Secure Cloud Networks for Connected & Automated Vehicles

Madhusudan Singh (IEEE Member)
Display Research Team
SAMSUNG Display Co. Ltd (SDC)
Yongin, South Korea
madhusudan.iiita@gmail.com

Dhananjay Singh* (SMIEEE)
Dept. of Electronics Engineering
Hankuk Univ. of Foreign Studies,
Yongin, South Korea
dan.usn@ieee.org

Antonio Jara (IEEE Member)
Institute of Information Systems, Uni. of Applied Sciences (HES-SO)
Western, Switzerland
jara@ieee.org

Abstract— An intelligent transportation management system is rapidly evolving. Nowadays, the convergence of ICT (Information communications technology) and cloud computing are widely adaptation among many services. The automobile industry has great expectations from these futuristic solutions so that they can improve safety of people, security of vehicles as well as reduce the cost of ownership of an automobile. This paper presents connected vehicles architecture solutions for both safe and secure driving for personal/public vehicles. And also paper has shown the performance of the secure cloud networks from that every driver (client) update real-time information for self-aware. The concept of penetration testing and vulnerability assessment are used to analysis the transportation data in real-time computing such as traffic, weather, accident prevention/monitoring and access control.

Keywords— Cloud Computing; Security; ICT; Transportation

I. INTRODUCTION

The smart transportation system is integrated through internet and their cloud computing integration and the information is collected using the sensors namely front and rear camera module for recording the pre and post-accident data. This information is simultaneously sent to the end users who are nearby the ad-hoc wireless network, without any intervention from third party electronics device so that they can receive the news about the nearby vehicles and the drivers can decide, whether to overtake the vehicle or not. In the event of untoward incident, the video recorded and the location specified by the location are transferred over the cloud networks so that the associated authorities can take a suitable decisions [1, 2].

Cloud Computing is the internet based new computing system which is distributing services for the interest of clients such as shared network resources, software, and platform computing infrastructure. The major dynamic cloud providers present in the cutting-edge market segment that are offering different-different cloud services. With the rapid increase of cloud services and their cyber-crimes, provision of appropriate cloud network security has become necessary in order to protect the confidentiality, integrity and availability for transportation services. The prominent need of real-time communication in the transportation system necessitates, use of modern networking technology for all clients to support scalability and Quality of Service [3]. Even though, the virtualization and cloud computing delivers wide range of dynamic resources. The security concern is generally perceived as the huge issue in the cloud which makes the users to resist themselves in adopting the technology of cloud computing. Security is the major concern of cloud, cloud service providers as well as the clients who are facing tremendous security challenges.

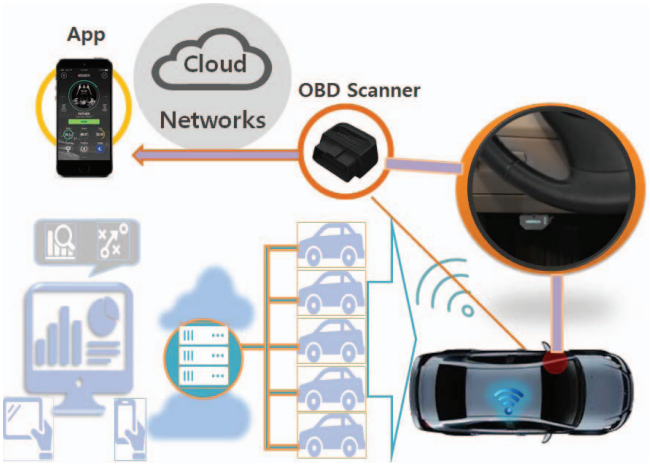

Fig. 1. Connected and automated vehicles.

