



Automotive Cybersecurity

Risks and Challenges

SIP-adus Workshop, Tokyo
27 October 2015
Mike Parris



NOKIA 'PAID BLACKMAIL HACKERS MILLIONS'

Mobile Phones



Source: BBC

ANTHEM INC. SPENDS \$50 MILLION A YEAR AND EMPLOYS 200 PEOPLE TO KEEP ITS INFORMATION TECHNOLOGY SECURE

Healthcare



Source: IBJ.com

CRITICAL INFRASTRUCTURE COMMONLY HIT BY DESTRUCTIVE CYBER ATTACKS, SURVEY REVEALS

Infrastructure

Critical infrastructure organisations are commonly targeted by cyber attacks aimed at manipulating equipment or destroying data, a survey reveals.

Source: ComputerWeekly.com

TARGET SAYS CREDIT CARD DATA BREACH COST IT \$162M IN 2013-14

Retail - Groceries



Source: techcrunch.com



Why is this Relevant?

The product or service is irrelevant.

Hackers focus on the outcome.

Historically, automotive was not a target.

There was **no cybersecurity concern.**

Connecting cars to the IoT makes both the **vehicles** and **vehicle manufacturers potential targets.**

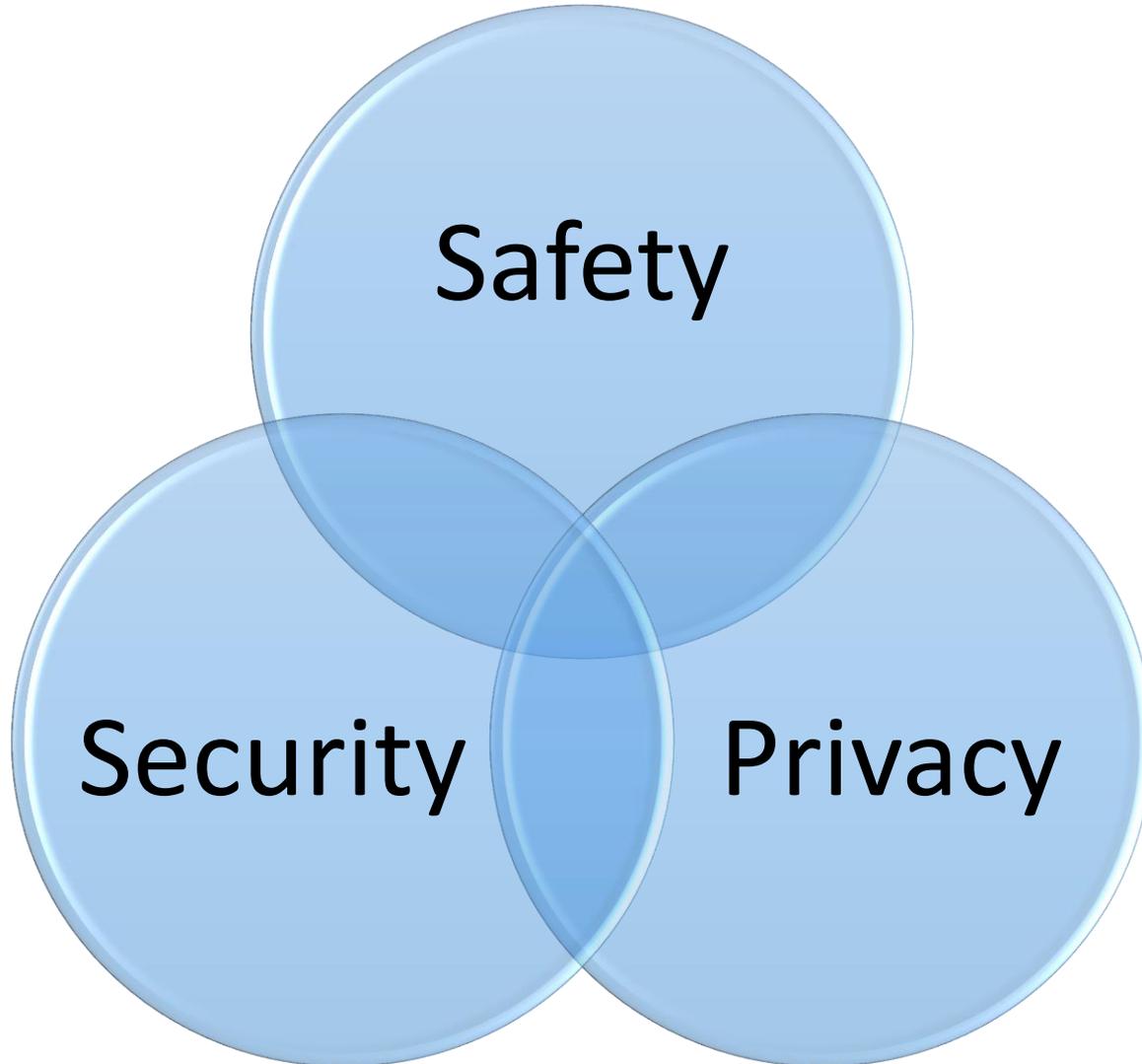
We cannot assume hackers want to take remote control of a connected vehicle.

