Mitigating the Risks of Cybersecurity Threats to the Transportation System

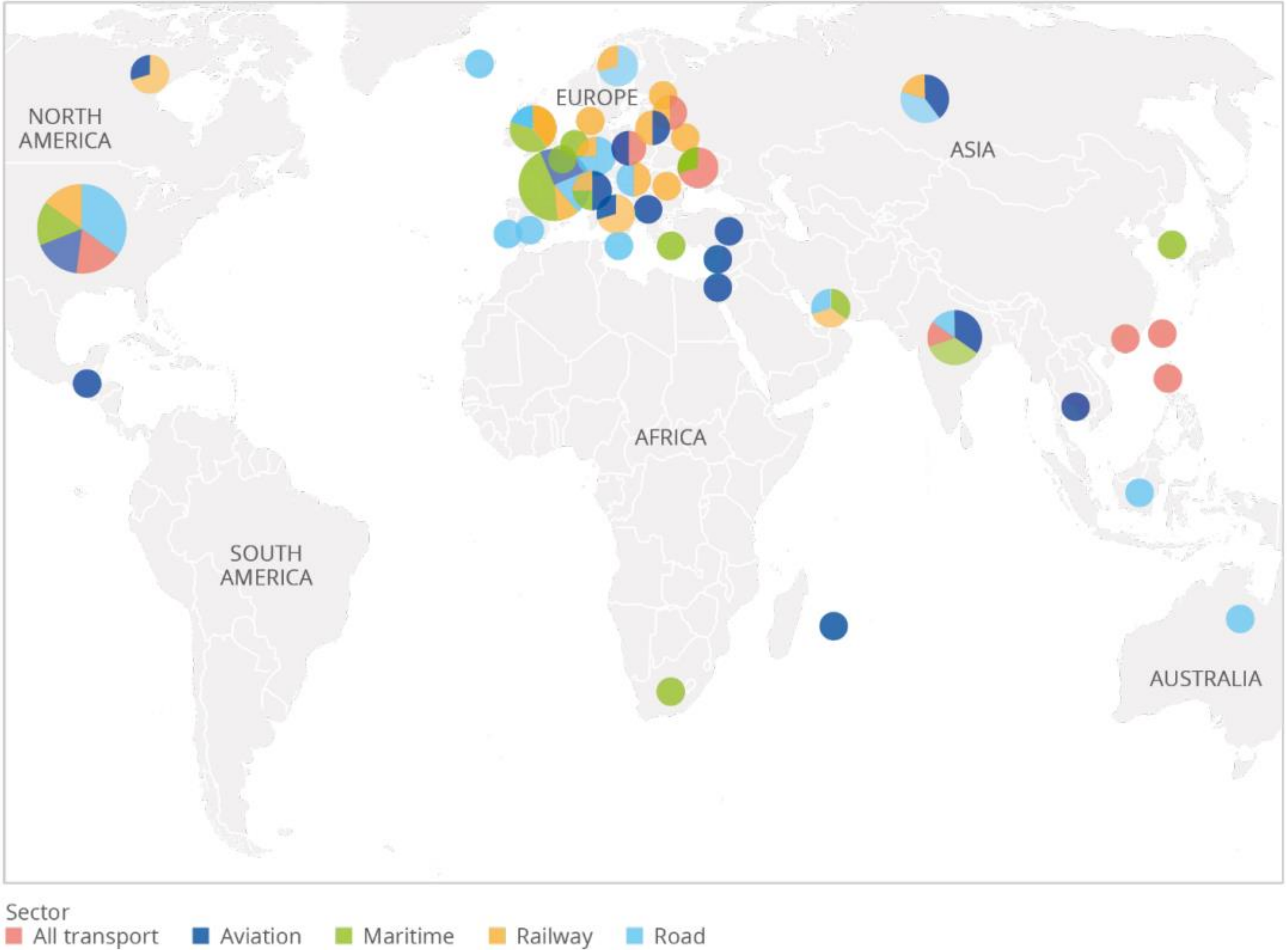
2023 Southeast Wisconsin Transportation Symposium

Zhen Zeng, Ph.D.
Assistant Professor
Department of Computer Science
zhenzeng@uwm.edu