In order to assure high availability, integrity and confidentiality of vital data located on a cloud network, various security implementations have been shown in Fig. 1. However, every measure comes with a known or an unknown vulnerability. Vulnerabilities are weak spots in a cloud network where it is made possible for threats to occur in networking infrastructures. These threats are usually aimed at valuable data

978-1-5090-0264-1/15/$31.00 ©2015 IEEE

DOI 10.1109/ICCVE.2015.94

or perhaps available resources of a target cloud server. To maintain a stable and secure cloud network, the cloud server needs to ensure that all necessary measures have been implemented and that correct access rights have been put in place by defining boundaries and enforcing them by the client's aid of policies. Hence, the real-world is evolving with the cloud platforms terms of applications and integration in to real-world services [4-7]. It is difficult to gauge the scale of cloud networks and their deployable feasibility but in this paper we have conceded connected & automated vehicles with cloud demand for the growth of driver's security points of view. In this case, the internal/external processing and computation have delivered to the cloud networks. In this paper we have explored a novel secure cloud networks for the connected vehicles services to enhanced the transportation system. Hence, cloud networks has to provide access and control from multiple vehicles on the road to improve the safety of the passengers and optimize service of the transportation system in a real-time traffic situation.

The remaining of the paper is organized as follows. The section 2 presents a brief discussion about cloud computing and its security concern issues for transportation system as well as discuss a secure cloud transportation services. The section 3 presents secure cloud test-bed setup model. We have analyzed performance evaluation in section 4. Finally we have concluded the paper in section 5.

II. SECURE CLOUD NETWORKS FOR VEHICLES

A. Cloud Computing

Cloud computing is gaining more popularity, more and more organizations want to move towards cloud but the key concern about moving towards cloud has been security. Today security is required in each of the deployment models. According to NIST [4]. The cloud model is composed of major four deployment models such as Public, Private, Community and Hybrid cloud. The public cloud infrastructure is procured for open use by the general public. It may be held, managed, and operated by a business, academic, or government organization, or some combination of them. The private cloud infrastructure is procured for privileged use by a single organization comprising numerous consumers. The community cloud infrastructure is procured for privileged use by a specific community of consumers from organizations that have shared interest (e.g. mission, security requirements, policy, and compliance considerations). Hybrid cloud infrastructure is an amalgamation of two or more distinct cloud infrastructures (private, community, or public) that have unique existence, but are bound together by standardized or proprietary technology that facilitates data and application portability [5]. However, cloud computing is being widely adopted across many industry sectors. Cloud Computing is experiencing significant growth, with rapid adoption among various regions around the world. With adoption comes, security concern. The essential characteristics of cloud computing are broad network access, on demand self-service, rapid elasticity, resource pooling and measured service. That has explained broad network access is the access of the various resources hosted in a cloud network from a wide range of locations which offers online access. On demand self-service is the availability of services and resources by the cloud vendors, when needed. Rapid elasticity is to provide scalable services by the vendors, when required. Resource pooling is serving maximum clients and customers with scalable and provisional services. Measured service is the monitoring of the services provided by the vendors to the client which includes billing and adequate use of resources.

B. Security concerns in Cloud Networks

Most of the cloud users are unaware of the risk of storing and transmitting private information in a shared environment. Therefore, key technological constraints like transparency, multi-tenancy, velocity-of-attack, information assurance, data privacy and ownership, compliance, encryption, integrity should be addressed carefully. Hence, the clients are completely not secure or immune to the threats over the Internet and this calls for a proper secure cloud mechanism and regular revisions to handle today's technologies. To achieve the highest level of secure cloud server, it is important that every client (Driver) in the cloud network is secure and self-aware.

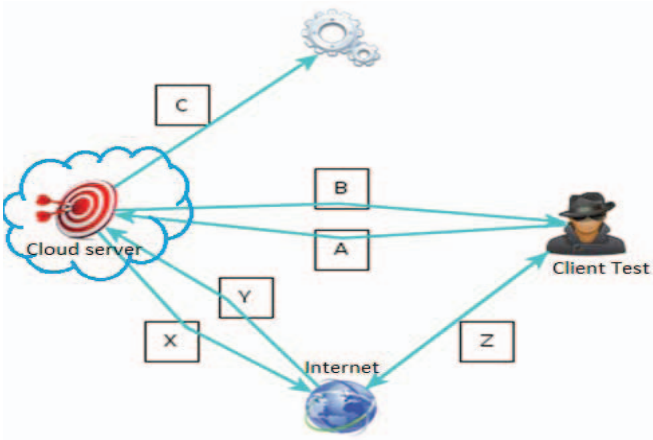

Fig.2. Interaction mechanism of 4PP.

