2012 4th International Conference on Cyber Conflict
C. Czosseck, R. Ottis, K. Ziolkowski (Eds.)
2012 © NATO CCD COE Publications, Tallinn

Paradigm Change of Vehicle Cyber Security

Hiro Onishi
Alpine Electronics Research of America, Inc.
Strategic Research Group
Torrance, CA, USA
honishi@alpine-la.com

Abstract: Recently, cyber security for non-computers, such as transportation, utility, home appliance and others has become a serious social concern. Intelligent and electrificated modern vehicles have more MCU(micro controller unit)s, more software code than ever, which comes with huge cyber risks. Especially increased connectivity between vehicles and smart-phones / portable music-players changes the paradigm of vehicle cyber security, as virus and malware in smart-phones or music-players can invade automotive electronics. In this paper, first we introduce this new risk and assess the severity of this risk by a public risk assessment tool. Then we analyze the difficulties of cyber security in automotive electronics with limited network connectivity and low computational performance. Finally we conclude it with key findings and suggestions against this new risk.

Keywords: *cyber security, automotive electronics, vehicle connectivity, smart-phone, application download, DoS (Denial of Services)*

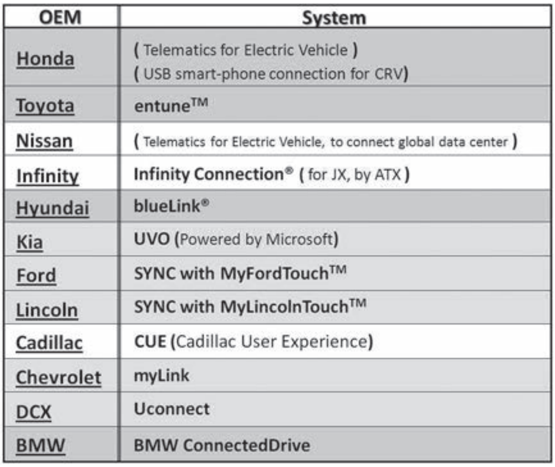
1. INTRODUCTION

Cyber security for computers has been discussed for a long time and many standards and guidelines have been published [1]. On the other hand, recently, cyber security for non-computers, such as transportation, utility, home appliances and others has become a serious social concern [2,3]. Even in automotive industry, from a long time ago, vehicles have large security risks, because they are expensive and frequently parked at unsecured locations. Besides illegally manipulated vehicles threaten drivers and passengers lives, and in the worst case, they damage communities in a large area [4,5]. Moreover current intelligent and electrificated modern vehicles have more MCU(micro controller unit)s, more software code than ever, which increases the risks to cyber attack [4,6,7]. Furthermore, increased standards or interoperability and common platforms or OS(operating system)s, such as, Windows^{TM}, LINUX^{TM}, AUTOSAR, GENIVI and others increase the cyber risks. Finally, “Road vehicle functional safety standard”, ISO-26262 is raising the industrial concern about automotive electronics cyber risks [8].

2. EMERGING NEW VEHICLE CYBER RISK

As modern vehicles have more convenient functions with wireless technologies, vehicle external connectivity increases cyber risks for automotive electronics [4,9,10]. At the initial phase of vehicle connectivity, GM OnStar, for example, mainly wireless communication modules installed within a vehicle, were used for emergency calls, concierge services, remote diagnosis and other automotive applications. However, recently, vehicle connectivity with carry-in devices, such as smart-phones, portable silicon music-players, portable GPS navigation systems, drive recorders and others is providing greater benefits to drivers. Table I shows recent factory-installed connectivity systems, which have been observed in “Los Angeles Autoshow - 2011”. You can tell that under the red column systems, smart-phone has significant important roles, and under blue column systems, smart-phone that provides additional features or mobile phone connectivity is critical. As you can see in Table I, recently, mobile phones, especially smart-phones have more significant roles even in factory-installed connectivity systems. The growth of after-installation smart-phone connectivity system is obvious.

