Business School
UNIVERSITY OF COLORADO DENVER

IEEE COMMUNICATIONS SOCIETY
Denver Chapter

IT Professional
Technology Solutions for the Enterprise

Cybersecurity – Grid, IoT and Emerging Threats

Cyberthreats and Security

Tim Weil – CISSP/CCSP, CISA, PMP
IEEE Senior Member

CU-Denver School of Risk Management
Denver, CO
Nov. 19, 2019

Objectives of this Presentation

Cyberthreats and Security

-- The Changing Landscape (2015 v 2018)

-- Information Security – A body of knowledge

Grid Cybersecurity Resilience (Ukraine)

-- Advanced Persistent Threats (APT)

-- Cyber Attack Strategy

-- Industrial Control Systems (ICS) Kill Chain

-- Remediation Defenses (Passive, Active, Architecture))

Mirai Distributed Denial of Service – IoT Security

-- IoT Landscape

-- Mirai DDoS IoT Attack (Oct 2016)

-- Internet of Things (IoT) Forensics

-- How Mirai Works

-- Remediations and the CSA IoT Security Guidelines

Emerging Threat Landscape

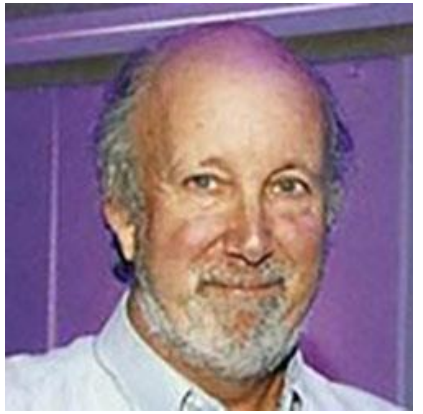
-- SamSam Ransomware Attack

-- Vehicular PKI Hits the Highway

Table of Contents

- Introduction – IT Pro SI on Cyberthreats and Security
- Grid Cybersecurity (Ukraine)
- CSA IoT Security (Controls and Mitigations)
- SamSam Ransomware Attack - US DOT
- VPKI Hits the Highway
- References + Q-A

Tim Weil – Audit and Compliance Engineer / Architect



Tim is a Security Architect/IT Security Manager with over twenty five years of IT management, consulting and engineering experience in the U.S. Government and Communications Industry. His technical areas of expertise includes FedRAMP/FISMA compliance for federal agencies and cloud service providers, IT Service Management, cloud security, enterprise risk management (NIST) for federal agencies and ISO 27001 compliance for commercial clients.

He is a Senior Member of the IEEE and has served in several IEEE positions -

Chair of the Denver Section (2013); Chair of the Washington Section (2009); Cybersecurity Editor for IEEE IT Professional magazine. General Chair - IEEE GREENTECH Conference (2013)

His publications, blogs and speaking engagements are available from the website - http://securityfeeds.com

A Writer's Life –

Timothy Weil
Editor - IEEE IT Professional magazine
Cloud Security, RBAC, Identity Management, Vehicular Networks
Verified email at securityfeeds.com - Homepage

Citation indices	All	Since 2012
Citations	1148	1086
h-index	7	6
i10-index	7	4

Co-authors View all...
Georgios Karagiannis, D. Richard (Rick) Kuhn

Title 1–20	Cited by	Year
Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions G Karagiannis, O Altintas, E Ekici, G Heijenk, B Jarupan, K Lin, T Weil IEEE communications surveys & tutorials 13 (4), 584-616	705	2011
Adding attributes to role-based access control DR Kuhn, EJ Coyne, TR Weil Computer 43 (6), 79-81	306	2010
ABAC and RBAC: scalable, flexible, and auditable access management E Coyne, TR Weil IT Professional 15 (3), 0014-16	53	2013
Final report: Vehicle infrastructure integration (VII) proof of concept (POC) test–Executive summary R Kandarpa, M Chenzaie, M Dorfman, J Anderson, J Marousek, ... US Department of Transportation, IntelliDrive (SM), Tech. Rep	25	2009
Service management for ITS using WAVE (1609.3) networking T Weil GLOBECOM Workshops, 2009 IEEE, 1-6	14	2009
Final Report: Vehicle Infrastructure Integration Proof-of-Concept Results and Findings-Infrastructure R Kandarpa, M Chenzaie, J Anderson, J Marousek, T Weil, F Perry, ... US Department of Transportation, Washington, DC, USA	11	2009

IEEE National Capital Area **scanner**

IEEE SCANNER - Above the Fold (Mostly)

Stories in Engineering and Science (2005-2009)

In my tenure as Washington DC Editor of the IEEE SCANNER(2005-2007) and AdCom officer (2007-2009) I had the wonderful chance to tour the science, engineering and technology world of IEEE as a roving reporter and editor of this newspaper. My travels took me to Deep Space (NASA), Satellite Communication(InterlSat), the flagship conference of the Telecom industry (GLOBECOM) and beyond. As the son of an AP journalist and itinerant newspaper reporter the SCANNER gave me a front row seat to the journeys of science and engineering.

The stories and photographs below are the journalistic opportunities presented to me by the SCANNER newsletter.

- Nov-Dec 2009 - Celebrating the 125th IEEE Anniversary Year (UDC)
- Sept-Oct 2009 - Preserving History at the History of Technical Societies Conference
- July-Aug 2009 - Washington Section Participates in Congressional Visit Day
- May-June 2009 - Passing The Gavel
- Nov-Dec 2008 - A Tour of NASA Goddard Test and Integration Facility (pg. 6)
- Sept-Oct 2008 - Globecom Committee Closes the Books at ICC 2008 in Beijing
- Sept-Oct 2007 - Globecom Volunteers Prepare for the November Conference
- July-Aug 2007 - DC COMSOC Hosts WiMax Lecture at JDSU
- Jan-Feb 2007 - Globecom Volunteers Visit the San Francisco Conference
- Nov-Dec 2006 - Sensors Conference Panel Reviews DoD Technologies
- July-Aug 2006 - Globecom 2007 Committee Builds a Program
- Sept-Oct 2005 - COMSOC Members Tour the IntelSat Satellite Center
- May-June 2005 - DCCEAS Recognizes Jerry Gibbon as Engineer of the Year

SECURING IT

VPKI Hits the Highway

Secure Communication for the Connected Vehicle Program

Tim Weil, SCRAM Systems

IT Professional Security Issue (2015 vs 2018)

IN THIS ISSUE

14
Guest Editors' Introduction: IT Security
Morris Chang, Rick Kuhn, and Tim Weil

16
Security—A Perpetual War: Lessons from Nature
Wojciech Mazurczyk and Elżbieta Rzeszutko

23
Securing Health Information
A.J. Burns and M. Eric Johnson

30
A Right to Cybercounter Strikes: The Risks of Legalizing Hack Backs
Jan Kallberg

36
Protected Web Components: Hiding Sensitive Information in the Shadows
Philippe De Ryck, Nick Nikiforakis, Lieven Desmet, Frank Piessens,

TABLE OF CONTENTS

Cyberthreats and Security

20 GUEST EDITORS' INTRODUCTION
Cyberthreats and Security
Morris Chang, Rick Kuhn, and Tim Weil

23 Advancing Cybersecurity: The Growing Need for a Cyber-Resiliency Workforce
Logan O. Mailloux and Michael Grimaila

31 The New Threats of Information Hiding: The Road Ahead
Krzysztof Cabaj, Luca Caviglione, Wojciech Mazurczyk, Steffen Wendzel, Alan Woodward, and Sebastian Zander

40 Internet of Things Forensics: The Need, Process Models, and Open Issues
Maxim Chernyshev, Sherali Zeadally, Zubair Baig, and Andrew Woodward

50 Experiments with Ocular Biometric Datasets: A Practitioner's Guideline
Zahid Akhtar, Gautam Kumar, Sambit Bakshi, and Hugo Proenca

64 The Evolving Cyberthreat to Privacy
A.J. Burns and Eric Johnson

Feature Articles

73 Understanding Privacy Violations in Big Data Systems
Jawwad A. Shamsi and Muhammad Ali Khojaye

Columns and Departments

6 FROM THE EDITORS
IoT Metrology
Jeffrey Voas, Rick Kuhn, and Phillip A. Laplante

A Cybersecurity Body of Knowledge – IEEE Security and Privacy (May/June 2018)

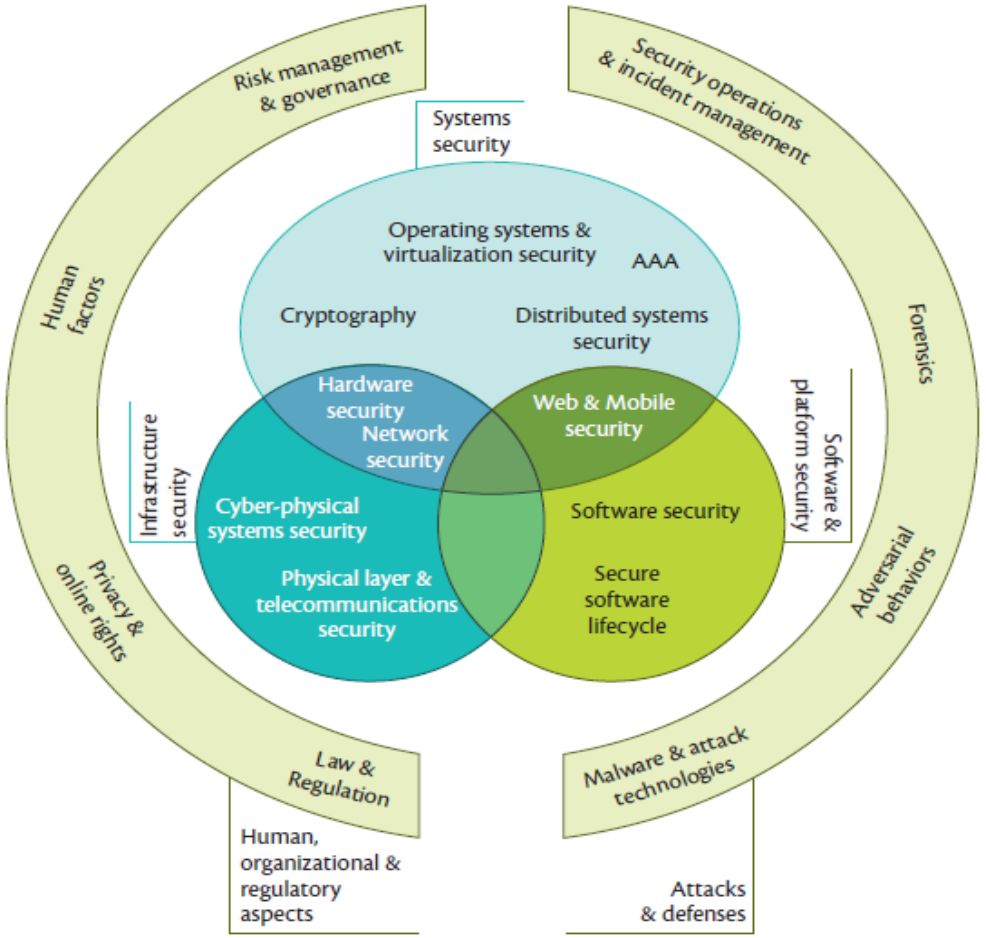


Figure 3. The 19 knowledge areas and their categorization within CyBOK.

Table 3. Overview of the 19 knowledge areas.

Human, Organizational, and Regulatory Aspects	
Risk Management and Governance	Security management systems and organizational security controls, including standards, best practices, and approaches to risk assessment and mitigation.
Law and Regulation	International and national statutory and regulatory requirements, compliance obligations, and security ethics, including data protection and developing doctrines on cyber warfare.
Human Factors	Usable security, social and behavioral factors impacting security, security culture and awareness as well as the impact of security controls on user behaviors.
Privacy and Online Rights	Techniques for protecting personal information, including communications, applications, and inferences from databases and data processing. It also includes other systems supporting online rights touching on censorship and circumvention, covertness, electronic elections, and privacy in payment and identity systems.
Attacks and Defenses	
Malware and Attack Technologies	Technical details of exploits and distributed malicious systems, together with associated discovery and analysis approaches.
Adversarial Behaviors	The motivations, behaviors, and methods used by attackers, including malware supply chains, attack vectors, and money transfers.
Security Operations and Incident Management	The configuration, operation, and maintenance of secure systems including the detection of and response to security incidents and the collection and use of threat intelligence.
Forensics	The collection, analysis, and reporting of digital evidence in support of incidents or criminal events.
Systems Security	
Cryptography	Core primitives of cryptography as presently practiced and emerging algorithms, techniques for analysis of these, and the protocols that use them.
Operating Systems and Virtualization Security	Operating systems protection mechanisms, implementing secure abstraction of hardware, and sharing of resources, including isolation in multiuser systems, secure virtualization, and security in database systems.

"Scoping the Cyber Security Body of Knowledge" Awais Rashid, et. al

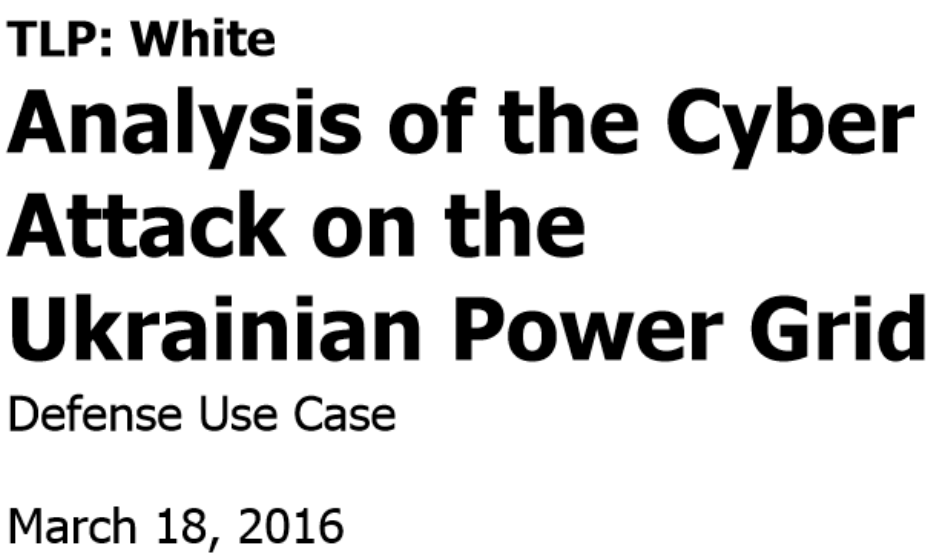
Table of Contents

- Introduction – IT Pro SI on Cyberthreats and Security
- Grid Cybersecurity (Ukraine)
- CSA IoT Security (Controls and Mitigations)
- SamSam Ransomware Attack - US DOT
- VPKI Hits the Highway
- References + Q-A

Grid Cybersecurity in the News

SANS ICS Industrial Control Systems

E-ISAC ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER



On December 23, 2015, the control centers of three Ukrainian electricity distribution companies were remotely accessed. Taking control of the facilities' SCADA systems, malicious actors opened breakers at some 30 distribution substations in the capital city Kiev and western Ivano-Frankivsk region, causing more than 200,000 consumers to lose power Nearly a year later, on December 17, 2016, a single transmission substation in northern Kiev lost power. These instances of sabotage took place on the tail of a political revolution in Kiev, the annexation of Crimea, and amid military clashes in the eastern Donetsk and Luhansk regions.

https://www.forbes.com/sites/kateoflahertyuk/2019/07/03/u-s-government-makes-surprise-move-to-secure-power-grid-from-cyber-attacks/#46ecff7a3191

A Decade of Energy Cyber Infrastructure Attack Malware

http://www.aaes.org/sites/default/files/Sanders_Convocation2018.pdf

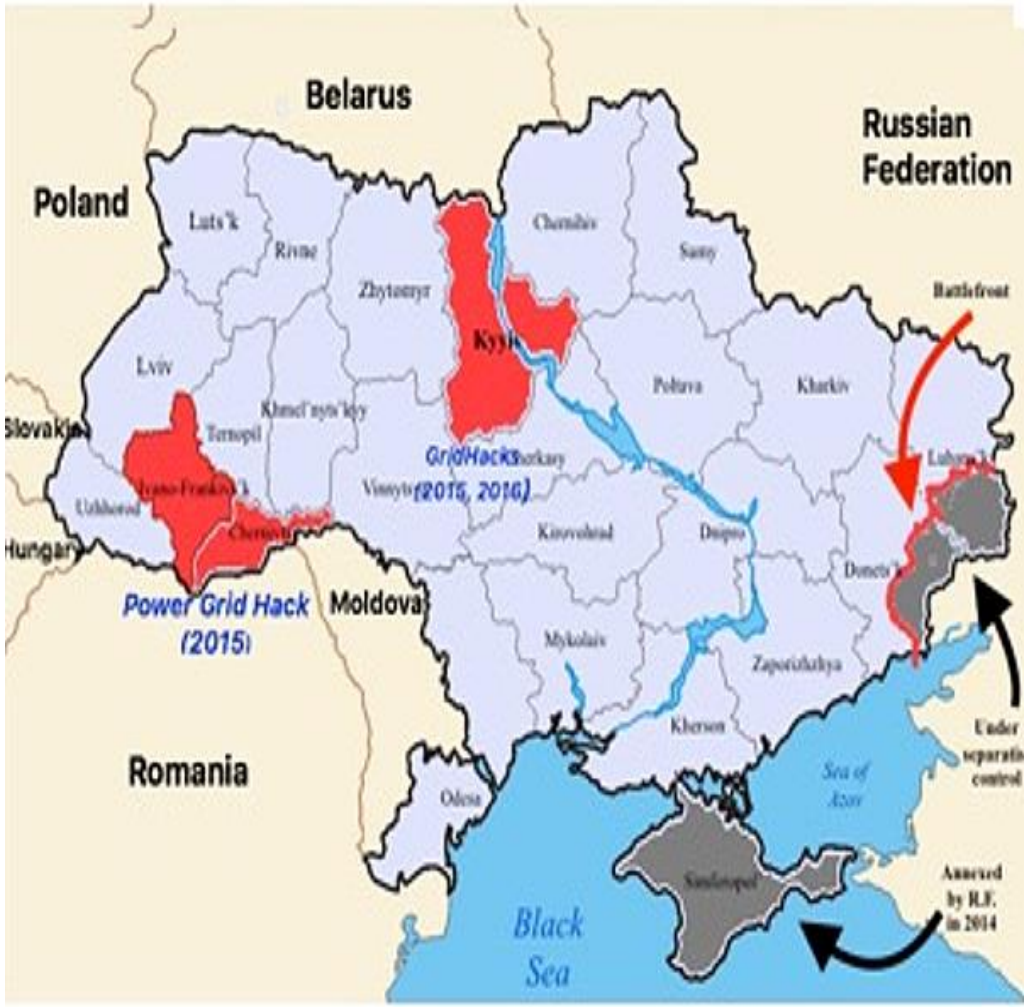
- **2010: Stuxnet:** Targeted Siemans industrial control systems in Iran. Was first discovered malware that spies on and subverts industrial systems and the first to include a programmable logic controller (PLC) rootkit.
- **2014: Dragonfly/Havex:** Focus was to collect ICS network and access control information. Evidence suggests this was provided to a well organized and funded group outside countries from which the data was collected.
- **2015: Black Energy 3:** Used in attack on the Ukraine power grid. Considered to be the first known power grid cyberattack. Hackers were able to successfully compromise information systems of three energy distribution companies and temporarily disrupt electricity supply to the end consumers.
- **2016: CRASHOVERRIDE:** Second known attack in Ukraine. Impacted a single transmission level substation. Significant increase in sophistication of attack code relative to past attacks.
- **2017: TRISIS/TRITON:** Incident at a critical infrastructure organization which targeted Schneider Electric's Triconex safety instrumented system (SIS) and where an attacker deployed malware which targeted systems provided emergency shutdown capability for industrial processes. Deployed against at least one victim in the Middle East.

Ukrainian Shale Deposits and Russian Electrical Grid Attacks

The discovery of shale deposits has prompted Russian attempts to stall their developments and sabotage much needed business deals for Ukraine's foreign capital thirsty economy. Russia's military operation on the ground solved the prospects of Ukrainian energy competition problem for Russia, albeit *partially*.[83] The warzone in the Eastern Ukraine covers the Donetsk region part of Yuzivska shale bloc, and, thus, closed it to development.

In addition, the Kharkiv region (second half of the shale bloc) has been subject to destabilizing activities. Among these actions were the recent explosions at an arms warehouse in Balaklia, in the Kharkiv region, which, according to Ukraine's defense minister Poltorak, was staged by Russia.[84] It is also worth noting that at the beginning of the unrest in the Eastern Ukraine, there were numerous attempts, however unsuccessful, to create Russia-backed third separatist enclave in Kharkiv region.[85]

To prevent the development of energy sources in Ukraine's west, Moscow has employed various methods to destabilize the region – including attacks on the electrical grid. On December 23, 2015, Russian-led cyberattack on the Prykarpattyaoblenergo distribution center created enough uncertainty to hurt the prospects of setting up industrial fracking operations in that region. Ivano-Frankivsk region that hosts part of Olesska's shale block. Russian has also financed fracking protests The map illustrates the locations of the major attacks on the electrical grid



Ukraine Grid Utility Cybersecurity Attack – FireEye

https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf

In the first publicly documented power outage attributed to a cyber attack, Russian-nexus actors caused blackouts in several regions in Ukraine. The actors used spear phishing to plant BlackEnergy3 malware, which was used to disable control system computer. Responders also found a wiper module called killdisk that was used to disable both control and non-control systems computers. At the same time, the attackers overwhelmed utility call centers with automated telephone calls, impacting the utilities' ability to receive outage reports from customers and frustrating the response effort.

While killdisk does not have the functionality to open breakers – which would cause the outages – it would impede utility visibility of breaker status, and inhibit remote control of the substations. This suggests that the attackers used another method to cause the power outage, perhaps using interactive access via compromised corporate and SCADA accounts to remotely open individual breakers or initiate load shedding, sending simultaneous trip commands to multiple breakers.

Who is behind this attack?

BlackEnergy malware is a tool that first appeared in the Russian underground for use in distributed denial-of-service attacks. A later variant called BlackEnergy2 added credential theft functionality useful for cyber crime. BlackEnergy3 is a distinctive tool only used by the Sandworm team for cyber espionage. Documents recovered from an open command and control server indicate that Russian speakers operate the tool.

