



ISOAG Meeting February 7, 2018

Welcome to CESC



Virginia Information Technologies Agency



Welcome and Opening Remarks

Michael Watson

February 7, 2018



ISOAG February 7, 2018

- | | |
|---|--------------------|
| I. Welcome & Opening Remarks | Mike Watson, VITA. |
| II. Cybersecurity Risk for Automated Vehicles in the Commonwealth | Kevin Heaslip, VT |
| III. COV Security Requirements 101 | Joy Young, VITA |
| IV. Upcoming Events | Mike Watson, VITA |
| V. Operations Update | NG |

Potential Cybersecurity Risks for Automated Vehicles in the Commonwealth of Virginia

Presentation to VITA

February 7, 2018

Dr. Kevin Heaslip
Associate Director
Electronic Systems Lab

Virginia Tech National Security Enterprise

The Center for National Virginia Tech Applied Security and Technology Research Corporation

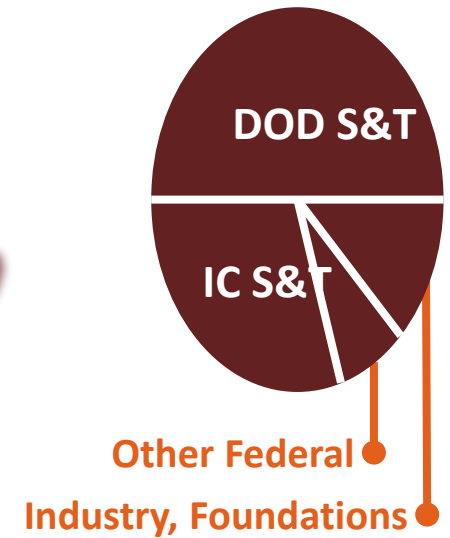
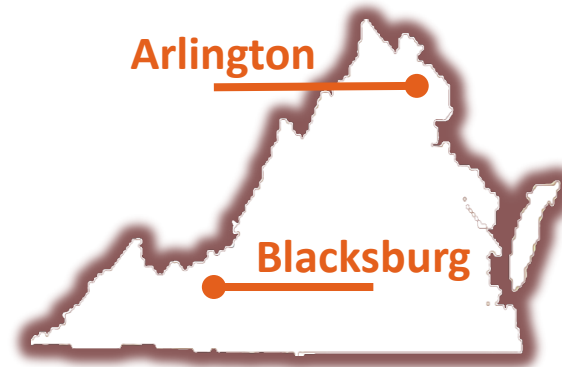
Defense Workforce Development Collaborative Innovation
Advanced Research Technology Domain Awareness
Breakthrough Technologies Applied R&D

University Center
6.1 through 6.3

Integrated 501(c)3
6.2 through 6.4



NSA/DHS Center for Academic Excellence
IC Center for Academic Excellence
CyberCorps Scholarship for Service Site



\$18M
Annual Program
Revenue



100
Researchers, Staff
and Professors



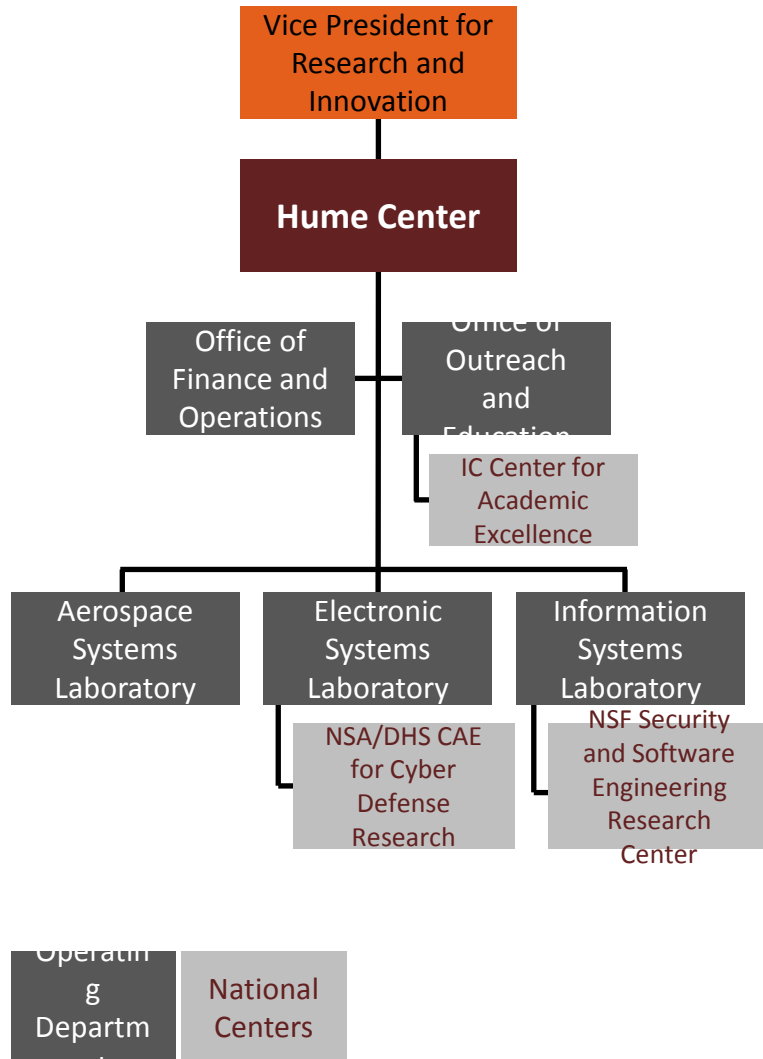
300
Annual Academic
Publications



250
Students Engaged
Annually



Hume Center Organization and Leadership



Charles Clancy
Director

ECE



Mark Goodwin
Deputy Director



Bob McGwier
Chief Scientist

ECE, AOE



Christie Thompson
Director of Finance and Operations



Christine Callsen
Director of Outreach and Education
Kira Gantt
Associate Director of Outreach and Education



Jon Black
Director, Aerospace Systems Lab



Alan Michaels
Director, Electronic Systems Lab



Kevin Heaslip
Associate Director, Electronic Systems Lab

CEE

Academic Appointments

AOE Aerospace and Ocean Engineering
CEE Civil and Environmental Engineering
ECE Electrical and Computer Engineering

Hume Center Program Summary

Outreach & Education



National- and
Cyber-Security
Curriculum



Extracurricular
Programs



Student Career
Mentorship



Experiential
Learning

Electronic Systems Lab



Assured
Communications



Radar and
Spectrum



Electronic and
Cyber Warfare



Counter A2AD

Aerospace Systems Lab



Space Situational
Awareness



Unmanned
Platforms



Autonomy &
Mission
Orchestration



Cubesats and
Small Satellites

Information Systems Lab



Embedded
System Security



Secure and Resilient
Infrastructure

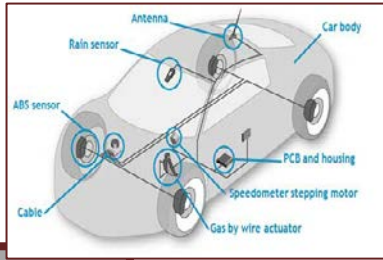


Applied Deep
Learning

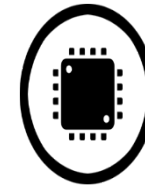


Security and Privacy
for IoT

CIKR Security Safety-Critical Systems IOT Privacy



Research Areas



Embedded



Wireless



Cloud

Embedded

- RTOS Access Control
- Physically Unclonable Functions
- Embedded RNG
- AES Sidechannel Attacks
- *Whitelist* firewall for SCADA transactions

Wireless

- LTE Jamming
- LTE/EPC Security
- Android Security
- Software Radio Exploitation
- Mobile Key Management

Transportation

- Key FOB Security
- Vulnerability Assessments
- V2X Security
- ADS-B Encryption
- UAV C2 Attacks
- Navy

Airworthiness
Center

Energy

- MODBUS Encryption
- Smartgrid Security (Transmission and Distribution)
- Nuclear Reactor Control Systems

Automotive Security Team



Dr. Kevin Heaslip
Associate Director,
Electronic Systems
Lab

Research Areas:

- Intelligent Transport
- Vehicle Operations
- Transport Cybersecurity



Dr. Alan Michaels
Director of Research
Electronic Systems

Research Areas:

- Digital Communications
- Satellite Communications
- LPI/LPD
- Digital chaos



Dr. William C. Headley
Senior Research Associate

Research Areas:

- Signal Detection
- Signal Classification
- Digital Signal Processing



Michael Fowler
Senior Research Associate

Research Areas:

- Cyber electronic warfare
- Wireless security
- Communications



Zach Leffke
Research Associate
Aerospace Systems

Research Areas:

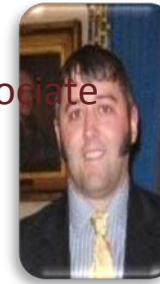
- Wireless signal processing
- Software radio
- Satellite communications



Dr. Ryan Gerdes
Affiliated Faculty
Electrical and Computer Engineering

Research Areas:

- Signal and data authentication
- Hardware and device security
- Computer and network security
- Transportation Security