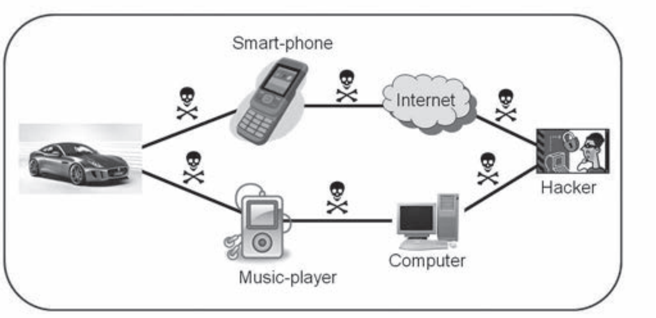
TABLE I. OEM(CAR MAKER)S’ CONNECTIVITY SYSTEM (IN LOS ANGELE AUTOSHOW 2011)



OEM	System
Honda	(Telematics for Electric Vehicle) (USB smart-phone connection for CRV)
Toyota	entune™
Nissan	(Telematics for Electric Vehicle, to connect global data center)
Infinity	Infinity Connection® (for JX, by ATX)
Hyundai	blueLink®
Kia	UVO (Powered by Microsoft)
Ford	SYNC with MyFordTouch™
Lincoln	SYNC with MyLincolnTouch™
Cadillac	CUE (Cadillac User Experience)
Chevrolet	myLink
DCX	Uconnect
BMW	BMW ConnectedDrive

The growth of vehicle connectivity with carry-in devices is increasing vehicle cyber risk. FIGURE I shows the emerging vehicle cyber risks, caused by carry-in device connectivity. In this cyber risk, virus and malware attached with application software or music /video file, are first downloaded in carry-in devices. When carry-in devices are connected to the vehicles, virus and malware invade into the automotive electronics through vehicle entertainment systems or vehicle information terminals. In 2011 July, 82.2 million people in the US owned smart-phones [11]. Also, the number of application downloads on mobile phones is forecasted to reach 48 billion by 2015 [12]. Even now, many malware of Android™ OS smart-phone have been detected and they are increased by 472% from 2011 July to 2011 November [13]. Though this new type of cyber attack is not effective for the specified vehicles, this type of cyber attacks has become a critical threat for DoS (Denial of Service) for large number of unspecified vehicles, via anti-social activities.

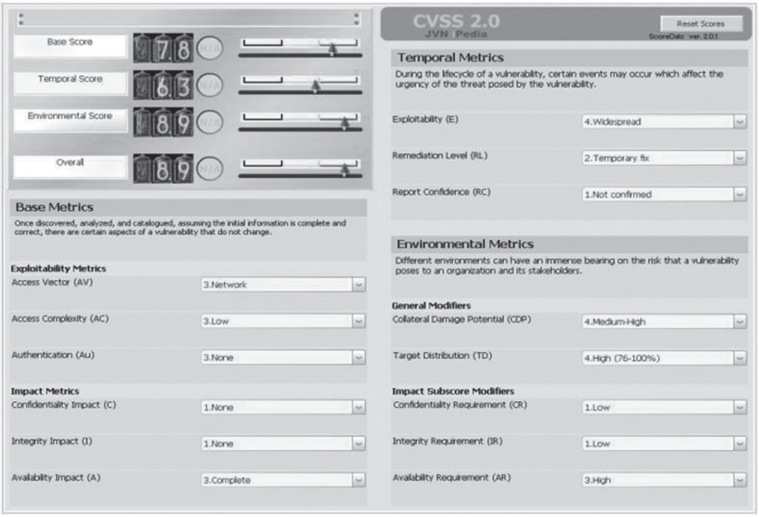
FIGURE 1. NEW VEHICLE CYBER RISK CAUSED BY CARRY-IN DEVICE CONNECTIVITY



3. ASSESSMENT OF NEW VEHICLE CYBER RISK

There are already many tools that can assess cyber security vulnerabilities. CVSS (Common Vulnerability Scoring System) calculator can score the cyber security vulnerability of systems or products with simple inputs and operations [14]. FIGURE II shows the vulnerability scores of the above mentioned new cyber risk by using this CVSS calculator. CVSS calculator assesses the highest severity-level of cyber risk as, “Level-3 (hazardous) - 8.9 of 10”, due to its vulnerability against remote cyber attacks, lack of monitoring or protection mechanisms, wideness of damaged locations and the hazard of drivers, passengers or pedestrians lives.

FIGURE 2. OUTPUT OF CVSS (VERSION 2.0)
ABOUT CYBER RISKS CAUSED BY VEHICLE /CARRY-IN DEVICE CONNECTIVITY [14]



Base Score 7.8
Temporal Score 6.3
Environmental Score 8.9
Overal 8.9

Base Metrics
Once discovered, analyzed, and catalogued, assuming the initial information is complete and correct, there are certain aspects of a vulnerability that do not change.

