Vehicle Cyber-Security: Carry-in Device Vulnerabilities

Hiro Onishi, Kelly Wu
Alpine Electronics Research of America, Inc.

22nd ITS World Congress
Bordeaux, France
5 to 9 October
2015

session: TS06
paper: AM-1940

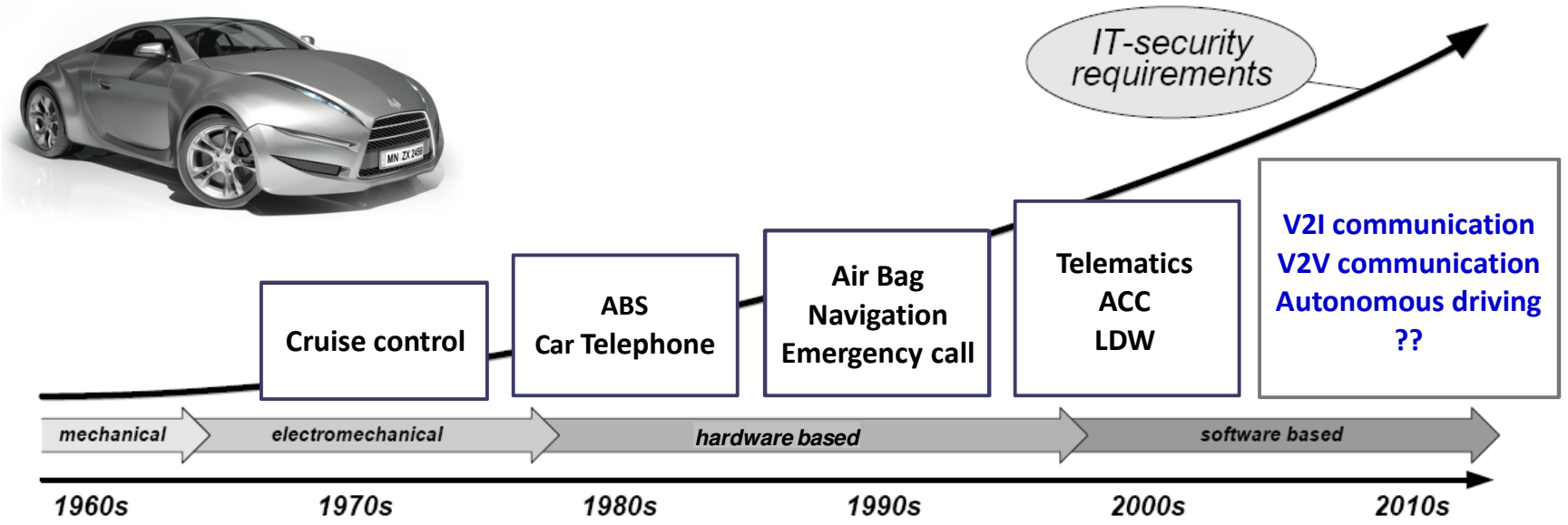
TOWARDS INTELLIGENT MOBILITY
Better use of space

Outline

1. Background
2. Carry-in Device Vulnerabilities
   - 2.1. Smart-phone vulnerabilities
   - 2.2. USB (Universal Serial Bus) vulnerabilities
   - 2.3. Bluetooth vulnerabilities
3. Countermeasures (against Carry-in Device Attacks)
   - 3.1. Protections (against carry-in device attacks)
   - 3.2. Smart-phone utilization (for vehicle cyber-security)
4. Summary

Acknowledgement

1. Background



Modern vehicles with up to ~80 CPUs, ~2 miles of cable, and several hundred MB of software are NO longer just "Mechanical Systems"

Reference: A. Weimerskirch, "*Security Considerations for Connected Vehicles*", in SAE Government and Industry Meeting, Washington DC, Jan. '12

1. Background – recent affairs

FCA(Fiat Chrysler Automobiles**) issued a voluntary recall of 1.4 M vehicles, due to cyber-vulnerabilities proven by security consultants (**Jul. 2015**).**

Picture

Reference:

~ FCA, Statement: Software Update: http://media.fcanorthamerica.com/newsrelease.do?id=16849

~ (picture), https://blog.kaspersky.co.jp/blackhat-jeep-cherokee-hack-explained/8480/

