DHS S&T Automotive Cybersecurity R&D Program

December 10, 2015

Dr. Dan Massey

Program Manager
Cyber Security Division
Science and Technology Directorate

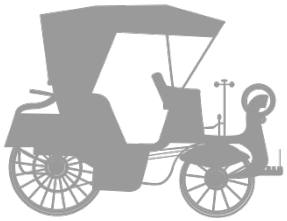
Homeland Security
Science and Technology

WHY ARE WE LOOKING AT VEHICLE CYBERSECURITY?

Not Vulnerable to Cyber Attacks

Demonstration of Cyber Vulnerabilities

Cyber Exploits Cause Damage ??



Not Vulnerable to Cyber Attacks

Addition of Cyber Components

You are Here

Homeland Security
Science and Technology

THE DAILY NEWS

Thursday, April 16, 2018 THE WORLD'S FAVORITE NEWSPAPER $1.25

CHAOS AND TERROR

Cyber-Sabotaged Fire Trucks Crash Into Bombing Scene

Fire trucks responding to the bombing scene careened out of control after being sabotaged in apparent cyber attacks.

At least 20 people are dead and hundreds are injured in what appears to be a coordinated terrorist attack. Fire trucks and police units rushing down city streets to the scene of a downtown car bombing had their brakes and steering remotely disabled by cyber attacks.

Hundreds of bomb victims lay injured in the streets waiting for hours for help and many died because they did not get to a hospital in time.

According to police sources, officials have been aware for some time that emergency vehicles could be vulnerable to remote "car hacking" attacks but they did not consider it a likely terrorist threat.

RESEARCH REQUIREMENT INPUTS

White House and NSS

Departmental Inputs

Interagency Collaboration

State and Local

Cyber Security Division

Critical Infrastructure Sectors
(Private Sector)

International Partners

Homeland Security
Science and Technology

CYBER SECURITY DIVISION MISSION

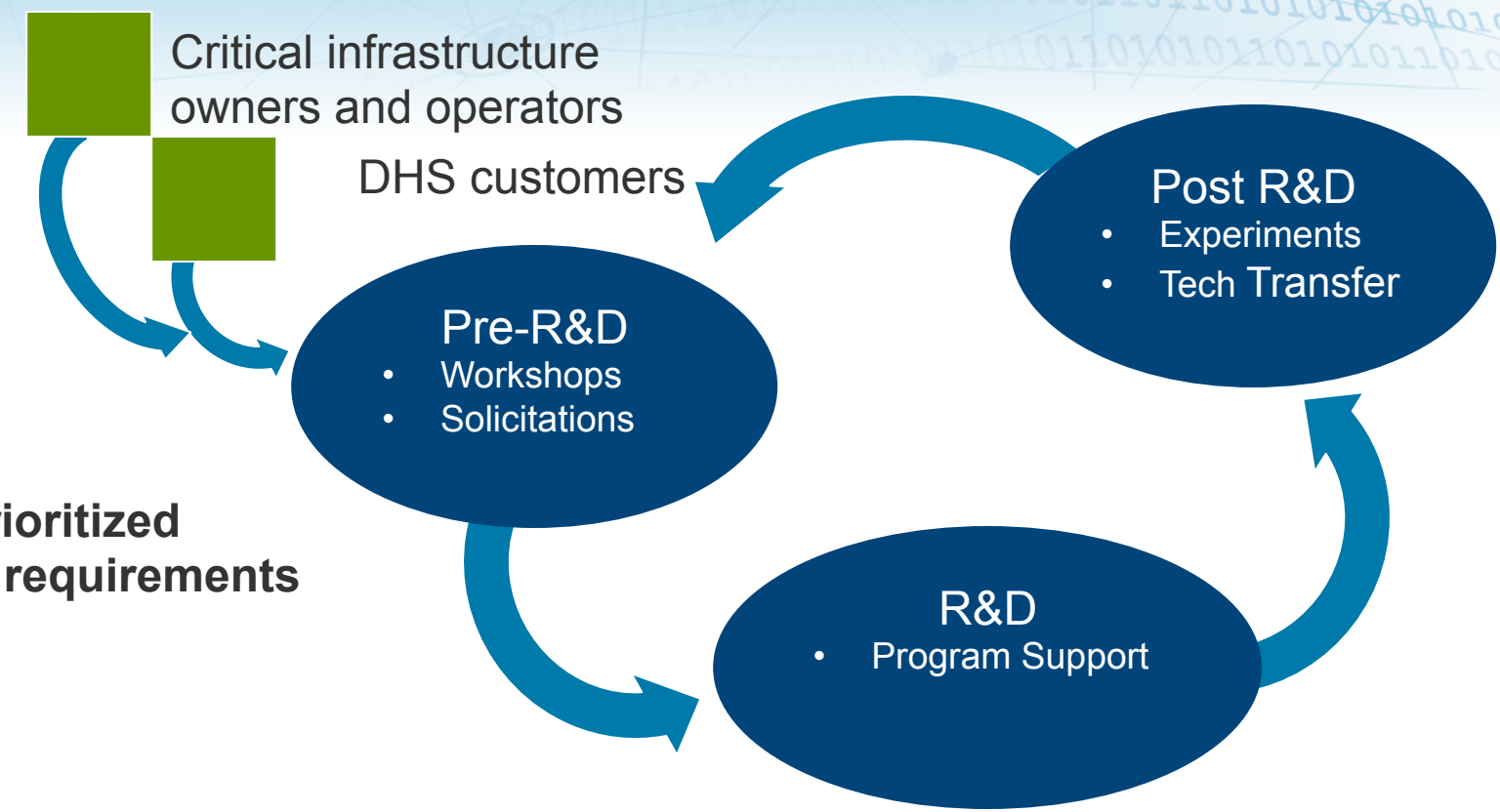
- **Develop and deliver new technologies, tools and techniques** to defend and secure current and future systems and networks
- Conduct and support **technology transition** efforts
- Provide **R&D leadership and coordination**