Single-attack-point / single-countermeasure cases are rare.

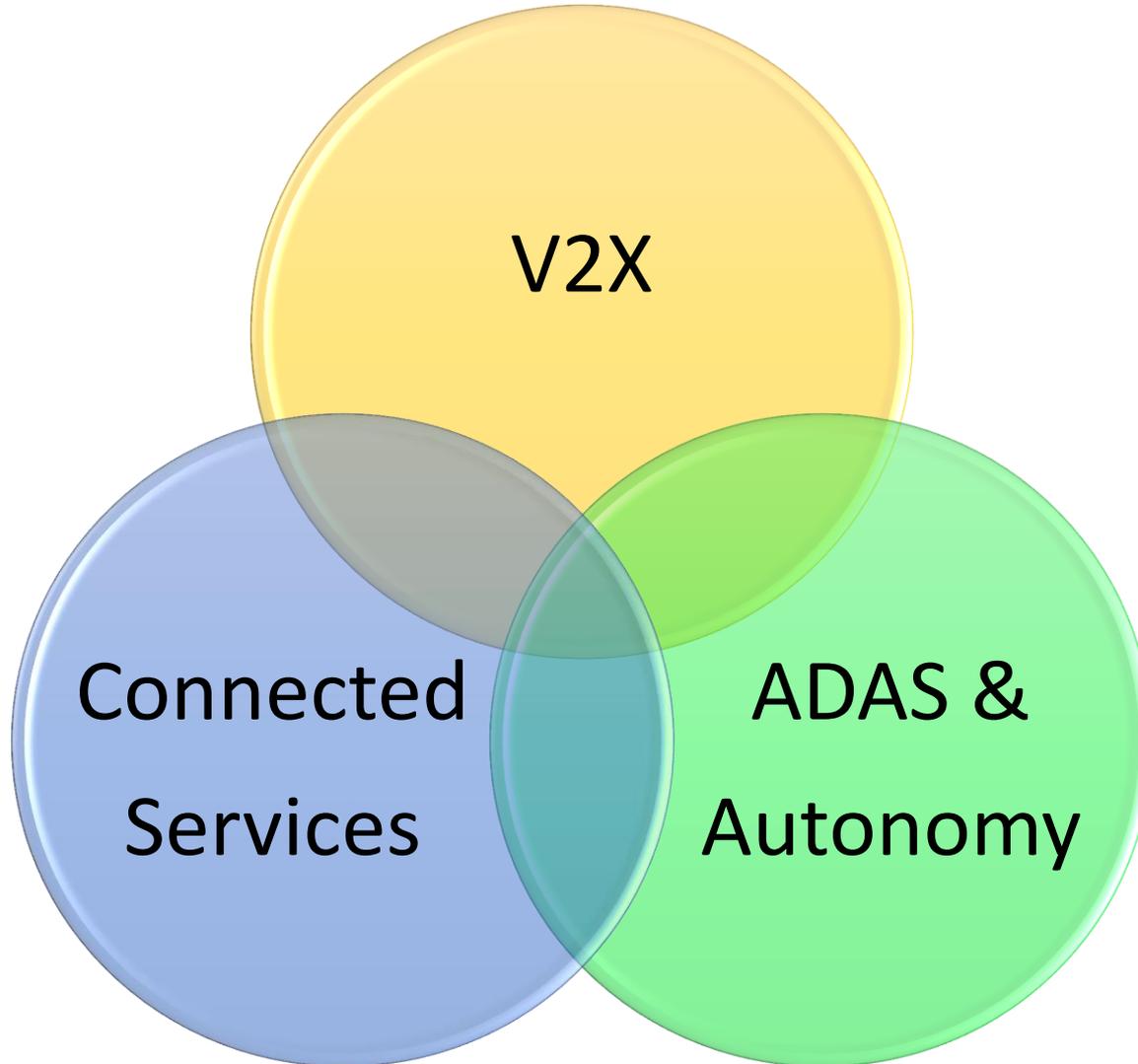
Financial impacts can be huge:

\$100 millions or billions!