Kevin Sterne
Research Associate

Research Areas:

- RF Engineering
- Radar
- Wireless communications



Dr. Joseph M. Ernst
Research Assistant Professor

Research Areas:

- Statistical signal processing
- Cyber-physical systems security
- Intelligent Transportation Systems
- Secure Communications

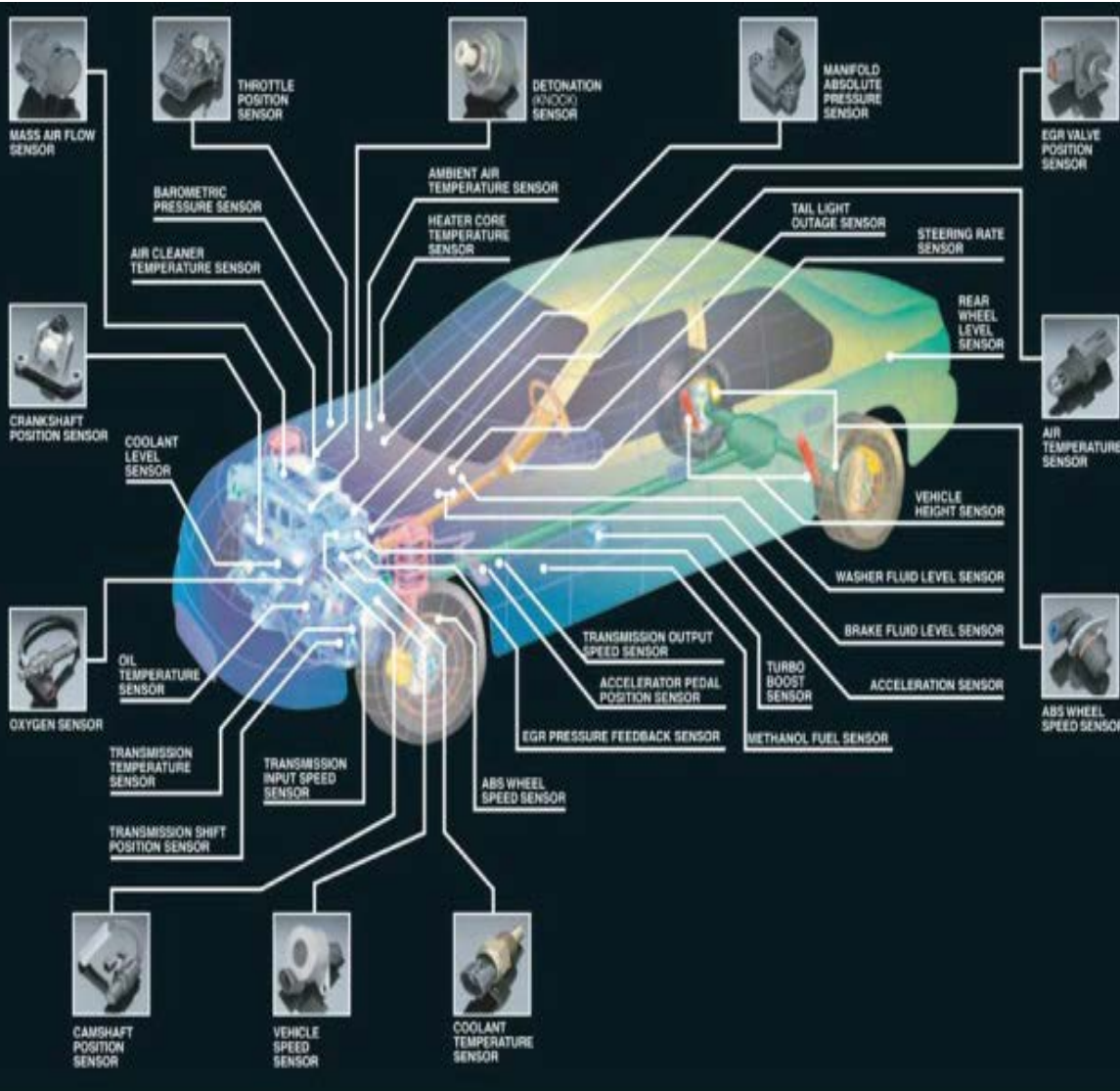
- Over time technology has become integral to the automobile.
- If you do not like computers in your car, a great car for you to have is:



1975 Ford Granada

- Emissions standards and the 1970's fuel crisis made the computerization of automobiles necessary
- Efficiency, not brute force power, was the reasoning for adding microchips to the car.
- Sensors and microchips are the heart of the automobile now.
 - Average of 60 to 100 sensors aboard
 - Automated vehicles should double to triple the amount of sensors aboard
- The typical new car comes with more than 100 million lines of code

Computers in the Car



“A cyber incident is not a problem just for the automaker involved,” Barra said at an industry conference held in Detroit. “It is a problem for every automaker around the world. It is a matter of public safety.”

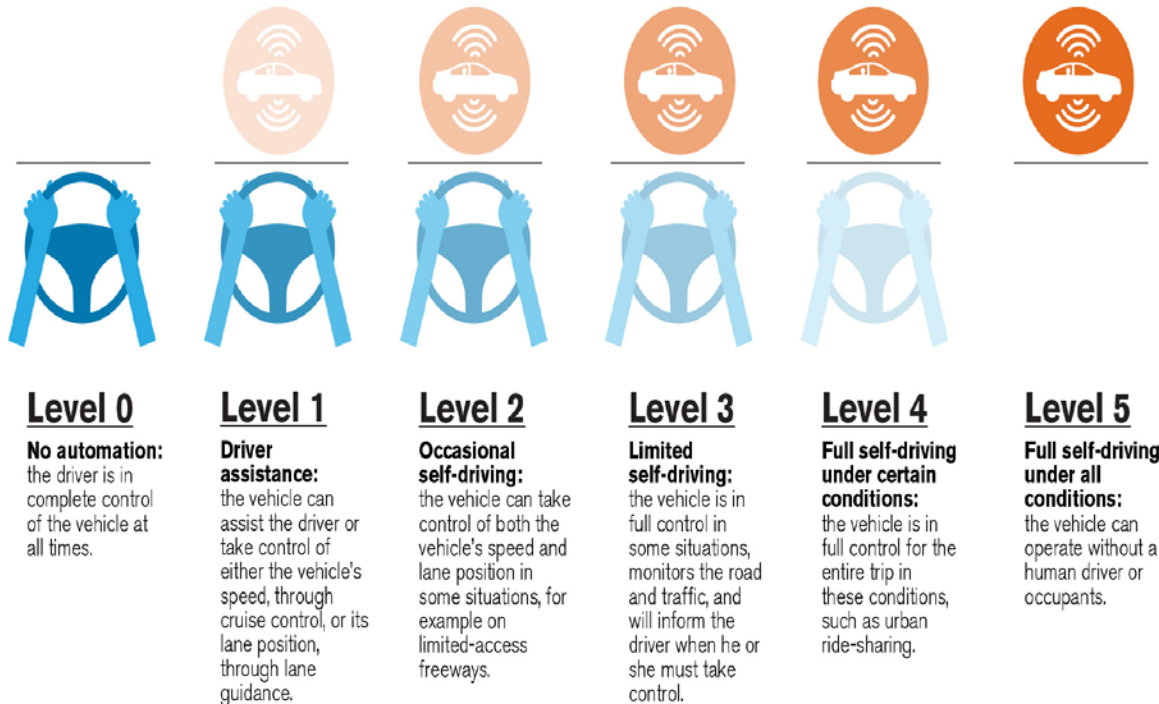
- Autonomous
 - “acting independently or having the freedom to do so”
- Automated
 - “convert (a process or facility) to largely automatic operation”
 - Automated Driving

- Alan Taub of General Motors stated at the 2011 ITS World Congress that the vehicle of tomorrow will be:
 - Autonomous (Automated)
 - Connected
 - Electric