Trustworthy Cyber Infrastructure	Cybersecurity Research Infrastructure	Network, System Security and Investigations	Cyber Physical Systems	Transition and Outreach

Open Source Venture Capital
Government Industry and integrators

Homeland Security
Science and Technology

CSD R&D EXECUTION MODEL



"Crossing the 'Valley of Death': Transitioning Cybersecurity Research into Practice,"
IEEE *Security & Privacy,* March-April 2013,
Maughan, Douglas; Balenson, David; Lindqvist, Ulf; Tudor, Zachary
http://www.computer.org/portal/web/computingnow/securityandprivacy

Homeland Security
Science and Technology

CPSSEC OPPORTUNITY AND SOLUTION

Internet Design Goals

ARPAnet design goals (Clark,1988)

- Function despite loss of networks/ gateways
- Support multiple types of services
- Accommodate a variety of networks
- Distributed management of resources
- Cost effective
- Low level of effort to add a host
- Provide accounting of resources used

Led to today's challenges in accounting (last goal) and lack of security (non-goal)

CPS Design Goals Being Set Now

Security will NOT emerge on its own

Build Security In

Promote security at onset

Connect research and industry

Enable security as an integral component

Homeland Security
Science and Technology

CPS SECURITY PYRAMID

OBJECTIVE		APPROACH
Enable progress through market-driven requirements	**1. Specific Industry**	**Industry Consortium** Develop sector-specific groups
Develop economically feasible mitigations	**2. DHS Focus Areas**	**Applied Research** CPSSEC Program
Leverage cross-cutting CPS research	**3. Cyber Physical System Concepts**	**Joint Research** Inter-Agency Efforts

Homeland Security

Science and Technology

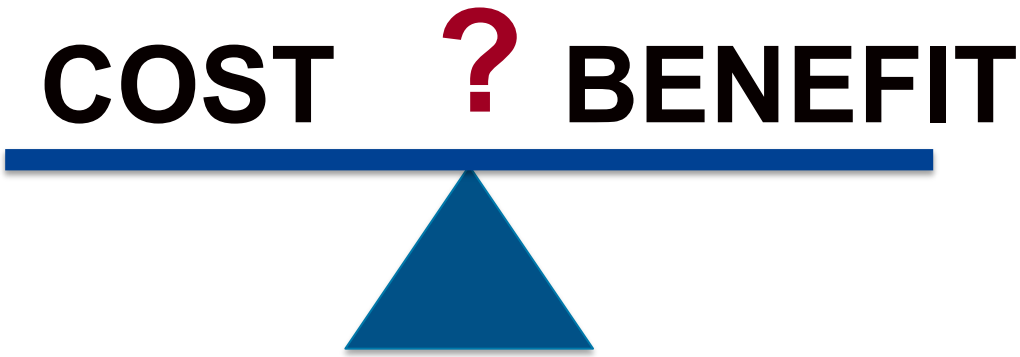
COLLABORATION ON VEHICLE SECURITY

- Promote automotive cybersecurity best practices and guidelines in the private sector
- Develop with pre-competitive research consortium with industry
- Address cyber security needs for government vehicles

