THE UNIVERSITY OF WESTERN ONTARIO
DEPARTMENT OF COMPUTER SCIENCE
Computer Networks 2

5 Layer Security Architecture for Connected Vehicle System

Akanksha Nayer *anayer@uwo.ca*
Harsh Dhillon *hdhill48@uwo.ca*
Jessica Patel *jpate272@uwo.ca*
Pankaj Kumar *pkumar59@uwo.ca*
Sai Deepthi *srajaput@uwo.ca*

ABSTRACT- Modern vehicles represent a complex distributed network of connected hardware and software systems, which aim to provide full automation to the Connected Vehicles (CV). But every IT system that operates via communication networks is a subject to potential security vulnerabilities. In this project, we identify the required security and privacy guidelines as well as design a security framework to safeguard the Connected Vehicles. We aim to address the many challenges of security and privacy risks, which will further help to increase the level of confidence and trust in connected vehicle systems.

INTRODUCTION

In current modern age, all electronic devices need network connectivity to perform their specific tasks. Every device we come across operates in one form or another by using various network communication channels. Advances of in-vehicle technology have paved the way to connect vehicles to the external world. Car makers are adding various connectivity and telematics solutions for passenger and fleet vehicles. Connected Vehicles are not an exception either. This wasn't the case few decades ago, when vehicles were simple electromechanical artifacts. Modern vehicles are advanced cyber physical systems that depend on hardware and software connectivity for their daily operations. Connected Vehicles Systems (CVS) integrate various hardware and software modules where several of its key components depend on the internet to run efficiently.
Communication (cellular) and wireless connections (Wi-Fi) are capable to make the car equipped with a large amount of information regarding weather, road traffic, police, accidents and other essential information. Making the entire system susceptible to external attacks. Automotive industry has seen a remarkable progress in the past few decades. Future of the modern vehicles is connectivity, automation and a secure integration with the intelligent IT systems. The shift of automobiles from being an electro-mechanical system to cyber physical system has opened a lot of business and technological opportunities. But every IT system that operates via communication networks and open internet is a subject to security vulnerabilities.

Same is the case with security in connected vehicle systems that has become a new factor that needs to be considered in systems engineering and security analysis. Automobiles already work in fast paced and dynamic environments, this makes it a very complex and vital challenge to create security assurance frameworks which can become scalable and form a global consensus.

This in turn leads to a very stringent requirement on the security network interfaces being used by the vehicle to transmit and receive data. The vulnerable system must be safeguarded with various security measures and protected from any possible future attacks. To maintain the public trust in connected vehicle systems, efficient security assurances frameworks must be designed and delivered. High security assurance levels can be very hard to maintain, but it should be an utmost requirement when we

consider systems engineering and security analysis for the connected vehicles systems.

PROBLEM STATEMENT

Connected Vehicles have a very large attack surface in one go, that makes it very susceptible to the possible harmful cyber-attacks against the network. If any component of the connected vehicle gets compromised there exists a greater possibility that a wide range of key functions of the system can be manipulated thus compromising the security of the driver. The network system is at a high risk in a Connected Vehicle of being hacked or hijacked, its control unit being compromised, or functionalities being exploited[1]. This can easily be achieved by hackers through USB firmware update attack, OTA (Over the Air) malicious updates, harmful application installation or even if vehicle communicates with unknown vendors that might misuse personal data.

One of the prime challenges that Connected vehicle face is the unauthorized access to the system that can be gained through external interfaces such as On-board diagnostics (OBD) ports, Telematics unit, in-vehicle connection points, and wireless system. Due to the large attack surface and non-existence of any standard mechanisms to handle security threats in the current automotive system, there is a crucial requirement to design optimum security frameworks for maintaining and keeping the control of CVS with their users and making it a very secure ecosystem for communication and data exchange with other connected vehicles and various network channels.

RELATED WORK

Researchers in the past have performed comparative analysis between two instances of vehicle-to-infrastructure communication [2]. From the experimentation results they have gained useful insights about how different technologies, road-side units, cloud-based service and entities involved in the connected car paradigm influence the numerous levels of security assurance framework. The techniques being used are outlined in order to limit the attacks at the application layer with the help of security modules. However, these techniques are still incompetent because there separation is quite logical between the ECU (Electronic Control Units) and computation. Software protection from tampering and from getting manipulated from invasive and internal attacks is required, by using physical bus access in the network controller. In the current scenario the vehicular technology architecture is bound by some restrictions which aren't feasible in the real time environment for the very practical reasons.

