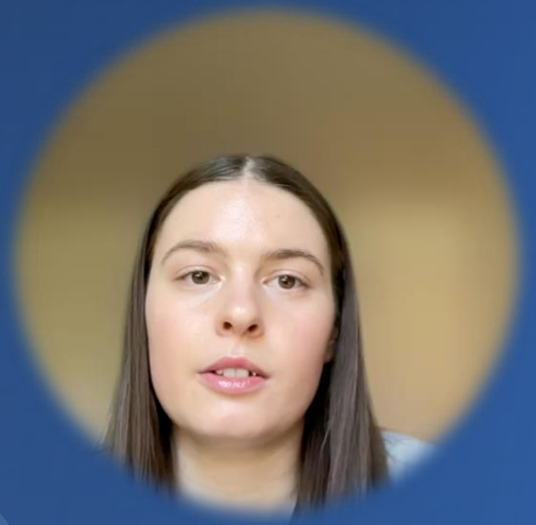
FLINDERS UNIVERSITY

ANALYSING CYBER CHALLENGES: TOWARDS ENHANCING AUTONOMOUS VEHICLE CYBERSECURITY RESILIENCE



Tanisha Soldini, Ass. Prof. Elena Sitnikova, Prof. Karl Sammut

PRESENTER: TANISHA SOLDINI, PHD STUDENT
COLLEGE OF SCIENCE AND ENGINEERING, FLINDERS UNIVERSITY
TANISHAROSE.SOLDINI@FLINDERS.EDU.AU

IARIA

FLINDERS UNIVERSITY

PRESENTER

Tanisha Soldini

- Graduate of Master of Engineering (Electronics)/Bachelor of Engineering (Robotics) (Honours) in 2024.

- PhD Student currently studying at Flinders University.

- Skills:
  - Knowledge in multiple programming languages.
  - Circuit design.
  - Control theory.
  - Simulation and modeling.
  - Interdisciplinary collaboration between engineering and cybersecurity.

CURRENT STATE OF AUTONOMOUS VEHICLE ADOPTION

- AV adoption has the potential to enhance efficiency, reduce costs, lower emissions, and improve mobility and accessibility.
- Interconnected systems and communication protocols increase the potential attack surface.
- Compromised safety, breaches of information, financial losses, and damage to reputation.

IMPORTANCE OF CYBERSECURITY IN AV ADOPTION

1 2 3 4 5 6

1

01

ECONOMIC IMPACT

- AV adoption may disrupt traditional jobs in trucking and taxi services, but it also opens opportunities in cybersecurity, software development, and AV maintenance.

- Enhanced security can reduce accident-related costs and insurance premiums, benefiting both individuals and the economy.

2 3 4 5 6

1 2

02

SAFETY OF OCCUPANTS AND PEDESTRIANS

- Ensuring safety is paramount for public acceptance.
- AVs must effectively detect and avoid collisions with pedestrians, cyclists, and other vehicles.
- Ethical programming for unavoidable accidents is crucial, impacting public trust in AV safety.

3 4 5 6

03

PRIVACY CONCERNS

- AVs collect extensive data on users and surroundings. Protecting this data is essential for maintaining user trust and complying with data protection regulations.
- Safeguarding against unauthorized access to location data and personal information is critical.

1 2 3 4

04

SYSTEM INTEGRITY

- Security breaches and perceived risks can hinder public acceptance.
- Transparent safety measures, reliable testing, and positive early adopter experiences are key to building trust and encouraging broader adoption.

5 6

1 2 3 4 5

05

OPERATIONAL STABILITY

- Strong cybersecurity measures are needed to prevent hacks that could disrupt vehicle control or navigation.
- Securing software updates, protecting against malware, and ensuring safe communication with infrastructure are vital for operational stability.

6

123456

06

TRUST AND ADOPTION

- Securing the complex networks of sensors, processors, and actuators is essential.
- Redundancy, fail-safe mechanisms, and rigorous testing are necessary to maintain system integrity and public confidence.

