

ITS AMERICA

ITS America Update on Cybersecurity, Technology and Regulatory Issues



September 8, 2015

Steven Bayless, Vice President – Technology and Markets
Intelligent Transportation Society of America (ITSA Safety Forum)





Connectivity Benefits (and Vulnerabilities)

“The Cloud,” Enterprise Systems, & Consumer Devices



iCar Jacking? – Embedded Systems



Highway Hacking?
Advanced Traffic Management Systems

*Cybercrime is a multi-billion dollar global business
Days of “security through obscurity”
may be over*



Future ITS Security Landscape

- With more vehicle/mobile device connectivity, security is of renewed interest
- There is a need to eliminate or minimize risk of unintended consequences
 - Concern voiced that automotive electronics and traffic control devices are vulnerable to attack through connected device “stepping stones”
 - Ensure that safety and mobility information is not used to compromise drivers privacy. (However, need to be realistic about threats and not scare monger)
 - Future Cooperative Crash Avoidance Systems – “Connected Vehicles” to trust each other – ensure only valid information is exchanged vehicle-to-vehicle
 - Reduce risk that liability concerns will have a chilling effect on deployment of crash avoidance by OEMs (or road operators)
 - ... or that privacy or security concerns will have chilling effect on consumer demand for crash avoidance and ITS