Exploitability Metrics
Access Vector (AV) 3.Network
Access Complexity (AC) 3.Low
Authentication (Au) 3.None

Impact Metrics
Confidentiality Impact (C) 1.None
Integrity Impact (I) 1.None
Availability Impact (A) 3.Complete

Temporal Metrics
During the lifecycle of a vulnerability, certain events may occur which affect the urgency of the threat posed by the vulnerability.

Exploitability (E) 4.Widespread
Remediation Level (RL) 2.Temporary fix
Report Confidence (RC) 1.Not confirmed

Environmental Metrics
Different environments can have an immense bearing on the risk that a vulnerability poses to an organization and its stakeholders.

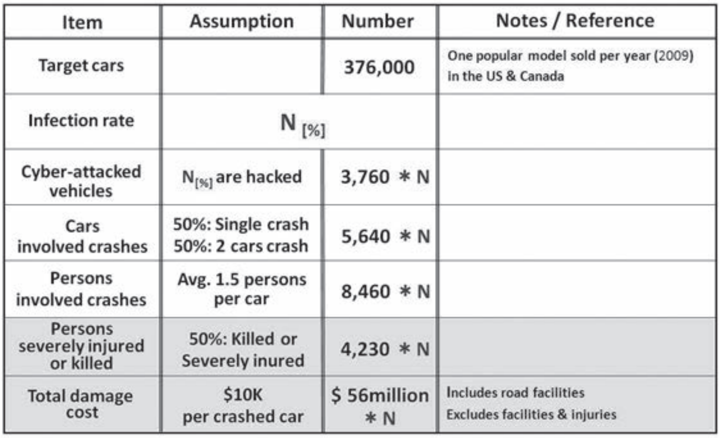
General Modifiers
Collateral Damage Potential (CDP) 4.Medium-High
Target Distribution (TD) 4.High (76-100%)

Impact Subscore Modifiers
Confidentiality Requirement (CR) 1.Low
Integrity Requirement (IR) 1.Low
Availability Requirement (AR) 3.High

We have also estimated rough damages of this new emerging cyber risk with our assumption. First of all, 376,000 of one popular model vehicles were sold in the US and Canada, only for year 2009. We assume that N [%] of these vehicles, i.e. (3,760 * N) vehicles are infected with virus. If we assume that 50% of these infected vehicles caused single-car-crashes and another 50% of these infected vehicles caused 2-cars-crashes, a total of (5,640 * N) vehicles are involved in crashes caused by this cyber risk. To more on, if we assume that average passenger number (including a driver) per vehicle is 1.5, a total of (8,460 * N) persons are involved in these crashes. If 50% of these (8,460 * N) persons would been killed or severely injured, the total number of fatalities or injuries would reach (4,230 * N). If we estimate an average of $10k financial damage per vehicle is involved in these crashes, including road facility damages (excluding fatality or injury damages), the total financial damage will reach ($56M * N). Table II shows these rough calculations based on our assumptions.

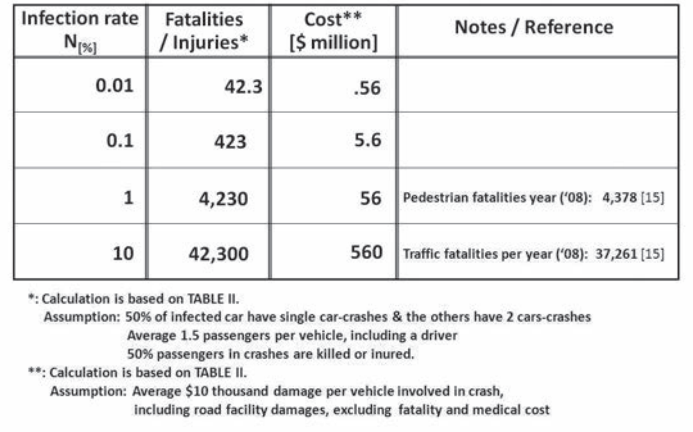
Table III shows the infection rates, N [%] vs. fatalities /injuries and financial damage estimations. Under the condition that N [%] is 1 [%], total number of fatalities and injuries becomes 4,230. This number is similarly equal to the total pedestrian traffic fatalities in the US per year (2008) and roughly 10% of all traffic fatalities in the US nationwide per year (2008) [15]. Besides, the total financial damage estimation reaches $56M, under the same condition.

