DORSEY always ahead

accenture High performance. Delivered.

Reducing Risk in the Internet of Things

Michael Rossman, Managing Director, Accenture

Chip Magid, Co-Chair, Products Liability Practice Group, Dorsey & Whitney LLP

1

The Internet of Things

- Public Sector: "smart cities," security, traffic control, lighting control
- Automotive: driving behavior monitoring, new consumer services, automated vehicle control for safety and efficiency
- Manufacturing: smart sensors and automated, interconnected industrial control systems (ICS) and SCADA systems
- Healthcare: remote monitoring of patients/equipment, remote control of medical devices, exchange of medical information

The Internet of Things

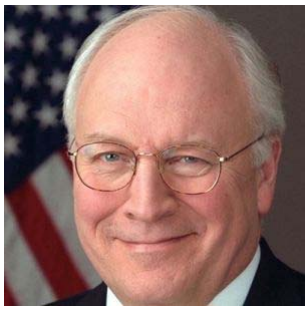
- **Aviation: Remote access to aircraft systems for operational monitoring, maintenance and support**
- **Utilities: Smart Grid, Smart Meters (AMI), Utility of the Future, ICS automation and interconnectivity throughout power generation/transmission/ distribution systems**
- **Smart Homes: consumer appliances, entertainment systems, Home Area Network (HAN) and WiFi connectivity of IoT components**

Image omitted

Scene from the Aurora Generator Test video released by the Department of Homeland Security, depicting an early test and demonstration of how an attack in cyberspace can destroy a critical infrastructure asset in physical space. (March 4, 2007)

Internet of Things (IoT). "Smart" devices incorporated into the electric grid, vehicles—including autonomous vehicles—and household appliances are improving efficiency, energy conservation, and convenience. However, security industry analysts have demonstrated that many of these new systems can threaten data privacy, data integrity, or continuity of services. In the future, intelligence services might use the IoT for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials.

James R. Clapper, Director of National Intelligence, Statement to the Senate Select Committee on Intelligence, 'Worldwide Threat Assessment of the US Intelligence Community,' February 9, 2016



Dick Cheney, as a work of the Federal Government this image is in the public domain.

Image omitted

Hospira Symbiq Infusion Pump subject to FDA safety communication.

Postmarket Management of Cybersecurity in Medical Devices

Draft Guidance for Industry and Food and Drug Administration Staff

DRAFT GUIDANCE

Image omitted

Samsung advertisement for SmartTV.

Image omitted

Scene illustrating the hacking of a Jeep Cherokee from "*Hackers Remotely Kill a Jeep on the Highway—With Me In It*," Andy Greenberg, WIRED (July 21, 2015).

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

This PSA is a joint product by the Federal Bureau of Investigation, the Department of Transportation and the National Highway Traffic Safety Administration.

March 17, 2016

Alert Number
I-031716-PSA

MOTOR VEHICLES INCREASINGLY VULNERABLE TO REMOTE EXPLOITS

As previously reported by the media in and after July 2015, security researchers evaluating automotive cybersecurity were able to demonstrate

Other Hacked Devices

- **Nest thermostats**
- **Internet-connected Hello Barbie doll**

Federal Trade Commission

- **Federal Trade Commission Act, 15 U.S.C. § 45(a) prohibits "unfair or deceptive acts or practices in or affecting commerce."**
- **Beginning in 2005, FTC has pursued administrative actions alleging that deficient cybersecurity was "unfair" under § 45(a).**
  - **TRENDnet (home monitoring cameras)**
  - **HTC America (mobile devices)**
  - **ASUSTeK Computer (routers)**
- ***FTC v. Wyndham Worldwide Corp*., 799 F.3d 236, 259 (3d Cir. 2015) ("fair notice" does not entitle a defendant "to know with ascertainable certainty the cybersecurity standards by which the FTC expected it to conform.")**

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS

BRIAN FLYNN; and GEORGE and KELLY BROWN on behalf of themselves and all others similarly situated,	)	
Plaintiffs,	)	Case No. 3:15-cv-855
v.	)	
FCA US LLC f/k/a CHRYSLER GROUP LLC and HARMON INTERNATIONAL INDUSTRIES, INC.	)	
Defendants.	)	

