Trends of Automotive Threats and Attacks

Global Technical & Cybersecurity Advisor
Dennis Kengo Oka
dennis.kengo.oka@iav.jp

GlobalPlatform Cybersecurity Vehicle Forum
May 22, 2025, Tokyo, Japan

Introduction of IAV

Founded

1983

Berlin

Software Systems & Connectivity

Vehicle Solutions & Autonomous Driving

Powertrain Systems

6,600

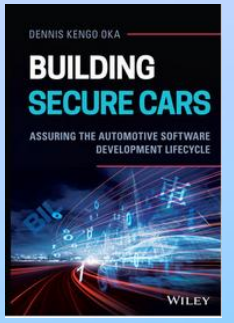
Employees

26

Locations worldwide

Dr. Dennis Kengo Oka

- Started working on automotive security in 2006
- Involved in standardization and best practices activities
- 70+ publications and presentations at events
- Global Technical & Cybersecurity Advisor



Author of books: "*Building Secure Cars: Assuring the Automotive Software Development Lifecycle*" and "*Building Secure Automotive IoT Applications: Developing Robust IoT Solutions for Next-Gen Automotive Software*"

Agenda

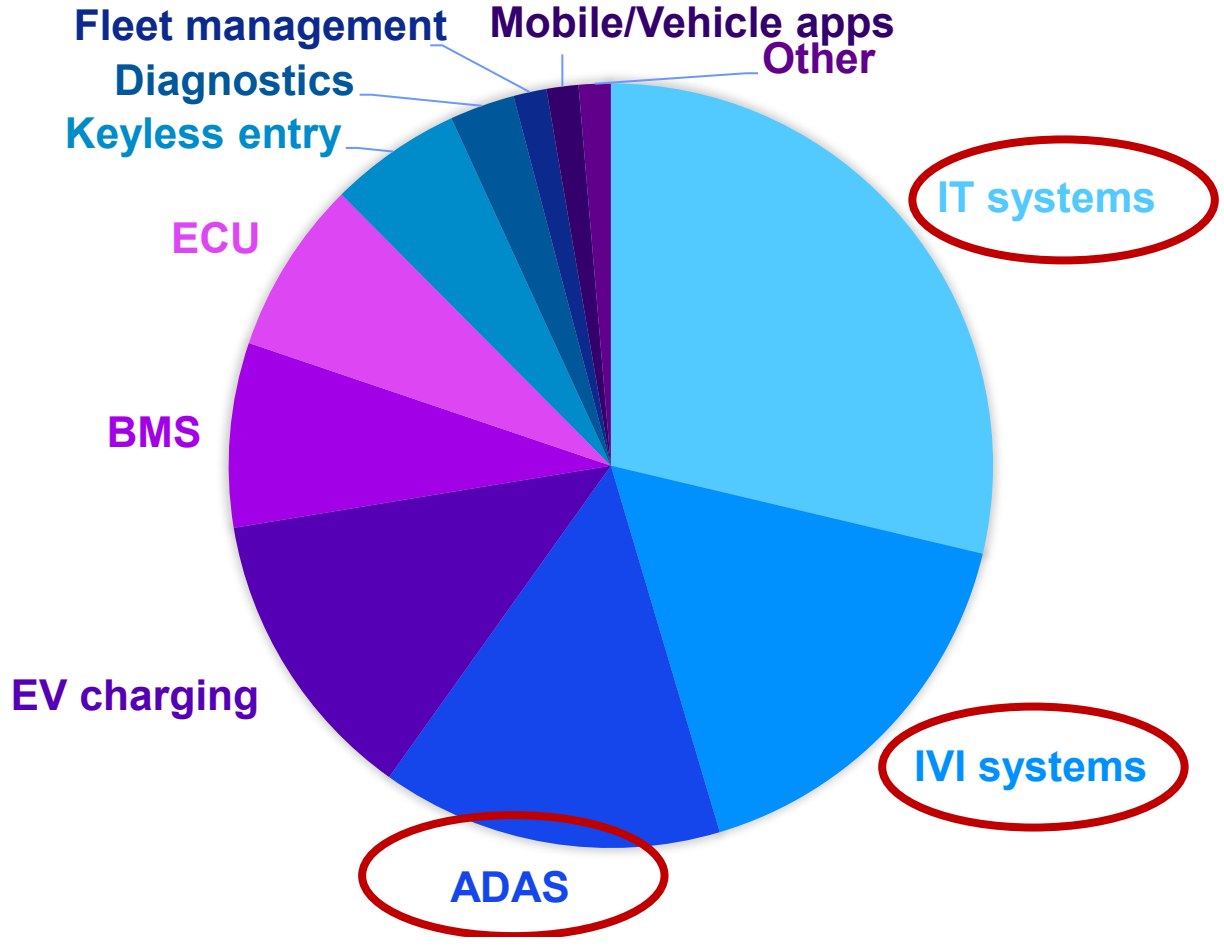

Overview of threats and attacks trends
Review of attack examples

Agenda


Overview of threats and attacks trends
Review of attack examples

ECU: Electronic Control Unit
BMS: Battery Management System
EV: Electric Vehicle
ADAS: Advanced Driver Assistance System
IVI: In-Vehicle Infotainment

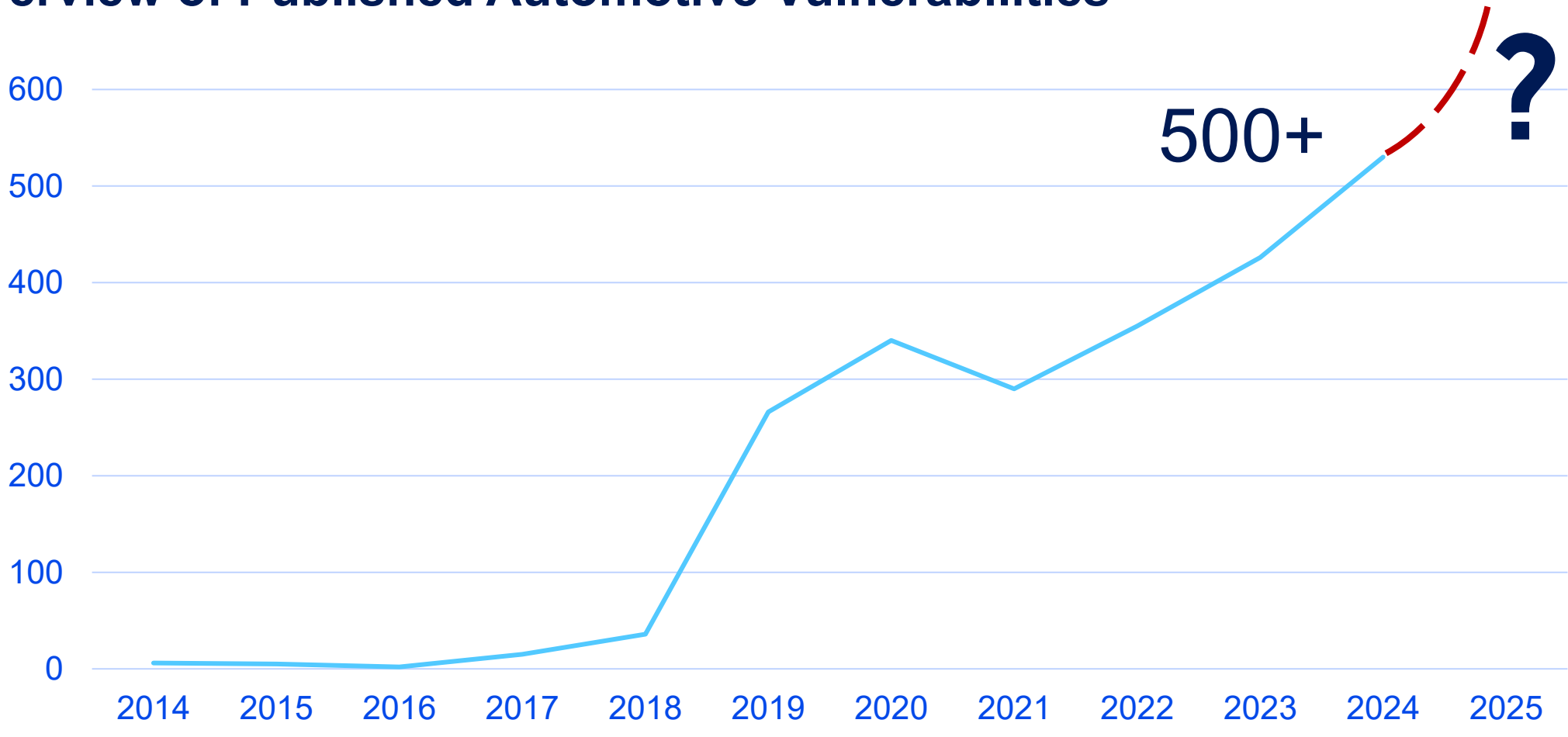
Overview of Automotive Threats in 2024



Incidents targeting IT systems, IVI systems and ADAS were most prevalent

Ref: VicOne 2025 Automotive Cybersecurity Report
VIcOne Automotive Cybersecurity Snapshot

