42crunch

API Security Insights for the Connected Vehicle Ecosystem

Speakers

Anthony Lonergan

Head of Product Marketing and editor of APIsecurity.io

42Crunch

Darren Shelcusky

Senior Consultant Vehicle & Mobility Cybersecurity

Ex Ford, GM & Dupont

Recommended whitepaper

End-to-end API Security for the Software Defined Vehicle

End-to-end API Security for the Software Defined Vehicle

Implementing a DevSecOps Approach for Developing and Protecting APIs

crunch

https://42crunch.com/whitepaper-automotive-api-security-sdv/

Speaker

Darren Shelcusky

Senior Consultant
Vehicle & Mobility Cybersecurity

Ford, GM & Dupont

Speaker

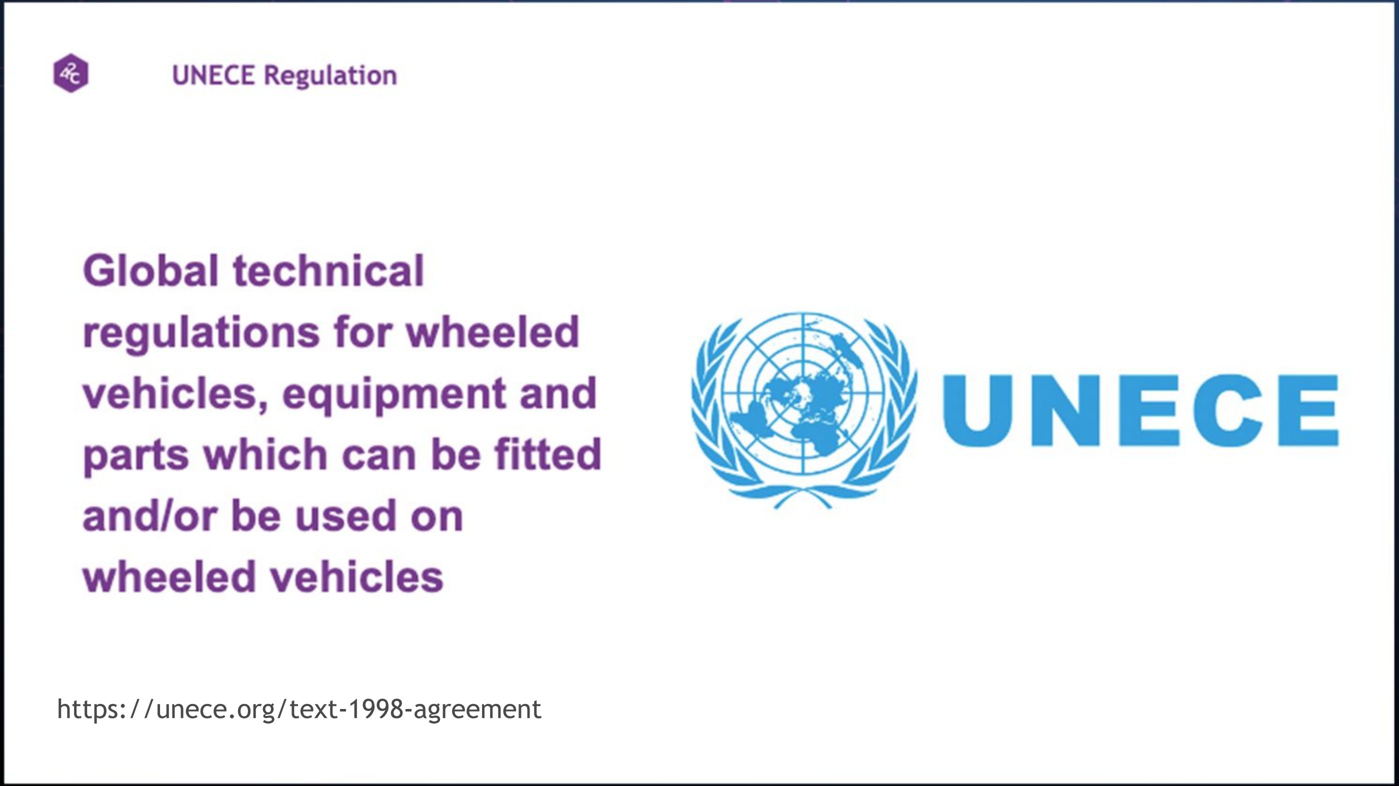
Darren Shelcusky

- Cybersecurity for connected vehicle ecosystem
- Vehicle Techstack
- Clients, cloud, APIs, VSOC
- Cybersecurity systems
- Software development

