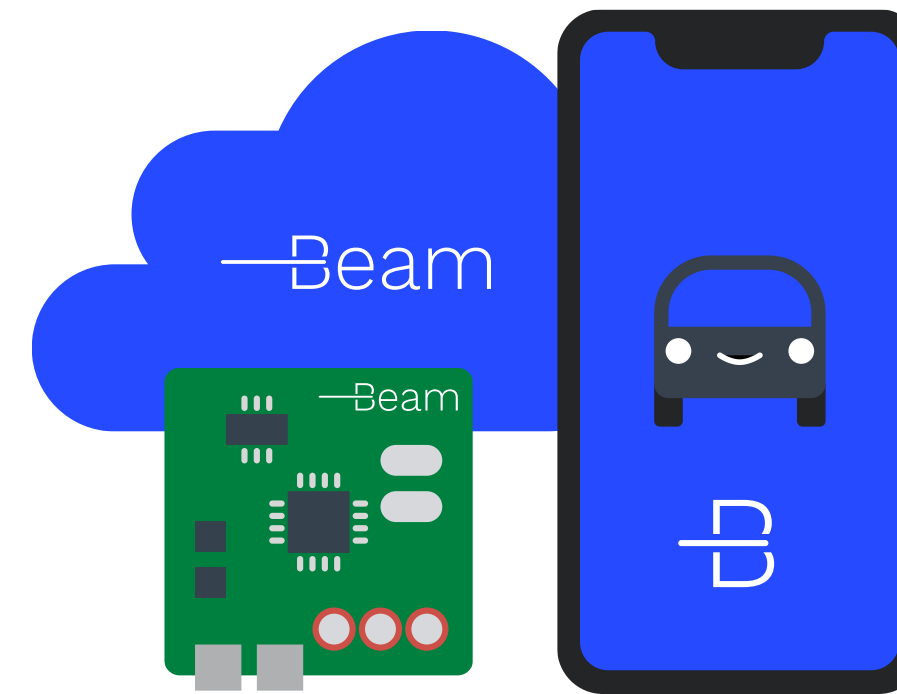


Hardware Security for Connected Vehicles

Rob Potter
Chief Technology Officer
Beam Connectivity

—Beam Connectivity



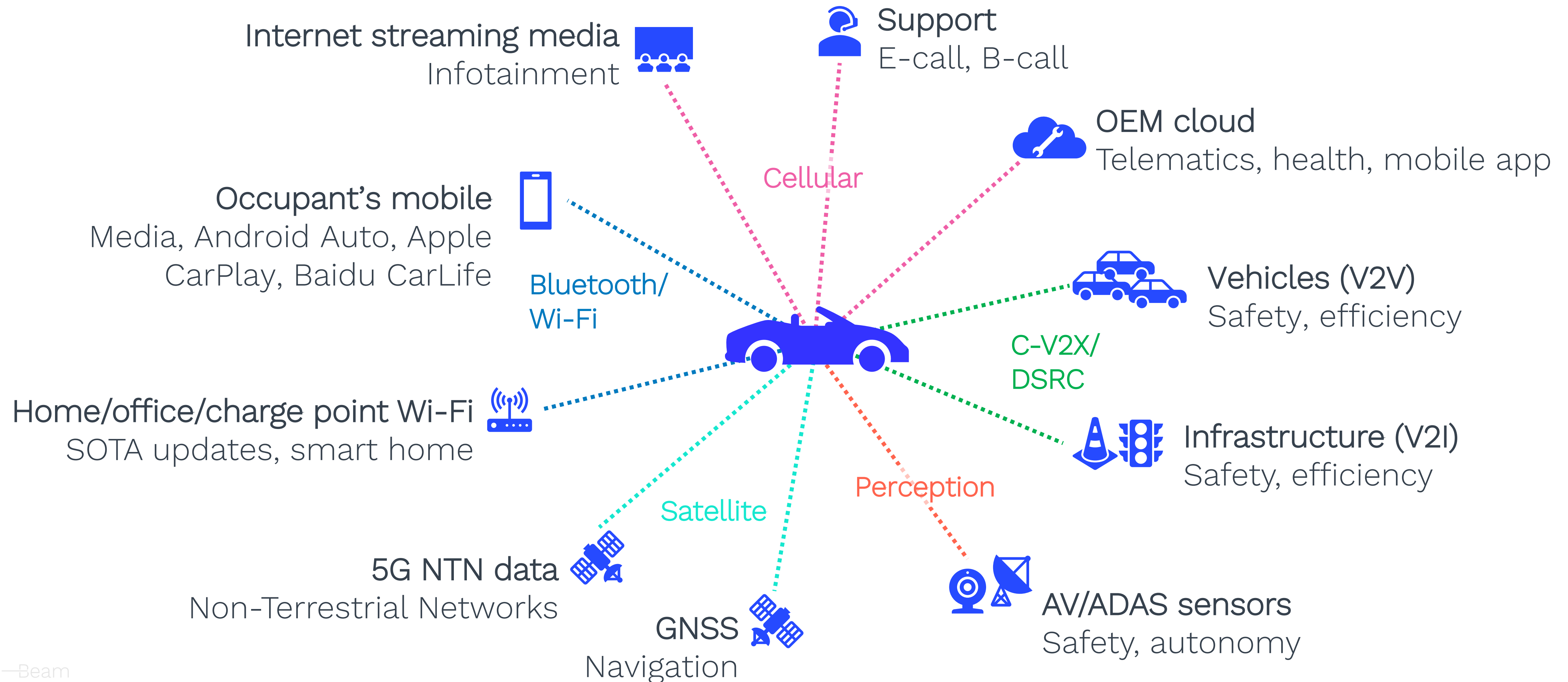
- CTO and co-founder, Beam Connectivity
- 20 years building connected software systems; digital identity, cyber security, automotive
- Beam Connectivity sole focus: high performance and high security connected vehicle systems
- Backed by WAE Technologies

