IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Passive Keyless Entry and Start (PKES): Cybersecurity Issues in Modern Vehicles

Muhammad Ali Nadeem[1]
[1]triOS College of Business, Technology and Healthcare, Toronto, Canada

Corresponding author: Muhammad Ali Nadeem (e-mail: ali.nadeem@trios.com).

ABSTRACT: The growing integration of *Internet of Things* (IoT) technologies and interconnected subsystems in modern vehicles has enabled unprecedented levels of automation, connectivity, and user convenience. However, this expanded connectivity has significantly increased the automotive attack surface, as evidenced by the recent rise in cyber-enabled vehicle theft across Canada and the United States. These incidents underscore the limitations of traditional security mechanisms in protecting next-generation vehicles. This paper presents *AutoGuardX*, a comprehensive cybersecurity framework designed for connected and software-defined vehicles. The framework addresses critical attack vectors, including relay attacks, Controller Area Network (CAN) bus exploitation, and vulnerabilities associated with 5G-enabled interfaces, as well as emerging threats posed by future quantum-capable adversaries. *AutoGuardX* aligns with established industry standards—namely *ISO/SAE 21434* and *ISO 26262*—while incorporating advanced security features such as machine-learning-based intrusion detection, secure IoT communication protocols, and encrypted in-vehicle and vehicle-to-everything (V2X) communication channels. The proposed framework is evaluated through controlled simulations, empirical testing, and analysis of evolving vehicle theft techniques. The results demonstrate its scalability, adaptability, and practical applicability across diverse vehicular architectures. By integrating real-time threat monitoring, secure over-the-air update mechanisms, and embedded forensic capabilities, *AutoGuardX* provides a forward-looking security paradigm for connected vehicles. This work offers actionable insights and a robust architectural blueprint for enhancing resilience within the automotive cybersecurity

INDEX TERMS Automotive cybersecurity, CAN bus intrusion, Machine learning anomaly detection, Relay attacks, IoT vehicle security.

I. INTRODUCTION

A. BACKGROUND

Modern vehicles are no longer purely mechanical machines. They are complex digital systems made up of software, wireless communication technologies, sensors, and interconnected electronic control units (ECUs). These systems enable features such as keyless entry, push-button start, remote unlocking via mobile applications, navigation, driver assistance, and over-the-air software updates. While these technologies provide significant convenience and improved functionality, they have also introduced new cybersecurity risks that did not exist in traditional vehicles.

One of the most widely adopted features in modern vehicles is the **Passive Keyless Entry and Start (PKES)** system. PKES allows drivers to unlock and start their vehicles without physically inserting a key. As long as the key fob is nearby, the vehicle automatically authenticates it and grants access. This technology was designed to improve user experience; however, it has become one of the most exploited components in modern vehicle theft.[1]

Over the last decade, vehicle theft has evolved from a largely physical crime into a cyber-enabled activity. Criminals no longer need to break windows, force locks, or hotwire ignition systems. Instead, they increasingly rely on electronic tools, wireless relay devices, and network-based attacks that allow them to unlock and start vehicles silently, often in seconds. These attacks leave little to no physical evidence, making detection, investigation, and prevention significantly more difficult.

This shift is particularly evident in regions such as **Canada, the United States, and Europe**, where connected and keyless vehicles are widespread. Organized criminal groups now specialize in exploiting weaknesses in vehicle electronic systems. Stolen vehicles are frequently transported to ports and exported internationally or dismantled for parts, creating a highly profitable and low-risk criminal enterprise.[2]

The growing frequency of these incidents highlights a fundamental problem: many vehicle security systems were not designed with modern cyber threats in mind. Traditional anti-theft mechanisms such as alarms, immobilizers, and mechanical locks are largely ineffective against attacks that exploit wireless communication protocols and internal vehicle networks.[3],[4],[5]

B. OVERWIVE OF PKE SYSTEMS

Passive Keyless Entry and Start systems work by enabling communication between the vehicle and a wireless key fob. When the driver approaches the vehicle, the car sends out a low-power radio signal. If the key fob is within range, it responds with an authentication message. Once the vehicle verifies this response, the doors unlock automatically. A similar process occurs when the driver presses the start button inside the car.[6]

From a functional perspective, PKES systems rely on:

- Radio Frequency (RF) communication
- Cryptographic challenge–response mechanisms
- Proximity-based assumptions (the key is close to the vehicle)

The core security assumption behind PKES is that if the key fob responds correctly, it must be physically close to the vehicle. Unfortunately, this assumption is flawed.[7]

PKES systems do not reliably verify actual distance. Instead, they verify whether a valid response is received within a certain time window. This design decision makes them vulnerable to **relay attacks**, where attackers artificially extend the communication range between the vehicle and the key fob.

As a result, a key fob stored safely inside a house—sometimes dozens of meters away—can still be used to unlock and start a vehicle parked outside. The owner may be asleep, and the theft can occur without any visible signs of forced entry.

C. RELAY ATTACKS

A **relay attack** is a method where attackers trick the vehicle into believing that the legitimate key fob is nearby when it is not. Typically, this attack requires two devices and two attackers:

- One attacker stands near the vehicle with a relay device.
- The second attacker stands near the victim's home, close to where the key fob is stored.

The device near the vehicle captures the car's authentication request and transmits it wirelessly to the second device. The second device then relays this request to the key fob, which responds as if the car were nearby. That response is relayed back to the vehicle, which then unlocks and allows the engine to start.

From the vehicle's perspective, everything appears normal. A valid key responded correctly, so access is granted. Key characteristics of relay attacks include:

- No physical damage to the vehicle
- No need to steal the key
- Minimal technical skill required once tools are obtained
- Extremely fast execution (often under 60 seconds)

Because the vehicle's alarm system is not triggered and there is no forced entry, owners often do not realize their car has been stolen until much later.[8]

Traditional vehicle security systems were designed to protect against physical threats. Alarms are triggered by forced entry. Immobilizers prevent engines from starting without a correct key. Steering wheel locks restrict physical movement. Cyber-enabled attacks bypass all of these mechanisms. In relay attacks and similar electronic exploits:

- The vehicle believes the authentication process is legitimate
- Alarms are not activated
- Immobilizers are disengaged normally
- No abnormal physical behavior is detected

This exposes a major gap between **functional safety**, **physical security**, and **cybersecurity**. While manufacturers have focused heavily on safety systems to protect occupants during accidents, cybersecurity has historically received less attention, especially at runtime. As vehicles continue to adopt:

- Wireless connectivity
- Telematics modules
- Cloud services
- Over-the-air updates
- Vehicle-to-everything (V2X) communication

the attack surface continues to grow.