IETF defines Denial-of-Service (DoS) [8] attack, in which one or more machines target a victim and attempt to prevent the victim from doing useful work. DoS is one of the oldest and longest, many of the attacks launched on networks nowadays fall under this category. Usually DoS attacks can be detected by analyzing the characteristics of the victim network. The most effective defenses against DDoS attacks need, filtering routers, disabling IP broadcasts, applying security patches and disabling un used services performing intrusion detection [9]. Fig. 2 depicts four main key processes for each client to identify and test individually in the cloud server which are Induction, Inquest, Interaction and Intervention. *Induction* is the process of the

978-1-5090-0264-1/15/$31.00 ©2015 IEEE

DOI 10.1109/ICCVE.2015.94

analyst, gaining principle understanding of the target by analyzing the environment in which it is located in. This is because of the targets dependability on its surrounding environment. This process is marked as (Z). The concept of Inquest marked as identifier (C) can be simply explained as the process of investigating the target's foundation. In this process the target is analyzed for any emanations or any identifier of those emanations. *Interaction* marked identifier (A & B), these interactions are simply responses to queries or agitations initiated from the analyst. From examples of such interactions ICMP replies and trace route operations. Finally, *Intervention* is the process of analyst mimicking certain resources and services that the target requires for operation. This process helps identify the extreme levels at which the target could still operate. This is shown by (X, Y and Z) in Fig. 3. Multi-tenancy is also very important security concern for cloud clients, colocation of multiple virtual machines in a single server and sharing the same resources that increases the attack surface.

C. Transportation Scenario

Today the economy of every country is increasing at a tremendous pace. People in every part of the world are having cars to travel. Some buy it for status symbol while others buy it for necessity. We can often see the increasing overflow of cars in every street. On the other hand, there are an increasing number of disastrous car accidents which have become a common place incident. Fig.4 shows a road-show of current transportation system. Hence, the advantage of the secure cloud system can support sustainable and permanent services like computing, amateur radio, aviation etc. The proposed cloud authentication mechanism for transportation system is presented in section IV. In the transportation stratum, if we have a Wi-Fi/Bluetooth module connected using their respective interfaces to the embedded processor [9].

III. Connected and Automated Vehicles

Siren systems are effective only within the audible perimeter and un-obstructed sight of the vehicle, which in today's world is a luxury. Most of the people live or work in a crowded city where parking is far away or beyond the audible range of the sirens. There is no way for you to ascertain intrusions into your vehicle. Also every vehicle with the siren-based system sounds same, so there is no surety about your car alerting until you reach the parking-spot. Such systems also eat up a lot of vehicle battery power. Therefore, we would be addressing the issues of vehicle-security, owner safety, greener cars, better understanding over their vehicles to get the maximum performance from vehicles. Despite the technical advancements, only options in market for vehicle security are restricted to GPS tracker and Siren based systems. The proposed mechanism is to design technology for making intelligent vehicles and our scope is tremendous. In this paper we have focused on the genesis of interconnected vehicles. Which are grossly in-effective to solve the ever intricate situations resulting with increased vehicles, diminishing parking spaces and cramped developments leading to easy chances of vehicle break-in and even vehicle thefts.