Potential Power-System-Specific Cyber Attack Strategies

http://www.aaes.org/sites/default/files/Sanders_Convocation2018.pdf

- Tripping breakers
- Changing values breaker settings
  - Lower settings can destabilize a system by inducing a large number of false trips
  - Lowering trip settings can cause extraneous other breakers, causing overloading of other transmission lines and/or loss of system stability
- Corrupting Control Information: Smart Meters, SCADA Data, PMU Data, Dispatch Information, etc.
- Sophisticated lateral movement attacks
- Life cycle attacks
- Insider threats
- Physical damage by cyber means
- Combined physical and cyber attacks

Lateral Movement in Cyber Kill Chain Demands Resiliency

http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/tlp_lateral_movement.pdf

- Port scanning
- Media analysis

Reconnaissance

- Spear phishing
- Zero-day exploits

Delivery

- Control channels

Command and Control

- Remote desktop
- Privilege escalation

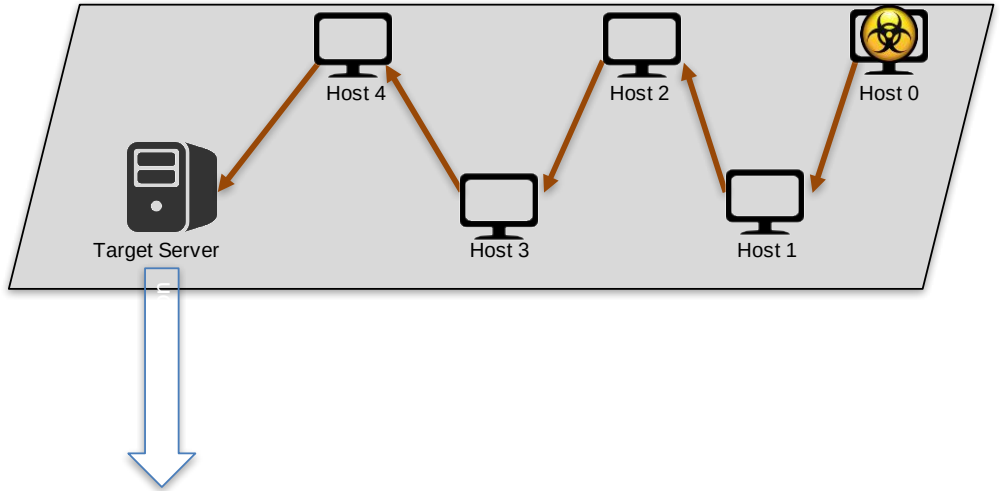
Lateral Movement

- Data exfiltration
- Physical damage

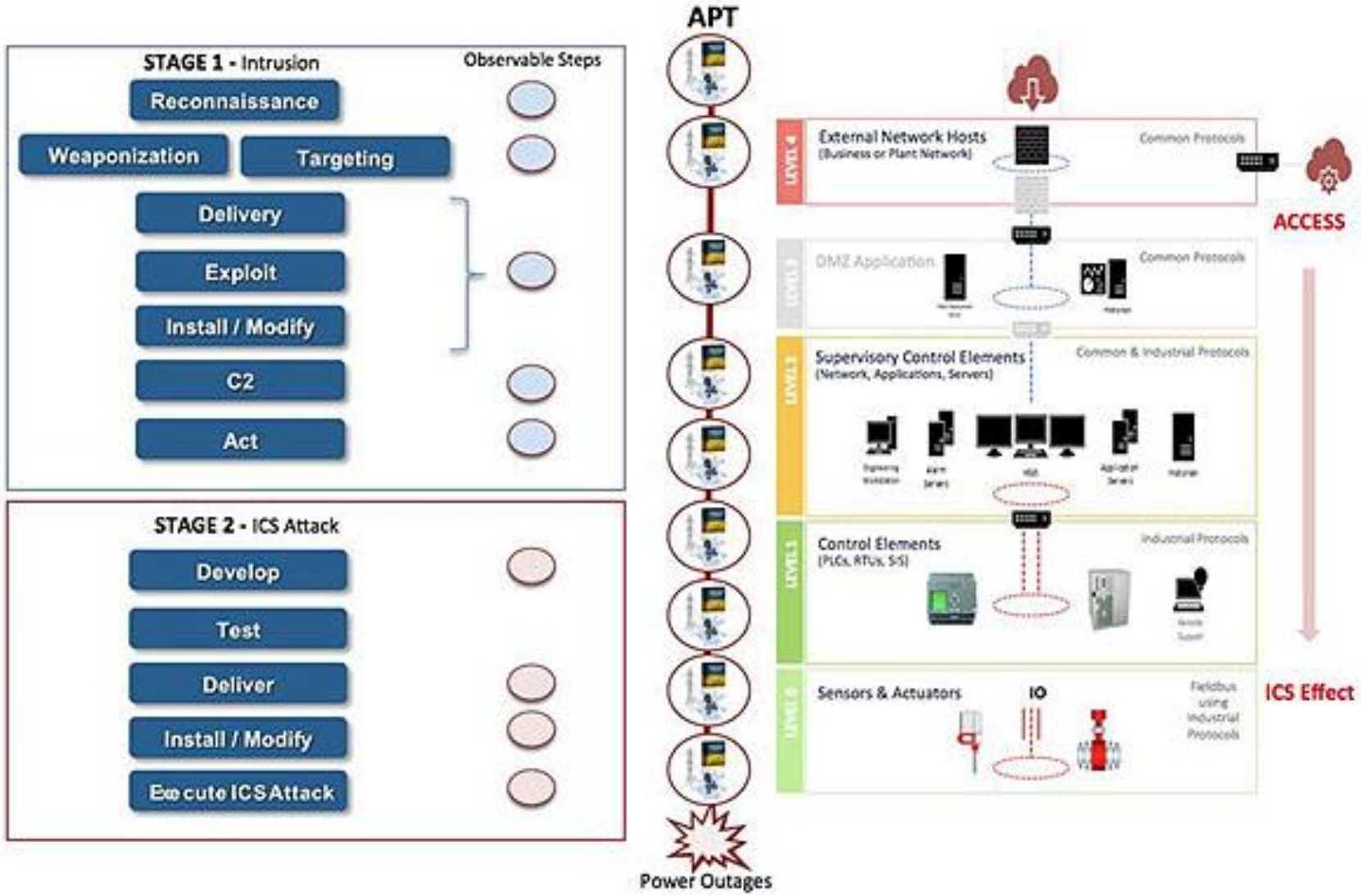
Goal Accomplishment

During lateral movement:

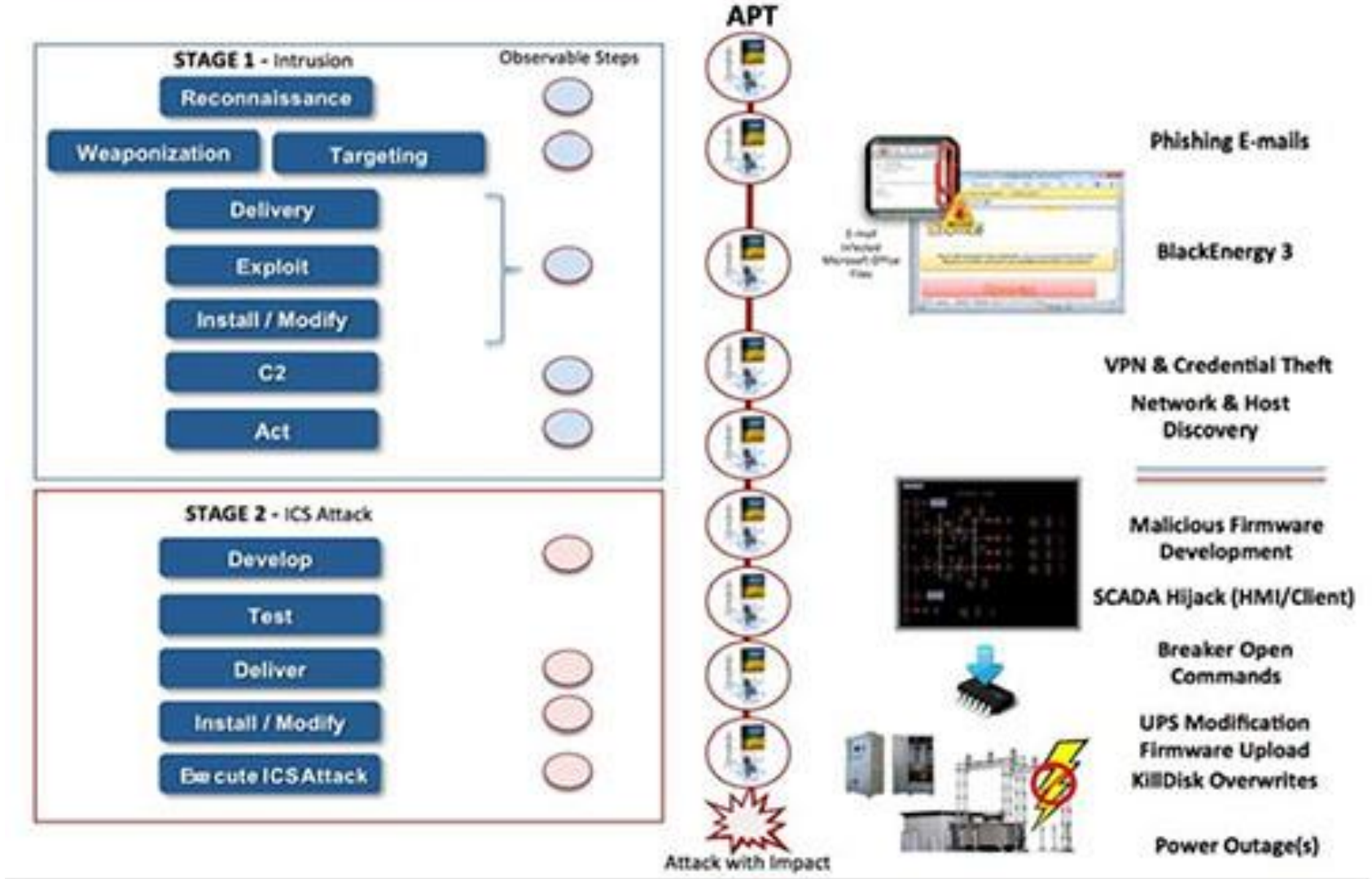
- Attacker moves laterally between hosts
- Attacker uses remote desktop connections, SSH, Windows management inventory, administrator tools



Ukraine Cyber Attack ICS Kill Chain (1 of 2)



Ukraine Cyber Attack ICS Kill Chain (2 of 2)



Ukraine Attack Consolidated Technical Components

1. Spear phishing to gain access to the business networks of the
2. oblenergos
3. Identification of BlackEnergy 3 at each of the impacted oblenergos
4. Theft of credentials from the business networks
5. The use of virtual private networks (VPNs) to enter the ICS network
6. The use of existing remote access tools within the environment or issuing commands directly from a remote station similar to an operator HMI
6. Serial-to-ethernet communications devices impacted at a firmware level
7. The use of a modified KillDisk to erase the master boot record of impacted organizationsystems as well as the targeted deletion of some logs
8. Utilizing UPS systems to impact connected load with a scheduled service outage
9. Telephone denial-of-service attack on the call center

Ukraine Attack – Black Energy Malware (APT 1 of 2) -

https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

During the cyber intrusion stage of **Delivery, Exploit, and Install**, the malicious Office documents were delivered via email to individuals in the administrative or IT network of the electricity companies. When these documents were opened, a popup was displayed to users to encourage them to enable the macros in the document as shown in Figure. Enabling the macros allowed the malware to Exploit Office macro functionality to install BlackEnergy 3 on the victim system and was not an exploit of a vulnerability through exploit code.

Figure 6: A Sample of a BlackEnergy 3 Infected Microsoft Office Document[27]

Upon the **Install** step, the BlackEnergy 3 malware connected to command and control (C2) IP addresses to enable communication by the adversary with the malware and the infected systems. These pathways allowed the adversary to gather information from the environment and enable access. The attackers appear to have gained access more than six months prior to December 23, 2015, when the power outage occurred. One of their first actions happened when the network was to harvest credentials, escalate privileges, and move laterally throughout the environment (e.g., target directory service infrastructure to directly manipulate and control the authentication and authorization system). At this point, the adversary completed all actions to establish persistent access to the targets.

Ukraine Attack – Kill Disk Malware -

https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

During **the ICS Attack Stage**, the adversaries used native software to Deliver themselves into the environment for direct interaction with the ICS components. They achieved this using existing remote administration tools on the operator workstations. The threat actors also continued to use the VPN access into the IT environment.

In final preparation for the attack, the adversaries completed the **Install/Mo**dify stage by installing malicious software identified as a modified or customized KillDisk across the environment. While it is likely the attackers then ensured their modifications to the UPS were ready for the attack, there was not sufficient forensic evidence available to prove this. The last act of modification was for the adversaries to take control of the operator workstations and thereby lock the operators out of their systems. Figure shows the static analysis of the KillDisk API imports following the event

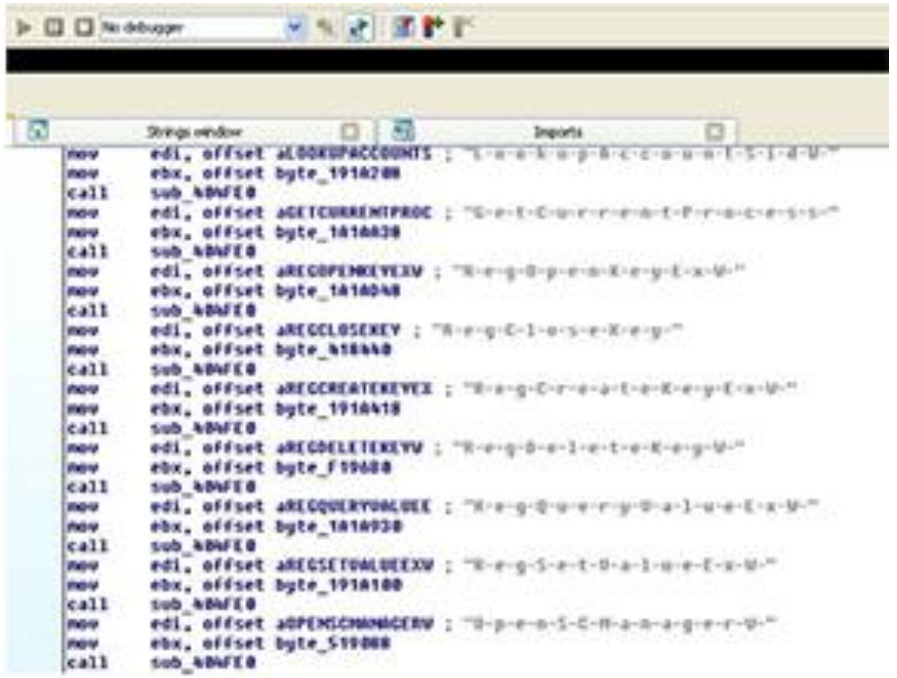


Figure 7: Static Analysis of KillDisk Identifying API Imports[32]

Finally, to complete the ICS Cyber Kill Chain and to Execute the ICS Attack, the adversaries used the HMIs in the SCADA environment to open the breakers. At least 27 substations (the total number is probably higher) were taken offline across the three energy companies, impacting roughly 225,000 customers. Simultaneously, the attackers uploaded the malicious firmware to the serial-to-ethernet gateway devices. This ensured that even if the operator workstations were recovered, remote commands could not be issued to bring the substations back online

Ukraine Grid Attack – Remediation Defenses

Active Defense

Recommendations:

- Train defenders to hunt for odd communications leaving the networked environment such as new IP communications.
- Perform network security monitoring to continuously search through the networked environment for abnormalities.
- Plan and train to incident response plans that incorporate both the IT and OT network personnel.
- Consider active defense models for security operations such as the active cyber defense cycle.
- Ensure that personnel performing analysis have access to technologies such as sandboxes to quickly analyze incoming phishing emails or odd files and extract indicators of compromise (IOCs) to search for infected systems.
- Use backup and recovery tools to take digital images from a few of the systems in the supervisory environment such as HMIs and data historian systems every 6-12 months. This will allow a baseline of activity to be built and make the images available for scanning with new IOCs such as new YARA rules on emerging threats.
- Train defenders on using tools such as YARA to scan digital images and evidence collected from the environment but do not perform the scans in the production environment itself.

Architecture Recommendations:

- Properly segment networks from each other
- Ensure logging is enabled on devices that support it, including both IT and Operational Technology (OT) assets.
- Ensure that network architecture, such as switches, are managed and have the ability to capture data from the environment to support Passive and Active Defense mechanisms.
- Make backups of critical software installers and include an MD5 and SHA256 digital hash of the installers.
- Collect and vault backup project files from the network

Passive Defense

Recommendations:

- Application whitelisting can help limit adversary initial infection vectors and should be used when not too invasive to the ICSs.
- DMZs and properly tuned firewalls between network segments will give visibility into the environment and allow defenders the time required to identify intrusions.
- Establish a central logging and data aggregation point to allow forensic evidence to be collected and made available to defenders.
- Implement alarm package priorities for abnormal cyber events within the control system.
- Enforce a password reset policy in the event of a compromise especially for VPNs and administrative accounts.
- Utilize up-to-date antivirus or endpoint security technologies to allow for the denial of known malware.
- Configure an intrusion detection system so that rules can be quickly deployed to search for intruders.

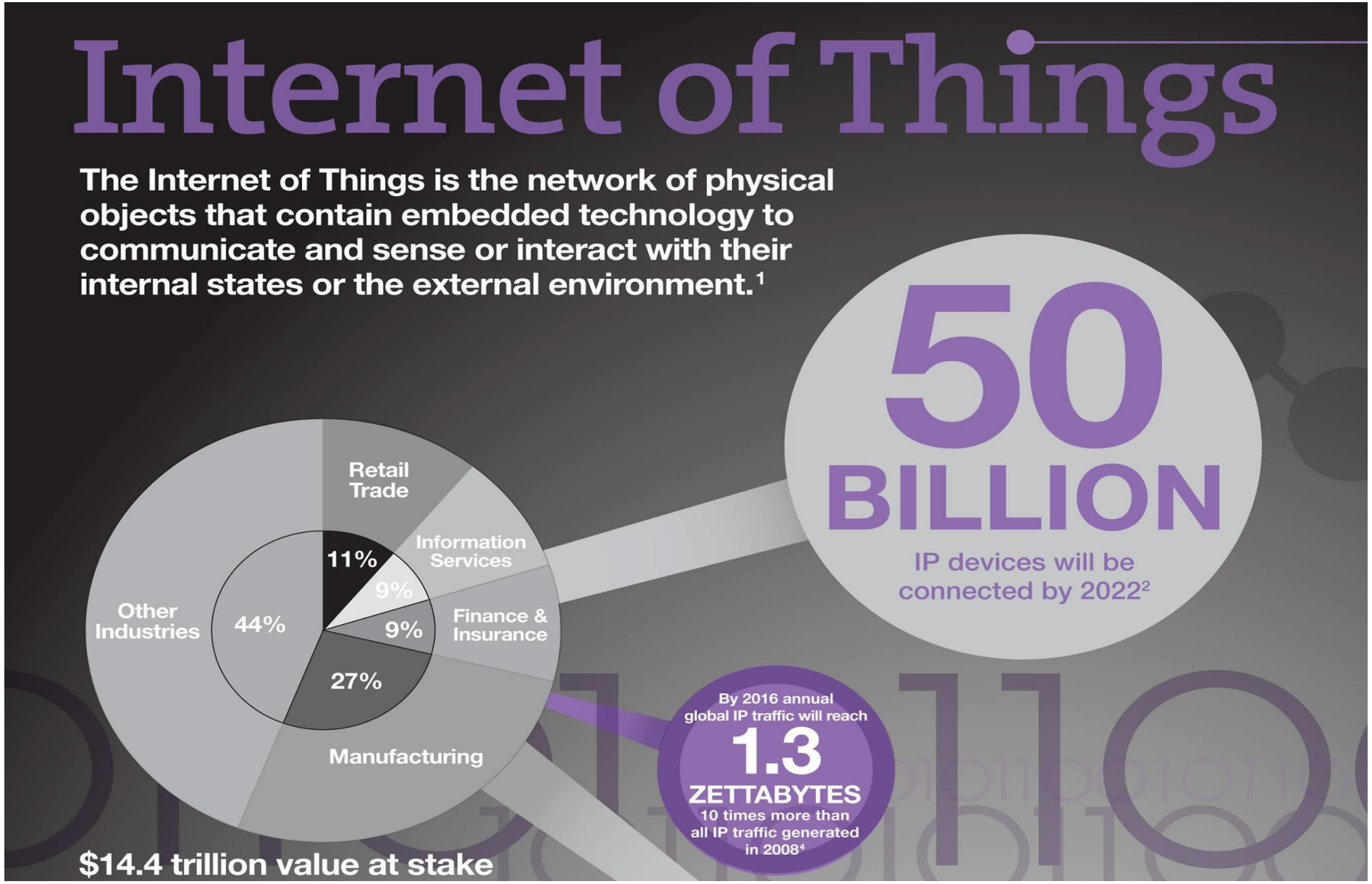
Architecture Recommendations:

• Test the tools and technologies that passive and active defense mechanisms will need (such as digital imaging software) on the environment to ensure that it will not negatively impact systems.
• Prioritize and patch known vulnerabilities based on the most critical assets in the organization.
• Limit remote connections only to personnel that need them. Use two-form authentication on the remote connections.
• Consider use of a system event monitoring system, configured and monitored specifically for high-value ICS/SCADA systems.

