Threats, Vulnerabilities, Recommended Control and Proposal of Immediate AT revocation for Cooperative Intelligent Transport System

Jun Hong Marcus CHAN

S45057377

The University of Queensland

Abstract— Cooperative Intelligent Transport System represents a step forward in technology for the land transport industry. For the system to work, it must transmit information from one point to another to share its data within the network. However, with every system, there will likely be a few hacktivists that find out the weaknesses and exploit it for their gains. As such, protection against this threat is vital. Some of the threats are Denial of Service, Eavesdropping and Masquerading attack. There are also ways to improve the current security system of the Cooperative Intelligent Transport System such as integrating a Blockchain-based PKI.

***Keywords*— Attack, Blockchain, C-ITS, Intelligent Vehicle, PKI, Security**

I. Introduction

Cooperative Intelligent Transport System (C-ITS) aims to improve road safety and driver experience [1] by allowing communication between vehicles and infrastructures to keep the driver safe by alerting the driver of traffic changes and the surrounding through the exchange of information within a wireless network [2].

Vehicle communicates in an ad hoc manner, some of the technologies are [2, 3]:

- **Vehicle-to-Vehicle communications (V2V)**
  E.g. Communication with surrounding vehicles.

- **Vehicle-to-Infrastructure communications (V2I)**
  E.g. Communication with traffic lights.

- **Vehicle-to-Everything(V2X)**
  E.g. A combination of V2V and V2I communications

The objective and goals of incorporating C-ITS are [2]:

- **Safety**
  C-ITS provides early warning to drivers of a potential event that is likely to happen around the vehicle

- **Efficient and sustainability**
  C-ITS provides information to drivers on traffic conditions such as congestion, road closures and incidents. Drivers will use that information to make a detour to avoid bad traffic conditions as such; the driver can take a shorter route. Therefore benefiting the environment as it saves on fuel and emission reductions.

- **Accessibility and mobility**
  C-ITS mobility application can notify users ahead of time about road traffic conditions. While accessibility application may assist the user, for example, while crossing the road, wireless devices will be able to communicate with traffic signals for the pedestrian to cross the street safely.

The essentials for V2X communications are ‘Cooperative Awareness Messages’ (CAM) and ‘Decentralized Environment Notification Messages’ (DENM). Both DENM and CAM are signed to provide integrity and authenticity to the receiver end [4].

CAM sends ‘single-hop’ messages. These messages are transmitted in low latency for short-range communication to other vehicles or infrastructures for others to receive it fast [5]. The purpose of these CAM is to convey on vehicle information such as the speed, time and another vehicle status to the nearby vehicle or infrastructure [4].

.

DEMN sends ‘multi-hop’ messages. These messages sent by the ITS system from another ITS system which deduces the meaning of ‘multi-hop’ [6]. The purpose of this DENM is to send information such as weather conditions, visibility and other urgent emergency situations [4].

II. Threat

A. Denial of Service

Denial of Service (DoS) is a threat towards availability to C-ITS communication [7]. The availability of ITS system is crucial as it ensures the safety of the driver [8]. There is however 3 level of DoS which are overwhelming of node resources, jamming the channel and lastly distributed Denial of Service [9].

The motivation for the attacker to launch a DoS attack is to flood the network thus slowing down or potentially jamming up the communication between vehicles and infrastructure, therefore not able to get an accurate warning of an accident on the road ahead [10, 11, 12].

B. Eavesdropping

Eavesdropping is a threat towards confidentiality to C-ITS communication [7]. The confidentially of the ITS system is crucial as it ensures the information of the vehicle is only accessible to authorised users [3].

The motivation for the attacker to carry out an eavesdropping attack is by tapping into the network and listening on the unsuspected vehicle, collecting vehicle information such as location data to pinpoint vehicle location. Therefore, the data of the vehicle and the owner will be invaded [3, 10, 12].