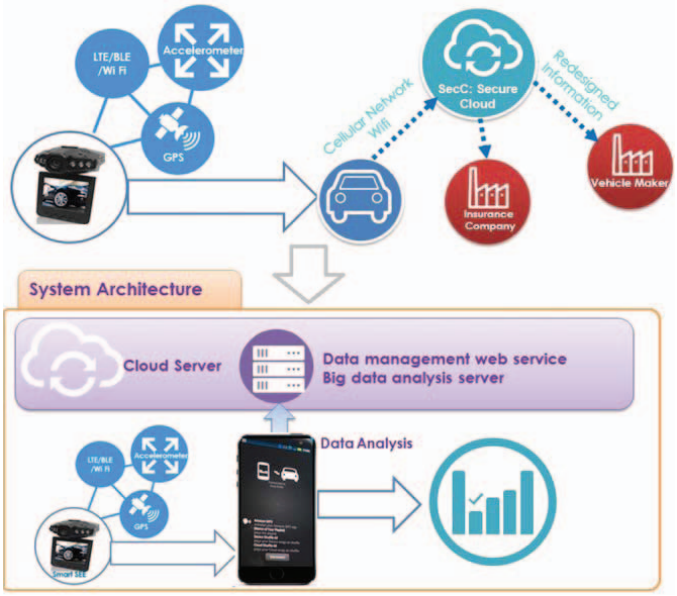

Fig.3. Secure and connected cloud networks.

In the Fig.3 shown secure cloud networks which is considering ICT which can play a very crucial role to establish communication between cloud server and clients (driver) to enhance accident prevention and control. Generally, the security is a joint responsibility of the cloud client and cloud server because the data security and privacy issues pose serious concern. To prevent these issues, we present an authentication mechanism to analyze the transportation services and to aid in better comprehending the concept of penetration testing and vulnerability assessment to improve authentication and access control in cloud services [9].

Fig.4 Connected vehicle services

The proposed a mechanism coherent an array of sensors, data-communication controllers, processors and telemetry chipsets

with a proprietary firmware that we develop. The data will be directed to a cloud-based processing system armed with proprietary software, UI, databases pertaining to different vehicles and user-selectable preferences. Complete environment has interacted with the existing vehicle environment and enhances the overall utility, as shown in Fig.4. It will continually monitor the vehicle performance, understands the driving patterns, automatically sets the user customized parking alerts. It also senses and detects the event of accidents and vehicle break-down. As we keep adding the secondary link, tertiary link and other higher links, we can enforce a truly connected environment and a smart vehicle.

IV. Secure Cloud Testbed Setup

The logical client-server topology implemented in the test-bed. The network has been designed to accommodate common Enterprise Standards. Hence, utilizes the hierarchical model in which redundancy, scalability and link aggregation are key.

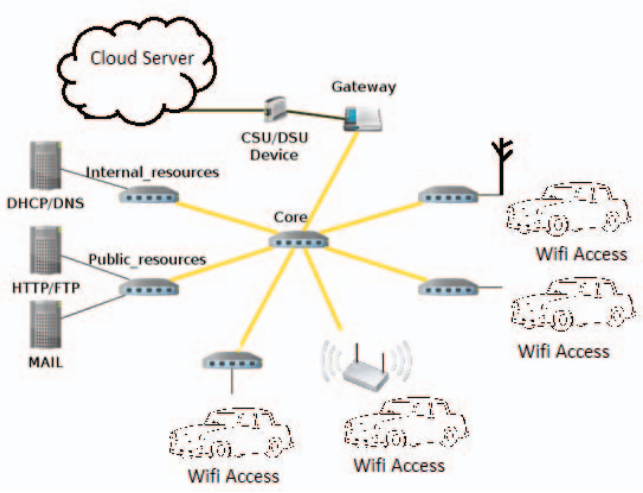

Fig.5. SecC: Logical Topology.

There are two links between the Core and each distribution switch. Use of Virtual Local Area Networks (VLANs) in WANs of this scale is common. Implementation of VLANs significantly increases time efficiency and assists the in charge network manager in configuring remote devices via Telnet sessions. To ease the process of configuring VLANs and to centralize such task, Virtual Trucking Protocol (VTP) has been used at the core level as server and as client in the rest of the devices in the network. So VLANs are configured in the core switch and the VTP server running on the core sends regular updates over the network to ensure each device has ample information on VLAN settings. These updates contain a revision number, so when they get to the client, these revision numbers can be compared and the client will update its VLAN database information based on such process. The two links between the network core and each distribution switch, are set up as trunks to accommodate VLAN traffic. Also each connection supports the native VLAN to enable the transport of untagged VLAN traffic over the network, between different segments [7].