TABLE II. ROUGH DAMAGE CALCULATION
(CAUSED BY VEHICLE /CARRY-IN DEVICE CONNECTIVITY)



Item	Assumption	Number	Notes / Reference
Target cars		376,000	One popular model sold per year (2009) in the US & Canada
Infection rate	$N_{[\%]}$		
Cyber-attacked vehicles	$N_{[\%]}$ are hacked	3,760 * N	
Cars involved crashes	50%: Single crash 50%: 2 cars crash	5,640 * N	
Persons involved crashes	Avg. 1.5 persons per car	8,460 * N	
Persons severely injured or killed	50%: Killed or Severely inured	4,230 * N	
Total damage cost	$10K per crashed car	$ 56million * N	Includes road facilities Excludes facilities & injuries

TABLE III. ROUGH DAMAGE ESTIMATION
(CAUSED BY VEHICLE /CARRY-IN DEVICE CONNECTIVITY)



Infection rate $N_{[\%]}$	Fatalities / Injuries*	Cost** [$ million]	Notes / Reference
0.01	42.3	.56	
0.1	423	5.6	
1	4,230	56	Pedestrian fatalities year ('08): 4,378 [15]
10	42,300	560	Traffic fatalities per year ('08): 37,261 [15]

*: Calculation is based on TABLE II.
Assumption: 50% of infected car have single car-crashes & the others have 2 cars-crashes
Average 1.5 passengers per vehicle, including a driver
50% passengers in crashes are killed or inured.
**: Calculation is based on TABLE II.
Assumption: Average $10 thousand damage per vehicle involved in crash,
including road facility damages, excluding fatality and medical cost

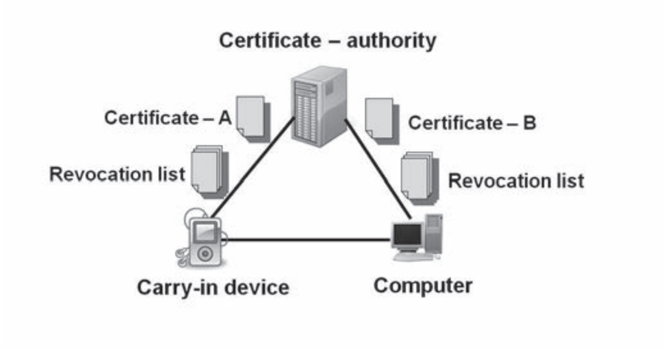
4. APPROACH FOR VEHICLE CYBER SECURITY

A. Reference: Approaches in Computer Cyber Security

In general, computer cyber security consists of encryption and certificate management. There are two types of encryptions, which are public key cryptosystem and common key cryptosystem [16]. Initially, public key cryptosystem, for example, RSA or DH (Diffie Hellman) is used to exchange small data, such as common keys in common key cryptosystem, for example, DES (Data Encryption Standards) or AES (Advanced Encryption Standards). Once a data sender and a data receiver can share with a common key, encrypted data with the common key can be exchanged between the sender and the receiver securely. Considering the balance between the required security level and durations of encryption and decryption (that depend on computational performance), a proper encryption algorithm is selected. Normally, current encryption algorithms cannot be broken within a reasonable time by existing ordinary computational performance [17].

A certificate-authority (also called as certification-anchor, certification-centre or trust-anchor) is monitoring whether a carry-in device is infected or under extraordinary conditions (FIGURE III). After a certificate-authority verifies a carry-in device condition, the certificate-authority can provide a certificate to the carry-in device without any issues. The carry-in devices with valid certificates can then connect to computers securely after a computer checks carry-in device certificates. In some security systems, a certification-authority distributes the revocation list, which includes names of carry-in devices with problems, so the revocation list can avoid the communication between carry-in devices with falsified certificates. This technique is called as "Remote (software) certification (=attestation) [18]. Secure boot is one different type of approach of certificate management system. It allows only signed software to run at the initial booting [19]. Though manufactures or system vendors cannot always track status of carry-in devices, because carry-in devices are connected at various locations, to various access points, and to various usages, Thus, computer network can be protected against cyber attacks by using the certificate management system.