C. Masquerading Attack

Masquerade attack is a threat towards integrity and authenticity to C-ITS communication [7]. The integrity or authenticity of the ITS system is crucial as it ensures that message is not tampered by attackers intentionally or unintentionally. Additionally, it is to ensure that the message comes from the destination source and not by an attack, therefore making it trusted [11].

The motivation for the attacker to carry out a masquerading attack is to mislead another vehicle by sending a message that appears to be from a legitimate source with malicious or rational intend [11]. For example, by acting as an emergency vehicle, the vehicle would slow down and give way to the emergency vehicle, therefore leading it to believe that it as a real emergency vehicle which in turn deceive other vehicles within the network [8, 10].

III. Vulnerability

A. Vulnerability to Availability

One of many vulnerabilities that will lead to a denial of service attack is both the road site unit, and the vehicle’s ITS inability to process a message quickly enough to validate whether the message will be of use and from a valid source [7].

The vulnerability can be exploited by installing malware on ITS on vehicle or roadside unit by sending out messages with no value deeming to be valid and broadcasting the data at a high rate so that the ITS would not be able to process it promptly [7].

B. Vulnerability to Confidentially

One of many vulnerabilities that will lead to an eavesdropping attack is both the roadside unit and vehicle’s ITS communication are broadcast in a 5, 9Ghz radio bandwidth which is capable of being intercepted by any receiver [7]. In addition to that, some of the ITS basic set of application messages can reveal the geographical location of the vehicle [7].

The vulnerability can be exploited by posing as a real ITS vehicle or roadside units through the recording of ITS messages with the malicious intent of content and behavioural patterns [7].

C. Vulnerability to Integrity

One of many vulnerabilities that will lead to a masquerade attack is that both the roadside unit and vehicle’s ITS is not able to be verified the source of the message sent out by another V2X system in the network, as CAM and DNM messages do not include any form of identification, it can only detect whether the message is valid [7]. In addition to that, all ITS messages distributed in a 5, 9 GHz radio bandwidth which is capable of being intercepted by any receiver that is capable of doing so [7].

This vulnerability can be exploited by posing as a real ITS in vehicles and roadside units that send ITS messages that is deeming to be legitimate and fabricating its messages [7].

IV. Threat Mitigation

A. Denial of Service Mitigation

The exchange of information from within the V2X should be processed and made available at all time such that C-ITS should withstand this kind of attack and risk of being brought down [11].

Some of the countermeasure strategies are by the including a sequence number in each new message and add a source identification across the stack in ITS messages [7]. By introducing the countermeasures to the ITS, it will benefit by rejecting old messages, inappropriate messages,

anonymous messages and messages without any form of identification [7, 13].

With both sequence number in each new message and add source identification across the stack in ITS messages, it will ensure that messages have some form of integrity as well as reducing the risk of a DoS attack.

B. Eavesdropping Mitigation

The transmission message of personal and private data such as the driver positioning data and vehicle identification data should be encrypted [7, 12].

Some of the countermeasure strategies are by adding a key distribution management system to the ITS architecture such as a Public Key infrastructure [7, 14]. Another way to prevent an eavesdropping attack is by adding a layer of security within the network with the use of a firewall [15] that can be installed in both infrastructure and vehicles.

Both the Public Key infrastructure and added firewall security will ensure that all data will not transmit in plain text over the air, reducing the risk of an eavesdropping attack.

C. Masquerade Attack Mitigation

The interchange of a message between V2X should not be tampered with by the attacker and should have the ability to resist any unauthorised creation or alteration of a message [8, 11].

Some of the countermeasure strategies are the use of a certificate revocation list (CRL) to detect malicious vehicle by distributing the CRL across the ITS network [8]. Another way is to have a digital signature to verify that the sender of the message that is legitimate from a V2X entity [7, 8].

With both the use of a Certification Revocation List and to authenticate digital signature, it will ensure that messages will have integrity and authenticity that will reduce the risk of a Masquerading attack.