We have setup two Access Points for testing purposes in the enterprise on two separate distribution level switches. Network Address Translation (NAT) has been configured to secure inside local addresses and make sure they cannot be accessed via un-secured transport protocols such as ICMP. NAT has been configured to allow certain addresses to be visible to the outside world (i.e. Web and File Servers). For the router to be able to undertake the task of Inter-Vlan routing, Enhanced Interior Gateway Routing Protocol (EIGRP) is chosen.

The vectors are the main links of communication for clients to the service provider's cloud. These Vectors have been graphically demonstrated in Fig.5. Essentially, each of these vectors can correlate to a separate testing scenario. This allows for better results due to its compartmentalized structure, hence occurrence of too many changes can be avoided. Above steps were taken to complete the information gathering and planning phase of the test. The scanning process however was not conducted separately for each vector. This scanning and enumeration process produces general information about the visible technologies and transportation services.

V. Performance Evaluations

Fig. 7. CDPSnarf Output.

To better understand the underlying causes of vulnerabilities in the implemented test-bed, Metasploit was used as the main information gathering and vulnerability assessment tool. This section exhibits the results collected from the Graphical User Interface (GUI) of Metasploit framework. The results gathered from Metasploit are in form of reports, but these reports have redundant information which will not all be used for evaluation and analysis in this paper. However, only the necessary information, relevant to this concept has been presented in this paper. To better distinguish the outputs of operating system fingerprinting, we can refer Fig. 6 and overview of the information in the test-bed.

Discovered Operating Systems

Operating System	Hosts	Services
Cisco IOS	6	16
Microsoft Windows	3	34
Netgear embedded	4	5
Unknown	1	1

Fig. 6. OS Fingerprints Enumeration.

CDPSnarf is a linux based package that is used for sniffing Cisco Discovery Packets (CDPs) and gaining information about the devices in the network. Fig. 7, is a screen-shot showing the output of such procedure regarding the network gateway. This information was gathered from outside the network. CGE.pl is a purl module that operates linux environment. This packet has the capability of overloading ports on networking devices, hence deeming them unusable. Fig.8 shows the successful exploit that was conducted using this tool [8].

Fig. 8. CGE.pl Output.

Zenmap is a powerful scanning tool. This is the same tool that metasploit utilizes for the purpose of network scanning and enumeration. Fern WiFi Cracker is an automated tool which uses other packages such as air cracking to crack wireless access point passwords by using various methods like dictionary files. As an example one of the APs in the test-bed was successfully attacked in Fig.9.

Fig. 9. Fern-WiFi-Cracker Attack Successes.

According to the generated reports, Simple Network Management Protocol (SNMP) v2.0 community strings are vulnerable to exploit and can easily be cracked. The problem is not specific to one portion of the network. However, because, having access to the community strings used by the SNMP software also means having access to every device in the network including the main management console. Hijacking this session could result in detrimental consequences to the company. By having access to the SNMP credentials one can easily manipulate network configurations and cause DoS attacks as a front for obtaining information from the enterprise network illegally. Another important aspect to consider would be the CDPs traversing the network. By using the information included in these packets, one can easily determine open ports and various capabilities of the devices. Software version of Cisco devices is also advertised in CDPs. Therefore, the attacker could search for exploits, specific to that Inter-networking Operating System (IOS) image. To counter this trend, it is recommended to turn off CDP updates on all Cisco devices unless they are undergoing troubleshooting. To maintain connectivity during such attacks, it is recommended that routing protocols such as Border Gateway Protocol (BGP) to be used since it has the capability to support multiple gateways and therefore will maintain connectivity even if one of the gateways is paralyzed. Fern-Wifi-Cracker is a dangerous tool, since it supports multiple exploitation methods and uses updated dictionary files to crack the passwords on wireless APs. Zenmap is a very strong information gathering tool that can be used to gather a large

volume of information about the target network. The intense scan in Zenmap can identify open ports, OS fingerprints and a partial topology map. But it is not a time efficient tool for network testing. Finally, the strongest tool for penetrating a network is the Metasploit framework. Not only does this framework conduct attacks but also it provides reports for further evaluation and analysis. On top of that, Compliance tests can be arranged to gain a better understanding of the status of the network.