FIGURE 3. BASIC CONFIGURATION FOR COMPUTER CYBER SECURITY



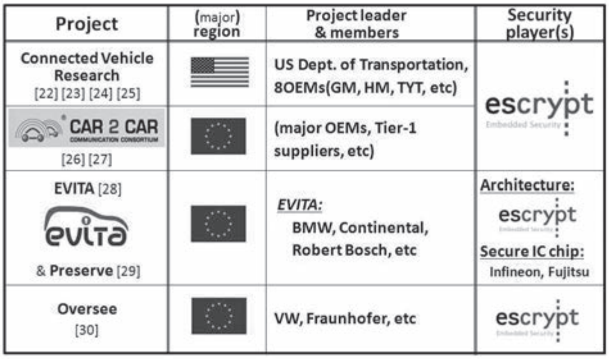
B. US Government Initiatives

In the US federal government, mainly ICS-CERT(Industrial Control Systems Cyber Energy Response Team) in US DHS(Department of Homeland Security) is leading cyber security of industrial facilities, such as electric plants, electric-grids, water-lines and others, as well as all of the transportation systems, such as stations, trains, airport, airplanes, roads, bridges, vehicles, fleet and others. Recently US DOT(Department of Transportation) started cyber security activities in transportation areas. In August 2011, US DOT issued RFI(Request For Information) about vehicle cyber security, to collect information in this topic widely from automotive industry, IT industry, academia and others [20]. In December 2011, US DOT provided the first web seminar about cyber security, - "Introduction to Cyber Security Issues for Transportation"[3], and over 200 audiences joined it in real time. Besides, NHTSA(National Highway Transportation Safety Agency) of US DOT is strongly concerned about cyber security of automotive electronics [21]. Even TRB(Transportation Research Board) of NSF(National Science Foundation) established "Cyber security Subcommittee" under "Critical Transportation Infrastructure Protection Committee (committee number ABE40). This new subcommittee will cover cyber security for all transportation modes, such as aviation, airports, trains, rails, stations, transit, road infrastructure, vehicles, trucks, fleets and others, with communicating between other TRB committees or related US DOT organizations.

C. Key Players for Vehicle Cyber Security

Table IV shows government or public automotive research projects related with cyber security in the US and Europe. Right columns show security experts in each research project. As you can see, cyber security experts have already started research activities for the entire vehicle cyber security, such as vehicle-to-vehicle communication, MCU (Micro Controller Unit) protection and others [22-30].

TABLE IV. SECURITY PLAYERS FOR AUTOMOTIVE RESEARCH PROJECTS



Project	(major) region	Project leader & members	Security player(s)
Connected Vehicle Research [22] [23] [24] [25]	🇺🇸	US Dept. of Transportation, 8OEMs(GM, HM, TYT, etc)	escrypt Embedded Security
CAR 2 CAR COMMUNICATION CONSORTIUM [26] [27]	🇪🇺	(major OEMs, Tier-1 suppliers, etc)	
EVITA [28] evita & Preserve [29]	🇪🇺	*EVITA:* BMW, Continental, Robert Bosch, etc	Architecture: escrypt Embedded Security Secure IC chip: Infineon, Fujitsu
Oversee [30]	🇪🇺	VW, Fraunhofer, etc	escrypt Embedded Security

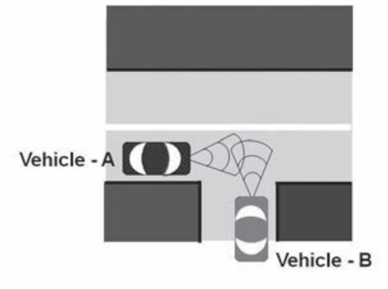
5. KEY FINDINGS AND SUGGESTIONS

A. Cyber Security Difficulties in Automotive Electronics

The certificate management system mentioned in the previous chapter can protect automotive electronics against ordinary cyber attacks, however new types or skilful virus or malware cannot be detected by a certificates-authority. In computer cyber security, virus or malware protection software is updated when a new virus or malware emerges. But, the first difficulty of automotive electronics is that online software updates have not prevailed yet, because of the limited vehicle external connectivity and risks caused by incomplete software updates [19].