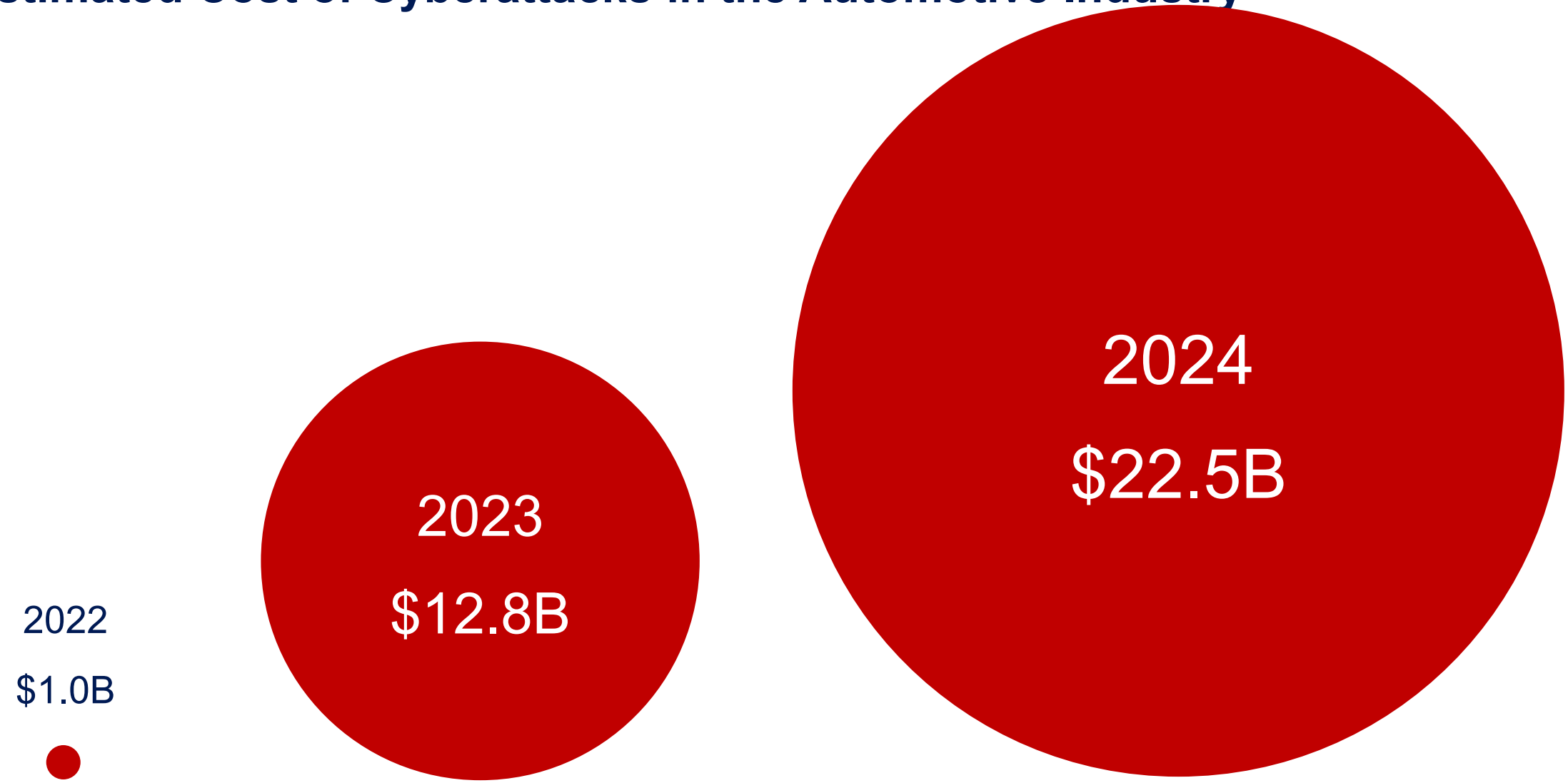
Overview of Published Automotive Vulnerabilities