GAPS IN EXISTING RESEARCH

Research Questions

GAPS IN EXISTING RESEARCH

Research Questions

What types of cyber-attacks are most relevant to AV systems, and how can they be categorized?

What are the effective mitigation strategies for these attacks, and how can they be systematically classified?

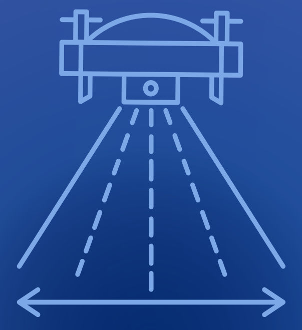
NEED FOR A COMPREHENSIVE TAXONOMY

01. ORGANISING AND CATEGORISES THREATS

02. FACILITATING TARGETED SOLUTIONS

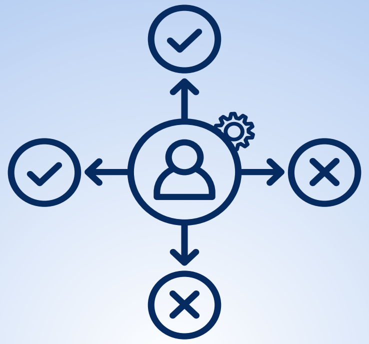
ARCHITECTURE OF AUTONOMOUS VEHCILES

01. SENSOR AND PERCEPTION INTEGRATION



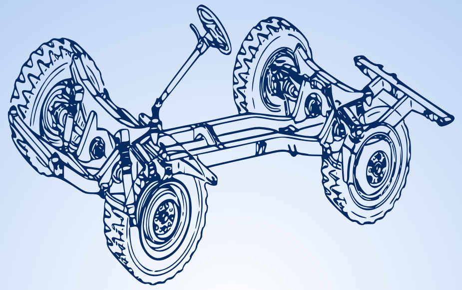
AVs use various sensors—Radar, LiDAR, Cameras, and GPS—to understand their surroundings and determine location.

02. DECISION AND CONTROL



Sensor data is processed for decision-making, such as planning routes, avoiding obstacles, and controlling vehicle movement.

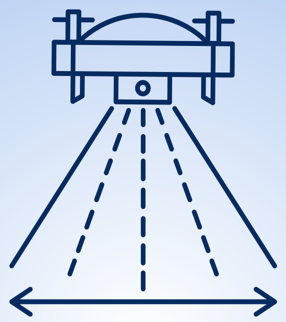
03. CHASSIS



The chassis interfaces with the decision and control system to manage the vehicle's mechanical components

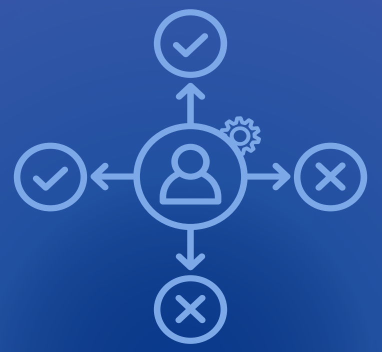
ARCHITECTURE OF AUTONOMOUS VEHCILES

01. SENSOR AND PERCEPTION INTEGRATION



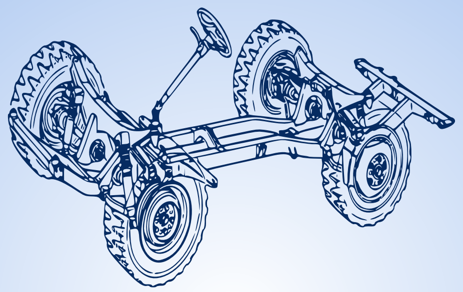
AVs use various sensors—Radar, LiDAR, Cameras, and GPS—to understand their surroundings and determine location.

02. DECISION AND CONTROL



Sensor data is processed for decision-making, such as planning routes, avoiding obstacles, and controlling vehicle movement.

