IHS AUTOMOTIVE

Presentation

# Cyber-Security in the Connected Car Age

GENIVI Conference – Seoul, October 21, 2015

ihs.com

IHS AUTOMOTIVE
driven by POLK

**Egil Juliussen,** Director Research & Principal Analyst
+1 630 432 1304, egil.juliussen@ihs.com

© 2015 IHS

# Cyber-Security in the Connected Car Age

- What is the problem?
- What are the risks & negative impact?
- What can be learned from other industries?
- What are the big-picture solutions?
- Are there automotive solutions?
- Summary & take-away

**Egil Juliussen, Ph.D. Director Research & Principal Analyst**

© 2015 IHS

# Auto Security Problem

| | Key Information | Problem/Comments |
|---|---|---|
| Complacency | ▶ Not needed previously<br>▶ "It will not happen to us"<br>▶ Too much effort vs. rewards<br>▶ No known actual breaches | ▶ Hard to justify cost and effort<br>▶ Common view in all industries<br>▶ True, but is now changing<br>▶ Only R&D; proof of concept |
| Connected Car Growth | ▶ Opens door to remote access<br>▶ Multiple connection points | ▶ Connected cars on the road:<br>▶ 2015-83M; 2022-430M |
| Security Knowledge | ▶ New skill set needed<br>▶ Rare skill in auto industry | ▶ Not part of SW testing yet<br>▶ Shortage in most industries |
| Examples | ▶ Chrysler Jeep: July 2015*<br>▶ OnStar RemoteLink app: 7/15<br>▶ Tesla (physical access): 8/15<br>▶ BMW ConnectedDrive: 1/15<br>▶ Many models are hackable | ▶ Open H-U port allowed access<br>▶ App spoofing via own device<br>▶ Fixed via remote SW update<br>▶ Fixed via remote SW update<br>▶ Based on hacking R&D |

* Resulted in Chrysler recall of 1.4M vehicles → Cost of $140M+
OnStar RemoteLink downloaded 3M+ times; BMW security flaw in 2.2M vehicles

© 2015 IHS

**SOURCE: IHS Automotive**
***Software Apps & Service Portal***

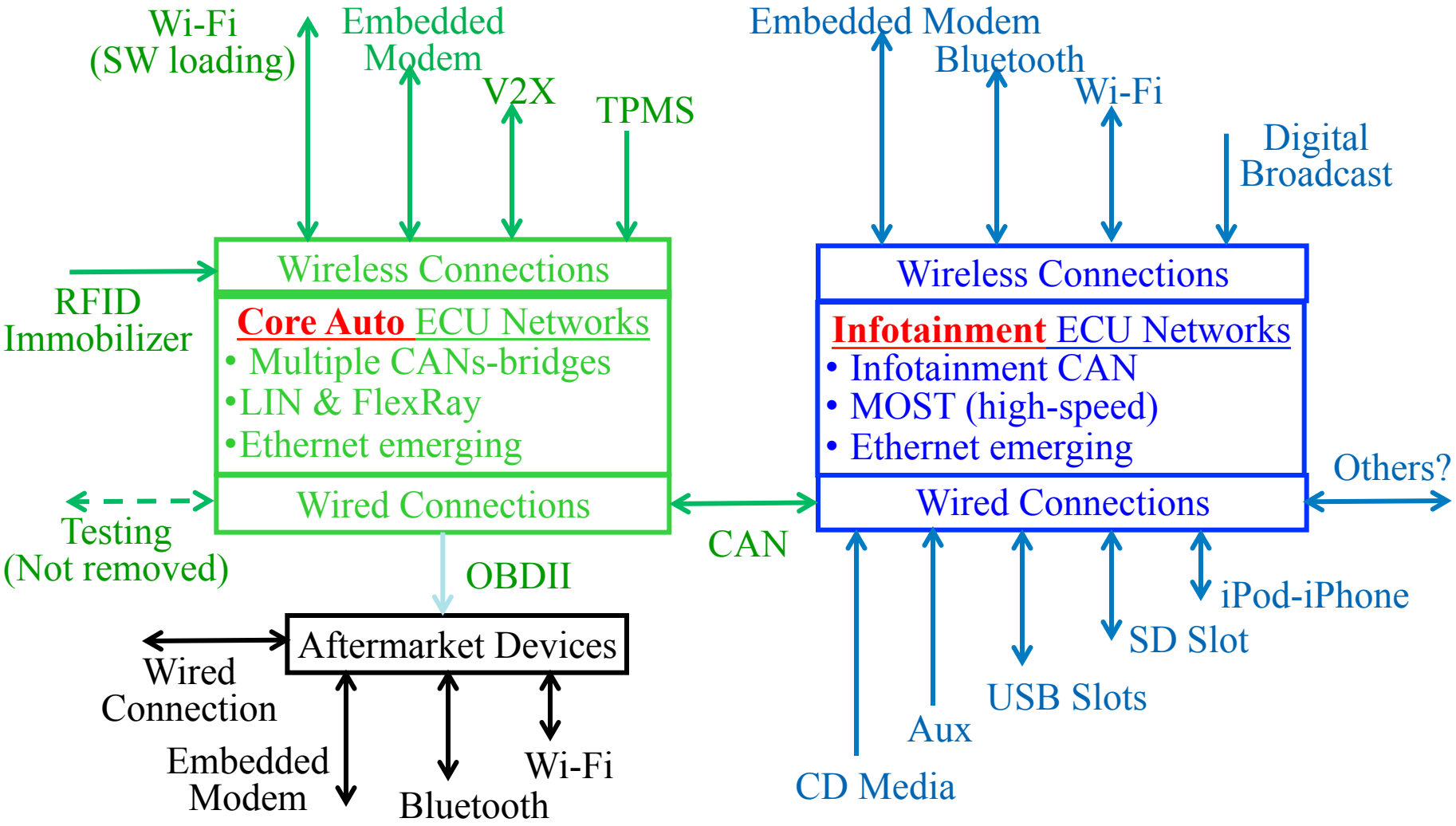
# What Makes Future Cars More Vulnerable to Security Threats?

