

A Special Issue of IEEE IT Professional Magazine

## Risky Business - Cyberthreats and Security



Cyberthreats and Security



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

CU-Denver  
Denver, CO  
Dec 4, 2018

# Objectives of this Presentation

## **Cyberthreats and Security**

- A Writer's Life
- The Changing Landscape (2015 v 2018)
- Information Security – A body of knowledge

## **Information Security Management Models for Risk Management**

- Risk Management Framework (NIST SP 800-37)
- Deming Cycle - Plan-Do-Check-Act
- OODA Loop (Joe Boyd, USAF Fighter Pilot)
- NIST Cybersecurity Frameworks

## **Featured Articles**

- Cyber-Resiliency Workforce
- Ocular Biometric Datasets
- Evolving Cyberthreats to Privacy

## **VPKI Hits the Highway (use case)**

- Connected Car and Cooperative ITS
- Security Communication for Intelligent Transportation Systems
- Security Credential Management System (SCMS)

## **AI and Machine Learning–Risk Management for Finance Industry**

- AI-ML are a Hot Topic
- Under Construction

# Table of Contents

- ▶ Introduction – IT Pro SI on Cyberthreats and Security
- ▶ Information Security Management Models for Risk Management
- ▶ Featured Articles
- ▶ VPKI Hits the Highway
- ▶ AI and Machine Learning – Risk Management for Finance Industry
- ▶ References + Q&A

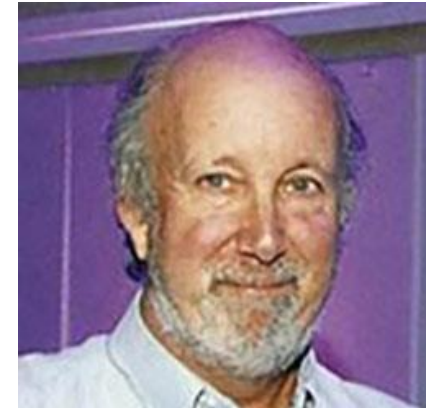
## Tim Weil – Network Program Manager

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://dev.securityfeeds.us>



# A Writer's Life –



**Timothy Weil**  
 Editor - IEEE IT Professional magazine  
 Cloud Security, RBAC, Identity Management,  
 Vehicular Networks  
[Verified email at securityfeeds.com - Homepage](mailto:tim@securityfeeds.com)

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



## 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(InterSat), 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 - DCCAS Recognizes Jerry Gibbon as Engineer of the Year](#)



EDITORS: Rick Kuhn, US National Institute of Standards and Technology, [kuhn@nist.gov](mailto:kuhn@nist.gov)  
 Tim Weil, SCRAM Systems, [tim@scram.com](mailto:tim@scram.com)



