Until quite recently, automotive security was synonymous with theft prevention. But with the software pie in the automobile growing exponentially to realize visions of the connected car and autonomous driving, security is now becoming synonymous with safety. And safety is undoubtedly the primary concern of every vehicle manufacturer. Recent experiments by researchers have demonstrated unaltered vehicles being remotely hacked into via their connected telematics unit and commanded to execute malicious code that allows the attacker to remotely control the vehicle. Thus, it has been proven beyond a shadow of doubt that security breaches in automobiles can have serious safety consequences. Therefore, vehicle manufacturers have to make security as much a priority as safety.

This paper gives an overview of security from an automotive perspective touching upon the motivations of attackers and the attack surfaces that a modern-day vehicle presents. This is followed by a brief discussion on the security characteristics unique to the automobile and mechanisms to address some, if not all of them. The paper concludes with a few approaches for the automotive industry to address the security requirement and Sasken's involvement in this area.

Author: Vinod Vasudevan, Senior Architect
Table of Content

Motivation for attacks ................................................................. 04
Automobile attack surfaces ...................................................... 06
Automotive-specific security considerations ......................... 10
Security mechanisms and techniques .................................. 11
Approach for addressing security in the automotive industry ... 18
Conclusion and future work ..................................................... 20
Motivation for attacks

Among the many motivations for hacking a vehicle, **theft** ranks highest. Theft is not new to automobiles. Being a high-value asset, thieves have long targeted vehicles. What the recent explosion of software in automobile and its increasing cyber-physical nature (like keyless entry and ignition) has done is unwittingly make stealing easier and less conspicuous. The increasing amount of sensitive, private information that vehicles are going to store (like credit card information) to enable ‘smart’ features in the near-future including automatic payments, are likely to become new targets for theft apart from the vehicle itself.
Next, would be espionage. Infotainment systems in vehicles track and record sensitive information like current location, location history, call history, contacts and addresses and with telematics becoming increasingly popular (mandatory in some countries), targeted exploits can be used to track people, eavesdrop on their calls and in-cabin conversations. It would be possible to even visually monitor them through compromised ADAS cameras intended for driver distraction detection.

Owners themselves may have motives using exploits to subvert regulatory constraints like emission controls for better fuel efficiency and performance. Used-car dealers might use exploits to hide faulty components by suppressing its notifications and avoid incurring replacement expenses. Depending on the ECUs targeted, such motives can affect the safety of the vehicle.

Research and ‘hacktivism’ have the more benign motive of exposing security vulnerabilities to get manufacturers and regulators to act. Pranksters and ‘black-hat’ hackers may indulge in it for the thrill or to show-off their technical prowess, though less likely given the high investment both in terms of time and funds required to craft a serious vehicle exploit.

Finally, nation-states, the underworld and terror organizations would have more sinister motives including espionage, physical harm and wide-spread damage. They are also likely to be the well-funded among the lot.
Attack surfaces refer to potentially vulnerable entry-points in the vehicle that can be tapped and exploited to gain unauthorized access. Windows, doors, exposed brake wires were the common attack surfaces in the bygone era of largely mechanical cars. The increased use of software and the introduction of different wireless connectivity technologies have significantly expanded the attack surface of a vehicle and the attendant risk of exploitation. In general, the larger the software content, the larger the attack surface owing to the higher probability of security-related bugs.
From a safety perspective, the prime targets for attacks are the ECUs that control critical vehicle components like the engine, brakes and steering. The vehicle network that interconnects these ECUs presents the attack surface. The most prevalent network technology in automobiles today is the CAN bus, short for Controller Area Network. Designed primarily for efficiency and reliability in the harsh automotive environment, CAN has very little provision for security. It is a broadcast bus where a message sent by one ECU is received by every other one in the network making it vulnerable to snooping. Further, CAN’s use of functional addressing means that messages have no information about the sending and receiving nodes making it easy to spoof messages on the network.