UNIVERSITY of WISCONSIN
UWMILWAUKEE

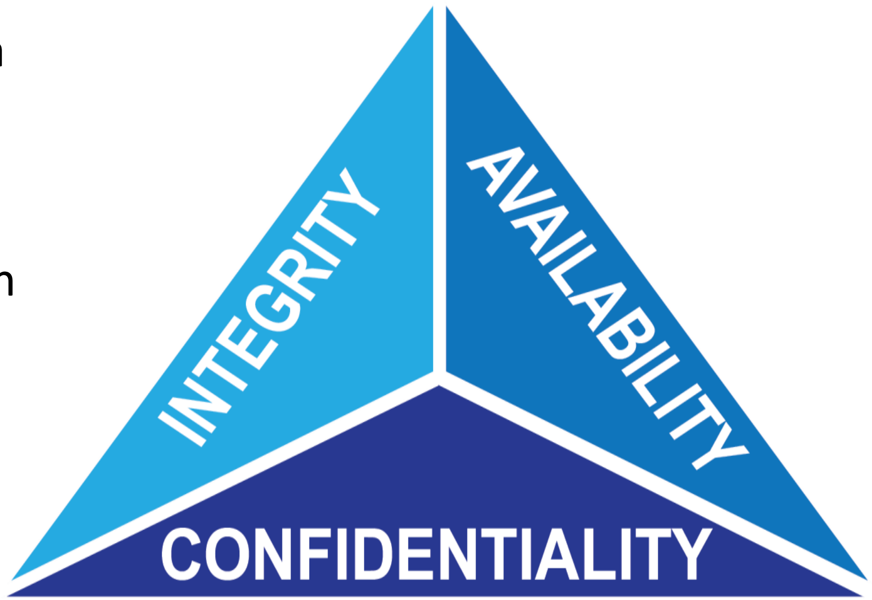
College of
Engineering & Applied Science

Cybersecurity Threats in Transportation Sector (Jan 2021- Oct 2022)



European Union Agency for Cybersecurity (ENISA) report (2023)