42crunch

“…In the safety critical world DevSecOps has been around for a long time…”

The connected vehicle ecosystem is anything that can read or change the state of a vehicle

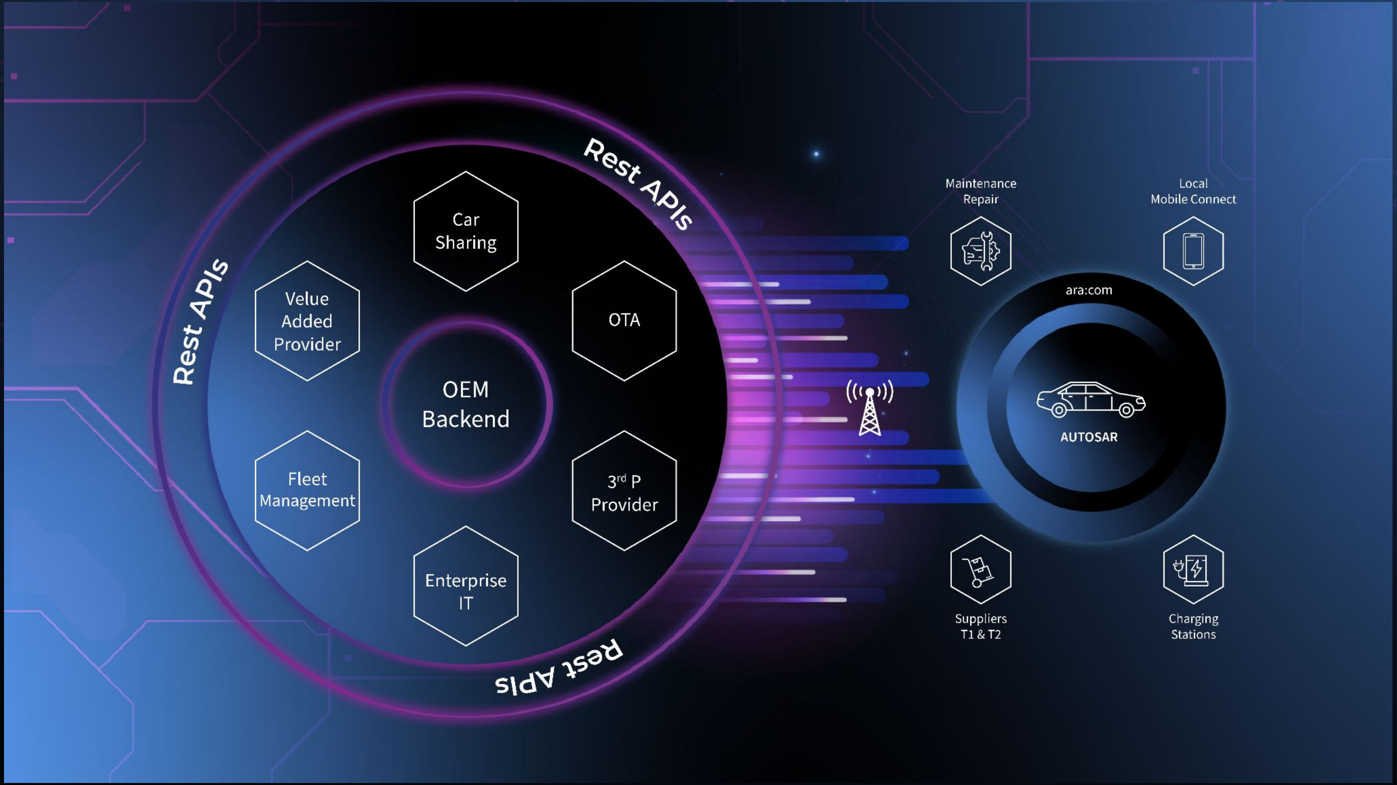


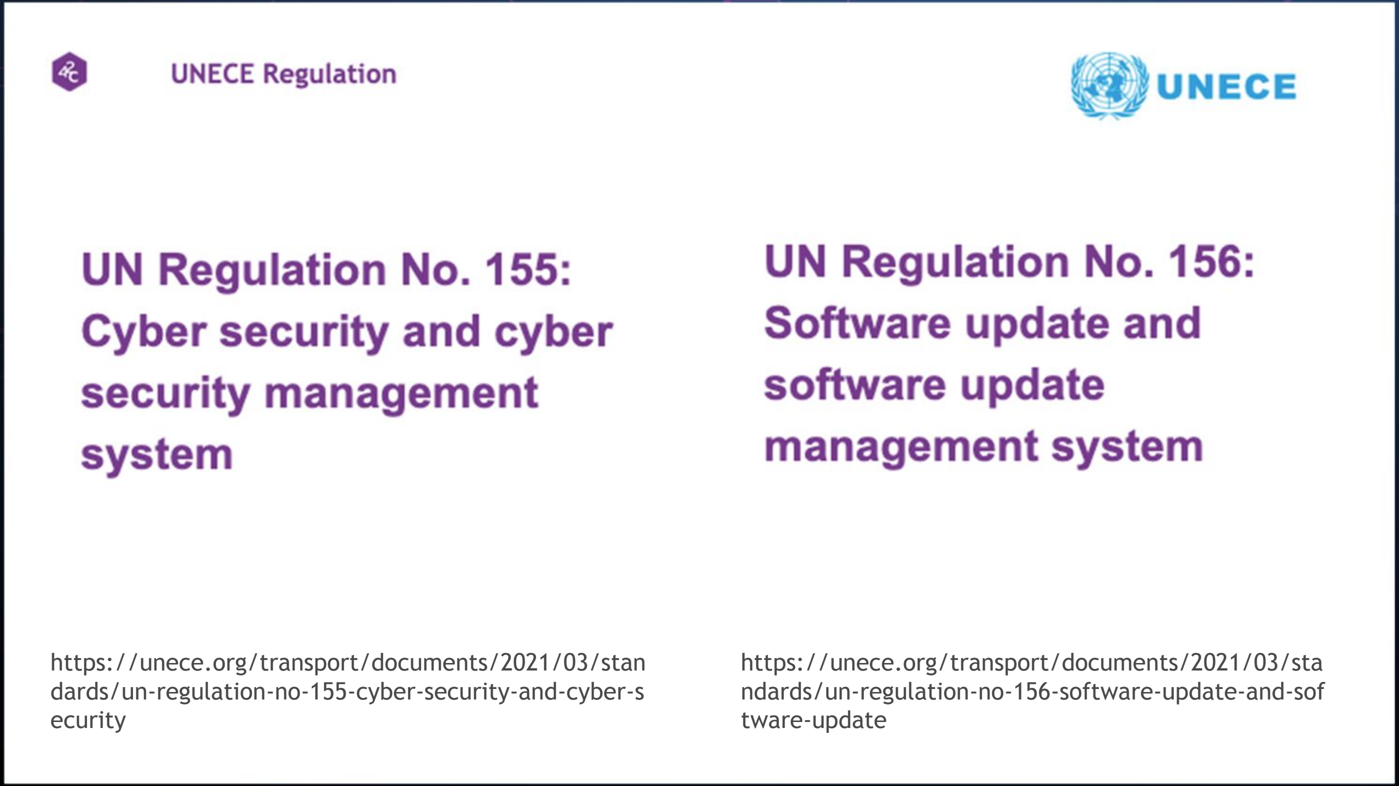
UNECE Regulation

Global technical regulations for wheeled vehicles, equipment and parts which can be fitted and/or be used on wheeled vehicles

UNECE

https://unece.org/text-1998-agreement


Rest APIs
Rest APIs
Rest APIs
Car Sharing
Velue Added Provider
OTA
OEM Backend
Fleet Management
3rd P Provider
Enterprise IT
Maintenance Repair
Local Mobile Connect
ara:com
AUTOSAR
Suppliers T1 & T2
Charging Stations



UNECE Regulation

UNECE

UN Regulation No. 155: Cyber security and cyber security management system

https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

UN Regulation No. 156: Software update and software update management system

https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update

“...It’s not just the APIs you write, it’s the supplier ecosystem, it’s the third party, it’s the frameworks...”