Cyber security headwinds

Secure hardware foundations: CHERI

Project AutoCHERI

Variety of wireless attack vectors



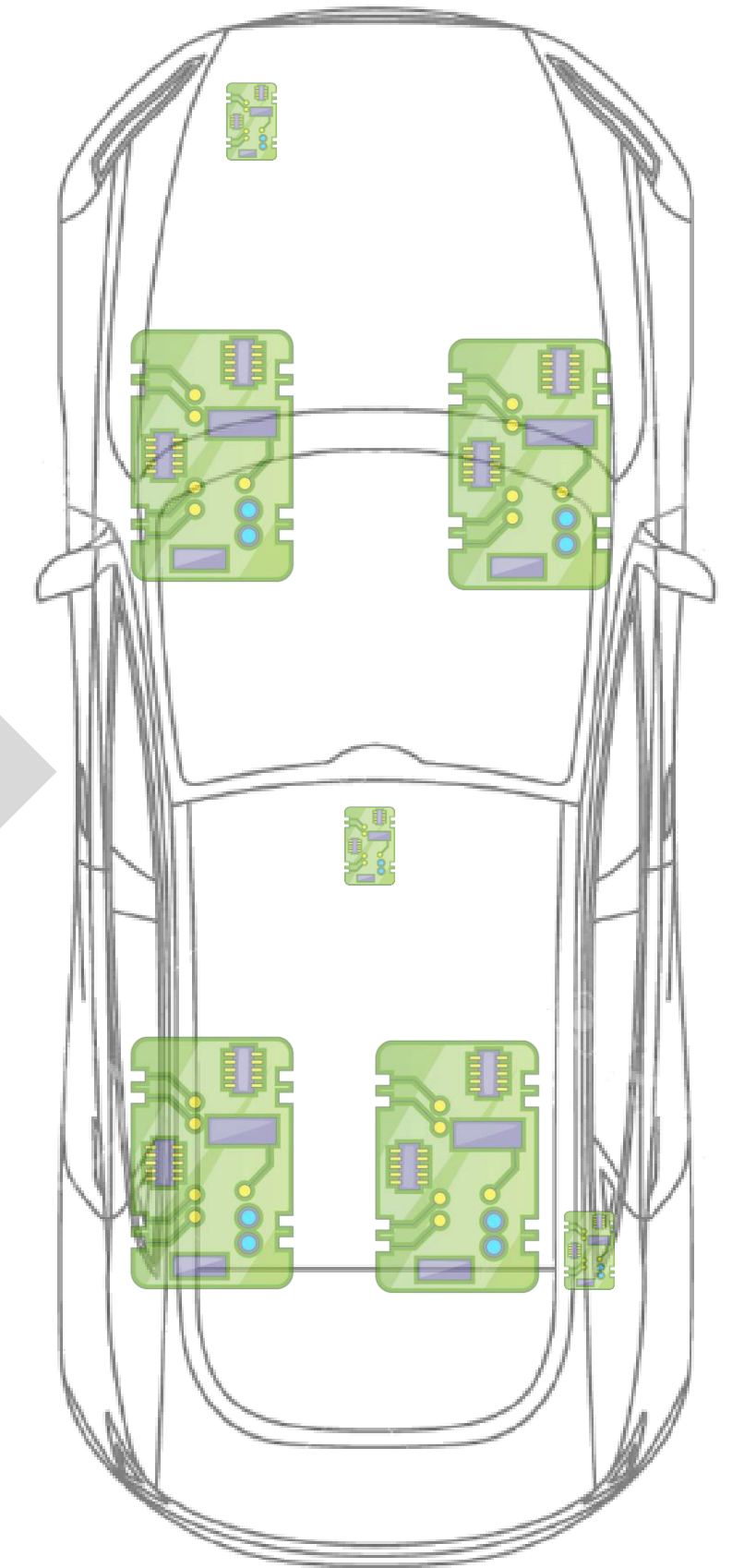
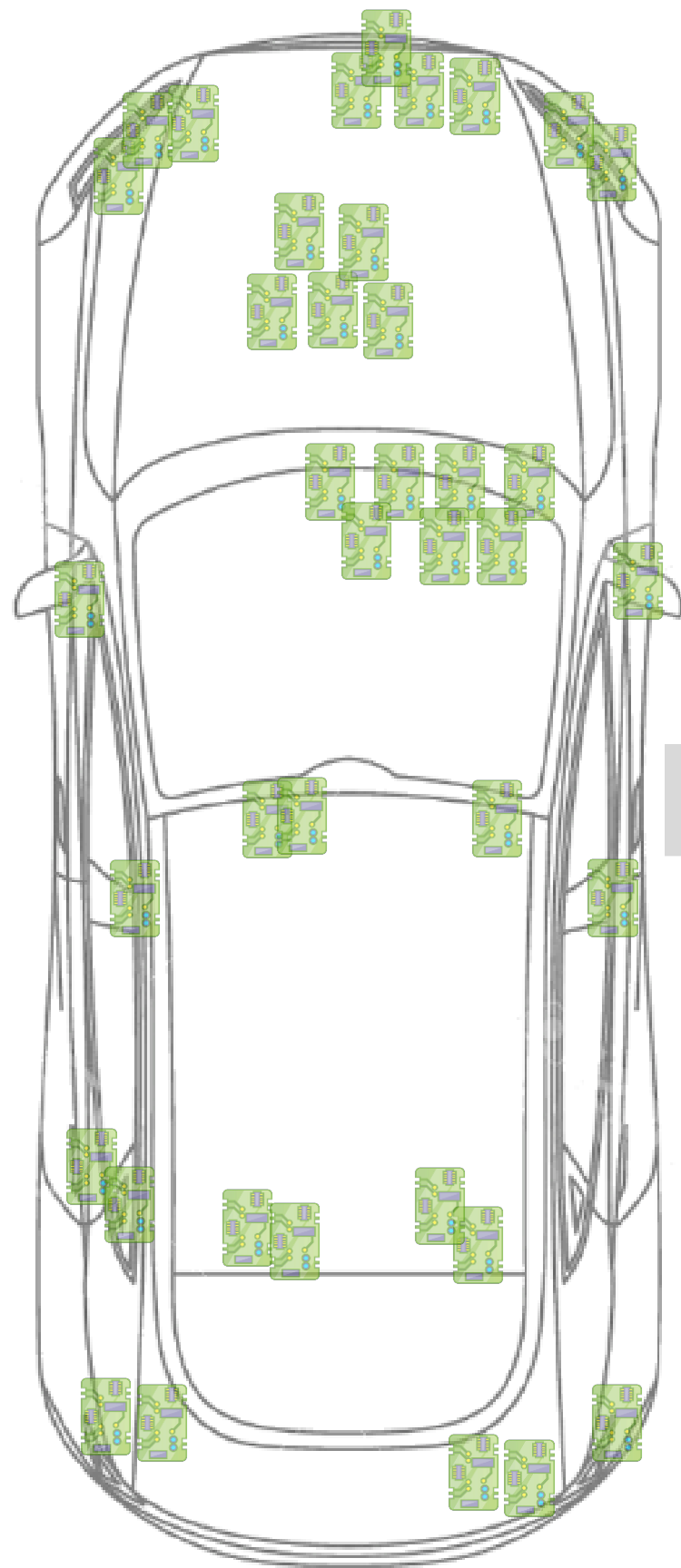
Vehicle architecture evolution