Increasing number of automotive vulnerabilities published year over year

Ref: VicOne 2025 Automotive Cybersecurity Report
VIcOne Automotive Cybersecurity Snapshot

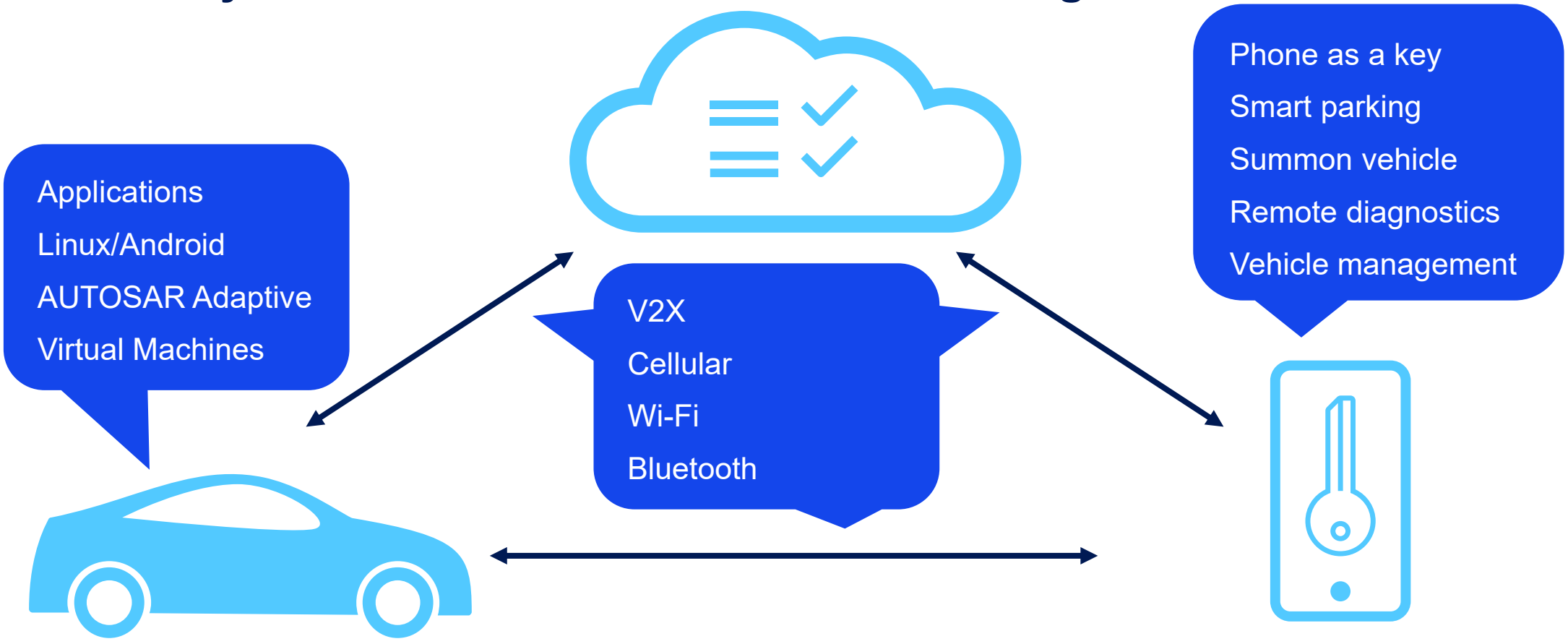
Estimated Cost of Cyberattacks in the Automotive Industry



Ref: VicOne 2025 Automotive Cybersecurity Report
VIcOne Automotive Cybersecurity Snapshot