42crunch

“…API security it no longer a nice to have, it is a critical component…”

Recommended article

The Future of Automotive Cybersecurity: Why Learning Car Hacking is Essential

https://securityboulevard.com/2025/01/the-future-of-automotive-cybersecurity-why-learning-car-hacking-is-essential/

Recommended article

Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More

https://samcurry.net/web-hackers-vs-the-auto-industry

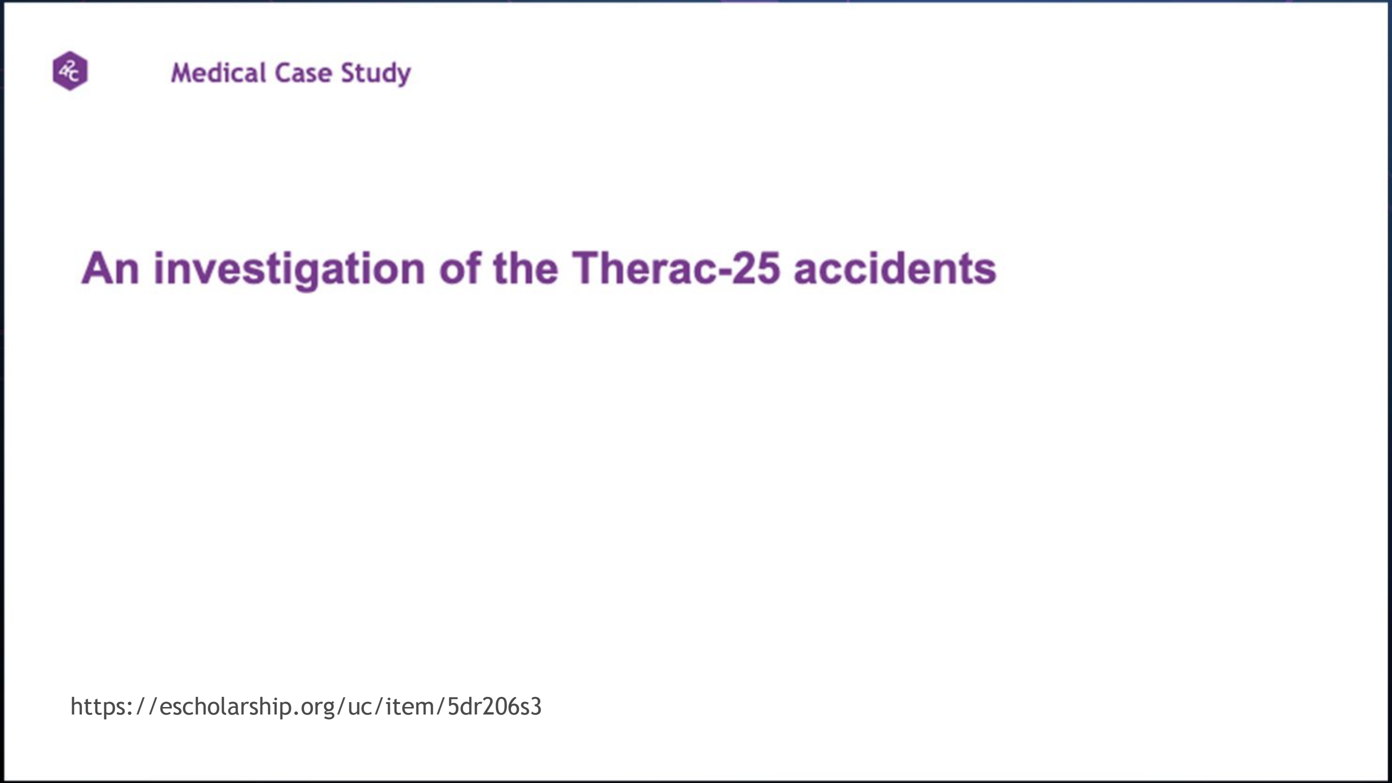
“...Sam Curry and team: 3 months, 19 OEMS, remote command and control, access to backend systems, dealer hubs, source code...”

“…APIs are the soft underbelly of the automotive ecosystem…”

"...What Sam Curry and his team did was not novel, it was the issue of automotive companies not addressing known vulnerabilities against APIs..."

“...The hackers were looking for the weakest point in the ecosystem...”

Can your APIs handle unusual inputs, will they respond unpredictably?



Medical Case Study

An investigation of the Therac-25 accidents

https://escholarship.org/uc/item/5dr206s3

“…APIs should be defined through a contract…”

“...Either the contract was poorly written or the implementation of the code did not enforce the contract...”

