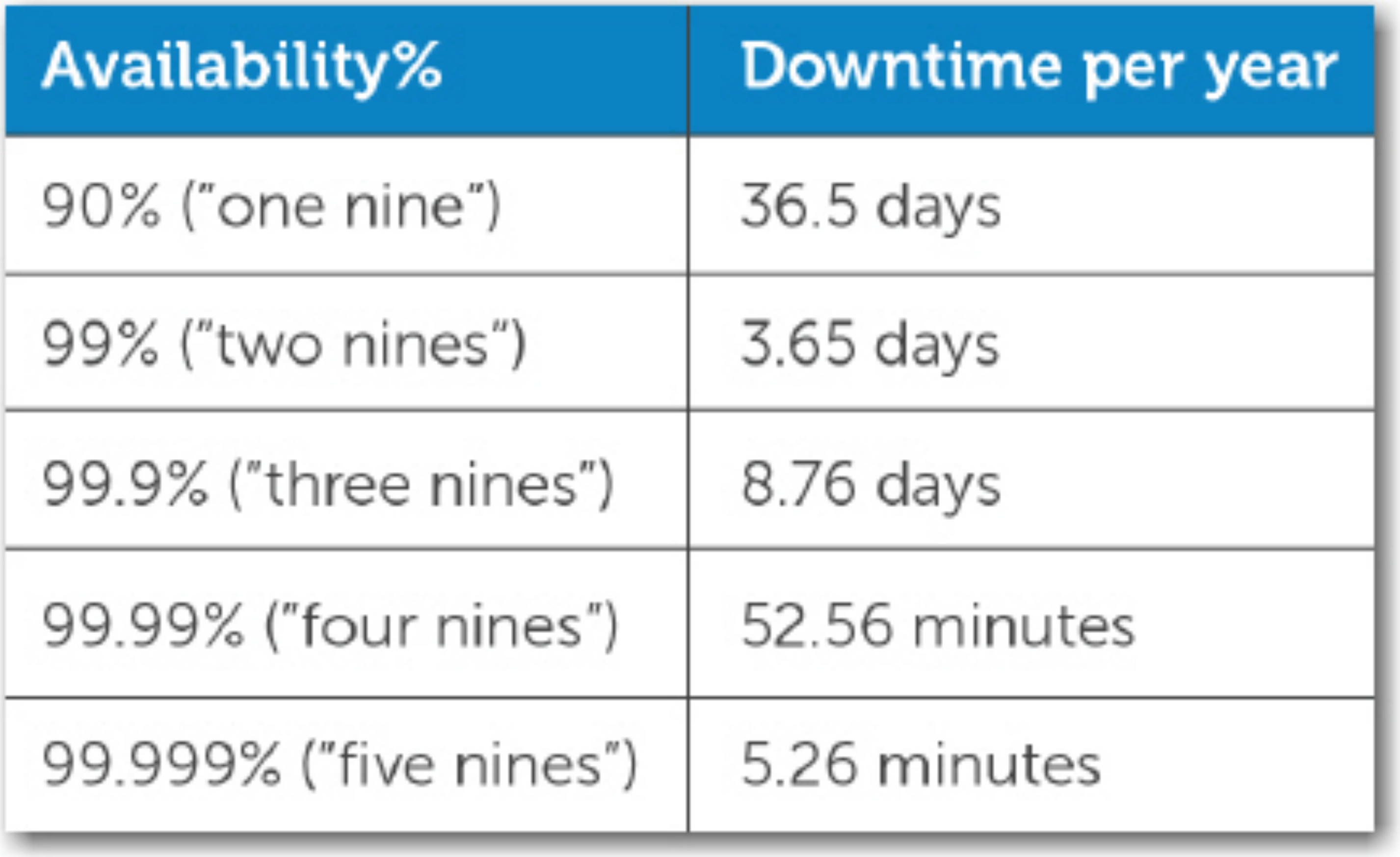
Off-Vehicle Process is Important

But Not Sufficient



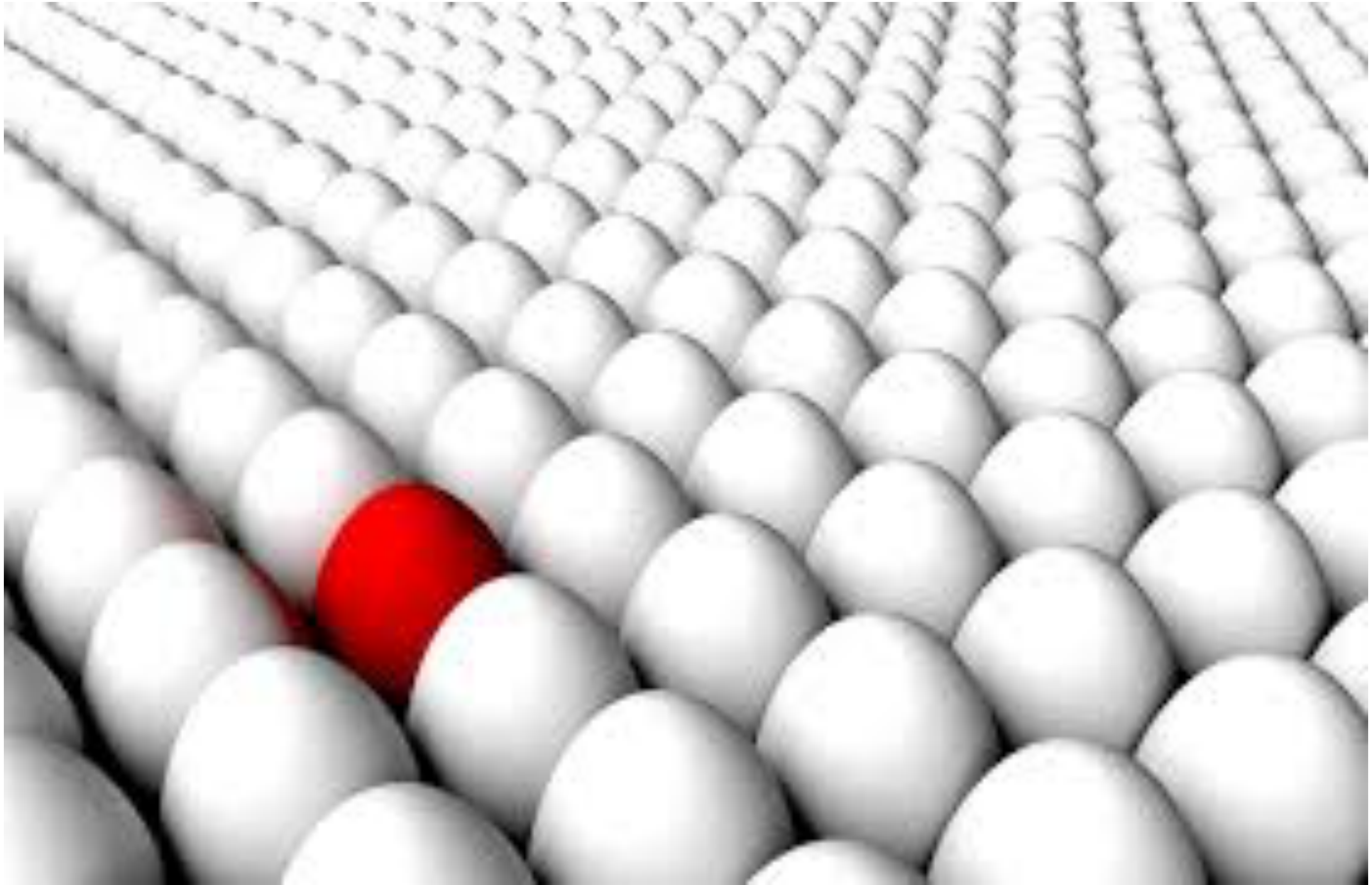
High Availability for Automotive Cybersecurity

