Applus IDIADA

Beam Connectivity

CATAPULT
Compound Semiconductor Applications

University of Exeter

Swansea University
Prifysgol Abertawe

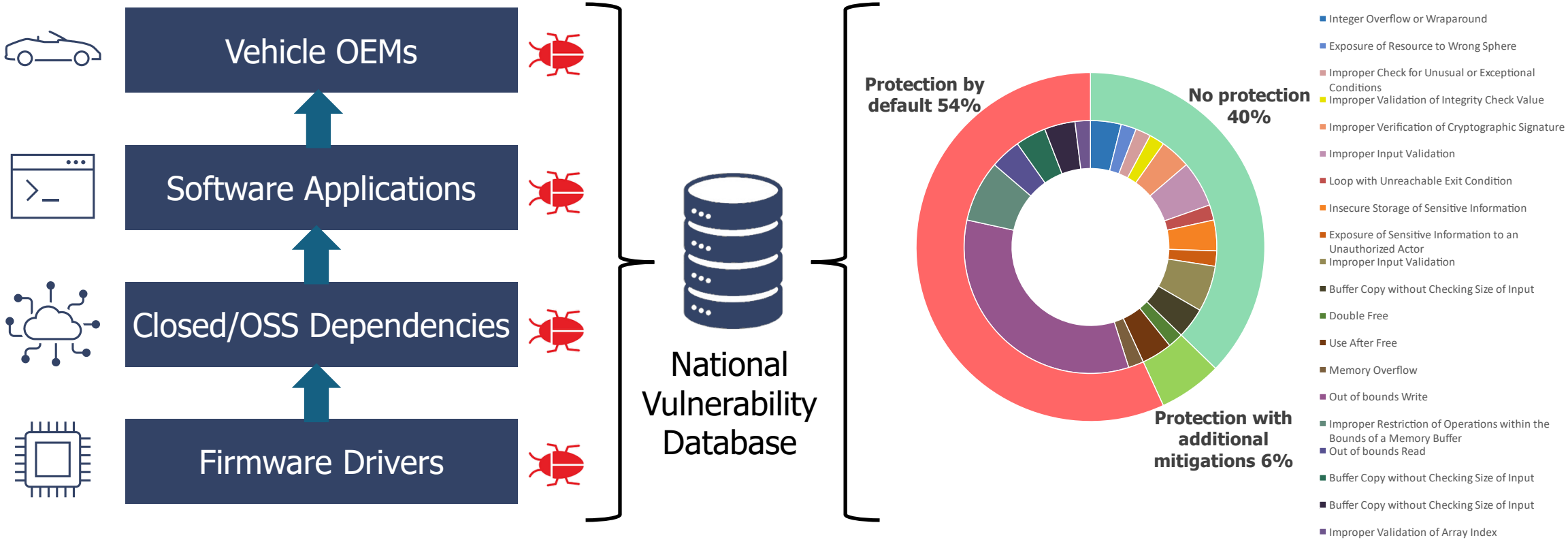
AutoCHERI

"Understanding the trade-offs of CHERI for cyber and safety critical automotive applications"

https://autocheri.tech

arm
Morello Program

Memory Safety: How Big of a Problem is it?



CHERI has a security benefit for automotive applications. Majority of vulnerabilities link back to two key components, the TCU and infotainment unit, both of which play significant roles in enabling connectivity.