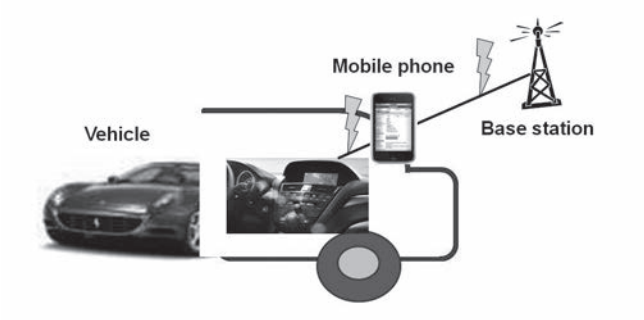
The second difficulty in vehicle cyber security is that automotive electronics have lower computational performance than ordinary computers, because of the high endurance (temperature, humidity, vibration and others) and longer vehicle life-cycle (over 10 years) compared to a computers' one (average 3 years). Then, in automotive electronics, old-generation MCU(Micro Controller Unit)s with low computational performance have to compete with hackers' latest-generation computers with high computational performance [4,31]. Therefore, cyber security, such as encryption or certificate management for automotive electronics has a higher risk to be broken in than ordinary computers' cyber security, because of the large computational performance difference between automotive electronics MCU(Micro Controller Unit)s and hackers' computers. Though secure encryption key storage is a very effective security method in ordinary computer cyber security, an encryption key has a higher risk to be stolen in automotive electronics, for the same reason. Once an encryption key is stolen, data inside or on the communication channels will be exposed. Furthermore, in the case that vehicles communicate with each other for crash avoidance (Figure 4), only limited encryption and certificate management are available, because of the time constrain (100 millisecond order). Due to the first and second difficulties, in general automotive electronics have higher risks to be infected than ordinary computers. Thus, counter measures for infected automotive electronics are more important than counter measures to avoid being infected, as compared to ordinary computer cyber security cases.

FIGURE 4. DIFFICULTY – (A) VEHICLE-TO-VEHICLE COMMUNICATION FOR CRASH AVOIDANCE



As for the third difficulty, the status of automotive electronics is more difficult to be monitored by a certificate-authority, as “Always-on connection” is not available yet. Especially, in the case if the vehicle can be connected externally only through a mobile phone (Figure 5). Once this mobile phone has been infected, this vehicle cannot receive diagnosis or treatment through the network. Though counter measures after infection are important in automotive electronics, a certificate authority cannot always monitor the status of automotive electronics, because of this difficulty. Therefore, in automotive electronics, the infection or extraordinary situation have to be detected within a vehicle. Another option is to trap virus or malware within a limited vehicle area, once a virus or malware enters in a vehicle to minimize the damages.

FIGURE 5. DIFFICULTY – (B) VEHICLE CONNECT THRU MOBILE-PHONE



In computer cyber security, DoS (Denial of Services) cyber risks can be reduced by treatment or isolates the infected computers, However as the last (forth) critical difficulty of automotive electronics, even if a small number of vehicles are infected, an infected vehicle can still threaten the drivers and passengers’ lives. Because of this reason, even when automotive electronics are infected, vehicles safety should be maintained. Last but not the least, we should focus more on avoiding safety risks that threaten driver or passenger lives. In other words, we should analyse what happens when automotive electronics are infected and feedback these review results to vehicle designs.

B. Suggestions for Vehicle Cyber Security

FIGURE 6. SUGGESTED CONCEPT FOR VEHICLE CYBER SECURITY

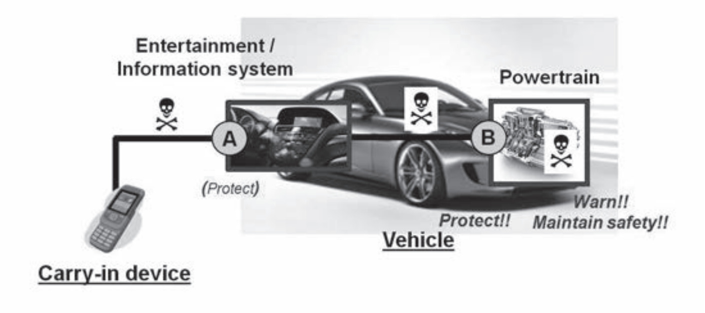


Figure 6 shows our basic suggestion with the consideration of the above mentioned difficulties. First, carry-in devices, such as smart-phones, portable music players or vulnerable mass-production computing devices, have high possibilities of being infected, because of various usages /applications, various places where they are been used and various access points. Therefore, virus or malware should be protected after point (A). However because of the limited computational performance and the limited connectivity of automotive electronics, it is difficult to protect against virus or malware at point (A), For these reasons, the first suggestion is to avoid virus or malware invasion into safety critical components or areas at point (B). One basic approach is to divide safety critical domains (areas, networks or components) from informative and convenient domains that have higher risks to be infected with more frequent external connectivity. Even if physical domain partitioning is difficult, logical partitioning, such as gateway insertion or virtual partitioning can be one of the approaches [4]. For the same purpose, hardware roles and software roles should be examined to avoid software manipulation caused by cyber attacks [19].