Homeland Security
Science and Technology

AUTOMOTIVE CYBERSECURITY CONTEXT

- DHS S&T and DOT-Volpe are NOT regulatory agencies
  - Working with industry to find solutions to cybersecurity issues
- Goal is measured, balanced, and cost effective ways to mitigate cyber threats

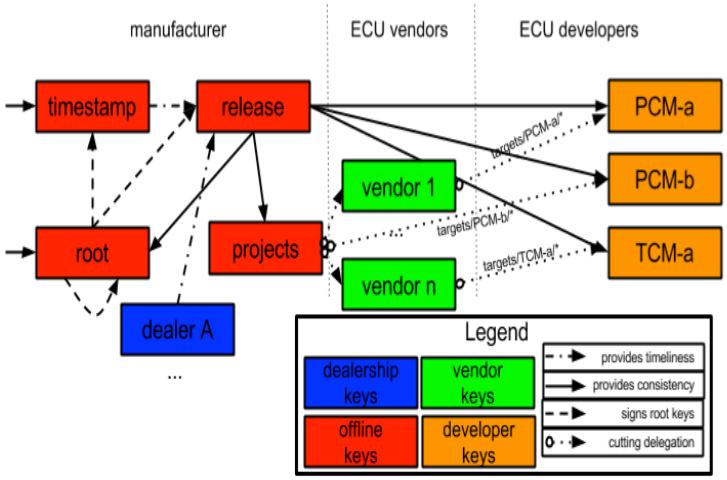


Homeland Security
Science and Technology

CPSSEC BAA PROJECTS - AUTOMOTIVE

ORGANIZATION	PI(S)	TITLE
New York University	Justin Cappos w/ Damon McCoy	UPTANE: Securely Updating Automobiles
University of Michigan w/ SwRI	Andre Weimerskirch w/ Brian Anderson	Secure Software Update Over-the-Air for Ground Vehicles Specification and Prototype
HRL Laboratories w/ DATA61 and UCI	David Payton w/ Gernot Heiser and Gene Tsudik	Side-Channel Causal Analysis for Design of Cyber-Physical Security

Securely Updating Automobiles



Operational Capability to be Provided:

- Securely Perform Software Updates of Automobiles
  - Resilience to key compromise
  - Resist and detect malicious MITM, dealerships, vendors, etc.
  - Detect and discard malicious OTA updates
- User friendly (no intervention) when system is not under attack

Demonstrate practical security in both OTA and dealership dissemination models

Proposed Technical Approach: New Effort

Task 1:

Analyze the security of existing updaters
Demonstrate attacks on these systems

Task 2:

Draft specification for metadata layout, formats, client verification behavior
Reference implementation (specific environment)
Demonstrate resilience to attacks via unit tests and full system attacks

Task 3:

Reference implementation
Security review
Assist vendors in practical deployment

Schedule:

Period of performance:
Task 1: Months 0-5
Task 2: Months 6-18
Task 3: Months 19-33

Deliverables:

Standards document for update metadata formats and secure updater specification
Reference implementation for secure updater
Reports as listed in Section 4.1 of the BAA

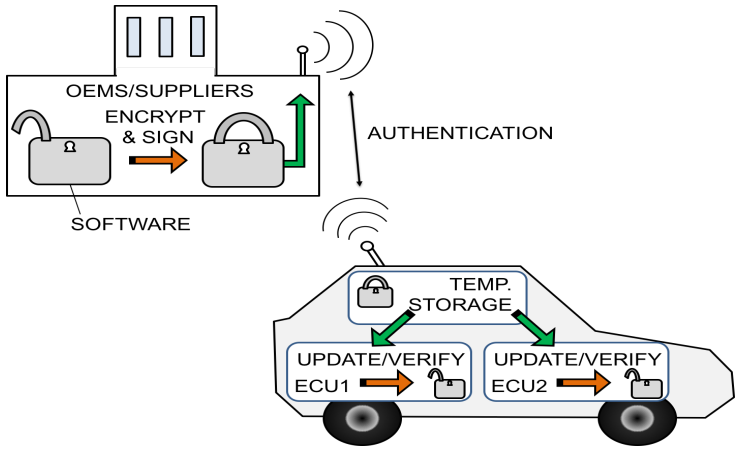
Technical Contact Information:

Justin Cappos
New York University
jcappos@nyu.edu

BAA Number: HSHQDC-14-R-B0016 Offeror Name: UMTRI & SwRI

Title: Secure Software Update for Ground Vehicles Date: December 1, 2015

Concept



Operational Capability:

- **Performance targets**: Create secure software over-the-air (SOTA) update reference specification and implementation that is ready for use in ground vehicles.
- **Quantify performance for key parameters**: Verify integrity of firmware in automotive ECU (in order of seconds), acceptance by car makers (quantified in stakeholder workshops), and proof of security.
- **Cost of ownership or licensing**: Open source for interested stakeholders.
- **Addressing goals in the BAA call**: Secure software update is a necessary operational feature to mitigate security vulnerabilities.