For cybersecurity professionals and IT project managers, vehicle theft is no longer just a criminal issue—it is a **systems security problem**. From a risk management perspective, cyber-enabled vehicle theft:

- Increases financial losses for insurers and consumers
- Damages brand trust for manufacturers

- Creates regulatory and compliance challenges
- Introduces safety risks if vehicles are remotely manipulated
- Enables organized crime and cross-border trafficking

Most importantly, it demonstrates that vehicles must now be secured like enterprise IT systems, but with far stricter safety and real-time constraints. This reality demands:

- Continuous monitoring instead of static security controls
- Detection of abnormal behavior rather than reliance on fixed rules
- Secure communication at every layer of the vehicle architecture
- Integration of cybersecurity with safety and lifecycle management

These needs form the foundation for the AutoGuardX framework, which will be introduced and explained later in this document as a comprehensive, practitioner-oriented solution.[9]

II. THE EVOLUTION OF VEHICLE THEFT

Vehicle theft has changed significantly over the past decade. What was once a largely opportunistic crime has evolved into a structured, technology-driven operation carried out by organized criminal groups. These groups operate with planning, specialization, and access to advanced electronic tools that allow them to exploit weaknesses in modern vehicle systems.[10]

In the past, stealing a vehicle often required visible force, mechanical knowledge, or prolonged effort. Today, many vehicles can be stolen quietly in minutes, sometimes in broad daylight, without attracting attention. This shift has reduced the risk to criminals while increasing the success rate of thefts, particularly for high-value vehicles equipped with keyless entry and connected features.

Organized groups often divide responsibilities among members. Some specialize in reconnaissance, identifying vehicles with vulnerable systems. Others operate electronic tools used to unlock and start vehicles. Additional members handle logistics, including transport, storage, and export. This level of organization reflects the growing profitability of cyber-enabled vehicle theft and the reduced likelihood of immediate detection.[11]

Stolen vehicles are rarely kept for personal use. In many cases, they are quickly transported to shipping ports and exported to international markets, or dismantled for parts that can be sold separately. This rapid turnover further complicates recovery efforts and weakens traditional law enforcement strategies that rely on visible evidence or delayed reporting.[12]

At the core of every modern vehicle is the **Controller Area Network (CAN) bus**. The CAN bus is a communication system that allows electronic control units (ECUs) to exchange messages. These ECUs manage essential vehicle functions such as braking, steering, engine control, lighting, door locks, and alarms.

The CAN bus was designed decades ago with reliability and efficiency in mind, not cybersecurity. As a result, it lacks many of the protections commonly found in modern IT networks. In most vehicles:

- Messages are not encrypted
- Devices are trusted by default
- There is little or no authentication between ECUs

This design means that if an attacker gains access to the CAN bus, they can send commands that appear legitimate to the vehicle. The vehicle has no built-in way to determine whether those commands came from a trusted ECU or a malicious device.[13]

From a cybersecurity perspective, this creates a serious vulnerability. The CAN bus effectively becomes an internal network that assumes all participants are trustworthy, even when they are not.

A **CAN bus injection attack** occurs when an attacker connects a malicious device to the vehicle's internal network and sends unauthorized messages. These messages can instruct the vehicle to unlock doors, disable alarms, or start the engine. One of the most common attack methods involves gaining physical access to the CAN wiring. Attackers often do this by:

- Removing or damaging a headlight assembly
- Accessing wiring through the wheel arch
- Connecting through exposed body panels

Once connected, the attacker plugs in a small electronic device that communicates directly with the CAN bus. The vehicle treats this device as a legitimate ECU and accepts its commands.[14],[15]

Unlike relay attacks, which exploit wireless communication, CAN injection attacks exploit **internal trust assumptions**. Even vehicles with advanced keyless systems can be compromised if attackers reach the internal network. These attacks are particularly dangerous because:

- They bypass key fob authentication entirely
- They work even if the key fob is stored securely

- They leave minimal physical evidence
- They can be executed quickly

For vehicle owners, the result is the same: the vehicle disappears without signs of forced entry or alarm activation.

CAN bus attacks are difficult to detect because they blend in with normal vehicle behavior. From the vehicle's perspective, the commands received appear identical to those sent by legitimate ECUs. There is typically no centralized monitoring system that evaluates whether CAN messages are abnormal or malicious. As long as the message format is correct, the vehicle executes the command.[16]

This lack of visibility creates a major blind spot. Vehicle systems are excellent at responding to physical faults, such as sensor failures, but they are far less capable of recognizing cyber intrusions occurring at the network level. Additionally, many attacks are completed within minutes. By the time the owner notices the vehicle is missing, there is little forensic evidence available to reconstruct what happened.

Modern vehicle theft rarely relies on a single technique. Instead, attackers often combine multiple methods to increase reliability and reduce the risk of failure. For example:

- A relay attack may be used to unlock the vehicle
- A CAN injection attack may then disable alarms or immobilizers
- Diagnostic interfaces such as OBD-II ports may be used to program new keys. [17]

This hybrid approach allows attackers to adapt to different vehicle models and security configurations. If one method fails, another can be used.

