Virginia Information Technologies Agency

Welcome and Opening Remarks

Mike Watson

June 3

June ISOAG AGENDA

- Mike Watson, Opening & Welcome Remarks
- Kathy Bortle, VITA- Foreign VPN Logins
- Kevin Heaslip, VT - Information Security for Connected and Automated Vehicles
- Arlyn Burgess, UVA School of Data Science- Data Science Opportunities and Barriers: The Power of Partnership”
- Alan Gernhardt, VA Freedom of Information Advisory Council - Public Records
- Darrell Raymond, ATOS- Managed Security Services

Foreign VPN Logins

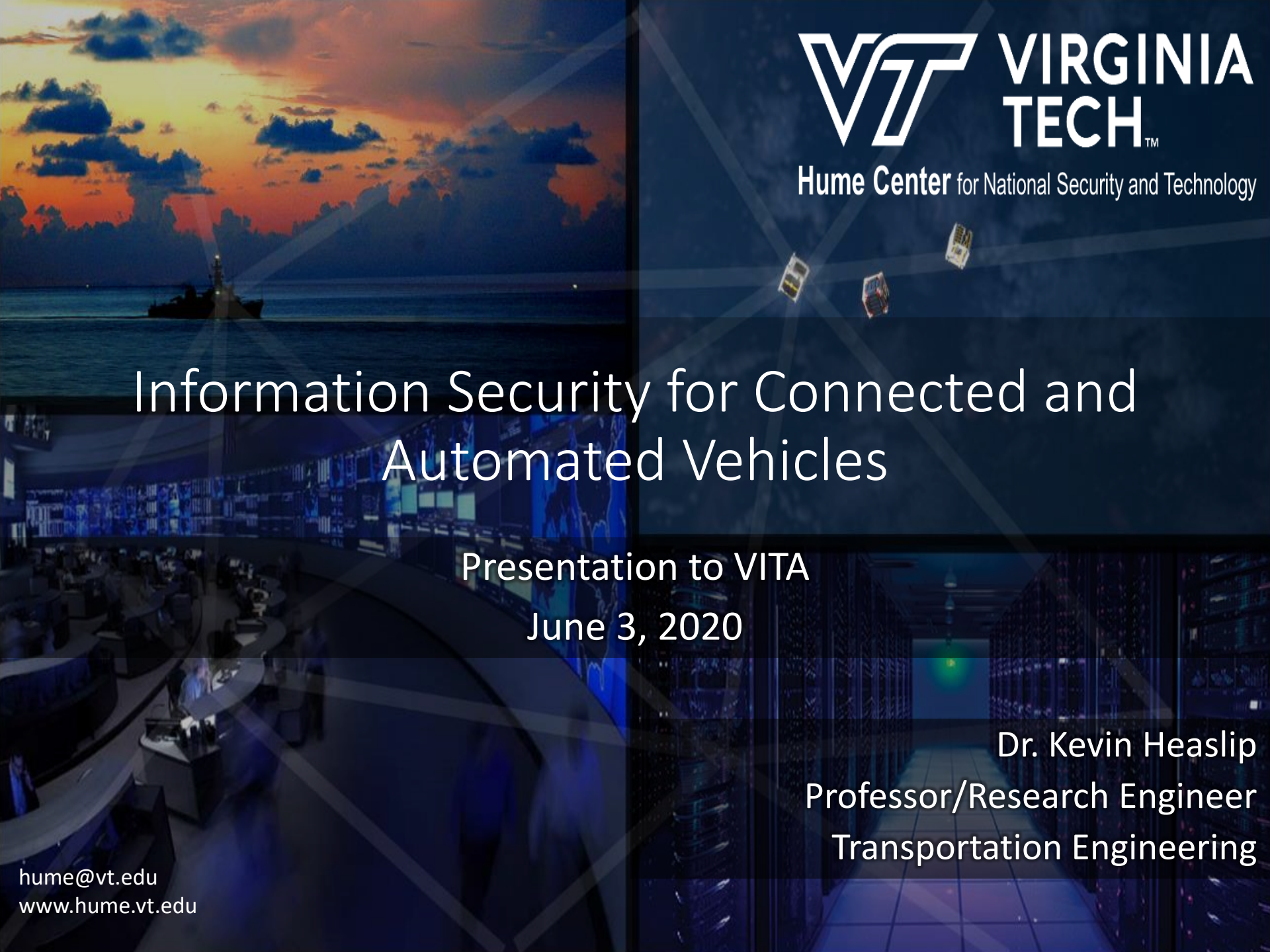
For employee travel (prior to travel)

- Name of the individual traveling
- The travel dates
- Travel location(s)

For contracts with companies outside the US (upon contract signing)

- Name and Location of the company supporting the agency
- List of employees on the contract using VPN
- Expiration date of the contract
- Periodic review for staffing changes

Link to KSE Knowledgebase Article:
https://vccc.vita.virginia.gov/nav_to.do?uri=%2Fkb_view.do%3Fsys_kb_id%3D4a737ddd1b741054b658113d9c4bcb7b%26sysparm_rank%3D1%26sysparm_tsqueryId%3D3b5faf8f1bb89050a7f3ed7bbc4bcbc3



VIRGINIA TECH™

Hume Center for National Security and Technology

Information Security for Connected and Automated Vehicles

Presentation to VITA

June 3, 2020

Dr. Kevin Heaslip
Professor/Research Engineer
Transportation Engineering

hume@vt.edu
www.hume.vt.edu

Introduction

- 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:

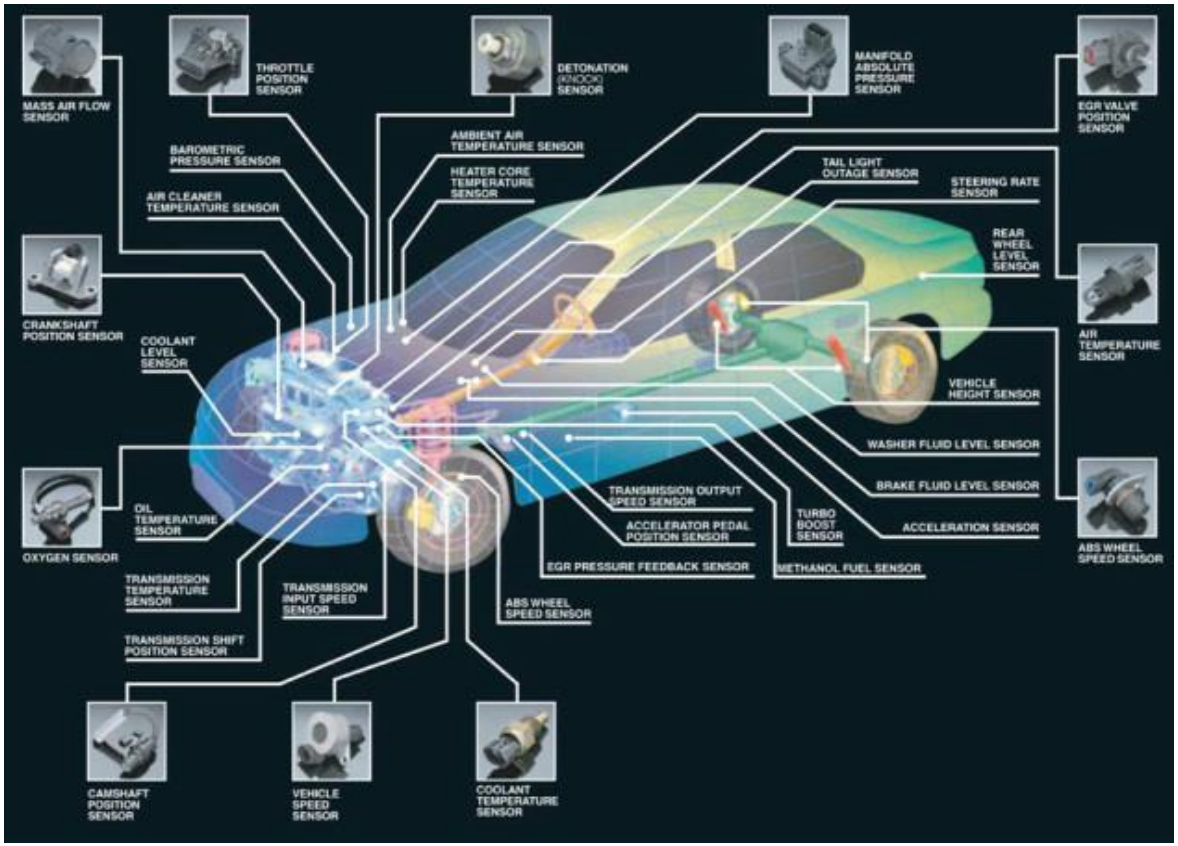
Computerization of the Automobile

- 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."