High Availability for Automotive Cybersecurity

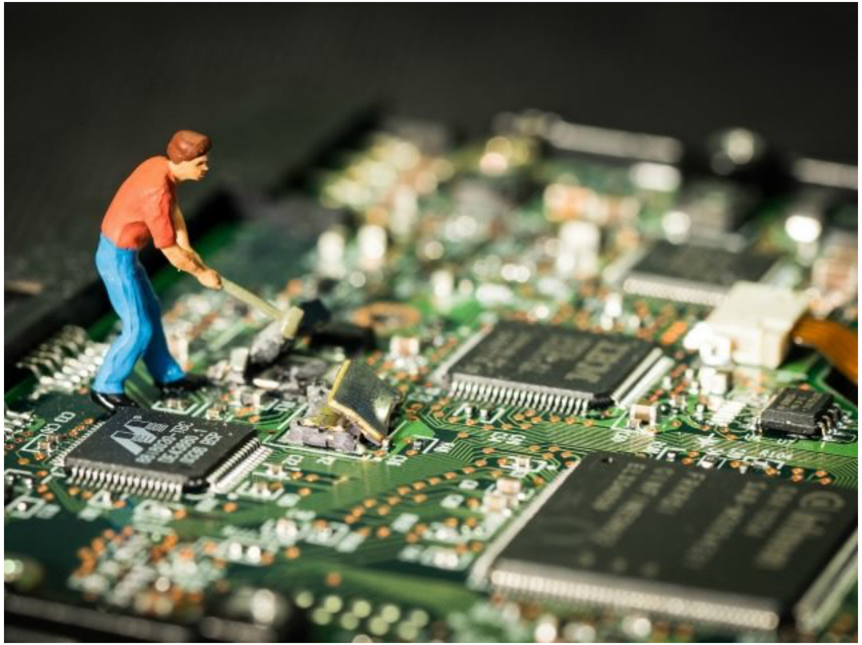


Availability%	Downtime per year
90% ("one nine")	36.5 days
99% ("two nines")	3.65 days
99.9% ("three nines")	8.76 days
99.99% ("four nines")	52.56 minutes
99.999% ("five nines")	5.26 minutes

System Integrity addresses unanticipated operating conditions



Cybersecurity guards against Intentional faults and malicious actions



Attackers take in the Entire Landscape

ATTACK SURFACE

- The Device
- (Receives the most focus)

- Smartphone app
- (Everyone has one)

- Communications
- (The bit that makes it connected)

- The things the device connects to

- Cloud
- (via the Internet)