1. Background – recent affairs

Cyber-vulnerability of OnStar smart-phone App, which could maliciously unlock vehicles, has been proven by security consultants. GM subsequently updated its software (Jul. 2015**).**

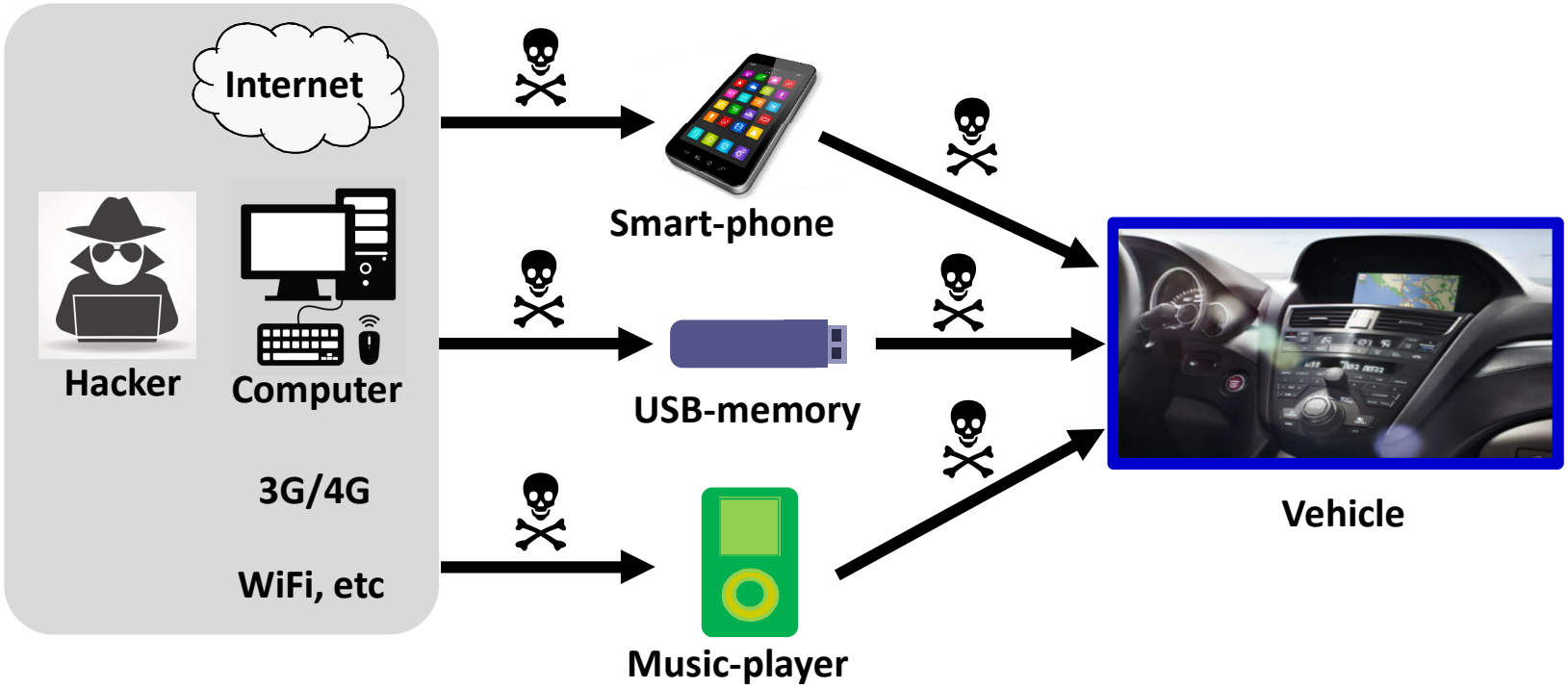
Picture

Reference/picture:

This gadget hacks GM cars to locate, unlock, and start them (Updated)
www.wired.com/2015/07/gadget-hacks-gm-cars-locate-unlock-start/

New paradigm of vehicle cyber-risks

Carry-in devices (i.e. smart-phones, USB-storage, music-players, etc) brought in and connected to vehicles may increase vehicle cyber-risks.