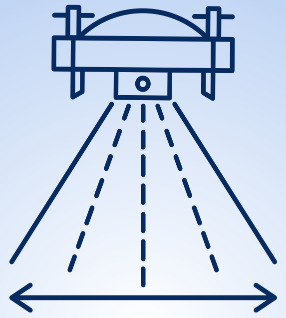
03. CHASSIS



The chassis interfaces with the decision and control system to manage the vehicle's mechanical components

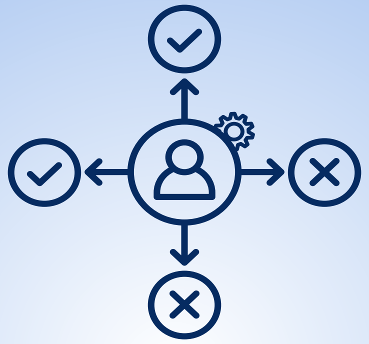
ARCHITECTURE OF AUTONOMOUS VEHCILES

01. SENSOR AND PERCEPTION INTEGRATION



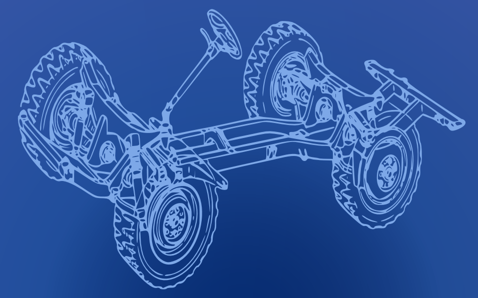
AVs use various sensors—Radar, LiDAR, Cameras, and GPS—to understand their surroundings and determine location.

02. DECISION AND CONTROL



Sensor data is processed for decision-making, such as planning routes, avoiding obstacles, and controlling vehicle movement.

03. CHASSIS



The chassis interfaces with the decision and control system to manage the vehicle's mechanical components

LEVEL OF AUTONOMY

00.

ALL TASKS ACCOMPLISHED BY HUMAN DRIVERS.

01.

HUMAN DRIVER CONTROLS THE VEHICLE, AUTOMATION SYSTEMS CAN ASSIST.

02.

HUMAN DRIVER CONTROLS DRIVING PROCESS AND MONITORS THE ENVIRONMENTS WITH AUTOMATED FUNCTIONS APPLIED.

03.

AUTOMATED VEHICLE WITH HUMAN OPERATOR PREPARED TO ASSUME COMMAND OF THE VEHICLE AT ANY INSTANCE.

04.

UNDER SPECIFIC CONDITIONS, AUTOMATED DRIVING OCCURS, OTHERWISE THE OPERATOR CAN ASSUME CONTROL OF THE VEHICLE.

05.

UNDER ALL CONDITIONS, AUTOMATED DRIVING OCCURS, AND THE OPERATOR CAN TAKE CONTROL OF THE VEHICLE.

CYBER ATTACKS AND TARGETED COMPONENTS

01.

02.

03.

04.

05.

01.

02.

03.

04.

05.

REMOTE ACCESS AND CONTROL

Exploitation of electronic control systems, gaining unauthorised access and critical functions control.

01.

02.

SENSOR MANIPULATION

Attacking sensors (e.g., spoofing or jamming) to mislead the AV's perception and decision-making, which can lead to hazardous driving.

03.

04.

05.

01.

02.

03.

WIRELESS NETWORKS

Vulnerabilities in vehicle-to-vehicle (V2V), vehicle-to-network (V2N), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) communications can be exploited to disrupt operations or inject false data.

04.

05.

01.

02.

03.

04.

SOFTWARE VULNERABILITIES

Exploiting software flaws or malware, such as ransomware, to disrupt AV operations or extort users.

05.

01.

02.

03.

04.

05.