Driver Automation Levels

Five Levels of Vehicle Autonomy



Source: SAE & NHTSA

Automated Driving in Action

Google's Self Driving Car



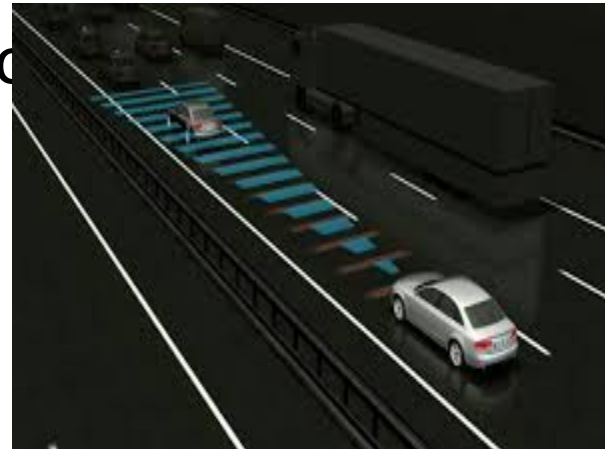
Different Automated Vehicles

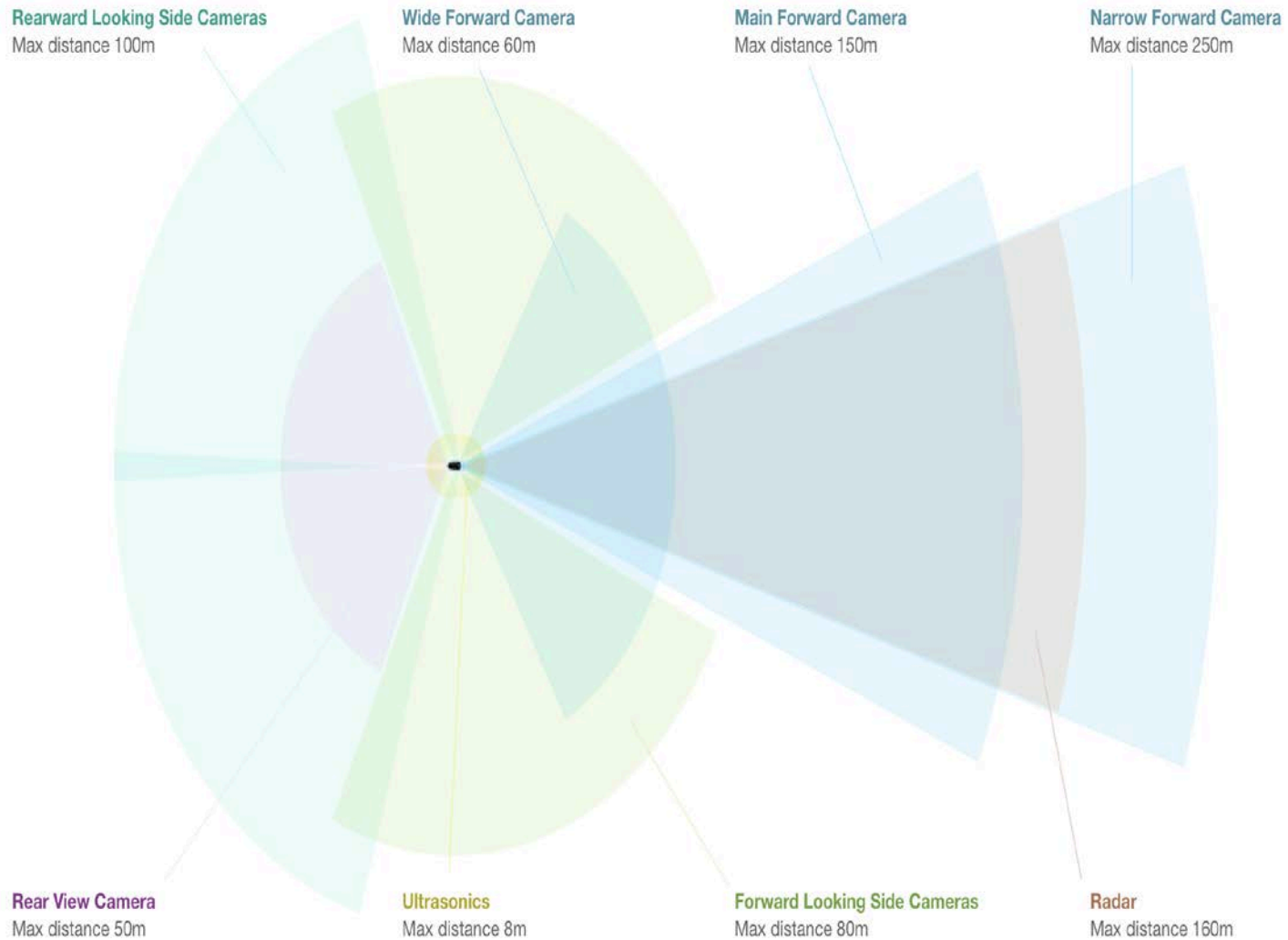
- Automated Vehicles



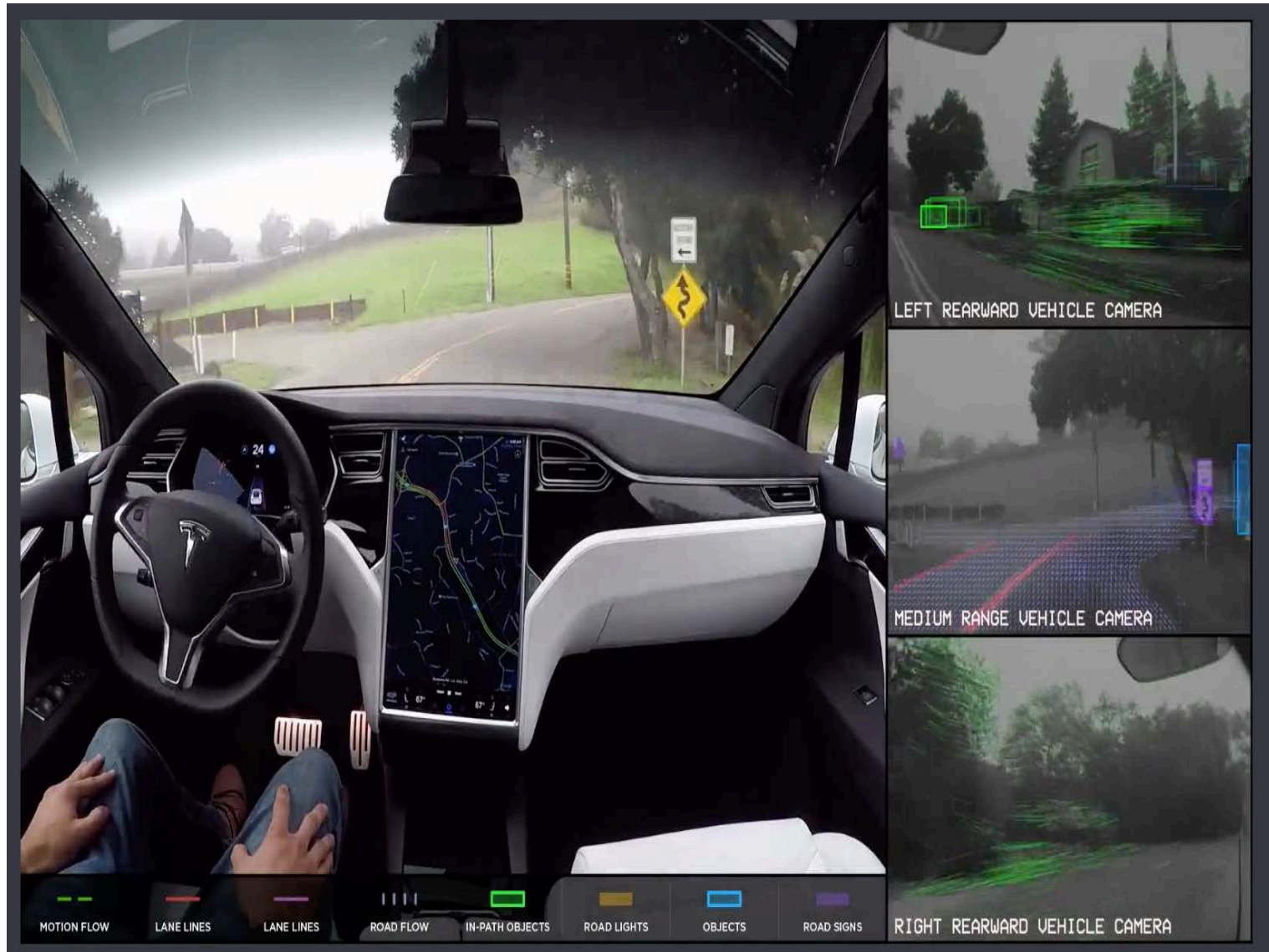
Automation Available Today

- Adaptive Cruise Control
- Lane Keeping
- Jam Assist
- AutoPilot





Use of Machine Vision



Automation Benefits/Challenges

- Benefits
 - Significantly Less Crashes Possible
 - Increased Capacity Possible
 - Platooning
 - Reduced Lane Width
 - More Ridesharing / Less Vehicles
- Challenges
 - Liability Issues
 - Cybersecurity