What is Security of a Connected Car?



Where are the Security Risks?



Where are the Security Risks?

Technology centric

Telematics/Connected Services

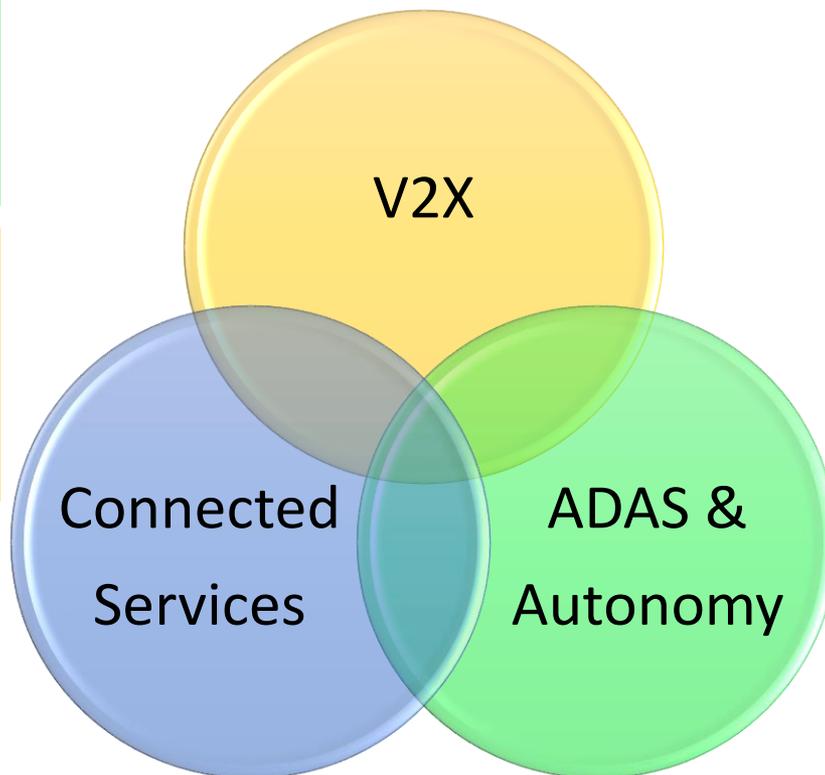
- Absence of security standards
- Geographic coverage

ADAS/Autonomous

- Emerging technology still being developed
- Sophistication & speed of processing algorithms

V2X Services

- Performance
- Security, safety (& privacy) trade-offs
- Pilot projects still proving the technology



Use-case centric

Penetration of software updates

Communications latency in congested areas

GPS accuracy in tunnels or 'urban canyons'