The diagnostic OBD-II port and exposed bus wires that control external vehicle components like ORVMs and lights can be exploited to gain access to the vehicle network but require physical access to the vehicle and, in the case of OBD-II, entry into the vehicle. Accessing the exposed bus wires would require an attacker to break open the ORVMs or the lights which is likely to set off the burglar alarm. As such, they present a lesser risk of a cyber-physical attack and are limited to the motives of people with legitimate access to the vehicle like technicians and owners.

Modern infotainment and telematics systems connect to the CAN bus to provide features like touch-screen based climate and body controls, remote diagnostics and remote vehicle status and control. The wireless connectivity features provided by these systems including Wi-Fi, Bluetooth and 3G/LTE, present remote attack surfaces that do not require the attacker to have physical access to the vehicle. These protocols offer wide attack surfaces owing to their large code size and complexity and they extend the range of remote attacks to many tens of meters, even kilometers.
of meters, even kilometers. Attacks on this surface typically exploit authentication bugs in the protocol implementations to gain access to the infotainment or telematics ECU and exploit further bugs like buffer overflows and unprotected software updates to plant malicious code that can then control other safety-critical ECUs through spoofed CAN messages.

**Key-less entry and ignition systems** also offer a remote attack surface. These systems employ RF-based protocols for detection and authentication of owners to unlock the doors and start the engine. These protocols lend themselves to remote eavesdropping using ‘sniffers’ and, as shown by the hacking of the Megamos Crypto transponder, rather easy exploitation by spoofing. The attack surface is relatively small and is unlikely to contain a back-door to more safety-critical systems but a compromise grants an attacker access to the vehicle’s OBD-II port which can be exploited to plant safety-threatening code in any of the ECUs connected to the CAN bus.

**FM radio receivers** in car radio systems have been known to be attacked by fake FM transmitters broadcasting RDS-TMC information that adversely influences the navigation system. Similarly, **media content distributed via CDs and USB-sticks** under the guise of marketing offers have been known to exploit vulnerabilities in the media parsing code to plant malicious software in the infotainment ECU. While these exploits may not have directly compromised the safety of the vehicle, they did jeopardize the safety of the occupants by distracting, confusing or alarming the driver.

With ADAS (advanced driver assistance systems) taking more and more control of the vehicle away from the drivers, the sensor technologies that these systems rely on like **radar, ultrasound, cameras and DSRC (for V2X)** present attack surfaces that could seriously impact the safety of a vehicle. One can easily imagine spoofed radar or DSRC signals being used to confuse ADAS algorithms into braking hard and steering away to avoid a non-existent obstruction or signal jammers preventing algorithms from detecting potentially dangerous driving situations.
**Smartphones** can also present a vehicle attack surface via downloadable Trojan Horse applications. An attacker could use these applications to gain entry through a paired Bluetooth or authenticated Wi-Fi connection into an otherwise secure infotainment system.

Lastly, **compromised dealership or workshop infrastructure** could open doors to attacks on vehicles brought in for repairs or regular maintenance. ‘Pass through’ devices used in workshops for access to a vehicle’s OBD-II port from a remote computer or laptop over a Wi-Fi connection are prime examples of such vulnerability. Weak IT security policies in these workshops could lead to its Wi-Fi network being compromised allowing unauthorized computers remote access to a vehicle’s OBD-II port.

The primary focus for IT security is confidentiality of information whereas for automotive it would be integrity and availability.
Automotive-specific security considerations

Thankfully, cyber-security itself is not a new topic and the decades of research into it has yielded a wealth of solutions and strategies for many fields of application, e.g., IT security. As the compute and connectivity technologies of these fields make their way into the automobile along with their attendant security risks, it is instructive to study the security strategies and solutions employed in those fields for adaptation to the automotive context.