PHASES OF AN ATTACK

Investigation

Leverage a weakness

Rinse and repeat

Create an attack

Scale the attack

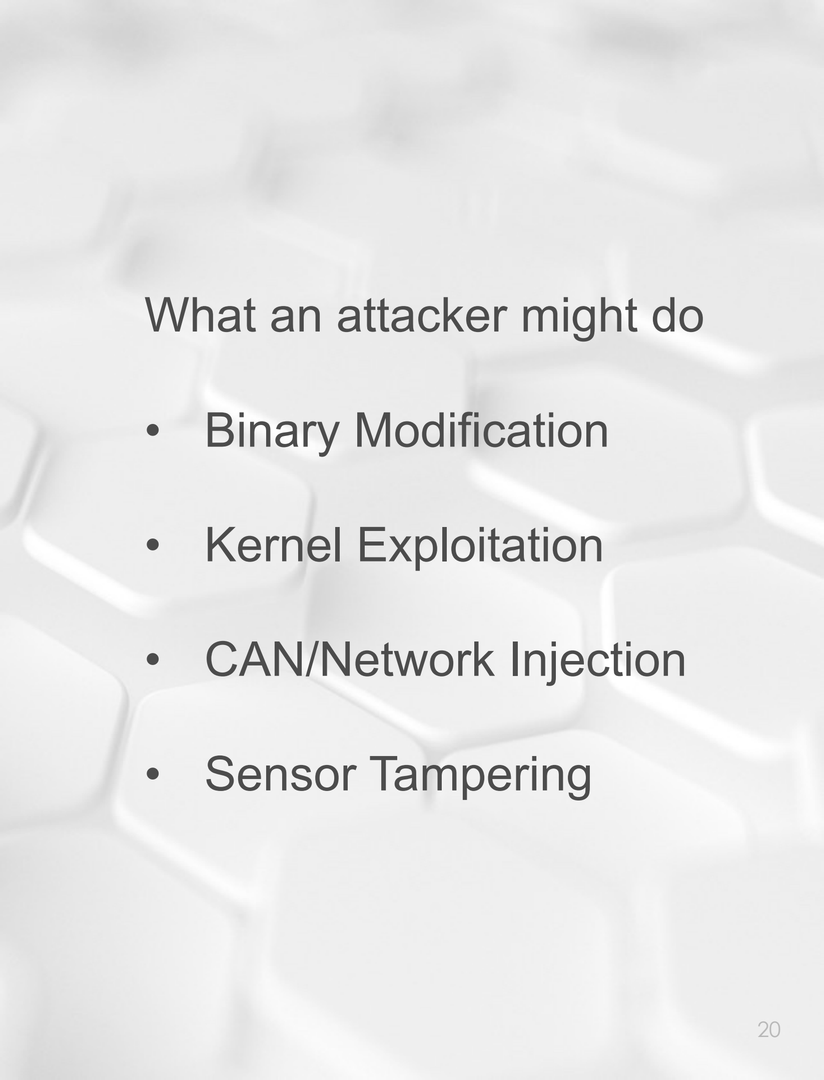
$$$$

Security by Design

Holistic coverage of the system from the ground up

High Availability

Malicious Fault - Tolerance



What an attacker might do

- Binary Modification
- Kernel Exploitation
- CAN/Network Injection
- Sensor Tampering

Self-Healing Systems Prepare for Attack

Binary-Level Integrity Verification

- Integrity Verification is the cryptographic means to identify if a binary has been tampered with by means of signing the payload at build time and validating at runtime.

- This should be done for the validation of firmware and image updates, but can also be used to validate individual programs.

- Without Integrity Verification there is no way to know that your system has been tampered with

Binary-Level Integrity Verification

- Like an IDS, Integrity Verification is only a detection, but it can trigger programmed responses that provide active mitigation.
- Failures on firmware load can halt the boot, or load the last known-good image
- Failures on OTA Update Images in systems that do A/B upgrades can invalidate the update, and request a new one while maintaining the known good OS
- Detection of failures does not have to do full system updates. The verification and response can be segmented into image sections, or even files.

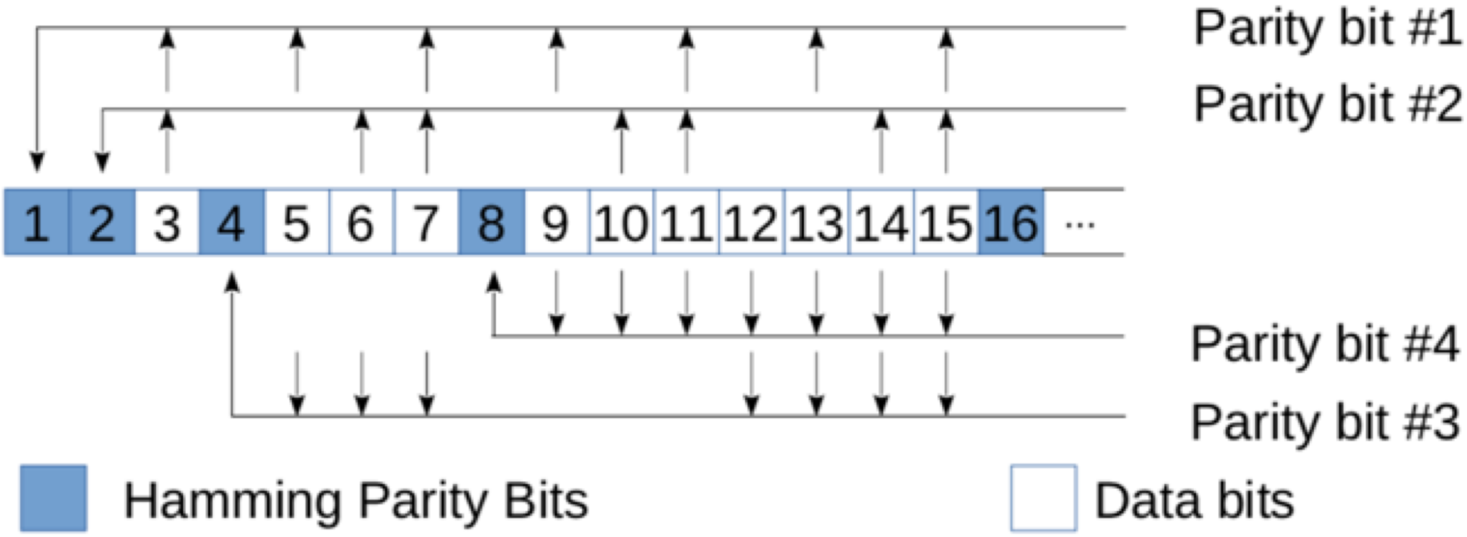
Binary-Level Self Repair

- Error-Correcting Codes (ECC) have existed since the 1950s
  - Parity Bits, CRCs, and Hamming Codes

- Error-Correcting Hamming Codes were developed to correct punched paper tape read failures

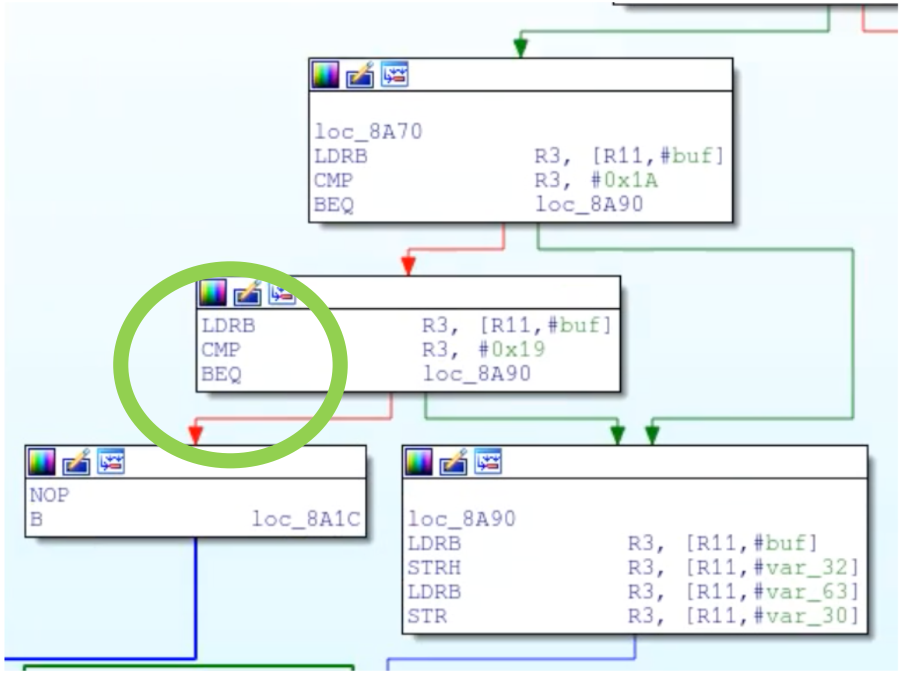
“Damn it, if the machine can detect an error, why can’t it locate the position of the error and correct it”