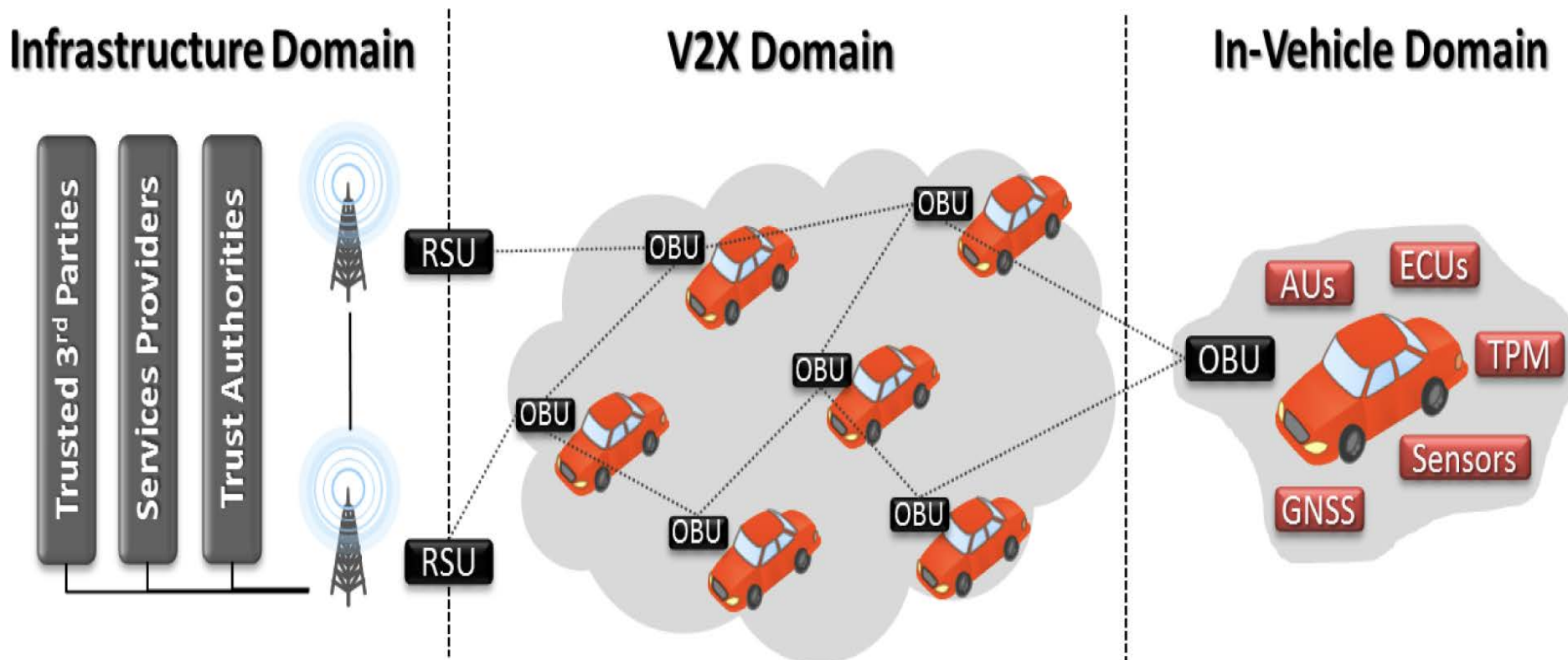
Intelligent Transportation Infrastructure

- Traditional Intelligent Transportation Systems have been shown to be vulnerable.
 - Traffic Signals
 - Variable Message Signs
 - Electronic Toll Collection
 - GPS Navigation
 - Vehicle to Infrastructure Communication
 - Road Weather Information Systems
 - Weigh-In-Motion Systems
 - Traffic Operating Center Communications



Communications Domains in Surface Transportation

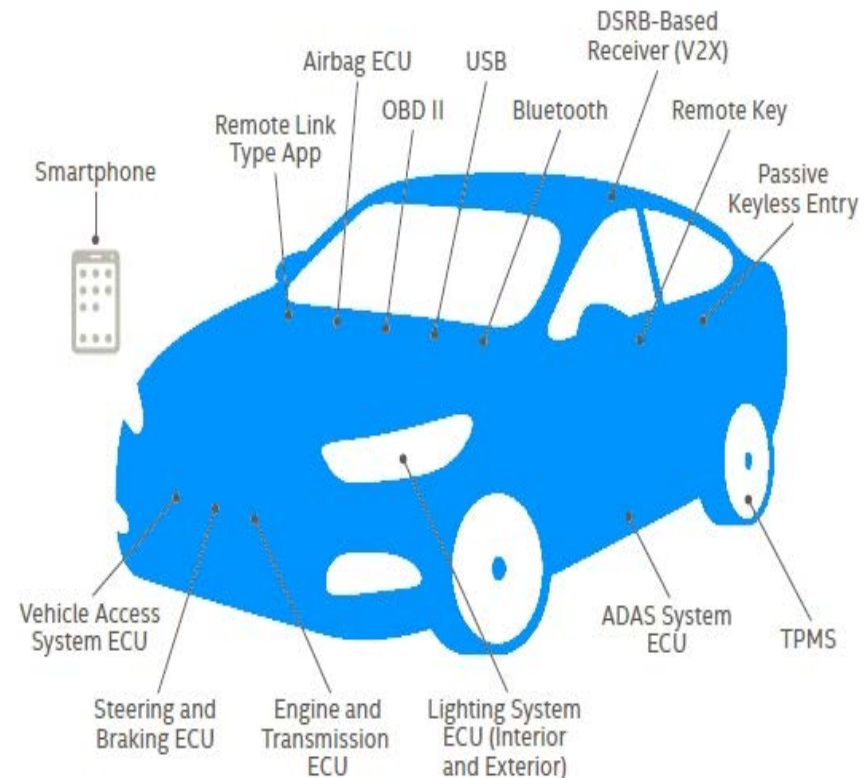
- Each domain requires security to ensure safety and efficiency of the transportation system
- Integrated infrastructure and vehicle security is needed



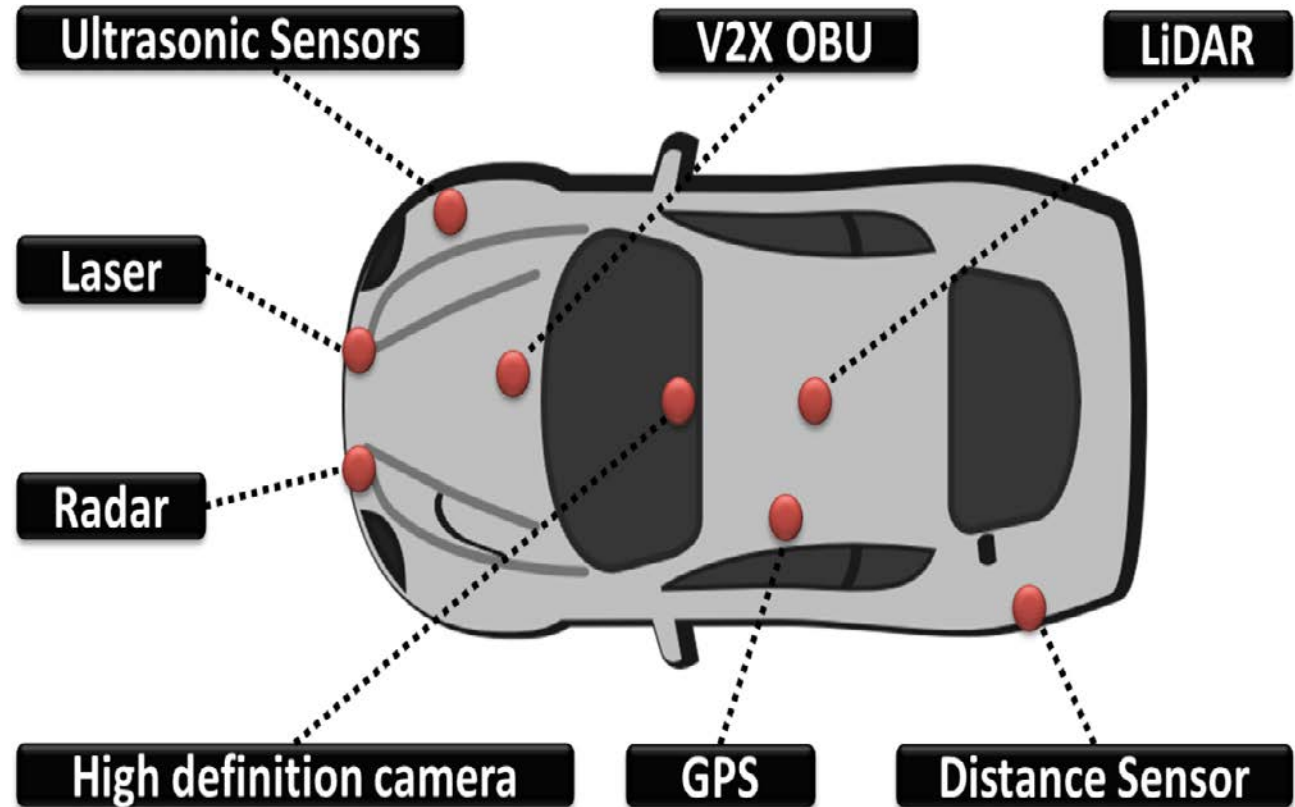
- Vulnerabilities Include:

- On-Board Diagnostic Security
- Tire Pressure Monitor Security
- Key Fob Security
- Infotainment Security