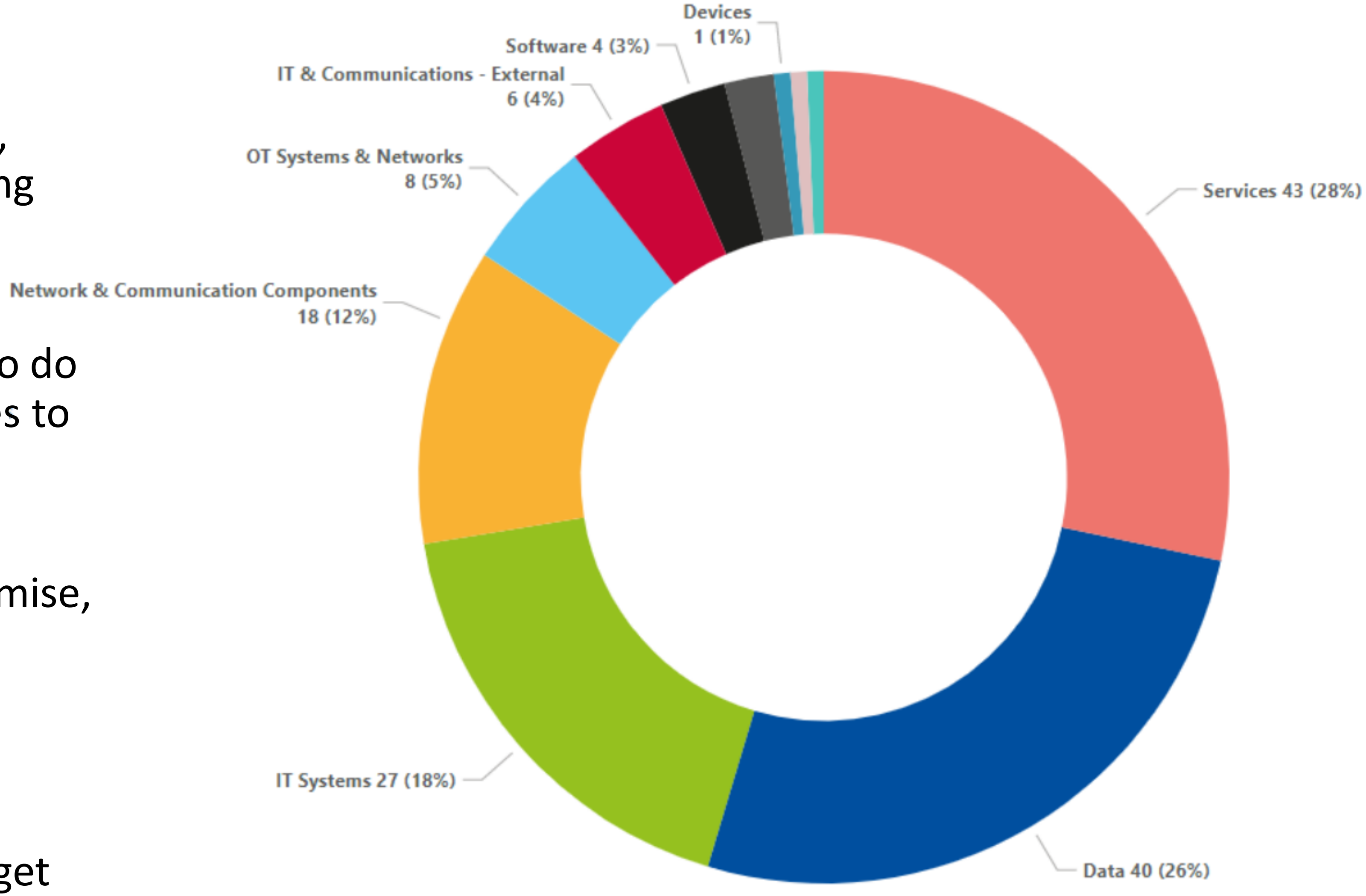
- Prime threats affecting the transportation sector
  - Ransomware attacks (38%)
    - Threat actors take control of a target’s assets and demand a ransom in exchange for the return of the asset’s availability
  - Threats against data (30%)
    - Data breach, data leaks. Threat actors gain unauthorized access and disclosure, and manipulate data to interfere with the behavior of system.
  - Malware
    - Malicious code (viruses, worms, trojan horses…)
  - Denial-of-service attacks
    - Attacks target system and data availability.
  - Phishing/spear phishing;
    - Attackers deceive people into revealing sensitive information or installing malware.
  - Supply-chain attacks.
    - Attacks target both the supplier and the customer.
    - Attacks to suppliers that caused disruptions or losses to entities in the transportation sector.



The CIA triad in Cybersecurity

https://www.enisa.europa.eu/news/understanding-cyber-threats-in-transport

- Threat actors
  - Cybercriminals
    - Primary motive is financial gain, often stealing data or demanding ransom
  - Hackers-for-hire
    - Sell their services to people who do not have the skills or capabilities to do so
  - State-sponsored
    - Target organizations to compromise, steal, change, or destroy information.
  - Hacktivists
    - Are politically, socially, or ideologically motivated and target victims for publicity or to effect change.



Affected Assets

https://www.enisa.europa.eu/news/understanding-cyber-threats-in-transport

- Cyberattacks in road sector

  - *September 2021*, attackers impersonated the US Department of Transportation in a two-day phishing scam.

  - *February 2022*, Kia Motors America, ransomware attack, demanding USD 20 million for a decrypter and to not leak stolen data.

  - *March 2022*, Japanese car parts giant Denso, network attack, 1.4 terabytes of data leakage.