Efforts have already been presented that unify protection efforts using SHE(Secure Hardware Extension) a cryptographic accelerator integrated in the vehicle system [3].The Secure hardware extension has been defined in the EVITA project [4]. They have implemented protection in terms of securing the ECU using SHE. The paper Qiang Hu et al. has used the layer approach but it is quite different than our idea, and made use of MAC predominantly and mentioned SHE and its functionality in the paper. The most recent work in this domain is done in 2015 by Shreejith and Fahmy [5], wherein their alternative approach for integrating encryption into standard network controllers has been briefly explained, here it shows no impact on communication latency. A fully featured implementation with symmetric cryptography and protocol obfuscation has been shown in Shreejith and Fahmy [5].

However, these approaches rely on network controllers mainly non-standard on FPGAs. [6] state through their work that approaches like SHE are computationally simpler than asymmetric approaches and are even faster, because SHE is a hardware support. There has been a mention of mitigated scaling effects through obfuscation of Controller Area

Networks (CAN) message IDs, proposed in a latest paper Lukasiewycz et al. [7].

TECHNICAL CONTRIBUTION

Internal networks can be easily manipulated by hackers which can lead to tragic events such as total loss of control. Our project contributes towards the development of an efficient authentication and authorization framework that would emphasize on key components of security, privacy and safety protocols in a single design process, eventually making it completely compatible with the current Connected Vehicle's processes. Externally-connected devices collect in-vehicle data, and makes sure the messages are injected into the in-vehicle networks. This paper highlights the methods for such integration of the framework into the automotive cycle creating an authenticated data transmission in-vehicle and vehicle with infrastructure, justifying and addressing the issues mentioned in the first section of the paper. Focusing on the loopholes that pull back the efficient working of the connected vehicles making it vulnerable, we have covered the ECU, single component data exchange, security measures through encryption like (SHE), authentication provided to each message through (MAC), Hypervisor Approach and (HSM). Eventually, we have identified several gaps that exist in the connected vehicle environment.

PROPOSED SOLUTION

As a solution to the security issues we have developed a high level architecture for each module that depict particular layer of the Connected vehicle paradigm that focuses on internal as well as the external framework of key units which are extremely prone to potential hacks if left unsecured.

We explored various units, networks and protocols involved in the development of connected car paradigm. Based on our exploration and research, we have designed an efficient and reliable security system. Secure Internal Framework is a vital part of a Connected Vehicle Architecture.
Our architecture takes into account two communication channels for providing security.

Path1: To secure communication over the in-vehicle network, e.g., CAN

Path2: To secure communication over a wired/wireless network, e.g., Wi-Fi, USB, etc.

Our design of secure architecture will also include these key features:

Access Prevention: Gateway Firewalls must be designed and authenticated in such a way that any intruders are not able to access and tamper safety such as the braking system of the vehicle.

Detection: Intrusion detection capability is a must in security architecture and it should also validate the authenticity of the software in use to maintain the root of trust.

Intrusion handling: We built the architecture in such a way that it detects and handles any possible intrusions. It needs to have a pre-programmed protocol and lockdown procedure in case of any successful attack in the system.

Update vulnerable system: Connected vehicle architecture must be able to update the core system and modules securely in a timely manner so that vulnerabilities are fixed and it prevents the vehicle from exploitation.

We used these following key features for our secure framework development that have summed 5 layers of protection to provide end to end security to the connected system.

Secure Interface works at securing the communication channels.

Secure Gateway works at providing domain isolation along with separation of various components.

Secure Network secures communication between ECU's.

Secure processing of the software before they are deployed on the CV system.

Secure Update provides the core system updates which reduce the chance of attacks in an efficient and convenient way.

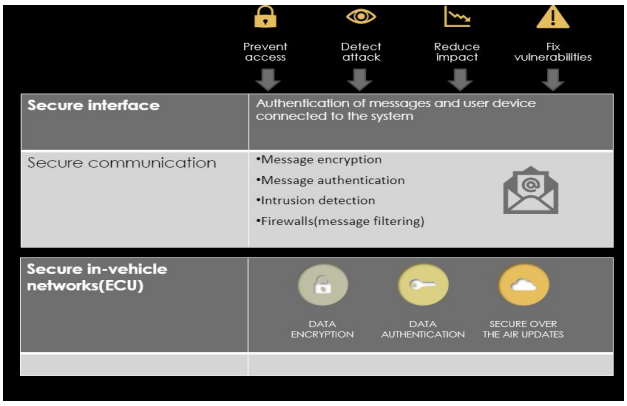

Figure 1.0

Layer 1: Secure Interface

Originally the automotive systems were closed systems that had only OBD port as the single possible interface to connect to the outer world. With more advancements CV interfaces with multiple devices in order to provide more features and services like Advanced Driver Assistance Systems which entails the increase in number of external interfaces. This integration can introduce severe security threat to the Connected Vehicle as several studies have already suggested that an in-vehicle network can be easily be targeted and compromised and security can be breached via the On-Board Diagnosis Port(OBD), Telematics Control Unit or the infotainment system. [8]

Attack Scenarios

For this layer we worked on the following attack scenarios:

Scenario 1: Compromised User Device (UD): This attack can be made by attaching corrupted devices or compromising a genuine User device. The use of compromised device can easily affect the functionality of Connected Vehicle as interaction between communication devices eg: Telematic Control Units (TCU) and OBD port and User device is done over generic network.