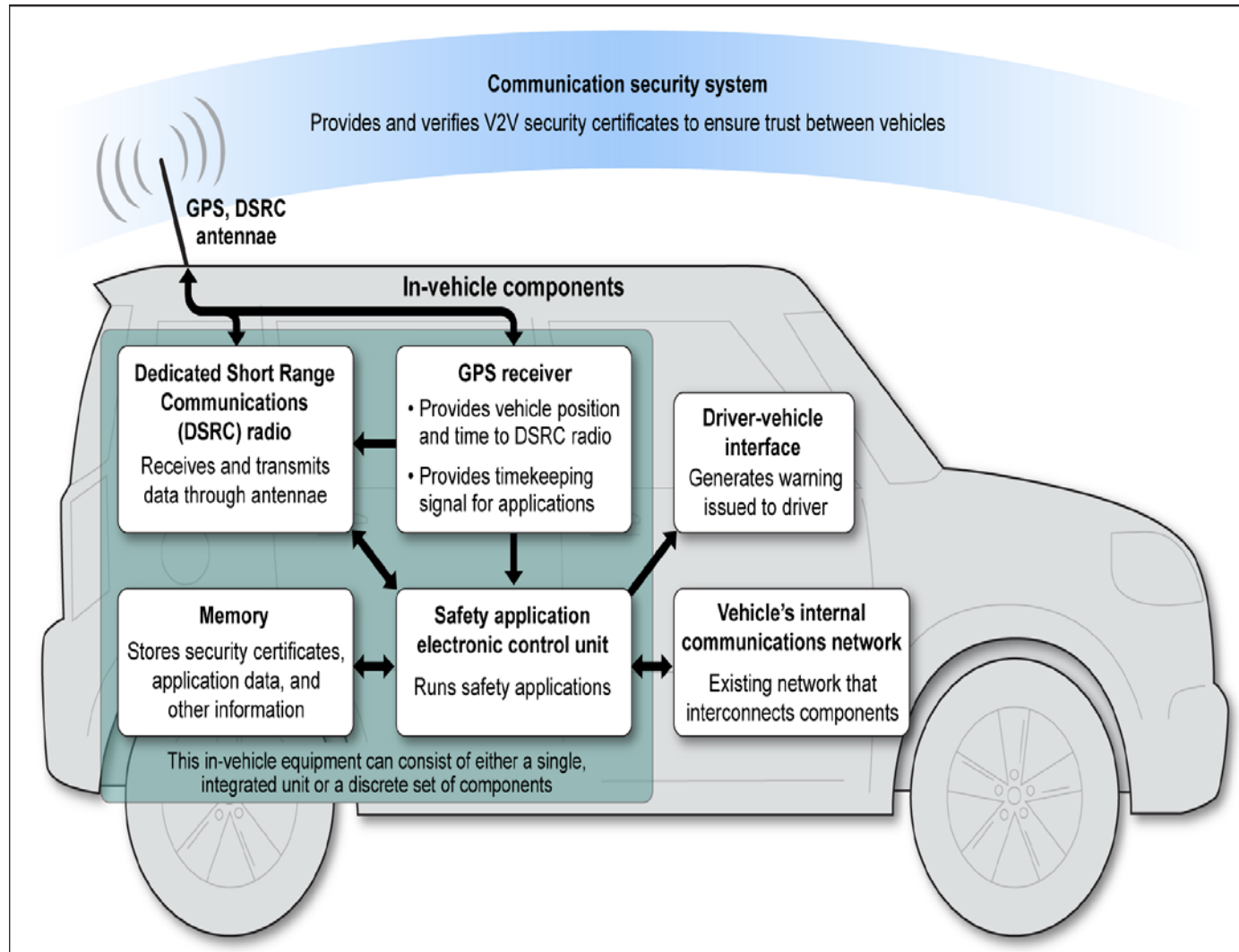
Automobile Attack Surfaces



- Communication systems and sensing systems add attack vectors that have not been seen in previous iterations of vehicles.
- These technologies enable efficiencies and create vulnerabilities.