From a defender's perspective, this complexity makes protection more challenging. Security controls that address only one attack vector are often insufficient, as attackers simply switch to another pathway.[18]

A. DIAGNOSTIC INTERFACES AS AN ATTACK VENTOR

The **On-Board Diagnostics (OBD-II)** port is another commonly exploited interface. This port is intended for maintenance and diagnostics, allowing authorized technicians to read vehicle data and update configurations. In many vehicles, the OBD-II port provides direct access to critical systems. If an attacker gains access to this port, they may be able to:

- Program new key fobs
- Disable immobilizers
- Modify vehicle settings
- Extract sensitive data

Although some manufacturers have introduced additional protections, many vehicles—especially older models—remain vulnerable. Attackers can purchase key-programming tools on underground markets, making these attacks accessible even to individuals with limited technical expertise.[19]

B. IMPLICATIONS FOR CYBERSECURITY

For cybersecurity professionals and IT project managers, these attack techniques illustrate the importance of treating vehicles as **complex, networked systems** rather than isolated machines. Key lessons include:

- Security must be embedded at the architectural level, not added later
- Trust assumptions within internal networks must be challenged
- Runtime monitoring is essential for detecting abnormal behavior
- Physical and cyber security must be addressed together. [20]

Traditional risk management approaches that focus on compliance alone are no longer sufficient. Effective vehicle security requires continuous assessment, detection, and response capabilities that operate throughout the vehicle's lifecycle. These insights set the stage for understanding why existing standards and solutions, while valuable, often fall short in practice. They also explain the need for a more comprehensive framework—such as **AutoGuardX**—that integrates real-time monitoring, adaptive defenses, and lifecycle management.[21]

C. ROLE OF IOT IN MODERN VEHICLES

Modern vehicles are no longer isolated machines. They are part of a broader digital ecosystem commonly described as the **Internet of Things (IoT)**. Vehicles now include numerous connected components that communicate with each other, with external infrastructure, and with cloud-based services. These connected components include:

- Telematics control units
- GPS and navigation systems
- Infotainment platforms
- Mobile applications
- Remote diagnostics and maintenance tools
- Advanced driver assistance systems (ADAS) [22]

From a functional perspective, IoT connectivity enables features such as real-time traffic updates, remote unlocking, vehicle health monitoring, emergency services, and predictive maintenance. From a cybersecurity perspective, however,

every connected component represents a potential entry point for attackers.

IoT devices in vehicles often operate under strict performance and power constraints. As a result, security mechanisms may be simplified or inconsistently implemented. In some cases, legacy design decisions persist across multiple vehicle generations, increasing long-term exposure to known vulnerabilities.[23]

The **telematics control unit (TCU)** acts as a gateway between the vehicle and external networks. It typically communicates with cellular networks, cloud servers, and mobile applications. Because of its central role, the TCU is a high-value target for attackers. If compromised, a telematics system can potentially allow:

- Remote unlocking or immobilization
- Location tracking
- Data exfiltration
- Injection of malicious commands into internal vehicle networks [24]

Unlike relay or CAN injection attacks, telematics-based attacks can be conducted remotely, sometimes from another country. This significantly increases the scale and reach of potential threats.

Several real-world incidents have demonstrated that vulnerabilities in telematics software, backend APIs, or authentication mechanisms can expose entire fleets of vehicles to risk. Even a small configuration error can have widespread consequences. [25]

Over-the-air updates are a critical feature of modern vehicles. They allow manufacturers to:

- Fix software bugs
- Improve functionality
- Deploy security patches
- Update infotainment and driver assistance features

While OTA updates provide clear benefits, they also introduce new risks. If the update process is not properly secured, attackers may attempt to:

- Inject malicious firmware
- Roll back security patches
- Intercept or modify update packages
- Exploit update mechanisms to gain persistent access

OTA security failures can turn a single vulnerability into a fleet-wide issue. For this reason, secure update mechanisms must include strong authentication, integrity checks, and cryptographic validation. From a project management perspective, OTA updates require careful coordination between engineering, cybersecurity, operations, and compliance teams. Security cannot be treated as an afterthought; it must be built into update workflows from the beginning.[26]

The introduction of **5G** and **Vehicle-to-Everything (V2X)** communication is transforming transportation systems. Vehicles can now communicate with:

- Other vehicles (V2V)
- Traffic infrastructure (V2I)
- Pedestrians and devices (V2P)
- Cloud services (V2N)

These capabilities enable safer and more efficient transportation, including collision avoidance, traffic optimization, and autonomous driving support. However, they also increase the number of external interfaces exposed to potential attack. V2X communication relies on complex protocols, certificates, and trust models. If these mechanisms are misconfigured or compromised, attackers may:

- Send false messages
- Disrupt traffic coordination
- Manipulate vehicle behavior
- Exploit trust relationships between systems [27],[28]

As vehicles become more connected to public infrastructure, cybersecurity failures can have broader societal impacts, extending beyond individual vehicle theft.

Modern vehicles depend heavily on cloud-based backend systems. These systems manage:

- User authentication
- Vehicle data storage
- Remote commands
- Analytics and diagnostics
- Fleet management

From a cybersecurity standpoint, the vehicle is only one part of the system. Weaknesses in cloud infrastructure, APIs, or access controls can undermine even well-secured in-vehicle systems.[29]

Several incidents have shown that attackers do not need to compromise the vehicle directly. Instead, they exploit backend systems to issue legitimate-looking commands that vehicles accept without question. This highlights the importance of **end-to-end security**, where protection extends from the vehicle to the cloud and back. Traditional vehicle security assumed:

- Limited external access
- Short operational lifetimes
- Minimal software updates
- Isolated systems

Connected vehicles invalidate these assumptions. Vehicles now:

- Remain online for years
- Receive frequent software updates
- Interact with external services continuously
- Share data across ecosystems [30]

This shift requires a new security model based on:

- Continuous monitoring
- Behavior-based detection
- Rapid response and recovery
- Lifecycle risk management

Static security controls are no longer sufficient. Instead, vehicles must be treated as dynamic systems that require ongoing protection.

III. MANAGING CONNECTED VEHICLE RISK

For practitioners, several key principles emerge:

- Connectivity must be matched with security investment
- Trust boundaries must be clearly defined and enforced
- Every external interface should be assumed hostile
- Monitoring and detection are as important as prevention
- Security responsibilities extend beyond the vehicle itself [31]

These principles apply not only to vehicle manufacturers but also to fleet operators, service providers, insurers, and regulators. Each stakeholder plays a role in managing risk across the connected vehicle ecosystem.