Scenario 2: Compromised communication device: In this kind of attack scenarios the most convenient way for hackers to connect with the

	Communication Device(TCU)	UD(User device)	Attack cases(A1,A2,A3,A4)	Security Countermeasures
Scenario 1	Not Compromised	Compromised	A1,A2,A3	A1,A2: Key Management, Password management A3: Require update authentication Maintain update server Verification of server certification
Scenario 2	Compromised	Compromised	A1,A2,A3	
Scenario 3	Compromised	Not Compromised	A1,A2,A4	A4:Communication path between the user device application and the server should be encrypted, e.g., https.

Table 1: Possible attack scenarios and their countermeasures

vehicle is through USB ports or if given physical access to vehicle NAND flash chip components can be altered.

Scenario 3: Both User device and communication device are compromised (This is a subpart of scenario 2).

These attack vectors can be further classified as follows:

Attack Vector 1(A1): Extracting the key after compromising entities (TCU /UD)

Attack vector 2(A2): Making use of invalid keys.

Attack vector 3(A3): The applications installed on the User device that connect the user to the vehicle contain vulnerability that does not verify

the server's certificate.(Man in the middle-field attack).

Attack vector 4(A4): Fraudulent requests can be sent to the CV as vehicle's 2G/3G protocols include vulnerabilities(Man in the middle remote attack).

Countermeasures

Key Management: Every device has both private keys and public keys stored for logging in to the updated server. By having private key on the device the automotive manufacturers create a new attack vector for the device [9]. Use of public key should be sufficient. If in any case device authentication is needed every device should have a unique key.

Verify server certification/Require update authentication: The SSH/SCP over which the update is performed provides privacy protection and integrity over all the communication done but the remote host is not verified by the device which means that the device authenticates itself to the server but does not check if the server update is authentic or not. To check the authenticity of the received update code signing should be done.

Layer 2: Secure Gateway

Gateway provides all sorts of in-vehicles interactions to take place in the connected vehicle. It is the access point for the other external connecting devices to the vehicle.

The prime motive here is to make the communication as safe as possible between the networks and the ECUs (electronic control units). One of many ways would be to link the vehicle's internal and external network. The transfer to not get disrupted and function smoothly must contain the authenticity and ample necessary information. For a range of vehicles, central gateway acts as a hub to securely interconnect and process data [10]. This security element provides physical isolation such that data is shared privately between concerned functional domains.

Message authentication codes (MAC) provide authentication based on symmetric cryptography that can be used to provide security to data control, data exchange and inter and intra layer communication. This acts as a checksum to data to be in typed in. Having this functionality enabled us to put it in practice for our project, securing the gateway layer.

Advanced encryption standard based MAC gives better outcome where securing the communication is concerned when it is applied onto the **Secure Hardware Extension (SHE)**. Further working for the architecture and processes for information exchange are significantly faster when support by SHE is extended upon the hardware.

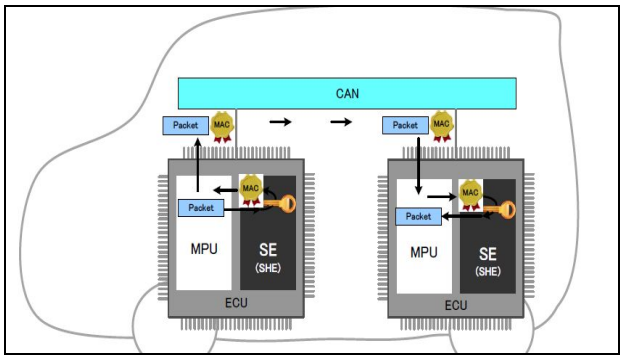

Fig 2: Gateway with SHE and MAC security

The access to external device is constrained by authentication. Thus, the encryption through SHE makes sure the system abides by the rules and render smart protection to the components in ECU[11].

There are two aspects that come into picture here, exchange of keys in secure manner as well as distribution of keys to the control unit that would in turn enable encrypting their messages, eventually maintaining the authentication of ECU and other components in it.