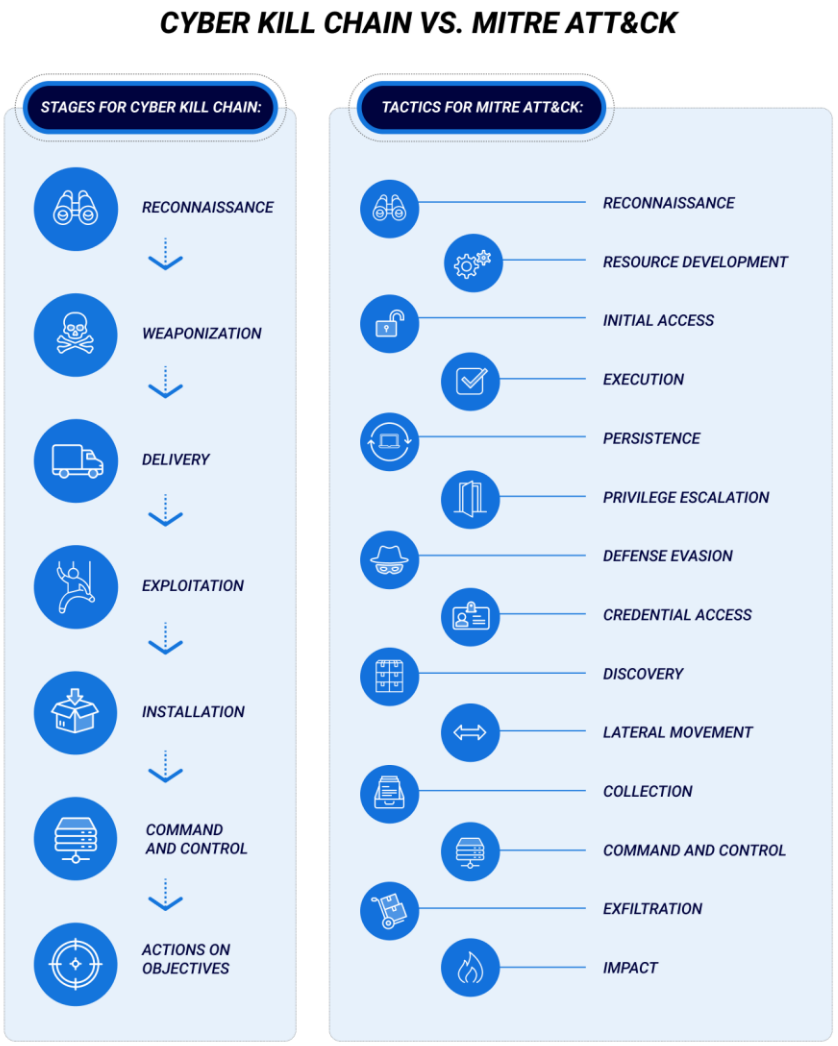
  - *May 2022*, AGCO Corporation sites in China, France, Germany and the US, ransomware attack, making servers inaccessible and halting production for 2 days

  - *June 2022*, US subsidiary of Nichirin, ransomware attack, shut down some production control systems and switch to manual processes.

  - *September 2022*, Microsoft365 phishing attacks impersonate US government agencies including the Department of Transportation.

  … …

Understanding Cyberattack



CYBER KILL CHAIN VS. MITRE ATT&CK

STAGES FOR CYBER KILL CHAIN:

- RECONNAISSANCE
- WEAPONIZATION
- DELIVERY
- EXPLOITATION
- INSTALLATION
- COMMAND AND CONTROL
- ACTIONS ON OBJECTIVES

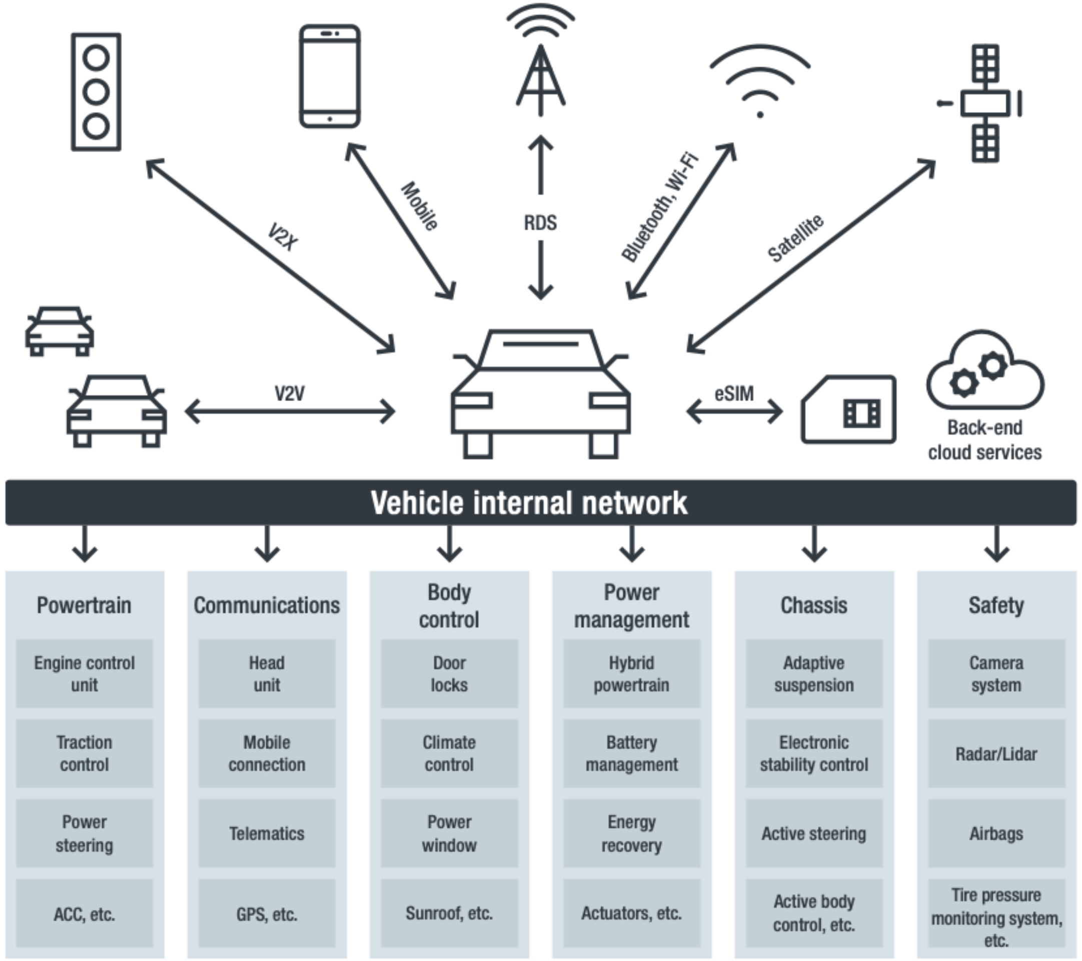
TACTICS FOR MITRE ATT&CK:

- RECONNAISSANCE
- RESOURCE DEVELOPMENT
- INITIAL ACCESS
- EXECUTION
- PERSISTENCE
- PRIVILEGE ESCALATION
- DEFENSE EVASION
- CREDENTIAL ACCESS
- DISCOVERY
- LATERAL MOVEMENT
- COLLECTION
- COMMAND AND CONTROL
- EXFILTRATION
- IMPACT

- Cyber Kill Chain:
  - A cyberattack framework developed by Lockheed Martin and released in 2011
  - Steps of a cyberattack
- MITRE ATT&CK :
  - An open knowledge base of cybersecurity information first released by the MITRE Corporation in 2018
  - Adversarial tactics, techniques, and procedures.

https://www.blackberry.com/us/en/solutions/endpoint-security/mitre-attack/mitre-attack-vs-cyber-kill-chain