Richard Hamming

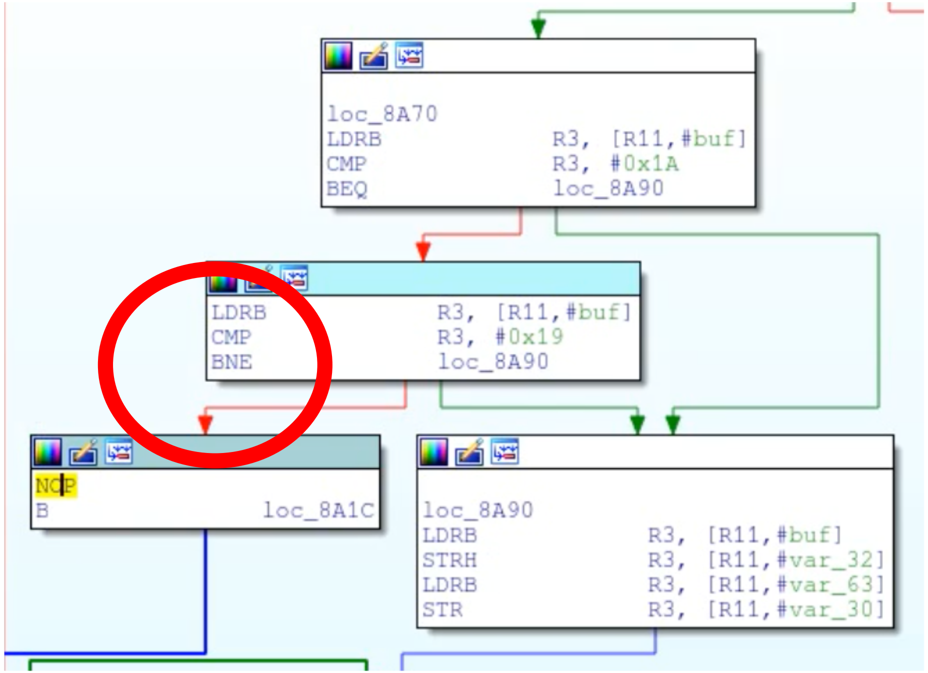

Parity bit #1
Parity bit #2
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
...
Parity bit #4
Parity bit #3
Hamming Parity Bits
Data bits

- If we consider the data stream turned 90 degrees and replicated 7 times, this concept can be applied to data bytes within a program, able to repair 1- and 2-byte errors.
- Similarly, the idea can be expanded to multi-byte spans. The overhead for such a scheme can range between 4% and 30%.

Simple Branch Jam

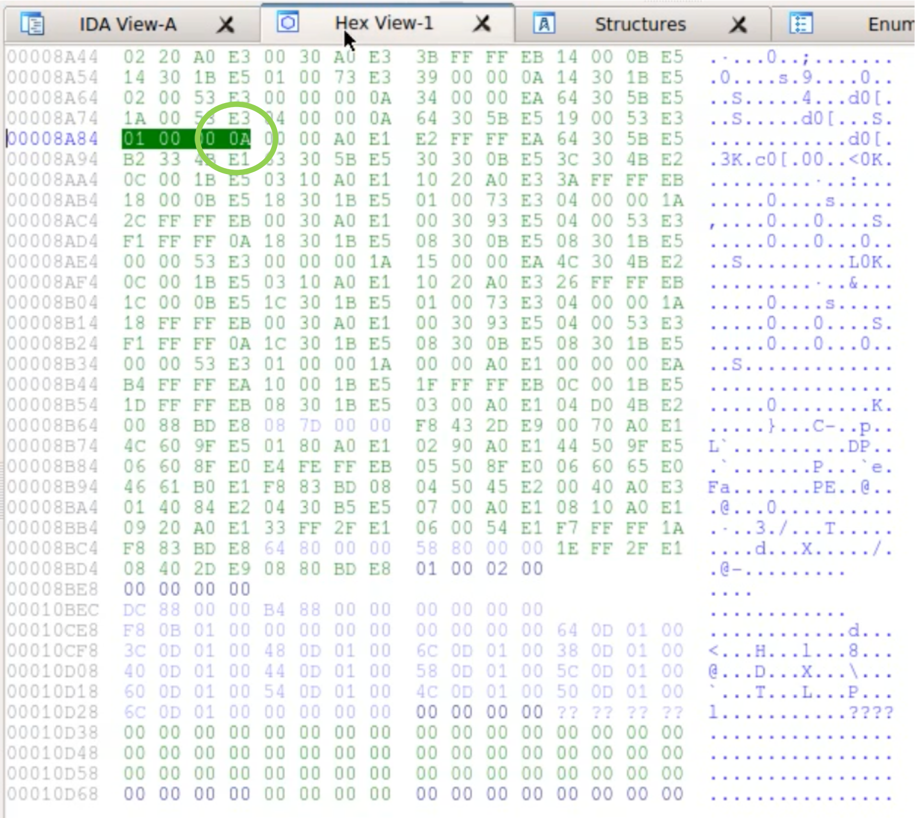


```
loc_8A70
LDRB                R3, [R11,#buf]
CMP                 R3, #0x1A
BEQ                 loc_8A90

LDRB                R3, [R11,#buf]
CMP                 R3, #0x19
BEQ                 loc_8A90

NOP
B               loc_8A1C

loc_8A90
LDRB                R3, [R11,#buf]
STRH                R3, [R11,#var_32]
LDRB                R3, [R11,#var_63]
STR                 R3, [R11,#var_30]
```