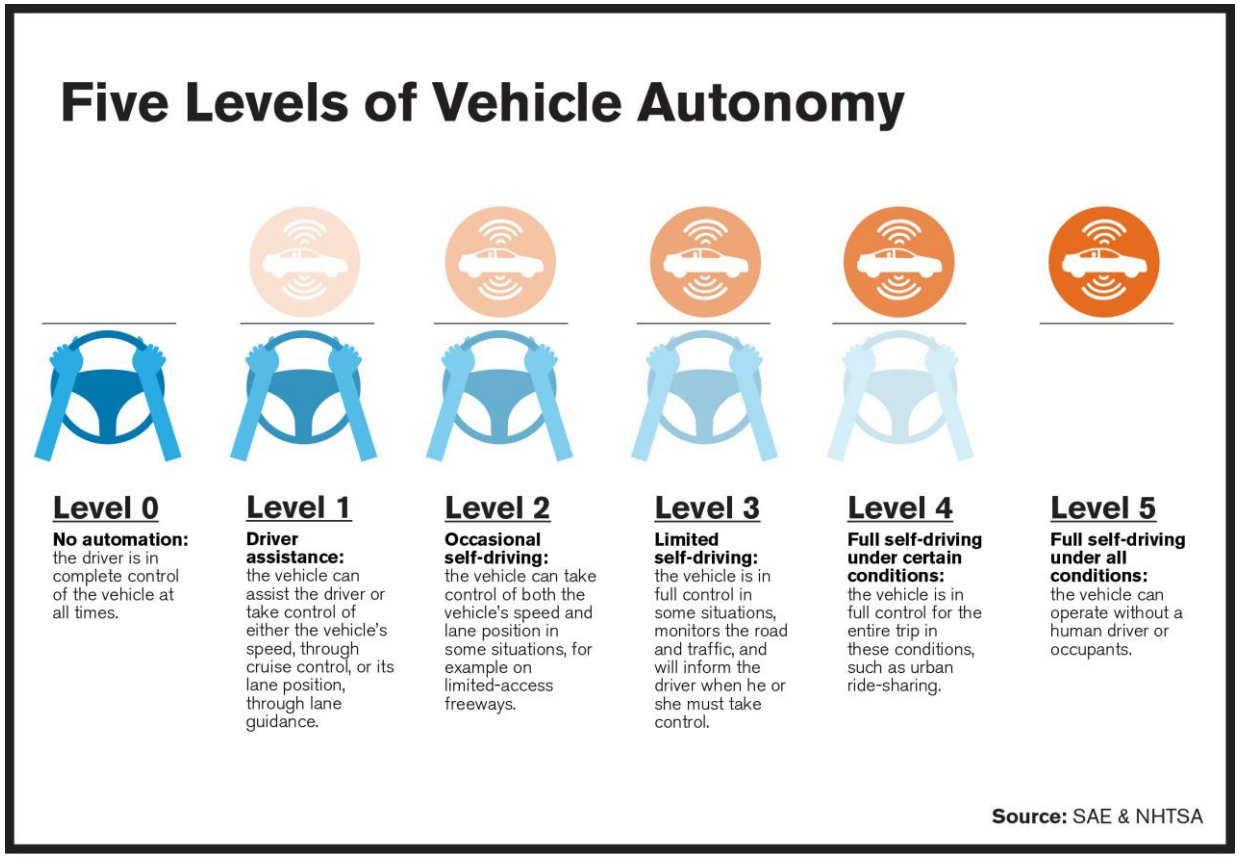
- GM CEO, Mary Barra

Definitions

- Autonomous
  - "acting independently or having the freedom to do so"

- Automated
  - "convert (a process or facility) to largely automatic operation"
  - Automated Driving

Driver Automation Levels

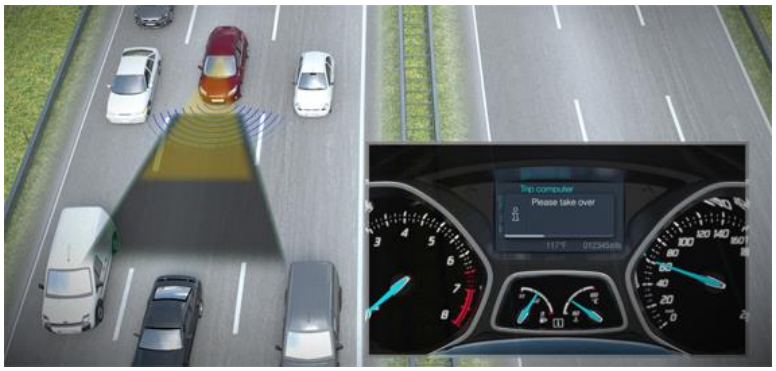


Automated Driving in Action

Google's Self Driving Car

Automation Available Today

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



Tesla AutoPilot

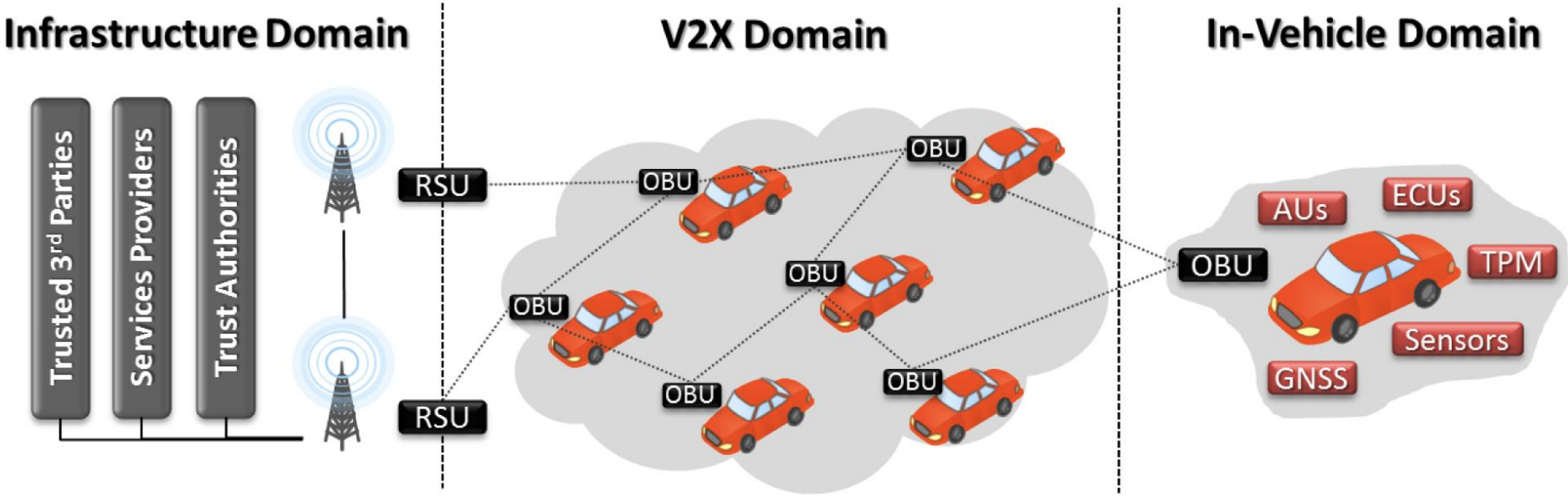
Use of Machine Vision

Automation Benefits/Challenges

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

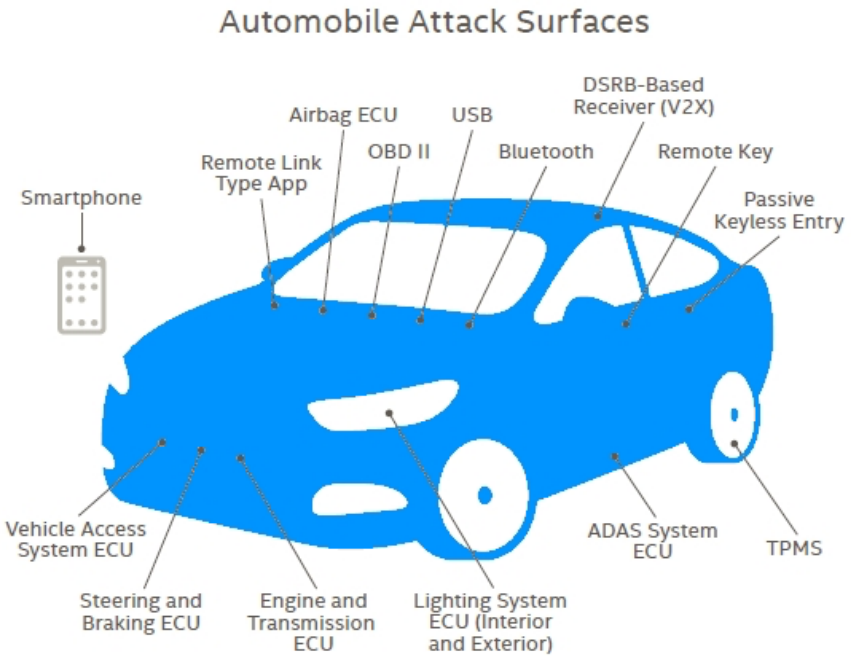
Communications Domains in Surface Transportation