| | Key Information | Comments |
|---|---|---|
| Connected Car | ▸Cloud connected car content<br>▸Connected ECU architecture<br>▸Self-driving & driverless cars | ▸More wireless connections<br>▸Remote software updates<br>▸Always connected |
| Platform Design | ▸ Hardware platforms<br>▸ Software platforms<br>▸ Application platforms | ▸More standardization<br>▸More system knowledge<br>▸More program knowledge |
| Attack Access Points | ▸OBDII<br>▸OBDII w/wireless module<br>▸Telematics modem link(s)<br>▸Smartphone links<br>▸Wi-Fi network link(s) | ▸Need physical access<br>▸Bluetooth, Wi-Fi, cellular<br>▸2.5G, 3G, 3.5G, 4G, 4.5G<br>▸Bluetooth, USB & others<br>▸Router & Direct |
| Security Deployment Speed | ▸Connected car growth<br>▸Many current security holes<br>▸Security is new skill set<br>▸Built-in security needed | ▸Many access points<br>▸Need to be found & updated<br>▸Low auto security knowledge<br>▸How quickly will this happen? |

© 2015 IHS

**SOURCE: IHS Automotive**
***Software Apps & Service Portal***

# Auto System Access Points: 2015




**Hacking research has shown that nearly all access points can be compromised!**

© 2015 IHS

SOURCE: IHS Automotive
*Software Apps & Service Portal*

# Cyber-Security in the Connected Car Age

- What is the problem?
- What are the risks & negative impact?
- What can be learned from other industries?
- What are the big-picture solutions?
- Are there automotive solutions?
- Summary & take-away

**Egil Juliussen, Ph.D. Director Research & Principal Analyst**

© 2015 IHS

# Auto Security Threat Overview

| | Security Attack Goals | Comments |
|---|---|---|
| Property Theft | ▸ Steal vehicle<br>▸ Steal valuable auto components | ▸ Via unauthorized access<br>▸ Via unauthorized access |
| Industrial Espionage | ▸ Steal OEM's intellectual property<br>▸ Spy on OEM's expertise | ▸ Software & hardware<br>▸ Intellectual property value |
| Deception | ▸ Circumvent HW-SW functionality<br>▸ Manipulate auto equipment<br>▸ Manipulate contracts & agreements | ▸ Speed, features, chip tuning<br>▸ Toll device, digital tachograph<br>▸ Lease, warranty |
| Privacy & Data | ▸ Location tracking<br>▸ Event data recorders<br>▸ Credit card & financial information | ▸ Stalking, VIP tracking<br>▸ Accident investigations<br>▸ If stored in car electronics |
| Damage & Destruction | ▸ Harm driver and passengers<br>▸ Harm auto OEM's reputation<br>▸ Harm transportation system | ▸ Accidentally or for-profit<br>▸ Accidentally or for-profit<br>▸ Cyber warfare |