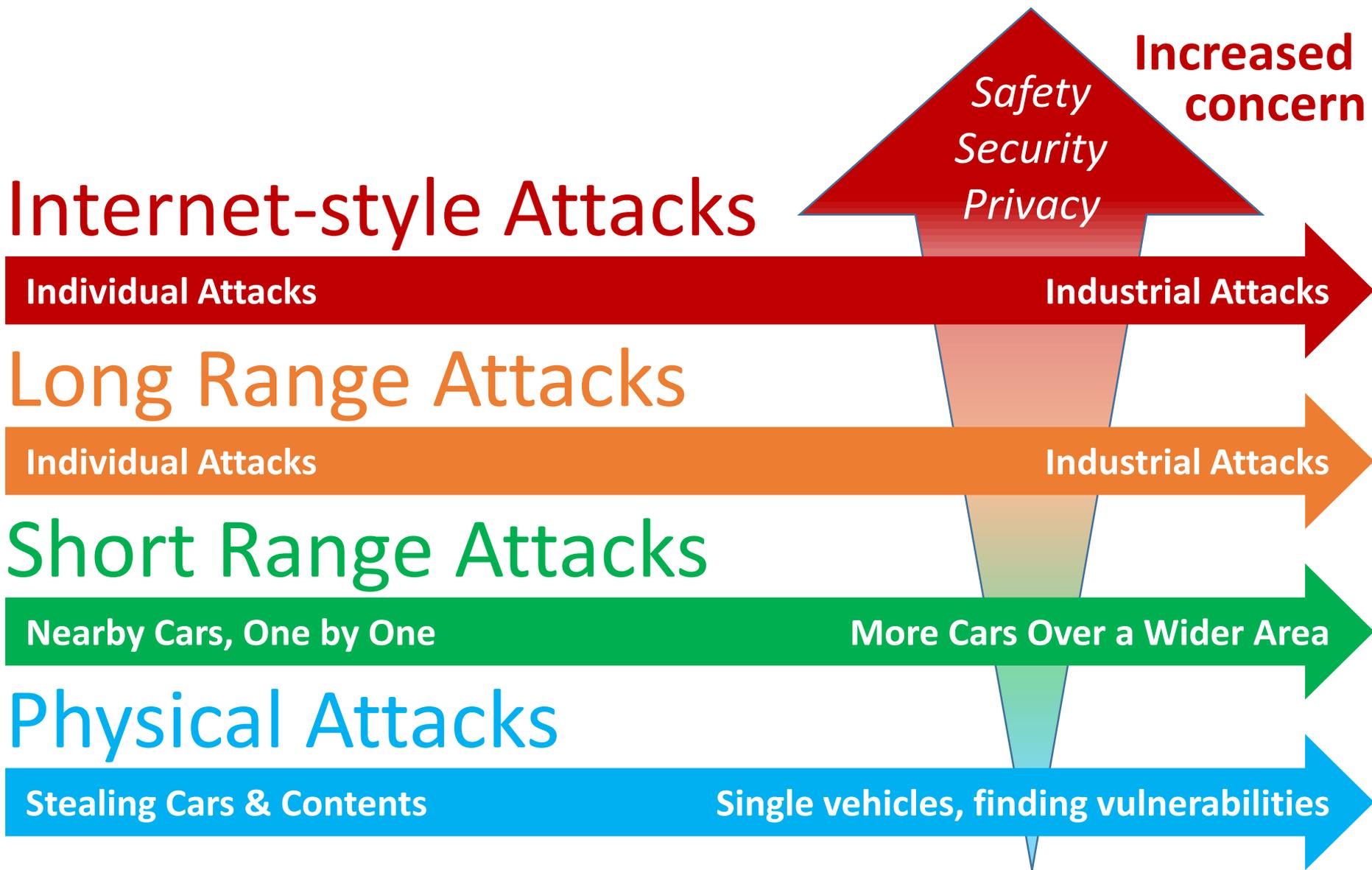
Granularity of map data

Clock accuracy – Tidal Lanes

Differentiation between:

- False Positive
- Denial of Service
- Malicious Attack

Evolution of Automotive Threats



Myth: Hacking is a technical problem, so it needs a technical solution

➤ **Fact: Hacking is a business problem that needs a business solution**



Guidelines,
Processes &
Standards

(alone)



(always)



Success



Understand (remember) the scope of Cyber-security

- Any system
- Any interface
- Any part of the eco-system
- High profile researcher-based hacks are not necessarily representative of real world threats

Security is for life, not just for launch

- Counter-measures must evolve as threats evolve
- OTA updates are a necessity

Sustainable business model for key management infrastructure

- Who pays for a V2X SCMS

Safety and Security (and Privacy) may be a trade-off

- May vary by region

Financial Impact of getting it wrong could be massive

- Corporate Responsibility and Liability will become a key driver
- **Negligence** and **Absolute Liability** will be applied to Connected Cars

V2X

- Significant resources already deployed (financial/intellectual/pilots)
- Key management infrastructures well understood (if undecided)

ADAS/Autonomy

- Progress on sensor fusion and processing algorithms
- Understood that safety needs security (and vice-versa)

Connected Services

- Political will in USA to promote sharing and standards
- Hacks remain 'proof of concept' demonstrations

V2X

- Verification speed vs crypto level
- Sustainable business models for key management infrastructures

ADAS/Autonomy

- Differentiation between false positives, denial of service and malicious hacks

Connected Services

- Attack surfaces still open enabling (relatively) unsophisticated attacks
- Culture of secrecy (source code & algorithms)



Secrecy does not ensure security

- Proprietary solutions are not secure
- The quality of your (supplier) code is the quality of your brand

OEMs will be legally liable for all software in their vehicles

- Independent vulnerability assessments will be vital
- A lack of knowledge or awareness is no defence

Cyber Security intelligence needs to be shared and collaborative

- Cyber threats cut across products and companies
- Cyber threats cut across conventional boundaries, sectors and geographies



A Final Thought...

cars

"There are only two types of **companies:**
those that have been hacked,
and those that will be."

Robert Mueller
FBI Director, 2012