Table of Contents

- Introduction – IT Pro SI on Cyberthreats and Security
- Grid Cybersecurity (Ukraine)
- CSA IoT Security (Controls and Mitigations)
- SamSam Ransomware Attack - US DOT
- VPKI Hits the Highway
- References + Q-A

Internet of Things (IoT) Attack Surface

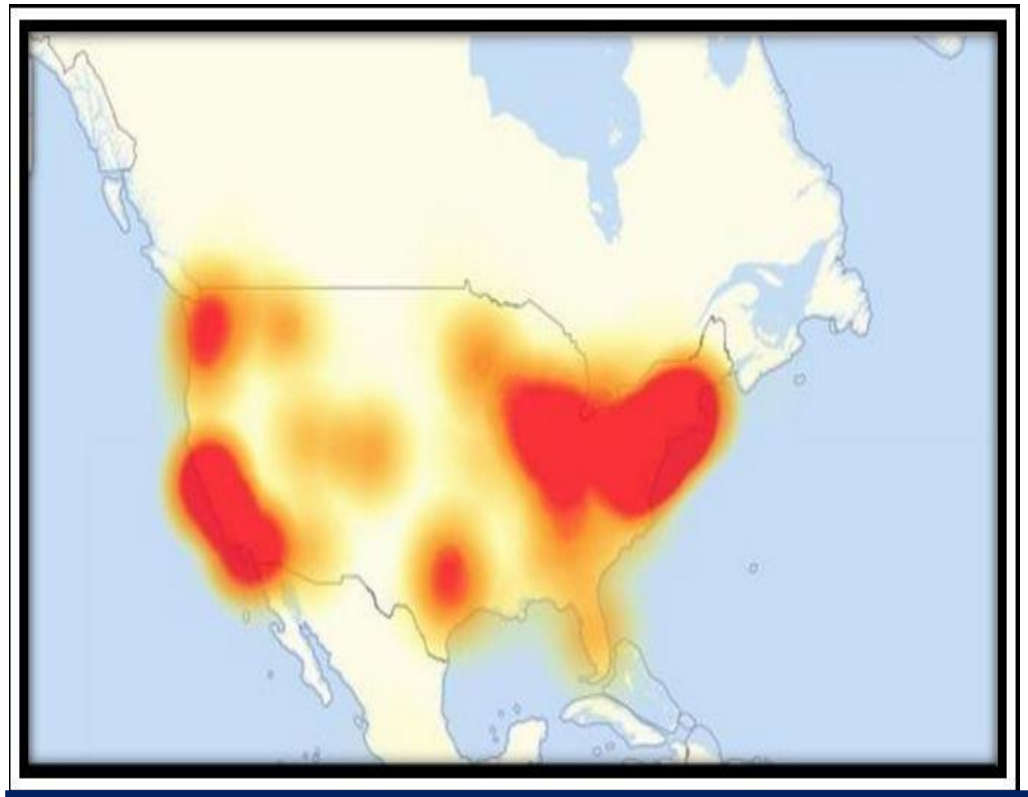


Typical IoT Devices

CCTV cameras
DVRs
Digital TVs
Home routers
Printers
Alexa
Cars
Other stuff

Security systems
Garage doors
Industrial systems
Medical systems
Home appliances
Smart Utility Meters

Mirai Botnet: IoT Botnets Performed Massive Distributed Denial of Service Attacks (Oct 2016)



What is Mirai Botnet

Mirai is a self-propagating botnet virus. The source code for Mirai was made publicly available by the author after a successful and well publicized attack on the Krebs Web site. Since then the source code has been built and used by many others to launch attacks on internet infrastructure (ref Dyn).

The Mirai botnet code infects poorly protected internet devices by using telnet to find those that are still using their factory default username and password. The effectiveness of Mirai is due to its ability to infect tens of thousands of these insecure devices and co-ordinate them to mount a DDOS attack against a chosen victim.

The Internet didn't "break" on October 21, 2016, but the attackers who launched the DDoS attacks against Dyn exploited a known DNS Weakness that negatively impacted MANY Internet-related businesses and millions of users.

http://www.billslater.com/mirai.ppsx

https://www.corero.com/resources/ddos-attack-types/mirai-botnet-ddos-attack.html

Mirai Impact

http://www.billslater.com/mirai.ppsx

INTERNET OF THINGS, SECURITY

Report: Mirai Botnet DDoSed 17 Dyn Data Centers Globally

BY YEVGENIY SVERDLIK ON OCTOBER 26, 2016 ADD YOUR COMMENTS

Tweet

All but three data centers where DNS provider Dyn hosts its global infrastructure came under attack in last week's massive DDoS strike that disrupted some of the internet's most popular destinations, such as Spotify, Amazon, HBO Now, Twitter, and The New York Times, among others.

Dyn's servers sit in 20 data centers spread around the world, and the attack — implemented at least in part by using a botnet created by software called Mirai, which hijacks poorly secured IoT devices, such as CCTV cameras and DVRs — was directed at 17 of those sites, according to an analysis by ThousandEyes, a provider of global network monitoring services. The three data centers that were not affected are in Warsaw, Beijing, and Shanghai.

"At the height of the attack, approximately 75 percent of our global vantage points sent queries that went unanswered by Dyn's servers," Nick Kephart, senior director of product marketing at ThousandEyes, wrote in a blog post. "In addition, the critical nature of many of these affected services led to collateral damage, in terms of outages and performance impacts on sites that are only tangentially related to Dyn (including this blog)."

WHO WAS HIT BY THE ATTACK?

Thousands of sites were hit, including:

Twitter
Reddit
Spotify
Esty
Box
Wix Customer Sites
Squarespace Customer Sites
Zoho
CRM
Iheart.com (iHeartRadio)
Github
The Verge
Cleveland.com
hbonow.com
PayPal
Big cartel
Wired.com
People.com
Urbandictionary.com
Basecamp
ActBlue
Zendesk.com
Intercom
Twillo
Pinterest
Grubhub
Okta
Starbucks rewards/gift cards
Storify.com
CNN
Yammer
Playstation Network
Recode Business Insider
Guardian.co.uk
Weebly
Yelp

How Mirai Works (1 of 3)

http://www.billslater.com/mirai.ppsx

There are two main components to Mirai, the virus itself and the command and control center (CnC). The virus contains the attack vectors, Mirai has ten vectors that it can launch, and a scanner process that actively seeks other devices to compromise. The CnC is a separate image that controls the compromised devices (BOT) sending them instructions to launch one of the attacks against one or more victims.

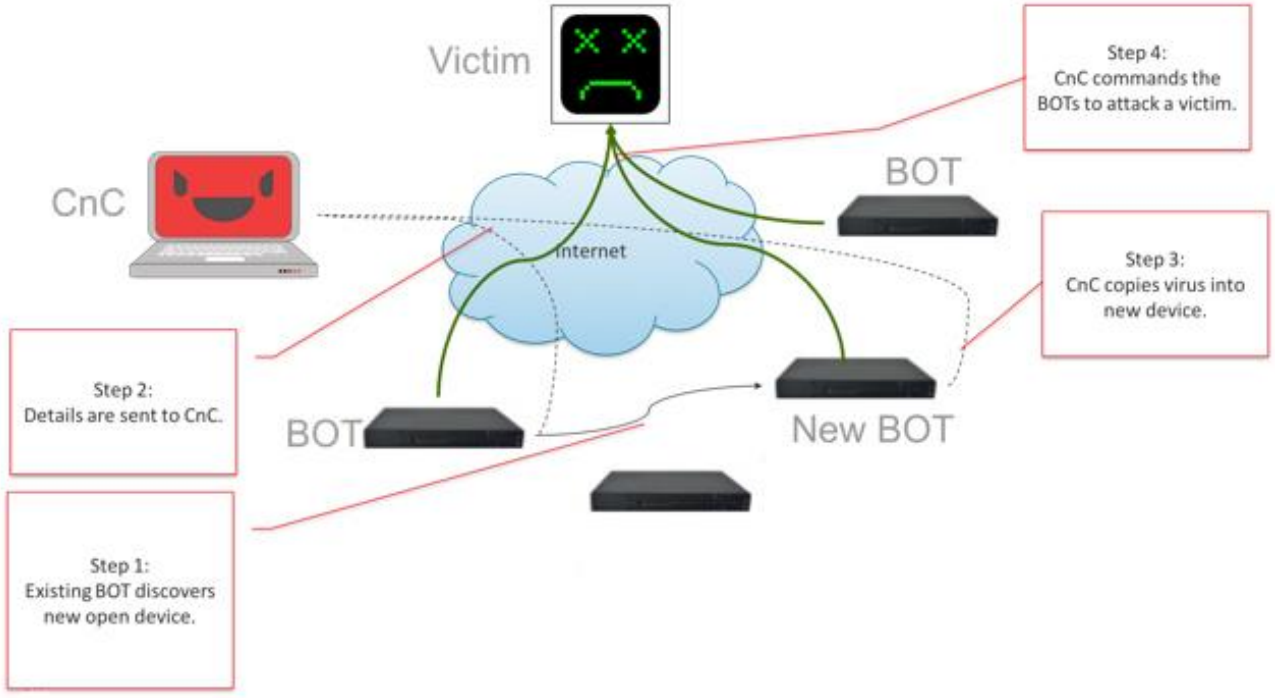


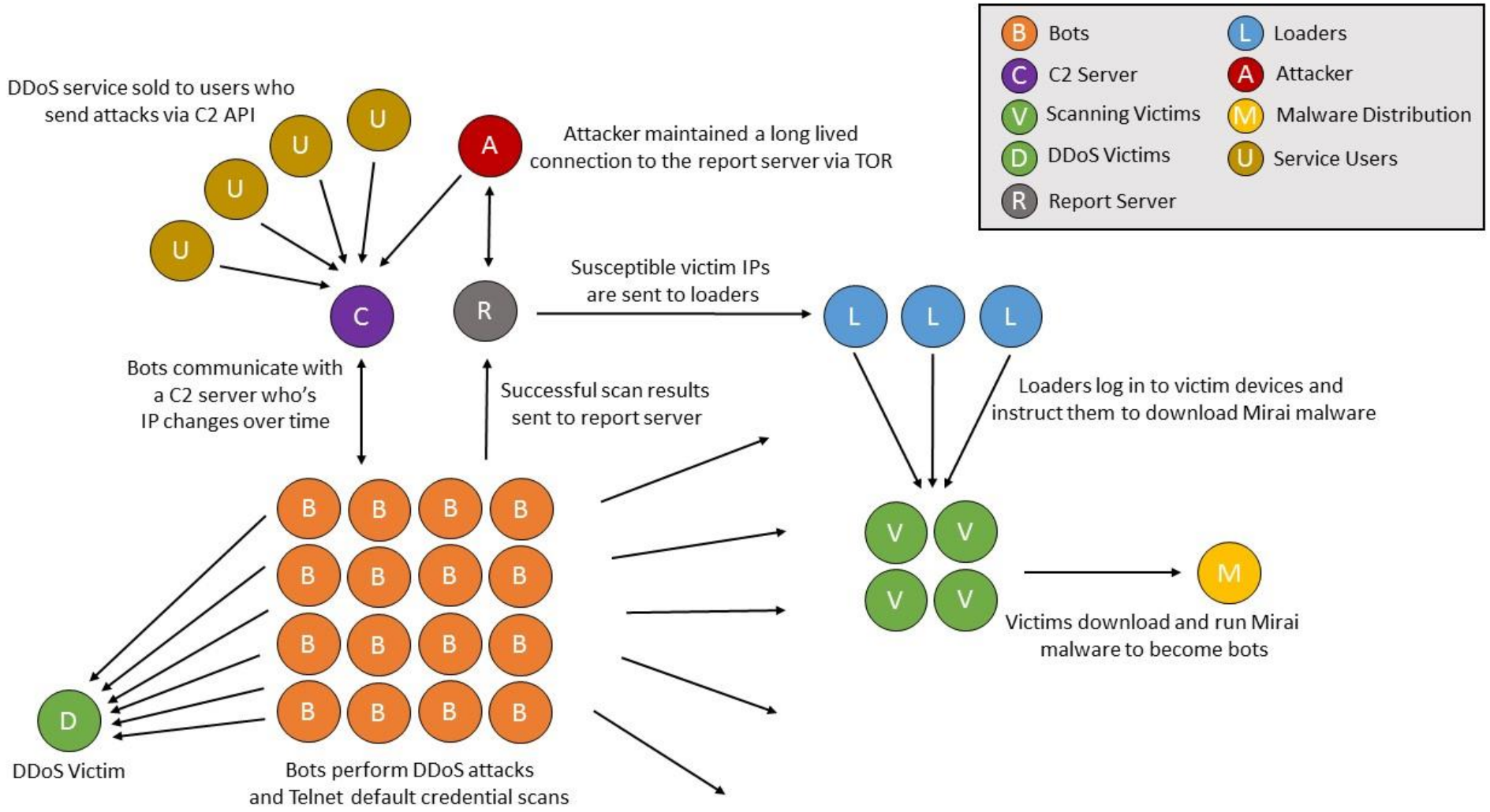
Figure 1 Mirai System

The scanner process runs continuously on each BOT using the telnet protocol (on TCP port 23 or 2323) to try and login to IP addresses at random. The login tries up to 60 different factory default username and password pairs when login succeeds the identity of the new BOT and its credentials are sent back to the CnC.

The CnC supports a simple command line interface that allows the attacker to specify an attack vector, a victim(s) IP address and an attack duration. The CnC also waits for its existing BOTs to return newly discovered device addresses and credentials which it uses to copy over the virus code and in turn create new BOTs.

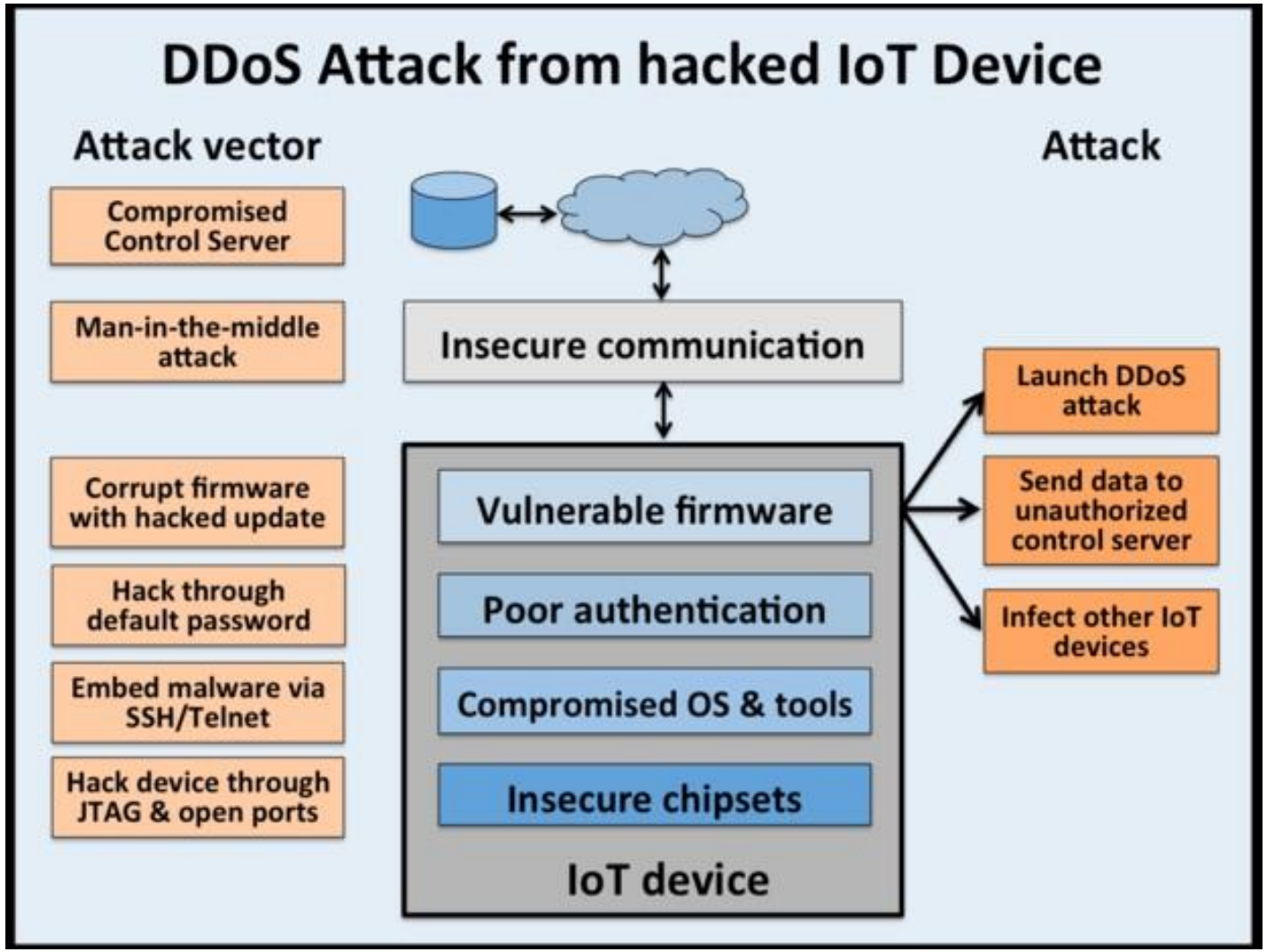
How Mirai Works (2 of 3)

http://www.billslater.com/mirai.ppsx



How Mirai Works (3 of 3)

http://www.billslater.com/mirai.ppsx



Infected IoT Devices:

1) Launch DDoS Attacks
2) Report data to C2 Servers
3) Infect other IoT Devices

Where Mirai Botnet Attacks Came From

http://www.billslater.com/mirai.ppsx

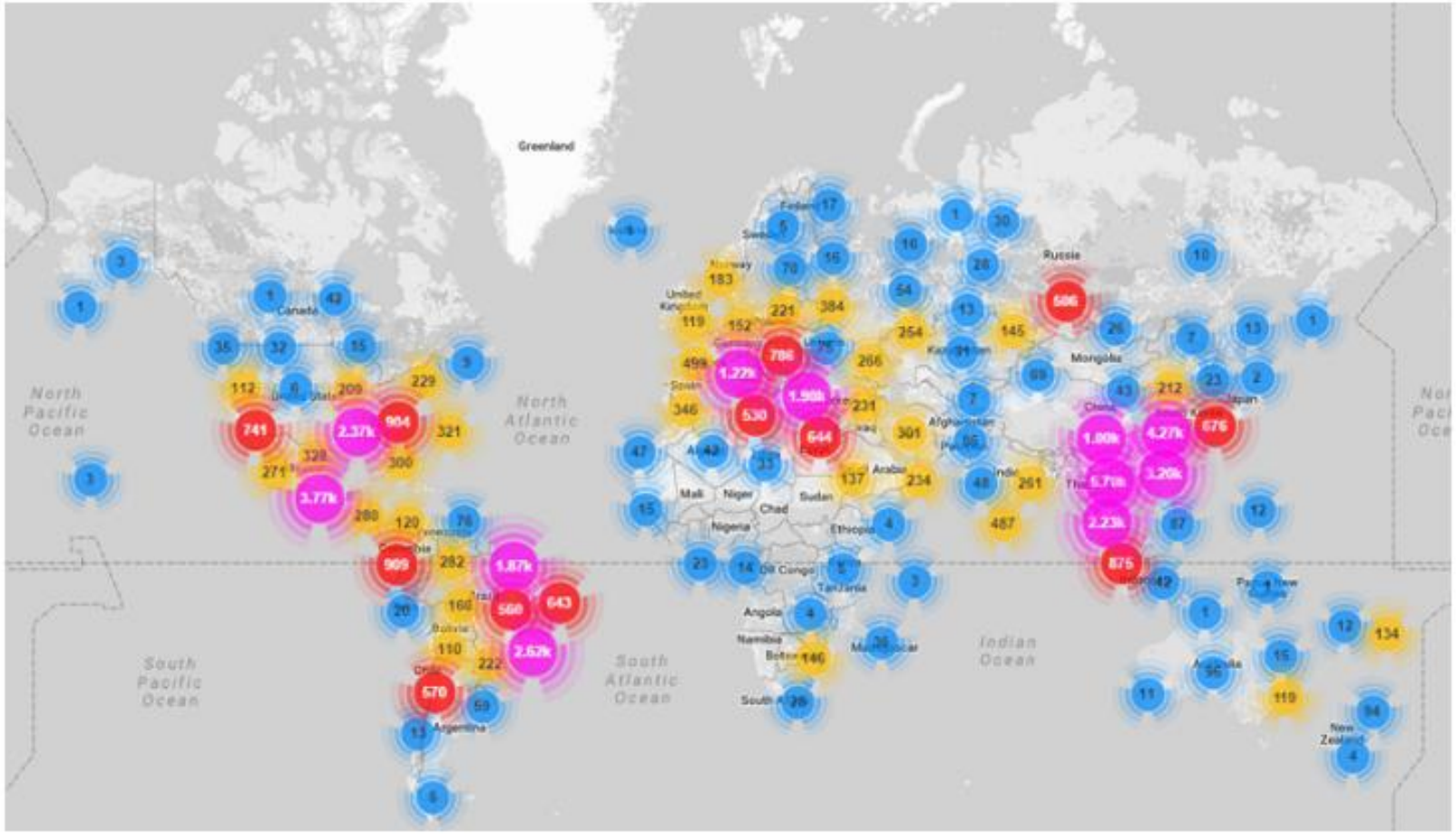


Figure 2: Geo-locations of all Mirai-infected devices uncovered so far

Country	% of Mirai botnet IPs
Vietnam	12.8%
Brazil	11.8%
United States	10.9%
China	8.8%
Mexico	8.4%
South Korea	6.2%
Taiwan	4.9%
Russia	4.0%
Romania	2.3%
Colombia	1.5%

Source:
https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

Mirai – Statistical View of the Attacks

- Mirai-powered GRE floods, peaked at 280 Gbps/130 Mpps
- Investigation of the attack uncovered 49,657 unique IPs which hosted Mirai-infected devices. As previously reported, these were mostly CCTV cameras—a popular choice of DDoS botnet herders.
- Other victimized devices included DVRs and routers.
- Overall, IP addresses of Mirai-infected devices were spotted in 164 countries. As evidenced by the map below, the botnet IPs are highly dispersed, appearing even in such remote locations as Montenegro, Tajikistan and Somalia.

Protecting IoT Devices Against Mirai (Botnets)

http://www.billslater.com/mirai.ppsx

- ***Change Your Password.*** This is not only good advice for those of us who shop online or who have been notified that the e-commerce site we recently shopped on has been breached, but likewise for IoT devices. In fact, according to this report, these better credentials can be used to provide a bulwark against botnet attacks like Mirai by substituting the hard-coded username and password with ones that are unique to your organization and not, of course, easily guessed.
- ***Turn them off.*** For currently deployed IoT devices, turn them off when not in use. If the Mirai botnet does infect a device, the password must be reset and the system rebooted to get rid of it.
- ***Disable all remote access to them.*** To protect devices from Mirai and other botnets, users should not only shield TCP/23 and TCP/2323 access to those devices, but also to disable all remote (WAN) access to them.
- ***Research Your Purchase.*** Before you even buy a product, research what you are buying and make sure that you know how to update any software associated with the device. Look for devices, systems, and services that make it easy to update the device and inform the end user when updates are available.
- ***Use It or Lose It.*** Once the product is in your office, turn off the functions you're are not using. Enabled functionality usually comes with increased security risks. Again, make sure you review that before you even bring the product into the workplace. If it's already there, don't be shy about calling customer service and walking through the steps needed to shut down any unused functions.