CLASS ACTION COMPLAINT

NOW COMES Plaintiffs Brian Flynn and George and Kelly Brown, on behalf of themselves and all others similarly situated, and for their Class Action Complaint pursuant to Rule 23 of the Federal Rules of Civil Procedure, allege as follows:

Legal Theories

- **Negligence**
  - Defective design
  - Failure to notify
  - Failure to remedy
- **Contract**
  - Breach of implied warranties
- **Invasion of Privacy**
- **Fraud**
- **Damages**
  - Direct damages
  - Consequential Damages
  - Loss of Value

Standing/Injury-in-Fact

- *Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138, 1143 (2013) ("respondents' theory of future injury is too speculative to satisfy the well-established requirement that threatened injury must be 'certainly impending.'")
- *U.S. Hotel and Resort Management, Inc. v. Onity, Inc.*, 2014 WL 3748639 (D.Minn. July 30,2014) ("the fact that a plaintiff incurs present costs to safeguard against the merely possible future injury does not amount to any present injury in fact.")
- *Cahen v. Toyota Motor Corp.*, 2015 WL 7566806 (N.D.Cal. Nov. 25, 2015) ("plaintiffs fail to establish economic injury in fact because they have not alleged the required 'something more' beyond the speculative risk of future harm that underlies the allegations of economic damage.")

Questions Yet to Be Answered

- **Interplay Between Tort Law and Software Licenses**
- **Cyber Insurance Coverage and IoT**

Image omitted.

Image of Uconnect Terms of Service.

Uconnect Terms of Service

Mandatory Arbitration. AS SET FORTH FULLY IN THE TS&CS, YOU, FCA US, AND SPRINT AGREE TO A MANDATORY ARBITRATION PROVISION THAT PROVIDES THAT (EXCEPT FOR MATTERS PROPERLY BROUGHT TO SMALL CLAIMS COURT) ANY CLAIM, CONTROVERSY, OR DISPUTE IN ANY WAY RELATED TO OR CONCERNING THE UCONNECT SERVICES MUST BE RESOLVED BY FINAL AND BINDING ARBITRATION ON AN INDIVIDUAL AND NOT A CLASS-WIDE, REPRESENTATIVE, OR CONSOLIDATED BASIS. WITH RESPECT TO SUCH CLAIMS, YOU, SPRINT, AND FCA US WAIVE THE RIGHT TO A TRIAL BY JURY AND THE ABILITY TO BRING OR PARTICIPATE IN CLASS OR REPRESENTATIVE ACTIONS IN COURT OR ARBITRATION.

Best Practices for IoT Cyber Security

Cyber Security is Mandatory

- **Producers of IoT products, systems and related services must deliver highest level of confidence and assurance of security to consumers – Confidentiality, Integrity, Availability:**
  - **Personal information is protected**
  - **Secure from compromise, misuse, corruption**
  - **Secure from operational disruption**
  - **Prevention of unauthorized access and enabling compromise of other interconnected systems**

Overarching Cyber Security Concepts

- Address security at IoT at component level as well as end-to-end system and ecosystem
- Assume multiple, sophisticated adversaries (APT)
  - Adversaries will compromise monitoring, command & control, safety, backup components and systems
  - Understand potential adversaries, motives, capabilities
- Integrate security into design, integration, operations
- Engineering reliability does not assure cyber security in of itself
- Compliance ≠ Security

IoT Design & Integration Cyber Security Considerations

- Security by design
  - Integrate security expertise and process into design teams
    - Application & firmware security
    - Hardware component security
    - Interface security…
- Threat modeling: attack vectors, impact
- Assume each system component may be compromised
  - Build systems assuming minimal trust between components
  - Authentication between components
  - Resilience to withstand component compromise

IoT Design & Integration Cyber Security Considerations

- Ensure integrity of command & control, monitoring communications – encryption based
- Encryption of data in transit and data at rest
- Built in anomalous event alerting, logging and auditability
- Penetration testing, independent security assessment of components and systems, with interconnections, prior to release
- Built in security patch/updating capability

IoT Manufacturing Cyber Security Considerations

- Manage cyber security in the supply chain, throughout the procurement and production lifecycle
  - Vendors & suppliers
  - Service providers
- Cyber security oversight for business partners
- Testing of components in supply chain and at key manufacturing steps