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



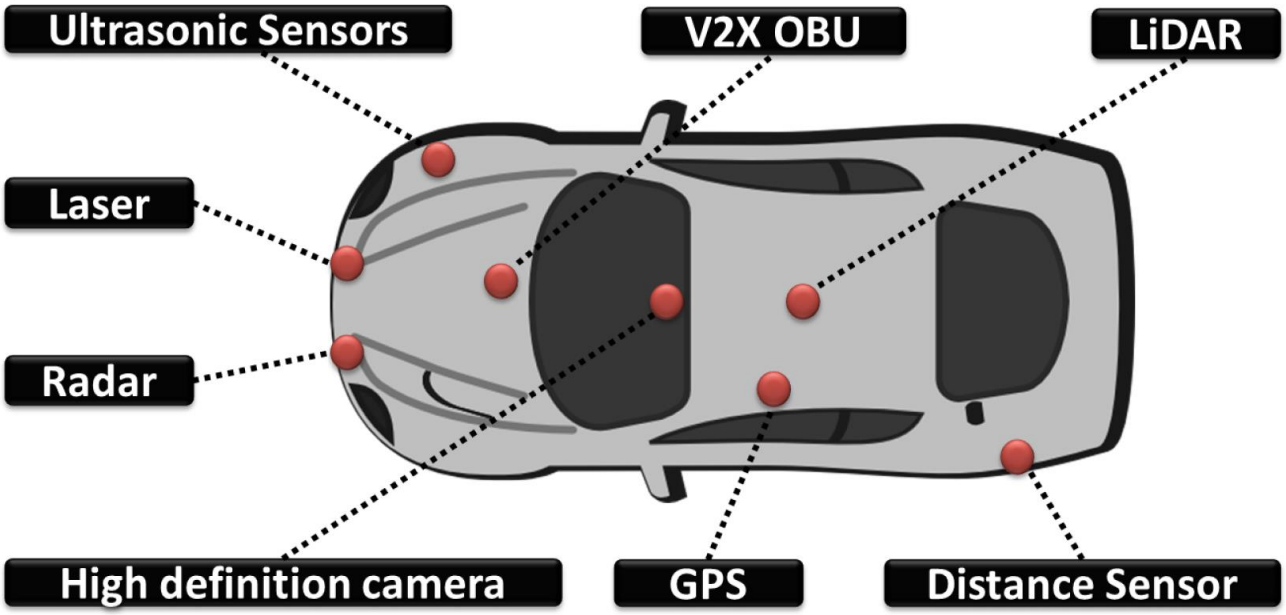
Potential Traditional Vehicle Vulnerabilities

- Vulnerabilities Include:
  - On-Board Diagnostic Security
  - Tire Pressure Monitor Security
  - Key Fob Security
  - Infotainment Security

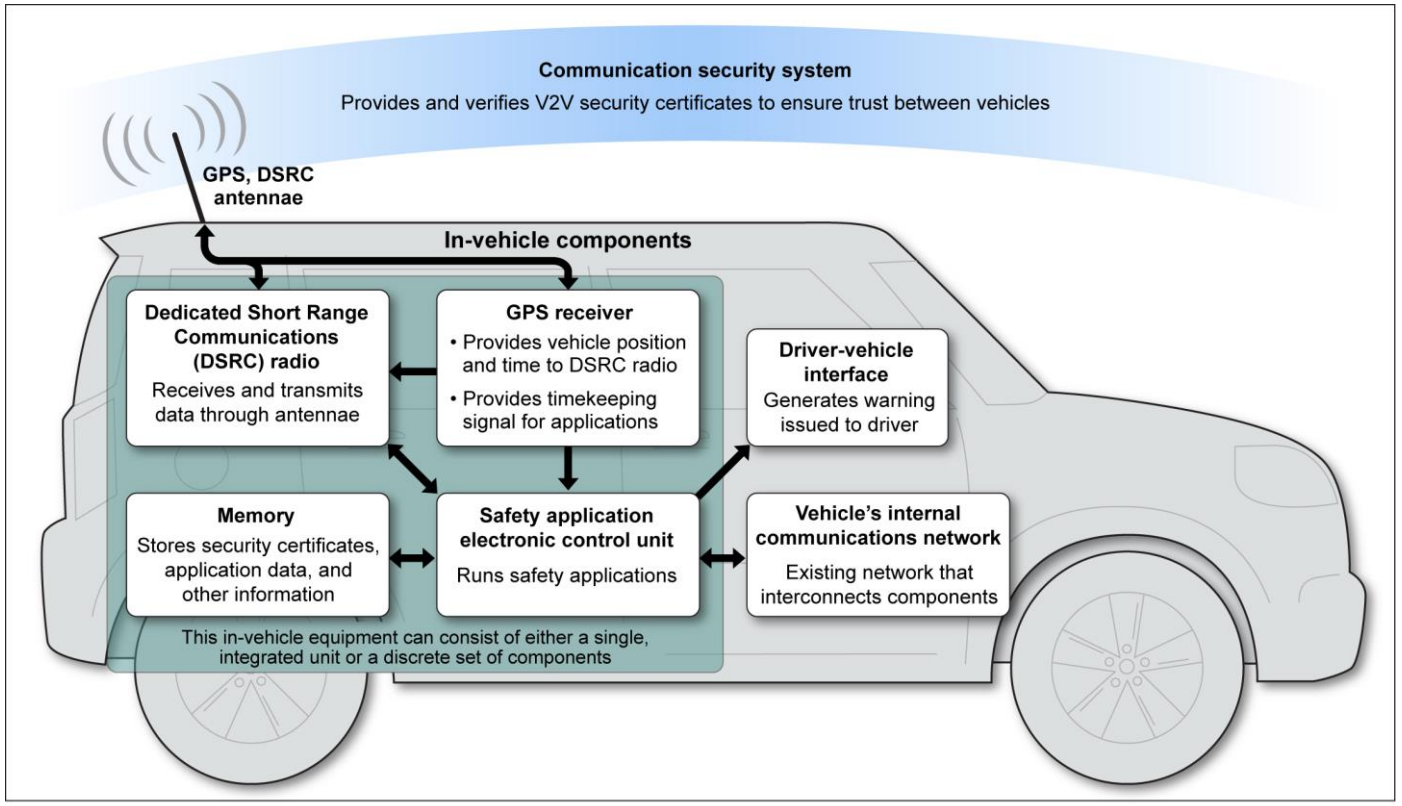


Advanced Vehicle Communication and Sensing

- 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.

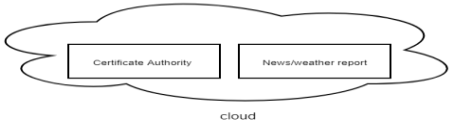


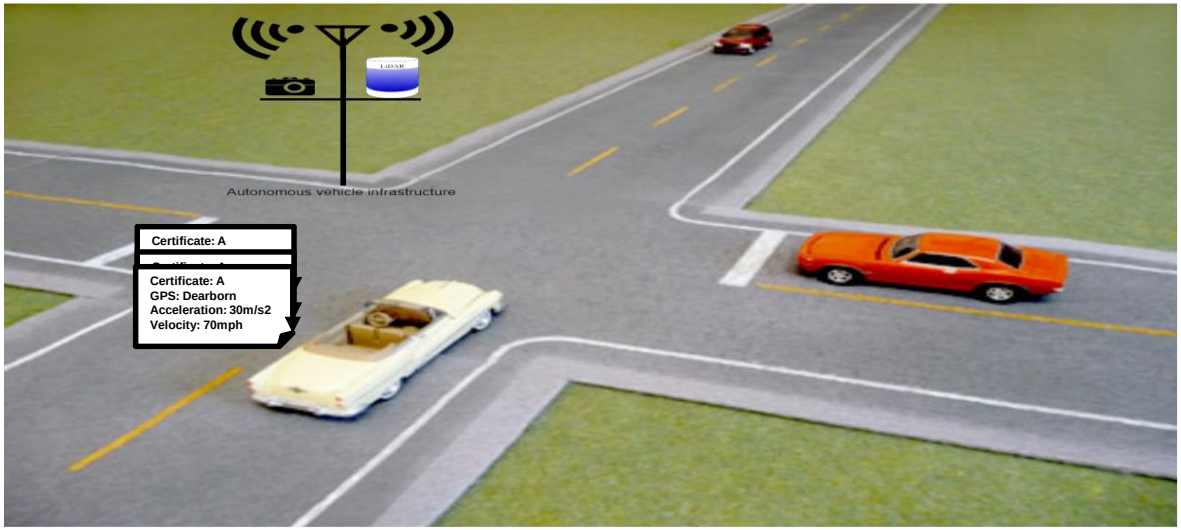
Attacks possible on next generation vehicles