VI. Conclusions

This paper shows clearly, that technology grows so does the need for more advanced security measure which is triggered by rise of vulnerabilities and evidently attack sophistication. On the plus side, the growth in technology has a negative impact from an attacker's point of view. So the lack of knowledge on attacker's side can be exploited in the process of trace-back. In general, the very first conclusion is that network security is mostly about visibility. Means, if one can hide their network resources well enough from prying eyes of attackers, possibility of threats to the network will significantly decrease. This is due to the framework by which penetration tests are conducted. Enumeration is one of the very first steps of every penetration test. If it were to be removed from the cycle, the next phases will become obsolete. There has always been a balance between security threats and their counter measures, but these measures usually concentrate on detecting and blocking the threats rather than to hide important network resources from them. Hence, Cloud service provider has less transparency than other information security policy. As a result, it may create clash with the enterprise's information.

Acknowledgement

This work was supported by Hankuk University of Foreign Studies South Korea research fund in 2015 and The University of Applied Sciences Western Switzerland (HES-SO), the Swiss national government through the Sciex-NMSch with the project code 13.121, named BASTION "Bootstrapping, Authentication, Security and Trust for the Internet of Things Networks". The authors would like to thank also projects SAFESENS ENIAC Joint Undertaking with the Grant Agreement no: 621272, and the EU Horizon 2020 projects ENTROPY with the Grant Agreement no: 649849 and INPUT with the Grant Agreement no: 644672.

References

[1] C. Wijaya, "Performance Analysis of Dynamic Routing Protocol EIGRP and OSPF in IPv4 and IPv6 Network," in Informatics and Computational Intelligence (ICI), 2011 First International Conference on, 2011, pp. 355–360.

[2] Singh D., Alberti A.,"Developing NovaGenesis Architecture for Internet of Things Services: Observation, Challenges and ITMS Application", International Conference on ICT Convergence 2014, Paradise Hotel in Busan, Korea, October 22-24, 2014.

[3] M. Hogan, F. Liu, A. Sokol, J. Tong, NIST Cloud Computing Standards Roadmap – Version 1.0, Natl. Inst. Stand. Technol. Spec. Pub., 83 pages, July 5, 2011.

[4] A. Albeshri W. Caelli, "Mutual Protection in a Cloud Computing Environment", 12th IEEE International Conference on High performance Computing and Communications (HPCC), pp. 641-646, Sept 2010.

[5] U. Khalid, A. Ghafoor, M. Irum, M. Awais Shibli, "Cloud Based Secure and Privacy Enhanced Authentication and Authorization Protocol", Procedia, (2013), Vol.22, pp. 680-688.

[6] Singh D., Singh M., Singh I., Lee H. J., "Secure and Reliable Cloud Networks for Smart Transportation Services, "The 17th IEEE International Conference on Advanced Communication Technology, Phonix Park, South Korea, 1-3 July 2015.

[7] Y. Tan, S. Sengupta, and K. P. Subbalakshmi, "Analysis of coordinated denial-of-service attacks in ieee 802.22 networks," Selected Areas in Communications, IEEE Journal on, vol. 29, no. 4, pp. 890–902, 2011.

[8] M. Handley and E. Rescorla, "Internet Denial-of-Service Considerations," Internet Engineering Task Force, Tech. Rep., 2006.

[9] S. Almulla, Y-Y Chon, "Cloud Computing Security management", 2nd International Conference On Engineering Systems Management and Its Applications, pp.1-7, March 2010.

[10] A. Sedigh, K. Radhakrishnan, C. E-A Campbell, D. Singh, "Trust Evaluation of the Current Security Measures Against Key Network Attacks", MAGNT Research Report, Vol.2 (4), pp.161-171, 2014

[11] Alberti M. A, Singh D. "Developing a NovaGenesis Architecture Model for Service Oriented Future Internet and IoT: An Advanced Transportation System Scenario", IEEE World Forum on Internet of Things 2014, Seoul, Korea, 6-8 March 2014.