IoT Services & Operations
Cyber Security Program Framework

- **Establish an enterprise cyber security program to ensure the integrity of IoT service delivery and operational support**

Cyber Security Program Framework
a) Cyber Security (IS) Program Governance
b) IS Risk Management – (Enterprise, Operational, Business Project, Technology Platform & Services Acquisition, 3rd Party Oversight..)
c) IS Compliance Management
d) IS Awareness Program
e) Security Configuration Standards Compliance
f) Vulnerability & Patch Management
g) Identity & Access Management
h) Application Security
i) Information Security Architecture
j) IS Engineering & Operations
k) Threat Intelligence Management
l) Cyber Security Monitoring / Threat Detection
m) Incident Response
n) Incident Recovery

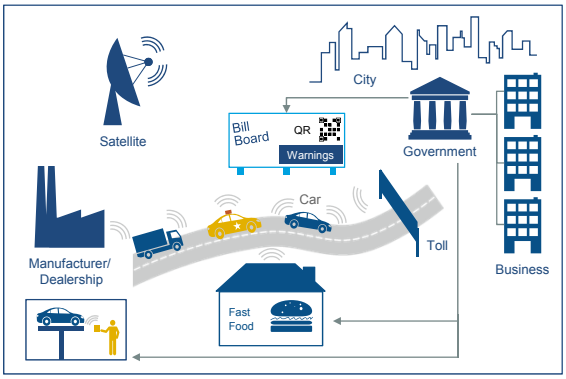
Example Key Enterprise Functions Complementary to Cyber Security
q) IT- Technology Portfolio Management
r) IT - Technology Asset Management, Technology Refresh
t) Regulatory Compliance Management – Controls Definition, Assurance, Testing
u) Enterprise Risk Management – Corporate Risk Prioritization, Risk Appetite Rationalization
w) Supply Chain – Procurement Cycle Management, In-production Service Provider Oversight
y) HR – Individual Goal/Objective Setting, Measurement, Evaluation

Case Study :
Securing the Connected Car

Components & Considerations

The Connected Vehicle Ecosystem

With enhancements to computing power, sensors, and communications the modern day vehicle is now equipped to deliver interactive services, improved maintenance, and automated functionality



Connect with what?
- Other vehicles (V2V)
- Traffic/municipal services (V2I)
- Manufacturer (maintenance)
- Entertainment services
- Navigation services
- Advertising/Retail

What will be shared or leveraged?
- Personal information (location, preferences, etc.)
- Diagnostics
- Entertainment
- Payment mechanisms

What this means to the manufacturer?
- The benefits to the manufacturer are vast (like diagnose vehicle faults and send software upgrades over the air to vehicles when safe to do so – e.g., when parked – to remedy the error, avoiding expensive recalls), but these benefits have to be tempered with the potential for misuse by an attacker.

DORSEY always ahead | accenture High performance. Delivered.

REDUCING RISK IN THE INTERNET OF THINGS (IoT)

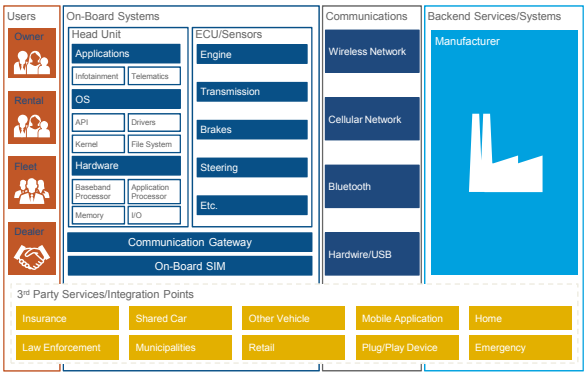
29

Components & Considerations

Connected Car Ecosystem Components and Security Considerations

The Connected Vehicle ecosystem includes the vehicle itself (and all its internal components, as part of the supply chain to the manufacturer), the manufacturer's backend services and 3rd party service providers.