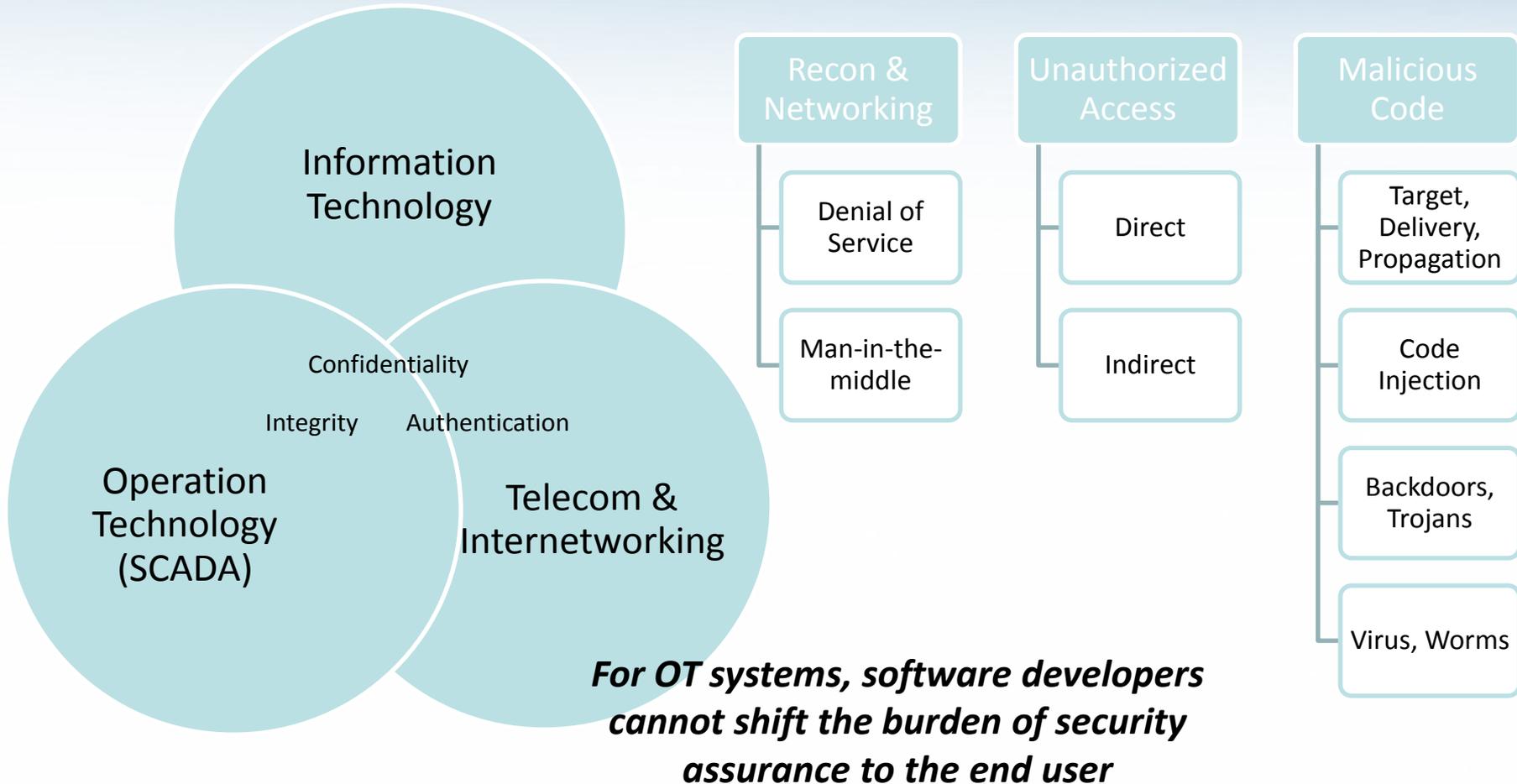


Risk Management Landscape

- Threat environment - black market that takes vulnerabilities and monetizes them
 - For example, in 2012 there were 8K vulnerabilities publicly disclosed in IT systems, 42% of which were exploited. Number is likely steady, despite improvements in SW designs
 - Zero Day exploits hoarded for high profile targeted attacks, but once publicly known, are integrated into attack toolkits and remarketed. Zero day lasts average of 10 months
 - Ten percent of vulnerabilities are responsible for 90% of all the exposure – most are entirely preventable, where patches are either not shipped, or not applied
- Ship Monday/Patch Tuesday – IT systems defer security to maintained phase of software development process, most often putting burden on end users to patch
- Hacker environment – in PC ecosystem evolves from individual attacks to mass exploitation (viruses, worms) to third party markets selling compromised hosts
- Hackers go for scale and path of least resistance -- Looking for systems that are widely used, and easy to hack



Types of Systems, Security Goals & Attack Vectors





Assessment of Security Vulnerabilities

- Security is not about the achievement of complete and unrealistic state of unassailability, but the mitigating important risks to a system at a reasonable cost (both in terms of costs and lost opportunities)
- Which risks are important and can be mitigated at a reasonable cost?
 - Most risks you must live with because outside of your control or integral to your business plan, but you can plan for and put up countermeasures
 - Common threats (unmaintained software, firewalls, weak encryption, weak authentication)
 - Some risks are structural cannot be proactively prevented (eg. Denial of service attack)
 - Some risks can only detected and mitigated after compromise (Zero-Day Attacks and Advanced Persistent Threats)
 - Structural problems obviously exist – Complexity, Liability, changing definitions of privacy etc..



Operational Technology

- IT to Control systems - Embedded Devices developed at a time when they were not connected – Environment has shifted around systems
 - Automotive and Highway Infrastructure systems are not that homogenous, often proprietary and arcane
 - but that is changing – See Miller/Valsek “Remote Exploitation of an Unaltered Passenger Vehicle”
- Regulations are shifting– new requirements, new interpretations by regulators and auditors, but may still be a gap between requirements and good security.
- Hackers attack, but auditors (and possibly regulators) reshape liability and economics
- Good security supports trust, commerce and privacy but sometimes engenders too much dependence on technology



Road User /Road Operator Security

Road User
Privacy

Road User
Authentication

Safety
Device/Service
Integrity



Info Systems in Transportation

- Broad categories of security policies in transportation information systems – confidentiality, integrity and authentication
 - **Road User Privacy** -- seeks to de-identify or obfuscate data to preserve' confidentiality of driver data that may be used for other useful purposes
 - **Safety Device/Service Integrity** -- seeks to maintain integrity of vehicle or traffic control devices messages/data need to support safety function
 - **Road User Authentication** - verify identity to process toll/transit/parking payment, or assert identity – bona-fide emergency vehicle seeking to access and execute signal priority function



Why Are Systems So Vulnerable?

- Why are systems that are trusted (with critical tasks) not always “trustworthy”
 - **Poor requirements** – no explicit security policy (critical assurance requirement is poorly specified or specified too late after design and development)
 - **Poor design, development, operation and maintenance** – lack of fault tolerance in design (not just random errors but malicious threats lead to faults or breaks in security policy)
 - **Poor implementation** - flawed security protocols that govern communications between systems, or obsolescence.
 - Protocols designed under certain threat assumptions that may no longer apply
 - Vulnerabilities arise at the boundaries between different protection technologies (e.g. hardware tamper resistance, authentication) with different assumptions made
 - **Extensibility** – Poorly planned (bootstrapping security from another systems onto yours) or emergent (unplanned) dependencies



Security-by-Design and Defense-in-Depth

- **Constructive:** Software security covers software development lifecycle and focuses on reducing vulnerabilities in the early stages (requirements & design)
 - Privacy Policy Drives Requirements (Privacy-by-Design)
- **Operational:** Host Security and Data Security protects computing resources and assets – focus on both maintenance and operations
 - Host security through patching vulnerabilities operating systems and applications
 - Data Security protects data at rest and in motion– the Asset is information
- **Reactive:** Perimeter security protects you local network (Firewalls, intrusion detection) –reactive focus on operations
 - Example: Specialized Firewalled Network Subdomain for Vehicles that blacklists intruders, or white-lists only trusted
 - Looks for “signatures’ or precursors for attack (Advanced Persistent Threats)