Source:
https://www.pwnieexpress.com/blog/mirai-botnet-part-2

Cloud Security Alliance (CSA) Internet of Things (IoT) Security Controls Framework

https://cloudsecurityalliance.org/artifacts/iot-security-controls-framework/

Cloud Security Alliance (CSA) Internet of Things (IoT) Security Controls Framework

https://cloudsecurityalliance.org/artifacts/iot-security-controls-framework/

CSA cloud security alliance® iot CONTROLS FRAMEWORK	For more details about the framework, download the "Guide to the CSA IoT Controls Framework" at: https://cloudsecurityalliance.org/artifacts/guide-to-the-iot-security-controls-framework	Supplement
Control Domain	**Control Specification**	**Additional Direction**
Secure Networks *Botnets*	Task network security tools to search for new botnet activity, and immediately remove infected IoT devices upon detection. Keep up to date on botnet characteristics using the CSA IoTWG botnet tracker (https://gitlab.com/brianr/CloudSA_IoT_WG/wikis/iot_botnets).	Use threat management to identity new botnet-based attacks and configure your audit systems based on indicators of compromise (e.g., outbound communications on specific ports). Bring any infected devices offline promptly to avoid spread.
Secure Networks *NFC*	Install Near Field Communication (NFC) technology devices in locations that do not lend themselves to installation of sniffers in close proximity. Establish physical security protection measures (e.g. cameras/guards) to monitor access to these devices.	
Secure Networks *Wireless Network Boundaries*	Define physical boundaries for WSNs and limit the power rating of ZigBee and ZWave devices to minimize signal leakage.	
Secure Networks *ZigBee Master Keys*	Distribute ZigBee Master Keys out of band. Never pass master keys over the network. Master keys are used to establish additional key material.	
Secure Networks *ZigBee Networks Keys*	Rotate ZigBee Network Keys at least annually, and disable prior keys upon distribution/establishment of the new network key.	
Secure Data *Data Classification*	Document data collected, processed, and stored within your IoT system. Classify that data based on data type and value (criticality to the organization and sensitivity). Tag data with metadata that can be used to identify types of data in your system.	Effective control requires an understanding of the data's value and the impact to the organization if security of that data is compromised. The level of control should correspond with that value.
Secure Data *DAR Encryption Controls*	After cataloging data in an IoT system, identify any locations and systems that store the data, and apply Data-at-Rest encryption controls to those locations and systems. Monitor to ensure new systems and components are not implemented without having been evaluated for their security when storing sensitive information.	NIST has two approved block ciphers: AES and TDEA (or TDES). Either of these would be recommended. However, because computational resources are limited on IoT devices, Lightweight Cryptography is being researched as an option.

Table of Contents

- Introduction – IT Pro SI on Cyberthreats and Security
- Grid Cybersecurity (Ukraine)
- CSA IoT Security (Controls and Mitigations)
- SamSam Ransomware Attack - US DOT
- VPKI Hits the Highway
- References + Q-A

Colorado DOT Ransomware Attack

https://www.govtech.com/security/Colorado-Hack-Offers-Larger-Lessons-for-Cybersafety.html

Colorado Hack Offers Larger Lessons for Cybersafety

The ransomware cyberattack against the Colorado Department of Transportation earlier this year was an impactful event but reinforced useful best practices.

by Theo Douglas / November 2, 2018
Shutterstock/Michael Traitov

The ransomware cyberattack against the city of Atlanta in March was arguably the year's most devastating cyberattack against a municipality, but the state of Colorado suffered a significant attack one month earlier that remains a source of valuable lessons for the public sector.

The Colorado Department of Transportation (CDOT) was hit by a brute-force attack in late February by a variant of the SamSam ransomware that penetrated a temporary system being tested without full security. (Officials strongly recommended securing even systems being tested or in limited deployment.) Once inside, bad actors used it to access CDOT, ultimately affecting roughly half its computing environment, around 400 servers, all databases and applications and around 1,300 workstations.

The event impacted CDOT's financial system, which processes around $100 million of financial payments monthly, forcing officials to find other ways including workarounds to pay vendors and employees. And while good network segmentation contained the outbreak, the malware reactivated roughly one week after the initial attack, prompting officials to seek additional resources from the Office of Emergency Management (OEM). Ultimately, Gov. John Hickenlooper issued an executive order making the event the first-ever state emergency declared for a cybersecurity incident.

RELATED

After CDOT Attack, Colorado CTO Talks Layers of DefenseWhat New Tech Holds the Most Promise for Colorado?Colorado Takes Point with Demanding Data Protection Standards

At the annual National Association of State Chief Information Officers (NASCIO) conference last month, Colorado Chief Technology Officer David McCurdy praised the governor and Legislature for being very supportive of efforts to stay ahead of cyberthreats and maintain a layered approach to cybersecurity. A criminal investigation by the FBI is believed to be ongoing, and while state agencies have recovered from the incident, state and local officials say it impressed upon them several key lessons about preparing for a cyberattack.

Iranian Hackers Arrested in Colorado DOT Ransomware Attack

https://www.govtech.com/security/Colorado-Hack-Offers-Larger-Lessons-for-Cybersafety.html

WANTED BY THE FBI

SAMSAM SUBJECTS

Conspiracy to Commit Fraud and Related Activity in Connection with Computers; Conspiracy to Commit Wire Fraud; Intentional Damage to a Protected Computer; Transmitting a Demand in Relation to Damaging a Protected Computer

Mohammad Mehdi Shah Mansouri

Faramarz Shahi Savandi

REMARKS

Mohammad Mehdi Shah Mansouri is an Iranian male with a date of birth of September 24, 1991. He has brown hair and brown eyes and was born in Qom, Iran.

Faramarz Shahi Savandi is an Iranian male who was born in Shiraz, Iran, on September 16, 1984. Both men are known to speak Farsi and reside in Tehran, Iran.

DETAILS

Mohammad Mehdi Shah Mansouri and Faramarz Shahi Savandi are wanted for allegedly launching SamSam ransom ware, aka MSIL/Samas.A attacks, which encrypted hundreds of computer networks in the United States and other countries. Since December of 2015, Shah Mansouri and Shahi Savandi have received over $6 million in ransom payments from victims across several sectors, including critical infrastructure, healthcare, transportation, and state/local governments.

Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses

A federal grand jury returned an indictment unsealed today in Newark, New Jersey charging Faramarz Shahi Savandi, 34, and Mohammad Mehdi Shah Mansouri, 27, both of Iran, in a 34-month-long international computer hacking and extortion scheme involving the deployment of sophisticated ransomware, announced Deputy Attorney General Rod J. Rosenstein, Assistant Attorney General Brian A. Benczkowski of the Justice Department's Criminal Division, U.S. Attorney Craig Carpenito for the District of New Jersey and Executive Assistant Director Amy S. Hess of the FBI.

The six-count indictment alleges that Savandi and Mansouri, acting from inside Iran, authored malware, known as "SamSam Ransomware," capable of forcibly encrypting data on the computers of victims. According to the indictment, beginning in December 2015, Savandi and Mansouri would then allegedly access the computers of victim entities without authorization through security vulnerabilities, and install and execute the SamSam Ransomware on the computers, resulting in the encryption of data on the victims' computers. These more than 200 victims included hospitals, municipalities, and public institutions, according to the indictment, including the City of Atlanta, Georgia; the City of Newark, New Jersey; the Port of San Diego, California; the Colorado Department of Transportation; the University of Calgary in Calgary, Alberta, Canada; and six health care-related entities: Hollywood Presbyterian Medical Center in Los Angeles, California; Kansas Heart Hospital in Wichita, Kansas; Laboratory Corporation of America Holdings, more commonly known as LabCorp, headquartered in Burlington, North Carolina; MedStar Health, headquartered in Columbia, Maryland; Nebraska Orthopedic Hospital now known as OrthoNebraska Hospital, in Omaha, Nebraska and Allscripts Healthcare Solutions Inc., headquartered in Chicago, Illinois.

According to the indictment, Savandi and Mansouri would then extort victim entities by demanding a ransom paid in the virtual currency Bitcoin in exchange for decryption keys for the encrypted data, collecting ransom payments from victim entities that paid the ransom, and exchanging the Bitcoin proceeds into Iranian rial using Iran-based Bitcoin exchangers. The indictment alleges that, as a result of their conduct, Savandi and Mansouri have collected over $6 million USD in ransom payments to date, and caused over $30 million USD in losses to victims.

Table of Contents

- Introduction – IT Pro SI on Cyberthreats and Security
- Grid Cybersecurity (Ukraine)
- CSA IoT Security (Controls and Mitigations)
- SamSam Ransomware Attack - US DOT
- VPKI Hits the Highway
- References + Q-A

Connected Vehicle and Intelligent Transportation Systems

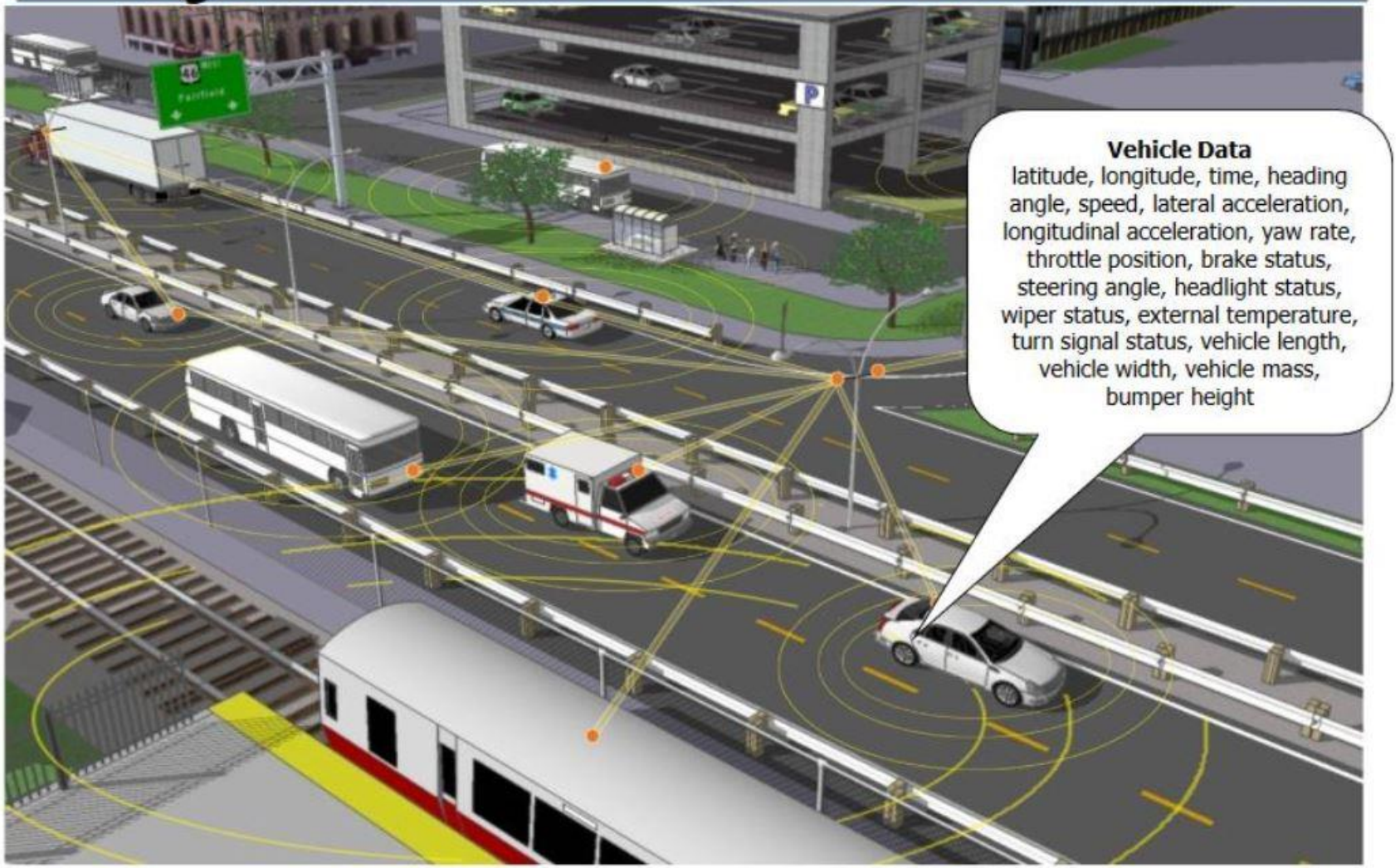
US DOT Connected Vehicle Pilot Program and EU Cooperative ITS (C-ITS)

Tim Weil – CISSP/CCSP, CISA, PMP
Alcohol Monitoring Systems
IEEE Senior Member
Member COMSOC, ITS Societies

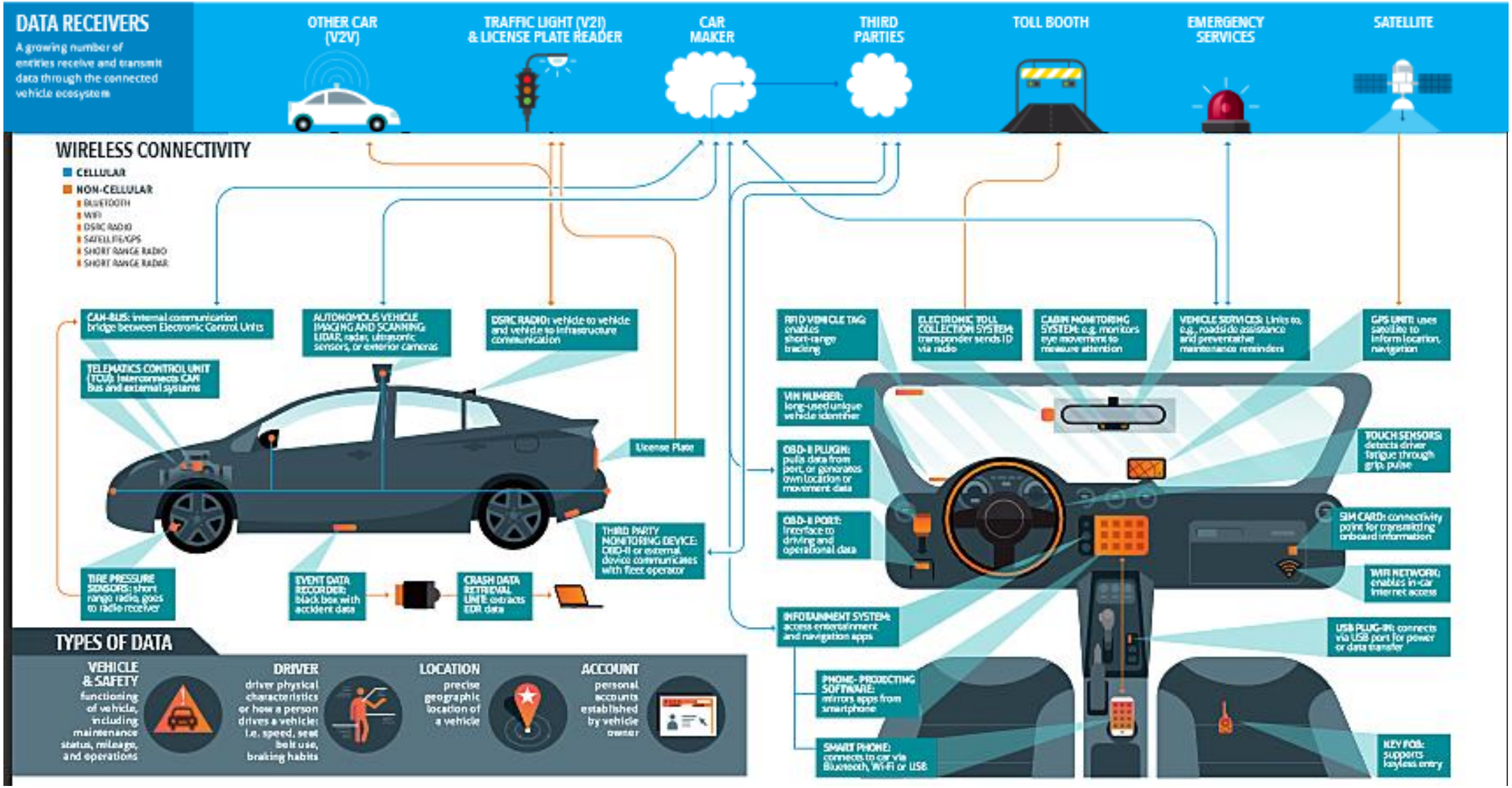
AT&T
Greenwood Village, CO
6 Dec 2017

US DOT Model

Fully Connected Vehicle



Future of Privacy Forum Infographics - Data and the Connected Car https://fpf.org



Today's connected technologies are making transportation safer and more convnient. Many new features are enabled by the collection and processing of data. Cars are becoming part of a trusted mobile ecosystem that ensures data flows between a network of carmakers, vendors and others to support individuals' safety, logistics, infotainment, and security needs. This visual represents devices that may be employed in today's connected cars; no single vehicle will have all of these features, but most new vehicles have some. Much connected car data is protected by technical controls, laws, self-regulatory commitments, privacy policies, and other emerging mechanisms or controls.

Introduction – USDOT ITS National Architecture (ARC-IT)

http://local.iteris.com/arc-it/index.html

United States Department of Transportation

About DOT | Briefing Room | Our Activiti

ARC-IT Version 8.0

Including the National ITS Architecture and CVRIA

Architecture ▾ | Architecture Use ▾ | Architecture Resources ▾ | Architecture Terminology ▾ | Contact The Architecture Team

Home

Architecture Reference for Cooperative and Intelligent Transportation

The Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) provides a common framework for planning, defining, and integrating intelligent transportation systems. It is a mature product that reflects the contributions of a broad cross-section of the ITS community (transportation practitioners, systems engineers, system developers, technology specialists, consultants, etc.).

ARC-IT is a reference architecture: it provides common basis for planners and engineers with differing concerns to conceive, design and implement systems using a common language as a basis for delivering ITS, but does not mandate any particular implementation. ARC-IT includes artifacts that answer concerns relevant to a large variety of stakeholders, and provides tools intended for transportation planners, regional architects and systems engineers to conceive of and develop regional architectures, and scope and develop projects.

To get started, begin with the menu bar above:

- Architecture contains links to all of the content inside the architecture, and describes the structure of the architecture. In particular:
  - Service Packages provide the most straightforward entry into ARC-IT content. Similar in appearance to CVRIA applications, these include all of the services defined in both CVRIA and the National ITS Architecture 7.1.
  - Views and its sub-menus provide view-specific content; if for example you are looking for a particular information flow, or a particular communications profile, browse the relevant physical and communications sections here.
  - Methodology and its sub-menus describe the structure of the architecture: how it is built, how the artifacts within are inter-related.
  - The Security section describes how security is addressed throughout the architecture and provides links to cross-cutting security content.
- Architecture Use describes how to use ARC-IT, from the perspective of a regional architect or project systems engineer.
- Architecture Resources provides access to all ARC-IT content in user-downloadable forms. Notably this also includes access to our tools: RAD-IT and SET-IT, that provide you with means to manipulate the architecture according to models' rules, customizing the reference architecture to your regional or project needs.
- Architecture Terminology provides those definitions that permeate these pages.
- Contact the Architecture Team gives you a direct line to the source. We want to hear from you! If you have questions, concerns or find an error (say it isn't so!) we'd like to know about it!

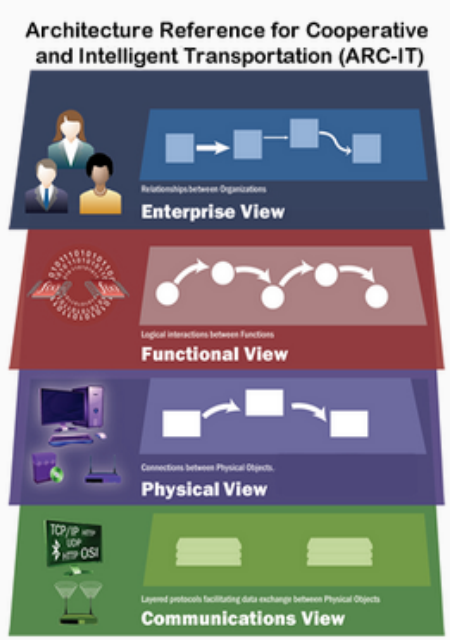
Latest News

RAD-IT Version 8.0.47 is available as a download from the Tools page. Read more...

ARC-IT Version 8.0 is a major release of the National ITS Architecture that merges, unifies, and enhances Version 7.1 of the National ITS Architecture and CVRIA Version 2.2. Read more...