V. PROPOSE

The purpose of authorisation ticket is public key certificates that are also sometimes referred as a short-term certificate or pseudonym certificate that is issued by the authorisation authority which is part of the Public Key Infrastructure (PKI) of ETSI TS 102 731 of Intelligent Transport System (ITS); Security; Security Services and Architecture [4, 16].

All certificates from the Certification Authority (CA), Enrolment Authority(EA) and Authorisation Authority(AA) is published to a certification revocation list (CRL) in the network. A CRL is a mechanism to check whether the certificate is valid [17]. Usually, the process of validating against CRL is slow and efficient [18].

To achieve immediate AT certificate revocation using Blockchain-Based PKI. A block stores the data, a hash value and a hash value of the previous block [19]. The hash is created based on the data, and by altering a single block will change the value of the hash, in turn, the following block will be invalid as the block of the previous block will be different as it needs to recalculate the proof of work [19]. A blockchain distributed which uses a Peer to Peer network, when a new block has is created, it will be sent within the network, and each node verifies the block if it is valid [19].

Blockchain-based PKI creates timestamping to prove that the file exists at a particular time on any documents [20] as such it will be able to comply with EU standard certificate and message formats.

The advantage of using a Blockchain-Based PKI over a traditional PKI is that validation of a certificate with CA certificate chain takes a shorter amount of time [21, 22]. Another advantage to the Blockchain-Based PKI is that it does not require the use of the CRL as blockchain synchronises between nodes where any modification of the certificate would notify all other nodes in the network [21, 22].

VI. CONCLUSION

C-ITS are not entirely secure as there are much-known weaknesses that hacktivist can exploit but with the correct security measure, the risk can be reduced and mitigate. The proposal of the blockchain-based PKI will allow the system to run as it is and to provide a more secure environment for the current C-ITS PKI architecture; the primary purpose is that it will be able to do an immediate revocation of certification as it synchronises between nodes.

REFERENCES

[1] Allianz Australia Limited, “Cooperative Intelligent Transport Systems,” [Online]. Available: https://www.allianz.com.au/car-insurance/news/cooperative-intelligent-transport-systems. [Accessed 17 September 2018].

[2] Queensland Government, “About cooperative and automated vehicles,” Queensland Government, 10 August 2017. [Online]. Available: https://www.qld.gov.au/transport/projects/cavi/cooperative-automated-vehicles. [Accessed 6 September 2018].

[3] N. Huq, R. Vosseler and M. Swimmer, “Cyberattacks Against Intelligent Transportation System - Assessing Future Threats to ITS,” 24 October 2017. [Online]. Available: https://documents.trendmicro.com/assets/white_paper

s/wp-cyberattacks-against-intelligent-transportation-systems.pdf. [Accessed 3 September 2018].

[4] Data Protection WG, “Processing personal data in the context of C-ITS,” 1 March 2017. [Online]. Available: https://smartmobilitycommunity.eu/sites/default/files/images/2017.03.01_Processing_personal_data_C_ITS_context_vF.PDF. [Accessed 16 September 2018].

[5] ESTI, “ETSI EN 302 637-2 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service,” November 2014. [Online]. Available: https://www.etsi.org/deliver/etsi_en/302600_302699/30263702/01.03.02_60/en_30263702v010302p.pdf. [Accessed 16 September 2018].

[6] ESTI, “ETSI EN 302 637-3 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service,” September 2014. [Online]. Available: https://www.etsi.org/deliver/etsi_en/302600_302699/30263703/01.02.01_30/en_30263703v010201v.pdf. [Accessed 16 September 2018].

[7] ESTI, “ETSI TR 102 893 - Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA),” March 2017. [Online]. Available: https://www.etsi.org/deliver/etsi_tr/102800_102899/102893/01.02.01_60/tr_102893v010201p.pdf. [Accessed 15 September 2018].