Emergent Properties and Resilience

- Emergence means that when simple things combine to a certain degree, new properties, patterns, and behaviors develop
 - ...that often cannot be explained or understood in the context of their components
 - Emergent properties of a system of systems can reveal vulnerabilities
 - But emergent properties can also mean more security - Defense in Depth
 - **See Tech Scan webinar on CMU CERT Resilience Management Model**

Introduction to Resilience Management Model (CERT-RMM)

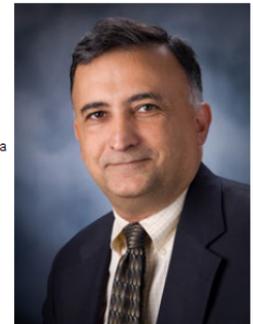
Tuesday, December 9 at 1pm EDT

Dr. Nader Mehravari, Carnegie Mellon University

Click [here](#) for a recording of the session.

CERT Resilience Management Model (CERT-RMM) is the most modern and comprehensive framework for managing operational resilience in a variety of organizations; small or large, simple or complex, public or private. It enables a structured, repeatable, and integrated method for organizations to plan, assess, manage, and sustain not only traditional preparedness planning efforts (e.g., disaster recovery, business continuity, crisis management) but also other key operational risk management activities such as information security and IT operations.

The CERT Resilience Management Model (CERT-RMM) is an innovative and transformative way to approach the challenge of managing operational resilience in complex, risk-evolving environments. By improving operational resilience management processes, the organization in turn improves the mission assurance of high-value services.





Business Opportunities vs. “Vulnerability”

- Business (or efficiency) opportunities require management of cyber-risk
- Decisions to provide new services, such as adding connecting a system to improve functionality, may incur risk
 - As connectivity grows attack surface..
- Attack Surface is the aggregate of all vulnerabilities and controls across all systems and networks. It is the collection of targets exposed to an attacker.
- WHERE WE ARE TODAY...
 - Cloud computing centralize info systems containing sensitive data, you risk creating a more valuable asset (for attack) while simultaneously giving more individuals connections to it.
 - Even if you have a rock solid commitment to privacy – without **effective** controls in place, that privacy assurance can not be maintained.



Vehicle Systems Security

- Traditional security focused on theft prevention
- New security focuses on protection of software Integrity and road user data
 - New software is loaded or “flashed” into vehicle electronic controllers, either at the end of the assembly line or in the field
 - Nomadic devices (smartphones) are paired with vehicle telematics systems
- Next Generation Security focuses on Driving Automation and Future V2X Communications
 - Misbehavior Detection / Sensing Integrity
 - Privacy Protection



Vehicle: UW/USCD Case Studies 2010

- Univ Washington/UC San Diego demonstrate the ability to adversarially control a automotive functions and completely ignore driver input, assuming compromised access
- Vehicle systems respond appropriately when components are prevented from communicating—but tolerance of attacks not part of the same design criteria
- Standard access controls are weak/non-existent/un-used - once malicious code, installed, then no problem in injecting CAN messages/controlling vehicle systems
- Attack surface is changing: Indirect physical access (ODB-II), Tire Pressure Monitoring system, Multi-media device (USB, Bluetooth), and Telematics (2G-4G)
- PCs and Mobile Devices are “stepping stones” to access vehicle and traffic control devices for post compromise control
- HOWEVER– No detail on type of vehicle attacked or how attacked worked.



Vehicle: Charlie Miller/Chris Valasek – 2012-2013

- Adventures in Automotive Networks and Control Units 2012
 - Builds on work DARPA project to build tools/platform that would aid in automotive security research
 - Attempt to generalize attack surface across different models of vehicles and architectures (rely less upon security through obscurity)
 - “Fact that a risk of attack exists, but there is not a way for researchers to monitor or interact with the system is distressing...”
 - 2013 DARPA Grant to determine which vehicle would present the most obstacles to an attacker -
 - Chose 2014 Jeep because of large attack surface, simple architecture and advance features (automated braking/steering etc..)