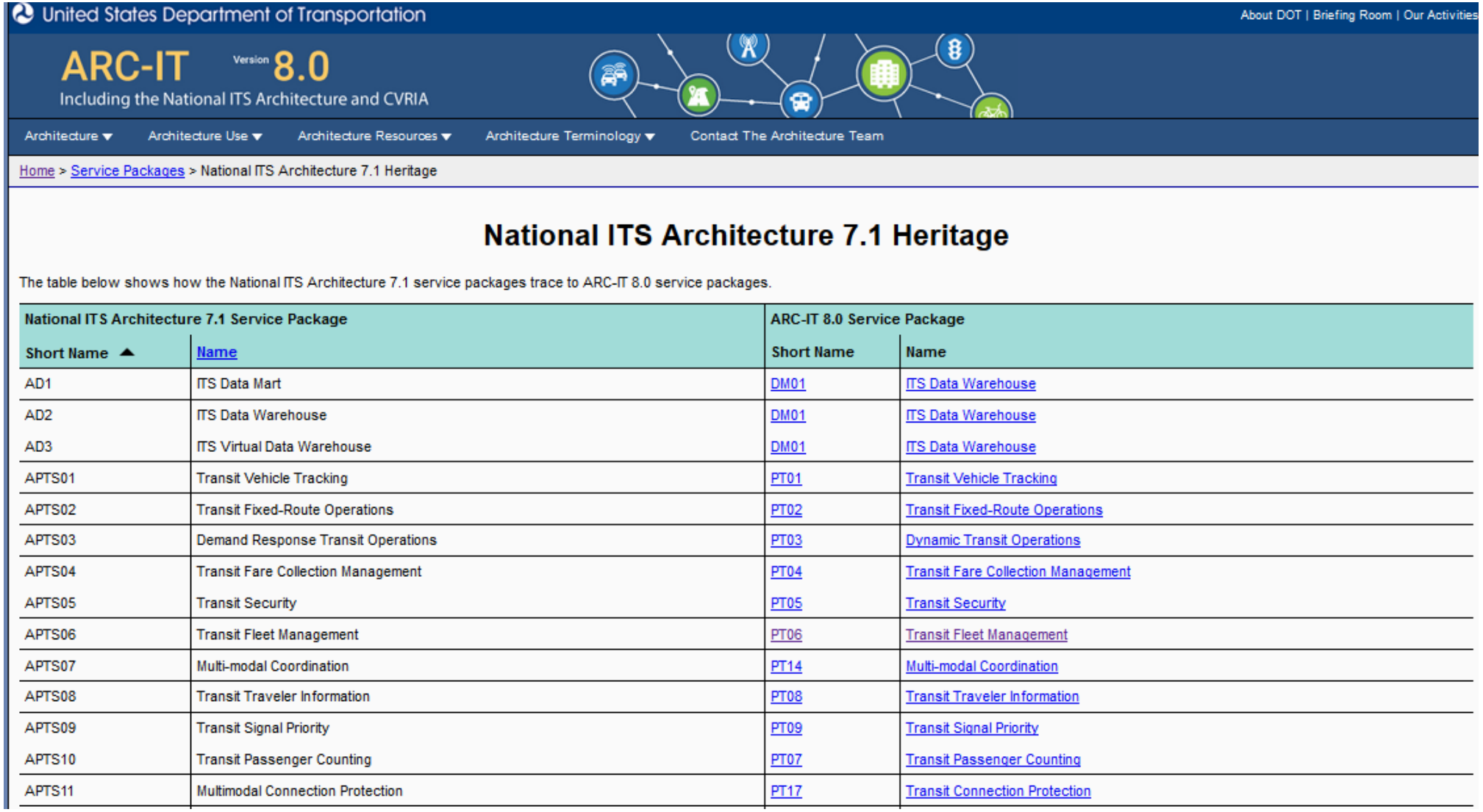
SET-IT Version 8.0 is a major new release of the systems engineering software tool that includes all of the ARC-IT content, spanning all of ITS, and includes many fixes and upgrades. Read more...

The architecture team is planning workshops to be held this summer in San Jose and Detroit. We will provide an in-person overview of the changes to ARC-IT, demonstrate its use and answer any and all questions. Read more...



Catalog of Services (CVRIA)

http://local.iteris.com/arc-it/html/servicepackages/servicepackages-areaspsort.html



United States Department of Transportation

About DOT | Briefing Room | Our Activities

ARC-IT Version 8.0

Including the National ITS Architecture and CVRIA

Architecture ▾ | Architecture Use ▾ | Architecture Resources ▾ | Architecture Terminology ▾ | Contact The Architecture Team

Home > Service Packages > National ITS Architecture 7.1 Heritage

National ITS Architecture 7.1 Heritage

The table below shows how the National ITS Architecture 7.1 service packages trace to ARC-IT 8.0 service packages.

National ITS Architecture 7.1 Service Package		ARC-IT 8.0 Service Package	
Short Name ▲	Name	Short Name	Name
AD1	ITS Data Mart	DM01	ITS Data Warehouse
AD2	ITS Data Warehouse	DM01	ITS Data Warehouse
AD3	ITS Virtual Data Warehouse	DM01	ITS Data Warehouse
APTS01	Transit Vehicle Tracking	PT01	Transit Vehicle Tracking
APTS02	Transit Fixed-Route Operations	PT02	Transit Fixed-Route Operations
APTS03	Demand Response Transit Operations	PT03	Dynamic Transit Operations
APTS04	Transit Fare Collection Management	PT04	Transit Fare Collection Management
APTS05	Transit Security	PT05	Transit Security
APTS06	Transit Fleet Management	PT06	Transit Fleet Management
APTS07	Multi-modal Coordination	PT14	Multi-modal Coordination
APTS08	Transit Traveler Information	PT08	Transit Traveler Information
APTS09	Transit Signal Priority	PT09	Transit Signal Priority
APTS10	Transit Passenger Counting	PT07	Transit Passenger Counting
APTS11	Multimodal Connection Protection	PT17	Transit Connection Protection

Introduction − ITS Use Cases Services and Applications

CONNECTED VEHICLE APPLICATIONS

V2I Safety

- Red Light Violation Warning
- Curve Speed Warning
- Stop Sign Gap Assist
- Spot Weather Impact Warning
- Reduced Speed/Work Zone Warning
- Pedestrian in Signalized Crosswalk Warning (Transit)

V2V Safety

- Emergency Electronic Brake Lights (EEBL)
- Forward Collision Warning (FCW)
- Intersection Movement Assist (IMA)
- Left Turn Assist (LTA)
- Blind Spot/Lane Change Warning (BSW/LCW)
- Do Not Pass Warning (DNPW)
- Vehicle Turning Right in Front of Bus Warning (Transit)

Agency Data

- Probe-based Pavement Maintenance
- Probe-enabled Traffic Monitoring
- Vehicle Classification-based Traffic Studies
- CV-enabled Turning Movement & Intersection Analysis
- CV-enabled Origin-Destination Studies
- Work Zone Traveler Information

Environment

- Eco-Approach and Departure at Signalized Intersections
- Eco-Traffic Signal Timing
- Eco-Traffic Signal Priority
- Connected Eco-Driving
- Wireless Inductive/Resonance Charging
- Eco-Lanes Management
- Eco-Speed Harmonization
- Eco-Cooperative Adaptive Cruise Control
- Eco-Traveler Information
- Eco-Ramp Metering
- Low Emissions Zone Management
- AFV Charging / Fueling Information
- Eco-Smart Parking
- Dynamic Eco-Routing (light vehicle, transit, freight)
- Eco-ICM Decision Support System

Road Weather

- Motorist Advisories and Warnings (MAW)
- Enhanced MDSS
- Vehicle Data Translator (VDT)
- Weather Response Traffic Information (WxTINFO)

Mobility

- Advanced Traveler Information System
- Intelligent Traffic Signal System (I-SIG)
- Signal Priority (transit, freight)
- Mobile Accessible Pedestrian Signal System (PED-SIG)
- Emergency Vehicle Preemption (PREEMPT)
- Dynamic Speed Harmonization (SPD-HARM)
- Queue Warning (Q-WARN)
- Cooperative Adaptive Cruise Control (CACC)
- Incident Scene Pre-Arrival Staging Guidance for Emergency Responders (RESP-STG)
- Incident Scene Work Zone Alerts for Drivers and Workers (INC-ZONE)
- Emergency Communications and Evacuation (EVAC)
- Connection Protection (T-CONNECT)
- Dynamic Transit Operations (T-DISP)
- Dynamic Ridesharing (D-RIDE)
- Freight-Specific Dynamic Travel Planning and Performance
- Drayage Optimization

Smart Roadside

- Wireless Inspection
- Smart Truck Parking

Connected Vehicle Pilot Deployment Program, V. Fessmann, US DOT ITS JPO
https://www.its.dot.gov/pilots/pdf/CV_PilotWebinar5_Devices_QPL.pdf

US DOT ITS JPO – Connected Vehicle Pilot Deployment Program

https://www.its.dot.gov/pilots/

Tampa-Hillsborough Expressway Authority (THEA) Pilot

https://www.its.dot.gov/pilots/pilots_thea.htm

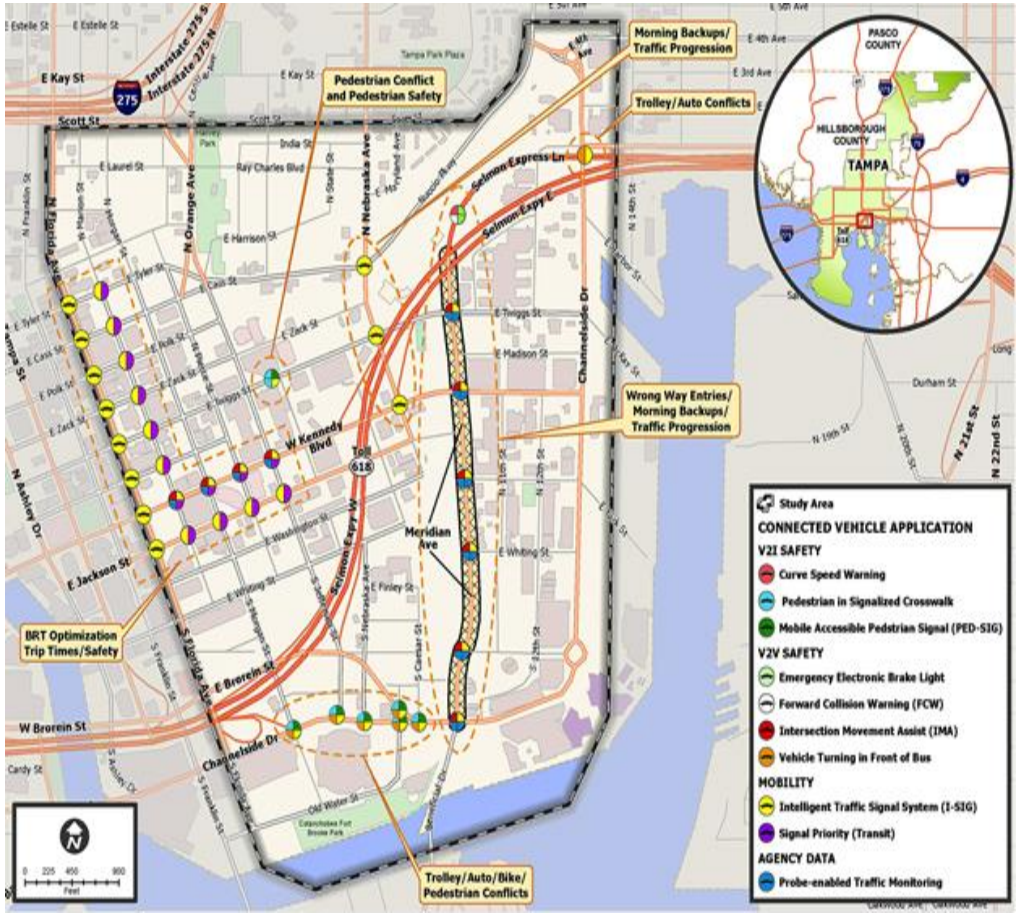


Table 1. Tampa (THEA) Pilot Site Proposed CV Applications

ID	Category	Tampa (THEA) – CV Application
1	V2I Safety	End of Ramp Deceleration Warning (ERDW)
2		Pedestrian in Signalized Crosswalk Warning (PED-X)
3		Wrong Way Entry (WWE)
4	V2V Safety	Emergency Electronic Brake Lights (EEBL)
5		Forward Collision Warning (FCW)
6		Intersection Movement Assist (IMA)
7		Vehicle Turning Right in Front of a Transit Vehicle (VTRFTV)
8	Mobility	Mobile Accessible Pedestrian Signal System (PED-SIG)
9		Intelligent Traffic Signal System (I-SIG)
10		Transit Signal Priority (TSP)
11	Agency Data	Probe-enabled Data Monitoring (PeDM)

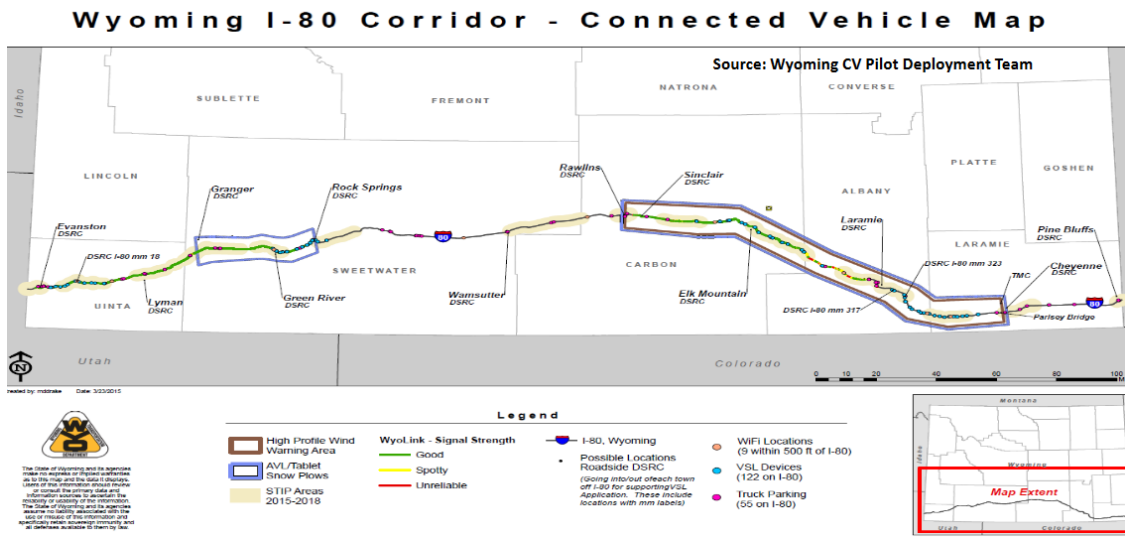
Table 2. Tampa (THEA) Pilot Site Proposed CV Devices

Tampa (THEA) – Devices	Estimated Number
Roadside Unit (RSU) at Intersection	40
Vehicle Equipped with On-Board Unit (OBU)	1,600
Pedestrian Equipped with App in Smartphone	500
HART Transit Bus Equipped with OBU	10
TECO Line Street Car Equipped with OBU	10
Total Equipped Vehicles	1,620

Tampa-Hillsborough Expressway Authority (THEA) owns and operates the Selmon Reversible Express Lanes (REL), which is a first-of-its-kind facility to address urban congestion. The REL morning commute endpoint intersection is on major routes into and out of the downtown Tampa commercial business district. Drivers experience significant delay during the morning peak hour resulting in, and often caused by, a correspondingly large number of rear-end crashes and red light running collisions. Because the lanes are reversible, wrong way entry is possible.The THEA CV Pilot will employ Dedicated Short Range Communication (DSRC) to enable transmissions among approximately 1,600 cars, 10 buses, 10 trolleys, 500 pedestrians with smartphone applications, and approximately 40 roadside units.

Wyoming (WY) DOT Connected Car Pilot

https://wydotcvp.wyoroad.info/



Wyoming is an important freight corridor that plays a critical role in the movement of goods across the country and between the United States, Canada, and Mexico. As shown in the figure below, Interstate 80 (I-80) in southern Wyoming which is above 6000 feet is a major corridor for east/west freight movement and moves more than 32 million tons of freight per year. During winter seasons when wind speeds and wind gusts exceed 30 mph and 65 mph respectively, crash rates on I-80 have been found to be 3 to 5 times as high as summer crash rates. This resulted in 200 truck blowovers within 4 years and often led to road closures.

Table 1. WYDOT Pilot Site Proposed CV Applications

ID	Category	ICF/WYDOT – CV Application
1	V2V Safety	Forward Collision Warning (FCW)
2	V2I/I2V Safety	I2V Situational Awareness*
3		Work Zone Warnings (WZW)*
4		Spot Weather Impact Warning (SWIW)*
5	V2I and V2V Safety	Distress Notification (DN)

Table 2. WYDOT Pilot Site Proposed CV Devices

ICF/WYDOT – Devices	Estimated Number
Roadside Unit (RSU)	75
WYDOT Fleet Subsystem On-Board Unit (OBU)	100
Integrated Commercial Truck Subsystem OBU	150
Retrofit Vehicle Subsystem OBU	25
Basic Vehicle Subsystem OBU	125
Total Equipped Vehicles	400

WYDOT will develop systems that support the use of CV Technology along the 402 miles of I-80 in Wyoming. As listed in Table 2, approximately 75 roadside units (RSUs) that can receive and broadcast message using Dedicated Short Range Communication (DSRC) will be deployed along various sections of I-80. WYDOT will equip around 400 vehicles, a combination of fleet vehicles and commercial trucks with on-board units (OBUs). Of the 400 vehicles, at least 150 would be heavy trucks that are expected to be regular users of I-80. In addition, of the 400 equipped-vehicles, 100 WYDOT fleet vehicles, snowplows and highway patrol vehicles, will be equipped with OBUs and mobile weather sensors. units along city streets

New York City (NYC) Connected Car Pilot - http://www.cvp.nyc/

The NYCDOT leads the New York City Pilot, which aims to improve the safety of travelers and pedestrians in the city through the deployment of V2V and V2I connected vehicle technologies. This objective directly aligns with the city's Vision Zero initiative. In 2014, NYC began its *Vision Zero* program to reduce the number of fatalities and injuries resulting from traffic crashes.

ID	Category	NYCDOT – CV Application
1	V2I/I2V Safety	Speed Compliance
2		Curve Speed Compliance
3		Speed Compliance/Work Zone
4		Red Light Violation Warning
5		Oversize Vehicle Compliance
6		Emergency Communications and Evacuation Information
7	V2V Safety	Forward Crash Warning (FCW)
8		Emergency Electronics Brake Lights (EEBL)
9		Blind Spot Warning (BSW)
10		Lane Change Warning/Assist (LCA)
11		Intersection Movement Assist (IMA)
12		Vehicle Turning Right in Front of Bus Warning
13	V2I/I2V Pedestrian	Pedestrian in Signalized Crosswalk
14		Mobile Accessible Pedestrian Signal System (PED-SIG)
15	Mobility	Intelligent Traffic Signal System (I-SIGCVDATA)

NYCDOT – Devices	Estimated Number
Roadside Unit (RSU) at Manhattan and Brooklyn Intersections and FDR Drive	353
Taxi Equipped with Aftermarket Safety Device (ASD)*	5,850
MTA Fleet Equipped with ASD*	1,250
UPS Truck Equipped with ASD*	400
NYCDOT Fleet Equipped with ASD*	250
DSNY Fleet Equipped with ASD*	250
Vulnerable Road User (Pedestrians/Bicyclists) Device	100
PED Detection System	10 + 1 spare
Total Equipped Vehicles	8,000

The NYCDOT CV Pilot Deployment project area encompasses three distinct areas in the boroughs of Manhattan and Brooklyn (see the figure below). The first area includes a 4-mile segment of Franklin D. Roosevelt (FDR) Drive in the Upper East Side and East Harlem neighborhoods of Manhattan. The second area includes four one-way corridors in Manhattan. The third area covers a 1.6-mile segment of Flatbush Avenue in Brooklyn. As shown in Table 2, approximately 5,800 cabs, 1,250 MTA buses, 400 commercial fleet delivery trucks, and 500 City vehicles will be fit with CV technology. The deployment will include approximately 310 signalized intersections for vehicle-to-infrastructure (V2I) technology using DSRC technology.

New York City (NYC) Connected Car Pilot - http://www.cvp.nyc/

Applications by Connected Vehicle Test Bed

ICF/Wyoming
Work Zone Warnings
Spot Weather Impact Warning
Situational Awareness
Freight-Specific Dynamic Travel Planning
Automatic Alerts for Emergency Responders
CV-enabled Weather-Responsive Variable Speed Limits
Road Weather Advisories for Trucks and Vehicles
Truck Parking Availability for Freight Carriers

Tampa (THEA)
Curve Speed Warning
Pedestrian in Signalized Crosswalk Warning (Transit)
Emergency Electronic Brake Lights (EEBL)
Forward Collision Warning (FCW)
Intersection Movement Assist (IMA)
Vehicle Turning Right in Front of Bus Warning (Transit)
Intelligent Traffic Signal System (I-SIG)
Mobile Accessible Pedestrian Signal System (PED-SIG)
Transit Signal Priority (TSP)
Probe-enabled Traffic Monitoring

New York City (NYC)
Curve Speed Warning
Pedestrian in Signalized Crosswalk Warning (Transit)
Red Light Violation Warning
Reduced Speed/Work Zone Warning
Blind Spot Warning (BSW) *
Emergency Electronic Brake Lights (EEBL) *
Forward Crash Warning *
Intersection Movement Assist (IMA) *
Lane Change Assist (LCA) *
Stationary Vehicle Ahead (SVA) *
Vehicle Turning Right in Front of Bus Warning (Transit)
Advanced Traveler Information System
Emergency Communications and Evacuation (EVAC)
Freight-Specific Dynamic Travel Planning and Performance Measurement (F-ATIS)
Intelligent Traffic Signal System (I-SIG)
Mobile Accessible Pedestrian Signal System (PED-SIG)
Eco-Speed Harmonization

- **Deployment of applications is dependent upon Final ConOps and funding*

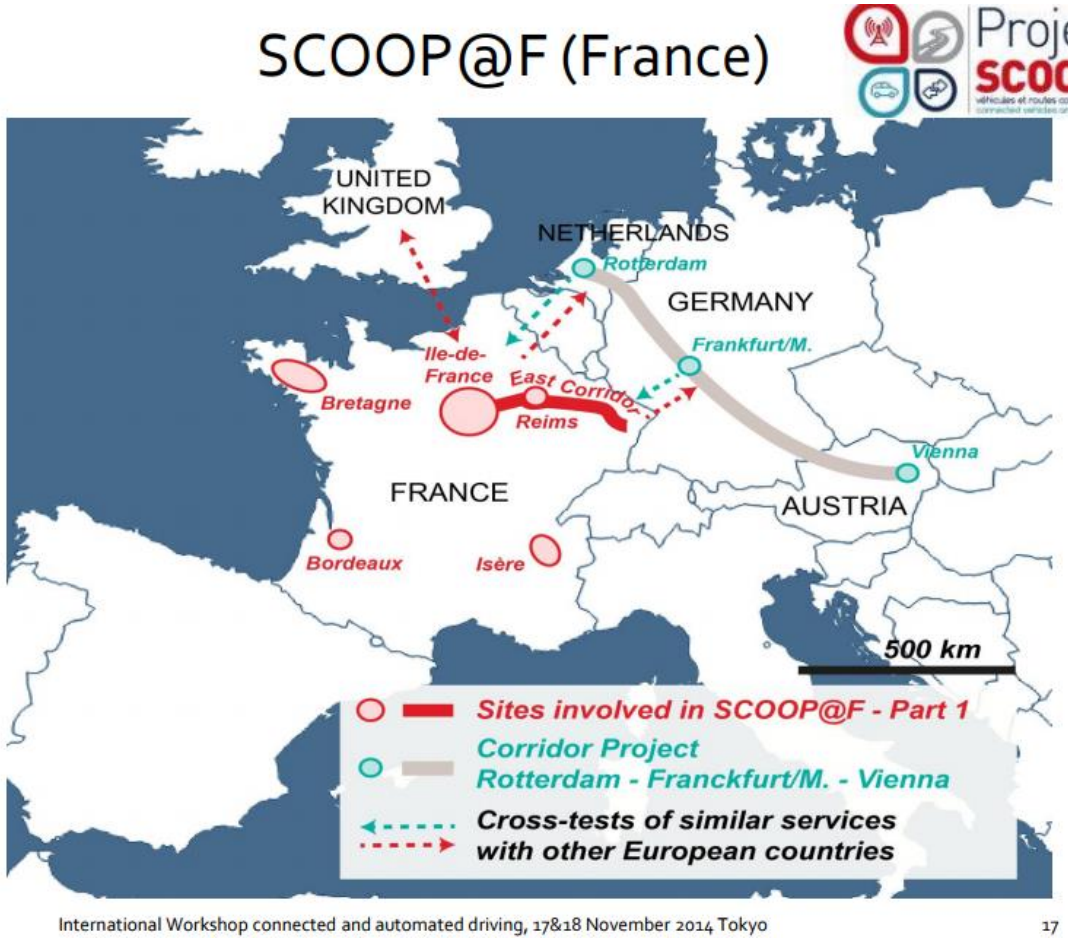
EU C-ITS Resources

EU Consortium Active ITS Road Projects (EU)