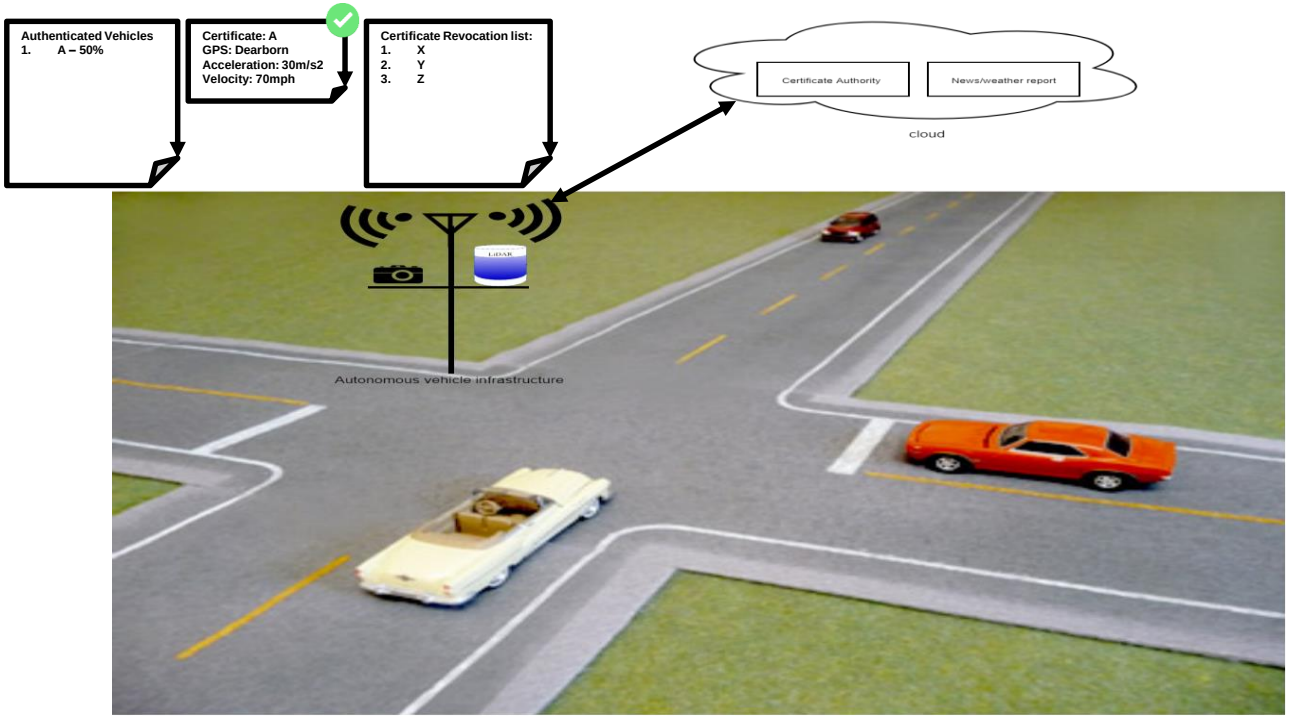
Sources: Crash Avoidance Metrics Partnership and GAO.

Problem statement: Why are we doing this research?

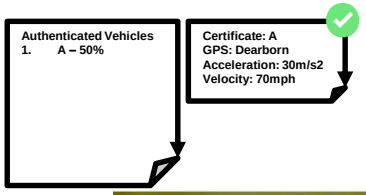


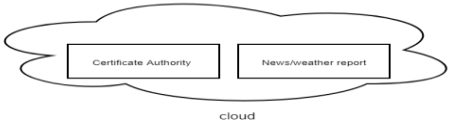


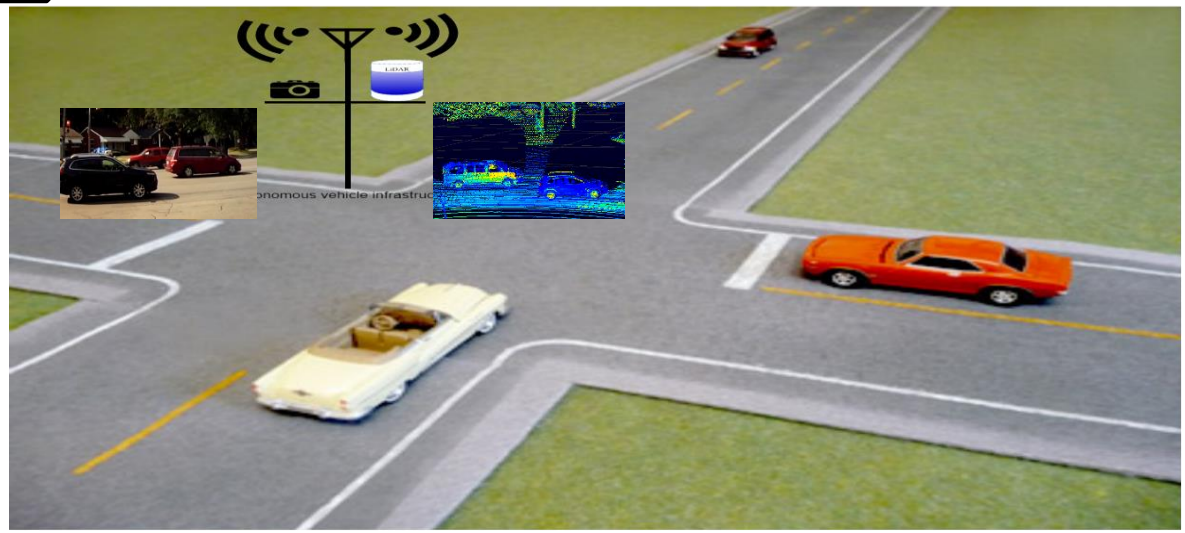
Problem statement: Why are we doing this research?



Problem statement: Why are we doing this research?

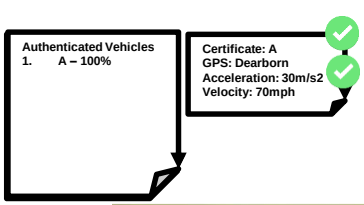


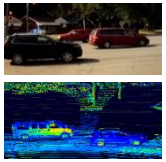


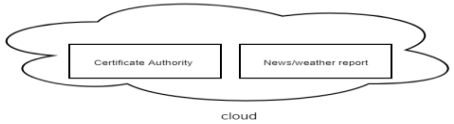


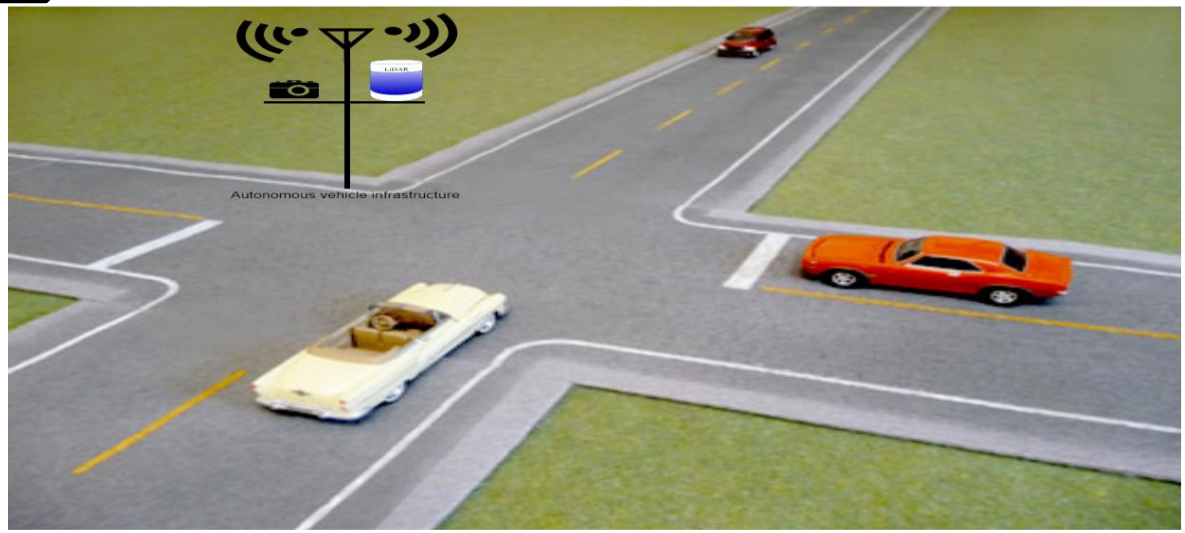
Problem statement: Why are we doing this research?

Is message a true representation of events?









INTERSECTION IMPACT ON DEGRADATION MODEL

1. Centralized

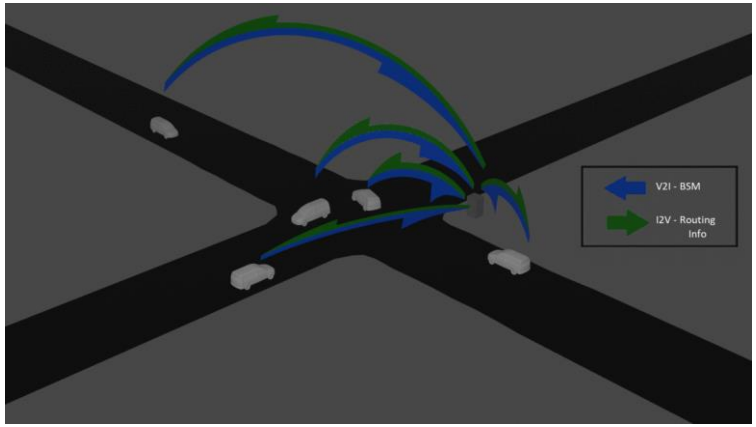
   - Communication and GNSS are most important
   - Sensor Degradation has minimal impact on model

2. Decentralized

   - Comm and GNSS still largest influences
   - Sensor Degradation more important, but still minor

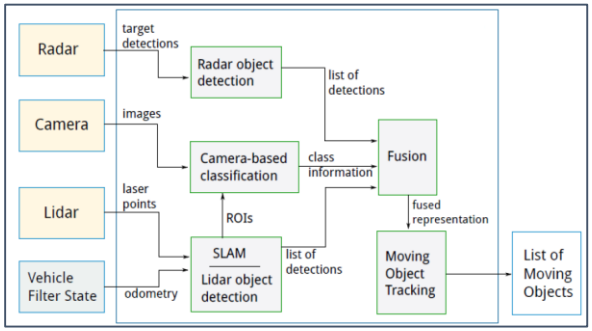
3. Communication Breakdown

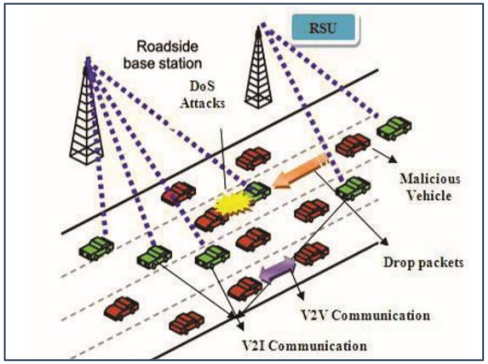
   - Best case scenario of this is still very poor
   - Extremely reliant on other sensors