So authentication of ECUs play the major role in ensuring the participation in communication and to detect intruders, also to recognise legitimate ECUs.

Layer 3: Secure Network

Authentication protocols and gateway isolation reduce the attack surface significantly by the time network layer is reached. But the sub-network is still vulnerable to attacks via message manipulations that can be attempted by hacking various Original Equipment Manufacturer (OEM) units present in the system. It is not possible to apply security upgrades to existing microcontrollers and their proprietary software. Different manufacturers share different standards and protocols.

So, we require a solution which we can integrate with the existing internal hardware. Layer 3 protects the ECU (Electronic Control Units) domain by doing 4 vital things –

Adding message authentication scheme: Each message is extended with a cryptographic code to guarantee an authenticated sender and receiver relationship.

Encryption: Data and identity theft can be mitigated by encrypting the messages between different ECU's inside the vehicle.

Pattern recognition: This can be used to detect anomalies in the network traffic and to identify and block malicious packets before they reach microcontrollers, this also includes message rate limiting to avoid denial of service attacks.

ECU level validation: Regularly validate the authenticity of ECU's software.

These features can be enabled by security subsystems (including cryptographic accelerators) that are integrated in the microcontroller [12]. However, it is not feasible for Equipment Manufacturers to apply a security upgrade to all existing microcontrollers. The associated cost for validation and integration of the modified hardware would simply be too high. A software centric approach is a more cost-effective solution, as it reduces the need for each OEM to re-develop their software for every ECU.

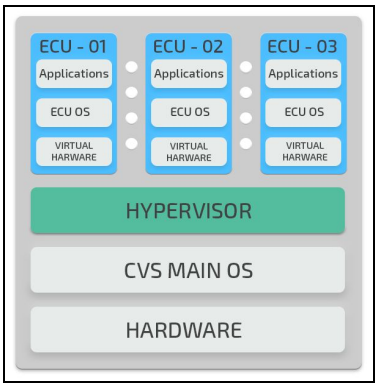

Fig:3 HYPERVISOR Architecture

Software Solution - Hypervisor Approach

Hypervisor is a software architecture developed to manage virtual machines which can be used in ECU domain [13].
Virtualization has been in use for decades for servers and other high-level computing areas. Machine virtualization is a perfect fit for connected vehicle as it makes it much harder for hackers to gain access. Hypervisor can be enabled by in-car infotainment systems. This layer of complexity is prone to latency, but processing speed of microcontrollers is expected to rise. Making virtualization possible in future connected vehicles.

Hardware Solution – Hardware Security Module:

HSM is a physical computing device that provides message authentication between Electronic units present in the CAN layer. It also acts a digital key manager. HSM's can be used with existing microcontrollers. They will provide secure storage and a local root of trust. They also enable cryptographic processing of CAN messages [14]. Industry recognizes that digital certificates and encryption are a key to provide safety. Hardware security modules

address the ECU safety in various case studies cited in our research. Further, HSM also enable authentication control for third party apps, which safeguards the customer's private data as per new GDPR laws.

Layer 4: Secure Processing

Connected Vehicles are all about software. Hidden flaws in software can help bad actors to access, modify and corrupt software and it will lead to accident and potential threat to life and property. These vulnerability will not only provide threat to life and property but can also have serious risk of exploitation which will result in system compromise, information leak or denial of service at a very large scale. Common Vulnerability and Exposures (CVE) is a database which provide a reference method for publicly known for information security vulnerabilities and exposure. CVE vulnerability data are taken from National Vulnerability Database (NVD) which is provided by National Institute of standards and Technology and other sources [15].

Most of the vulnerabilities in a software are due to lack of attention paid by programmer and because of code reusability which is available publicly over internet. There need to have a guidelines for the connected vehicle software industry which should be mandatorily followed to minimize the flaws in system when they are deployed into the connected vehicle. Providing an interface where the stepwise approaches are attained with least anomalies and highest degree of security possible, we bring into picture 'secure processing'.

1. All chips must be authenticated and loaded with trustable software – We need a robust system where all the chips which will be used in the connected cars should be injected with private keys and a certificate, wherein it will work as root of trust. Shifting security to chips will take longer time but security advantage of this root of trust system is that user identities and keys which once embedded on chips will allow them to store more securely.

2. All the IT companies are certified by one or another **certificate** level like International Organization of Standards (ISO), Capability Maturity Model Integration (CMMI) etc. These certifications helps customer to select which vendor to approach. In the same way Connected Vehicles Vendors and their sites should be certified via vulnerability assessment and should be require to maintain a certificate. This will not only maintain safety to customers but it will also create industry standards. IEC 61508[16] is one of the example of International Standard which was published by International Electrotechnical Commission which provides a guidelines for the automated vehicles to follow some of the methods like how to apply, design, deploy, and maintain automatic protection systems.