Use the OpenAPI definition to build predictable APIs

“…API development,
As designed,
As built,
As consumed…”

42Crunch API security solutions:

- As designed - API Security Audit
- As built - API Conformance Scan
- As consumed - API Protect Firewall

Produce predictable software

Not a question of
“Why would someone do that?”,
it is more about
“What happens when someone does that?”

“...Undefined behaviour is very scary.. because you have no clue on how your API will respond...”

Remove API vulnerabilities using better API design practices

Leverage the OpenAPI contract to ensure that you are building and deploying APIs that are more predictable and secure

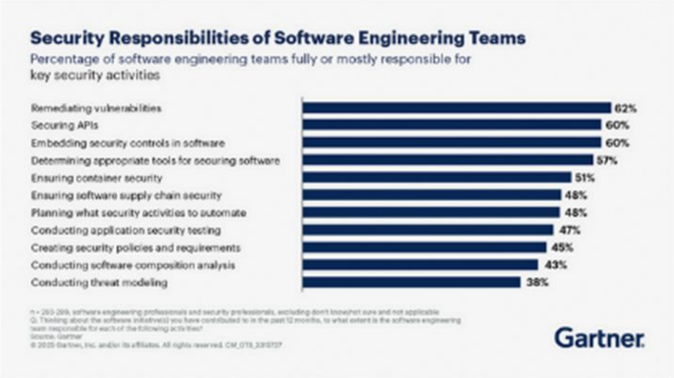
Integrating API security into DevSecOps

"…Make the right thing the easiest thing;
Work side by side with developers;
Learn from failures…"

“…reverse engineering via monitoring is guessing..instead I state (in a definition) how the (API) will operate…”

Recommended article

Gartner: Security Responsibilities of Software Engineering Teams



Security Responsibilities of Software Engineering Teams

Percentage of software engineering teams fully or mostly responsible for key security activities

n = 293-299, software engineering professionals and security professionals, excluding don't know/not sure and not applicable
Q. Thinking about the software initiative(s) you have contributed to in the past 12 months, to what extent is the software engineering team responsible for each of the following activities?
Source: Gartner
© 2025 Gartner, Inc. and/or its affiliates. All rights reserved. CM_GTS_3315727

https://www.gartner.com/en/articles/software-security

"…electrification changes everything…"

“…the software defined vehicle is enabled by electronics, software and APIs…”

- Remove vulnerabilities with secure design
- OpenAPI contract as single source of truth
- OpenAPI contract drives security across the API lifecycle
- Automate to achieve scale
- Foster collaboration between development and security teams

Q & A

You spoke about making security easy to do. Was there anything specific about the 42Crunch products that enabled this?

42Crunch provides users with API access to run static and dynamic testing of APIs in CICD pipelines

42Crunch OpenAPI Editor IDE plugin lets users create & edit OpenAPI contracts and test APIs during development

“...Seamless automated integration (provided by 42Crunch) helped a lot...”

You referenced the OpenAPI contract as the single source of truth. How does it work for the firewall when APIs are in production?

The 42Crunch API Protect firewall uses the OpenAPI contract as the basis of what API traffic to allow or block

42crunch

"…You need to decide how your firewall will handle undocumented behavior…"

Undocumented behavior is a defect, proactive management of defects allows for continuous improvement

You mentioned about having a single API to deploy APIs. How did you ensure the quality of the APIs in production when changes were made?

- Static and binary analysis on the source code
- Look for CVEs in 3rd party libraries
- Clean security audit and conformance scan from 42Crunch tooling

The pipeline needs to automatically check if tests have passed before allowing any changes to go live.

You spoke about “as consumed” and
anticipating unpredictable behavior,
but how can you think of every possible scenario of
the API being used in a way that was not expected?

Monitoring alerts will highlight either
an implementation problem
or a documentation problem

Unanticipated usage: look at usage patterns that are outside of the design constraint

“...Refactoring the API may be required to handle use cases that were not initially anticipated...”

“…Understand who your customers are and
how they use your product,
including understanding the ways they use
your product that was not anticipated…”

Learn more

#1 API SECURITY NEWSLETTER

APIsecurity.io
By 42Crunch

https://apisecurity.io/

FREE TOOLS

https://42crunch.com/freemium/

WHITE PAPER

End-to-end
API Security
for the Software
Defined Vehicle

Implementing a DevSecOps Approach
for Developing and Protecting APIs

crunch

https://42crunch.com/whitepaper-automotive-api-security-sdv/

42crunch

API Security Insights for the Connected Vehicle Ecosystem