As for the second suggestion, even if virus or malware invade safety critical areas, it is very important to detect infection or abnormal condition quickly, and to inform them to the driver. This approach avoids critical accidents that threaten driver or passenger lives. So, the infection or extraordinary situation is supposed to be detected within a vehicle, because of the limited vehicle external connectivity. In other words, “Self-diagnosis”, “Self-detection” and “Self-warning” are more important. It is value that many automotive electronics devices or components are monitoring their individual status periodically and immediately warning drivers when something happen.

The last suggestion is to maintain safety even if safety critical components are infected. We should review what happens when automotive electronics are infected and feedback these review results to vehicle designs. As one example, when automotive electronics are infected, minimum fail-tolerance operations, such as, braking, stopping engines and opening the doors from inside, etc, are very effective to keep track. In this process, the concept of functional safety is very useful.

6. CONCLUSIONS AND NEXT STEPS

The growth of vehicle carry-in devices, such as smart-phones, portable silicon music-players and others are changing the paradigm of vehicle cyber risk. In the new emerging vehicle cyber risk, first, virus and malware are attached to applications or music /video file, and are downloaded to in carry-in devices, they then invade into automotive electronics (Figure 1). We assessed the vulnerability of this new emerging cyber risk by using a public cyber risk assessment tool (CVSS: Common Vulnerability Scoring System) [14] (FIGURE II), and also estimated the rough damages of this cyber risk based on our assumptions (Table II and Table III).

Comparing to ordinary computers, vehicle cyber security has many difficulties, such as "Limited connectivity", "Low computational performance" "Difficulty to monitor status of automotive electronics" and "Critical risk for drivers or passengers lives". As a consequence, counter measures after automotive electronics are infected, are more important than counter measures to avoid being infected. At the first plan, when virus or malware invade automotive electronics, safety critical components or areas, such as powertrain, braking and steering should be protected. Even if virus or malwares invade into safety critical areas, abnormal condition should be detected and be informed to a driver, quickly. Finally, when virus or malware invades into safety critical areas, at least, critical accidents that can threaten drivers or passengers' lives should be avoided.

In this paper, we have introduced risk analysis and problem findings. On a whole, as the next step, we are planning further the study on counter measures against this new cyber risk, and keep track with related governments initiatives, standards, researches and other activities worldwide.

REFERENCES:

[1] ISO "Information technology - Security techniques - Hash-functions" ISO/IEC 10118; ISO "Information technology - Security techniques - Key management" ISO/IEC 11770; ISO "Information technology - Security techniques - Trusted Platform Module" ISO/IEC 11889; ISO "Information technology - Security techniques - Evaluation criteria for IT security" ISO/IEC 15408 and others

[2] J. Cambridge *et al*., "Security and Critical Infrastructure Protection" TR NEWS, No. 275, Jul-August 2011

[3] M. Dinning *et al*., (2011, Dec, 7) "Introduction to Cyber Security Issues for Transportation" [Web seminar]. Available: www.pcb.its.dot.gov/t3/s111207/s111207_cybersecurity_intro.asp

[4] Information-Technolgy Promotion Agency (of Japanese government). (2011, Apr) "2010 report: Movements of Vehicle Cyber-security", (Japanese). Available: www.ipa.go.jp/security/fy22/reports/emb_car/documents/embsec_car2011.pdf

[5] K. Poulsen. (2010, Mar, 17). "Hacker Disables More Than 100 Cars Remotely" [Internet]. Available: www.wired.com/threatlevel/2010/03/hacker-bricks-cars/

[6] T. Kohno *et al*., "Experimental Security Analysis of a Modern Automobile" in IEEE Symposium on Security and Privacy 2010 [Internet]. Available: www.autosec.org/pubs/cars-oakland2010.pdf

[7] A. Weimerskirch, "Do Vehicles Need Data Security?" Society of Automotive Engineers World Congress, Detroit, MI, 2011