3. Connected Vehicles need to have a **standardized software** so that even though different vendors develop these softwares, still they should be able to transfer data amongst each other and make decisions on the shared data and avoid crashes.

4. In current standard where software companies scan their source code through different **scanning tools** during software development process which is used to detect certain vulnerabilities based on defined rules have limited capabilities. With the recent enhancement in the technology and the amount of data source available, it has become possible to train the data source and find the pattern in the source code to detect the vulnerabilities using Machine Learning [17].

5. In Machine learning, we need to extract features from the source code on which the models can be trained using Deep Representation Learning. The models which

can be used for Deep Representation Learning would be Convolutional Neural Network which will be used for feature extraction from the source code and Recurrent Neural Network can be used for functional level source vulnerability classification.

6. **KeYmaera:** Can be used for testing and verification of the softwares[18]. It is a hybrid verification tool for systems that have real algebraic, analytics, and computer algebraic play major role in their technologies. It is used to prove the different algorithms using analytics and mathematical algebra. Thus, this tool can help to check properties like correctness, controllability, reactivity, in a hybrid system[18].

Figure 4 shows the process of manufacturing the vehicle and its components and the assembly of vehicle in the factory. Every device should be programmed with an ID and a certificate. Access Control List(ACL) are supplied to the security module for the vehicle. All participants are certified by the central Certificate Authority (CA) of the Original Equipment Manufacturer (OEM).

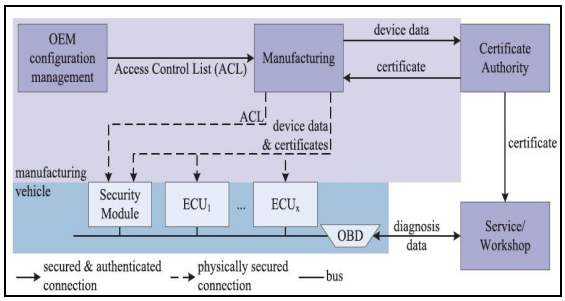

Fig 4: Overview of system setup and workstation situations

Inside the connected vehicles, microcontroller in the system need to scan at the boot and real-time to guarantee that the software which is in use is genuine. This layer will also have potential lockdown procedure during a successful attack against the system.

Layer 5: Secure Update

As the software updates are made on the smartphones with wireless connection, in the similar way the updates for the control units(ECU's) are done through Over the Air Update(OTA). This update feature is considered more convenient and efficient as it saves customers from repairing any bugs that exist in the system. But this opens a new attack vector for which we propose a solution that uses biometric iris scan and cryptographic checksum mechanisms which eliminates the threat of attack that can be caused by malicious software updates.

Overall Process of a Secure OTA Update

The OEM initiates the update process by downloading and installing the software updates to the corresponding control unit in each vehicle through its remote servers. Once the installation is done an encrypted checksum is created with the OEM's private key. Then the software packages along with the encrypted checksum and the digital signature of the OEM's are sent to the OEM server. Radio links are used to send the updates to the cars and when updates are received they are transferred to the Central Gateway.

All the updates and the collected user data are connected to the Central Gateway and the iris scan authentication unit where they are securely stored before being sent over to the ECU. Before any software download is made they are verified with the information that is already available in the central gateway such that the version of the software being installed is liable with the one available in the database.

Our proposed method undergoes authentication through verification module before any updation is made. This module stores the car owner's iris scan and gives the vehicle's owner the flexibility to install a particular update at a particular time slot available to the ECU. This way attacker cannot misinterpret the ECU and the sensors that are connected to them.Also,

there are chances that the owner might not be available at the time of updates, then the updates will be stored in the database.

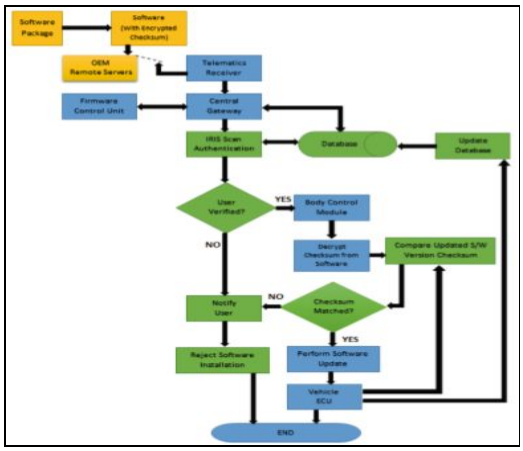

Fig 5: OTA Update Flowchart

The stored files are protected against any kind of unwanted changes with the help of encryption and authentication techniques. Authentication is done before receiving the updates from the Body Control Module (BCM). The Iris scan camera is fitted on the steering wheel such that the owner can authenticate the updates. Once the owner starts the vehicle he/she will be prompted about the new update. Before the BCM sends the updates to the ECU, the genuinity of the software packages is verified by checking the digital signature.