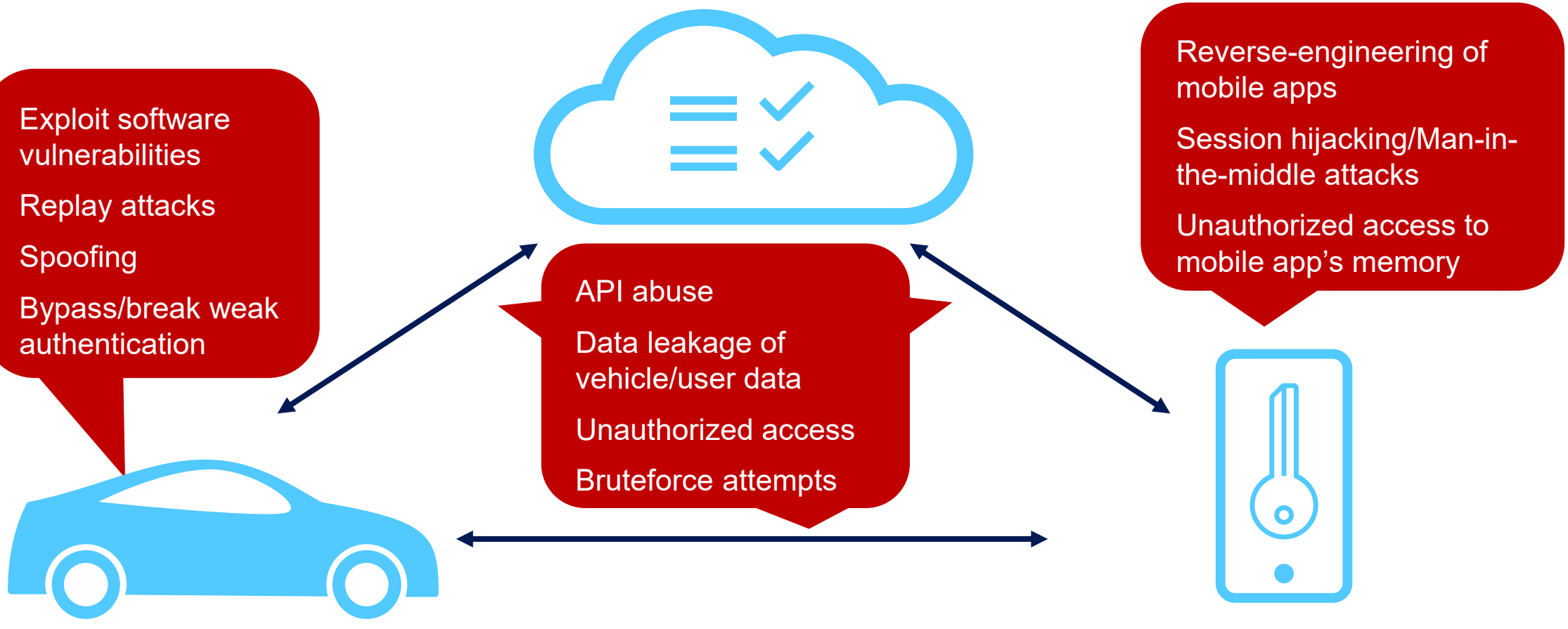
SDV: Software-Defined Vehicle
V2X: Vehicle to X

SDV Ecosystem – New Use Cases and Technologies



Advanced software and increased connectivity to support new SDV use cases

Increased Attack Surface



Advanced software and increased connectivity lead to increased attack surface

Future Technologies – Quantum Computing

Microsoft's Majorana 1 chip carves new path for quantum computing

Written by

Catherine Bolgar

Published

February 19, 2025

Check out the world's first Quantum Operating System

2441 Views | 24 Apr 2025, 06:00 PM | Abhijeet V Singh

Fujitsu and RIKEN develop world-leading 256-qubit superconducting quantum computer

Kawasaki and Wako, Japan, April 22, 2025

New advancements in Quantum Computing

Ref: https://content.techgig.com/technology/the-dawn-of-quantum-computing-introducing-qnodeos-the-first-quantum-operating-system/articleshow/120586133.cms
https://news.microsoft.com/source/features/innovation/microsofts-majorana-1-chip-carves-new-path-for-quantum-computing/
https://www.fujitsu.com/global/about/resources/news/press-releases/2025/0422-01.html

RSA: Rivest Shamir Adleman
ECC: Elliptic Curve Cryptography
AES: Advanced Encryption Standard

Quantum Computing Impact on Cybersecurity

Shor's algorithm

- Can factor large integers exponentially faster than best-known classical algorithms
- Affects: Asymmetric encryption algorithms that rely on the difficulty of factoring large integers or finding discrete logarithms
- Result: Big threat – e.g., RSA and ECC could be completely broken – private keys can be extracted from public keys