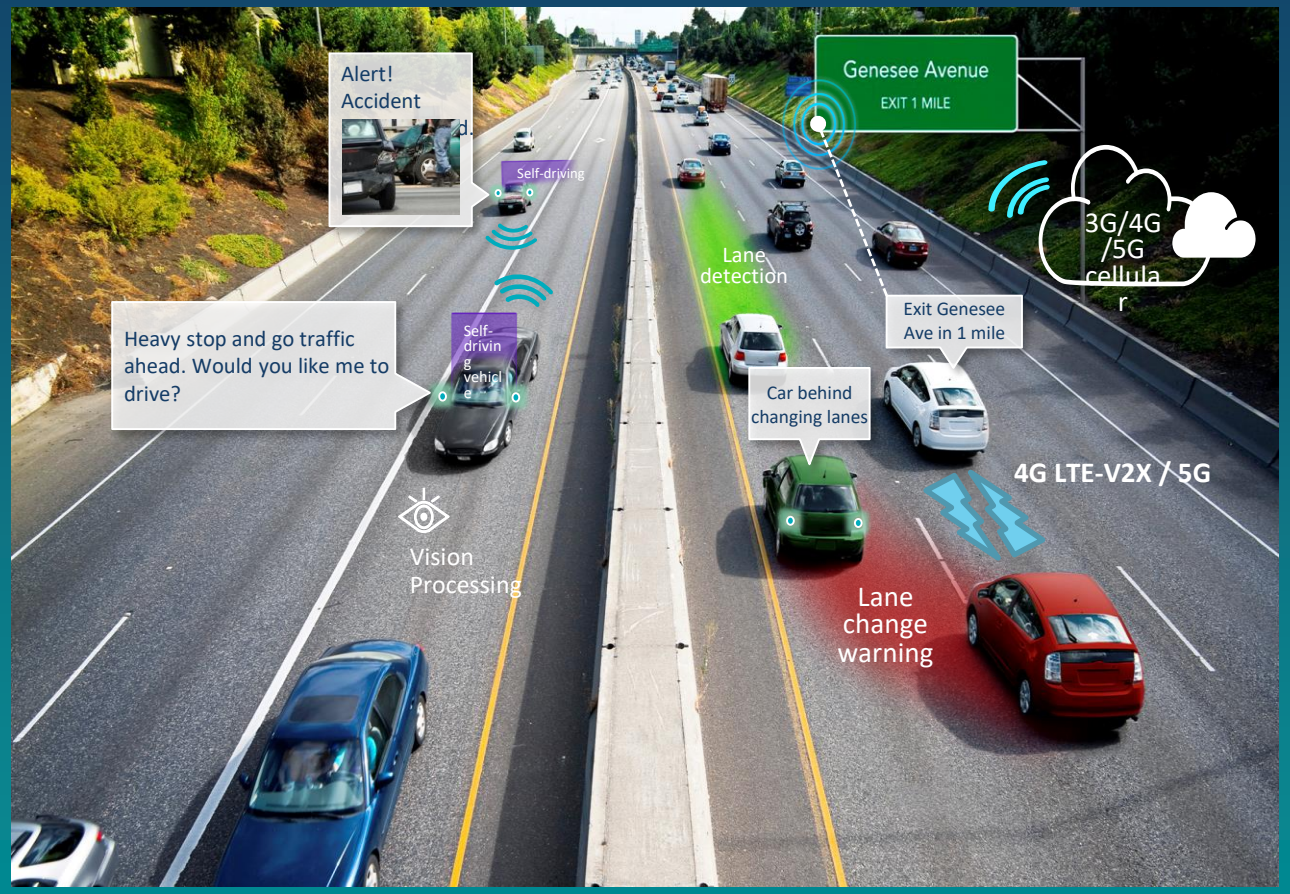
- C-ITS Cooperative, Connected and Automated Mobility
- EU Open In-Vehicle Platform
- EU ITS Road Corridor Initiatives - Amsterdam Group
- Connected Vehicles and Roads - Project Scoop@F
- Cooperative ITS Deployment Coordination Support
- Project Scoop@F- EU ITS Corridors
- C-ITS Applications – SCOOP@F

EU Consortium Foundation Projects (EU)

- Secure Vehicle Communication (SeVeCom)
- Car-To-Car Consortium (Car2Car)
- ITS-Europe(Ertico)
- EU C2C Pilot Program
- CVIS - Cooperative Vehicles Infrastructure Systems



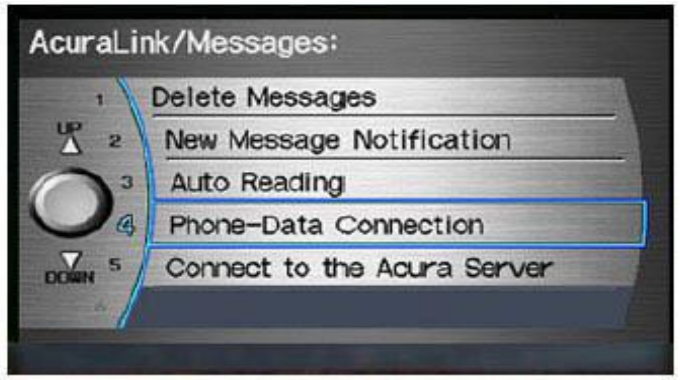
A New Era of Connected Car Capabilities



The variety of connected vehicle applications can be handled by a variety of over the air technologies, depending on application requirements

ITS Security and Privacy – Data You Can Trust

Privacy



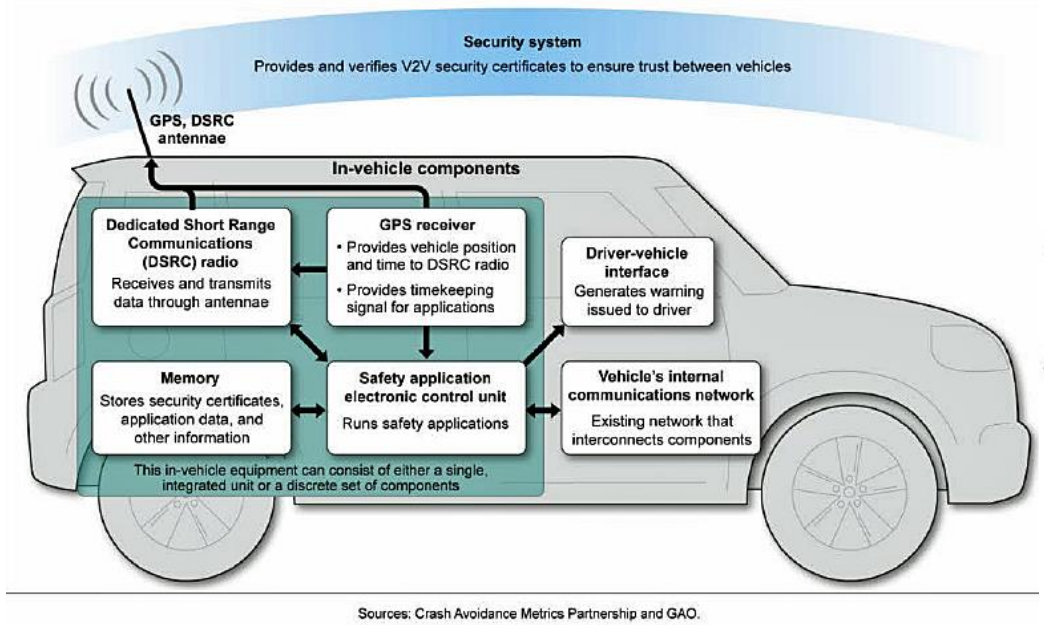
Confidentiality

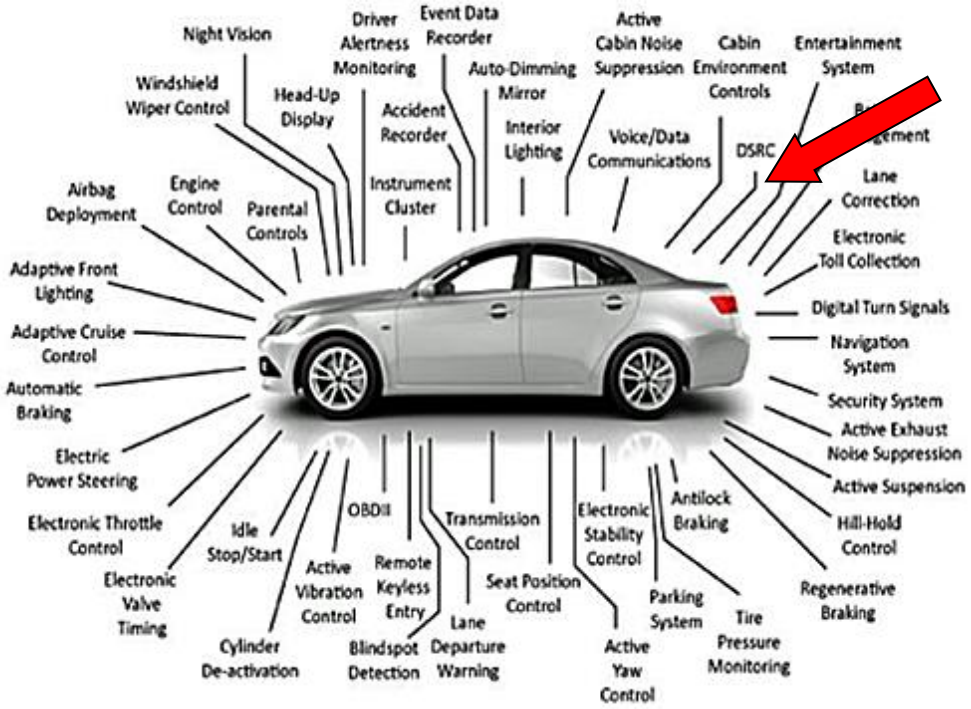
Availability

Integrity

Note – SCSM Design emphasizes ‘Authenticity’ (trust the sender) and ‘availability’ is not highlighted in the VPKI specification

Smart vehicle are *unsecure robots*





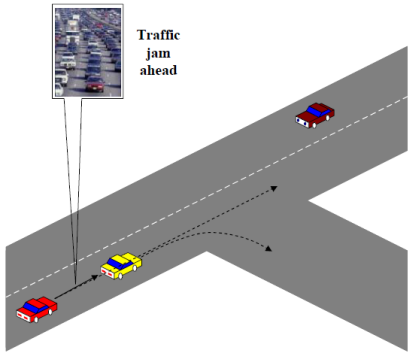
- Modern cars include:
  - more than 80 ECUs
  - many logically interacting subsystems

- …sensors, actuators, and their intelligent interconnection

**** A. Bicchi, L. Pallottino, et al, "Misbehavior Detection in Large Networks of Heterogeneous Vehicles", CAMP Workshop on Misbehavior Detection - https://stash.campllc.org/projects/SCMS/repos/mbd-workshop/browse/Day%202%20-%203%20-%20V2X%20Talk%20Fagiolini.pptx**

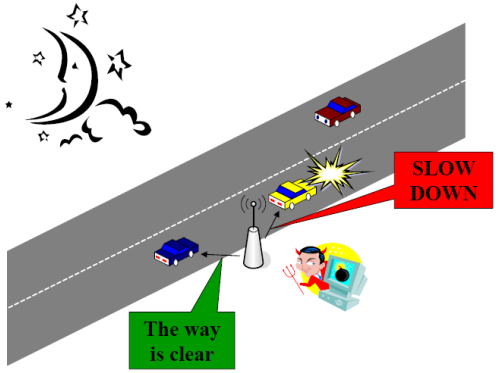
Security Architecture for VANETS (EPFL V-PKI – J.Hubaux et. al.) - 2004

Attack 1 : Bogus traffic information



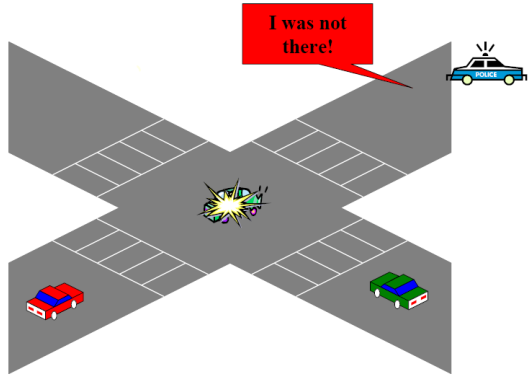
- Attacker: insider, rational, active

Attack 2 : Disruption of network operation



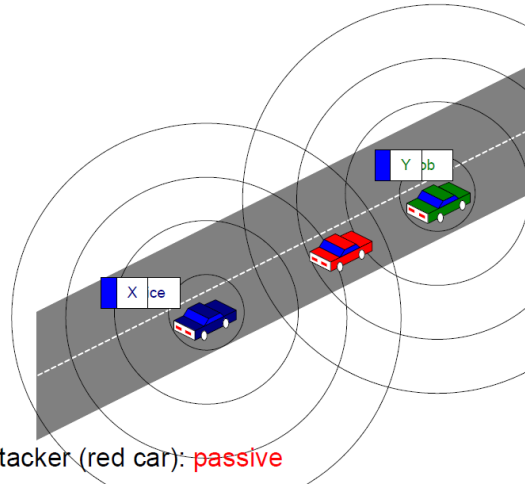
- Attacker: malicious, active

Attack 3: Cheating with identity, position or speed



- Attacker: insider, rational, active

Attack 4 : Uncovering the identities of other vehicles

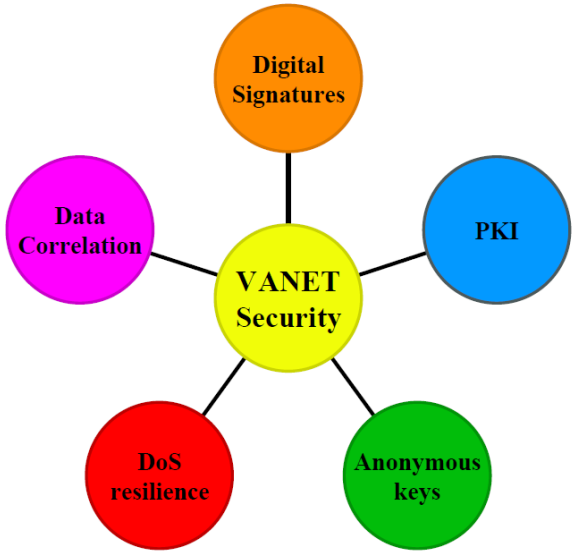


- Attacker (red car): passive

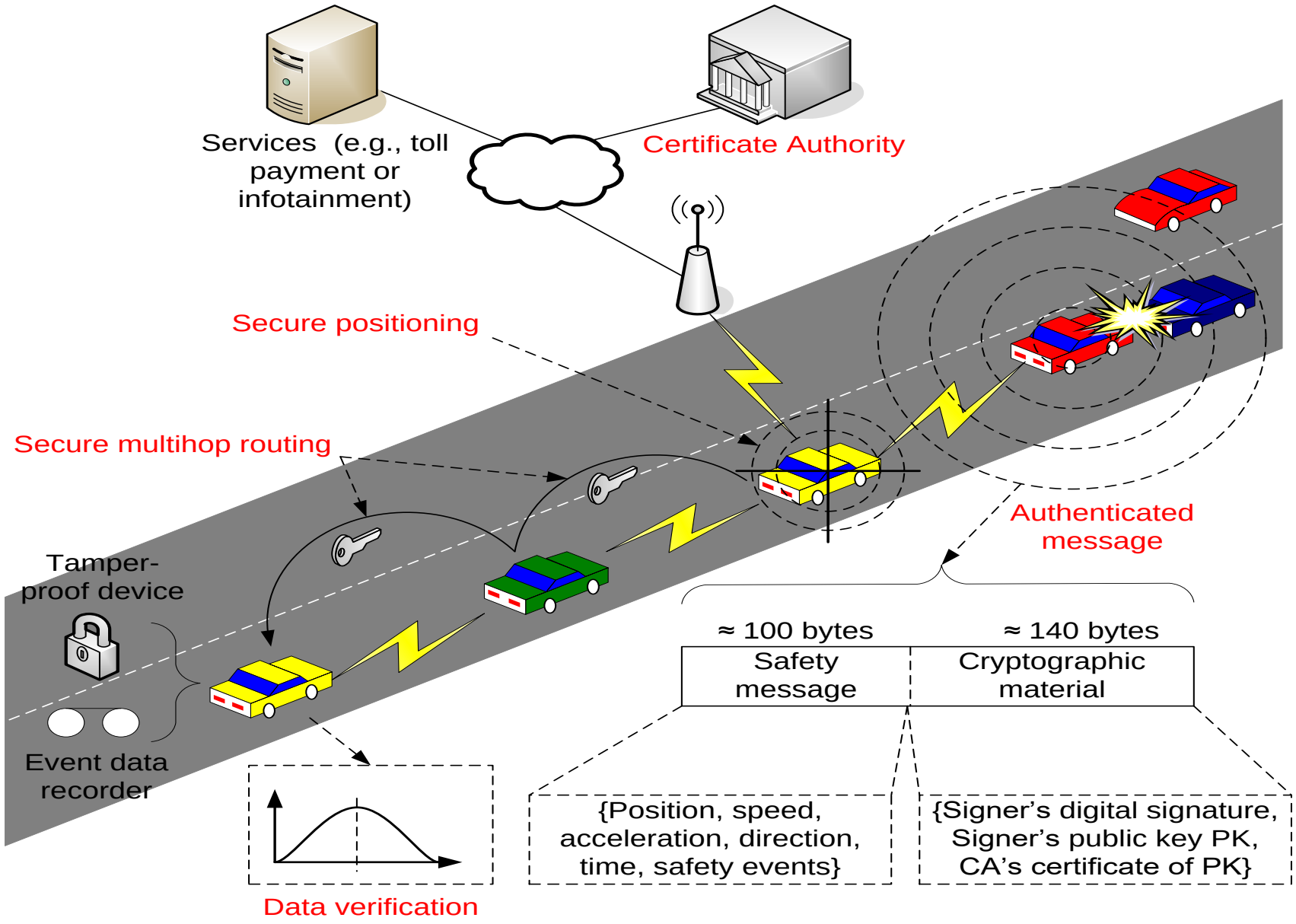
Attacker's model in Vehicular Communications

- An attacker can be an outsider or an insider and malicious or rational
- An attack can be active or passive
- Attacks against anonymous messages:
  - Bogus information
- Attacks against liability-related messages:
  - Cheating with own identity
  - Cheating with position or speed
- Attacks against both kinds of messages:
  - Uncovering identities of other vehicles
  - Disruption of network operation (Denial of Service attacks)

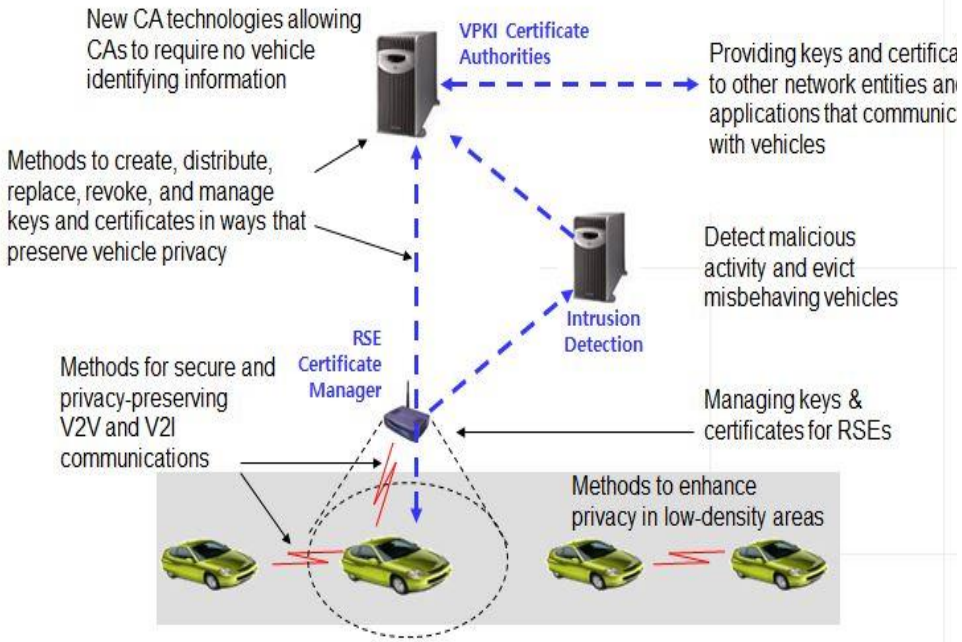
How to secure VANETs

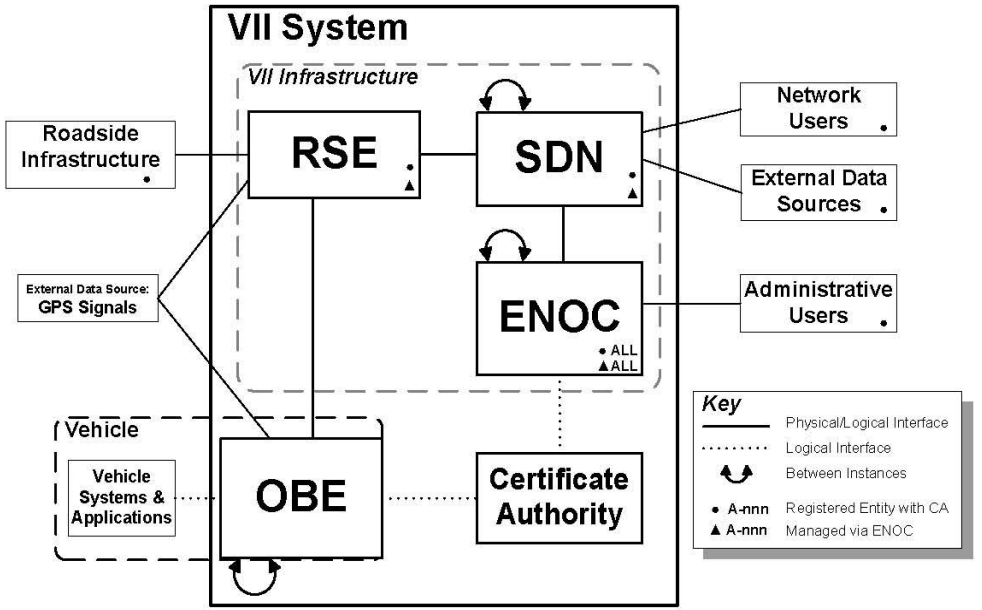


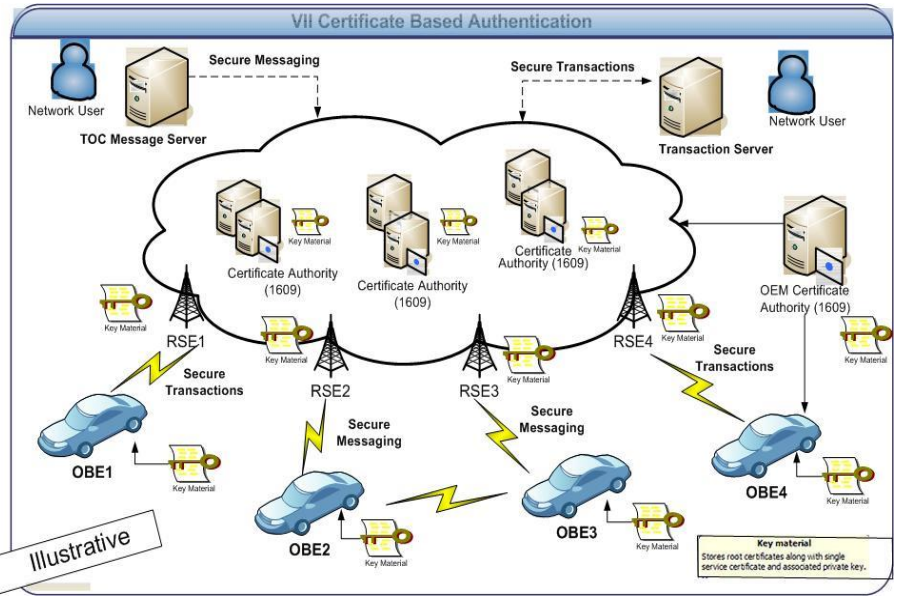
Security Architecture (EPFL V-PKI – J.Hubaux et. al.)