Today: 100+ legacy compute nodes

- One ECU per function, e.g. windows, locks, heated seats
- Connected via simple networking: CAN, LIN, FlexRay

Tomorrow: High performance compute nodes

- More powerful, shared processors
- Variety of cyber critical & performance sensitive workloads
- Software applications need strong isolation



Cyber security headwinds

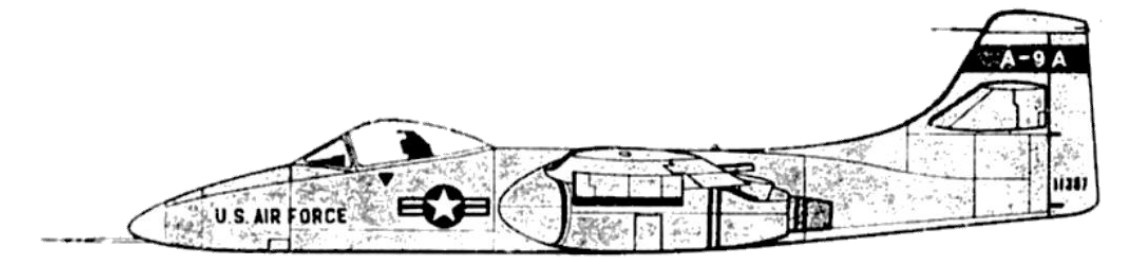
Secure hardware foundations: CHERI

Project AutoCHERI

History of Memory Safety

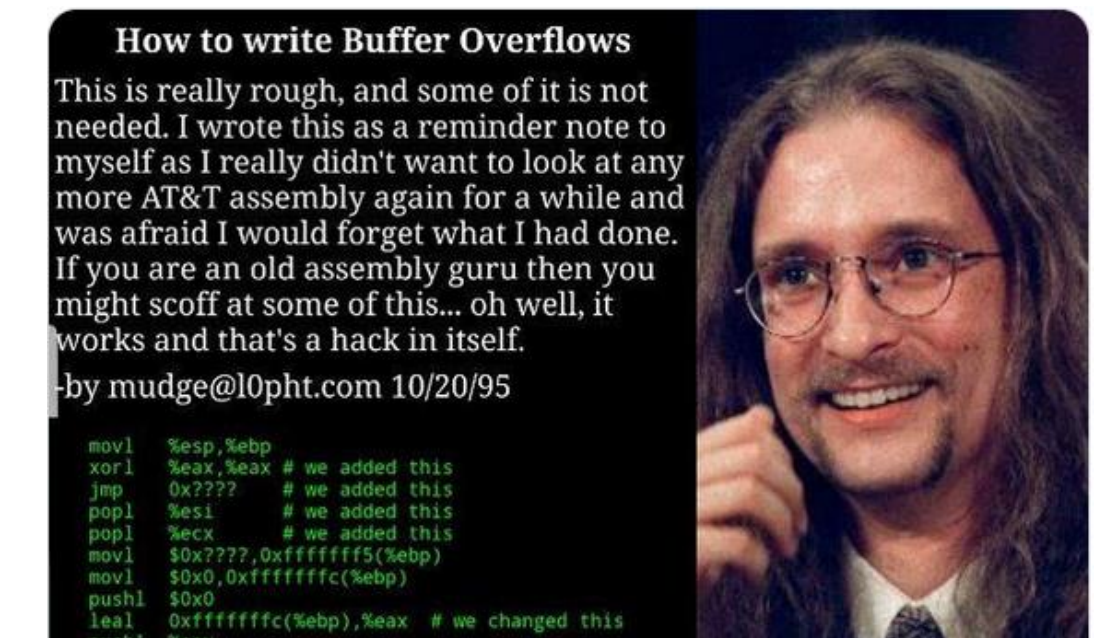
1972

October 1972: USAF study first documented a memory safety vulnerability



1996

Memory safety as a hacking tool: Aleph One publishes the seminal article 'Smashing the Stack for Fun and Profit'

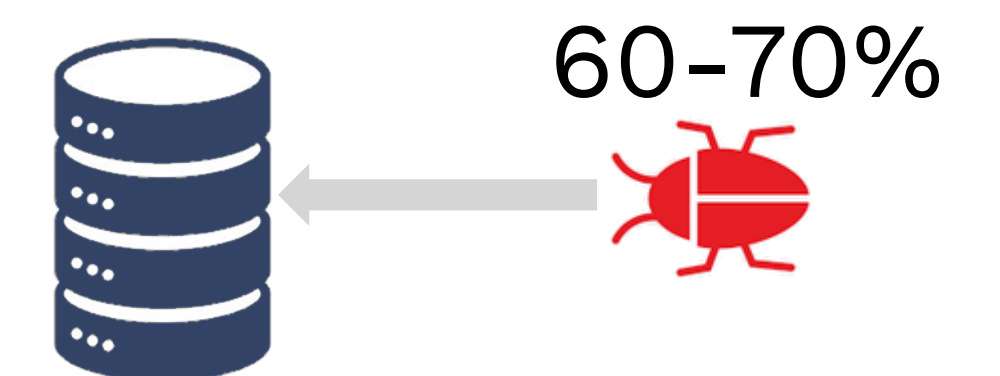


2022

In Q1 over 400 memory safety vulnerabilities reported to the National Vulnerability Database

CVE-2022-42431 – Tesla Model 3

- *Flaw exists within the bcmhdhd Broadcom Bluetooth driver*
- *Lack of validation of the length of user-supplied data.*
- *CWE-120: Buffer Overflow: Copy without Checking Input Size*



Capability Hardware Enhanced RISC Instructions

2012-2023: DARPA, University of Cambridge, SRI, Arm, Microsoft, Google, et al

CHERI processors extend instruction set with two new features:

Memory-safe pointers

Allow memory-unsafe languages such as C to provide **strong, compatible,** and **efficient** protection.