Grover's algorithm

- Can speed up bruteforce attacks (but only by a square root)
- Affects: Symmetric encryption algorithms that rely on key size and infeasibility of bruteforcing all possible keys
- Result: Partial threat – e.g., AES-128 would be weakened to half the security (64-bit strength)

Quantum Computing has severe impact on Cybersecurity

PQC Approaches

PQC: Post-Quantum Cryptography
RSA: Rivest Shamir Adleman
ECC: Elliptic Curve Cryptography
ECDSA: Elliptic Curve Digital Signing Algorithm
ECDH: Elliptic Curve Diffie Hellman
AES: Advanced Encryption Standard
SHA: Secure Hash Algorithm
HMAC: Hash-based Message Authentication Code

Traditional Algorithm	Quantum Vulnerability	PQC Approach
RSA	Broken by Shor's algorithm	CRYSTALS-Kyber (key exchange)
ECC	Broken by Shor's algorithm	CRYSTALS-Dilithium (signatures)
AES-128	Grover's algorithm halves security (64 bits)	Use AES-256
SHA-2 (SHA-256)	Grover's algorithm halves preimage resistance (128 bits)	Continue with SHA-2 or use SHA-512 for extra margin
SHA-3-256	Grover's algorithm halves preimage resistance (128 bits)	Continue with SHA-3-256 or use SHA-3-512 for extra margin
HMAC	Depends on underlying hash (SHA-2 or SHA-3)	See above for SHA-2 and SHA-3-256
ChaCha20 (256 bits)	Grover's algorithm halves security (128 bits)	Continue with ChaCha20 (256 bits)

Post Quantum Computing Crypto solutions are needed to address the risks

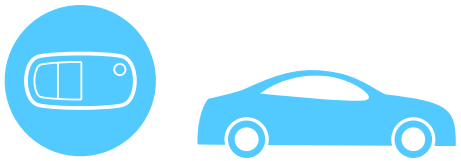
Agenda


Overview of threats and attacks trends
Review of attack examples

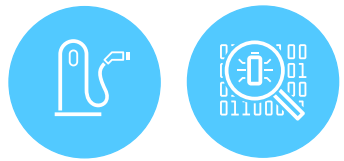
EV: Electric Vehicle
DoS: Denial of Service
IVI: In-Vehicle Infotainment

Examples of Past Attacks

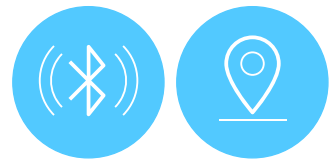
- **Entry point**: Vehicle - key fob
- **Vulnerability**: in the keyless entry system/immobilizer (weak cryptographic authentication)
- Attack device uses specific algorithm and calculates the correct key ⇒ sends to vehicle
- **Impact**: use attack device as key and drive off with target vehicle



- **Entry point**: Physical access to the EV charging station interface
- **Vulnerability**: in firmware (not checking lower bounds) and proprietary communication protocol (allows malformed frames)
- Send custom malformed payloads
- **Impact**: DoS, undefined behavior or command injection