References:

H. Onishi, Paradigm Change of Vehicle Cyber Security, in CyCon (Jun. '12, Tallinn, Estonia)

ALPINE
Driving Mobile Media Innovation

Challenges to protect vehicle cyber security against attacks on vulnerable carry-in devices

+ Difficulty to isolate carry-in devices from external IT world.
+ Carry-in devices
  - can be used in various locations,
  - can access various websites, and
  - can download various apps/files
+ Popular Apps and music/video files may be open-doors to cyber-attacks.
+ Carry-in device security is limited, because of limited CPU performance, furthermore, sometimes users disable even limited security mechanism.
+ Once carry-in device is infected, virus/malware can cause malfunctions of various invehicle electronic systems/components.

ALPINE
Driving Mobile Media Innovation

Examples of recent actions for vehicle cyber-security

Congress:

- Senator Ed Markey (D-MA) requested information pertaining to vehicle cyber-security from major auto makers (Dec. 2013)[*1].
- Senators introduced "SPY-Car(Security & Privacy in Your car)" Act[*2].

NHTSA (National Highway Safety Administration) of Dept. of Transportation:

Department of Transportation issued RFC(Request for Comments) for vehicle cyber-security (Sep. 2014)[*3].

SAE(Society of Automotive Engineers) international:

Developing J3061 "Cybersecurity Guidebook for Cyber-Physical Automotive Systems"[*4].

(Auto-industry):

Established Auto-ISAC (Information Sharing and Analysis Center) to share security threats and vulnerabilities of vehicle cyber-security (Jul. 2014)[*5].

AAM(Alliance of Automobile Manufacturers):

Published auto-industry self-regulatory principles (Nov. 2014)[*6].

Reference:

*1: E. Markey, Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk, (Feb. 2015)

*2: 114TH CONGRESS 1ST SESSION S. ll To protect consumers from security and privacy threats to ….

*3: NHTSA, NHTSA-2014-0071, (Sep. 2014)

*4: SAE-International, "Cybersecurity Guidebook for Cyber-Physical Automotive Systems"

*5: Letter by AAM and Global Automakers, "Cybersecurity Initiative by the Alliance of Automobile …. (Jul. 2014)

*6: AAM, "Consumer Privacy Protection Principles"(Nov. 2014)

2. Carry-In Device Vulnerability – Smart-phone

ALPINE Driving Mobile Media Innovation

Smart-phone integration has become mainstream in vehicles

Smart-phones have been used for *Emergency-call*, *Remote-diagnosis*, *Stolen-vehicle-tracking* & *Internet-access*, etc.

→ *In Four Years, Most Cars Will Work With Smart Phones*[*1], (May, '12) ~ Forbes

+ Apple: CarPlay[*2]

+ Google: Android-Auto[*3]

References:

*1: M. Paula, *In Four Years, Most Cars Will Work With Smart Phones*, FORBES, (May, 2012) www.forbes.com/sites/matthewdepaula/2012/05/19/in-four-years-most-cars-will-work-with-smart-phones/

*2: www.apple.com/ios/carplay/

*3: www.android.com/auto/

2. Carry-In Device Vulnerability – Smart-phone

ALPINE
Driving Mobile Media Innovation

Smart-phone integration has become mainstream in OEM systems

Brand	System
Cadillac	Cadillac Shield
Chevrolet	MyLink
Buick	OnStar®
GMC	
Chrysler	Uconnect®
Jeep	
Dodge	
Fiat	
Ford	SYNC® / MyFordTouch®
Lincoln	MyLincolnMobile™
BMW	Connected Drive
Mercedes-Benz	mbrace®

Brand	System
VolksWagen	Car-Net®
Toyota	Entune®
Lexus	Enform
Honda	HondaLink®
Acura	AcuraLink®
Subaru	STAR LINK™
Nissan	NissanConnect®
Infinity	Infiniti Connection®
Mazda	MAZDA CONNECT™
Hyundai	BlueLink®
Kia	UVO