The challenges described in this section—IoT exposure, telematics vulnerabilities, OTA risks, and cloud dependencies—cannot be addressed through isolated fixes. They require a coordinated, system-wide approach.

Existing standards provide valuable guidance, but they often focus on design-time processes rather than runtime protection. [32] This gap between compliance and real-world defense is a key motivation for developing a more comprehensive framework. In the next section, the document will examine:

- Limitations of existing automotive cybersecurity standards
- Why compliance alone does not stop vehicle theft
- The need for integrated, real-time defense mechanisms

This discussion will set the foundation for introducing AutoGuardX as a practical, adaptive cybersecurity framework designed to address modern vehicle threats.

As vehicles have become more complex and connected, the automotive industry has introduced several standards and regulations to improve safety, quality, and cybersecurity. These frameworks are essential for establishing common practices, ensuring accountability, and meeting regulatory expectations. [33],[34]

The most relevant standards in the context of modern vehicle cybersecurity include:

- **ISO 26262** – Functional safety for road vehicles
- **ISO/SAE 21434** – Cybersecurity engineering for road vehicles
- **UNECE WP.29 (UN R155 and R156)** – Cybersecurity and software update management regulations
- **Automotive SPICE** – Process maturity and quality assurance [35]

These standards play a critical role in shaping how vehicles are designed, developed, and maintained. However, it is important to understand both their strengths and their limitations, particularly when addressing cyber-enabled vehicle theft. [36]

ISO 26262 focuses on **functional safety**, which means ensuring that electrical and electronic systems behave safely in the presence of faults. The standard addresses risks such as sensor failures, software bugs, and hardware malfunctions that could lead to accidents or injuries.

While functional safety is essential, ISO 26262 does not directly address malicious cyber threats. The standard assumes that system failures are accidental rather than intentional. As a result:

- It does not require protection against hacking or intrusion
- It does not mandate runtime security monitoring
- It does not account for adversarial behavior

This creates a gap in modern vehicles, where a cyberattack can trigger safety-relevant behavior without being considered a "fault" under traditional safety definitions. [37]

ISO/SAE 21434 was introduced to address the growing need for cybersecurity in road vehicles. It provides a structured

approach to managing cyber risks across the vehicle lifecycle, including:

- Threat analysis and risk assessment (TARA)
- Secure design and development processes
- Verification and validation activities
- Incident response planning

This standard represents a significant improvement over earlier approaches by formally recognizing cybersecurity as a core engineering discipline within automotive development.

However, ISO/SAE 21434 is primarily **process-oriented**. It emphasizes documentation, governance, and design-time risk assessment. While these elements are necessary, they are not sufficient on their own to stop real-world attacks. [38]

UNECE WP.29 regulations, specifically **UN R155** (Cybersecurity Management Systems) and **UN R156** (Software Update Management Systems), introduce legal requirements for vehicle manufacturers in many global markets. These regulations require manufacturers to:

- Establish cybersecurity management systems
- Demonstrate ongoing risk management
- Secure software updates throughout the vehicle lifecycle
- Monitor and respond to emerging threats

WP.29 represents an important shift from voluntary standards to enforceable regulation. It compels organizations to take cybersecurity seriously and invest in long-term security programs.

However, like ISO/SAE 21434, WP.29 focuses heavily on **organizational processes** rather than technical runtime defenses.

A. THE MAIN ISSUE – STANDARDS FALL SHORT

Despite their value, existing automotive standards share a common limitation: they are primarily designed to ensure **compliance**, not **real-time protection**. Key gaps include:

- Limited requirements for runtime intrusion detection
- Minimal guidance on in-vehicle anomaly monitoring
- No mandate for adaptive or machine learning-based defenses
- Weak integration between cybersecurity and operational monitoring

As a result, a vehicle may be fully compliant with all relevant standards and still be vulnerable to relay attacks, CAN injection, or telematics exploitation. [39]

This disconnect explain why cyber-enabled vehicle theft continues to rise despite increased regulatory attention.

B. A PRACTITIONER'S DILEMMA

For IT project managers and cybersecurity professionals, compliance is often a necessary but insufficient goal. Passing audits and meeting regulatory requirements does not guarantee that systems are secure in practice. In the automotive context:

- Compliance demonstrates due diligence
- Security requires active defense

A compliance-driven approach may result in extensive documentation and process maturity without meaningful improvements in attack detection or response.

Practitioners must therefore balance regulatory obligations with operational security needs. This often requires going beyond minimum requirements and implementing additional technical controls. [40]

One of the most significant gaps in existing frameworks is the lack of a **runtime security layer**. Runtime security refers to the ability to:

- Monitor system behavior continuously
- Detect abnormal or malicious activity as it occurs
- Respond automatically or semi-automatically to threats

Most automotive standards focus on:

- Design-time risk analysis
- Development and testing processes
- Post-incident investigation

They provide limited guidance on how to protect vehicles once they are deployed in the real world and exposed to evolving threats.

Cyber-enabled vehicle theft demonstrates why runtime protection is essential. Attacks such as relay and CAN injection occur after the vehicle has left the factory. They exploit real-world conditions and adversarial behavior that cannot be fully anticipated during design. Without runtime monitoring:

- Attacks go undetected
- There is no immediate response
- Forensic evidence is limited
- Vulnerabilities persist across fleets

Runtime protection enables vehicles to transition from passive targets into active defenders. [41]

Another challenge is the historical separation between **functional safety** and **cybersecurity**. In modern vehicles,

these domains are increasingly interconnected. A cyberattack can:

- Disable safety systems
- Trigger unsafe behavior
- Manipulate sensor data
- Affect driver assistance functions

Security frameworks must therefore consider safety implications and ensure that defensive actions do not introduce new hazards. [42]

C. THE NEED FOR AN INTEGRATED FRAMEWORK

The limitations of existing standards highlight the need for a framework that:

- Complements regulatory requirements
- Adds real-time detection and response
- Integrates safety and cybersecurity
- Scales across vehicle platforms
- Adapts to emerging threats

This need forms the foundation for **AutoGuardX**, a comprehensive automotive cybersecurity framework designed to operate alongside existing standards while addressing their practical limitations. In the next section, AutoGuardX will be introduced in detail, including its architecture, key components, and how it addresses modern vehicle theft and cyber threats. [43]

IV. *AUTOGUARDX*: A PRACTICAL CYBERSECURITY FRAMEWORK

AutoGuardX is a comprehensive cybersecurity framework designed specifically for modern, connected, and software-defined vehicles. It was developed in response to the growing gap between traditional automotive security standards and the real-world threats faced by today's vehicles.