This ecosystem today lacks of a holistic security approach, and presents different risks as threats are introduced into its lifecycle from different sources, including:
- Hardware parts and associated firmware are not being thoroughly inspected at key points in the supply chain, etc.
- Software for the vehicles being developed by 3rd parties that are not inspected.
- Wireless Connection Agreements between Carriers are not thoroughly assessed from a risk perspective.
- External aftersales components/add-ons/services not properly secured and tested together with the vehicle.



DORSEY always ahead | accenture High performance. Delivered.

REDUCING RISK IN THE INTERNET OF THINGS (IoT)

30

Connected Vehicle Vulnerabilities and Exploits

Bluetooth
Used to connect personal devices to Infotainment system to allow then to be controlled as an integrated part of the vehicle internal network of devices

Wi-Fi
Increasingly vehicles can connect to Wi-Fi Hotspots to enable internet services and remote connection to other Wi-Fi equipped devices

Cellular
Used to stream vehicle telematics to manufactures for quality monitoring and value add pay services. Also used for automated emergency assistance calls in event of accident

Cyber/Physical
Sensors used to derive environmental information such as proximity for adaptive cruise control, automated parking/ park assist, emergency obstacle avoidance, plus others for road sign and lane recognition

Internet Applications
Internet connectivity will enable users to download applications and data streams via connected smart phones, or directly via integrated sim or Wi-Fi- introducing the possibility of malware running on in car systems from third parties

OBD2 Port
Physical port for connecting diagnostic devices to vehicle can bus and controllers for fault diagnosis, monitoring and firmware upgrades. Increasingly, third party devices can be fitted to read and display CAN bus information to driver.

V2V
Wireless mesh network enabling vehicle to vehicle communication for long range hazard alert. Although v2v range is only 300m, vehicles will relay information to each other – so a message with 4 vehicles hops will give warning of hazards 1.2km distant

TPS
Tyre Pressure Monitoring System – Short range radio communications to tyre pressure monitor in each wheel. Gives early indication of pressure loss to avoid blow outs.

Keyless Entry
Low power radio interface for unlocking car doors without the need take the key out of pocket. Activated by the key holder pulling a door handle, a radio interrogation request is sent to the key. If the correct key is within range, it will respond with the correct id code, and the door will unlock

Passive Anti Theft
Similar to keyless Entry – when the start button is pressed, or ignition key turned, a low powered radio request will be sent. The car key must respond with the correct coded response for eth engine to start

31

DORSEY always ahead | accenture High performance. Delivered.

REDUCING RISK IN THE INTERNET OF THINGS (IoT)

Components & Considerations

Challenges to be addressed to get on the right track

There are many potential vulnerabilities within the connected vehicle spanning entertainment, environmental and internal components

CAN Bus
Tampering or spoofing communications between nodes within the vehicle via the CAN bus.

Local Applications/ Interfaces
Downloadable 3rd party applications and software (malicious).

Sensors
Communicating and generating false data to core system sensors within the vehicle.

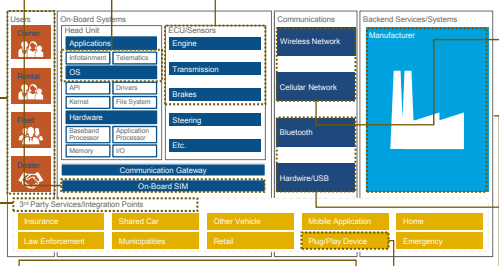
Poor End User Knowledge
Most of today's devices come with a default username and password (some still don't) – end users fail to change these default configurations.

Unsecure communications
Lack of encryption in communication between vehicle and backend/3rd party services.

Backend Services and Systems
Unprotected access of user information/system accounts for 3rd systems or services.

External Connected Devices
Exploit applications local to connected device (via Bluetooth or USB) to obtain access to vehicle systems.

Aftersales Market
Must ensure provenance of aftersales components to prevent insecure devices being fitted to the vehicle.



DORSEY always ahead | accenture High performance. Delivered.