From Washington DC Autoshow, 2015

ALPINE
Driving Mobile Media Innovation

Key vulnerabilities of smart-phone

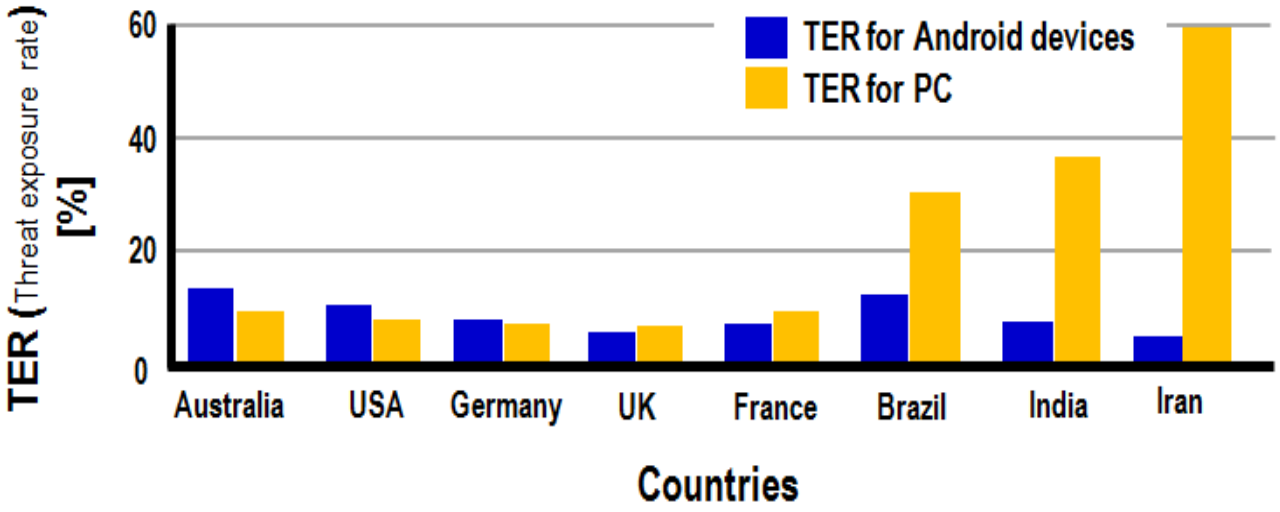
+ Limited security mechanism is installed,
  because of limited CPU performance, despite its functionalities.
+ Multiple communication channels: 3G/4G, WiFi, and Bluetooth
+ Multiple players:
  Mobile service providers, OS providers, handset manufacturers,
  application developers, etc
+ Personal use:
  e.g.: - Frequently downloading (3rd party) applications
  - Frequently accepting privilege requests
  from applications

References:

Smartphone cloud security study group (Ministry of Internal Affairs and Communications), Final report (**Japanese**), (2012) www.soumu.go.jp/main_content/000166095.pdf

Smart-phone threats are increasing

New malware type in (Android) smart-phones increased from 238 in 2012 to 804 new threat types in 2013



TER(Thread Exposure Rate) of PCs and Android devices

References:
~ Sophos, Sophos Security Threat Report 2013
~ Sophos, Mobile Security Solution – Sophos Mobile Control, (Japanese)

2. Carry-In Device Vulnerability – Smart-phone

ALPINE
Driving Mobile Media Innovation

Various phases of smart-phone malware attacks

+ Installation:
  - Repackaging attacks
  - Update attacks
  - Drive-by downloads
+ Activation
+ Malicious payloads:
  - Privilege escalation
  - Remote control
  - Financial charges
  - Personal information stealing

References:

Y. MA and M. Sharbaf, Investigation of Static and Dynamic Android Anti-virus Strategies, in IEEE International Conference on Information Technology: New Generations (April, 2013, Las Vegas, NV)

2. Carry-In Device Vulnerability – Smart-phone

ALPINE
Driving Mobile Media Innovation

Malicious (smart-phone) application installer

Security experts discovered:

Application installer can replace legitimate application by malicious different application with adding escalated privileges without users notification (Jan. 2014**).**

Nearly half of Android users may be exposed to this kind of attack.