Compartmentalization

Enable fine-grained decomposition of code, to **limit the effects** of security vulnerabilities.

<https://www.cl.cam.ac.uk/research/security/ctsrd/cheri>

<https://www.ncsc.gov.uk/blog-post/so-long-thanks-for-all-the-bits>

<https://alexgaynor.net/2020/may/27/science-on-memory-unsafety-and-security/>

CHERI: Recommended in EU, US, UK & others

PUBLICATION

Security-by-Design and -Default

Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default

Publish Date: April 13, 2023



Secure-by-Design Tactics

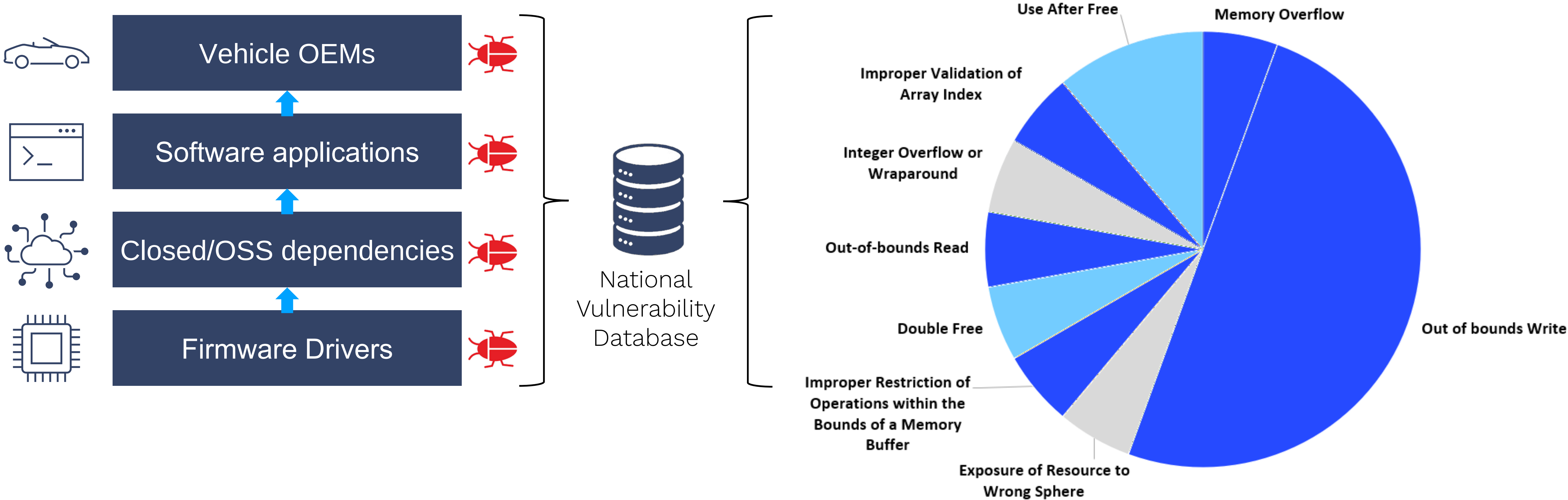
The Secure Software Development Framework (SSDF), also known as National Institute of Standards and Technology's (NIST) [SP 800-218](#), is a core set of high-level secure software development practices that can be integrated into each stage of the software development lifecycle (SDLC). Following these practices can help software producers become more effective at finding and removing vulnerabilities in released software, mitigate the potential impact of the exploitation of vulnerabilities, and address the root causes of vulnerabilities to prevent future recurrences.