Once the packages are known to be genuine ,the checksum value will be decrypted using the OEM's public key which is stored in the BCM. When the decryption is made, the updated software version and the software that is already installed in the car are compared by the vehicle's ECU. In this comparison the checksum values has to be equal to process an update. If the values are not equivalent then an error is notified and the installation is stopped. If they are equal, the software updates install successfully and hence updated version of the software gets approved by the ECU.

Checksum Comparison

During the Checksum comparison every module send messages to the other modules continuously to check if they are active at a time. Each module has a node with an unique source address. At the communication initiation phase, th service tool requests for the module to send its ID and when the ID is received it compares the received ID to the ID that is present in the database are matched.. The module requires to calculate the checksum of the every software program to be installed[

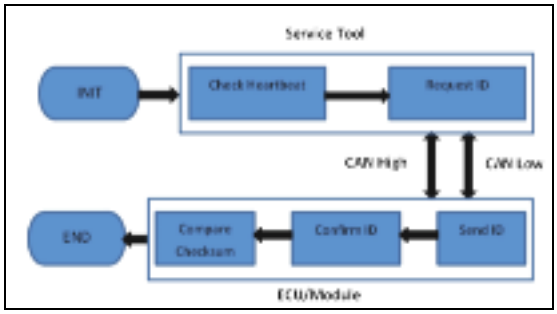

Fig 6 : Service Tool Processing

Once the checksum is calculated we compare it with the OEM's checksum value which is stored in the CAN database. Successful installation of the available updates are made when the checksum values compared are known to be matched and when they do not match that means there is an unauthenticated attempt to install the program, this will thus trigger information to stop the installation process in form of an error or a warning message[19].

Iris Scan Authentication: The other most important security mechanism in our proposed method is the Iris Scan Authentication. The security of the OTA updates depends on the iris authentication of the car owner. A digital camera scanning device in the car will activate immediately as the person starts the car. It will then scan the person's iris. The iris pattern that has been scanned will be encoded and compared with the stored iris scan in the database which is connected to the central gateway and the iris authentication unit. If the stored data and the scanned data of the person sitting in the car are

same then we will let the process of updation and installation continue[19].

PERFORMANCE METRICS

The deployment of a connectivity-dependent powertrain functions in automobiles can have implications on the security as well as the development of the system. It is important that we quantify the benefits associated with the solution as well as gain insights into security-connectivity trade off. The metrics we have used for analysis of the security framework are confidentiality, Integrity and authorization. In terms of Connected Vehicles,

Confidentiality describes the security of the messages that are transmitted over different communication paths (in-vehicle communication/wired & wireless communication) such that an attacker does not intercept these messages.

Integrity metric describes the security against creation of spam messages/alteration of the genuine ones that are sent or received over the CV's communication channels.

Authorization describes the protection provided against the interruption of messages sent over.
In our work, we have tried to achieve the protection of all three aspects through a security framework that provides protection to the vehicle at each node either through secure element, Gateway or using authentic streams to enable simplified enforcement of Confidentiality, Integrity and Availability.

ANALYSIS OF PROPOSED SOLUTION

We compared our proposed solution with two existing published proof of concept architectures. In the paper titled "Security Architecture for Vehicular Communication" by Matthias Gerlach et. all[20], the architecture is also organized in functional and modular layers, but the solution fails to include many core concepts such as TCU security and gateway implementation. This design will still lead to network security vulnerabilities. Rather than faster and more responsive approach, the paper is using latency prone certification protocols and registration schemes to enable security. There is a large set of such security concepts included in this research such as node identification, digital signature and certificates, plausibility checks etc. These concepts are not specific to vehicular communication and were not created with such purpose in mind. There is a huge requirement for researchers to commit to creating newer concepts specifically for connected car security. Our research is based upon this requirement, as we include only the technologies that are relevant to this particular sphere of interest.

Further, we delved into the research paper titled "Architecture for Secure and Private Vehicular Communications" by P. Papadimitratos et. all [21]. This research paper was primarily based upon using cryptographic keys for secure communication in the architecture. Our research also includes this similar approach in our secure network layer as an alternative recommendation. Because of overhead cost to include such a delayed response mechanism in existing car architectures by adding state-of-the art cryptographic accelerators and advanced circuitry, this solution is will not scale well with many original equipment manufacturers. Whereas, our research is based upon using a hypervisor and machine virtualization approach to make the security of connected vehicles very software centric.