Unlike frameworks that focus primarily on documentation, compliance, or design-time analysis, AutoGuardX emphasizes **continuous protection during vehicle operation**. Its goal is to help vehicles detect, prevent, and respond to cyber threats in real time while remaining aligned with existing automotive safety and cybersecurity standards.

AutoGuardX does not replace established standards such as ISO 26262 or ISO/SAE 21434. Instead, it complements them by adding the operational security capabilities that those standards do not fully address.

The design of AutoGuardX is guided by several key principles that reflect the realities of modern vehicle systems:

Lifecycle-Oriented Security: Security is applied across the entire vehicle lifecycle, from concept and design through production, deployment, and long-term operation.[44]

Defense in Depth: Multiple layers of security controls are implemented so that the failure of one mechanism does not result in complete system compromise.

Zero-Trust Assumptions: No internal or external component is trusted by default. All communications and access requests must be authenticated and validated.

Runtime Awareness: The framework continuously monitors vehicle behavior to detect abnormal activity as it occurs.

Scalability and Flexibility: AutoGuardX is designed to operate across different vehicle platforms, architectures, and market segments. [45]

Architectural Overview of AutoGuardX: AutoGuardX is structured as a modular framework that integrates with existing vehicle architectures. Its components can be deployed incrementally, allowing manufacturers and operators to adapt the framework to their specific needs. At a high level, AutoGuardX consists of:

- In-vehicle monitoring and detection modules
- Secure communication and authentication layers
- Update and configuration management mechanisms
- Forensic logging and telemetry systems
- Threat intelligence and response capabilities

This modular design ensures that AutoGuardX can support both new vehicle designs and retrofitted security enhancements for existing platforms. [46]

Machine Learning-Based Intrusion Detection: One of the core components of AutoGuardX is a **machine learning-based intrusion detection system (IDS)**. This system monitors:

- CAN bus traffic
- Internal network behavior
- Wireless communication patterns
- Keyless entry interactions

Rather than relying solely on predefined rules, the IDS learns normal vehicle behavior and identifies deviations that may indicate an attack. This allows it to detect:

- Relay attacks
- CAN injection attempts
- Abnormal diagnostic access
- Unusual telematics activity

By detecting threats in real time, the system can trigger alerts or initiate automated defensive actions.[47]

Secure Authentication and Access Control: AutoGuardX enforces strong authentication across all vehicle interfaces. This includes:

- ECUs
- Key fobs
- Diagnostic tools
- Telematics and cloud services
- V2X communication channels

Authentication mechanisms are designed to prevent:

- Key cloning
- Unauthorized ECU access
- Malicious device injection
- Backend impersonation

Access control policies ensure that each component can perform only the actions it is authorized to perform, reducing the impact of compromised systems. [48]

Encrypted Communication and Network Protection: AutoGuardX introduces robust encryption and integrity protection for both internal and external communications. This includes:

- Secured CAN and automotive Ethernet communication
- Encrypted wireless interfaces
- Protected keyless entry signals
- Secure gateways between network domains

By protecting data in transit, the framework prevents attackers from intercepting, modifying, or replaying messages used to control vehicle functions. [49]

Secure Over-the-Air Update Management: AutoGuardX includes a secure OTA update manager that ensures:

- Only authenticated software is installed
- Firmware integrity is verified before execution
- Rollback attacks are prevented
- Update processes are auditable

This component protects vehicles from malicious updates and ensures that security patches can be deployed safely across fleets.

Forensic Logging and Telemetry: To support investigation and continuous improvement, AutoGuardX embeds tamper-resistant logging and telemetry throughout the vehicle. These logs capture:

- Security events
- Anomalous behavior
- Access attempts
- System responses

This information supports:

- Incident analysis
- Regulatory reporting
- Threat intelligence development
- Long-term risk management

Threat Intelligence and Adaptive Response: AutoGuardX integrates threat intelligence from both internal observations and external sources. This enables the framework to:

- Recognize emerging attack patterns
- Adapt detection models over time
- Adjust defensive strategies dynamically

Automated or guided responses may include:

- Blocking malicious messages
- Isolating compromised components
- Restricting vehicle functionality
- Notifying users or operators

How AutoGuardX Differs from Traditional Frameworks: The key distinction between AutoGuardX and traditional automotive security frameworks lies in its operational focus. Traditional frameworks:

- Emphasize compliance and process maturity
- Focus on design-time risk analysis
- Provide limited runtime protection

AutoGuardX:

- Operates continuously during vehicle use
- Detects and responds to attacks in real time
- Integrates safety, security, and operations
- Adapts to evolving threats

This makes AutoGuardX particularly well-suited to addressing cyber-enabled vehicle theft and other emerging risks.

Deploying AutoGuardX in Real-World Vehicle Environments: The successful deployment of AutoGuardX requires a structured and practical approach that aligns cybersecurity objectives with engineering, operational, and regulatory constraints. Because modern vehicles differ widely in architecture, connectivity, and market requirements, AutoGuardX is designed to be deployed in phases rather than as a single, disruptive change. [50]

Deployment typically begins with a **baseline security assessment**. This assessment identifies vulnerable components such as keyless entry systems, CAN bus access

points, telematics units, and diagnostic interfaces. By understanding where risks are highest, organizations can prioritize which AutoGuardX modules to deploy first. Initial implementation often focuses on:

- Securing communication gateways
- Enabling intrusion detection on in-vehicle networks
- Hardening OTA update mechanisms

Advanced capabilities, such as machine learning-based threat prediction and adaptive response, can then be introduced incrementally to minimize operational risk.