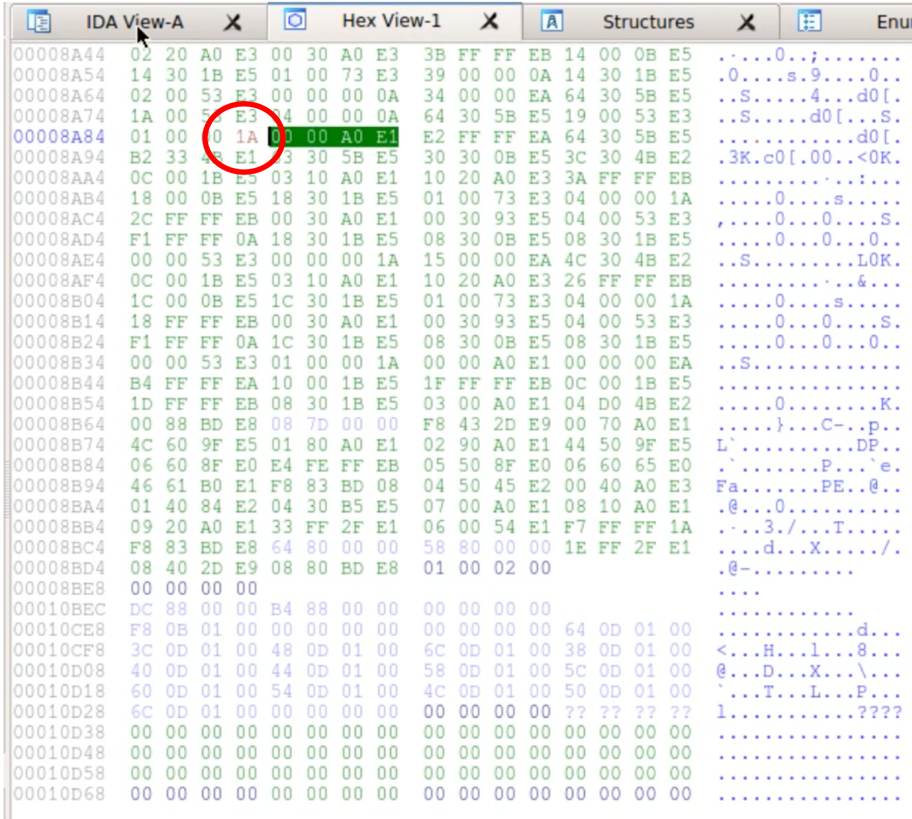


```
loc_8A70
LDRB                R3, [R11,#buf]
CMP                 R3, #0x1A
BEQ                 loc_8A90

LDRB                R3, [R11,#buf]
CMP                 R3, #0x19
BNE                 loc_8A90

NOP
B               loc_8A1C

loc_8A90
LDRB                R3, [R11,#buf]
STRH                R3, [R11,#var_32]
LDRB                R3, [R11,#var_63]
STR                 R3, [R11,#var_30]
```

Simple Branch Jam



```
00008A44  02 20 A0 E3 00 30 A0 E3  3B FF FF EB 14 00 0B E5  . ...0..;.......
00008A54  14 30 1B E5 01 00 73 E3  39 00 00 0A 14 30 1B E5  .0....s.9....0..
00008A64  02 00 53 E3 00 00 00 0A  34 00 00 EA 64 30 5B E5  ..S.....4...d0[.
00008A74  1A 00 53 E3 04 00 00 0A  64 30 5B E5 19 00 53 E3  ..S.....d0[...S.
00008A84  01 00 00 0A 00 00 A0 E1  E2 FF FF EA 64 30 5B E5  ............d0[.
00008A94  B2 33 4B E1 63 30 5B E5  30 30 0B E5 3C 30 4B E2  .3K.c0[.00..<0K.
00008AA4  0C 00 1B E5 03 10 A0 E1  10 20 A0 E3 3A FF FF EB  ......... ..:...
00008AB4  18 00 0B E5 18 30 1B E5  01 00 73 E3 04 00 00 1A  .....0....s.....
00008AC4  2C FF FF EB 00 30 A0 E1  00 30 93 E5 04 00 53 E3  ,....0...0....S.
00008AD4  F1 FF FF 0A 18 30 1B E5  08 30 0B E5 08 30 1B E5  .....0...0...0..
00008AE4  00 00 53 E3 00 00 00 1A  15 00 00 EA 4C 30 4B E2  ..S.........L0K.
00008AF4  0C 00 1B E5 03 10 A0 E1  10 20 A0 E3 26 FF FF EB  ......... ..&...
00008B04  1C 00 0B E5 1C 30 1B E5  01 00 73 E3 04 00 00 1A  .....0....s.....
00008B14  18 FF FF EB 00 30 A0 E1  00 30 93 E5 04 00 53 E3  .....0...0....S.
00008B24  F1 FF FF 0A 1C 30 1B E5  08 30 0B E5 08 30 1B E5  .....0...0...0..
00008B34  00 00 53 E3 01 00 00 1A  00 00 A0 E1 00 00 00 EA  ..S.............
00008B44  B4 FF FF EA 10 00 1B E5  1F FF FF EB 0C 00 1B E5  ................
00008B54  1D FF FF EB 08 30 1B E5  03 00 A0 E1 04 D0 4B E2  .....0........K.
00008B64  00 88 BD E8 08 7D 00 00  F8 43 2D E9 00 70 A0 E1  .....}...C-..p..
00008B74  4C 60 9F E5 01 80 A0 E1  02 90 A0 E1 44 50 9F E5  L`..........DP..
00008B84  06 60 8F E0 E4 FE FF EB  05 50 8F E0 06 60 65 E0  .`.......P...`e.
00008B94  46 61 B0 E1 F8 83 BD 08  04 50 45 E2 00 40 A0 E3  Fa.......PE..@..
00008BA4  01 40 84 E2 04 30 B5 E5  07 00 A0 E1 08 10 A0 E1  .@...0..........
00008BB4  09 20 A0 E1 33 FF 2F E1  06 00 54 E1 F7 FF FF 1A  . ..3./...T.....
00008BC4  F8 83 BD E8 64 80 00 00  58 80 00 00 1E FF 2F E1  ....d...X...../.
00008BD4  08 40 2D E9 08 80 BD E8  01 00 02 00              .@-.........
00008BE8  00 00 00 00                                       ....
00010BEC  DC 88 00 00 B4 88 00 00  00 00 00 00              ............
00010CE8  F8 0B 01 00 00 00 00 00  00 00 00 00 64 0D 01 00  ............d...
00010CF8  3C 0D 01 00 48 0D 01 00  6C 0D 01 00 38 0D 01 00  <...H...l...8...
00010D08  40 0D 01 00 44 0D 01 00  58 0D 01 00 5C 0D 01 00  @...D...X...\...
00010D18  60 0D 01 00 54 0D 01 00  4C 0D 01 00 50 0D 01 00  `...T...L...P...
00010D28  6C 0D 01 00 00 00 00 00  00 00 00 00 ?? ?? ?? ??  l...........????
00010D38  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00010D48  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00010D58  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00010D68  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```