Reported Vulnerability Trend

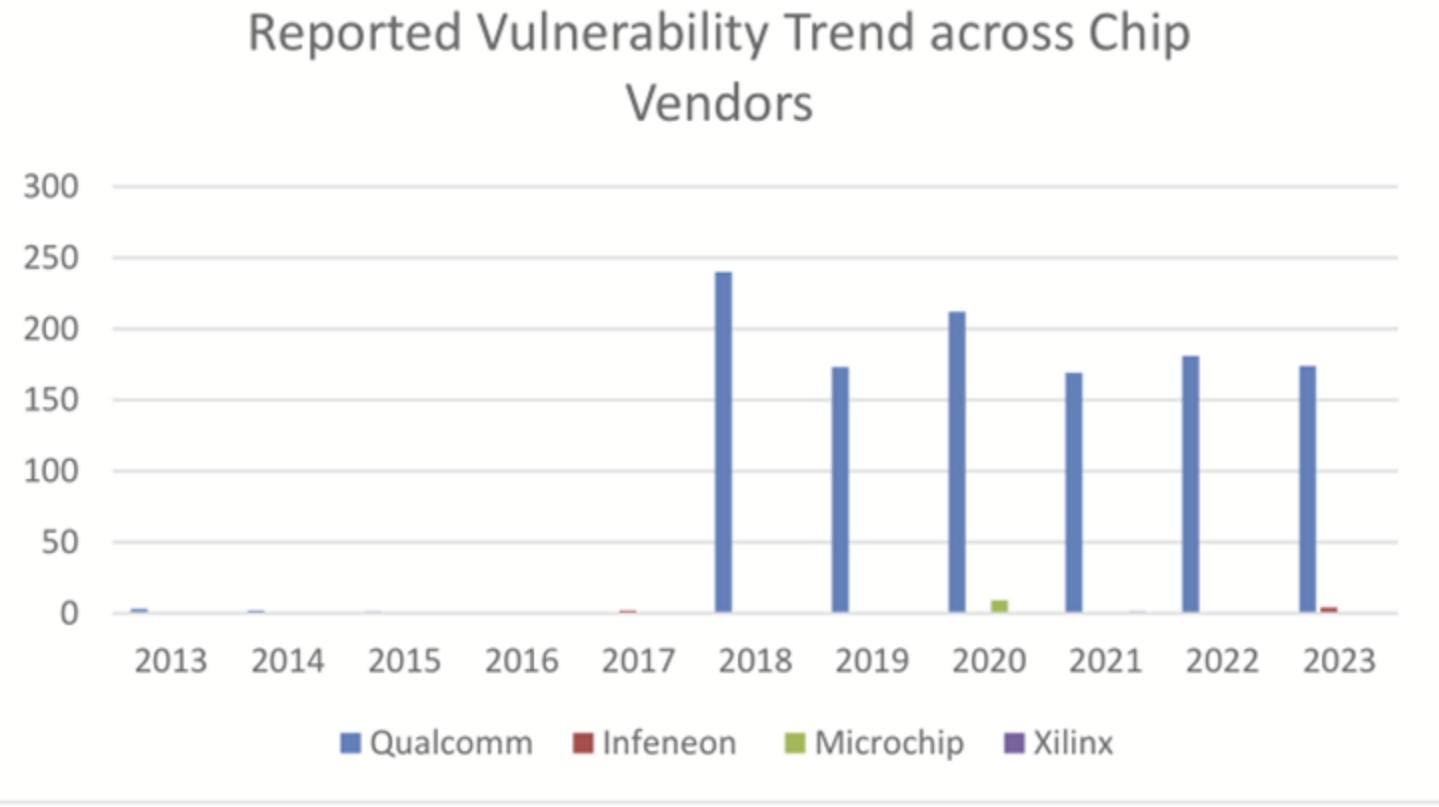


Figure 7: Reported vulnerability trend across chip vendors

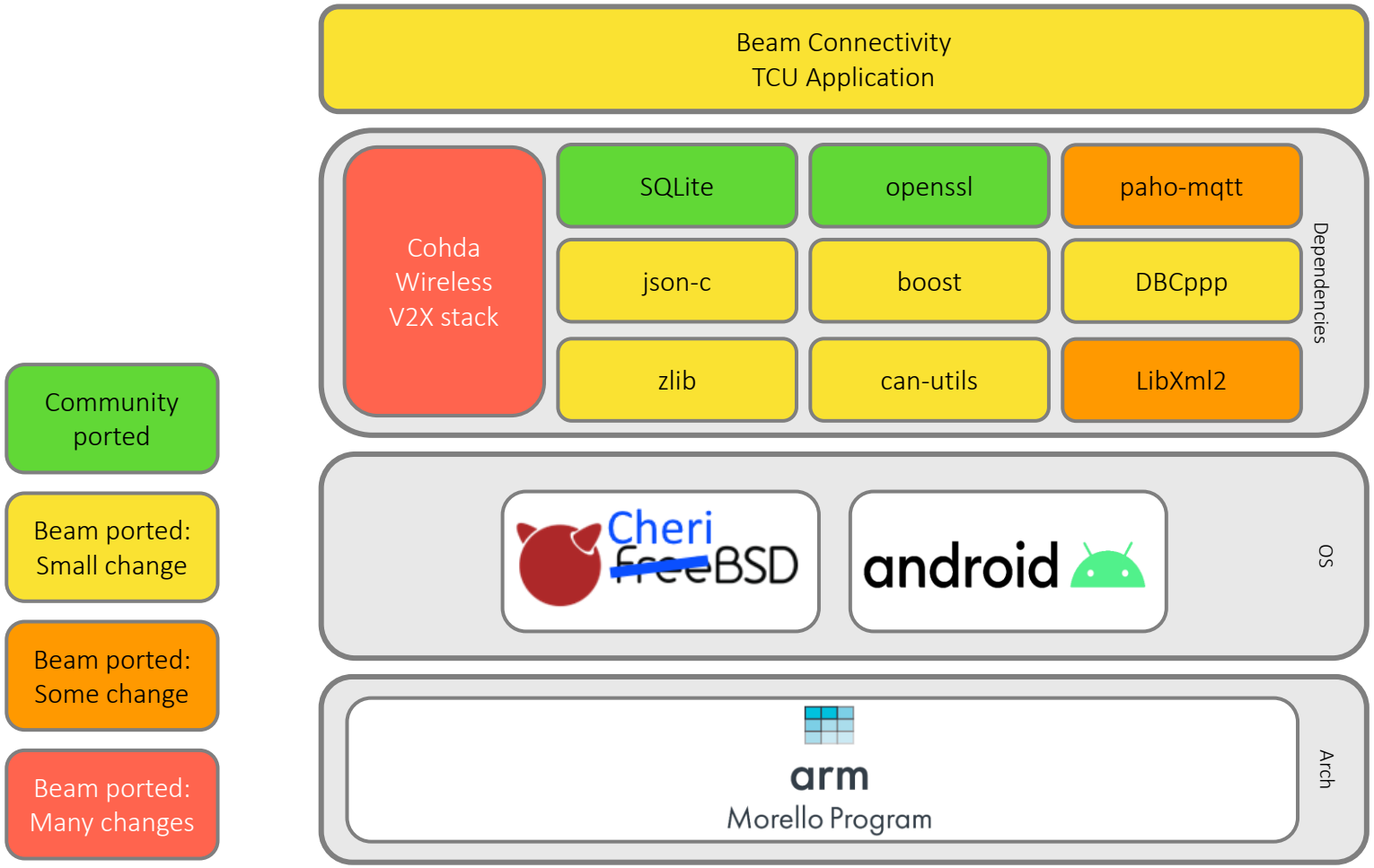
Qualcomm seems to have changed it disclosure policy in 2018. Are vulnerabilities about others being underreported in the NVD?