Integration with Existing Vehicle Architectures: AutoGuardX is designed to integrate with existing vehicle architectures rather than requiring a complete redesign. Key integration points include:

- Central gateway ECUs
- Telematics control units
- Infotainment platforms
- Cloud backend services

By operating at these strategic locations, AutoGuardX can monitor and control data flows between internal vehicle networks and external interfaces. This containment approach ensures that malicious activity is intercepted before it reaches safety-critical systems.

For older vehicles, partial deployment may still provide meaningful protection, particularly against relay attacks, CAN injection, and unauthorized diagnostic access.

Operational Monitoring and Incident Response: One of the most important benefits of AutoGuardX is its support for continuous operational monitoring. Through real-time telemetry and event analysis, the framework provides visibility into vehicle security posture throughout its operational life. This capability enables:

- Early detection of emerging threats
- Rapid response to active attacks
- Remote mitigation actions
- Improved forensic investigation

For fleet operators and manufacturers, this monitoring function supports centralized security operations and informed decision-making. [51]

Benefits for Key Stakeholders

Vehicle Manufacturers: AutoGuardX helps manufacturers:

- Reduce theft-related losses
- Protect brand reputation
- Meet regulatory requirements
- Strengthen customer trust
- Improve long-term product resilience

Fleet Operators: Fleet operators benefit from:

- Improved visibility into vehicle security
- Reduced downtime and loss
- Faster incident response
- Scalable security management across fleets

Consumers: For vehicle owners, AutoGuardX provides:

- Stronger protection against theft
- Reduced insurance risk
- Greater confidence in connected vehicle features
- Improved safety and reliability [52]

Economic and Societal Impact: Cyber-enabled vehicle theft imposes significant costs on society. These include increased insurance premiums, law enforcement expenses, and the growth of organized criminal networks. By reducing the success rate of theft and improving detection, AutoGuardX contributes to:

- Lower economic losses
- Disruption of criminal operations
- Enhanced public trust in vehicle technology
- More secure transportation systems

Future-Proofing Against Emerging Threats: The automotive threat landscape continues to evolve. Future challenges include:

- Increased reliance on 5G and V2X communication
- Growing software complexity
- Expanded use of cloud-based services
- Potential threats from advanced computing technologies [53]

AutoGuardX is designed with adaptability in mind. Its modular architecture and machine learning components allow it to evolve alongside new technologies and threat models. [54]

Alignment with Standards and Regulations: AutoGuardX aligns with existing automotive standards and regulations, including:

- ISO 26262
- ISO/SAE 21434
- UNECE WP.29 [55]

By complementing these frameworks rather than replacing them, AutoGuardX supports compliance while enhancing real-world security effectiveness. [56]

Strategic Implications for the Automotive Industry: The rise of connected and software-defined vehicles marks a

fundamental shift in the automotive industry. Cybersecurity is no longer optional; it is a core requirement that affects safety, reliability, and competitiveness. Organizations that proactively invest in comprehensive security frameworks will be better positioned to:

- Respond to emerging threats
- Meet regulatory expectations
- Maintain customer trust
- Support innovation safely [57],[58]

V. CONCLUSION

This document has examined how modern vehicle theft has evolved into a sophisticated, cyber-enabled problem driven by connectivity, software complexity, and weak runtime defenses. Techniques such as relay attacks, CAN bus injection, and telematics exploitation demonstrate the limitations of traditional vehicle security mechanisms. [59]

While existing standards provide essential guidance, they do not fully address the need for real-time detection and response. AutoGuardX was introduced as a comprehensive, practical framework designed to bridge this gap.

By integrating continuous monitoring, secure communication, adaptive threat detection, and lifecycle management, AutoGuardX transforms vehicles from passive targets into resilient, self-protecting systems.

As vehicles continue to evolve into intelligent, connected platforms, cybersecurity must evolve with them. Protecting vehicles against cyber-enabled theft is not solely a technical challenge—it is a strategic, economic, and societal imperative. AutoGuardX represents a forward-looking approach to automotive cybersecurity, providing a structured and adaptable framework capable of securing the future of connected mobility.

REFERENCES

[1] D. Lea, "The GTA is rich in expensive vehicles: Experts explain who is behind auto thefts in Burlington, Oakville, Ajax, Pickering, Oshawa, Whitby, plus York Region and why," *InsideHalton.com*, Oct. 22, 2024. [Online]. Available: https://www.insidehalton.com/news/crime/the-gta-is-rich-in-expensive-vehicles-experts-explain-who-is-behind-auto-thefts-in/article_6d1d52e6-c82b-5a41-bb6b-bb2475a033c7.html

[2] *ENISA Threat Landscape 2024*. European Union Agency for Cybersecurity. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[3] "Interpol detects 200 stolen vehicles from Canada each week," *INTERPOL*, Nov. 17, 2024. [Online]. Available: https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-detects-200-stolen-vehicles-from-Canada-each-week

[4] Insurance Bureau of Canada, "Auto theft is a National Crisis," *IBC Canada*, Dec. 18, 2022. [Online]. Available: https://www.ibc.ca/stay-protected/theft-prevention/end-auto-theft

[5] N. Yousif, "How Canada became a car theft capital of the world," *BBC News*, Jul. 9, 2024. [Online]. Available: https://www.bbc.com/news/articles/cy79dq2n093o

[6] B. Marcelo, "Toronto cybersecurity expert says it takes 1 minute for car thieves to get into your vehicle using this common tactic," *NOW Toronto*, Feb. 13, 2024. [Online]. Available: https://nowtoronto.com/news/toronto-cybersecurity-expert-says-it-takes-1-minute-for-car-thieves-to-get-into-your-vehicle-using-this-common-tactic/

[7] *Reddit user post on Lexus vehicle theft*. [Online]. Available: https://www.reddit.com/r/Lexus/comments/1etr1xt/psa_lexus_vehicles_easily_stolen_in_ca/?rdt=52001