AV ATTACKS & COUNTERMEASURES

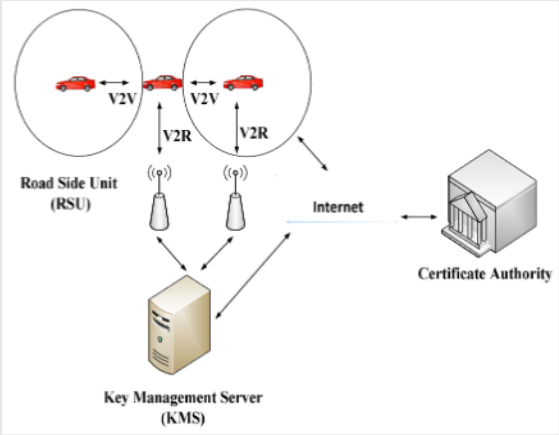
- Attacks (*Countermeasures*) by Sensor:
  - Camera
    - Vision Loss (*Angle diversity & Sensor fusion*)
  - Radar
    - Jamming and Spoofing (*Sensor Fusion*)
  - Lidar
    - Jamming and Spoofing (*Sensor Fusion & Machine Learning*)
  - GNSS:
    - Jamming and Spoofing (*Authentication & Signal Encryption*)
  - Communication:
    - Denial of Service (DoS)
      - Jamming, Flooding, & Blackhole
    - Message
      - Message Forgery, Replay Attacks, & Sybil
    - *Countermeasures*
      - *Cooperative Intersection Management*
      - *Frequency Hopping*
      - *Authentication with Timestamps*
      - *Pseudonyms*

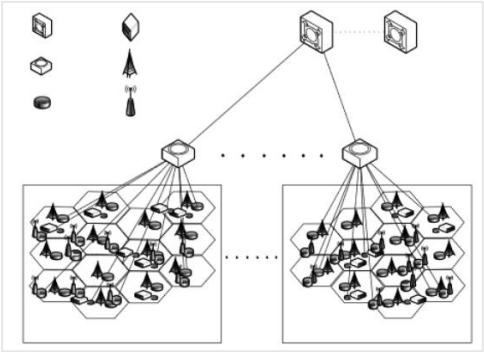




AV RESILIENCE CONCEPTS

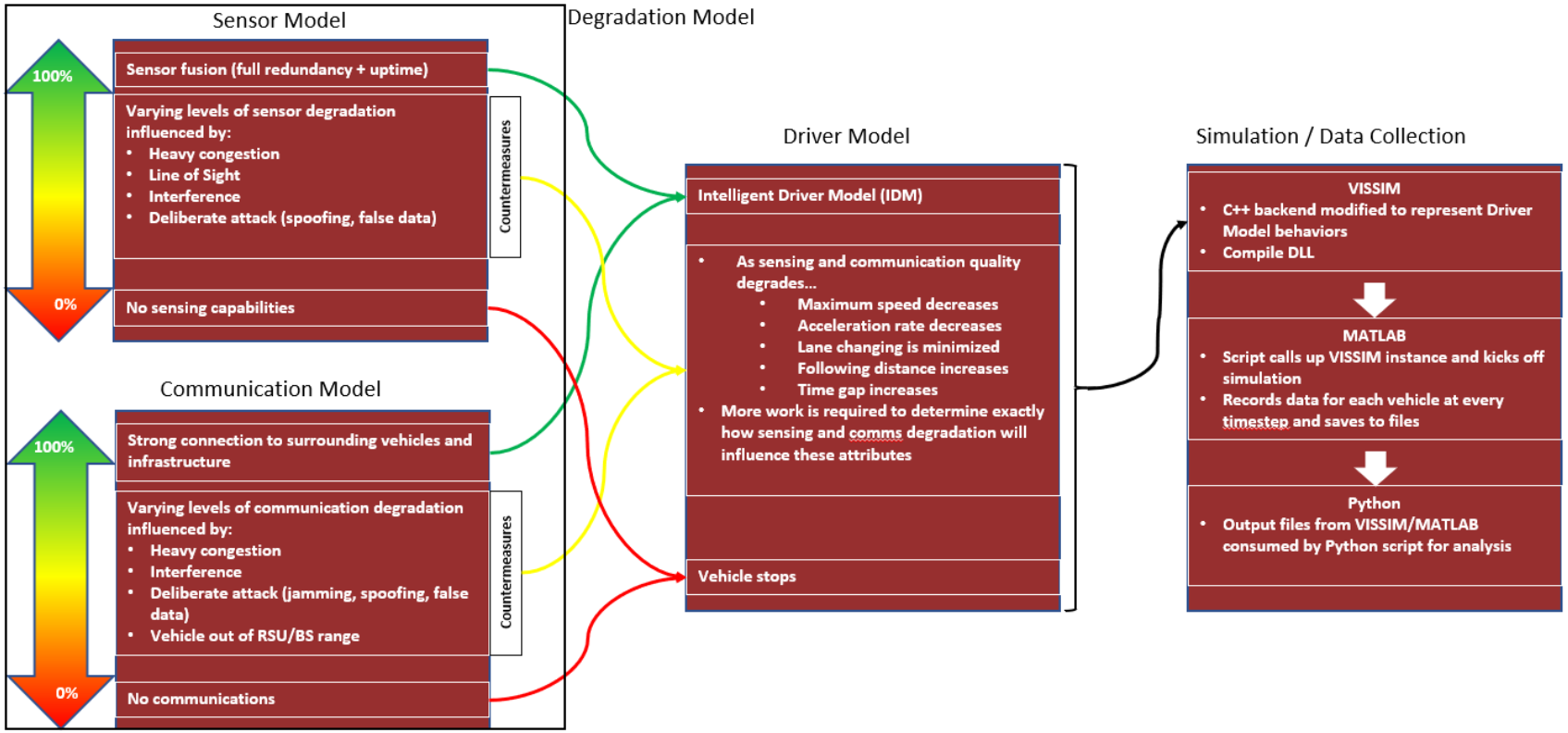
- Data Availability:
  - Sensor Fusion
  - Frequency Agility
  - Adaptive Coding
- Data Integrity and Authentication:
  - RF Fingerprinting
  - Key Management
- Network Optimization
  - Load Optimization
  - Autonomy Optimization: Cooperative Intersection Management





LINKING ATTACKS, COUNTERMEASURES, AND RESILIENCE CONCEPTS

Sensor	Attack	Countermeasure	Resilience Techniques	
Camera	Vision Loss	Sensor Angle Diversity	Sensor Fusion	
		Sensor Fusion		
Radar	Jamming	Sensor Fusion		
	Spoofing			
	Replay			
Lidar	Jamming	Sensor Fusion		
	Spoofing	Machine Learning Training		
GNSS	Jamming	Authentication	Key Management Authentication	Cooperative Intersection Management and Load Optimization
	Spoofing	Signal Encryption		
Comm	Jamming	Frequency Hopping	Frequency Agility	
	Flooding	Authentication	Key Management Authentication	
	Blackhole / Greyhole	Authentication		
	Message Forgery	Authentication		
	Replay	Authenticated Timestamps		
	Sybil	Pseudonyms	RF Fingerprinting	


Sensor Model
100%
0%
Sensor fusion (full redundancy + uptime)
Varying levels of sensor degradation influenced by:
• Heavy congestion
• Line of Sight
• Interference
• Deliberate attack (spoofing, false data)
No sensing capabilities
Countermeasures
Communication Model
100%
0%
Strong connection to surrounding vehicles and infrastructure
Varying levels of communication degradation influenced by:
• Heavy congestion
• Interference
• Deliberate attack (jamming, spoofing, false data)
• Vehicle out of RSU/BS range
No communications
Countermeasures
Degradation Model
Driver Model
Intelligent Driver Model (IDM)
• As sensing and communication quality degrades...
• Maximum speed decreases
• Acceleration rate decreases
• Lane changing is minimized
• Following distance increases
• Time gap increases
• More work is required to determine exactly how sensing and comms degradation will influence these attributes
Vehicle stops
Simulation / Data Collection
VISSIM
• C++ backend modified to represent Driver Model behaviors
• Compile DLL
MATLAB
• Script calls up VISSIM instance and kicks off simulation
• Records data for each vehicle at every timestep and saves to files
Python
• Output files from VISSIM/MATLAB consumed by Python script for analysis

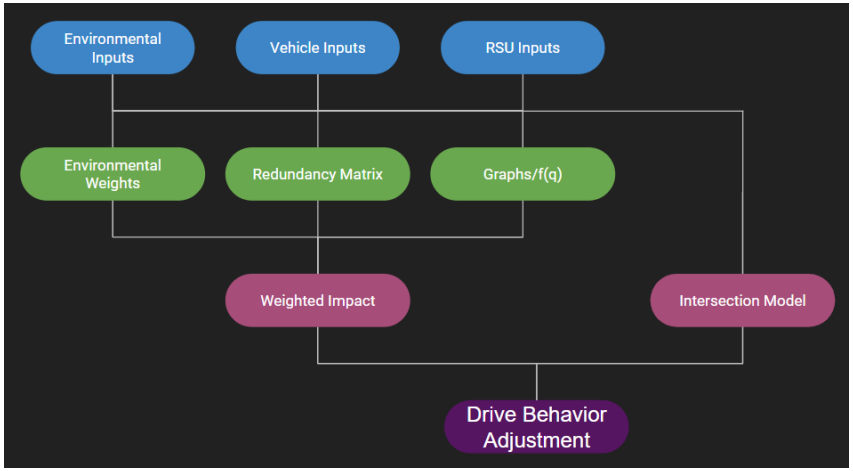
COMMUNICATION: DEVELOPMENT OF A VEHICLE OPERATIONS MODEL WITH REGARD FOR SECURITY

GOAL: To integrate security assessment in the operation of vehicles by building algorithms that change the vehicle state based upon security threats.