```
00008A44  02 20 A0 E3 00 30 A0 E3  3B FF FF EB 14 00 0B E5  . ...0..;.......
00008A54  14 30 1B E5 01 00 73 E3  39 00 00 0A 14 30 1B E5  .0....s.9....0..
00008A64  02 00 53 E3 00 00 00 0A  34 00 00 EA 64 30 5B E5  ..S.....4...d0[.
00008A74  1A 00 53 E3 04 00 00 0A  64 30 5B E5 19 00 53 E3  ..S.....d0[...S.
00008A84  01 00 00 1A 00 00 A0 E1  E2 FF FF EA 64 30 5B E5  ............d0[.
00008A94  B2 33 4B E1 63 30 5B E5  30 30 0B E5 3C 30 4B E2  .3K.c0[.00..<0K.
00008AA4  0C 00 1B E5 03 10 A0 E1  10 20 A0 E3 3A FF FF EB  ......... ..:...
00008AB4  18 00 0B E5 18 30 1B E5  01 00 73 E3 04 00 00 1A  .....0....s.....
00008AC4  2C FF FF EB 00 30 A0 E1  00 30 93 E5 04 00 53 E3  ,....0...0....S.
00008AD4  F1 FF FF 0A 18 30 1B E5  08 30 0B E5 08 30 1B E5  .....0...0...0..
00008AE4  00 00 53 E3 00 00 00 1A  15 00 00 EA 4C 30 4B E2  ..S.........L0K.
00008AF4  0C 00 1B E5 03 10 A0 E1  10 20 A0 E3 26 FF FF EB  ......... ..&...
00008B04  1C 00 0B E5 1C 30 1B E5  01 00 73 E3 04 00 00 1A  .....0....s.....
00008B14  18 FF FF EB 00 30 A0 E1  00 30 93 E5 04 00 53 E3  .....0...0....S.
00008B24  F1 FF FF 0A 1C 30 1B E5  08 30 0B E5 08 30 1B E5  .....0...0...0..
00008B34  00 00 53 E3 01 00 00 1A  00 00 A0 E1 00 00 00 EA  ..S.............
00008B44  B4 FF FF EA 10 00 1B E5  1F FF FF EB 0C 00 1B E5  ................
00008B54  1D FF FF EB 08 30 1B E5  03 00 A0 E1 04 D0 4B E2  .....0........K.
00008B64  00 88 BD E8 08 7D 00 00  F8 43 2D E9 00 70 A0 E1  .....}...C-..p..
00008B74  4C 60 9F E5 01 80 A0 E1  02 90 A0 E1 44 50 9F E5  L`..........DP..
00008B84  06 60 8F E0 E4 FE FF EB  05 50 8F E0 06 60 65 E0  .`.......P...`e.
00008B94  46 61 B0 E1 F8 83 BD 08  04 50 45 E2 00 40 A0 E3  Fa.......PE..@..
00008BA4  01 40 84 E2 04 30 B5 E5  07 00 A0 E1 08 10 A0 E1  .@...0..........
00008BB4  09 20 A0 E1 33 FF 2F E1  06 00 54 E1 F7 FF FF 1A  . ..3./...T.....
00008BC4  F8 83 BD E8 64 80 00 00  58 80 00 00 1E FF 2F E1  ....d...X...../.
00008BD4  08 40 2D E9 08 80 BD E8  01 00 02 00              .@-.........
00008BE8  00 00 00 00                                       ....
00010BEC  DC 88 00 00 B4 88 00 00  00 00 00 00              ............
00010CE8  F8 0B 01 00 00 00 00 00  00 00 00 00 64 0D 01 00  ............d...
00010CF8  3C 0D 01 00 48 0D 01 00  6C 0D 01 00 38 0D 01 00  <...H...l...8...
00010D08  40 0D 01 00 44 0D 01 00  58 0D 01 00 5C 0D 01 00  @...D...X...\...
00010D18  60 0D 01 00 54 0D 01 00  4C 0D 01 00 50 0D 01 00  `...T...L...P...
00010D28  6C 0D 01 00 00 00 00 00  00 00 00 00 ?? ?? ?? ??  l...........????
00010D38  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00010D48  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00010D58  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00010D68  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

Not-So Simple Branch Jam

When it repairs itself

Telemetry and Monitoring for Fleet-wide OTA

- Every security detection mechanism needs Telemetry
- Security Events need to be collected, aggregated and monitored externally.
- Monitor for indications that events have overwhelmed the in-vehicle defences
- OTA Security Update may be required regionally, or fleet-wide
  - Updates could be just to collect more data
- OTA Strategy is a complementary security aspect

Designing for Malicious Fault Tolerance

Designing for Malicious Fault Tolerance

Three things are needed to self-defend against an intrusion:

1. A way to detect the intrusion.

2. A local recovery mechanism when the problem is detected.

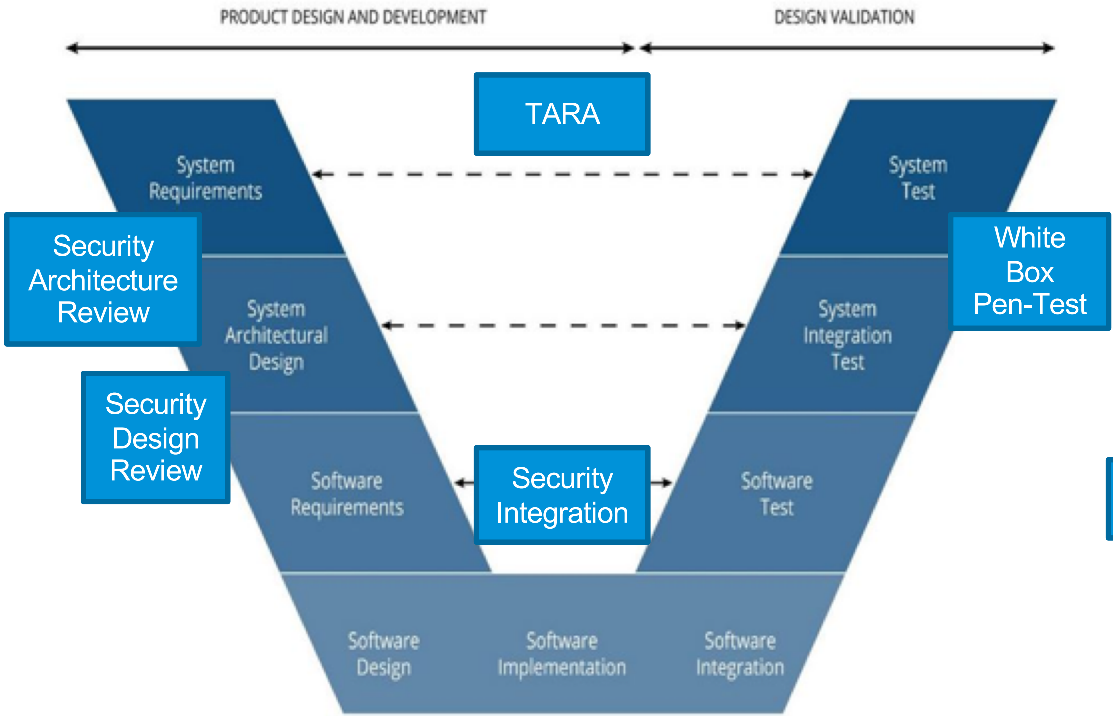
3. A fail-over mechanism that can be relied upon when a problem is detected and cannot be recovered.

Designing for Malicious Fault Tolerance

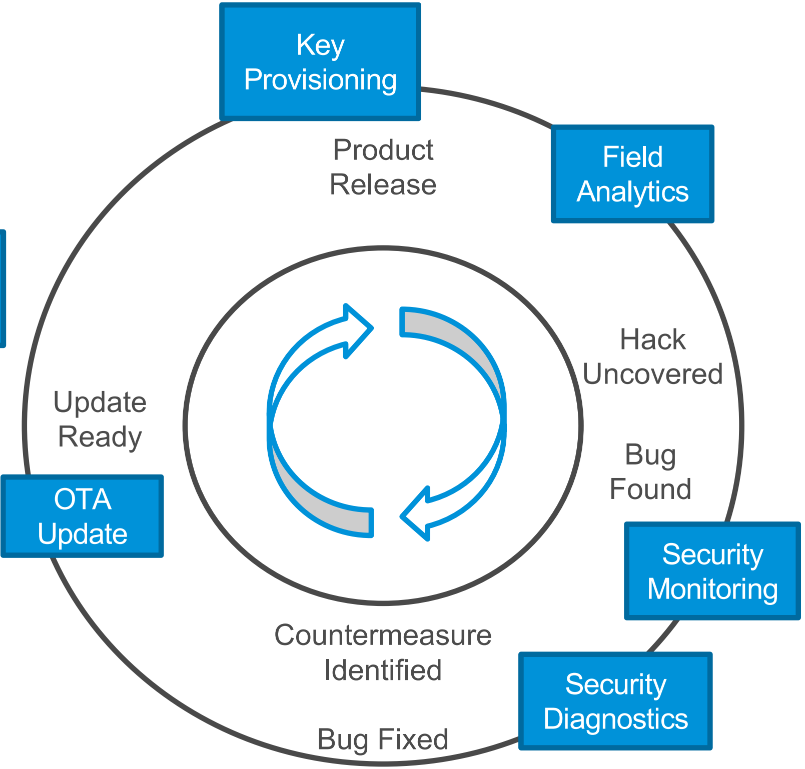
Beyond that, there are several additional considerations to make a robust, secure system:

- Multiple detection, local recovery, and fail-over mechanisms. (If one fails, the 2nd kicks in).
- Mechanisms placed at different levels of abstraction.
- An event logging, telemetry, and monitoring mechanism to track the occurrences of intrusion, local recovery, and fail-over in a set of systems.
- Security layers (defence-in-depth) to protect the detection, local recovery, fail-over, and logging mechanisms themselves.
- An incident response, disaster recovery, and remediation plan (e.g. monitoring & OTA updates).