[8] K. Tindell, "Can injection: Keyless car theft," *Ken Tindell's Blog*, Apr. 2, 2023. [Online]. Available: https://kentindell.github.io/2023/04/03/can-injection/

[9] D. E. Magda and B. R. Payne, *Kennesaw*, Sep. 2023. [Online]. Available: https://digitalcommons.kennesaw.edu/ccerp

[10] D. Goodin, "Canada declares flipper zero public enemy no. 1 in car-theft crackdown," *Ars Technica*, Feb. 10, 2024. [Online]. Available: https://arstechnica.com/security/2024/02/canada-vows-to-ban-flipper-zero-device-in-crackdown-on-car-theft/

[11] M. Mirhassani, Ed., "Securing the road ahead: Shield research centre leads in Automotive Cybersecurity," *Faculty of Engineering*, Nov. 13, 2024. [Online]. Available: https://www.uwindsor.ca/engineering/2024-11-25/securing-road-ahead-shield-research-centre-leads-automotive-cybersecurity

[12] S. Aziz, "With vehicle theft rising in Canada, what are automakers doing to beef up security? - national," *Global News*, Jan. 8, 2023. [Online]. Available: https://globalnews.ca/news/9392427/vehicle-theft-canada-security-measures/

[13] R. Verdult and F. D. Gracia, "Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer," 2022. [Online]. Available: https://www.cs.bham.ac.uk/~garciaf/publications/Dismantling_Megamos_Crypto.pdf

[14] H. Lopez-Vega and J. Moodysson, "Digital Transformation of the Automotive Industry: An Integrating Framework to Analyse Technological Novelty and Breadth," Jan. 2, 2023. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/13662716.2022.2161875

[15] *Stages Automotive Process Framework*. UL Solutions. [Online]. Available: https://www.ul.com/sis/stages/stages-automotive-process-framework

[16] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *Proc. IEEE Symp. Security Privacy*, 2010, pp. 305–316.

[17] R. H. Chowdhury et al., "The role of predictive analytics in cybersecurity: Detecting and preventing threats," *World J. Adv. Res. Rev.*, vol. 23, no. 2, pp. 1615–1623, 2024.

[18] S. Bebortta and S. K. Singh, "An adaptive machine learning-based Threat Detection Framework for Industrial Communication Networks," in *Proc. 10th IEEE Int. Conf. Commun. Syst. Netw. Technol.*, 2021, pp. 527–532.

[19] Y. Lu, "Security and privacy of internet of things: A review of challenges and solutions," *J. Cyber Secur. Mobility*, 2023.

[20] J. Bauwens et al., "Over-the-air software updates in the internet of things: An overview of key principles," *IEEE Commun. Mag.*, vol. 58, no. 2, pp. 35–41, Feb. 2020.

[21] M. Sathiyanarayanan, S. Mahendra, and R. B. Vasu, "Smart security system for vehicles using internet of things (IOT)," in *Proc. 2nd Int. Conf. Green Comput. Internet Things*, 2018, pp. 430–435.

[22] M. M. Raikar et al., "Fleet tracking and geofencing using the internet of things (IOT)," in *Proc. 3rd Int. Conf. Secure Cyber Comput. Commun.*, 2023, pp. 463–468.

[23] G.-H. Kim et al., "Vehicle relay attack avoidance methods using RF signal strength," *Commun. Netw.*, vol. 5, no. 3, pp. 573–577, 2013.

[24] A. H. Kumar et al., "Secure rolling code generation for remote keyless entry systems using AES-CTR, encryption with chacha20,"