The authoring agencies encourage the use of Secure-by-Design tactics, including principles that reference SSDF practices. Software manufacturers should develop a written roadmap to adopt more Secure-by-Design software development practices across their portfolio. The following is a non-exhaustive list of illustrative roadmap best practices:

- **Memory safe programming languages (SSDF PW.6.1):** Prioritize the use of memory safe languages wherever possible. The authoring agencies acknowledge that other memory specific mitigations, such as address space layout randomization (ASLR), control-flow integrity (CFI), and fuzzing are helpful for legacy codebases, but insufficient to be viewed as secure-by-design as they do not adequately prevent exploitation. Some examples of modern memory safe languages include C#, Rust, Ruby, Java, Go, and Swift. Read NSA's memory safety [information sheet](#) for more.
- **Secure Hardware Foundation:** Incorporate architectural features that enable fine-grained memory protection, such as those described by Capability Hardware Enhanced RISC Instructions (CHERI) that can extend conventional hardware Instruction-Set Architectures (ISAs). For more information visit, University of Cambridge's [CHERI webpage](#).
- **Secure Software Components (SSDF PW 4.1):** Acquire and maintain well-secured software components (e.g., software libraries, modules, middleware, frameworks,) from verified commercial, open source, and other third-party developers to ensure robust security in consumer software products.

<https://www.cisa.gov/resources-tools/resources/secure-by-design-and-default>

Memory safety – In the field



CHERI mitigation

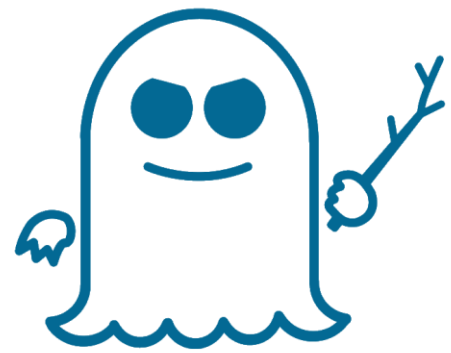


Cyber security headwinds

Secure hardware foundations: CHERI

Project AutoCHERI

“Performance penalty” of security



Spectre/Meltdown: Removing *speculative execution* feature from CPUs resulted in **5%-30% performance hit**, overnight.



Secure Boot: Verifying each software layer **increases total boot time by 4%** [*IEEE magazine*]



BitLocker: “Typically, there's a small IO performance overhead, often in **single-digit percentages**” [*Microsoft*]



SSL/TLS: Overhead of encryption for web traffic. 2005: 70% overhead; **Today: <1%** [*Intel*]

Applus⁺
IDIADA

— Beam
Connectivity

CATAPULT
Compound Semiconductor Applications

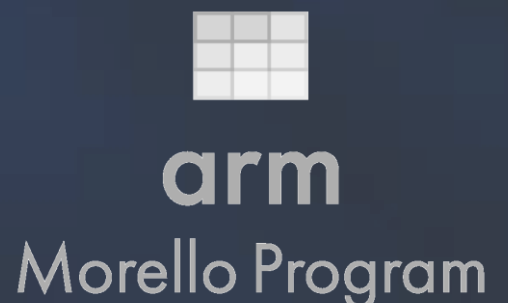


AutoCHERI

<https://autocheri.tech>

“Understand performance/security trade-off of CHERI* for cyber and safety critical automotive applications”

*Capability Hardware Enhanced
RISC Instructions





— Beam
Connectivity

AutoCHERI

<https://autocheri.tech>

Opportunities:

- Offer global perspective
- Partners for a next phase of work
- Automotive Security by Design Summit

01 February 2024, Birmingham, UK



University
of Exeter



Swansea
University
Prifysgol
Abertawe



arm

Morello Program

Business case for CHERI in Automotive

-  More secure software, without a performance impact
-  Doesn't require ground-up rewrite of code
-  Fewer in-field patches, recalls or SW updates
-  Increased productivity of software teams
-  Aligned to regulations: UN ECE 155 (cyber)

—Beam Connectivity

Pioneers in better connected vehicles



www.beamconnectivity.com
autocheri.tech

Rob Potter
Chief Technology Officer
rob@beamconnectivity.com