Hi All,

Please find attached the Weekly Automotive Industry Report covering April 3 - April 8.

This week's report includes articles on:

- Toyota partnering with Microsoft on a new cloud-based division led by the CIO,
- Intel acquiring a semiconductor manufacturer that builds chips for self-driving cars,
- Hyundai unveiling its connected vehicle "roadmap," and,
- Toyota planning to open a new autonomous vehicle research center in Michigan.

You can find past reports on site.

Please let me know if you have any questions. Have a great weekend.

---

Connecting the Community -
Auto-ISAC's Role in the Automotive Industry

*SANS Summit – Chicago, IL*

Faye Francy
Executive Director
May 8, 2018
The Emerging Cybersecurity Challenge
Significant Changes in the Automotive World

Digital Connected Vehicles provide operational efficiencies and risks...

➢ Digital Age
  ✓ Connectivity, automation brings efficiencies
  ✓ Interconnectedness increases cyber risk
  ✓ News, media, congressional oversight, regulatory demands action

➢ Connected Vehicles Integrated across Systems (SoS)
  ✓ Connectivity provides greater efficiencies & risk
  ✓ Cyber threats and vulnerabilities growing
  ✓ Best Practices are an imperative, standards
  ✓ And autonomy, V2V, V2I coming…. 
With connectivity comes cyber risk

Yesterday

- On-vehicle software and electronics

Limiting Vulnerability

- Physical connection to vehicle required

Today

- Convenience & Entertainment
  - Connected services
  - Partial automation
  - On-vehicle Wi-Fi

As connected features grow, cyber risks multiply

Yesterday

- Known vulnerabilities
  - Proven remote attack capability

Demonstrated Threat

Tomorrow

- Safety, Convenience, & Entertainment
  - IoT integration
  - On-vehicle commerce
  - V2V, V2I, V2X
  - Full automation

Industry-Wide Risk

- Expansive, complex attack surface
- Motivated, capable adversary
- Potential impact to safety, privacy, and quality

Cybersecurity Challenge
Evolution of the Cyber Threat

**Early Hacks (2010~2014)**

- **March, 2010:** Fired auto dealer employee disabled 100 vehicles via Remote Immobilization System
- **May, 2010:** UCSD and UW researchers hacked into unnamed mid-price sedan
- **January, 2012:** Start the CyberAuto Challenge
- **July, 2012:** Anonymous video showed keyless BMW hacked
- **August, 2013:** Scientists found a way to steal vehicle key authentication, Volkswagen blocked research publication
- **November 2014:** Researchers hacked a car with Zubie device

**Recent Hacks (2015-2017)**

- **February 2015:** Researchers demonstrated hacking a Tesla Model S and planting a remote-access Trojan
- **February 2015:** DARPA’s Dan Kaufman demonstrates vehicle hacking to CBS
- **February 2016:** Researcher discloses Nissan Leaf vulnerability
- **February 2017:** Kaspersky Labs discloses connected vehicle mobile app vulnerabilities
- **February 2017:** Researchers demonstrated remotely hacking a Chevrolet Corvette
- **May 2017:** Ransomware reportedly shuts down 2 OEMs’ mfg. operations
- **July 2015:** Researchers remotely hack a Jeep Cherokee while being driven on a highway
- **August, 2015:** Researchers remotely hacked GM’s OnStar Remote Link system to control vehicle
- **August, 2015:** Researchers demonstrated hacking a Tesla Model S and planting a remote-access Trojan
- **August, 2015:** Researchers hacked GM’s OnStar Remote Link system to control vehicle
- **August, 2015:** Researchers demonstrated remotely hacking a Chevrolet Corvette
- **August, 2015:** Researchers demonstrated hacking a Tesla Model S and planting a remote-access Trojan
- **August, 2017:** Researchers demonstrated remotely hacking a Tesla Model S and planting a remote-access Trojan
- **August, 2015:** 14 OEMs Incorporated Auto-ISAC
Today’s trending threats

What are we seeing in the wild today?

Vulnerabilities

Mobile Apps
- Mobile apps used to control car features are proliferating and may expose user data or vehicle functions if not properly secured

OBDII Dongles
- Although the OBDII port requires proximity to exploit, it provides access to the relatively insecure, safety critical CAN Bus.

Bluetooth Privacy
- Vehicle infotainment systems allowing access to data stored in vehicle

Real-World Exploits

Car Theft
- Key fob hacks (e.g. replay attacks) allow attackers to unlock cars using commercially available devices
- Attackers reportedly stole PII from an OEM’s IT system and used it to locate, unlock, and steal targeted vehicles

✓ Service Disruption
✓ PII/Payment Info Theft
✓ Physical Destruction
✓ Remote Control
✓ Manufacturing Disruption

Nation State
Criminal
Hacktivist

Vehicle Cyber Attack
Auto-ISAC Overview
Why an ISAC?