in *Proc. 3rd Int. Conf. Smart Generation Comput., Commun. Netw.*, 2023, pp. 1–6.
[25] Chain, "Understanding can bus vulnerabilities and how blockchain can amplify security," *Medium*, Sep. 19, 2024. [Online]. Available: https://medium.com/@chaincom/understanding-can-bus-vulnerabilities-and-how-blockchain-can-amplify-security-a58388bf1fb4
[26] P. Sharma and J. Gillanders, "Cybersecurity and forensics in Connected Autonomous Vehicles: A review of the state-of-the-art," *IEEE Access*, vol. 10, pp. 108979–108996, 2022.
[27] Dubi, "Information transparency and data sharing," *Toronto Police Service Board*, Mar. 6, 2023. [Online]. Available: https://tpsb.ca/policies-by-laws/board-policies/363-information-transparency-and-data-sharing
[28] R. Rieke et al., "Behavior analysis for safety and security in Automotive Systems," in *Proc. 25th Euromicro Int. Conf. Parallel, Distrib. Netw.-Based Process.*, 2017, pp. 381–385.
[29] D. Damor, C. Gittins, and P. West, "Automotive IOT security: Understanding risks and implementing strong measures," *IOT Insider*, Sep. 4, 2023. [Online]. Available: https://www.iotinsider.com/iot-insights/automotive-iot-security-understanding-risks-and-implementing-strong-measures/
[30] Z. Abdollahi Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in Connected Vehicle Systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 12, pp. 3893–3902, Dec. 2018.
[31] B. Poudel and A. Munir, "Design and evaluation of a reconfigurable ECU architecture for secure and Dependable Automotive CPS," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 1, pp. 235–252, Jan. 2021.
[32] F. Pascale et al., "Cybersecurity in automotive: An intrusion detection system in connected vehicles," *Electronics*, vol. 10, no. 15, p. 1765, 2021.
[33] *Motor Vehicle Safety Act*. Consolidated federal laws of Canada, Dec. 10, 2024. [Online]. Available: https://laws-lois.justice.gc.ca/eng/acts/M-10.01/
[34] *National Highway Traffic Safety Administration (NHTSA)*. USAGov. [Online]. Available: https://www.usa.gov/agencies/national-highway-traffic-safety-administration
[35] V. M. Macharia, V. K. Garg, and D. Kumar, "A review of Electric Vehicle Technology: Architectures, Battery Technology and its management system, relevant standards, application of artificial intelligence, cyber security, and interoperability challenges," *IET Elect. Syst. Transp.*, vol. 13, no. 2, 2023.
[36] I. Lee, "Cybersecurity: Risk Management Framework and Investment Cost Analysis," *Bus. Horizons*, vol. 64, no. 5, pp. 659–671, 2021.
[37] I. Fernandez de Arroyabe, T. Watson, and I. Phillips, "Cybersecurity maintenance in the automotive industry challenges and solutions: A technology adoption approach," *Future Internet*, vol. 16, no. 11, p. 395, 2024.
[38] S. Hakak et al., "Autonomous Vehicles in 5G and beyond: A survey," *Veh. Commun.*, vol. 39, p. 100551, 2023.
[39] T. Pradhan and P. Patil, "Quantum cryptography for Secure Autonomous Vehicle Networks: A Review," in *Proc. IEEE Int. Students' Conf. Elect., Electron. Comput. Sci.*, 2024, pp. 1–10.
[40] T. Shon, "In-vehicle networking/Autonomous Vehicle Security for internet of things/vehicles," *Electronics*, vol. 10, no. 6, p. 637, 2021.
[41] M. Girdhar, J. Hong, and J. Moore, "Cybersecurity of Autonomous vehicles: A systematic literature review of adversarial attacks and defense models," *IEEE Open J. Veh. Technol.*, vol. 4, pp. 417–437, 2023.
[42] G. O. Young, "Synthetic structure of industrial plastics," in *Plastics*, 2nd ed., vol. 3, J. Peters, Ed. New York, NY, USA: McGraw-Hill, 1964, pp. 15–64.
[43] W.-K. Chen, *Linear Networks and Systems*. Belmont, CA, USA: Wadsworth, 1993, pp. 123–135.
[44] J. U. Duncombe, "Infrared navigation---Part I: An assessment of feasibility," *IEEE Trans. Electron Devices*, vol. ED-11, no. 1, pp. 34–39, Jan. 1959.
[45] E. P. Wigner, "Theory of traveling-wave optical laser," *Phys. Rev.*, vol. 134, pp. A635–A646, Dec. 1965.
[46] M. De Vincenzi et al., "Contextualizing Security and Privacy of Software-Defined Vehicles: State of the Art and Industry Perspectives," *arXiv preprint arXiv:2411.10612*, 2024.
[47] European Union, "General Data Protection Regulation (GDPR)," 2016. [Online]. Available: https://gdpr.eu/
[48] State of California Department of Justice, "California Consumer Privacy Act (CCPA)," 2018. [Online]. Available: https://oag.ca.gov/privacy/ccpa
[49] S. R. M. Technologies, "Automotive Cyber Security: Threats and Protective Measures," 2023. [Online]. Available: https://www.srmtech.com/knowledge-base/blogs/automotive-cyber-security/
[50] "Stages automotive process framework," UL Solutions, https://www.ul.com/sis/stages/stages-automotive-process-framework (accessed Jun. 19, 2025).
[51] Murphy, "Automotive spice: 0-60 in no time flat," *IEEE Engineering Management Review*, vol. 47, no. 2, pp. 26–28, Jun. 2019. doi:10.1109/emr.2019.2915217
[52] S. Ashkenazy, "ISO/SAE 21434 & ISO 26262: Automotive Security & Safety," Cybellum, https://cybellum.com/blog/iso-26262-and-iso-sae-21434-automotive-cybersecurity-must-go-hand-in-hand-with-functional-safety/ (accessed Jun. 19, 2025).
[53] "Functional safety," UL Solutions, https://www.ul.com/sis/services/functional-safety (accessed Jun. 19, 2025).
[54] "NTLM relay attacks: A dangerous game of hot potato: Crowe LLP," Crowe, https://www.crowe.com/cybersecurity-watch/ntlm-relay-attacks (accessed Jul. 2, 2025).
[55] Luo, F., Zhang, X., & Hou, S. (2021). Security threat analysis of in-vehicle network using STRIDE-based attack tree and fuzzy analytic hierarchy process. SAE International Journal of Connected and Automated Vehicles, 4(4).
[56] Ebrahimi, M., Striessnig, C., Castella Triginer, J., & Schmittner, C. (2022). Identification and verification of attack-tree threat models in connected vehicles (arXiv:2212.14435). arXiv. https://doi.org/10.48550/arXiv.2212.14435
[57] Li, Y., Liu, W., Liu, Q., Zheng, X., Sun, K., & Huang, C. (2024). Complying with ISO 26262 and ISO/SAE 21434: A safety and security co-analysis method for intelligent connected vehicles. Sensors, 24(6), 1848. https://doi.org/10.3390/s24061848
[58] Ponsard, C., Ramon, V., & Deprez, J.-C. (2021). Goal and threat modelling for driving automotive cybersecurity risk analysis conforming to ISO/SAE 21434. In Proceedings of the 18th International Conference on Security and Cryptography (SECRYPT 2021) (pp. 592–599). SCITEPRESS. https://doi.org/10.5220/0010603000003265
[59] Sowka, K., Cobos, L., Ruddle, A., & Wooderson, P. (2022). Requirements for the automated generation of attack trees to support automotive cybersecurity assurance (SAE Technical Paper 2022-01-0124). SAE International. https://doi.org/10.4271/2022-01-0124

Muhammad Ali Nadeem received his Bachelor of Engineering degree in Computer Systems; Master of Science degree in Engineering Management from the University of Portsmouth; Master of Arts in Economics, Bachelor of Applied Arts degree in Paralegal Studies from Longo Faculty of Business, Humber College; and his Ontario Graduate Certificate in Alternative Dispute Resolution from Humber College. He received his paralegal license from the Law Society of Ontario in 2020 and his Project Management Professional certification from PMI USA in 2013. Nadeem is a professional engineer (P.Eng.) and full-time professor with triOS / Sault College Toronto, and St Clair college, Windsor, teaching in-class and online courses in Cybersecurity, Forensic Law, and Project Management. His previous professional experience included working as the Head of Delivery Channels with ANB bank, Vice President, Online Channels Security for Citigroup, USA, and Systems Analysts for the Monotype Corporation, London United Kingdom.