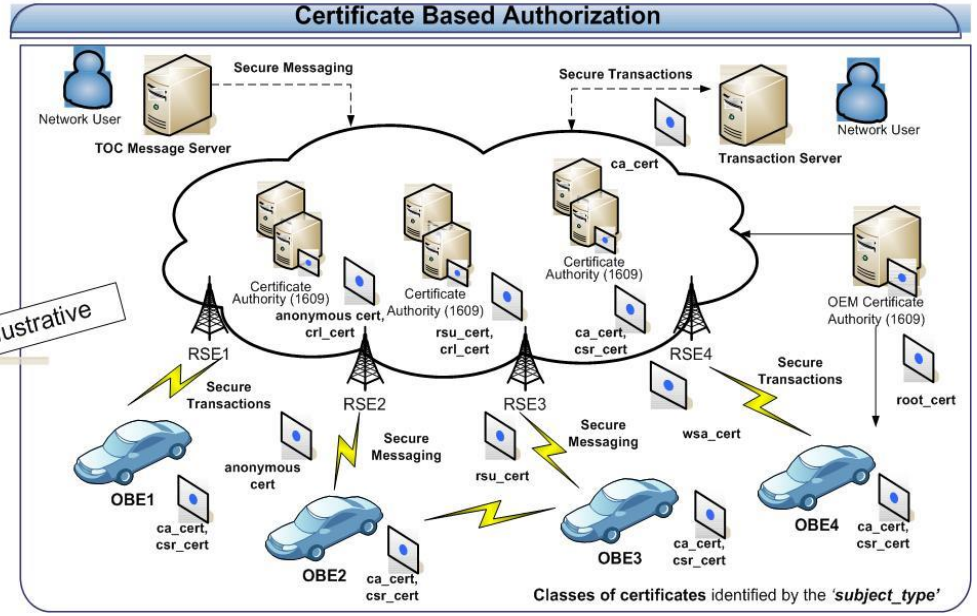


A quick look at VPKI for US DOT Pilots (10 year span)

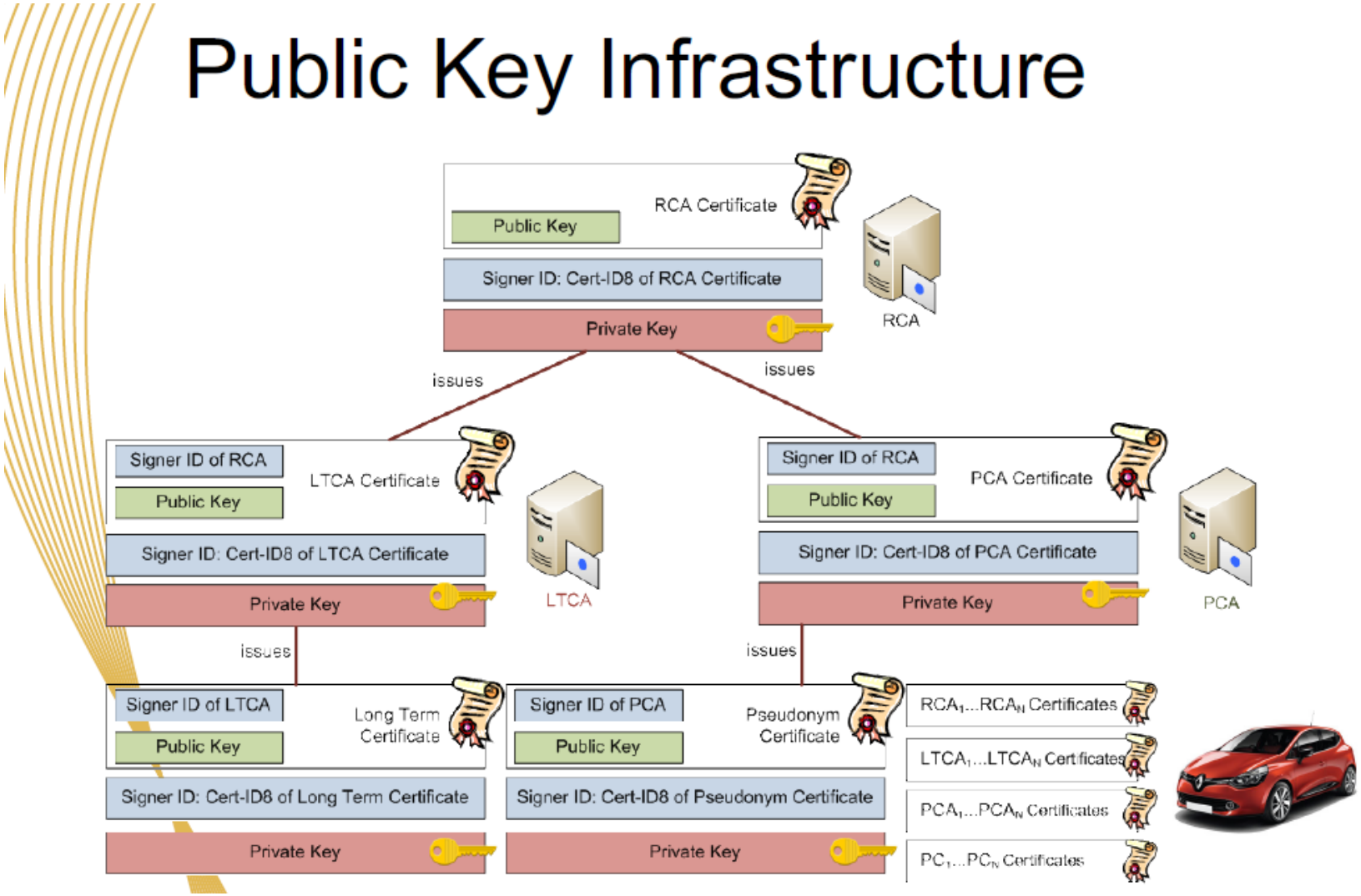






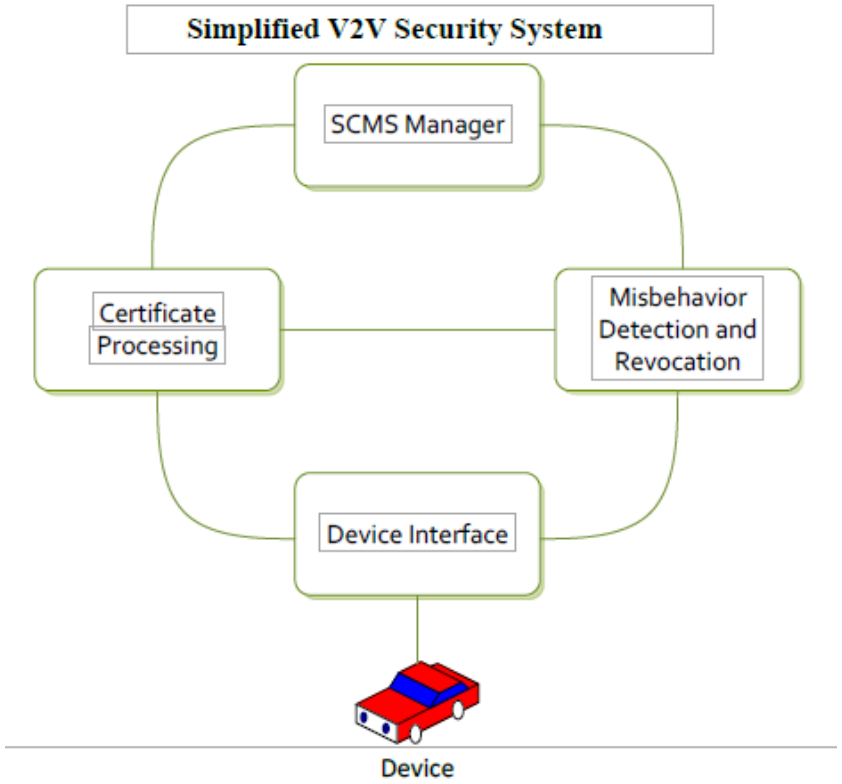


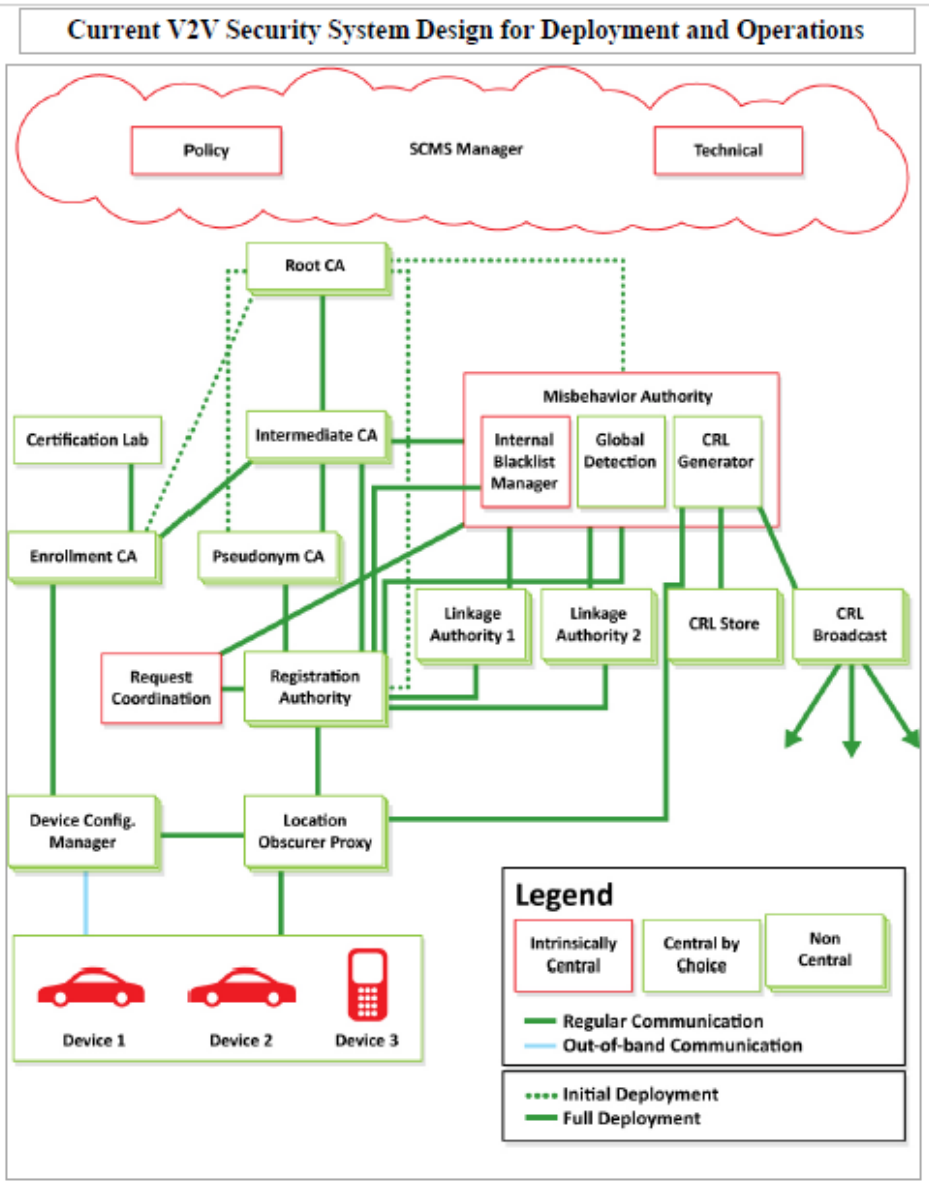
PRESERVE V-PKI Infrastructure (EU)



1) V-PKI Model PRESERVE Project - https://www.preserve-project.eu/sites/preserve-project.eu/files/preserve-ws-02-security-architecture.pdf

Introducing the Security Credential Management Systems (VPKI)





This image presents both an initial deployment model as well as a full deployment model. Note that this diagram shows the initial deployment model where there is no Intermediate CA and the Root CA talks to the MA, PCA, and ECA (dotted lines). In the full deployment model, these entities communicate with the Intermediate CA instead of the Root CA to protect the Root CA from unnecessary exposure (solid line)

[1] W. Whyte, A. Weimerskirch et al, Crash Avoidance Metrics Partnership, Technical Design of the Security Credential Management System (Final Report),

Adoption of V-PKI Models

A Security Credential Management System for V2V Communications

William Whyte*, André Weimerskirch†, Virendra Kumar*, Thorsten Hehn‡
*{wwhyte, vkumar}@securityinnovation.com
†andre.weimerskirch@escrypt.com
‡thorsten.hehn@vw.com

Conference Paper · December 2013
DOI: 10.1109/VNC.2013.6737583

Federal Register / Vol. 82, No. 8 / Thursday, January 12, 2017 / Proposed Rules

DOT HS 812 014 August 2014

Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application

VPKIs: State-of-the-Art, Challenges and Extensions

Hongyu Jin, Mohammad Khodaei and Panos Papadimitratos
Networked Systems Security Group
www.ee.kth.se/nss
Royal Institute of Technology (KTH)

June 24, 2015

DEPARTMENT OF TRANSPORTATION

National Highway Traffic Safety Administration

49 CFR Part 571

[Docket No. NHTSA–2016–0126]

RIN 2127–AL55

Federal Motor Vehicle Safety Standards; V2V Communications

AGENCY: National Highway Traffic Safety Administration (NHTSA), Department of Transportation (DOT).

ACTION: Notice of Proposed Rulemaking (NPRM).

SUMMARY: This document proposes to establish a new Federal Motor Vehicle Safety Standard (FMVSS), No. 150, to mandate vehicle-to-vehicle (V2V) communications for new light vehicles and to standardize the message and format of V2V transmissions. This will create an information environment in which vehicle and device manufacturers can create and implement applications to improve safety, mobility, and the

V2V Requirements from the NHTSA Notice of Proposed Rule Making

https://www.federalregister.gov/documents/2017/01/12/2016-31059/federal-motor-vehicle-safety-standards-v2v-communications

A. V2V Communications Proposal Overview
B. Proposed V2V Mandate for New Light Vehicles, and Performance Requirement for Aftermarket for Existing Vehicles
C. V2V Communication Devices That Would Be Subject to FMVSS No. 150
1. Original Equipment (OE) Devices on New Motor Vehicles
2. Aftermarket Devices
D. Potential Future Actions
1. Potential Future Safety Application Mandate
2. Continued Technology Monitoring
E. Performance Criteria for Wireless V2V Communication
1. Proposed Transmission Requirements
2. Proposed V2V Basic Safety Message (BSM) Content
3. Message Signing and Authentication
4. Misbehavior Reporting
5. Proposed Malfunction Indication Requirements
6. Software and Security Certificate Updates
7. Cybersecurity

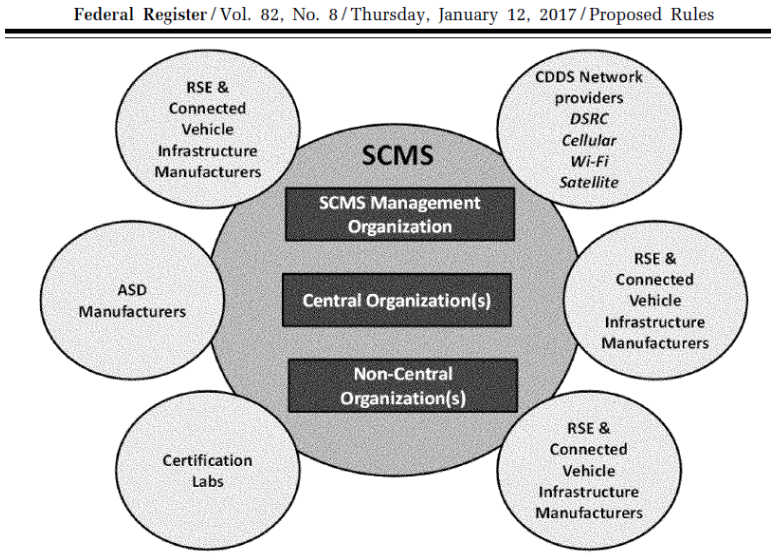
IV. Public Acceptance, Privacy and Security
A. Importance of Public Acceptance To Establishing the V2V System
B. Elements That Can Affect Public Acceptance in the V2V Context
1. False Positives
2. Privacy
3. Hacking (Cybersecurity)
4. Health
5. Research Conducted on Consumer Acceptance Issues
6. User Flexibilities for Participation in System
C. Consumer Privacy
1. NHTSA's PIA
2. Privacy by Design and Data Privacy Protections
3. Data Access, Data Use and Privacy
4. V2V Privacy Statement
5. Consumer Education
6. Congressional/Other Government Action
D. Summary of PIA
1. What is a PIA?
2. PIA Scope
3. Non-V2V Methods of Tracking
4. V2V Data Flows/Transactions With Privacy Relevance
5. Privacy-Mitigating Controls
6. Potential Privacy Issues by Transaction Type

V. Device Authorization
A. Approaches to Security Credentialing
B. Federated Security Credential Management (SCMS)
1. Overview
2. Technical Design
3. Independent Evaluation of SCMS Technical Design
4. SCMS RFI Comments and Agency Responses
5. SCMS ANPRM Comments and Agency Response
6. SCMS Industry Governance
C. Vehicle Based Security System (VBSS)
D. Multiple Root Authority Credential Management
VI. What is the agency's legal authority to regulate V2V devices, and how is this proposal consistent with that authority?
A. What can NHTSA regulate under the Vehicle Safety Act?
B. What does the Vehicle Safety Act allow and require of NHTSA in issuing a new FMVSS, and how is the proposal consistent with those requirements?
1. "Performance-Oriented"
2. Standards "Meeting the Need for Motor Vehicle Safety"
3. "Objective" Standards
4. "Practicable" Standards
C. How are the regulatory alternatives consistent with our Safety Act authority?
D. What else needs to happen in order for a V2V system to be successful?
1. SCMS
2. Liability

What If – Models for Industry Self Regulation (Risk Models)?