On the whole, our proposed framework is comprehensive and modular. This detailed approach aims to conquer all vulnerabilities posed in everyday life associated to in-vehicle and external communication with the Connected Vehicles. The intricate layered approach fulfils the idea providing an all-round infallible security system to sustain the shortcomings and loses. The attacks to the susceptible section of a CV focus towards slowly weakening the system. Attacks can be of varied nature, focussing on

either breaking the system or weakening it, but it all has the root by targeting the susceptible areas. In other words every layer has its own share of attack prone areas and communications, thus it is essential for the entire CV system to sustain to be able to harness threatening situations. Moreover, we are building our design in a software centric framework, which we recognize will fare far better in real life scenarios. Software centricity will also help with the global standardization process and will streamline the protocol designs, leading to an easier and practical formation of global consensus among car manufacturers.

CONCLUSION

Main contribution of this paper

We are moving to an era, where car security and many of car's key feature will rather be looked after by software installed on it. Our security architecture is designed with that vision in mind, so it can coexist in symbiosis with the Software Designed Cars of the future.

We recognized that ECU's that are critical systems of the vehicle need to be secured by the state of the art cryptographic functions and hardware security modules. These can physically prevent any intrusion into the system that can be life threatening.

Also modern gateways used in the vehicle system connect different parts of the connected vehicle along with the functionality that they provide security from malicious messages that can be sent over the in-vehicle network. To overcome the limitations of the control units the microcontroller manufacturers have started embedding security modules such as the SHE(Secure Hardware Extensions) to the system such that the only authenticated software can make updates in the system and the in-vehicular communication remains safe.

All of these efforts provide security to the single components of the system, thus resulting in partial protection of the Connected Vehicle architecture. Any attack does not merely focus on affecting the particular components of the vehicle. Instead vulnerabilities in the integrated system are the prime target for any attacker.

Our literature survey has led us to believe that a framework which can provide end to end protection is very non existent in academia currently. This requires to be thought out and built as a proof of concept. Our team has extensively researched and designed a layer based end to end security architecture which not only protects individual units in a connected car, but provides a complete system protection. Furthermore, it has been a proven fact that any system which is modularly divided and segmented is a much efficient system, as it's much easier to identify and solve any future anomalies or individual update requirements.

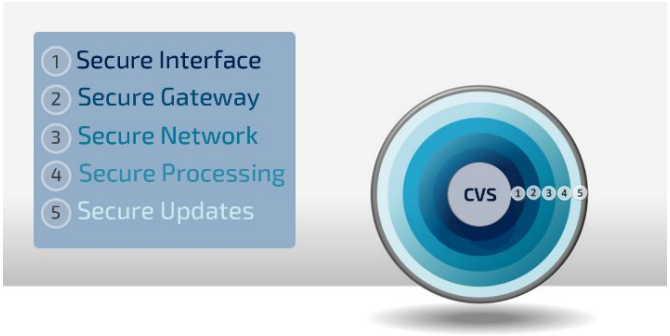

Fig. 7 - Visual Representation of Proposed Security Architecture

The layered approach also reduces the attack surface significantly. It becomes much harder for cyber-hackers to infiltrate such a layered architecture. In future, such layer based security architecture will not just be a commercial requirement, rather this will be mandated by governments to be implemented in each connected car, so as to mitigate life threatening situations and provide safety and security to the customers all over the globe.

FUTURE WORK

Our team plans to further enhance our technical framework. We are looking forward to build our proof of concept security architecture by simulating its key elements such as Hypervisor machine virtualization in VMware Workstation and other kernel based Linux environments. We are also planning to physically simulate our TCU approach as well as use python's CAN bus library pyCAN to simulate our proposed gateway system and CAN layer architecture. Furthermore, because our aim is to provide an end to end security solution. We might also add new technical layer based approach if we identify any potential vulnerabilities and loopholes in our current security design framework.

REFERENCES

[1] Bertolino, Antonia, et al. “A Tour of Secure Software Engineering Solutions for Connected Vehicles.”, vol. 26, no. 4, 2017, pp. 1223–1256., doi:10.1007/s11219-017-9393-3.

[2] Pantazopoulos, Panagiotis, et al. “Towards a Security Assurance Framework for Connected Vehicles.” 2018 IEEE 19th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), 2018, doi:10.1109/wowmom.2018.8449811.