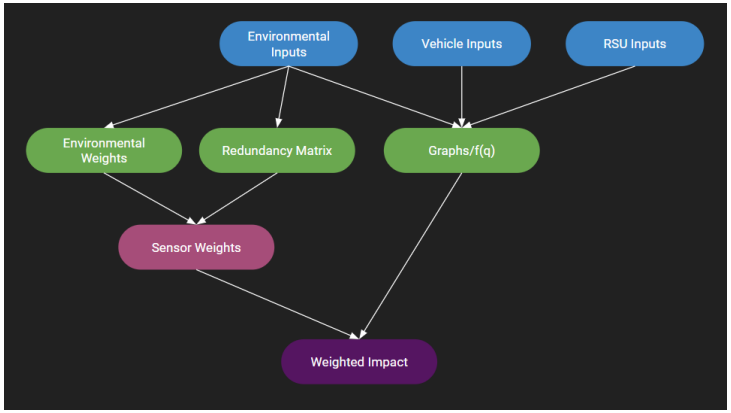
A. Uses the sensor inputs to determine the impact on the sensor data quality (*threat modeling/communication modeling*)
   - Based on environmental inputs such as visibility

B. Uses the V2I communication and GNSS inputs to determine modeling conditions (*scenario modeling*)
   - Centralized, Decentralized, or Communication Failure

C. The vehicle state model determines how the car will react based upon the *threat, communications, and scenario.*



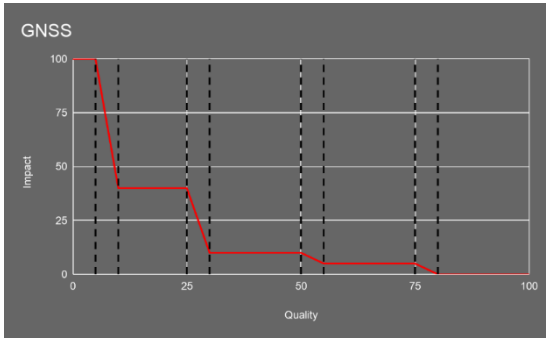
COMMUNICATION: SENSOR DEGRADATION MODEL



A. Sensor Weights
   - Adjustments for Density, Speed and Visibility
   - Includes an adjustment through the redundancy matrix which accounts for sensor fusion

B. Impact Graphs
   - Measurement of the impact occurring on each sensor based on the inputs provided

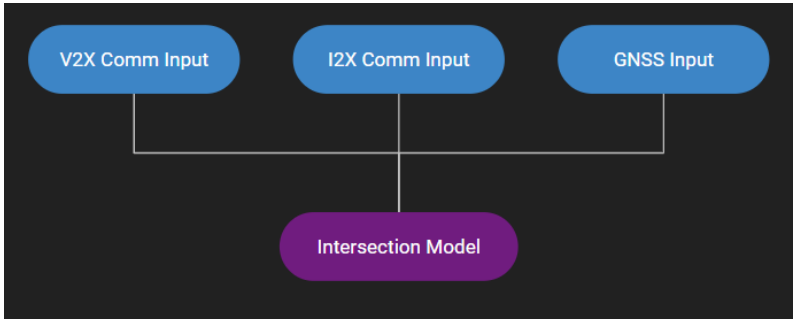
C. Weighted Impact
   - A product of the weights and impact values for each sensor



Impact Graph

COMMUNICATION: COMMUNICATION DEGRADATION MODEL

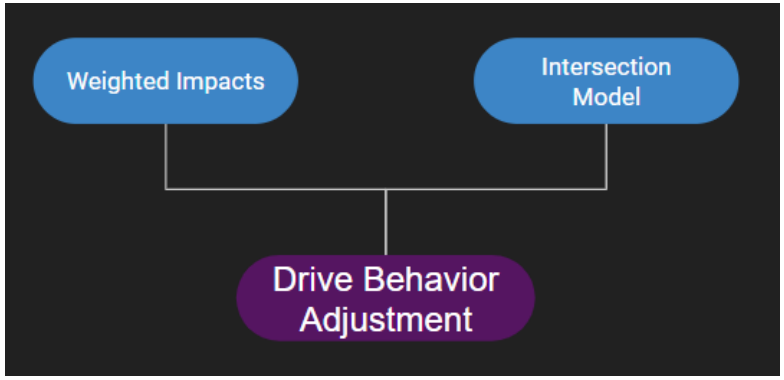
- Communication and GNSS inputs are used to determine which Vehicle Management Technique will be used.
- Centralized Intersection Management (CIM) has the highest priority and outputs
- Upon failure of the V2I communication, V2V is used
  - This reduces the ability to optimize slightly
- Failure of all communication or in GNSS leads to a 4-Way stop or graceful stopping of the vehicles.
  - Severe decrease in all vehicle operations



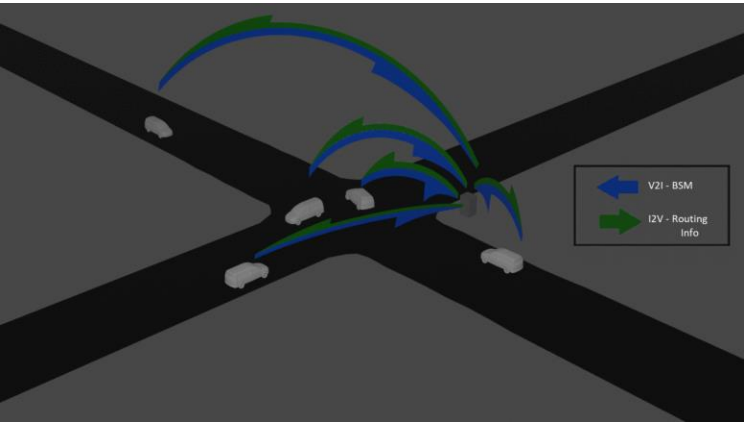
COMMUNICATION: VEHICLE STATE MODEL

GOAL: To understand the adjustments of vehicle operations needed when security threats occur and the most impactful countermeasures to implement.

- Once the intersection model has been selected, the weighted impacts are used to determine behavior adjustments
- Example
  - Under the 4-Way stop, radar is weighted the highest for determining speed due to it having the longest range to maintain a proper SSD



COMMUNICATION: COOPERATIVE INTERSECTION MODELING



	Centralized Intersection Manager (CIM)	Distributed Intersection Manager	Communication Failure
Description	Routing is coordinated through a centralized hub in a RSU	Routing is coordinated through a lead car, which is passed to another after leaving the intersection	Intersection transitions to a four-way stop
Requirements	V2I, I2V and GNSS data	V2V and GNSS data	Sensor Data
Benefits	• The most efficient form • Able to optimize for different parameters	• Second most efficient form • Minor optimizations possible	• Low reliance on communication or single sensors working correctly
Detriments	• Heavy reliance on many different systems working correctly	• Heavy reliance on a few systems working correctly • Unable to optimize as well as the CIM • Large cost to changing any planned vehicle routes	• Significantly less efficient than other two options • Reduction in safety

Any Questions?