However, not all of it may be directly relevant. For example, the primary focus for IT security is confidentiality of information whereas for automotive it would be integrity and availability. As such, it is important to keep in mind specific characteristics of automotive security while adapting existing solutions and strategies. Some of these characteristics are:

**Cyber-physical characteristics.** A cyber-security breach in an automobile could potentially have serious safety consequences leading to injury and loss of life and property. As such, it does share some similarity with other fields like industrial automation, aerospace and healthcare.

**Long product life.** The operating life of an automobile is anywhere between 10-20 years, much longer than the average lifespan of most security mechanisms. To exacerbate the problem, the long 2-3 year development life-cycle of an automobile means that the employed security mechanism is possibly obsolete almost as soon as it hits the roads.

**Easy physical access.** Vehicles are regularly left unattended for long periods of time in public places like parking lots giving attackers relatively easy physical access to them. Owners may turn attackers and hack the vehicle to get it to perform outside its permissible, safe limits for performance or fuel efficiency reasons inadvertently posing a safety threat to themselves and others on the road.

**Cost.** The effort, and therefore the cost, of securing a feature is typically many times more than the effort required to add it to the system. Unofficial estimates claim the delta to be in the region of 3-5 times. In a cost-sensitive market, security being a non-differentiating feature, buyers may be unwilling to shell out extra money to secure the differentiating connectivity features they desire.
Security mechanisms and techniques

The key tenets of automotive security in a rough order of priority are ensuring integrity, authenticity, availability, confidentiality and non-repudiation of the system.

- Integrity and authenticity of the hardware and software in the system, including firmware upgrades and downloaded applications.
- Authenticity, integrity and confidentiality of internal as well as external communications. Confidentiality of stored information.
- Availability of the critical components of the system at all times to ensure functional safety by preventing denial-of-service attacks.
- Tamper-proof ‘black-box’ collection of digital forensic data to aid in security breach investigations.

Security mechanisms to achieve (most, if not all) of the above goals fall broadly into two categories: cryptography-based schemes, and intrusion detection and prevention (IDPS) schemes.

Cryptography-based schemes. These schemes use various cryptographic algorithms to verify authenticity and integrity and to ensure confidentiality. There are two types of cryptographic algorithms: symmetric and asymmetric. Asymmetric algorithms like RSA and ECC, which use a pair of unidirectional keys, offer more reliability than symmetric algorithms like AES which use a single, shared secret key. However, asymmetric algorithms are computationally more intensive. For optimal resource usage, most schemes employ a combination of the two with an asymmetric algorithm for authentication and initial key exchange and a symmetric one for subsequent high volume operations.

Public key cryptography (PKI) is a cryptographic technique based on asymmetric algorithms and digital certificates.
It is an effective mechanism for verifying the authenticity and integrity of the system software. This is achieved using digitally signed software images which are verified by a secure boot mechanism on the ECU. A digest of the software image encrypted using the OEM’s private key is stored on the ECU. At start-up, the secure boot code of the ECU decrypts the stored digest using the OEM’s public key, computes the digest of the stored software image, and loads the image only if the two digests match. Once loaded, the software image can then verify the authenticity and integrity of other components like the file system, downloadable applications, and software upgrade packages thus establishing a chain of trust rooted in the secure boot code.
Similarly, transport layer security (TLS) protocols based on PKI can be effective in securing communications with external entities including telematics service providers, consumer smart devices and, in future, other vehicles and ITS infrastructure. The authenticity of the entities involved in the communication is verified using digital certificates and confidentiality is maintained by encrypting all communication. Here, typically, a strong asymmetric algorithm is employed for authentication and key exchange following which a symmetric algorithm is used for encryption of the communication. For communications with smart phones and other devices, the built-in authentication mechanisms of the underlying transport mechanism like Bluetooth and Wi-Fi add a further layer of security by allowing only authorized devices to connect to the vehicle’s personal-area network.