Proposed Technical Approach:

- **Meet goals in BAA call**: Comprehensive secure SOTA solution including reference specification and source code to guide stakeholders against flawed solutions.
- **Tasks**:
  - Requirements definition
  - Design solution
  - Implementation and integration
  - Testing and Evaluation
- **Actions done to date**:
  - Supported several car makers' implementation of proprietary limited software update mechanisms
- **Related ongoing effort**:
  - Resilient automotive architecture design
  - Design of secure CAN
  - Design of intrusion detection and prevention systems
  - Automotive penetration testing

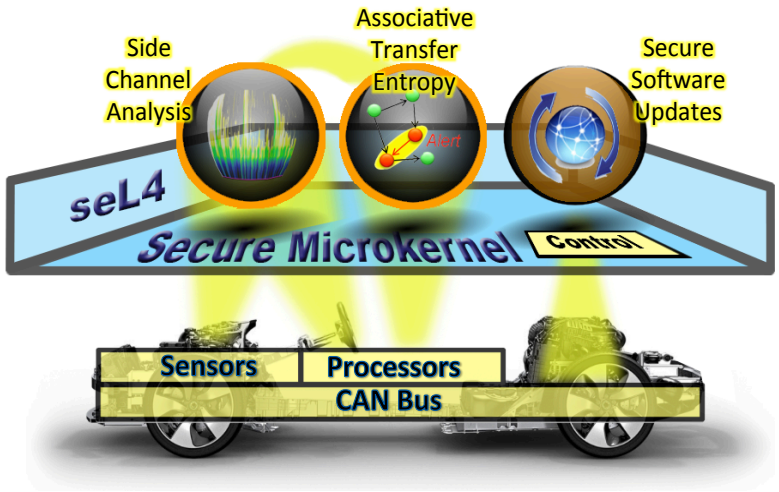
Schedule, Deliverables, & Contact Info:

- **Project length**: 24 months
- **Milestone decision points**:
  - *Month 6*: requirements specification
  - *Month 12*: design and prototype
  - *Month 18*: prototype implementation
  - *Month 24*: tested integrated solution
- **Deliverables**:
  - Requirements document
  - Design document
  - Test plan
  - Reference source code
- **Contact information:**

University of Michigan
Dr. André Weimerskirch
2901 Baxter Road, Ann Arbor, MI 48109
phone: 734-936-1046
email: andrewmk@umich.edu

BAA Number: HSHQDC-14-R-B0016

Title: Side-Channel Causal Analysis for Design of Cyber-Physical Security



Operational Capability:

Challenge	Innovation	Benefit	Metric
Detect covert intrusion.	**Side-channel defense** monitors physical signatures that are beyond the control of an attacker	Detect stealthy attacks from the way they alter physical signatures.	2x increase in attack coverage by increasing coverage to additional attack categories such as dormant and passive attacks.
Distinguish anomalous behavior	**Associative transfer-entropy** analysis detects deviations from known physical causal structure	Sensitive to the subtle causal changes related to attacks.	
Minimize added cost	**Real-time seL4 microkernel**: processes securely coexist on the same hardware.	Ensures isolation to limit possibility of corruption on existing hardware.	95% lower cost for designed-in security over bolt-on solutions.
Secure software updates	**The first provably-secure software-only attestation scheme**	Easy integration with any cyber-physical system.	< 10% cost of HW solution; < 300ms to attest 100 KB code.

Cost of ownership: seL4 will be open source (GPLv2 license). Other technology developed will be free to GM, Boeing, and their suppliers for commercialization.
Addressing BAA goals: Our method provides a unique way to exploit the causal cyber and physical linkages that are pervasive in cyber-physical systems.

Proposed Technical Approach:

1. ***Goals***: Detect intrusion and attacks to transportation systems using analysis of normal and side-channel data to reveal causal inconsistencies. Reduce added cost of security using the seL4 microkernel to avoid need for added hardware.
2. ***Tasks***:
   Task 1: evaluate side-channel data sets and develop feature extraction algorithms
   Task 2: develop causal analysis techniques for detecting attacks
   Task 3: develop develop real-time isolation for seL4
   Task 4: develop attestation and secure updates using unique properties of seL4
   Task 5: provide integrated tests and demonstrations in automobiles
3. ***Current Status:*** Associative Transfer Entropy proof of concept has been established; seL4 microkernel has been used to run virtualized Linux on x86 processors, running high-performance database workloads.
4. ***Actions to date:*** Pilot study of Associative Transfer Entropy using financial market time series data shows indicators of market transitions. Technique for using side-channels for system status has been demonstrated & patented. Virtualization with seL4 on ARM processors is under development.
5. ***Related ongoing effort:*** In the DARPA HACMS program, HRL is developing demonstration platforms for high-assurance control and operating system software for ground vehicles.