© 2015 IHS

**SOURCE: IHS Automotive**
***Software Apps & Service Portal***

# Auto Security Attacks: Financial Risks

| | Key Information | Comments |
|---|---|---|
| Legal Risks | ▸ Cost of lawsuits<br>▸ Cost of negligence | ▸ In 10s of millions of dollars<br>▸ Possibly 100s of millions of dollars |
| Business & Customer Loss | ▸ Loss of customer contracts<br>▸ Software upgrade/recall cost<br>▸ Future business loss | ▸ Possibly 100s of millions of dollars<br>▸ 10s to 100s of millions of dollars<br>▸ Until new product is re-established |
| Reputation Impact | ▸ Most severe for auto OEMs<br>▸ Public likely to shun autos with cyber-security issues | ▸ From $100M to $1B+<br>▸ Whether real or not<br>▸ Even after fixes have been done |
| Summary | ▸ Successful software security attacks have the potential to be among the most costly auto recall & reputation events | ▸ Legal risk will be substantial<br>▸ Product update cost may be low to extreme high<br>▸ Reputation impact will be severe |

© 2015 IHS

**SOURCE: IHS Automotive**
***Software Apps & Service Portal***

# Cyber-Security in the Connected Car Age

- What is the problem?
- What are the risks & negative impact?
- What can be learned from other industries?
- What are the big-picture solutions?
- Are there automotive solutions?
- Summary & take-away

**Egil Juliussen, Ph.D. Director Research & Principal Analyst**

© 2015 IHS

# Security Lessons from Other Industries

| | Key Information | Comments |
|---|---|---|
| PC Industry: Early 1990s | ▸ Mostly standalone PC<br>▸ Little connectivity<br>▸ None or minimal security | ▸ LANs emerging<br>▸ Email emerging<br>▸ Internet was a niche market |
| PC Industry: 2000s | ▸ Mostly Internet connected PCs<br>▸ Security is a major problem<br>▸ Add-on security software | ▸ Broadband-era established<br>▸ Poor and add-on security<br>▸ Limited anti-virus software |
| PC, Tablets & Smartphones 2010s | ▸ Internet-connected devices<br>▸ Add-on security software<br>▸ Security is a major problem<br>▸ Smartphone/tablet: new target<br>▸ Infected websites: new problem | ▸ Internet drives PC/CE industries<br>▸ Service-based anti-virus<br>▸ Improved PC security, but ….<br>▸ Security is lagging<br>▸ In addition to email |
| Lessons | ▸ Security has to be built-in<br>▸ Hardware security is lacking<br>▸ OS must use MPU HW security | ▸ In hardware and software<br>▸ Need to be part of MPU<br>▸ Apps must use OS/HW security |

© 2015 IHS

**SOURCE: IHS Automotive**
***Software Apps & Service Portal***

# Security Attack Sources: PC vs. Auto

| | Motivation | PC Industry | Auto Industry |
|---|---|---|---|
| Hackers: White Hat | ▸Reputation<br>▸Show vulnerable attack points | ▸Since beginning of PC<br>▸Mostly positive goals, but unintended impact | ▸First wave of hacking<br>▸Have shown many auto security flaws |
| Entre-preneurs | ▸Financial gains<br>▸Mostly legal | ▸Mostly email spam via unlimited broadband | ▸Limited, no unlimited data plans in future |
| Organized Crime | ▸Financial gains<br>▸Credit cards & bank accounts | ▸Mostly Botnet-based<br>▸Phishing multiplier<br>▸Moving to Smartphone | ▸Mostly via Smartphone<br>▸Harm-for-hire likely<br>▸Financial gains |
| Industrial Espionage | ▸Valuable IP theft<br>▸Co-sponsored<br>▸Gov-sponsored | ▸Common, but little data available<br>▸Competent hackers | ▸Long-term problem<br>▸Likely severe problem<br>▸Physical access likely* |
| Terrorism | ▸Political goals<br>▸Intention to harm | ▸Productivity tool using standard PC apps | ▸Future use, but rare<br>▸Auto as lethal weapon |
| Hacktivism | ▸Hacking used for political reasons<br>▸Unauthorized data access | ▸Unauthorized access tool to databases<br>▸Small group, very competent hackers | ▸Not likely or limited—at least in auto ECUs<br>▸Must know auto & very competent hackers |

© 2015 IHS

**SOURCE: IHS Automotive**
***Software Apps & Service Portal***

# Security Attack Categories: PC vs. Auto

| | PC Industry | Purpose | Auto Impact |
|---|---|---|---|
| Hacking Tools<br><br>(Learn) | ▶Vulnerability scanner<br>▶Port scanner<br>▶Password cracking<br>▶Packet sniffer<br>▶Spoofing, Phishing<br>▶Backdoor | ▶Find weaknesses<br>▶Find open ports<br>▶Recover password<br>▶Find access data<br>▶Illegitimate Website<br>▶Bypass authentication | ▶Yes, emerging<br>▶Yes, done (Chrysler)<br>▶Yes, done<br>▶Yes, w/physical access<br>▶Unlikely<br>▶Yes, diagnostics port |
| Attack Tools | ▶Viruses<br>▶Worms<br>▶Trojans<br>▶Root kits<br>▶Key loggers<br>▶Denial of service | ▶Self-replicating, user file<br>▶Self-replicating, by itself<br>▶Looks benign, but is not<br>▶Conceal security breach<br>▶Record keystrokes<br>▶Shut down a resource | ▶Via Smartphone<br>▶Via Smartphone<br>▶Yes done<br>▶Probably, later<br>▶Unlikely<br>▶Works on ECUs |