Case Study on Remote Attacks

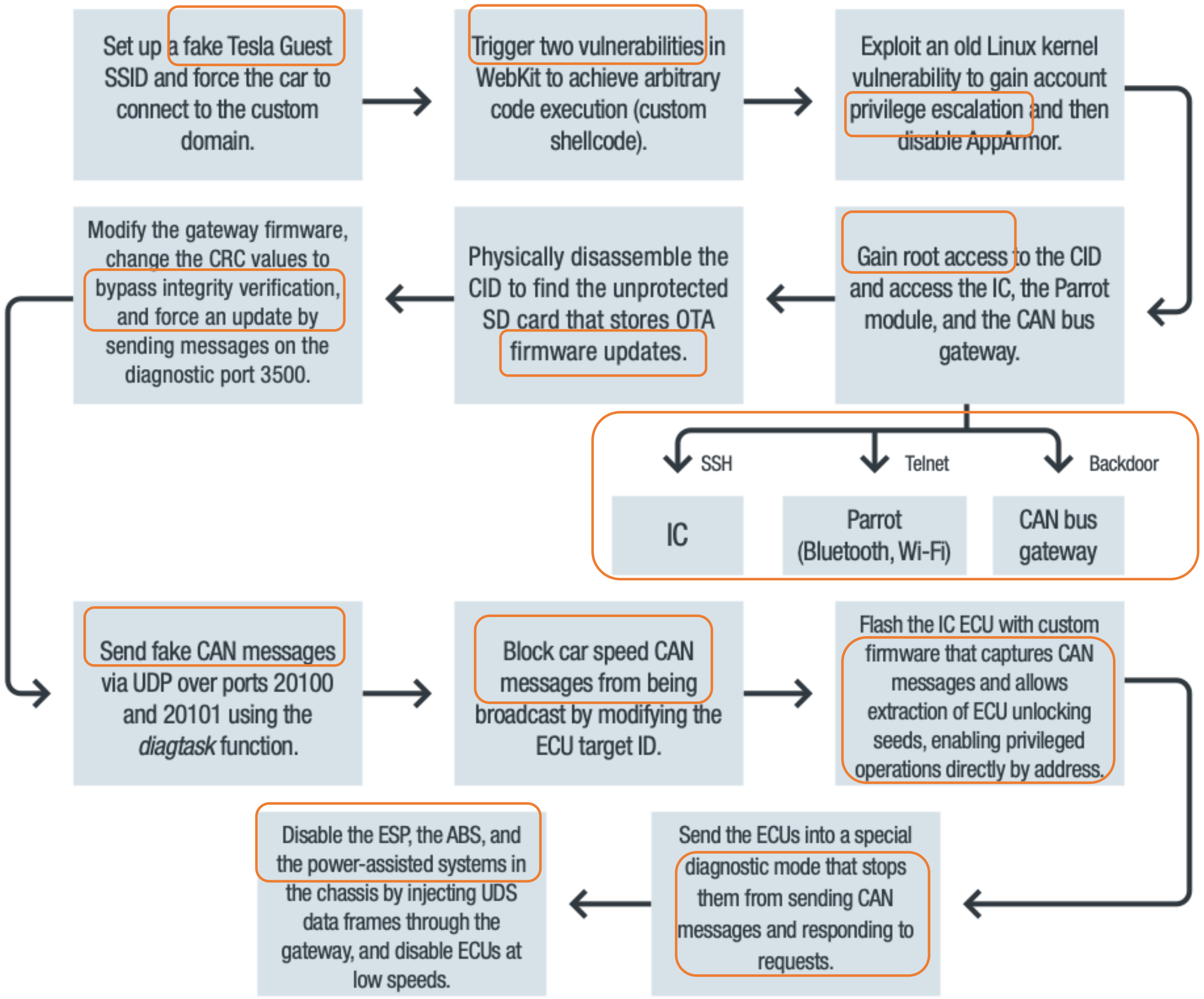


Powertrain	Communications	Body control	Power management	Chassis	Safety
Engine control unit	Head unit	Door locks	Hybrid powertrain	Adaptive suspension	Camera system
Traction control	Mobile connection	Climate control	Battery management	Electronic stability control	Radar/Lidar
Power steering	Telematics	Power window	Energy recovery	Active steering	Airbags
ACC, etc.	GPS, etc.	Sunroof, etc.	Actuators, etc.	Active body control, etc.	Tire pressure monitoring system, etc.

In 2015, Jeep remote attack leads to recall of 1.4 million Chrysler vehicles

The technologies and functionalities that make up the internal network of a connected car

https://www.trendmicro.com



Set up a fake Tesla Guest SSID and force the car to connect to the custom domain.

Trigger two vulnerabilities in WebKit to achieve arbitrary code execution (custom shellcode).

Exploit an old Linux kernel vulnerability to gain account privilege escalation and then disable AppArmor.

Gain root access to the CID and access the IC, the Parrot module, and the CAN bus gateway.