Information Sharing and Analysis Center (ISAC)

Organizations must act individually to manage cyber risk...

- Protect
- Detect
- Respond
- Internal Investment

...one company’s detection is another company’s prevention

- Identify emerging threats and vulnerabilities earlier
- Pool limited resources to better fight your adaptive adversary
- Share incident intelligence to act more quickly
- Proactively shape industry-wide best practices
- Protect overall trust in innovation across the industry
- Build resiliency across industry
- Connecting the community
Auto-ISAC Mission - Scope

Mission
Serve as an unbiased information broker to provide a central point of coordination and communication for the global automotive industry through the analysis and sharing of trusted and timely cyber threat information.

Scope
Light- and heavy-duty vehicles, commercial vehicle fleets and carriers. Currently, we are focused on product cyber security, and anticipate expanding into manufacturing and IT cyber related to the vehicle.

What We Do

Intel Sharing
Data curation across intel feeds, submissions and research

Analysis
Validation, context and recommendations

Best Practices
Development, dissemination and maintenance

Partnerships
Industry, academia, vendors, researchers and government

Community Development
Workshops, exercises, all hands, summits and town halls
A Framework for Cybersecurity

- Establish common cybersecurity best practices for automotive
- Establish a cybersecurity culture
- Understand the threat
- Understand the risk
- Communicate the threats and assure situational awareness
- Provide incident response
- Strengthen the defensive system
- Define design principles
- Define operational principles
- Conduct necessary research and development
- Ensure that private sector, government and partners work together

Resiliency Across the Global Automotive Industry
The Value of Engagement

Find and fix issues faster
Time is money, especially in cyber. Members receive verified, timely cyber threat, vulnerability, and remediation information.

Stay ahead of regulation – develop a unified voice
Uniting on the cyber challenge, and maintaining clear channels with global government bodies, helps inform and shape legislation.

Maintain a trusted brand
Customers demand safety and privacy. OEMs demand secure components from suppliers. Joining the ISAC demonstrates a commitment to protecting vehicles, services and, ultimately, drivers.

Enhance capabilities
Our community is a trusted forum to share insights and learn from one another. Formal activities —like exercises and workshops—and informal relationship-building cultivate this trust.

Education and Awareness
Collaboration and Cooperation Across the Ecosystem
Auto-ISAC Benefits

- Focused Intelligence Information/Briefings
- Cybersecurity Intelligence Sharing
- Vulnerability Resolution
- Member to Member Sharing / Partner- Community Sharing
- Distribute Information Gathering Costs Across the Sector
- Non-attribution and Anonymity of Submissions
- Information Source For the Entire Organization
- Risk Mitigation For Automotive Industry
- Comparative Advantage in Risk Mitigation
- Security and Resiliency

Building Security Across the Auto Industry
How we operate

Board of Directors
OEM Members* and Affiliate Advisory Board Chairman and Vice Chairman

Executive Committee
Chairman  Vice Chairman  Treasurer  Secretary  AAB Chairman

Standing Committees
Membership & Benefits  Information Sharing  Finance & Audit

Task Forces & Working Groups
Best Practices  Nominating  Analyst Community  Summit

Affiliate Advisory Board (AAB)
Gold and Platinum non-OEM Members

Supplier Affinity Group

Commercial Vehicle Affinity Group

Governance

Executive Director
Program Ops Manager  Support Staff  Third Party Services (e.g. legal)

Operations Team

*OEMs with >100M in global annual revenue.
**Spotlight: Intel Sharing & Analysis**

**Contributors**
- OEMs
- Suppliers
- Vendors
- Academia & Research
- Government
- Other ISACs

**Intelligence**
- Types of Information
  - Vulnerabilities
  - Threat feeds
  - Research
  - Best practices
  - Intelligence
  - Trends
  - Forecasts
  - Data feeds

**Auto-ISAC Analysis**
- Validation
- Analysis
- Impact assessment
- Pattern identification

**Auto-ISAC Portal**
- Intel reports
- Trend analysis & dashboards
- Wiki pages

**Results**
- Efficiently identify threats by supplementing internal intelligence with external sources
- Detect vulnerabilities faster with cross-industry vulnerability information sharing
- Validate risk analysis with reliable industry-level findings and best practices

**Key Takeaway:** A diversity of information sources is what drives value of our intel sharing and analysis capabilities.
Spotlight: Best Practices

Our Objective

Demonstrate the industry’s proactive collaboration to protect consumer safety through vehicle cyber security

Our Method

Define best practices for securing the vehicle ecosystem, and provide guidance to implement them

Our Outputs

Executive Summary

High-level document defining Key Cyber Functions and Best Practices. Currently available on our website.