- **UCSD & U of WA published 2 papers on the results of hacking MY 2009 car ECUs**
- **Methods marked in red used with physical access (able to compromise all ECUs)**
- **Methods marked in green used for remote access (able to compromise all ECUs)**

© 2015 IHS

**SOURCE: IHS Automotive**
***Software Apps & Service Portal***

# Cyber-Security in the Connected Car Age

- What is the problem?
- What are the risks & negative impact?
- What can be learned from other industries?
- What are the big-picture solutions?
- Are there automotive solutions?
- Summary & take-away

**Egil Juliussen, Ph.D. Director Research & Principal Analyst**

© 2015 IHS

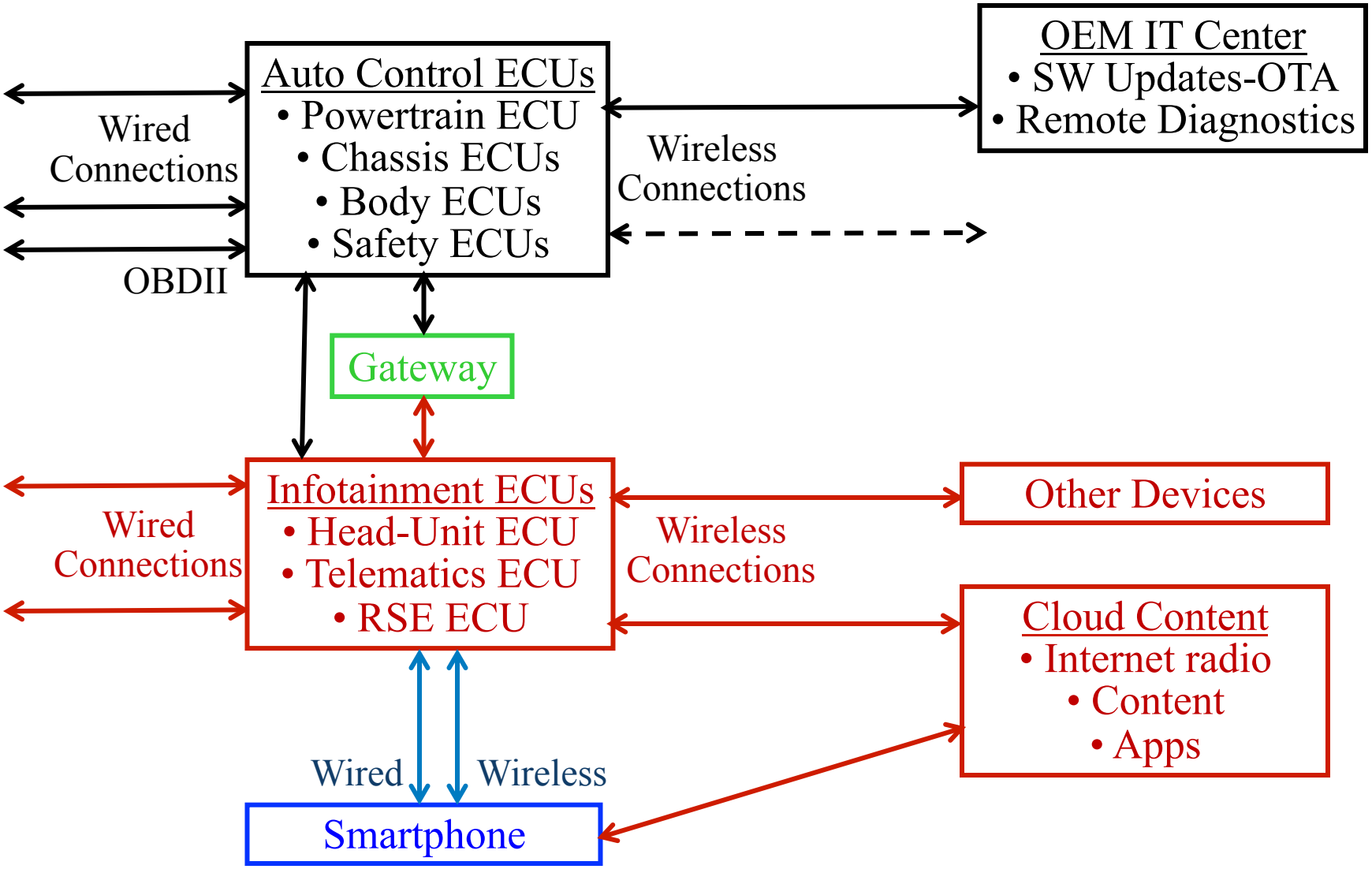
# Cyber-Security Solution Overview

| | Key Information |
|---|---|
| Iterative Process | ▸Cyber-security is an iterative process over the life-time of the system, sub-system, device, software and hardware |
| Best Practice | ▸Cyber-security is a life-cycle process that includes assessment, design, implementation and operations<br>▸It also includes an effective testing and certification program |
| Assessment Phase | ▸Establish security policy & System security evaluation<br>▸Iterative risk assessment (most important element) |
| Design Phase | ▸System prioritization & Security architecture |
| Implementation Phase | ▸Security architecture implementation<br>▸Security testing and evaluation |
| Operational Phase | ▸Awareness and security training<br>▸Intrusion detection and response (most important) |
| Strategy | ▸Best defense is to make security attacks unprofitable<br>▸Assume successful attacks and focus on detection & mitigation<br>▸Build software security on top of hardware security modules |