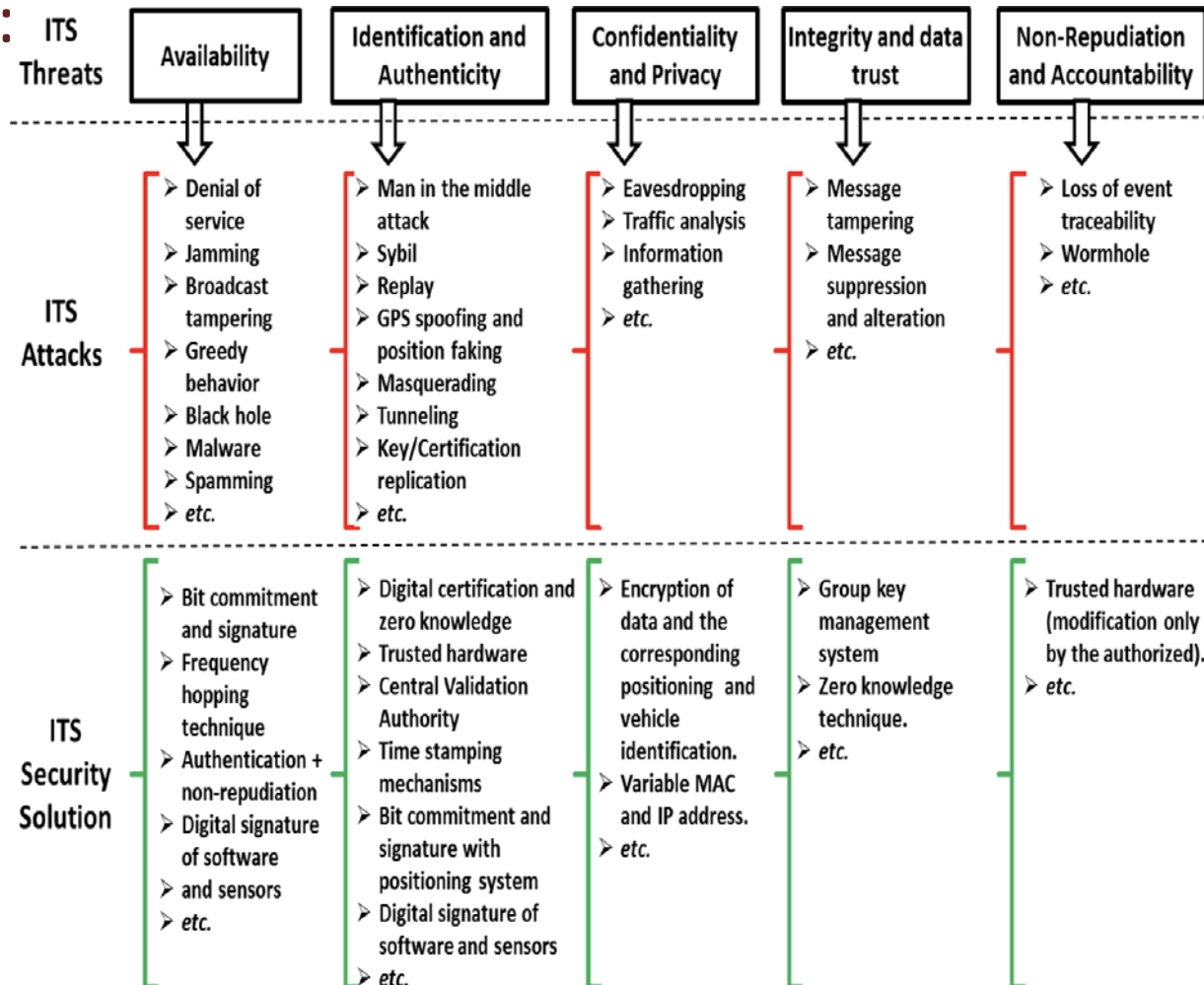


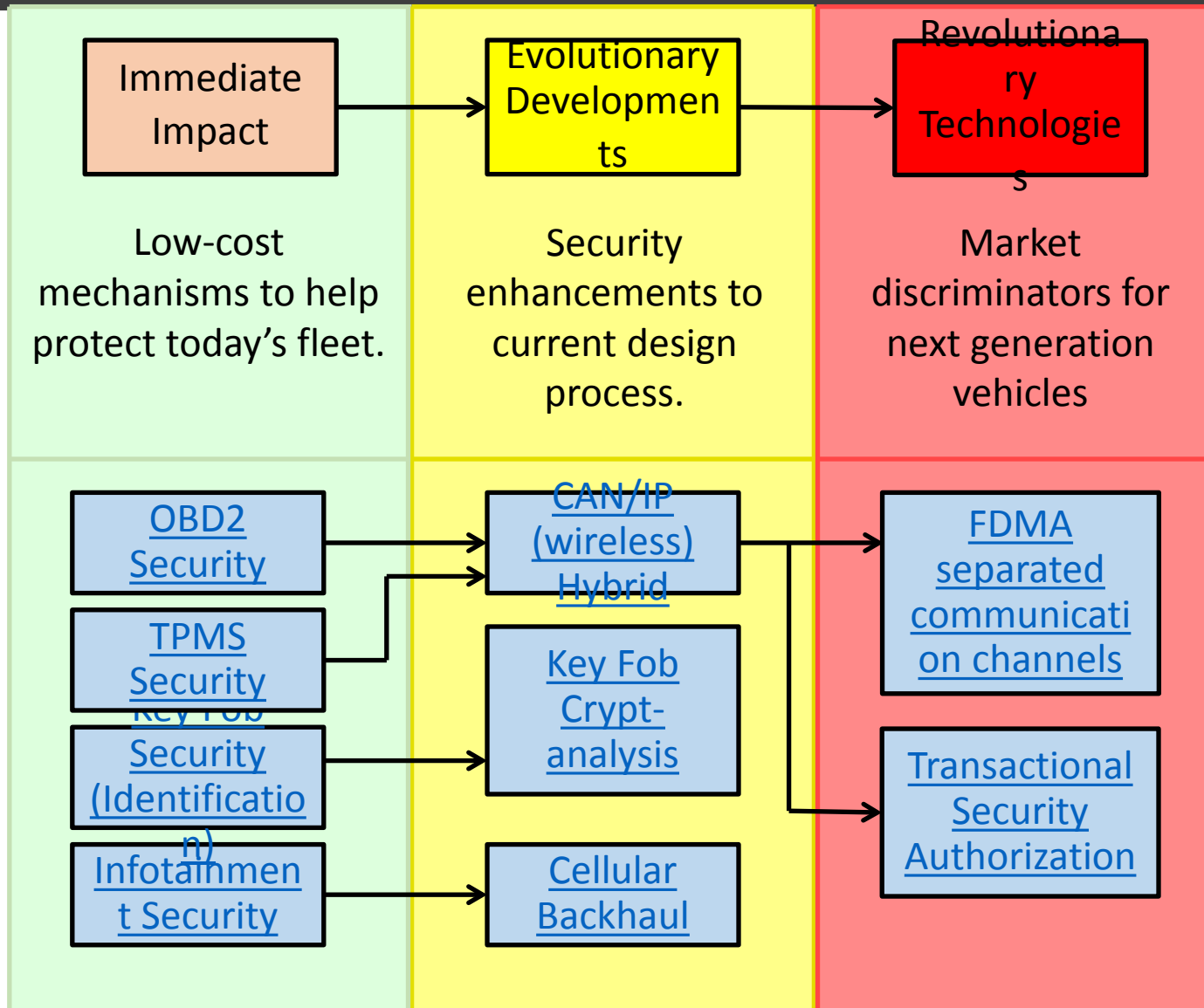
Attacks possible on next generation vehicles



Sources: Crash Avoidance Metrics Partnership and GAO.

• Additional solutions include:





Description

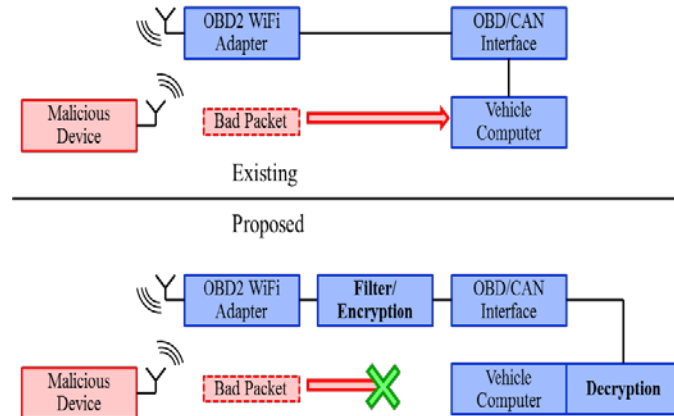
This project will develop a hardware OBD2 interface which would provide additional security while maintaining access required by the “right to repair” law. This cannot simply be an interface which would plug in to the existing system, but must also prevent bypassing of the OBD2 port.

Objective

- Design OBD2 hardware filter
- Design OBD2 CAN encryption
- Design decryption utility for vehicle computer
- Implement proof of concept

Payoff

- Address undesired cyber OBD2 vulnerability
- Prevent spoofed messages on CAN bus delivered to OBD2 port
- Additional layer to prevent buffer overflow type attacks
- Software/Firmware update solution



Deliverables

1. Monthly Technical reports
2. Quarterly Technical Exchanges
3. Final Report
4. Hardware demonstration of OBD2 filter system

Description

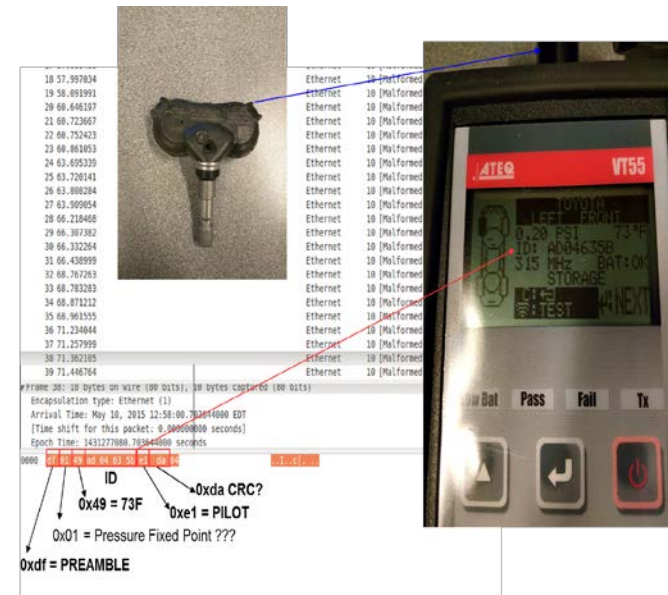
This project will develop a GNU Radio implementation of the Tire Pressure Monitoring System (TPMS) RF signals. It will use low cost software defined radios. The project will begin by developing an algorithm to spoof TPMS signals and will continue by analyzing the extent to which the CAN bus can be affected through the TPMS threat surface.

Objective

- Develop TPMS demodulator
- Develop TPMS transmitter
- Show feasibility of TPMS spoofing
- Design recommendations for robustness to spoofing
- Investigate to what extent the CAN bus is accessible through the TPMS wireless threat surface

Payoff

- Low cost TPMS testbed
- Design recommendations for robust TPMS receiver
- Threat assessment of TPMS->CAN lateral threat vector



Deliverables

1. Monthly Technical reports
2. Quarterly Technical Exchanges
3. Final Report
4. Hardware demonstration of TPMS spoofing

Description

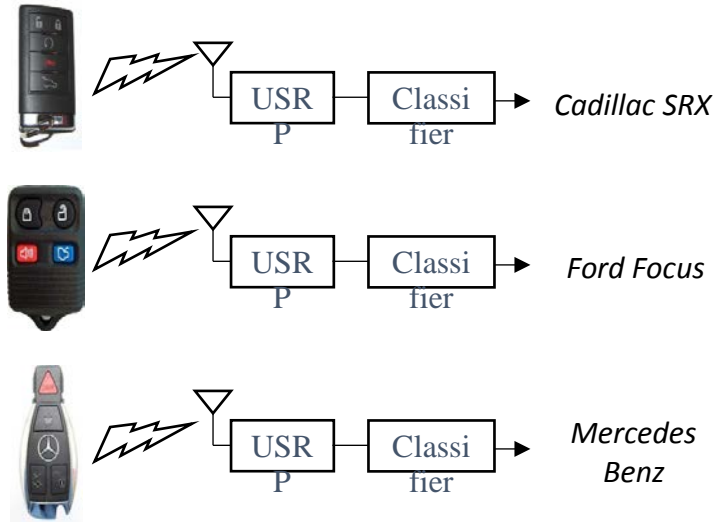
Our initial testing has indicated that different car manufacturers' key fobs have slight differences in their signaling that could be used to identify the key fob when visual cues are not available.

Objective

- Characterize the signaling formats of car key fobs based on make, model, year, and/or country.
- Develop a classification approach to identify a key fob's make, model, year, and/or country from signal captures.

Payoff

- Will determine if a car's key fob can be classified based on its signaling format alone (without using visual cues based on its form factor).
 - Potential Vulnerability: an attacker could find a target's car quicker based on measured responses from the target's key fob.
 - Potential Commercial Application: a car dealer could scan a potential buyer's key fobs and steer their interactions appropriately.
- Provide suggestions to improve key fob security based on the results of this work.



Deliverables

1. Report on the survey of key fob signal characteristics by car make, model, year, and/or country.
2. Classification software used to classify a key fob's make, model, year, and/or country from signal captures.
3. Demonstration of any developed algorithms as well as a report outlining potential improvements to key fob security.

Description

White hat hackers have recently demonstrated the ability to control different components of a vehicle by injecting malware into its infotainment system.

Objective

- Survey the possible user interfaces to the infotainment system on a vehicle and determine possible vulnerabilities
- Determine the impact of a compromised system to the occupants
- Develop mitigation techniques, like intrusion detection and isolation, to secure the interfaces into the infotainment center.

Payoff

- Determine possible attack vectors that can be used to compromise the security of the infotainment center in a vehicle.
- Determine how a compromised system can negatively affect the driver.
- Determine mitigation strategies to detect attacks, block attacks and reset the system if it is compromised.
- Infotainment system isolated from critical systems.



Deliverables

1. Vulnerability analysis of the infotainment center and any interfaces available to the customer
2. Mitigation techniques and overall strategy to secure the interfaces from outside attack.