[8] ISO "Road vehicles - Functional safety" standard ISO 26262

[9] M. Raya, P. Papadimitratos and J.P. Hubaux, "SECURING VEHICULAR COMMUNICATIONS," Wireless Communications, IEEE , vol.13, no.5, pp.8-15, October 2006

[10] J.P. Hubaux, S. Capkun and J. Luo, "The security and privacy of smart vehicles," Security & Privacy, IEEE , vol.2, no.3, pp.49-55, May-June 2004

[11] (2011, Aug) “comScore Reports July 2011 U.S. Mobile Subscriber Market Share,” [Internet]. Available: http://www.comscore.com/Press_Events/Press_Releases/2011/8/comScore_Reports_July_2011_U.S._Mobile_Subscriber_Market_Share

[12] R. Vogelei, (2011, Jun) “Mobile Application Downloads to Approach 48 Billion in 2015,” [Internet]. Available: http://instat.com/press.asp?ID=3155&sku=IN1104930MCM

[13] E. Chickowski, (2011, Dec 1) “Android Mobile Security: A Growing Threat,” [Internet]. Available: http://mobile.channelinsider.com/c/a/Security/Android-Mobile-Security-A-Growing-Threat-548275/

[14] Information-Technology Promotion Agency (of Japanese government), “CVSS (Common Vulnerability Scoring System) Calculator”. Available: http://jvndb.jvn.jp/cvss/index.html

[15] U.S. Department of Transportation Research and Innovative Technology Administration Bureau of Transportation Statistics (2009) “Transportation Statistics Annual Report 2009”

[16] Information-Technology Promotion Agency (of Japanese government), (2008), “E-learning textbook about Cipher”, (Japanese). Available: www.ipa.go.jp/security/fy19/development/e_Learning_Cipher/index.html

[17] Encryption and Certificates, 1st ed., (Japanese), Nikkei BP publish, Tokyo, Japan

[18] Wikipedia, [Internet]. Available: http://en.wikipedia.org/wiki/Trusted_Computing

[19] A. Weimerskirch, “Security Considerations for Connected Vehicles,” in SAE Government/Industry Meeting, Washington DC, 2012 January. Available: http://www.sae.org/events/gim/presentations/2012/weimerskirch_escrypt.pdf

[20] Department of Transportation, “Cyber security and Safety of Motor Vehicles Equipped with Electronic Control Systems”, Solicitation Number: DTRT57-11-SS-00007, (2011, Aug, 2). Available: www.fbo.gov/index?s=opportunity&mode=form&id=40c0c2730b334df090dba322a61e956f&tab=core&_cview=0

[21] D. Smith, Opening Address of SAE Government/Industry Meeting, Washington DC, 2012 January.

[22] J. Sayer, ITS World Congress 2011, “Safety Pilot Model Deployment Test Conductor”, Orlando FL, 2011, Oct, 20

[23] Department of Transportation, “Safety Pilot Program Overview”, [Internet]. Available: www.its.dot.gov/safety_pilot/index.htm#6

[24] Department of Transportation, “Connected Vehicle Safety Pilot Program”, [Internet]. Available: www.its.dot.gov/factsheets/pdf/SafetyPilot_final.pdf

[25] V. Briggs, (2011, Aug, 3) “ITS Policy Program: Safety Policy Review and Discussion Introduction” [Web workshop]. Available: www.its.dot.gov/presentations/August_PolicyDay_v12_files/frame.htm

[26] A Weimerskirch, “V2X Security & Privacy: The Current State and Its Future” in ITS World Congress, Orlando, FL, 2011

[27] N. BiBmeyer, H. Stubing et al., “A Generic Public Key Infrastructure for Securing Car-to-X Communication” in ITS World Congress, Orlando, FL, 2011

[28] “EVITA(E-safety Vehicle Intrusion Protected Applications)”, [Internet]. Available: http://evita-project.org/

[29] “European R&D Project: PRESERVE(Preparing SecureVehicle-to-X communication systems)”, [Internet]. Available: http://cordis.europa.eu/fetch?CALLER=PROJ_ICT&ACTION=D&CAT=PROJ&RCN=97466

[30] “OVERSEE(Open Vehicular Secure Platform)”, [Internet]. Available: www.oversee-project.com/

[31] P. Kleberger, T. Olovsson and E. Jonsson, “Security aspects of the in-vehicle network in the connected car,” Intelligent Vehicles Symposium (IV), 2011 IEEE , vol., no., pp.528-533, 5-9 June 2011