**Note: Most information from NHTSA Cyber-security Report**

© 2015 IHS

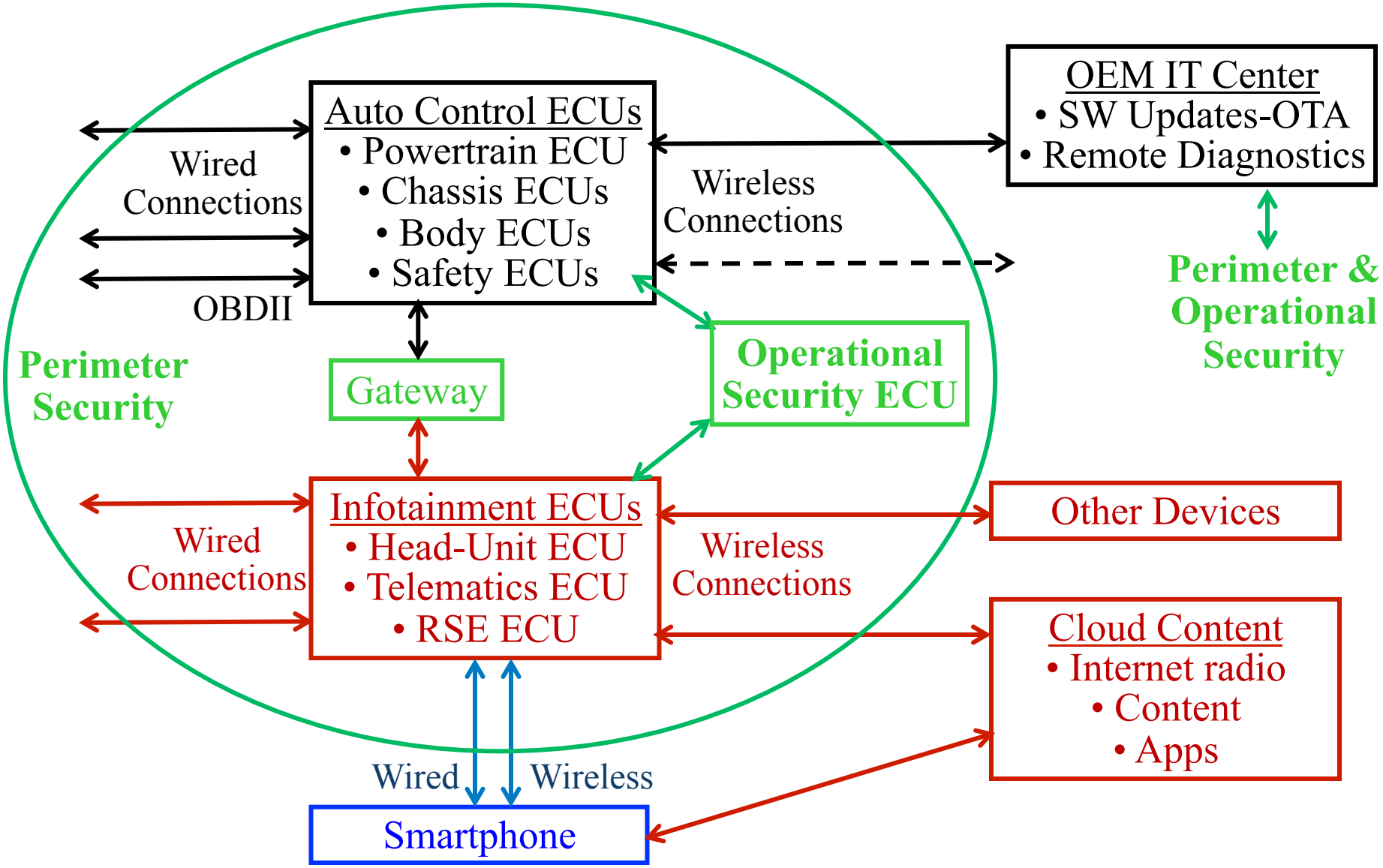
# Connected Car Overview




© 2015 IHS

SOURCE: IHS Automotive
*Software Apps & Service Portal*

# Big Picture Cyber-Security Solution




© 2015 IHS

SOURCE: IHS Automotive
*Software Apps & Service Portal*

# Auto Cyber-Security Solution

| | Key Information |
|---|---|
| Perimeter Security | ▸To detect and prevent unauthorized access<br>▸Via wireless, wired and other access points (i.e. media) |
| Perimeter Security Components | ▸Built-in microcomputer hardware security functionality<br>▸OS software security that leverage hardware security<br>▸Middleware security that leverage HW & OS security<br>▸Apps security that leverage HW & OS SW security<br>▸Every ECU will need these layers of security to check that any in-coming content is free of malware |
| Operational Security | ▸Perimeter security will not be 100% successful<br>▸Operational security is required to detect and prevent damage from malware that got through perimeter security |
| OEM IT Center | ▸Will need the best Perimeter & Operational security<br>▸OEM IT Center has the most valuable information! |

© 2015 IHS

**SOURCE: IHS Automotive**
***Software Apps & Service Portal***

# Cyber-Security in the Connected Car Age

- What is the problem?
- What are the risks & negative impact?
- What can be learned from other industries?
- What are the big-picture solutions?
- Are there automotive solutions?
- Summary & take-away

**Egil Juliussen, Ph.D. Director Research & Principal Analyst**

© 2015 IHS

# Auto Security Products & Solutions

| | Security Function | Company/Product |
|---|---|---|
| Cyber-Security Services | ▶Security risk assessment<br>▶Penetration testing<br>▶Vulnerability assessment | ▶Cisco OpSec<br>▶IOActive<br>▶Many others |