HARDWARE VULNERABILITIES

Hardware components, such as Electronic Control Units (ECUs), On-Board Diagnostic Port (OBD) and Controller Area Network (CAN), can pose potential weaknesses to their physical components and systems. These may be exploited through tampering and unauthorised access.

01.

02.

03.

04.

05.

MOTIVATIONS AND PERPETRATORS BEHIND CYBER ATTACKS

01. OPERATIONAL DISRUPTIONS

Compromises critical AV components that are essential for driving functionality, rendering autonomous driving inoperative.

02. GAINING VEHICLE CONTROL

Allows attackers to manipulate critical vehicular functionalities, such as route deviation, emergency braking, and speed modulation.

03. DATA THEFT

Stealing data from AV systems, potentially fueling subsequent cyber-attacks.

CYBER ATTACK *Classification*

INFECTION CYBER ATTACKS

SERVICE BASED CYBER ATTACKS

MAN-IN-THE-MIDDLE CYBER ATTACKS

IDENTITY BASED CYBER ATTACKS

DATA PRIVACY CYBER ATTACKS

TAMPERING CYBER ATTACKS

SOFTWARE BASED CYBER ATTACKS

CYBER ATTACK
Classification

INFECTION CYBER ATTACKS

SERVICE BASED CYBER ATTACKS

MAN-IN-THE-MIDDLE CYBER ATTACKS

IDENTITY BASED CYBER ATTACKS

DATA PRIVACY CYBER ATTACKS

TAMPERING CYBER ATTACKS

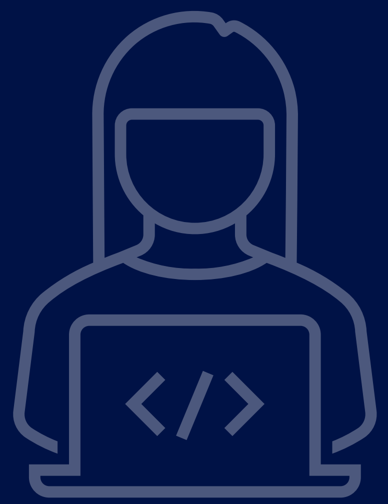
SOFTWARE BASED CYBER ATTACKS

MAN-IN-THE-MIDDLE CYBER ATTACKS

MAN-IN-THE-MIDDLE CYBER ATTACKS

MITM attacks occur when attackers intercept and alter communications between two components, compromising the integrity and confidentiality of the data exchanged.

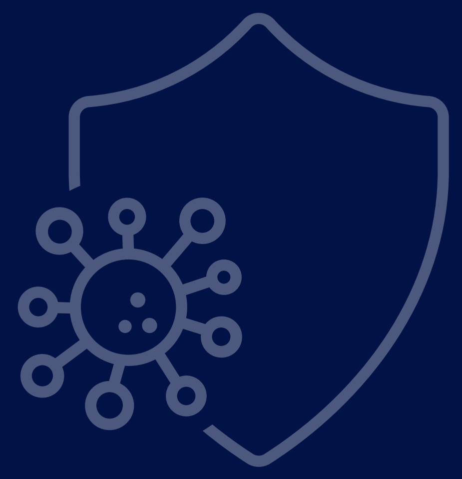
Methods include intercepting and tampering with vehicle communications, impersonating legitimate entities, exploiting wireless interfaces, rerouting messages and attacking dynamic rerouting.



INFECTION CYBER ATTACKS

INFECTION CYBER ATTACKS

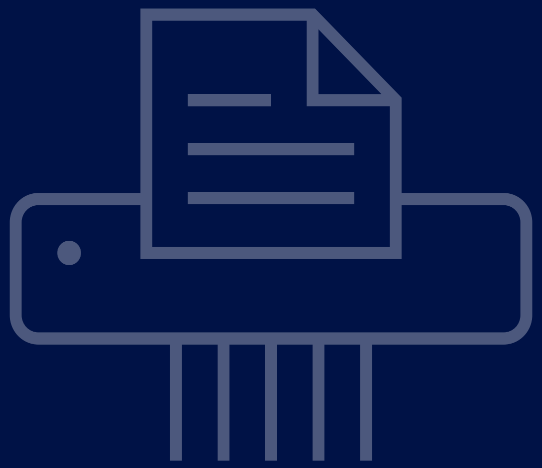
Infection attacks involve injecting malicious code into a vehicle’s systems, which can potentially compromise its functionality and safety. Methods include exploiting software vulnerabilities, violating wireless interfaces, supply chain attacks, infecting removable media, and compromising backend systems.