Best Practice Guides

- Incident Response
- Collaboration & Engagement
- Governance
- Risk Management
- Training & Awareness (in work)
- Threat Detection & Protection
- Security by Design

Members Contribute to Each Guide

Public Release after Time Period via our Website.
Community Engagement
Strategic Partnership Program

Not eligible for membership?

Individuals / organizations may participate on monthly Community Calls and contribute to Auto-ISAC

Solutions Providers
- For-profit companies that sell connected vehicle cybersecurity products & services.
- Examples: Hacker ONE, SANS, IOActive

Associations
- Industry associations and others who want to support and invest in the Auto-ISAC activities.
- Examples: Auto Alliance, Global Auto, ATA

Affiliations
- Government, academia, research, non-profit orgs with complementary missions to Auto-ISAC.
- Examples: NCI, A-ISAC, DHS, NHTSA

Community
- Companies interested in engaging the automotive ecosystem and supporting - educating the community.
  - Examples: Summit sponsorship – key events

INNOVATOR
- Paid Partnership
  - Annual investment and agreement
  - Specific commitment to engage with ISAC
  - In-kind contributions allowed

NAVIGATOR
- Support Partnership
  - Provides guidance and support
  - Annual definition of activity commitments and expected outcomes
  - Provides guidance on key topics / activities

COLLABORATOR
- Coordination Partnership
  - “See something, say something”
  - May not require a formal agreement
  - Information exchanges - coordination activities

BENEFACCTOR
- Sponsorship Partnership
  - Participate in monthly community calls
  - Sponsor Summit
  - Network with Auto Community
  - Webinar / Events
Strategic Partnership Programs

Activities

Intel Sharing
Some partners submit relevant data, insights and papers addressing threats against the automotive industry.

Research
Some partners share white papers and research projects—on threats & vulnerabilities—with our members.

Webinars
We are open to partners presenting at our Community Town Halls, with audience including members & beyond.

Member Discounts
Some partners promote discounts or special offers for services (e.g. conferences, software licenses).

Other
We are open to other types of in-kind support (e.g. training, infrastructure support) based on your expertise.

Benefits

Access to Auto-ISAC Reports
Our partners receive Auto-ISAC TLP Green/White reports and special reports at Auto-ISAC’s discretion.

Branding on the Auto-ISAC Website
Partner names and/or logos will be featured on the Auto-ISAC public-facing website.

Community Town Halls
We invite you to monthly calls featuring experts across the connected vehicle ecosystem.

Annual Executive Call
Our executives will host a call once a year for all Members and partners to present our strategic goals and priorities.

Summit Booth Priority
Partners will receive priority booth selection at future Auto-ISAC Summits.
Auto-ISAC Actions – Identified and analyzed event trends across Members and Sectors, responded to RFIs (internal and external), coordinated information sharing between Members, aggregated data for rolling informational and situational reports.

Exercise Accomplishments:
- Test incidence response process
  - Event identification and analysis
  - Information gathering and sharing (internal and external)
  - Member communications coordination
  - External outreach on behalf of members
- Engagement with NHTSA/Partners

Lessons Learned/Corrective Actions:
- Familiarize NHTSA on ISAC capabilities and processes
- Formalize process for sharing data outside of ISAC (w/NCCIC, NCI)
- Need for increased Member sharing to support sector-wide impact assessment and decrease duplication of effort between Members
Strategic Navigation

Building a Roadmap to Protect Automotive Industry

- **Culture of Security**
  - Embedded Network Security Requirements
  - Training & Awareness / New Skills

- **Design-in Cyber Requirements**
  - Value Chain Visibility/Traceability
  - Lifecycle Cyber Management
  - Shift to Risk Management

- **Institutionalize Incident Responses**
  - Threat Response and Recovery
  - Public – Private Information Sharing and Analysis
  - Forensics Analysis Capabilities
How to get involved

If you see something...

Although Auto-ISAC is not a coordinated disclosure or bounty-based organization, anyone can submit information to Auto-ISAC. Visit our website to contact us: www.automotiveisac.com.

Join as a Member

If you are an OEM, supplier or commercial vehicle company, please contact Membership Engagement, Kim Kalinyak at kimkalinyak@automotiveisac.com.

Partner with us

Individuals, vendors, researchers, government, academia, and others working in the connected vehicle ecosystem, contact Kim Kalinyak at kimkalinyak@automotiveisac.com to learn about opportunities to engage.
Our contact info

Faye Francy
Executive Director
c/o Booz Allen Hamilton Inc.
20 M Street Southeast
Suite 1000
Washington, DC 20003
703-861-5417
fayefrancy@automotiveisac.com

http://www.AutomotiveISAC.com