In analyzing SCMS governance options, NHTSA and its research partners have investigated a variety of industries with characteristics similar to those seen as critical for a V2V SCMS governance model, including security, privacy protection, stability, sustainability, multi-stakeholder representation and technical complexity. How risk was managed in the context these models. Some of the industries researched included:

- Internet Corporation for Assigned Names and Numbers (ICANN)
- DTE Energy Company
- Aeronautical Radio Incorporated (ARINC)
- End of Life Vehicle Solutions Corporation (ELVS)
- The FAA's Next Gen Air Transportation System
- The FRA's Positive Train Control
- Smart Grid
- The Rail/Transit Train Control Systems (ATC and CBTC)
- Medical Devices failure and liability
- Security in nuclear industry and liability
- Warning/Signal Failures
- UAVs
- HIPAA/Health Care industry/
- Electronic Health Records (EHRs)
- CONNECT system



** National Highway Traffic Safety Administration (NHTSA), Department of Transportation (DOT) Notice of Proposed Rulemaking, '*Federal Motor Vehicle Safety Standard (FMVSS), No. 150, to mandate vehicle-to-vehicle (V2V) communications for new light vehicles and to standardize the message and format of V2V transmissions*', Federal Register Vol 82, No 87, Jan 12, 2017,

Secure Communication for Connected Vehicles and C-ITS

https://dev.securityfeeds.us/secure-communication-connected-vehicles-and-c-its

Secure Communication For Connected Vehicles And C-ITS

ITS (Vehicular Networks) Industry Around The World

SecurityFeeds LLC IVC-ITS Vehicular Network Security Portals

- ITS Vehicular Networking Landscape and Security-Privacy Frameworks(Weil)
- Connected Vehicle and C-ITS Pilot Programs (Weil)
- VPKI Hits the Highway (Weil)
- Securing Vehicular Networks (Weil)

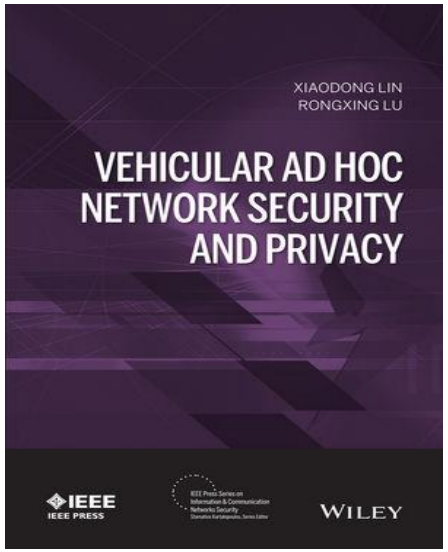
TAGS

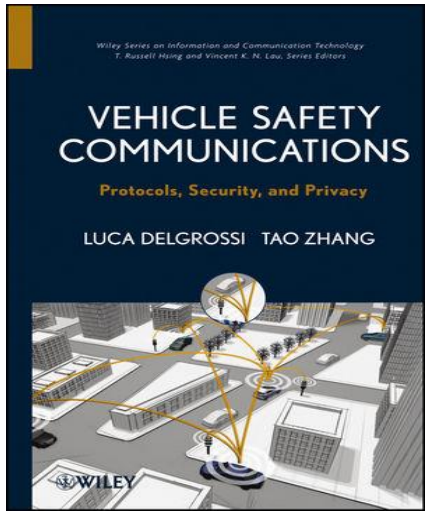
ComSoc | Greentech | Secure Automotive Networking | Press Release | Program Management

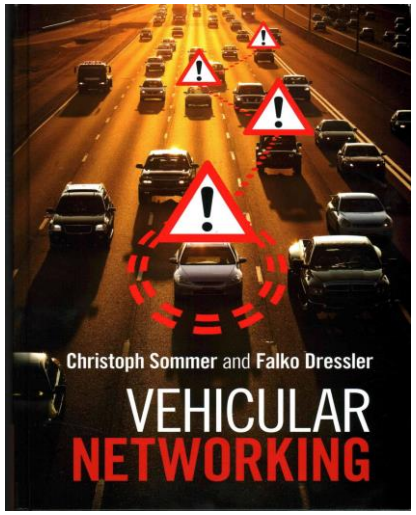
Table of Contents

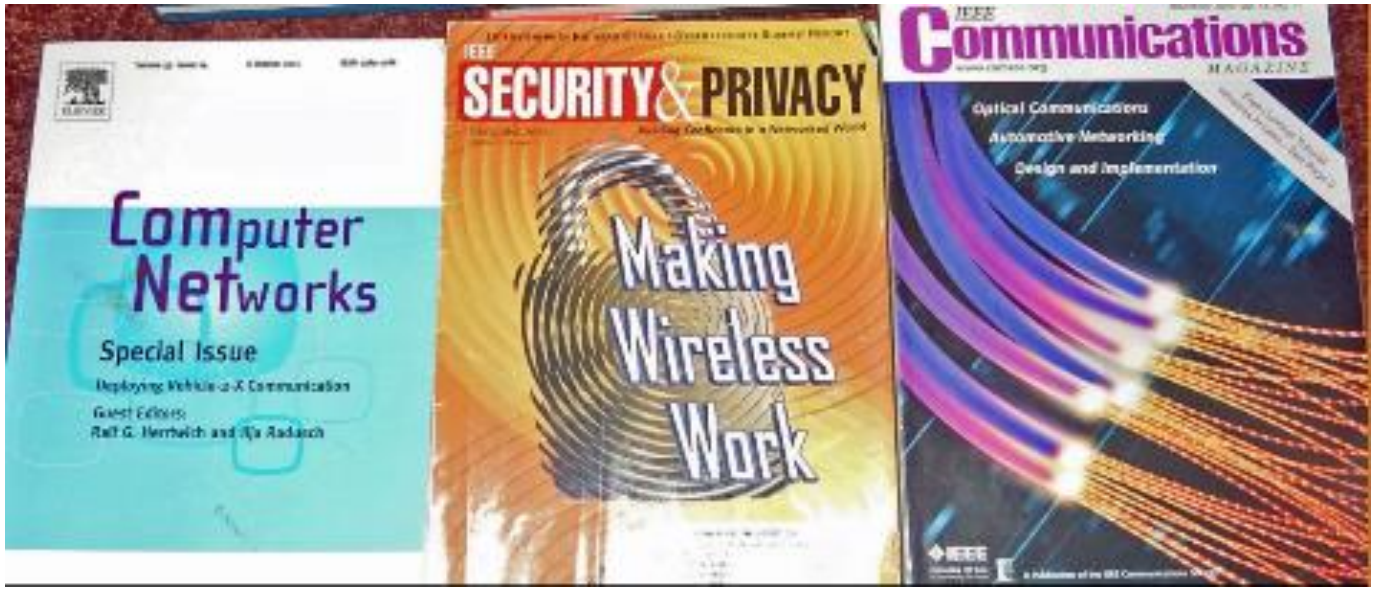
- Introduction – IT Pro SI on Cyberthreats and Security
- Grid Cybersecurity (Ukraine)
- CSA IoT Security (Controls and Mitigations)
- SamSam Ransomware Attack - US DOT
- VPKI Hits the Highway
- References + Q-A

Privacy-Preserving Vehicular PKI (a very broad subject)



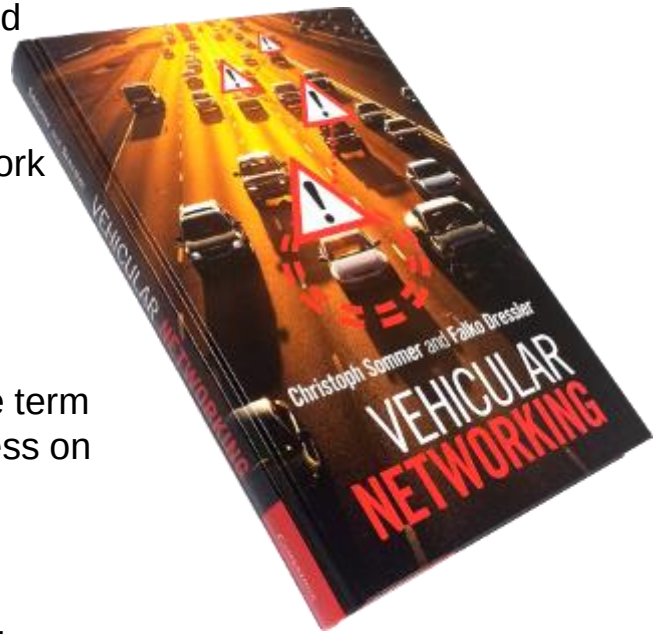






Car-to-X (C2X) communication patterns

Vehicular networking is what we adopted as the most general classifier, referring to the field of computer communications and networking as applied to vehicles. Vehicular networking thus encompasses both in-car and inter-vehicle communication aspects as well as their fusion.



Inter-vehicle communication (IVC) restricts this to exclude wired communication as well as any network (wired or wireless) within vehicles. It thus refers to a system where vehicles are participants in a wireless network. Other participants such as roadside units (RSUs) can explicitly be part of this network.

Vehicular ad-hoc network (VANET) has its origins in the discipline of mobile ad-hoc networks (MANETs), casting VANETs as a novel application domain. Being the basis for what we call IVC today, the term is still somewhat synonymous with IVC, but focuses on spontaneously created ad-hoc networks, much less on pre-deployed infrastructure like using RSUs or cellular networks.

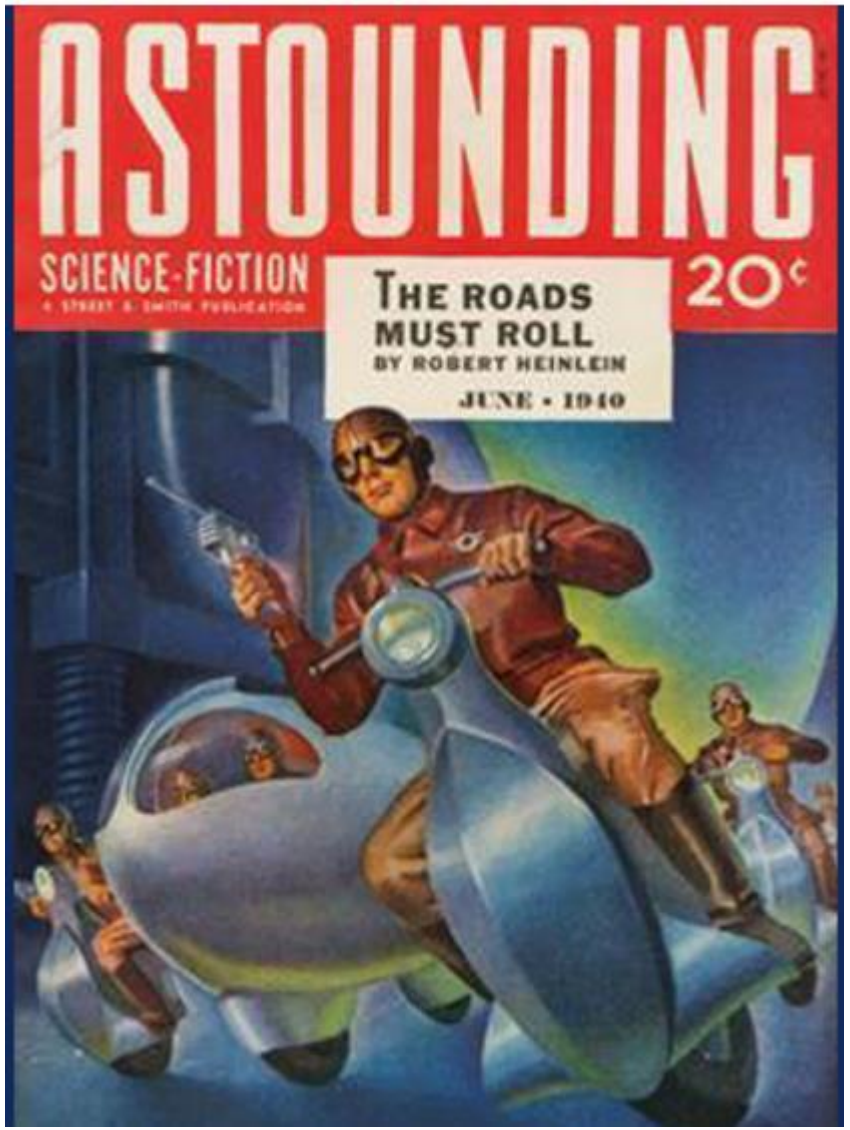
Intelligent transportation system (ITS) describes the overall goal of being able make better use of transportation networks, for which road networks are one of many such networks and IVC is one means among many. Lately, other modes of transportation have faded into the background and ITS has become synonymous with intelligent road networks.

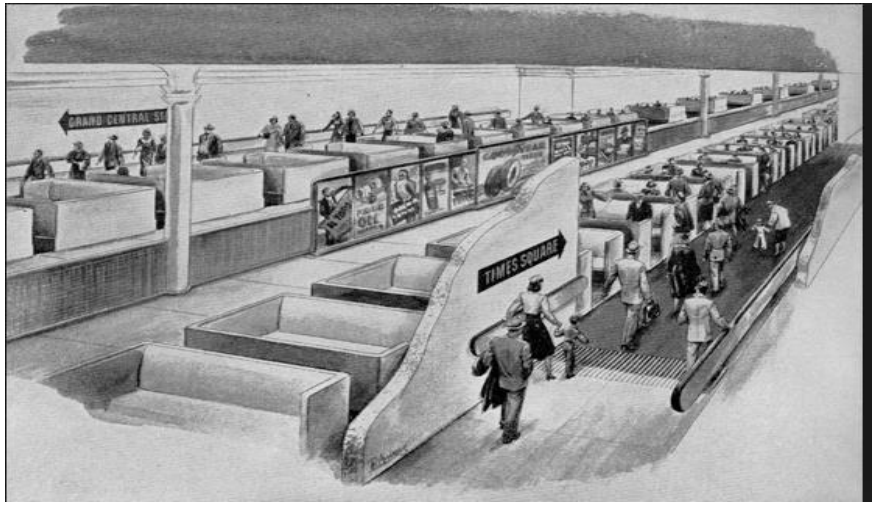
Vehicle to vehicle (V2V) as well as vehicle to infrastructure (V2I) andvehicle to X (V2X) all refer to the end points of communication, indicating whether information is being exchanged with other vehicles, with infrastructure (also called vehicle-to-roadside), or with arbitrary nodes – independently of the technology being used. car for vehicle (forming C2C, C2I, and C2X) to refer to the same concepts.

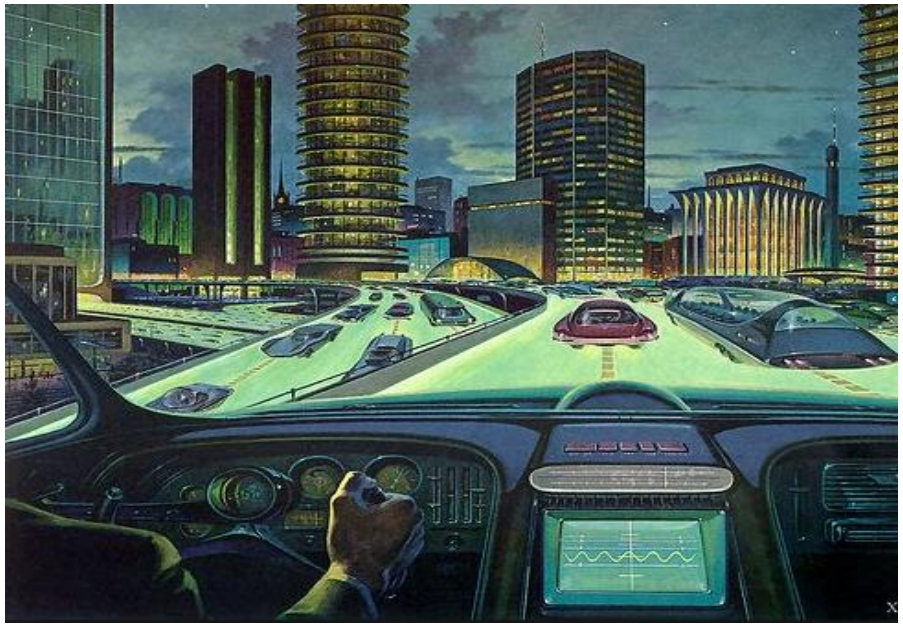
The real challenges of VC data sharing are policy and cultural issues

The Roads Must Roll – Robert Heinlein

GM Futurama – Connected Car (1956)



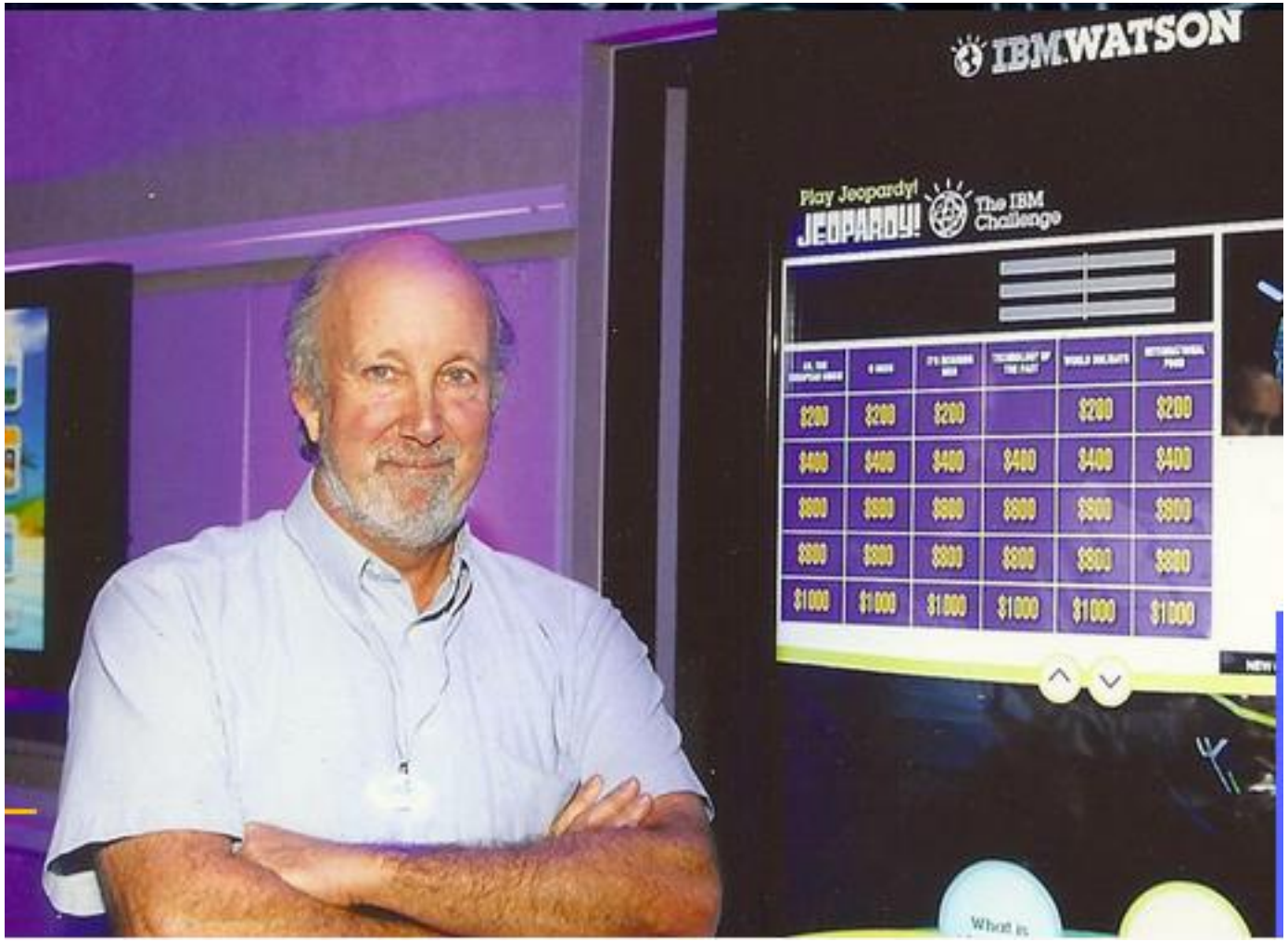




References Used in This Presentation

- Scoping the Cyber Security Body of Knowledge" Awais Rashid et al, IEEE Security and PrivacyMagazine, Volume 16, Issue 3, May, June 2018
- E-ISAC, SANS ICS. "Analysis of the Cyber Attack on the Ukrainian Power Grid" March 18 2016. p4. http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf
- Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks- https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/
- THREAT INTELLIGENCE REPORT CYBERATTACKS AGAINST UKRAINIAN ICS https://www.sentryo.net/wp-content/uploads/2017/09/EBOOK_CYBERATTACKS-AGAINST-UKRAINIAN-ICS.pdf
- Colorado DOT Ransomware Attack https://www.govtech.com/security/Colorado-Hack-Offers-Larger-Lessons-for-Cybersafety.html
- T.Weil, VPKI Hits the Highway: Security Communication for the Connected Vehicle Program, IT Professional Magazine, Volume 19, Issue 1, January 2017
- National Highway Traffic Safety Administration (NHTSA), Department of Transportation (DOT) Notice of Proposed Rulemaking, '*Federal Motor Vehicle Safety Standard (FMVSS), No. 150, to mandate vehicle-to-vehicle (V2V) communications for new light vehicles and to standardize the message and format of V2V transmissions*', Federal Register Vol 82, No 87, Jan 12, 2017, online available at - https://www.federalregister.gov/documents/2017/01/12/2016-31059/federal-motor-vehicle-safety-standards-v2v-communications

Thank you for joining us!



SecurityFeeds LLC
Information Assurance for the Enterprise Network

Tim Weil - CISSP/CCSP, CISA, PMP
Principal

PO Box 18385
Denver, CO. 80218

Phone: 301.452.3641 (m)
Fax: 240.337.1305
Email: tweil@securityfeeds.com
Website: http://securityfeeds.com

SecurityFeeds LLC provides IT Management Consulting services

- Communications and Security Engineering
- Data Processing (Systems Engineering)
- Project and Program Management
- Risk Management (ISO 27001)

Our expertise includes Enterprise Security Architecture, Cloud Security, Program Management, and Network Engineering.

"RISK is a four-letter word"

http://www.securityfeeds.com
trweil@ieee.org

SecurityFeeds
Your source for enterprise security management

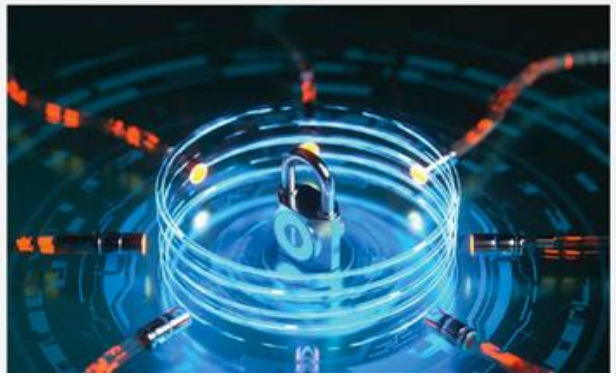
INTRODUCTION ABOUT SERVICES RESOURCES SECURITY INDUSTRY NEWS BLOG TOOLS CONTACT

Your Source For Enterprise Security Management

Security Architecture | Cloud Security | Program Management | Systems Engineering | ISO 27001 | Risk Management and Compliance | Secure Automotive Network (V-PKI Hits the Highway) | Secure Automotive Networking for ITS

IT Professional
Technology Solutions for the Enterprise

VOLUME 20, NUMBER 3 MAY/JUNE 2018



Welcome To SecurityFeeds

Tim Weil is an IT Security Program Manager with over twenty five years' experience in data processing, communications engineering, and information assurance (IA).

His areas of expertise include FedRAMP/FISMA compliance for federal agencies and cloud service providers, IT Service Management, cloud security (FedRAMP), enterprise risk management (NIST) for federal agencies and ISO 27001 compliance for commercial clients.