REDUCING RISK IN THE INTERNET OF THINGS (IoT)

32

Components & Considerations

Connected Vehicle Hacks: Means and Potential Consequences

Attack surfaces

Wireless connections

Wi-Fi | Bluetooth | Cellular | RFID

Accessible components

Up to 80 ECUs controlling:

- Brakes
- Throttle
- Navigation
- Steering
- Suspension
- Lights
- Door locks
- Mirrors
- Horn
- Sensors
- Can Bus
- Data stores

Potential Consequences

Consumers

- Human casualties
- Financial Impacts
  - Fees
  - vehicle damage
  - Stolen credentials
- Privacy violation
  - Stolen accounts

Manufacturers

- Costly fleet recalls
- Expensive law suits
- Image damage that translates in lower brand loyalty and shares price drop.

3rd party service providers

- Law suits caused by
  - Service malfunction
  - Data misuse
- Brand damage
- Consumer reluctance
- Loss of business partners

33

DORSEY always ahead | accenture High performance. Delivered.

REDUCING RISK IN THE INTERNET OF THINGS (IoT)

What can manufacturers and services providers do to achieve increased connected vehicle security?

Manufacturers and service providers must ensure security is addressed to avoid releasing insecure products that put consumers at risk

- Ensure security is a consideration throughout the product lifecycle: implement security early during product development, so that security is automatically embedded.
- Assume that multiple adversaries exist, so understanding of the threats and continuous monitoring will be necessary.
- Adopt an offensive mindset and assume that each component in the system may be compromised at some point by an attacker. Every component should place a minimal level of trust in every other component.
- Apply Industrial Control Systems (ICS) security lessons learned. Ensure secure connectivity and access controls between OT and IT systems.
- Apply mobile security lessons learned. The physical device itself is only part of the battle – backend systems and services can prove to be an additional threat vector, so security also needs to be addressed on backend systems and service provider side.
- In addition to testing individual components (mobile app, infotainment, TCU, ECU, etc.), perform pen testing before goes out of the factory, i.e. attack simulations against the ecosystem as a whole (prototype vehicle with all connected systems functioning).
- Adopt Privacy by Design (PbD) principles. Privacy has to be addressed and include up front within the design of the service function. Access and authorization rights to data can be established as data is collected, and then these rights are collocated with the data as it is moved and stored.
- Be aware of emerging standards from organizations like RITA, SAE, ISO, etc. and even consider joining standards bodies and groups to better align business objectives and security.
- Continue to educate users and raise security awareness with an open communication regarding new and malicious attacks that are propagating.

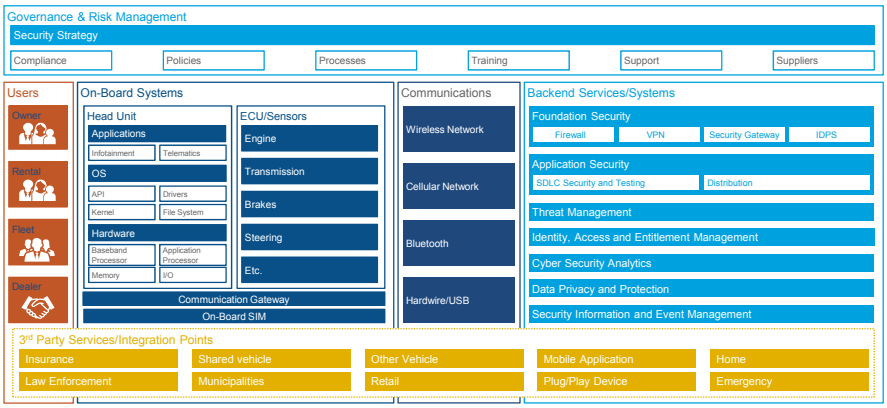
DORSEY always ahead | accenture High performance. Delivered.

REDUCING RISK IN THE INTERNET OF THINGS (IoT)

34

Define a security strategy and architecture for the entire connected vehicle ecosystem

A security strategy for the entire connected vehicle ecosystem and corresponding security controls must be in place, including backend services/systems



DORSEY always ahead

accenture High performance. Delivered.

REDUCING RISK IN THE INTERNET OF THINGS (IoT)

35

DORSEY always ahead

accenture High performance. Delivered.

Creighton Magid
Dorsey & Whitney LLP
1801 K Street, NW
Suite 750
Washington, DC 20006
(202) 442-3555
magid.chip@dorsey.com

Michael Rossman
Accenture
800 Glebe Road
Arlington, VA 22203
(443) 467-5060
michael.rossman@accenture.com

36