| Hardware Security | ▶Cryptographic processing<br>▶Secure microprocessor | ▶Freescale microcomputers<br>▶TI and others |
| Hypervisor Software | ▶Protect at software boot-up<br>▶OS & software isolation | ▶OpenSynergy, Mentor Graphics<br>▶Green Hills & others |
| Over-the-air SW Update | ▶Remote software update with built-in security | ▶Arynga<br>▶Redbend |
| Apps Security Framework | ▶Security framework for connected car apps | ▶Secunet Application Control Unit<br>▶Others expected |

© 2015 IHS

**SOURCE: IHS Automotive**
***Software Apps & Service Portal***

# Auto Security Products & Solutions

| | Security Function | Company/Product |
|---|---|---|
| CAN Bus Firewall | ▸Integrated CAN bus firewall<br>▸Add-on CAN bus firewall<br>▸CAN bus bridge firewall | ▸Arilou Technologies<br>▸Visual Threat OBDShield<br>▸Others likely in future |
| ECU Security | ▸ECU software monitoring<br>▸Can be embedded in ECUs | ▸TowerSec: ECUShield & TCUShield<br>▸Others expected in future |
| Operation Security | ▸Deep Packet Inspection for ECU intrusion detection | ▸Argus Cyber Security IPS<br>▸Other expected |
| Analysis Tools | ▸Framework for analysis and detection of CAN anomalies | ▸SWRI autoTREAD software<br>▸Reverse engineering: CAN signals |
| Backend IT | ▸Life cycle protection of flash software (cryptography-based) | ▸Secunet Advanced Backend Security (ABSec) |

© 2015 IHS

**SOURCE: IHS Automotive**
***Software Apps & Service Portal***

# Cyber-Security in the Connected Car Age

- What is the problem?
- What are the risks & negative impact?
- What can be learned from other industries?
- What are the big-picture solutions?
- Are there automotive solutions?
- Summary & take-away