Schedule, Cost Deliverables & Contact Info:

		Base		Option 1				Option 2					
Task	Name	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12
1	Side-Channel Monitoring & Analysis		1▲				2▲				3▲		3▲
2	Cyber-Physical Causal Analytics		4▲				5▲						6▲
3	Real-time Secure Microkernel				7▲		8▲						9▲
4	Attestation & Secure Updates		10▲				11▲				12▲		12▲
5	Platform Software Integration		13▲		14▲		15▲			16▲			17▲
6	Program Management	18▲	19▲		20▲	21▲	22▲		24▲	25▲	25▲		26▲

Total Program Cost = $2.487M

Major Milestones	
1. Detection algs of subsystem modes and behavior	10. Attestation scheme for single component
2. Detection algs of microcontroller modes and behavior	11. Secure code updates for single components
3. Enhanced detection algorithms	12. Secure code updates for heterogeneous components
4. Causal analysis for anomaly detection	13. Causal analysis of side-channels
5. Causal analysis incorporating switchable system states	14. Integrate attestation on sel4
6. Causal analysis with heterogeneous processor types	15. Integrate enhanced casual analysis on enhanced seL4
7. seL4 with process time management capabilties	16. Integrate single component secure code update
8. seL4 with real-time process temporal isolation	17. Integrate heterogeneous component secure updates
9. Verified real-time isolation in seL4	18-26: Program reviews and Annual PI Meetings
Deliverables	
Test & Evaluation Plan (Month 6)	Secure Code Update Design report (Months 6, 18, 36)
Design requirements (Month 6, 18, 36)	seL4 Enhancements Design report (Month 18)
Prototype software (Months 18, 36)	Enhanced seL4 software (Month 18, 36), Proof (Month 36)
Presentation materials from Program Reviews and PI Mtgs.	Monthly Status Reports, Final Report (Month 36)

Corporate Information: HRL Laboratories, LLC, Dave Payton (Technical POC)
3011 Malibu Canyon Road, Malibu, CA 90265,
Phone: (310) 317-5685, FAX: (310) 317-5676, Email: payton@hrl.com

AUTOMOTIVE CYBERSECURITY INDUSTRY CONSORTIUM (ACIC)

- Voluntary and technology-oriented Public Private Partnership (PPP) consortium
- Automotive OEMs with support from DHS S&T and the DOT-Volpe
- OEMs can pool resources and leverage them with government funding
- Cooperative “Pre-Competitive Research” (PCR) to improve the level of cybersecurity in automobiles
- Projects identified and selected by consortium members provide mutual benefit by reducing the threat of cybersecurity risks

Homeland Security
Science and Technology

HOW YOU CAN CONTRIBUTE

- Growing community of automotive cybersecurity R&D
- Submit to government research solicitations
  - DHS Silicon Valley IoT solicitation
  - NFS CPS solicitation (joint with DHS S&T, DOT, and others)
- Publish at appropriate conferences
  - ESCAR (Embedded Security in Cars) www.escar.info
  - SAE World Congress & Exposition www.sae.org/congress/
  - CPS Week 2016 www.cpsweek.org/2016/
  - ACSAC www.acsac.org

Homeland Security
Science and Technology

CONTACT INFORMATION

Dr. Daniel Massey
Program Manager
Department of Homeland Security
Science and Technology (S&T)
Cybersecurity Division (CSD)
Email: daniel.massey@hq.dhs.gov
Phone: 202-254-6669

Dr. Ulf Lindqvist
Program Director
SRI International
Computer Science Laboratory
Infrastructure Security Group
Email: ulf.lindqvist@sri.com
Phone: 650-859-2351

Kevin Harnett
Cybersecurity Program Manager
U.S. Department of Transportation
Office of Research and Technology
John A. Volpe National Transportation Systems Center (Volpe Center)
Email: kevin.harnett@dot.gov
Phone: 617-699-7086

David Balenson
Senior Computer Scientist
SRI International
Computer Science Laboratory
Infrastructure Security Group
Email: david.balenson@sri.com
Phone: 703-247-8551

Homeland Security
Science and Technology

Homeland Security

Science and Technology