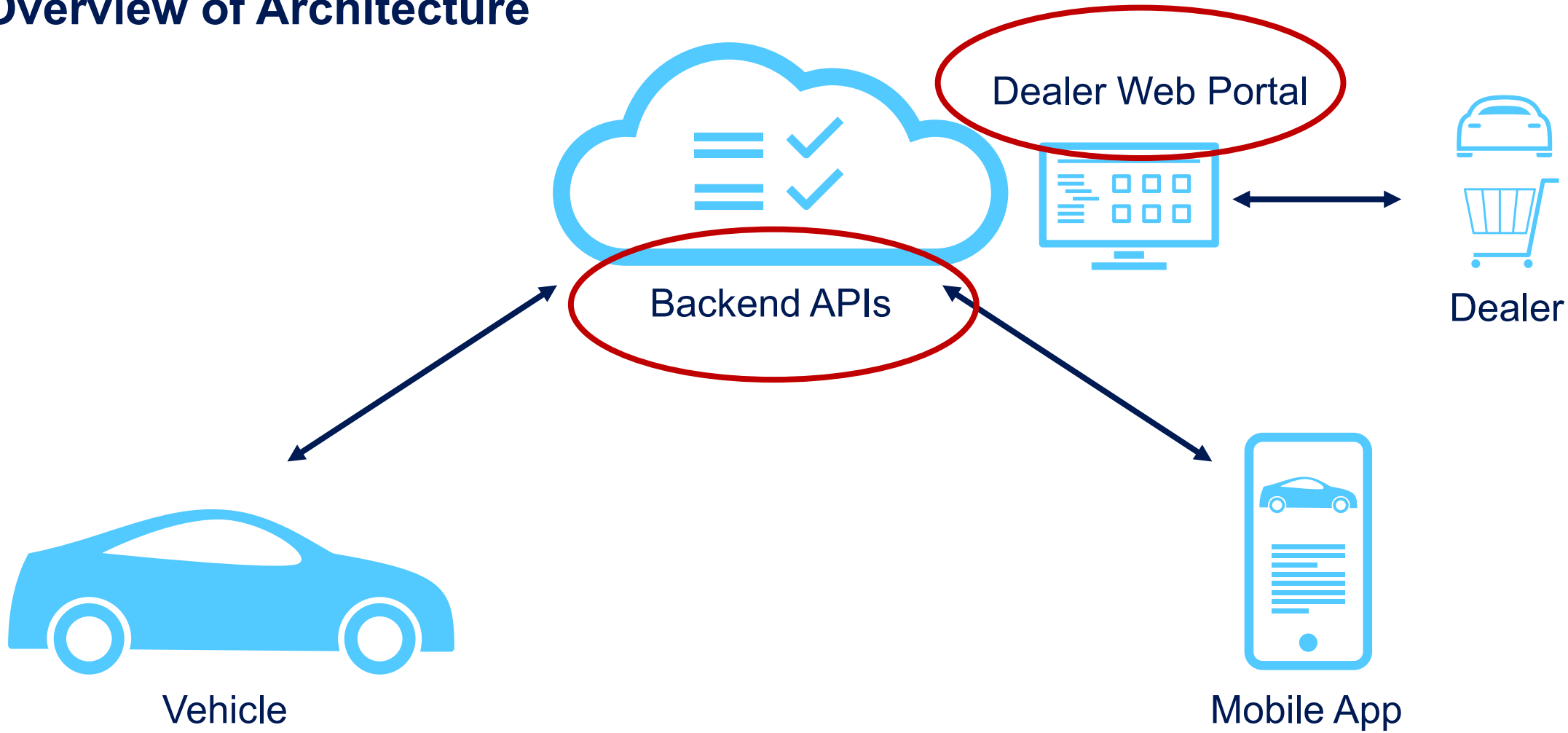


- Entry point: Bluetooth interface on IVI
- **Vulnerability**: in Bluetooth implementation
- Exposed unauthenticated Bluetooth services, firmware allows unsigned code execution
- Inject malware, extract vehicle data
- **Impact**: extract vehicle location data, contact and call history, record microphone audio etc.