**Egil Juliussen, Ph.D. Director Research & Principal Analyst**

© 2015 IHS

# What Should Auto Industry Do?

| | Key Information | Comments |
|---|---|---|
| Check current systems | ▸Check current connected car systems for security flaws | ▸To find, correct and update any security issues |
| Weakness Identification | ▸Offer rewards for finding auto security weaknesses | ▸Done by Google and other high-tech companies |
| Security Incident Response Center | ▸Auto industry organization to share security incident info | ▸Share security incidents info and attack methods |
| Continued R&D on auto security | ▸Continued NHTSA effort<br>▸Continued SAE effort | ▸Leverage high-tech R&D<br>▸Many security start-ups |
| Best Practice Guidelines | ▸Develop security guidelines<br>▸Deployment needed now | ▸NHTSA October 2014*<br>▸In progress from SAE |
| Security Standards | ▸Standards: NHTSA, SAE, etc.<br>▸Rapid deployment needed | ▸Leverage existing standards from aerospace and others |
| Testing & Certification | ▸Develop testing and certification standards | ▸SAE and/or NHTSA<br>▸Or others |

***DOT HS 812 075 (Multiple industries)**

© 2015 IHS

**SOURCE: IHS Automotive**
***Software Apps & Service Portal***

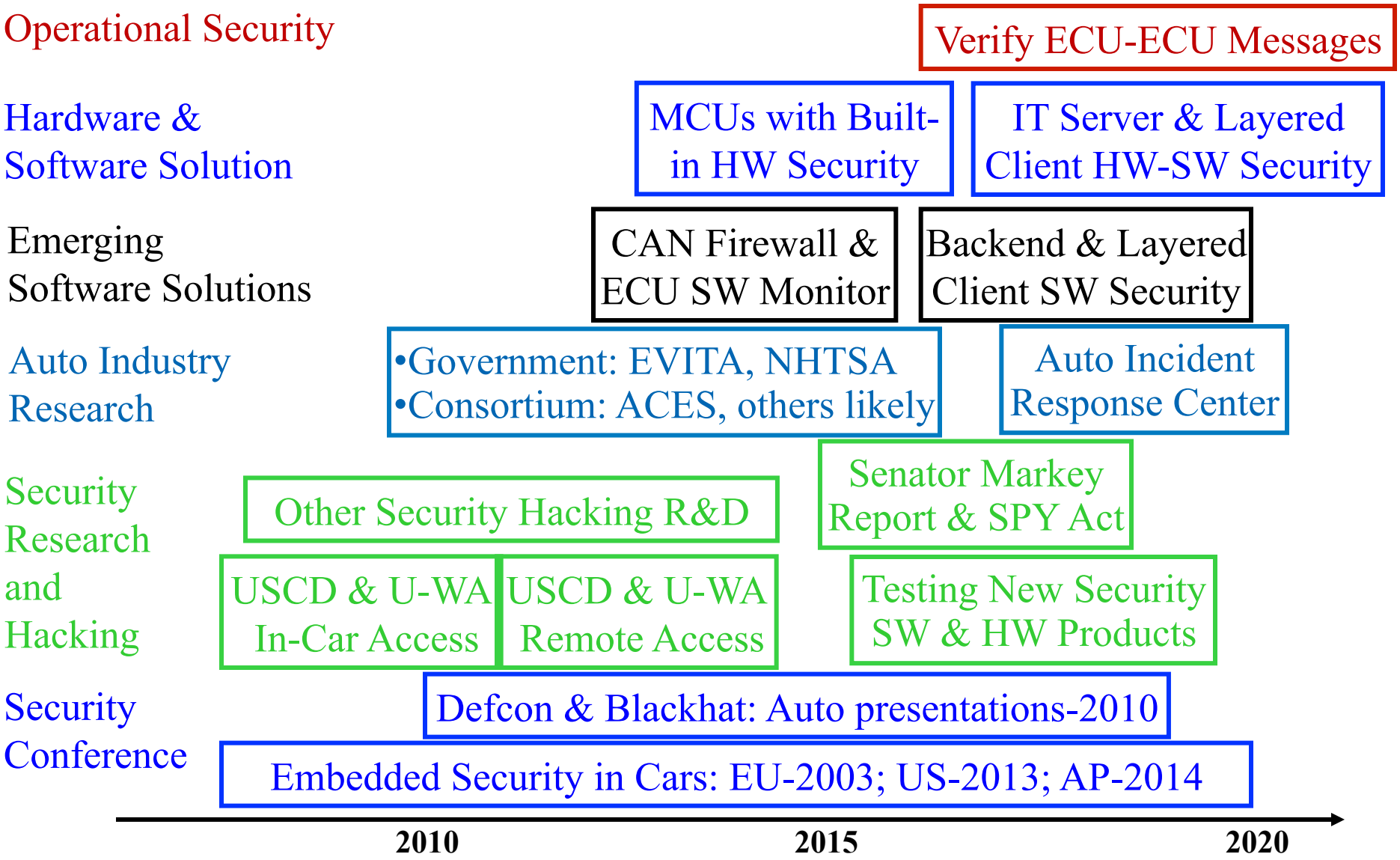
# Auto Security Requirements

| Requirements | Key Information |
|---|---|
| Hardware Integrity | ▸Hardware-based security is required<br>▸Tamper-proof: Prevention and detection |
| Software Integrity | ▸Unauthorized access must be detectable<br>▸Unauthorized alteration must not be feasible |
| Data Integrity | ▸Unauthorized access must be detectable<br>▸Unauthorized alteration must not be feasible |