TAMPERING CYBER ATTACKS

TAMPERING CYBER ATTACKS

Unauthorized manipulation of data, software, or hardware, including sensor data spoofing, software tampering, or physical interference.



IDENTITY BASED CYBER ATTACKS

IDENTITY BASED CYBER ATTACKS

Spoofing: Feeding false information to disrupt sensor or system data.

Impersonation: Disguising as legitimate entities to access or influence systems.

Sybil Attacks: Creating multiple fake identities to disrupt operations.

Replay Attacks: Replaying valid transmissions to bypass authentication.

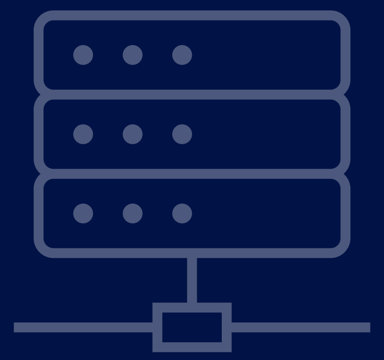
SERVICE BASED CYBER ATTACKS

SERVICE BASED CYBER ATTACKS

Denial of Service (DoS) / Distributed DoS (DDoS): Overwhelm systems with excessive data to impair operations.

Jamming: Interfere with wireless communications.

Routing Attacks: Disrupt routing protocols to cause network instability.



SOFTWARE BASED CYBER ATTACKS

SOFTWARE BASED CYBER ATTACKS

Introduces malicious code to compromise systems. Methods include exploiting software vulnerabilities, compromising wireless interfaces, supply chain attacks, removable media infection, and compromising backend systems.

DATA PRIVACY CYBER ATTACKS

DATA PRIVACY CYBER ATTACKS

Location Trailing: Unauthorized monitoring of a vehicle’s location.

Eavesdropping: Intercept private data transmissions.

POTENTIAL CONSEQUENCES

01. LOSS OF VEHICLE CONTROL

02. FINANCIAL LOSSES AND LEGAL LIABILITIES

03. PRIVACY AND DATA BREACHES

04. SAFETY RISKS

05. TRAFFIC DISRUPTIONS AND INFRASTRUCTURE DAMAGES

MITIGATION MECHANISMS

MALWARE DETECTION

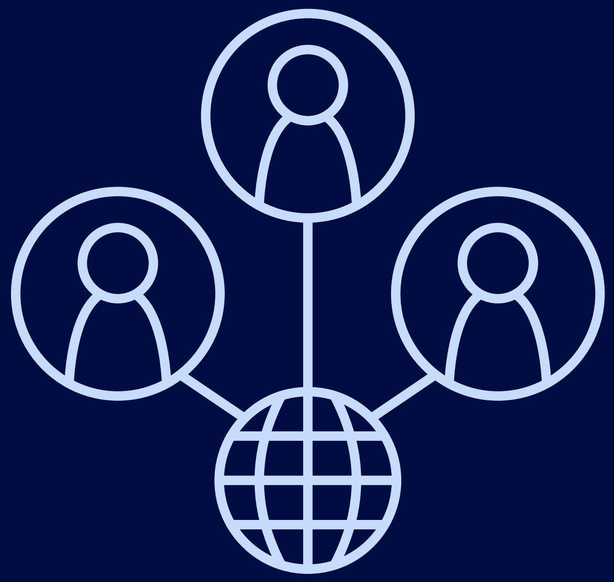
CRYPTOGRAPHY

NETWORK SECURITY

SOFTWARE SECURITY

BLOCKCHAIN TECHNOLOGY

MITIGATION MECHANISMS



NETWORK SECURITY

NETWORK SECURITY

Intrusion detection systems (IDSs) are employed to detect and mitigate various network- based attacks. There are four main IDSs implemented to secure AVs:

- Signature-based IDS: Functions by comparing observed behaviour against a database of known signatures.
- Anomaly-based IDS: Operates by recognising anomalies in a vehicle's behaviour that deviate from the normal or expected patterns.
- Specification-based IDS: Monitors a vehicle's behaviour against a set of predefined rules or specifications.
- Hybrid-based IDS: Combines the strengths of signature- based and anomaly-based detection methods to defend against a broader spectrum of cyber threats.

MALWARE DETECTION

MALWARE DETECTION

Malware detection systems, an extension of IDSs, employ signature and behaviour-based techniques to mitigate cyber-attacks. In addition to these, malware detection includes:

- Heuristic-based Techniques: Employ heuristic rules and algorithms to identify potential malware based on characteristics or patterns associated with malicious code.
- Cloud-based Techniques: Leverages cloud computing services for efficient and scalable malware detection in AVs.

Network IDSs in AVs utilise Machine Learning (ML) and Deep Learning (DL) models for their fast detection and response times to cyber threats, and ability to leverage insights from data analytics. Models include k-nearest neighbour (KNN), decision trees, auto-encoders and long short-term memory (LSTM) networks.

SOFTWARE SECURITY

SOFTWARE SECURITY

1. *Machine Learning Algorithms:* ML models are employed for various security tasks, including intrusion detection, malware analysis, and vulnerability assessment. Similar to ML for IDSs, ML models detect anomalies and deviations in normal software behaviour, identifying previously unseen attack vectors and zero-day exploits.

2. *Software Analysis Techniques:* Static and dynamic analysis methods are used to analyse AV software for potential vulnerabilities and malicious code:
   a. Static: Examines code without executing it to identify potential vulnerabilities.
   b. Dynamic: Executes code in a controlled environment and monitors for anomalies.

CRYPTOGRAPHY

CRYPTOGRAPHY

1) Encryption Techniques: Encryption (symmetric and asymmetric) techniques are used to secure data transmissions and communications in AVs. Public-key cryptography is employed for secure key distribution and authentication in V2V/V2I communications.

- Symmetric: Encrypts data transmissions in V2V/V2I communications.
- Asymmetric: Secures key distribution and authentication in V2V/V2I communications.

2) Authentication Techniques:

- Digital Signatures: Authenticate the source and integrity of messages or data transmitted between vehicles and infrastructure.
- Message Authentication Codes: Provide data origin authentication and integrity verification for V2V/V2I communications.

BLOCKCHAIN TECHNOLOGY

BLOCKCHAIN TECHNOLOGY

Blockchain (BC) technology is used to store and share information on an advanced database. Each dataset is stored in blocks, linked together in a chain. BC technology has gained popularity with its ability to prevent cyber-attacks through its inherent security measures of decentralisation, transparency, encryption, and immutability.

CURRENT LIMITATIONS IN MITIGATION MECHANISMS

COMPLEXITY OF SYSTEMS

REAL-TIME OPERATIONS

VEHICLE COMMUNICATIONS

MACHINE LEARNING ALGORITHMS

FUTURE WORK

Future Work

- Securing sensor data.
- Adversarial machine learning algorithms.
- Real time decision making.
- Securing autonomous vehicles with AI and BC technologies.
- Communication mechanisms.
- Architectural solution.

THANK YOU

Thank you

PRESENTED BY TANISHA SOLDINI
TANISHAROSE.SOLDINI@FLINDERS.EDU.AU

FLINDERS UNIVERSITY