The concepts of TLS can be adapted to secure internal communication over the vehicle bus too. Asymmetric algorithms can be used to distribute a periodically-changing network secret key that is subsequently used by ECUs to encrypt communications using symmetric algorithms. Inclusion of a random number field in the payload of the network packets combined with the encryption will be effective in preventing replay attacks. Since the prevalent protocols for vehicle networks like CAN (Controller Area Network) leave the specifications for the payloads open, such security mechanisms can easily be added as a layer above the protocol’s network layer implementation.

PKI-based authentication mechanisms can also be effective in securing internal communications between critical driver assistance systems and vehicle sensors, like cameras and radar, against man-in-the-middle attacks by counterfeit replacements. MirrorLink, a smartphone connectivity achievement effective security with acceptable latency would require a major upgrade of all ECU hardware with the attendant complexity of software re-design and re-validation, not to mention the challenge of getting ECUs from different suppliers to talk the same security language, all of which will translate to higher costs and delays.
Automotive Security

protocol that allows drivers safe access to their mobile applications by mirroring the phones screen on the head-unit, uses one such mechanism to authenticate MirrorLink-certified phones and validate the integrity of the frame-buffer data streamed by them. In MirrorLink, authentication is done using digital certificates and a session key is securely exchanged using an asymmetric algorithm. While streaming the frame-buffer data, the phone encrypts some property of each frame, e.g. frame-size, sequence number or a SHA-256 digest of the entire frame, using the shared, secret key which is subsequently validated by the head-unit. An adaptation of this mechanism can be used to prevent similar attacks on the data feed from the vehicle’s camera and radar sensor ECUs. Sensors with analog front-ends and exposed analog connectivity, however, present an attack surface immune to digital protection mechanisms. Key-based signal modulation and watermarking in the invisible spectrum (similar to Cinavia watermarking for audio) are options that can be explored for such sensors. However, a trade-off between CPU capabilities and the degree of security is inevitable.

Cryptographic algorithms are generally compute-intensive and would require support on the ECU platform for hardware acceleration to achieve strong security within acceptable latency limits, especially when used for time-critical communication on the vehicle bus. Further, support in the hardware for secure, tamper-proof storage of keys, certificates and user credentials would be required to protect their confidentiality. These requirements are beyond the capability of the typical micro-controllers used in majority of the ECUs in a vehicle today. Achieving effective security with acceptable latency would require a major upgrade of all ECU hardware with the attendant complexity of software re-design and re-validation, not to mention the challenge of getting ECUs from different suppliers to talk the same security language, all of which will translate to higher costs and delays.

Intrusion detection and prevention schemes (IDPS). IDPS schemes work by continuously monitoring the system for abnormal or unusual behavior (anomaly detection) and, on detection of such behavior, initiating processes to bring the system to a ‘safe mode’ and prevent further damage. These schemes can be an alternative, or used in conjunction with, cryptographic techniques for verification of the authenticity of the vehicle’s internal and external communication. As opposed to cryptographic methods, IDPS mechanisms are not as computationally intensive and do not require hardware support beyond what is available in typical automotive micro-controllers. This makes them an attractive proposition for securing the vehicle bus, especially the CAN bus.
As mentioned earlier, the design of the CAN bus makes it very easy for a rogue ECU to spy on all bus communications and also spoof messages from other ECUs. IDPS techniques offer a cost-effective alternative to cryptographic methods for preventing such attacks on the CAN bus. Some of these techniques include:

- Monitoring all broadcast messages on the CAN bus for anomalies with respect to the original OEM network design. Since rogue ECUs can only add messages to the bus and not remove messages from it, the typical modus operandi to spoof an ECUs message would be to flood the bus with the counterfeit message effectively ‘drowning out’ the authentic ECU. This would, however, imply a sudden spurt in the message frequency which can be detected as an anomaly by the monitor. Other parameters that can be monitored include the range of values of message fields, appropriateness to the current state of the vehicle, etc.
• Using sequence numbers for each message on the network. Since the rogue messages would have to use incremented sequence numbers to ensure that they are processed, subsequent communication from the authentic ECU is bound to carry a stale sequence number that can be detected as an anomaly.