Picture

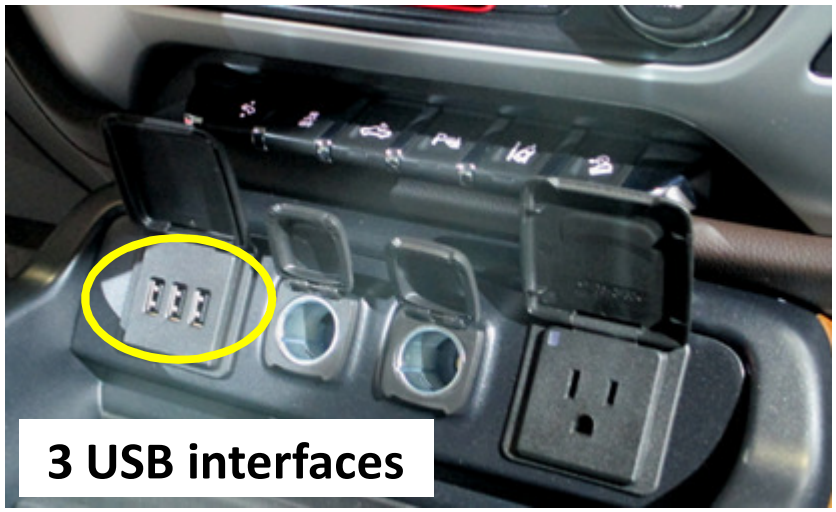
References:

Z. Xu, Android installer hijacking vulnerability could expose Android users to malware, (Mar. 2015), http://researchcenter.paloaltonetworks.com/2015/03/android-installer-hijacking-vulnerability-could-expose-android-users-to-malware/

USB-connections are standard options in many vehicles

USB devices are widely utilized to connect various electronic devices to vehicles.

(During development/maintenance, they also can be used to connect test-equipment and upload/download of software/data)



Various vehicle makes/models have USB port(s).
Many vehicles have 2 or 3 USB-ports.

2. Carry-In Device Vulnerability – USB

Serious USB vulnerability was disclosed in Aug. ’14

Hackers can re-write the firmware of a USB memory to

- Make the USB memory act as a USB keyboard for malicious inputs
- Include malicious boot virus in the USB memory

+ A wrong destination maliciously given to a navigation system, without the driver acknowledging.

+ Malicious boot virus makes a vehicle center console inoperable.

References:

~ K. Nohl et al., BadUSB – On accessories that turn devil, in blackhat – USA ’14 (Aug. ’14, Las Vegas, NV)

~ Security Research Labs, Turning USB peripherals into BadUSB

ALPINE
Driving Mobile Media Innovation

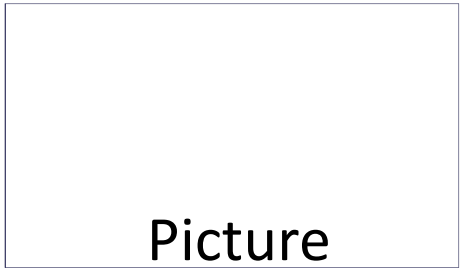
Bluetooth functionalities in vehicles

Phone: Voice calling, Voice dialing, etc.

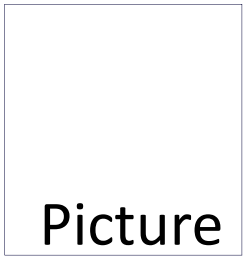
Entertainment: Streaming audio, etc.

Other: SYNC address-book/schedules, PC/tablet tethering, Car-diagnostics, Health-monitoring, etc.

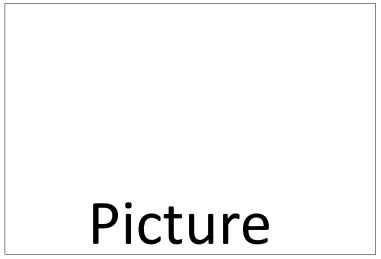
Smart-phone



Music Streaming



Health Monitoring



References:

*1: Bluetooth SIG, "Automotive Market" www.bluetooth.com/Pages/Automotive-Market.aspx

*2: Bluetooth SIG, "Cars" www.bluetooth.com/Pages/Cars.aspx (accessed on Sep. 2015)

2. Carry-In Device Vulnerability – Bluetooth

ALPINE
Driving Mobile Media Innovation

Increased attack-paths thru Bluetooth

Examples of Attacks:

- Eavesdropping,
- (High)jacking,
- Sniffing,
- Stealing personal information,
- Buffer-over-flow attack, etc

References:

J. Markus(Lucent Technologies), Security Weaknesses in Bluetooth, https://cse.sc.edu/~wyxu/2008-csce790/papers/Security_Weaknesses_Bluetooth.pdf.