[3] R. Escherich, I. Ledendecker, C. Schmal, B. Kuhls, C. Grothe, and F. Scharberth. 2009. SHE – Secure Hardware Extension Functional Specification.

[4] H. Seudie. 2009. Vehicular On-board Security: EVITA Project. (2009)

[5] Shreejith, Shanker, et al. “Reconfigurable Computing in Next-Generation Automotive Networks.” IEEE Embedded Systems Letters, vol. 5, no. 1, 2013, pp. 12–15., doi:10.1109/les.2013.2243698.

[6] Muehlberghuber, Michael, et al. “FPGA-Based High-Speed Authenticated Encryption System.” VLSI-SoC: From Algorithms to Circuits and System-on-Chip Design IFIP Advances in Information and Communication Technology, 2013, pp. 1–20., doi:10.1007/978-3-642-45073-0_1.

[7] Lukasiewycz, Martin, et al. “Security-Aware Obfuscated Priority Assignment for Automotive CAN Platforms.” ACM Transactions on Design Automation of Electronic Systems, vol. 21, no. 2, 2016, pp. 1–27., doi:10.1145/2831232.

[8] Mundhenk, Philipp, et al. “Security in Automotive Networks.” ACM Transactions on Design Automation of Electronic Systems, vol. 22, no. 2, 2017, pp. 1–27., doi:10.1145/2960407.

[9] Han, Kyusuk, et al. “On Authentication in a Connected Vehicle.” Proceedings of the ACM/IEEE 4th International Conference on Cyber-Physical Systems - ICCPS 13, 2013, doi:10.1145/2502524.2502546.

[10] Han, Kyusuk, and Kang G. Shin. “Prevention of Information Mis-Translation by a Malicious Gateway in Connected Vehicles.” 2016 14th Annual Conference on Privacy, Security and Trust (PST), 2016, doi:10.1109/pst.2016.7906970.

[11] “On authentication in a connected vehicle: Secure integration of mobile devices with vehicular networks” K Han, SD Potluri, KG Shin - ACM/IEEE 4th International Conference on, 2013 - dl.acm.org

[12] Thiruneelakandan, A., and T. Thirumurugan. “An Approach towards Improved Cyber Security by Hardware Acceleration of OpenSSL Cryptographic

Functions." 2011 International Conference on Electronics, Communication and Computing Technologies, 2011, doi:10.1109/icecct.2011.6077061.

[13] Reinhardt, Dominik, et al. "Mapping CAN-to-Ethernet Communication Channels within Virtualized Embedded Environments." 10th IEEE International Symposium on Industrial Embedded Systems (SIES), 2015, doi:10.1109/sies.2015.7185064.

[14] Wang, Eric, et al. "Hardware Module-Based Message Authentication in Intra-Vehicle Networks." Proceedings of the 8th International Conference on Cyber-Physical Systems - ICCPS 17, 2017, doi:10.1145/3055004.3055016.

[15] Khazaei, Atefeh, et al. "An Automatic Method for CVSS Score Prediction Using Vulnerabilities Description." Journal of Intelligent & Fuzzy Systems, vol. 30, no. 1, 2015, pp. 89–96., doi:10.3233/ifs-151733.

[16] Preschern, Christopher, et al. "Applying and Evaluating Architectural IEC 61508 Safety Patterns." Lecture Notes on Software Engineering, 2014, pp. 1–5., doi:10.7763/lnse.2014.v2.84.

[17] Wu, Fang, et al. "Vulnerability Detection with Deep Learning." 2017 3rd IEEE International Conference on Computer and Communications (ICCC), 2017, doi:10.1109/compcomm.2017.8322752.

[18] Platzer, André, and Jan-David Quesel. "KeYmaera: A Hybrid Theorem Prover for Hybrid Systems (System Description)." Automated Reasoning Lecture Notes in Computer Science, pp. 171–178., doi:10.1007/978-3-540-71070-7_15.

[19] "Security Enhancement of Over-the-Air Update for Connected Vehicles" Akshay Chawan , Weiqing Sun (&) , Ahmad Javaid , and Umesh Gurav College of Engineering, University of Toledo, Toledo, OH 43606, USA Weiqing.Sun@utoledo.edu Tech Mahindra Americas Inc., Schaumburg, IL 60173, USA.

[20] Gerlach, Matthias, and Florian Friederici. "Security Architecture for Vehicular Communication." VTC Spring 2009 - IEEE 69th Vehicular Technology Conference, 2009, doi:10.1109/vetecs.2009.5073588.

[21] Papadimitratos, P., et al. "Architecture for Secure and Private Vehicular Communications." 2007 7th International Conference on ITS Telecommunications,2007,doi:10.1109/itst.2007.4295890.