## 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*

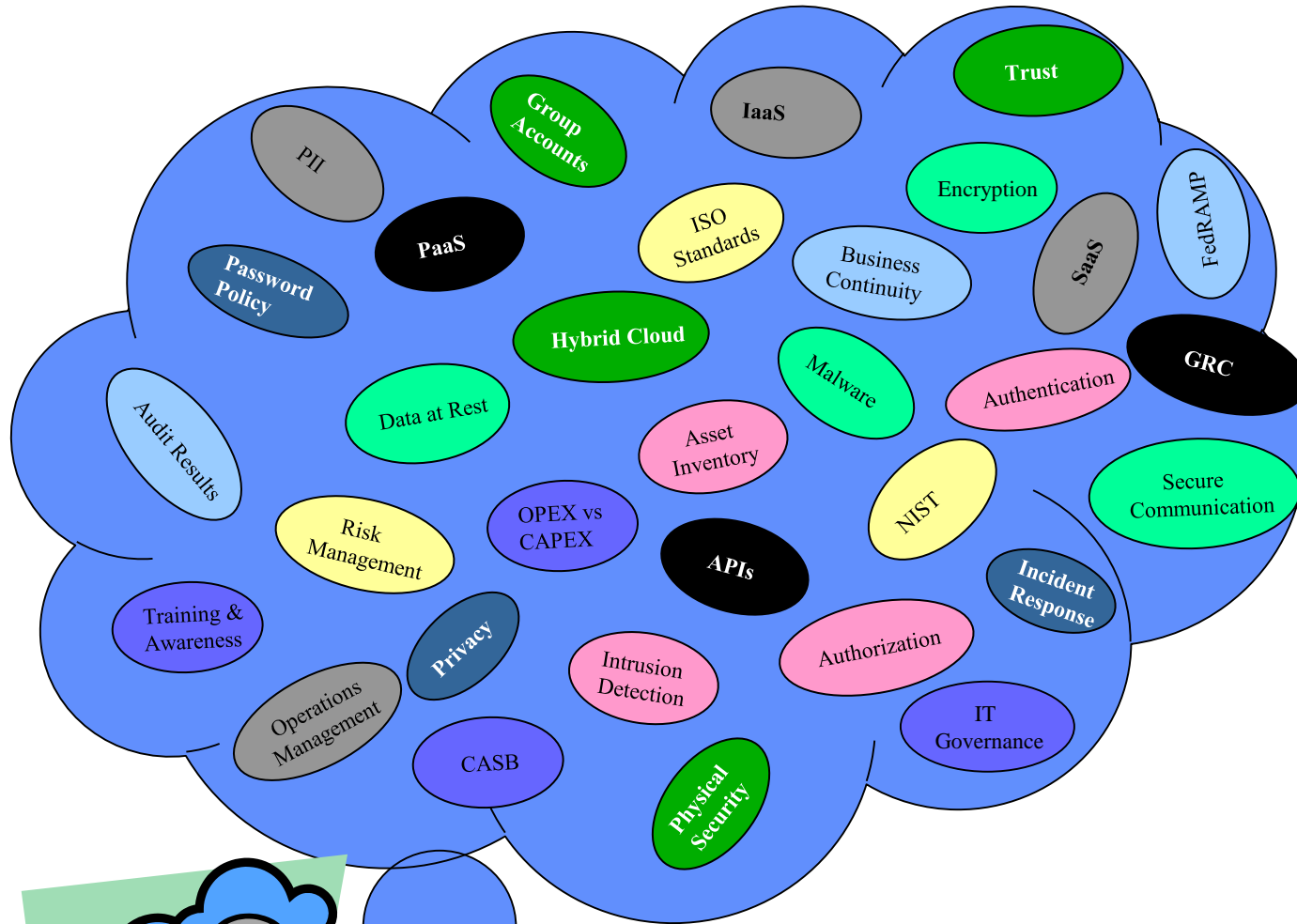
### Feature Articles

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

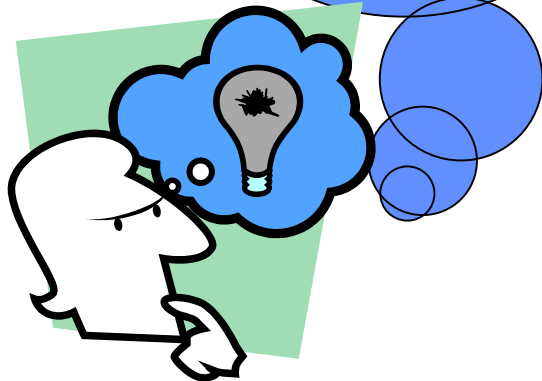
### Columns and Departments

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

# Managing Information Security Risk



IT 101 – What Problems Are We Trying to Solve?  
 Identify ‘Fix-It’ areas in the program  
 Understand Current State (Remediation)  
 Improve ‘ad hoc’, ‘not my problem’ state  
**Reduce Program Risk**  
 Improve Continuous Monitoring Process