SSH: IC

Telnet: Parrot (Bluetooth, Wi-Fi)

Backdoor: CAN bus gateway

Physically disassemble the CID to find the unprotected SD card that stores OTA firmware updates.

Modify the gateway firmware, change the CRC values to bypass integrity verification, and force an update by sending messages on the diagnostic port 3500.

Send fake CAN messages via UDP over ports 20100 and 20101 using the *diagtask* function.

Block car speed CAN messages from being broadcast by modifying the ECU target ID.

Flash the IC ECU with custom firmware that captures CAN messages and allows extraction of ECU unlocking seeds, enabling privileged operations directly by address.

Send the ECUs into a special diagnostic mode that stops them from sending CAN messages and responding to requests.

Disable the ESP, the ABS, and the power-assisted systems in the chassis by injecting UDS data frames through the gateway, and disable ECUs at low speeds.

INTEGRITY
AVAILABILITY
CONFIDENTIALITY

The CIA triad

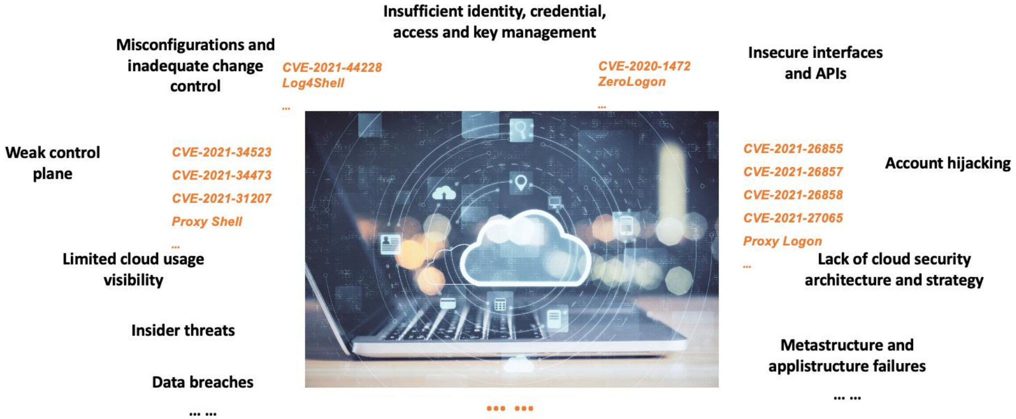
The Attack Chain of Tesla Model S Remote Attack identified by Cybersecurity Researchers in 2016

https://www.trendmicro.com

Securing Systems

- Threat modeling analysis
    - Threat model, a structured representation of all the information that affects the security of an asset.
  - To identify, communicate, and understand threats and mitigation within the context of protecting assets.
  - Can be applied to a wide range of things, e.g., software, applications, systems, networks, IoT devices, and business processes.

- Vulnerability management
    - Vulnerability, weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
  - A process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems.
  - Contains several steps for vulnerability
    - scan,
    - risk assessment,
    - prioritization,
    - Mitigation,
    - Continuous management.



Challenges of vulnerability management

- Vulnerabilities are numerous.
- Average time from vulnerability disclosure to exploitation continues to drop.
- Common Vulnerability Scoring System (CVSS) represents technical severity.
- More challenges for vulnerability management in cloud environments.

… …

Vulnerability

Less than 25% of vulnerabilities in the system can be patched within 30 days

-- Verizon Data Breach Report (2021)

How to efficiently and effectively fix high-risk vulnerabilities?

•Zeng, Z., etc. 2021. LICALITY—Likelihood and Criticality: Vulnerability Risk Prioritization Through Logical Reasoning and Deep Learning. *IEEE Transactions on Network and Service Management (TNSM)*.

•Zeng, Z., etc., 2023. ILLATION: Improving Vulnerability Risk Prioritization By Learning From Network. *IEEE Transactions on Dependable and Secure Computing (TDSC)*.

Some Commercial Tools

Nessus N ™
OpenVAS
Open Vulnerability Assessment Scanner
WIRESHARK
NMAP
VulnDB
VULNERS
COM
vFeed
TREND MICRO ™
Qualys.
tenable
RAPID7
tripwire

• • • • • •

Thank you!

Defender vs Attacker