• Messages on the CAN bus usually originate from unique ECUs. Thus, each ECU can monitor the bus for messages originating from that ECU but not sent by that ECU indicating spoofing by a rogue ECU.

IDPS is effective in certain attack scenarios where cryptography is ineffective. A good example is denial-of-service (DoS) attacks that affect the availability of the system. The CAN bus is especially prone to DoS attacks. Due to its unique, priority-based bus arbitration scheme, the protocol can be exploited by a rogue ECU to completely flood the bus with high priority junk messages effectively ‘drowning out’ all authentic communication and seriously jeopardizing the functionality of safety and time-critical components in the vehicle. A bus monitor can easily detect such a situation and initiate preventive safety measures.

Once an anomaly is detected, an IDPS scheme has to initiate measures to mitigate the safety risk due to the suspected intrusion. In the automobile context, this could be broadcasting a special message on the CAN bus to instruct all authentic ECUs to enter into a ‘safe mode’ with bare-minimum functionality enabled to bring the vehicle safely to a halt. The system could also display, via a separate ‘hot-line’ wiring, a warning on the instrument panel, similar to the ‘Check Engine’ light, to inform the driver of a suspected attack.

Given the unique benefits of cryptographic and IDPS mechanisms, a practical automotive security framework is likely to employ a combination of cryptographic and IDPS mechanisms for multiple reasons. One of the primary reasons is cost. As mentioned earlier, effective cryptography-based security schemes in automotive dictate an overhaul of the ECU hardware which has significant cost implications in terms of development and validation. A more practical approach would be to use such schemes in a few, critical ECUs that either already have the requisite horsepower or can be upgraded with minimal impact on the overall cost.

Security, therefore, is a moving target and a mechanism to continuously upgrade the vehicle’s security measures during its operational lifetime is crucial to its safety.
The infotainment and telematics ECUs that house all the external-facing wired and wireless connectivity services are good examples. These ECUs typically use high-end processors that already have advanced hardware support and software interfaces for security. Similarly, so-called gateway ECUs, that interface the sensitive vehicle bus with the rest of the system, that are ideal candidates for IDPS implementations, can be fortified with hardware enforced security to ensure that the IDPS code is authentic and not tampered with. Using such combinations of cryptography and IDPS based schemes a reasonable level of security can be achieved at a much lower cost. Another reason for a combined approach would be to cover the limitations of individual approaches and address a wider range of attack scenarios, the DoS attack being a case in point. Finally, multiple, orthogonal, redundant security schemes provide additional rings of protection making intrusion much more difficult.

Whatever the mechanism, the long product life of the automobile implies that the vehicle is more likely than not to outlive the effectiveness of (some if not all) security measures employed rendering it vulnerable to attacks eventually. Security, therefore, is a moving target and a mechanism to continuously upgrade the vehicle’s security measures during its operational lifetime is crucial to its safety. Firmware updates, either over-the-air or dealer distributed, as a result, are bound to be an integral part of automotive security and safety.
Approach for addressing security in the automotive industry

**Eschew security by obscurity.** The automotive industry has traditionally been a ‘closed’ system relying heavily on proprietary solutions the design and implementation of which is not publicly available. This may have lulled the industry into a false sense of security that needs to be abandoned as it is a well-established fact that security by obscurity is the least effective mechanism. Nowadays, sophisticated reverse engineering tools like IDA Pro significantly ease the job of extracting the implementation logic from object code effectively making all code ‘open-source’. The chosen security mechanism must be immune to scrutiny. PKI-based mechanisms are a good example.