- Thank you for your time

- Kevin Heaslip
  Professor
  Virginia Tech
  kheaslip@vt.edu
  540-231-2362


VIRGINIA
TECH™
Hume Center for National Security and Technology

SCHOOL of DATA SCIENCE

DATA SCIENCE OPPORTUNITIES AND BARRIERS: THE POWER OF PARTNERSHIP

ARLYN BURGESS
CHIEF OF STAFF
UVA SCHOOL OF DATA SCIENCE
ARLYN.BURGESS@VIRGINIA.EDU

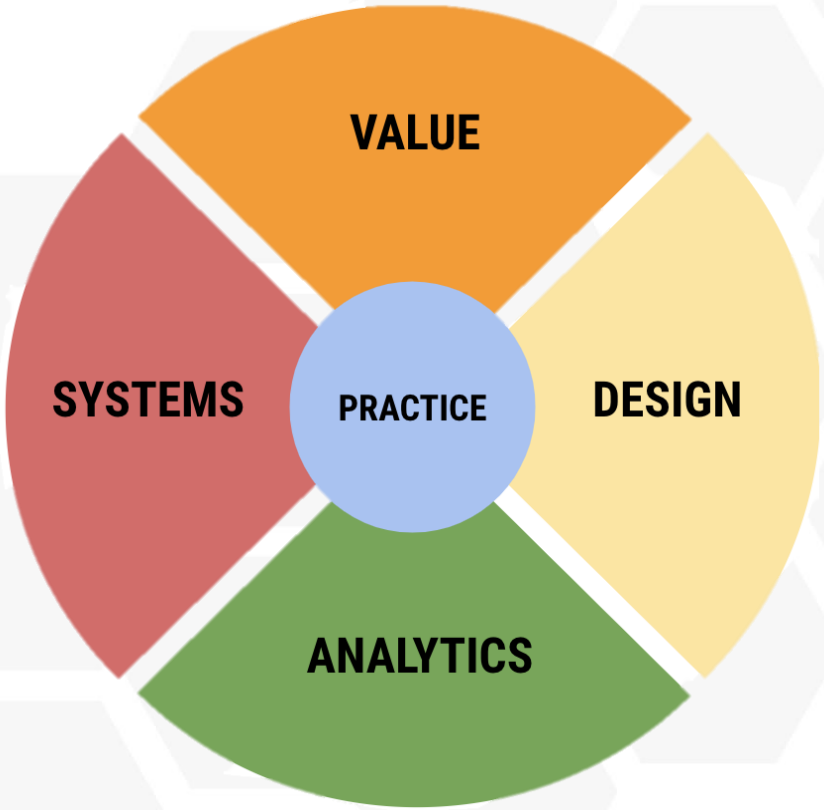
UVA | SCHOOL of DATA SCIENCE

DATA SCIENCE IS…

an interdisciplinary field that uses scientific methods, processes, algorithms and systems to extract knowledge and insights from data in various forms, both structured and unstructured. Data science sits at the intersection of computer science, statistics, mathematics and information science. Conducting data science transcends traditional disciplinary boundaries to discover new insights, often by combining disparate datasets that would not likely be brought together otherwise.

DATA SCIENCE IS...

UVA | SCHOOL of DATA SCIENCE



UVA | SCHOOL of DATA SCIENCE

A SCHOOL WITHOUT WALLS

Be ethical in data science and its application in the world and in the decisions it drives
Be constantly strategic and nimble given a fast-changing supply chain while remaining aligned with the UVA strategic plan
Be sustainable do not overreach
Be interdisciplinary engaging with scholars across the University and beyond
Be diverse, accessible and open with data, models, and structure
Be team not individually driven in all things
Strive for quality not quantity in education & research—know what you want to offer
Be innovative and translational through new forms of engagement with the private sector, government, NGOs, local, state, national and international partners

UVA | SCHOOL of DATA SCIENCE

DATA SCIENCE EDUCATION

Master of Science in Data Science (launched 2014)

- Integrated curriculum developed in consultation with practicing data scientists that leads to a real-world capstone project
- Core courses in analytics and computation
- Capstone projects focused on various disciplines, e.g. business, healthcare, policy, and social good
- Distinguished guest lecturers, case studies, proposal-writing, and presentation
- Course in data ethics, law, and policy
- Dual Degree programs (launched 2017)
  - MBA/MSDS
  - MD/MSDS
  - PhD/MSDS (currently with Nursing)

UVA | SCHOOL of DATA SCIENCE

DATA SCIENCE EDUCATION CON

Undergraduate Minor in Data Science (approved: 20-21)
Undergraduate Major in Data Science (estimated: 23-24)

- Engages with the conceptual and structural framework of data science
- Encourages depth in relation to domain areas
- Leverages University expertise
- Follows the model of systems, analytics, design, and value in course/curriculum development
- Includes real-world projects for the implementation of data science

PhD in Data Science (estimated: 21-22)

- Research focus—integrated with other schools
- Rotations in domain areas
  - Lab rotations
  - Industry rotations
- Not geared solely to academia
- Strong mentoring component
  - Dual mentors

UVA | SCHOOL of DATA SCIENCE

DATA SCIENCE RESEARCH & SERVICE

SAMPLE MSDS CAPSTONE PROJECTS

Using Adversarial Learning Models to Predict a Fraudster's Next Move
Preventing Credit Card Fraud

Detecting and Minimizing Network Intrusions
Using real-time network traffic data from UVA to test intrusion detection (BIG data!)

Reducing Repeat Patient Visits to the Emergency Room
Analyzing five years of data to help a hospital predict extraneous Emergency Department visits

COVID-19 DATA SCIENCE RESEARCH & SERVICE

Wikipedia: Increasing Accessibility to Health Information Around the World
Improving the most consulted source of information on the virus

Publication on the study and research of COVID-19
Scholia connecting and collating resources on the virus

Virginia Registry of Residents Providing Data on COVID-19
iTHRIV initiative to centralize valuable health information related to COVID-19

COLLABORATION

UVA | SCHOOL of DATA SCIENCE

Government

- Governor's Data Internship Program (Capstone Projects)
- Governor's Data Analytics Summit/Pre-Summit
- State-level Committees and Boards on Data Governance, Analytics & More
- Open Data Advisory Group—Open Data Portal in Charlottesville
- Representation/Support on Statewide Legislation for Data Governance

Industry

- Data Science Board
- Capstones
- Hosting/Sponsoring/Participating in Data Science Meetups
- Applied Machine Learning Conference
- Career Treks/Info Sessions/Site Visits
- Executive Education

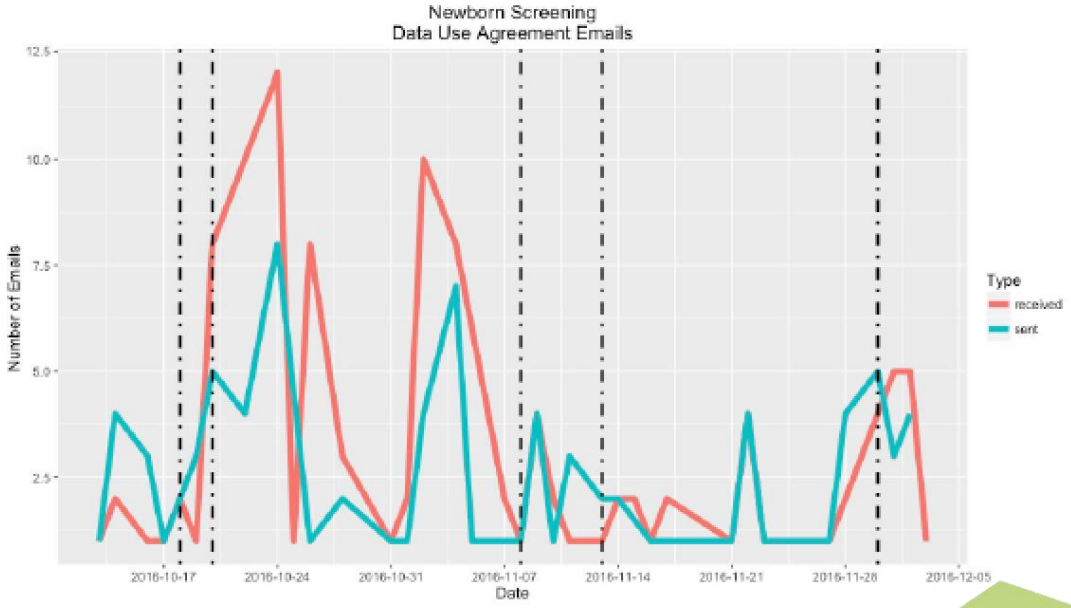
Academia

- Regional Analytics Directors Meeting
- Research Collaborations (e.g. NSF Solicitations from the Big Data Hubs)
- Asynchronous Healthcare Analytics Class for 4VA Initiative

DATA SHARING

UVA | SCHOOL of DATA SCIENCE

Setup: Data Use Agreement (DURSA)



Figures courtesy of Christopher Patrick and Hampton Leonard, 2017

DATAVA

ESTABLISHING A TRUSTING RELATIONSHIP

LEGAL REDEFINITION

SB 580 Government Data Collection and Dissemination Practices Act; amends Act to facilitate sharing data.

Introduced by: **Emmett W. Hanger, Jr.** | **all patrons** ... **notes** | **add to my profiles**

SUMMARY AS PASSED: **(all summaries)**

Data collection and dissemination; governance. Amends the Government Data Collection and Dissemination Practices Act (§ 2.2-3800 et seq.) to facilitate the sharing of data among agencies of the Commonwealth and between the Commonwealth and political subdivisions. The bill creates the position of Chief Data Officer of the Commonwealth (CDO), housed in the office of the Secretary of Administration, to (i) develop guidelines regarding data usage, storage, and privacy and (ii) coordinate and oversee data sharing in the Commonwealth to promote the usage of data in improving the delivery of services. The bill also creates a temporary Data Sharing and Analytics Advisory Committee (Advisory Committee) to advise the CDO in the initial establishment of guidelines and best practices and to make recommendations to the Governor and General Assembly regarding a permanent data governance structure.

The bill directs the CDO and the Advisory Committee to focus their initial efforts on developing a project for the sharing, analysis, and dissemination at a state, regional, and local level of data related to substance abuse, with a focus on opioid addiction, abuse, and overdose.