CAN/IP (wireless) Hybrid

Description

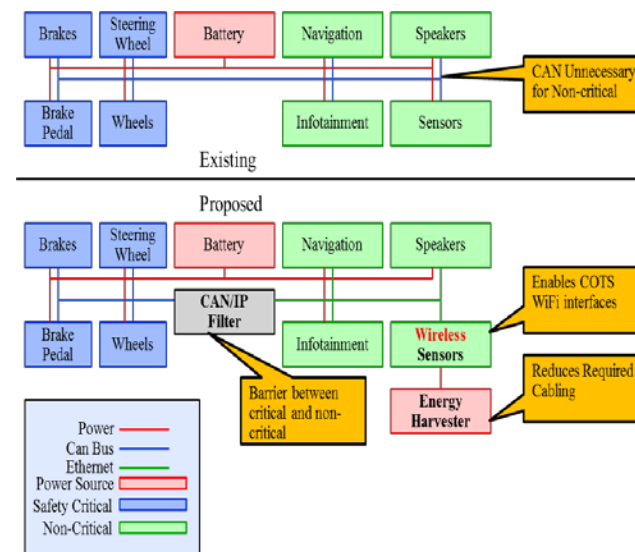
The current communications for today's automobiles are all connected through the CAN bus. Some have suggested replacing the CAN bus with Ethernet and an IP protocol, but this is unlikely to provide the low latency required for safety critical systems. This project will develop a hybrid system of CAN and IP (Ethernet and Wireless) connected devices.

Objective

- Design and implement proof of concept CAN/IP hybrid system
- Show feasibility of wireless sensors with energy harvesting
- Show cyber resilience enabled by CAN/IP filter

Payoff

- Separate safety critical systems from non-critical
- Reduction in cost of non-critical systems
- Easy interfacing with existing IP devices
- Reduction in cabling to wireless sensors



Deliverables

1. Monthly Technical report
2. Final Report
3. Hardware demonstration of CAN/IP(wireless) system

Automotive Key Fob Cryptanalysis

Description

- Many car manufacturers utilize rolling-codes for their key fobs, which change the encryption of the data transmitted between the key fob and the car each time an action is performed.

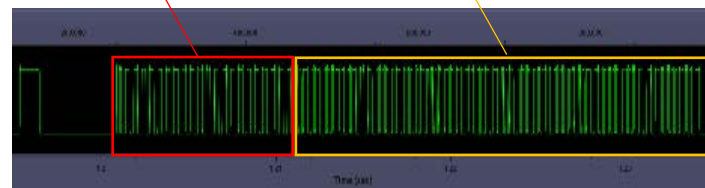
Objective

- Utilize cryptanalysis algorithms to determine how susceptible a car's rolling codes are to attack.
- Based on the results of these algorithms, provide insight on how to improve the security of these rolling codes.

Payoff

- Will determine how vulnerable key fob's rolling codes are as a function of make, model, and/or year.
 - Potential Vulnerability: an attacker could eavesdrop on a target's key fob and use cryptanalysis approaches to gain access to the car at will or spoof the key fob.
- Provide potential suggestions to improve a car's rolling code from a cryptanalysis perspective based on the results of this work.

Preamble Encrypted Data (using a rolling code)



**Key Fob's UHD Response
given a Door Unlock Button Press**

Deliverables

- Report on the survey of the characteristics of car rolling codes as a function of make, model, and/or year.
- Cryptanalysis software that can be used to attack a car's rolling code.
- Demonstration of any developed algorithms as well as a report outlining potential improvements to key fob security based on the outcome of the work.

Cellular Backhaul Threat Surface Analysis

Description

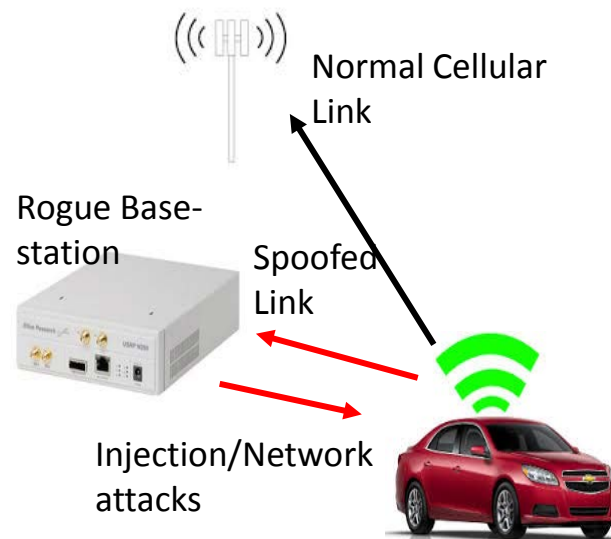
Many manufactures include cellular backhaul links in their vehicles to provide the connectivity required for systems such as OnStar. There is a possibility of these systems connecting to rogue base stations and those links being used to compromise the system.

Objective

- Determine the feasibility of hijacking the cellular communication link with a spoofing attack against the vehicle using a software defined rogue base station
- Vulnerability analysis of the embedded system supporting remote access. Run a penetration test on the component's operating system.

Payoff

- Determine the feasibility of hijacking the cellular link with a spoofing attack
- Vulnerability analysis of the interface between the vehicle's subsystems and the backhaul
- Determine the level of access to critical systems if the cellular system can be compromised.
- Proposed solutions to firewall the cellular interface from network intrusion.



Deliverables

1. Vulnerability analysis of the components providing the cellular backhaul connection for the vehicle
2. Solutions to secure vehicle against rogue base-station attacks and techniques to isolate critical components.

Description

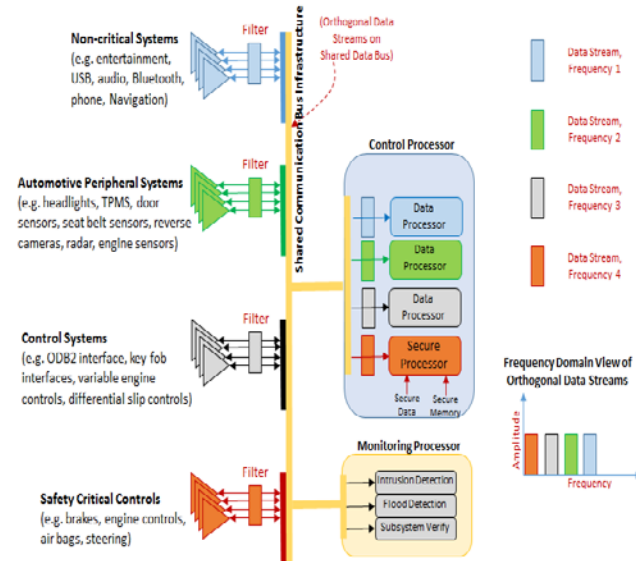
Many automotive hacks exploit the shared messaging structure of the CAN bus, yet many security measures have the potential to add unacceptable latency or design complexity. Transitioning the CAN bus to a frequency channelized bus where each channel has a specific security level (similar to multi-level secure DoD systems) enables robust new security mechanisms without latency or complexity impacts. (VT patent pending)

Objective

- Validate concept for a channelized CAN bus in a lab environment and perform targeted validation on a live vehicle (year 1).
- Demonstrate improvements against known hack attempts on a live vehicle and develop a system-wide framework to quantify security levels, costs, and benefits (year 2).

Payoff

- Transitioning to a multi-level secure messaging architecture in automotive systems offers significant improvements to the robustness of the core infrastructure. It also reduces the risk of integrating emerging technologies into vehicular systems, since impacts on life-critical systems are prevented by design.



Deliverables

1. Monthly Technical reports
2. Year 1 Interim Summary Report
3. Simulation and hardware demonstrations to show proof of concept (~quarterly)
4. Final Report

Description

Cyptosystems often concentrate on ensuring confidentiality, integrity, authentication, authorization, and nonrepudiation but cyber physical systems also have the necessity of understanding the context of a request. Transactional security takes into account the context of a request and applies acceptance/rejection based upon the situation.

Objective

The goal is to develop transactional security authorization into real-time serial communications of vehicular cyber physical systems without compromising real-time operation and with minimal impact to data overhead and computational resources.



Payoff

- Improve security posture of cyber physical systems using authorization mechanisms well-suited for real-time embedded serial communications that are not Enterprise IT Security wrappers.
- Adds context-ware security mechanisms that prevent authorized behavior during unauthorized situations.
- Establishment of an IEEE and/or RFC standard for industry wide adaptation and plug-and-play.

Deliverables

1. Monthly Technical report
2. Transactional Security Simulation & Algorithms (Yr. 1)
3. Transactional Security Laboratory Evaluation (Yr. 2)
4. Final Report consisting of an RFC/IEEE Standard Document for submittal for industry review and acceptance

Any Questions?