ALPINE
Driving Mobile Media Innovation

Bluetooth vulnerabilities

+ Limited security mechanism,
because of short-range (10m-100m) communication.

→ Sometimes, even limited security mechanisms are not activated by users.

→ The pairing of devices does not require the users' approval or permission.

→ Virus/malware in carry-in devices may remove/minimize even limited security mechanism.

+ Once the BT device is paired, important information (i.e. address book, password, etc**) can be exploited.**

→ Further attack can occur against in-vehicle onboard devices remotely.

+ Possibility to lead to cyber attack, such as Buffer overflow attack, etc.

Approach - 1: Protect safety critical areas

Isolation:

- Isolate safety critical areas from infotainment areas.
- Examine interactions between infotainment areas and safety critical areas
  (e.g.: retain “Slow-down” command, but exclude “Speed-up” command)
- Protect against malicious interactions from software or other components.

Others:

Secure-boot, Virtualization, Encryption, etc

References:

H. Onishi, Approaching Vehicle Cyber Security by Applying the Functional Safety Concept, in ITS World Congress (Oct. ’13, Tokyo, Japan)

Approach - 2: Minimize hazards

+ Multiple back-up mechanisms in emergency:
  Critical functions should be controlled by alternative options,
  → e.g.: Steering can be controlled manually even if power-steering is broken
+ Detecting malware intrusion and operation failures in a timely manner for safety critical areas
  → e.g.: periodically check an emergency call
+ Abnormal conditions should be immediately notified to the driver, to avoid or mitigate serious hazards.
  → e.g.: rearview camera monitor, navigation, etc

Photo © Alpine Electronics

References:
H. Onishi, Approaching Vehicle Cyber Security by Applying the Functional Safety Concept, in ITS World Congress (Oct. '13, Tokyo, Japan)

ALPINE
Driving Mobile Media Innovation

Smart-Phone's potentials

Smart-Phones (with high speed communication capability & high CPU performance**)**
can provide security functions (which are prevalent in IT industry)

+ Update (security) software on-the-fly

+ Remotely monitor (electronic) components

+ Have a certificate authority issue a certificate

+ Remotely remove threats from infected (electric) components

+ Record a software update history

References:
H. Onishi, Guidelines against Diversified Vehicle Cyber Risks, in IEEE-CNS (Oct. '14, SFO, CA)

ALPINE
Driving Mobile Media Innovation

Challenges

+ Continuous and real-time operations are required (in miliseconds)

+ Vulnerable smart-phones (with limited security mechanism) can jeopardize the entire vehicle system

→ Op. a:

Design a special-purpose smart-phone
(with high speed communication module and CPU)
to aid vehicle protection against cyber security threats

→ Op. b:

Restrict the use of smart-phone in a vehicle

Both options can cause further inconvenience to users.

References:
H. Onishi, Guidelines against Diversified Vehicle Cyber Risks, in IEEE-CNS (Oct. '14, SFO, CA)

4. Summary

+ Cyber-attacks against modern vehicle electronics with large amount of CPU and complex software has become a concern for society. Ultimately, autonomous vehicles could be targeted.

+ Besides direct cyber-attacks against onboard vehicle components, cyber-attacks exploiting carry-in device vulnerabilities (i.e. smart-phones, USB, Bluetooth, etc) have aroused great concerns due to:

  - Difficulties to isolate carry-in devices from external IT world

  - Limited security mechanism of carry-in devices and the prevalence of people putting less attention on carry-in device security

+ Approaches as to how to prevent cyber-attack via carry-in devices and how to securely utilize carry-in devices (i.e. smart-phones)' are essential.

Acknowledgement

To: Computer Science division
of CSU-DH(CA State University Dominguez Hills)

For: Advice regarding smart-phone vulnerability

Thank you for your attention!!

Alpine Electronics Research of America, Inc.

Hiro Onishi

honishi@alpine-la.com, Tel: +1-310-783-7281

Kelly Wu

kwu@alpine-la.com, Tel: +1-310-783-7275