Deep Dive

Overview of Architecture



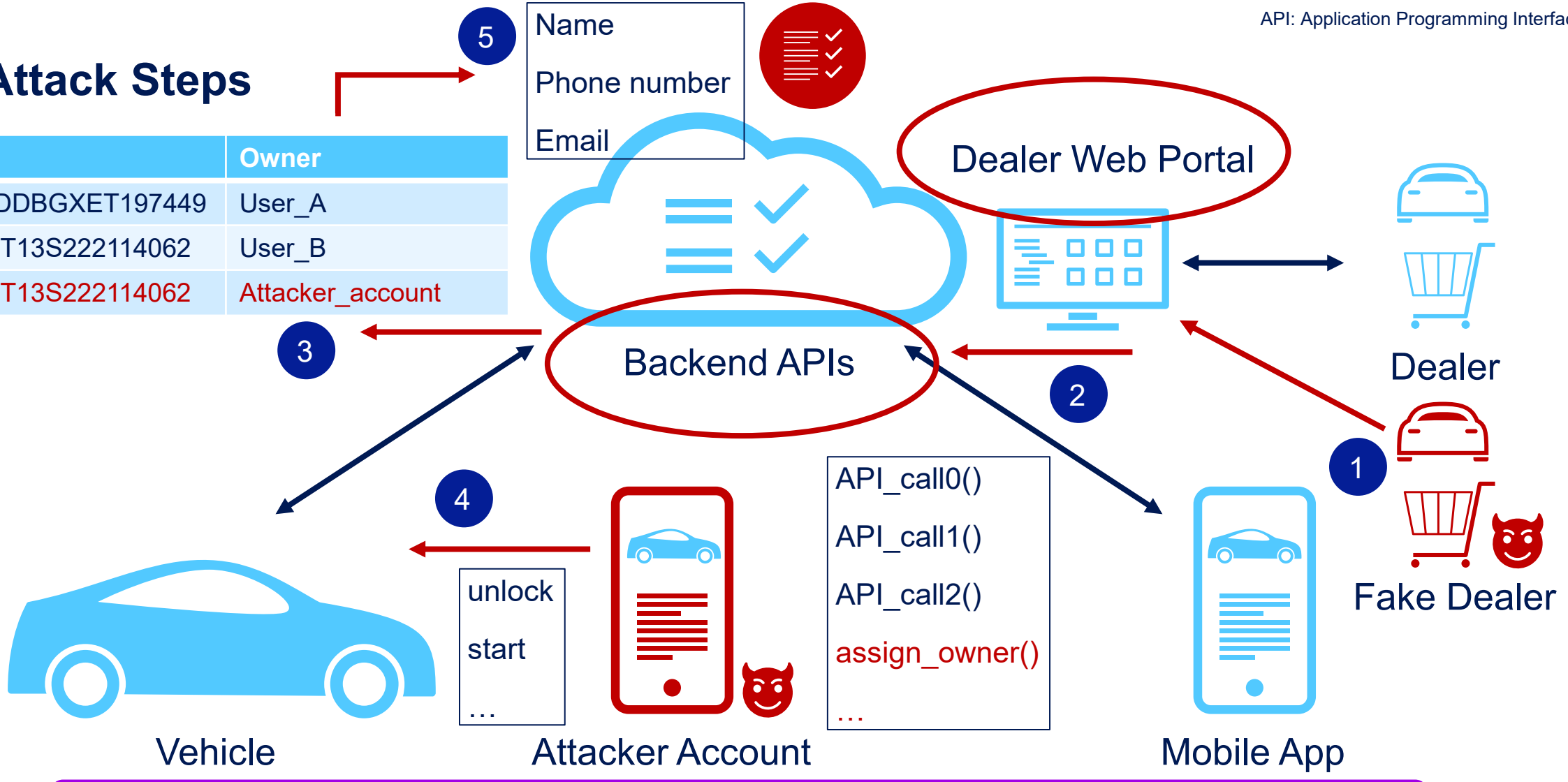
Several different entities involved in order to support the use cases

Weaknesses

No.	Component	Weakness	Results
1.	Dealer Web Portal	No access restriction and no approval process for newly created dealer accounts	Attacker can register as a dealer
2.	Dealer Web Portal	Exposed sensitive functionality via client-side JavaScript	Attacker as fake dealer can call privileged backend APIs
3.	Backend APIs	Missing authorization validation	Attacker can reassign a vehicle without owning it
4.	Backend APIs	No rate limiting	Attacker can brute-force or automate attacks
5.	Backend APIs	Sensitive data exposure	Attacker can extract user details including name, phone number and email address

Attack Steps

VIN	Owner
3C4PDDBGXET197449	User_A
1GHDT13S222114062	User_B
1GHDT13S222114062	Attacker_account



Multiple attacks steps involved to gain access to vehicle control and user data

Summary of the Attack

- An attacker could remotely access and control any vehicle associated with the VIN/license plate:
  - unlock the car
  - start the car
  - track its location and access location history

- An attacker could remotely extract information associated with the VIN/license plate:
  - Full name of vehicle owner
  - Mobile phone number
  - Email address
  - Vehicle information (VIN, license plate number, make, model, year)

Attacker could gain control of vehicles and extract personal information

Disclosure & Remediation

- Discovery: June 11, 2024, by security researchers

- Reported to OEM: Immediately upon discovery

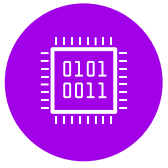
- Patch Released: August 14, 2024

Enable vulnerability disclosure program and remediate quickly

SDV: Software-Defined Vehicle
PQC: Post-Quantum Cryptography

Call to Action

- Stay up-to-date on automotive risks for the SDV ecosystem



- Get ready for PQC

- Apply best practices for secure end-to-end development lifecycle
  - Secure design and development
  - Security testing
  - Software updates/patches

Contact

Dr. Dennis Kengo Oka
IAV Co., Ltd.
dennis.kengo.oka@iav.jp
www.iav.com