- Thank you for your time
- Kevin Heaslip
Associate Professor
Virginia Tech
kheaslip@vt.edu
540-231-2362



Hume Center for National Security and Technology



Virginia Information Technologies Agency



COV Security Requirements 101

Joy Young

Information Assurance Analyst





Agenda

- IT Security Audit Plans
- IT Security Audit Reports
- Corrective Action Plans/Quarterly Updates
- Business Impact Analysis
- Risk Assessment Plans
- Risk Assessments



IT Security Audit Plan

- Submitted annually
- Approved by Agency Head
- Should be based on the BIA
- Include all **sensitive** applications
- Sensitive applications must have completed/planned audits at least once every 3 years

TIP: Application names on the plan should agree with the application names in Archer



IT Security Audit Plan

- IT security audit plan can be added in Archer

AP-221052 IT Security Audits

NEW COPY SAVE EDIT DELETE

RELATED RECALCULATE EXPORT

First Published: 12/18/2013 10:37 AM Last Updated: 11/15/2017 2:37 PM

GENERAL INFORMATION

Audit Plan ID: AP-221052

Agency: [Virginia Information Technologies Agency](#)

Agency Submission Status: **Submitted**

Date Audit Plan Submitted: 11/15/2017

Number of Audits Past Due: 0

Review Comments:

CSRM Approval: **Approved**

Date Audit Plan Approved: 11/15/2017

Previous Audit Plan Expiration Date: 12/31/2016

Percentage of Audits Complete: 59 %

3 Year Period Start Date: 1/1/2017

3 Year Period End: 2019



IT Security Audit Plan

- Scheduled audits can be added in Archer

Home | CSR Analyst Action Workspace | CSR Analyst Workspace | Risk Management | SHOW ALL | Search | Settings | Joy

AP-221052 IT Security Audits

NEW COPY SAVE EDIT DELETE

RELATED RECALCULATE EXPORT PRINT EMA

Domain Multiplier: 1

Most Current AP: Yes

Inherited Record Permissions: EM: Admin
EM: Read Only

IT Security Audit Plan Access | View Access History |
History:

SCHEDULED IT SECURITY AUDITS

Add New

Scheduled Audit Tracking ID	IT Systems Scheduled to Audit	Scheduled Audit Description	Scheduled Audit Completion ▼ 1	Actual Audit Completion ▼ 2	All Audits Complete	CSRM Review Status
SA-226914	VITA Architecture Review		6/30/2018		No	Approved
SA-226909	Consolidated Personnel Information Repository (CPIR)		6/30/2018		No	Approved
SA-226907	VITA Security Asset Inventory	Per Audit Plan - Archer	6/30/2018		No	Approved



IT Security Audit Plan

Date of submission	
--------------------	--

Agency Information	
Agency Name	
Agency Acronym	
Agency Number	

Contact Information	
Name	
Title	
E-mail	
Phone	

IT System Acronym *	IT System Name	Planned Auditor	Date Last Audited (MM/YY)	Scheduled Audit Completion Date (Minimum once every 3 years)			Areas for Special Emphasis and Additional Audit Requirements
				20xx (MM/YY)	20xx (MM/YY)	20xx (MM/YY)	



IT Security Audit Report

- Follow GAGAS Yellow Book or IIA Red Book Standards
- Submit audit report to Commonwealth Security
- Followed by a corrective action plan

Tip: The audit standard that was used should be stated clearly in the audit report



Corrective Action Plans/Quarterly Updates

- Submitted within 30 days of issuing the final audit report
- Updated corrective action plan must be submitted quarterly until all corrective actions are completed
- Must have evidence of agency head approval

Tip: Make updates in Archer where possible



Corrective Action Plans/Quarterly Updates

Updates to findings can now be made in Archer

Response

▼ REMEDIATION RESPONSE UPDATES

Quarter Date Applied ▲

CSRM Approved

Remediation Response Update

Revised Expected Due Date

No Records Found



Corrective Action Plans/Quarterly Updates

Template

Corrective Action Plan and *IT Security Audit Quarterly Summary* Template

PURPOSE: This Plan describes IT Security Audit findings; documents responsibility for addressing the findings; and describes progress towards addressing the findings. Provide enough information to enable the reader to understand the nature of the finding, the impacts, and the planned remedy.

Submission Date:	
------------------	--

Audit Name:						
IT System Names(s)						
Audit Finding Number	SEC501 Control Number	Summary	Agency Concurs ¹	Planned Corrective Action or Mitigating Controls ²	Responsible Person(s)	Status ³



BIA

- Every application must be associated with a business process
- Include required information



BIA

Budgeting Business Processes

NEW COPY SAVE EDIT DELETE

◀ Record 9 of 130 ▶

RELATED RECALCULATE

First Published: 4/28/2016 11:01 AM Last Updated: 12/27/2017 10:28 AM

▶ ABOUT

▼ GENERAL INFORMATION

First Published: 4/28/2016 11:01 AM

Risk Rating:

Process ID: BPID-251049

Process Name: Budgeting

Agency: [Virginia Information Technologies Agency](#)

Compliance Rating: **Not Rated**

Business Purpose: To develop and execute internal and external budgets for VITA so that financial resources are obtained and allocated and expended most strategically, ef

Notes:

Agency Submission Status: **Submitted**

Agency Submit Date: 11/30/2017

CSRM Review Status: **Approved**

CSRM Approval Date: 12/27/2017

Last Updated: 12/27/2017 10:28 AM

Initial Creation Date: 4/28/2016

Details

Business Impact Analysis

Mappings

▼ PERSONNEL

Business Owner: Jamev Doran



BIA

Details

Business Impact Analysis

Mappings

▼ BUSINESS IMPACT ANALYSIS

Operational Impact

Description:

Impact to Confidentiality: ●

Impact to Customer Service: ●

Impact to Safety: ●

Recovery Time Objective: 720 Hours

Manually Performed: No

Impact to Finances: ●

Impact to Life: ●

Regulatory Impact: ●

Recovery Point Objective: 720 Hours

Legal Impact: ●


► ATTACHMENTS



BIA

NO RECORDS FOUND

▼ APPLICATIONS

Application ID	Application Name ▲	Agency	Criticality Rating
APPID-205814	<u>Cardinal Interface</u>	<u>Virginia Information Technologies Agency</u>	



Risk Assessment Plan

- Submitted annually
- Include all **sensitive** applications
- Sensitive applications must have completed/planned audits at least once every 3 years
- Agencies can add RAP and SRA in Archer

TIP: Application names on the plan should agree with the application names in Archer



Risk Assessment Plan

RAP247465 IT Risk Assessment

NEW COPY SAVE EDIT DELETE

RELATED RE

First Published: 1/27/2016 12:03 PM Last Updated: 12/13/2017 2:22 PM

GENERAL INFORMATION

Risk Assessment Plan ID: RAP247465

Agency: [Virginia Information Technologies Agency](#)

Agency Submission Status: **Submitted**

Date Risk Assessment Plan 10/31/2017
Submitted:

Number of Risk Assessments 0
Past Due:

CSRM Approval: **Approved**

Date Risk Assessment Plan 10/31/2017
Approved:

Date Risk Assessment Plan 10/31/2018
Expires:

Percentage of Risk 67 %
Assessments Complete:

3 Year Period Start Date: 1/1/2018

3 Year Period End: 2020



Risk Assessment Plan

RAP247465 IT Risk Assessment

NEW COPY SAVE EDIT DELETE

RELATED RECALCULATE EXPORT PRINT

VITA ITRISK Assessment Plan opt-out (2).xlsx 12 20 20279
2016.xlsx

.xlsx

8/10/2017 11:23:35 AM

SCHEDULED RISK ASSESSMENTS

Scheduled Risk Assessment Tracking ID	Systems Scheduled for Risk Assessment	Scheduled Risk Assessment Description	Scheduled Risk Assessment Completion ▼ 1	Actual Risk Assessment Completion ▼ 2	All Risk Assessments Complete	CSRM Review Status
SRA247466	Comprehensive Billing - MBA - Direct Bill Mainframe Billing System Consolidated Personnel Information Repository (CPIR) Contact Repository (People System) Peoplesoft Financials zz-Retired: Personnel Action Application (PAA) (retired, not in use) zz-Retired: Sharepoint (VI) (Retired, No Longer in Use)	VITA Risk Assessment for listed application systems.	12/31/2018		No	Approved



Risk Assessments

- Should be conducted as needed, but not less than once every 3 years



Risk Assessment

IT System Name	Risk ID	Confidentiality	Integrity	Availability	Risk Assessment Completion Date (MM/YY)	Risk Vulnerability Family (Ref. SEC 501)	SEC 501 Control ID (e.g. AC-1, RA-5, etc)



Thank you



Virginia Information Technologies Agency



Upcoming Events





Future ISOAG

March 7, 2018 @ CESC 1:00-4:00

Speakers: Tom Arruda, IT Risk Management, Dominion Energy

J. Wesley Kleene, VITA

Bill Freda, VITA

John Craft, VITA

ISOAG meets the 1st Wednesday of each month in 2018



Registration is Now Open

"2018 COVA Information Security Conference: "Expanding Security Knowledge"

April 12 & 13

Location: Altria Theater

<https://wm.irisregistration.com/Site/VITA2018>

Registration Fee - \$175

***Contact CommonwealthSecurity@vita.virginia.gov for more
information**



Conference Keynote Speakers

Adam S. Lee,
Special Agent in Charge
Federal Bureau Investigations (FBI)
Richmond (Division) Field Office

Dr. Deanna D. Caputo
Principal Behavioral Psychologist
Human Behavior and Cybersecurity Capability
Steward
The MITRE Corporation

ADJOURN

THANK YOU FOR ATTENDING