Vehicle: Miller/Valasek 2012 and 2015

- Remote Exploitation of an Unaltered Passenger Vehicle, 2015
 - Proof that you didn't need physical access to vehicle – Remote exploitation was confirmed in tests as possible
 - Explore modem/telematics unit and move laterally to jump into CAN
 - First attempt was to connect to car via rogue femtocell, because assumed wireless carrier ISP would block traffic.
 - Wireless ISP did not block traffic/ports between devices on its network – researchers were able to scan and identify 2,695 vehicles
 - Vulnerability suggested worm could be created to scan for vulnerable vehicles, deliver payload through Telematics Unit and compromise control systems



Impact of Miller/Valasek and others 2015

- Miller/Valasek Researchers disclosed each vulnerability to NHTSA, OEMs and suppliers as they discovered them, before publishing report in 2015
- Reaction was swift - Wireless Carrier blocks ports, patches released by OEM, OEM recalls 1.4 Million vehicles
- Media articles –” Security Experts Identify 20 Most Hackable Cars” etc..
- Senators Markey (D-Mass.) Blumenthal (D-Conn.) introduce the *Security and Privacy in Your CAR (SPY CAR) Act of 2015* \ul>- Directs NHTSA and FTC to establish federal standards





SPY CAR Act 2015

- Security Provisions
 - Requirement that all wireless access points in the car are protected against hacking attacks, evaluated using penetration testing;
 - Requirement that all collected information is appropriately secured and encrypted to prevent unwanted access; and;
 - Requirement that the manufacturer or third-party feature provider be able to detect, report and respond to real-time hacking events.
- Privacy Provisions
 - Transparency requirement that drivers are made explicitly aware of data collection, transmission, and use of driving information;
 - Consumers can choose whether data is collected without having to disable navigation; and Prohibition on the use of personal driving information for advertising or marketing purposes.



Other Legislation

- Protecting Cyber Networks Act (PCNA, H.R. 1560 as passed by the House),
- the National Cybersecurity Protection Advancement Act of 2015 (NCPAA, H.R. 1731 as passed by the House), and the Cybersecurity Information Sharing Act of 2015 (CISA, S. 754, as reported in the Senate)
 - Three bills focus on information sharing among private entities and between them and the federal government.
 - No discussion of Liability



Liability is Complicated

- Lack of clear liability shifts burden for security (cost of attack) onto other parties
- Most liability of software contracted away in licensing agreements, likely for most road user mobility apps
- Failure to implement best practices can impose liability for safety system
 - Larsen vs. GM (1961) – no duty to produce a “Crash-proof” car, but possible for GM to have designed vehicle to minimize effect of crash
 - Obviously software assurance and security is a big topic in auto industry, and industry is used to addressing liability resulting from defects
- The unfortunate reality is that *no software product of nontrivial size and complexity can be assumed free of error or security weaknesses*
 - ...but courts lack of technical expertise and inherent complexity of software make it hard to establish fact patterns
 - Experience base may grow insurance claims and case law grows



Infrastructure Attacks

- Financial Transactions, Road user info services, Traffic Control
 - Dynamic Message Signs
 - Transit payment, toll or parking payment
 - Signal priority authentication (highway intersection and rail)
- Temptation to seek multi-function authentication devices (e.g. smart cards) for multiple services to improve convenience and usability.
 - Using same authentication mechanisms in more than one application risks Mafia-in-the-middle attack.
 - EZ pass, Emergency Vehicle transit signal priority cloned by attackers.



Basic Questions for ITS Stakeholders

- What current assets must you protect?
- What are the threats, vulnerabilities (e.g. how big is the attack surface)?
- What are the available protection countermeasures?
- Absent countermeasures or prior knowledge of threats or vulnerabilities - How do you prepare to minimize impact?
- How security strategies for your transportation systems differ from other systems?
- How do you improve your knowledge of emergent threats and solutions quickly to operate systems securely (reduce attack surface)?
- For future systems: can you incorporate security in the design phase to reduce vulnerabilities in the first place?



Intelligent Transportation Society of America

THANK YOU...

Steven H. Bayless



Connected Vehicle Privacy

- The goal of VII principles is to establish **trust** between application service providers and road users inside the Connected Vehicle environment,
- Where a lack of trust may have the unintended effect of discouraging road users from participating in the system
- Institute Privacy-By-Design and Security in Depth– system designed preserve road users privacy (level of anonymity)
- NHTSA Issued an Advance Notice of Proposed Rulemaking and an Request for Information (Security Credential Management System) in 2014



Privacy-by-Design - Model Principles

- Alliance of Automobile Manufacturers/Global Automakers Consumer Privacy Protection Principles – Vehicle Technologies and Services 2014
 - Transparency and Choice
 - Respect for Context
 - Data Minimization, De-identification, and Retention
 - Data Security
 - Integrity and Access
 - Accountability
- ITS America's Policy and Business is updating its principles, first established in 2007
- Vehicle Infrastructure Integration Privacy Policies Framework 2007