Where you should think about Security

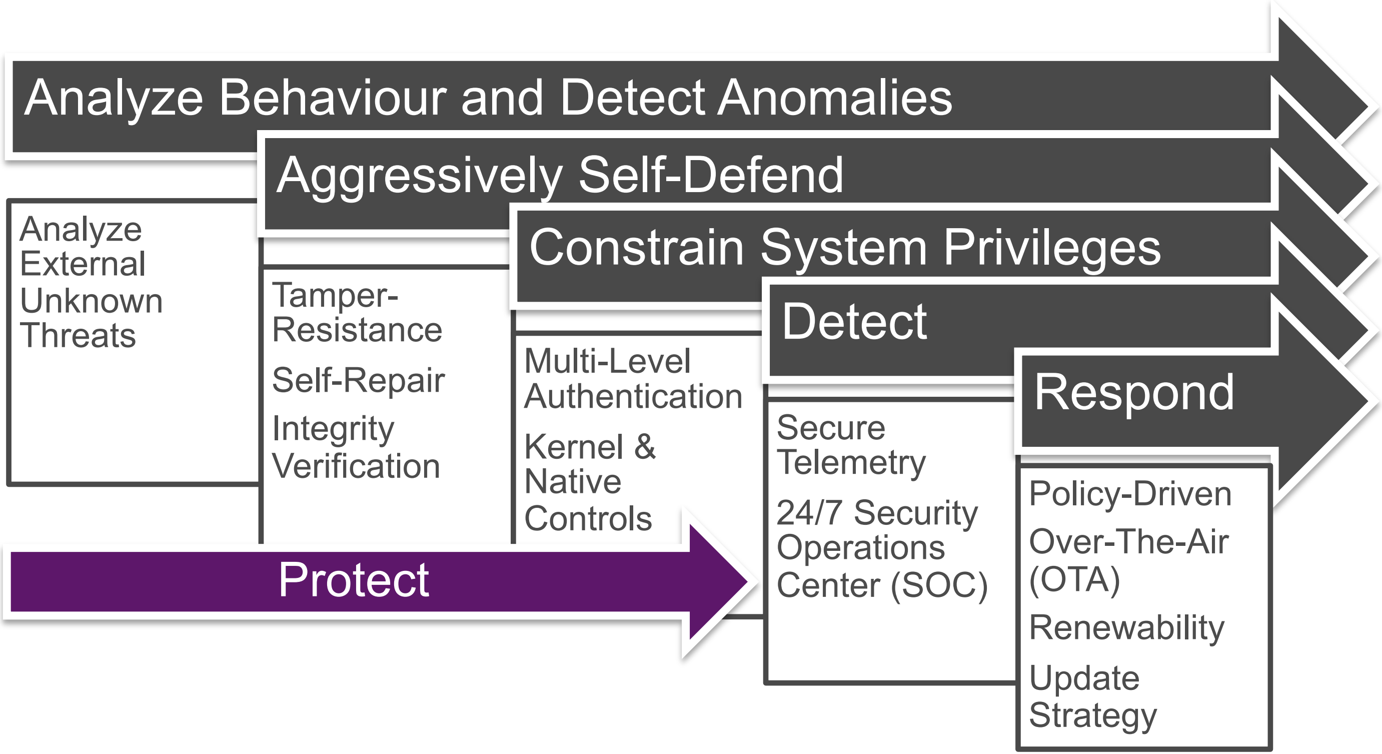


Product Development Lifecycle



Product Lifecycle

Security Tenants Moving Forward: Decoupling Protection Technologies



Analyze Behaviour and Detect Anomalies

Analyze External Unknown Threats

Aggressively Self-Defend

Tamper-Resistance

Self-Repair

Integrity Verification

Constrain System Privileges

Multi-Level Authentication

Kernel & Native Controls

Detect

Secure Telemetry

24/7 Security Operations Center (SOC)

Respond

Policy-Driven

Over-The-Air (OTA)

Renewability

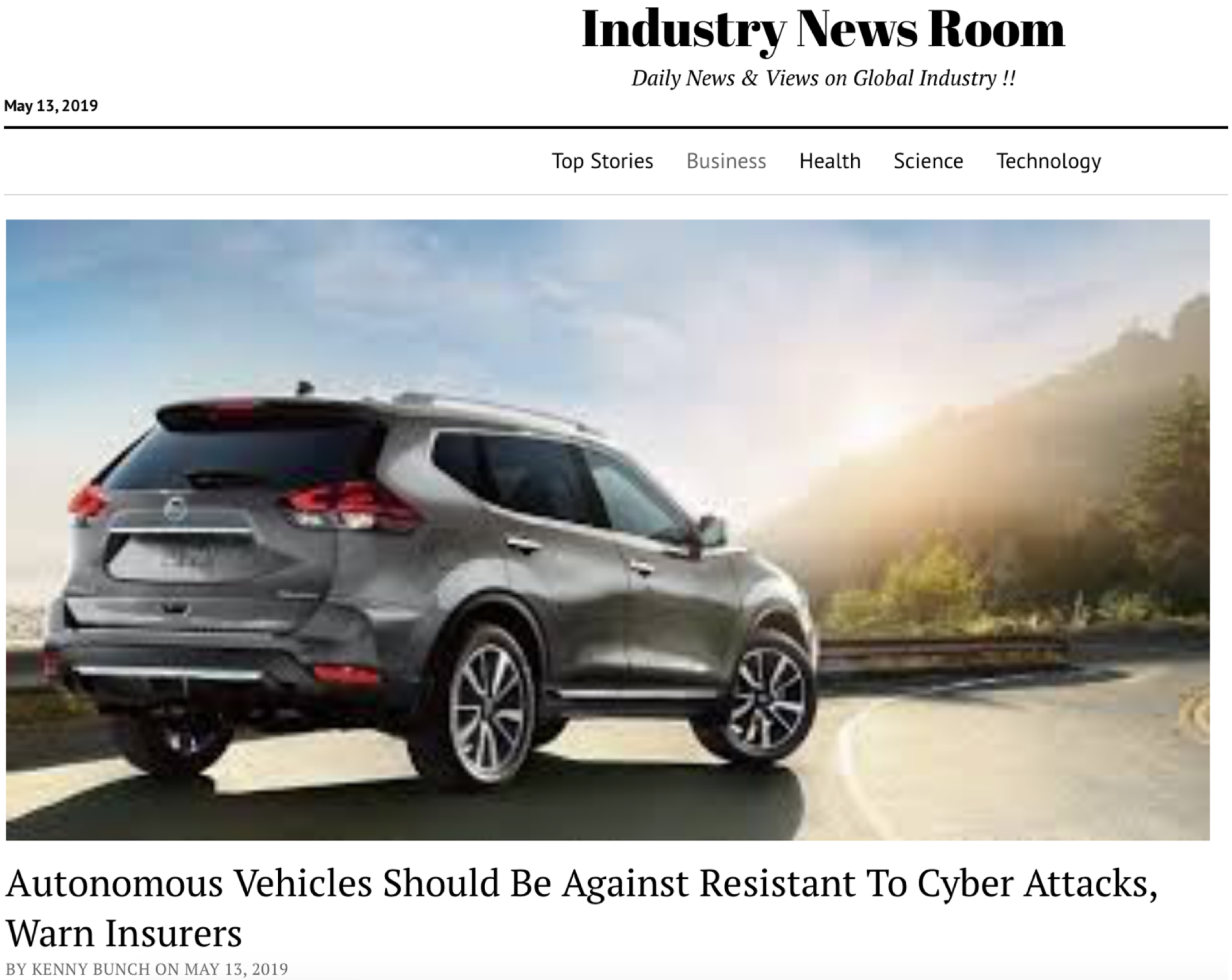
Update Strategy

Protect

Building a Secure Future.™

Deploying Cybersecurity in Current and Future Vehicles

Thank You



Industry News Room

Daily News & Views on Global Industry !!

May 13, 2019

Top Stories Business Health Science Technology

Autonomous Vehicles Should Be Against Resistant To Cyber Attacks, Warn Insurers

BY KENNY BUNCH ON MAY 13, 2019