ECU Classification

Application Class	ECU Name	Use Cases						Impact Category				OS					SW Development	
		Security events detection/reporting	Vehicle motion	Body control	Anti-theft	ADAS Feature	Battery charging	Safety	Operational	Financial	Privacy	Bare Metal	AUTOSAR	RTOS	QNX	Other	C	Model-based E.g.MATLAB
Safety-related	Anti-Lock Brakes (ABS), Vehicle Control Unit (VCU)		X					X	X			X	X	X	X		X	X
Emissions control	Powertrain Control Module (PCM), Engine Control Module (ECM)		X						X			X	X	X			X	X
Anti-theft	Body Control Module (BCM), Engine Control Module (ECM)				X				X	X		X	X	X			X	X
Cybersecurity specific functions	Gateway Module	X						X	X		X		X	X	X	X	X	X
Infotainment	Infotainment / Audio Control Module (ICM or ACM), Telematics Control Unit (TCU),	X							X		X				X	X	X	
ADAS	Automatic Cruise Control (ACC) Cruise Control (CC)					X		X	X				X	X	X	X	X	X
EV	Hybrid / Electric Vehicle Battery Management System (BMS), On-board Charger (OBC),						X	X	X		X	X	X	X			X	X

The TCU is not safety critical, has a feature rich OS and is used in security detection/reporting. Widely used automotive OS and software development are intended to stop memory issues occurring

Challenges: Porting to Morello

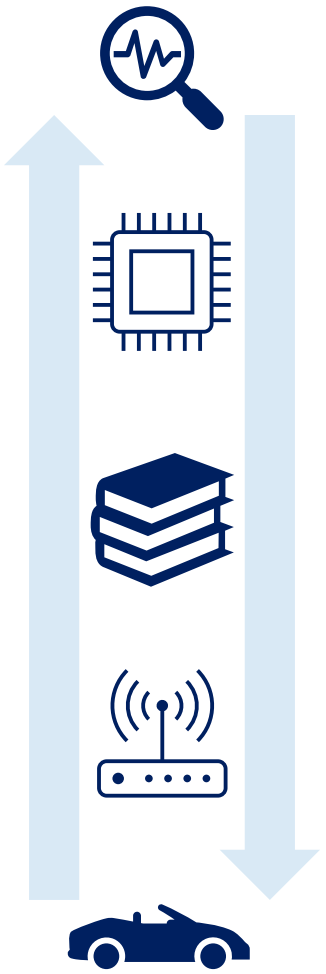


Issues faced:

- Single-origin provenance
- Alignment
- non-provenance-preserving copy
- Inter-process communication

Porting to CHERI is easy. Code not using implementation specific features or assumptions should require few to no changes.