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

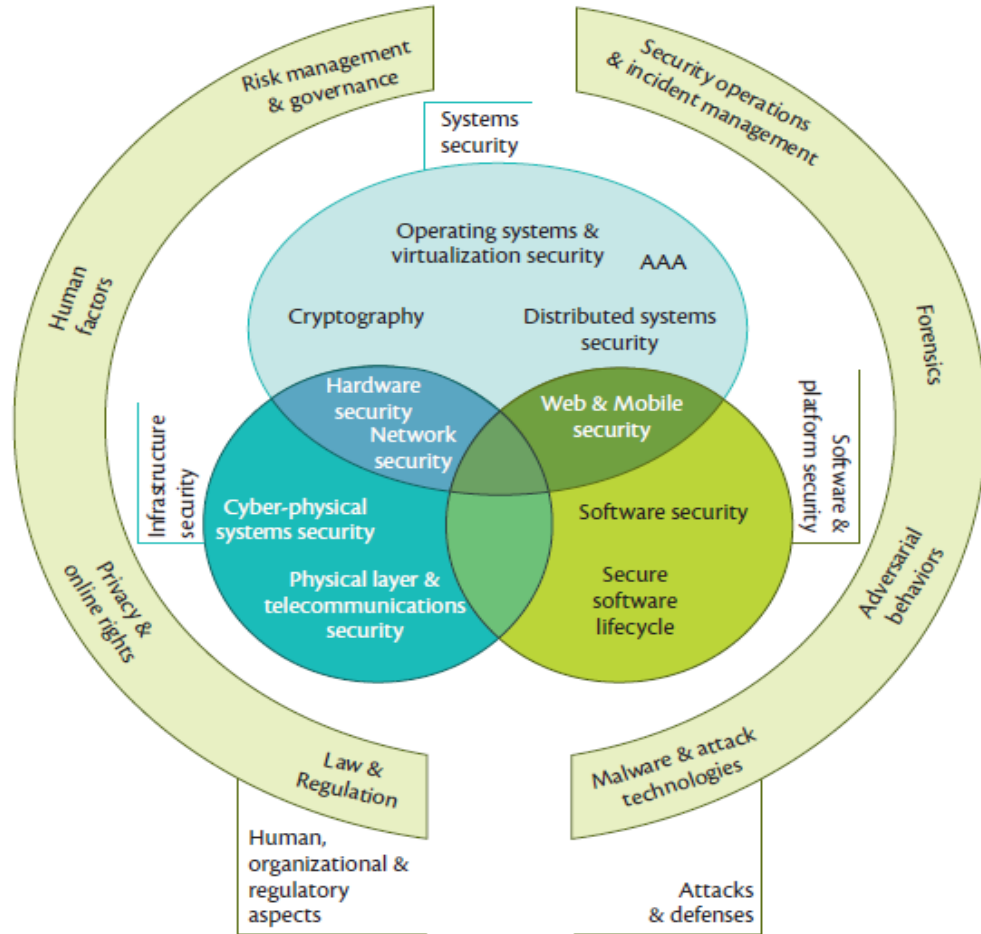


Figure 3. The 19 knowledge areas and their categorization within CyBOK.

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

12/4/2018



# Table of Contents

- ▶ Introduction – IT Pro SI on Cyberthreats and Security
- ▶ Information Security Management Models for Risk Management
- ▶ Featured Articles
- ▶ VPKI Hits the Highway
- ▶ AI and Machine Learning – Risk Management for Finance Industry
- ▶ References + Q&A

# Editor's Introduction

<https://www.computer.org/csdl/mags/it/2018/03/mit2018030020.html>

Cyberthreats should not be thought of just in the context of IT security and privacy design. Adequate cybersecurity must involve the active participation of everyone in an organization, as well as users. Approaches generally reflect some variation on the common-sense method of evaluating the problem, preparing, acting, and assessing the results.

Federal agencies use the **Risk Management Framework (RMF)** to Assess and Authorize enterprise systems

Managers learn a **Plan-Do-Check-Act (PDCA)** cycle.