| Communication Integrity | ▸Unauthorized modification from outside vehicle must be detected by receiver<br>▸Unauthorized in-vehicle communication must not be feasible and detectable |
| Access Control Integrity | ▸Authorized access must be well defined<br>▸Unauthorized access must be detectable<br>▸Development diagnostic access must be removed |
| Operational Security | ▸Monitor ECU-to ECU messages for suspicious events<br>▸Database of normal & hacked messages & events |

© 2015 IHS

**SOURCE: IHS Automotive**
***Software Apps & Service Portal***

# Auto Cyber Security Evolution




© 2015 IHS

**SOURCE: IHS Automotive**
***Software Apps & Service Portal***

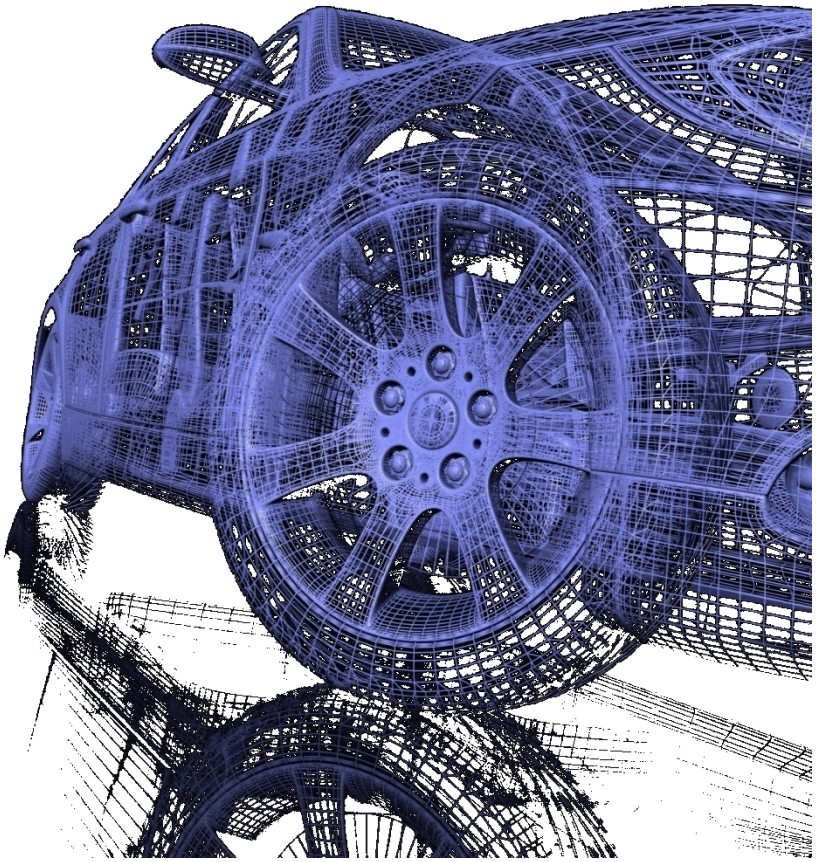
# Auto Cyber-Security Takeaway

| Good News | Bad News |
|---|---|
| ▶Successful auto hacking requires lots of time and expertise | ▶Good hacking tools & expertise expected in 3-5 years |
| ▶Business models for making money on car hacking is limited today | ▶Better hacking business models are likely (financial, ransomeware) |
| ▶Auto industry is investing in cyber-security solutions | ▶Deployment is lagging and may take a decade to catch up |
| ▶Remote software update emerging for quicker fix of security flaws (OTA) | ▶Cyber-security breaches could have many & high expenses |
| ▶Cyber-security big picture is simple: Perimeter & Operational security | ▶Cyber-security implementation details are extremely difficult |
| | ▶Security will require constant advances and is never done |
| | ▶Cyber-security is a new skill set and is a limited resource |

© 2015 IHS

**SOURCE: IHS Automotive**
***Software Apps & Service Portal***

# Questions?



Egil Juliussen, Ph.D. Research Director, Principal Analyst,
IHS Automotive Technology
October 21, 2015
egil.juliussen@ihs.com

© 2015 IHS