Interactions Along the Supply Chain



1. Research new ideas
   - Benefits and drawbacks
2. Hardware technology supply chain
   - IP and chip vendors
3. Software technology supply chain
   - OS and middleware vendors release compatible libraries & tools
4. Automotive Tier 1 products
   - ECU manufacturers
5. Vehicle manufacturer programmes
   - New vehicle programmes

Additional security is not a strong driver. Changing toolchains is difficult, but possible when incentivised. The platform re-architecture for new Electric Vehicles provides an opportunity for radical rethink on ECUs.

Safety Analysis of Software

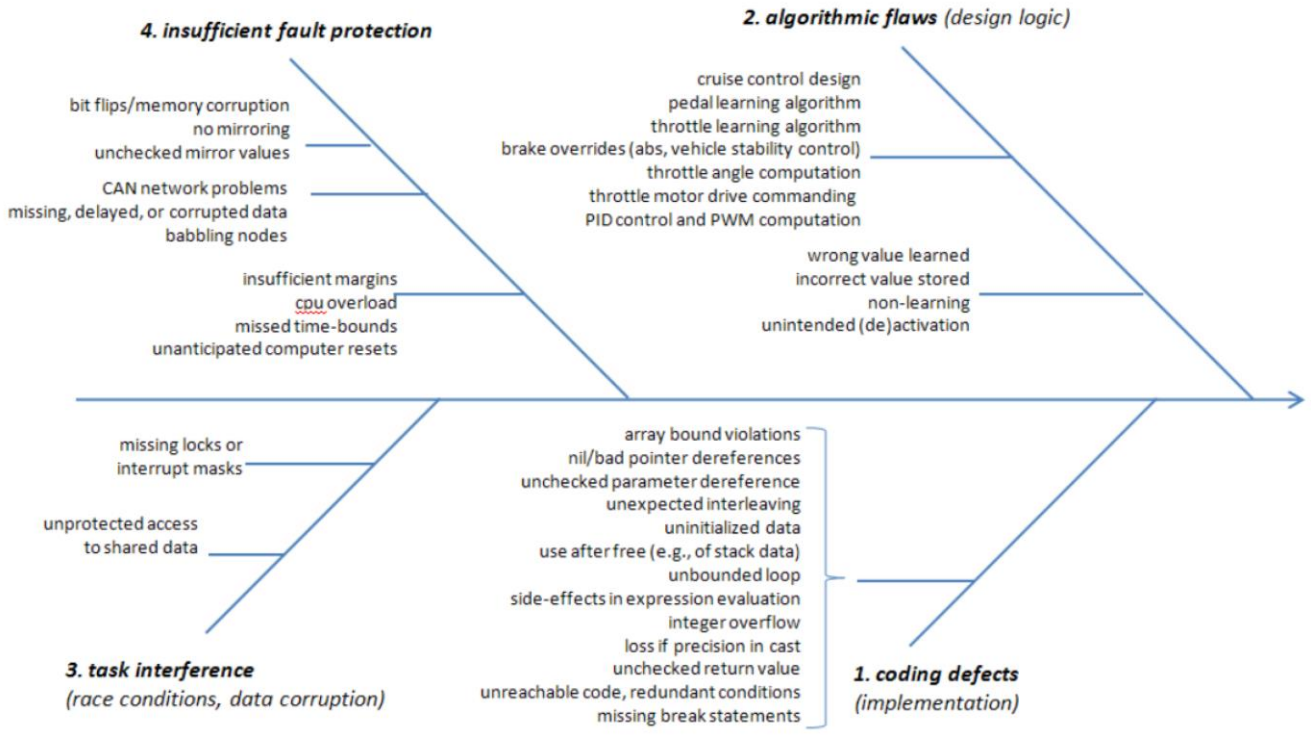


Figure A.5-1. Fishbone Diagram of Potential Software Causes for UA

- Unit tests
- Static analysis tools
- Code review
- Logic modelling
- Algorithm modelling
- Unexpected error analysis
- System behaviour

https://web.archive.org/web/20220625035237/https://one.nhtsa.gov/staticfiles/nvs/pdf/NASA_FR_Appendix_A_Software.pdf
https://www.eetimes.com/toyota-case-single-bit-flip-that-killed

Software development process for safe systems is very thorough. Memory safety is just one type of issue being prevented. New regulations focus on security.

Final Insights

- Security alone isn't a big enough benefit.
- Previous designs have been stopped as the timing constraints couldn't be met.
- Having deterministic memory safety at improved speeds is desirable.
- Portable memory safety implementation make development easier.

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-976.pdf
https://medium.com/volvo-cars-engineering/the-reality-of-autosar-and-the-way-forward-36af39ec4099

Examples of performance benefits. Library of code showing the ease of integration. Continue querying pain points and highlighting where CHERI could be a solution.

Thank You

Questions