**Depth-in-defense.** Rather than a secure-the-perimeter approach, which employs just one line of defense, a multi-level security approach is recommended to limit the extent of damage in case of a breach. Having multiple, orthogonal and possibly redundant mechanisms for security vastly reduces the probability of a single breach compromising the entire system.

**Holistic approach.** Security has to be treated on par with safety as it is clear that a security breach can seriously affect the safe functioning of the vehicle. Just as safety considerations are woven into each step of the automotive development fabric, security considerations too must be deliberated at each step of the development process from design to validation to procurement and vendor management. Security considerations must also extend to the infrastructure, tools and processes of after-sales services like dealerships, maintenance workshops and telematics service providers. It is not only about securing the automobile but the entire automotive development, distribution and after-sales service eco-system.
Eliminate software bugs. The best security mechanisms can be subverted by bugs either in the implementations of these mechanisms or in the software that they protect. Buffer overflow bugs in implementations of the pairing and authentication mechanisms of Bluetooth and Wi-Fi have been shown to be exploited to gain access to the vehicle’s infotainment system. Even on platforms protected by secure boot, such bugs can be exploited to load and execute malicious code after boot-up with potential safety consequences. The only real answer to this problem is to adopt processes, standards and tools like MISRA, JSF AV C++, etc. to reduce the occurrences of such bugs during development. Ethical, white-hat hackers must be encouraged, enabled, even employed, by the industry to find security holes before people with less noble motives do. As more and more manufacturers adopt standard open-source platforms, like GENIVI, for their infotainment and telematics systems, favorable models for sharing the cost of this security scrutiny among member OEMs could emerge, reducing the overall cost of security – after all a non-differentiating feature – for each individual OEM.

Reduce cost. Adopting a common, standard software platform does open up opportunities for cost reduction by sharing the cost of security validation with other manufacturers. From a hardware architecture perspective, reducing the number of ECUs by consolidating multiple functions into a single ECU can make inclusion of hardware cryptography economically viable. For example, individual ADAS algorithms typically reside in separate ECUs. The cost of securing all these ECUs with hardware-assisted cryptography is considerably more than securing one ECU with all algorithms integrated.

Store forensic data. As the electronics in the vehicle takes more and more control away from the driver to the point of autonomous driving, investigations into safety incidents due to security breaches will require the vehicle to securely log non-repudiable forensic data in a tamper-proof location for use as evidence. As such, a system security design should consider the system parameters that constitute forensic evidence and provision for a digital ‘black-box’ for secure logging of such parameters.
As vehicles become more connected and more autonomous, the distinction between security and safety becomes more blurred. As recent investigations have shown, security breaches can have serious safety consequences. The most recent event of an unaltered vehicle being remotely hacked and brought to a complete halt in the middle of a busy highway has caused not only the automotive industry but also governments to sit up and take notice. US Senator Ed Markey’s ‘Tracking and Hacking’ paper clearly outlines the threat to modern vehicles and mentions the need for NHTSA to come up with new standards and guidelines to protect the security of vehicles. Security, therefore, is as much a priority for the automotive industry as safety. The challenge is to find reliable, cost-effective solutions to secure the vehicle over its long operational life.

As part of our ‘Connected Car’ solution, featuring modern infotainment and telematics capabilities, Sasken has actively been considering security issues and exploring and experimenting with various mechanisms to mitigate them. Our immediate areas of focus are the following:

- Secure boot of a Linux-based platform
- Secure communications over telematics transport protocols like MQTT and AMQP
- IDPS mechanisms for securing the CAN bus

Our early work on secure boot of the Linux kernel has already been successfully adapted for use in a few of our customers products, including a mobile radio terminal from a leading UK-based manufacturer. Sasken has also forged strategic partnerships with industry leaders to integrate advanced features like secure FOTA into our ‘Connected Car’ solution which, as identified earlier in the paper, is a critical component of effective automotive security.

Conclusion and future work

Sasken has actively been considering security issues and exploring and experimenting with various mechanisms to mitigate them.