[8] E. B. Hamida, H. Noura and W. Znaidi, “Security of Cooperative Intelligent Transport Systems: Standards, Threats Analysis and Cryptographic Countermeasures,” 6 July 2015. [Online]. Available: http://www.mdpi.com/2079-9292/4/3/380/pdf. [Accessed 16 September 2018].

[9] M. S. Shrivastava, R. Khatri and A. S. Bisen, “Hybrid approach for detecting and preventing DOS attack in VANET,” in *2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, Paralakhemundi, 2016.

[10] A. Dhamgaye and N. Chavhan , “Survey on security challenges in VANET,” *International Journal of Computer Science and Network,* vol. 2, no. 1, pp. 88-96, 2013.

[11] K. Fysarakis, I. Askoxylakis, V. Katos, S. Ioannidis and L. Marinos, “Security Concerns in Co-operative Intelligent Transportation Systems,” 4 October 2017. [Online]. Available: https://www.researchgate.net/profile/Konstantinos_Fysarakis/publication/320198036_Security_Concerns_in_Co-operative_Intelligent_Transportation_Systems/links/59d4d2334585150177fc8294/Security-Concerns-in-Co-operative-Intelligent-Transportation-Systems.pdf. [Accessed 16 September 2018].

[12] H. Krishna and S. K. Arora, “Review of Vehicular Ad Hoc Network Security,” *International Journal of Security and Its Applications,* vol. 11, no. 4, pp. 27-44, 2017.

[13] E. Foo, C. Djamaludin and A. Rakotonirainy, “Security Issues for Future Intelligent Transport Systems,” in *In Proceedings of the 2015 Australasian Road Safety Conference*, Gold Coast, Queensland, 2017.

[14] Oracle Corporation, “The Public Key Infrastructure Approach to Security,” 2003. [Online]. Available: https://docs.oracle.com/cd/B14117_01/network.101/b10777/pki.htm. [Accessed 21 September 2018].

[15] J. Karasek , “Security 101: Protecting Wi-Fi Networks Against Hacking and Eavesdropping,” 13 June 2018. [Online]. Available: https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/security-101-protecting-wi-fi-networks-against-hacking-and-eavesdropping. [Accessed 21 September 2018].

[16] ESTI, “ESTI TS 102 731 - Intelligent Transport System (ITS); Security; Security Services and Architecture,” September 2010. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/102700_102799/102731/01.01.01_60/ts_102731v010101p.pdf. [Accessed 28 September 2018].

[17] proinity LLC, “What Is a Certificate Revocation List (CRL)?,” 29 March 2017. [Online]. Available: https://www.keycdn.com/support/certificate-revocation-list/. [Accessed 29 September 2018].

[18] T. Arwine, “The Value of Certificate Revocation Lists (CRLs) in a PKI,” Microsoft | TechNet, 9 February 2012. [Online]. Available: https://blogs.technet.microsoft.com/staysafe/2012/02/09/the-value-of-certificate-revocation-lists-crls-in-a-pki/. [Accessed 29 September 2018].

[19] MIT Technology Review Editors, “Explainer: What is a blockchain?,” MIT Technology Review, 23 April 2018. [Online]. Available: https://www.technologyreview.com/s/610833/explainer-what-is-a-blockchain/. [Accessed 30 September 2018].

[20] Nexus Group, “Public key infrastructure (PKI) will soon run on blockchain technology,” Nexus Group, 22 March 2017. [Online]. Available:

https://www.nexusgroup.com/blog/public-key-infrastructure-pki-blockchain-technology/. [Accessed 1 October 2018].

[21] A. Yakubov, W. M. Shbair, A. Wallbom, D. Sanda and R. State, “A blockchain-based PKI management framework,” in *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium*, Taipei, 2018.

[22] E. Sharret, “3 Ways Blockchain Can Improve PKI,” Telegrid, 26 July 2017. [Online]. Available: https://telegrid.com/3-ways-blockchain-can-improve-pki. [Accessed 1 October 2018].