LEVERAGING DATA SCIENCE RESPONSIBLY

UVA | SCHOOL of DATA SCIENCE

- All models are wrong, but some are useful – George Box
- We have a duty to explain the limitations in the data
- Accurate and meaningful visualization is critical
- COVID-19 example: Public health systems that are local, accessible, accurate and complete are lacking – we can't estimate the denominator now and may never get an accurate estimate

DATA SCIENCE MEETS COVID-19 (NON-VIRUS)

UVA | SCHOOL of DATA SCIENCE

Education	*Economics*	*Manufacturing*	*Finance*	*IT*	*Media & Culture*
					
Online Learning Educational Analytics	Health Disparities Health Knowledge Sharing Language Diversity	Supply Chains	Fraud	Cybersecurity	Social Media Sentiment Analysis Political Debate

Learn more:

- UVA School of Data Science site
- Call for Proposals – UVA Data Science Capstone Research Projects
- UVA Data Science Newsletter and COVID-19 Research Efforts
- UVA Women in Data Science Conference
- UVA Data Science Corporate Partnership Opportunities
- Email Arlyn Burgess (arlyn.burgess@virginia.edu)
- Follow us on Twitter @uvadatascience

UVA | SCHOOL of DATA SCIENCE

Access to Public Records

Virginia Freedom of Information Act

Virginia Freedom of Information Advisory Council

http://foiacouncil.dls.virginia.gov/

foiacouncil@dls.virginia.gov

(804) 698-1810

Introduction to Records & FOIA

- All public records are presumed open unless specifically exempt.
- Definition of "public record" (§ 2.2-3701)
  - all writings and recordings that consist of letters, words or numbers, or their equivalent . . . however stored, and regardless of physical form or characteristics, prepared or owned by, or in the possession of a public body or its officers, employees or agents in the transaction of public business.

Requesting Records
§ 2.2-3704

- Who can make a request?
  - Citizens of the Commonwealth
  - Representatives of newspapers & magazines with circulation in the Commonwealth
  - Representatives of radio & television stations broadcasting in or into the Commonwealth
- How to make a request
  - Reasonable specificity
  - Name & legal address

Responding to Requests

- Five working days to respond
- Five permissible responses to a request

Five Permissible Responses

1. Provide the requested records
2. Requested records are being entirely withheld
3. Requested records are being provided in part and withheld in part
4. Requested records could not be found or do not exist
5. Additional time needed to search for/produce records

How to Respond to a Request

- If any part of the answer is "no," the response must:
  - Be in writing
  - Identify with reasonable particularity the subject matter of the withheld records; AND
  - Cite the specific section(s) of the Code of Virginia that authorizes the records to be withheld
- **NOTE:** if being entirely withheld, response must identify with reasonable particularity the volume of the withheld records

How to Respond to a Request

- If the records cannot be found or do not exist, the response must:
  - Be in writing, AND
  - If the public body knows that another public body has the records, it must provide contact information for the other public body.
- If the public body needs more time, the response must:
  - Be in writing, AND
  - Specify the conditions that make production of the records within the five-working-day period impossible.

Responding to Requests

- Five working days to respond ☑
- Permissible responses to a request ☑
- Creation of new records not required ☑
- Charges for records

Charging for Records

- Reasonable charges for actual cost incurred in accessing, duplicating, supplying, or searching for requested records
  - Exclusion review allowed (*ATI v. UVA*, Va. Supreme Ct., 2014)
- Public body may request a deposit for charges in excess of $200
  - Time period is tolled until deposit is paid
- Unpaid amounts for previous record requests

Electronic Records

- Format of records
- Use and retention of e-mail
  - Virginia Public Records Act, §§ 42.1-76, et seq.
    - Definition of "public record"
  - Tips for using and managing email

Exemptions of General Application

- Personnel records
- Working papers and correspondence
- Attorney-client privilege
- Legal memoranda and other work product
- Contract negotiation records
  - Procurement records
- Account & routing numbers


Q&A

Virginia Information Technologies Agency

Managed security services

Bill Stuart, VITA
Managed security service owner

Darrell Raymond, ATOS
Service delivery manager

June 3, 2020

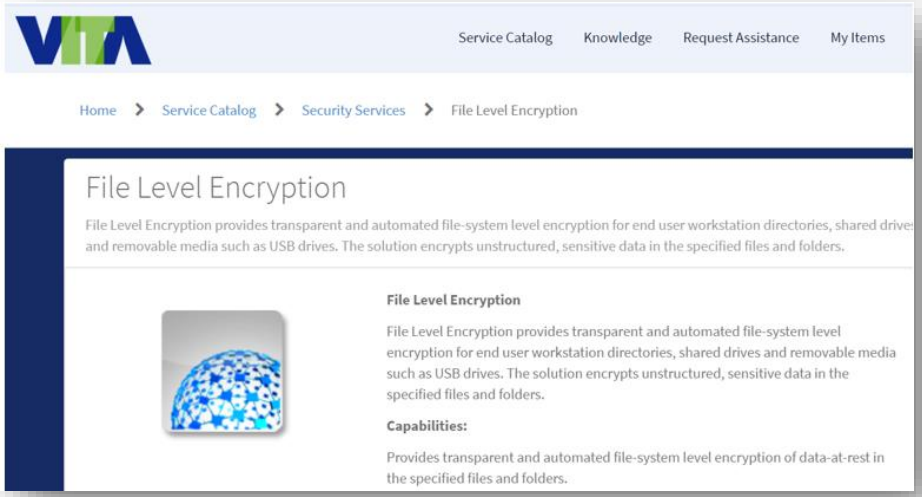
Agenda

- Recap
  - File-level encryption
  - Data loss prevention
- Web content reporting

File-level encryption

File-level encryption

File-level encryption service is now available in the VITA service catalog in the "Security Services" section.



Search → File level encryption

File-level encryption

File-level encryption provides **transparent** and **automated** file system-level encryption for:

- End-user workstation directories
- Shared drives and removable media (i.e. USB drives)

The solution encrypts unstructured, sensitive data in the specified files and folders.

File-level encryption

Benefits:
File-level encryption will allow agencies to ensure consistent and persistent data protection across devices:

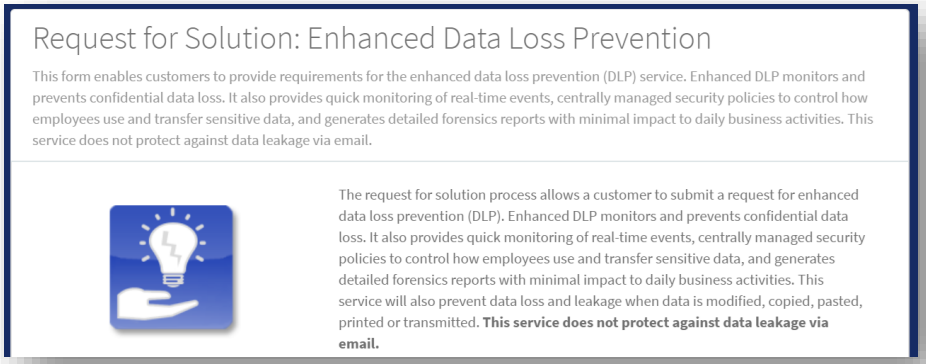
- Simplifies security management and enables broad, yet granular, visibility
- Centralized deployment, management, policy administration, auditing and reporting
- Allows users to easily and consistently enforce company-wide security policies

Enhanced data loss prevention

Enhanced data loss prevention (DLP)

The enhanced DLP service will **monitor** and **prevent confidential data loss**. Enhanced DLP provides quick monitoring of real-time events, controls how employees use and transfer sensitive data with centrally-managed security policies, and generates detailed forensics reports with minimal impact to daily business activities.

Enhanced data loss prevention (DLP)



This service is available in the VITA service catalog

Enhanced data loss prevention prevents data loss and leakage when data is modified, copied, pasted, printed or transmitted.

Note: This service does not protect against data leakage via email.

Enhanced data loss prevention (DLP)

Capabilities:

- Provides a highly scalable solution capable of automatically detecting or blocking transmissions containing sensitive data or quarantining messages (file transfer protocol (FTP) or hypertext transfer protocol (HTTP)) that may need approval to exit the customer's network.

- Provides a solution that allows users to add additional scanning categories and content filters (e.g., credit card information, backdoors, key logger, peer-to-peer (P2P), personal information, Social Security numbers).

Web content reporting

Web content reporting (WCR)

- Modernized web content reporting is an updated services that is part of the new EPS infrastructure
  - New infrastructure has been deployed for the application and database
- Web content reporting replaces the legacy McAfee web reporter
- Web content reporting provides information from the agency's web logs

Web content reporting (WCR) training

- Training will be provided to the agencies on how to access the tool and available reports.

- Additional topics include:
  - Who will have access
  - Process for others to request information
  - How the agency will access the tool

Web content reporting (WCR) training

- **Reports**
  - Examples of frequently used reports
  - Description of report data
- **Dashboards**
  - A graphic dashboard broken up into quadrants showing the top websites, the policy enforcement summary and the inbound web bandwidth for the agency
  - Description of the dashboard information

Upcoming Events

Virginia Information Technologies Agency

The next IS Orientation will be held on
June 30, 2020

1p-3p Remote only- Webex
Presenter: Marlon Cole (CSRM)

Registration Link:
http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10

Future ISOAG

July 8 , 2020

Speakers: - Travis Sarkees Virginia Interactive

Collin Suggs and Nick Lenaeus, RedHat

Kelly Dubois, AWS

ISOAG meets the 1st Wednesday of each month in 2020

ADJOURN

THANK YOU FOR ATTENDING

Picture courtesy of www.v3.co.uk