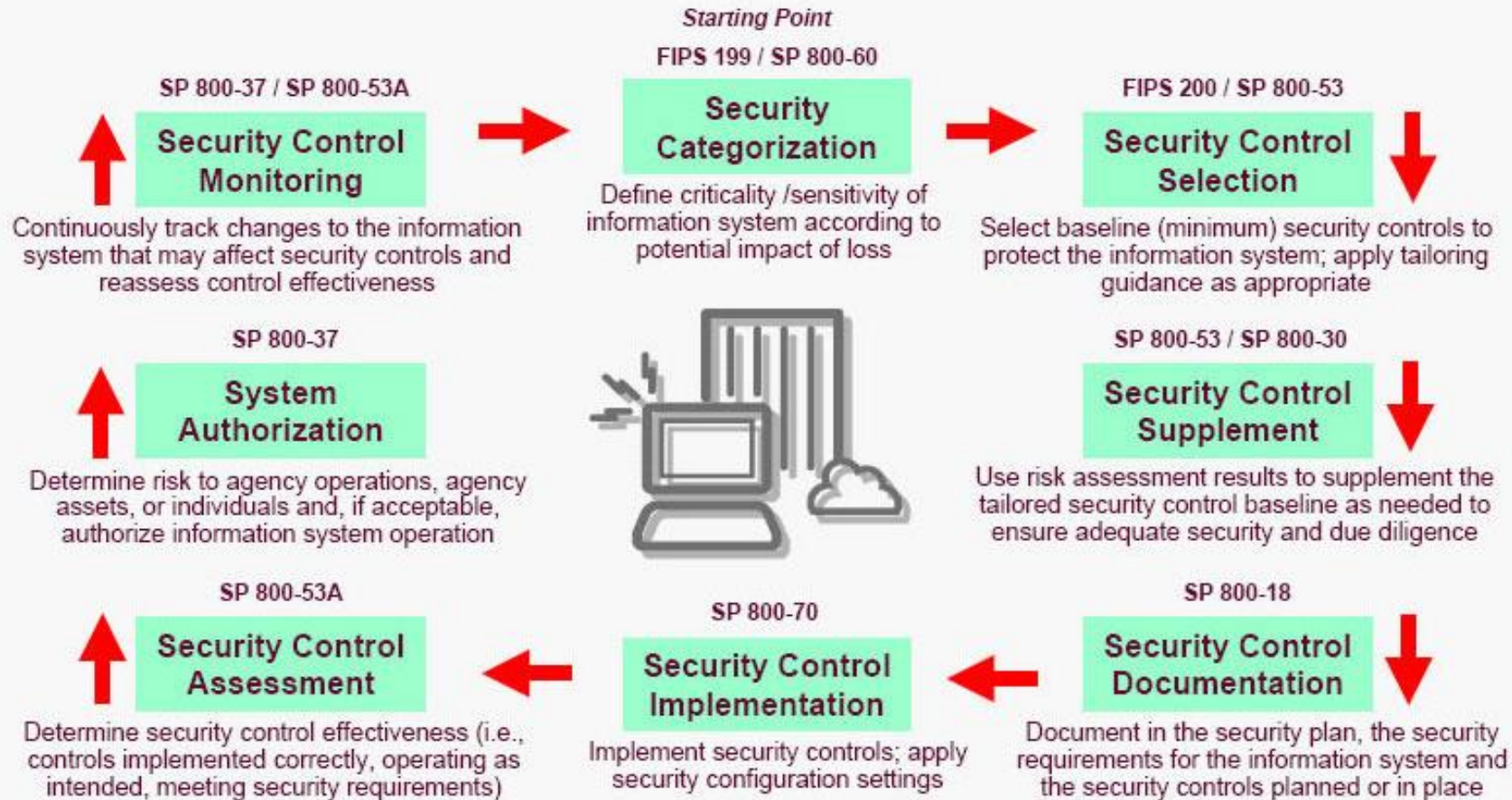
Fighter pilots are taught to **Observe-Orient-Decide-Act (OODA)**.

In cybersecurity the latest incarnation of this common-sense approach is the popular **NIST Cybersecurity Framework (CSF)**, which teaches **Identify-Protect-Detect-Respond-Recover**.

As in other fields, these activities are intended to be performed in a continuous cycle, modifying plans and actions as the organization learns from successes and failures.

# The FISMA Risk Management Framework.

**Information Risk Management (IRM)** is the practice of determining which Information Assets need protection and what level of protection is required, then determining appropriate methods of achieving that level of protection by understanding the applicable vulnerabilities, threats and countermeasures.



# The FISMA Risk Management Framework.

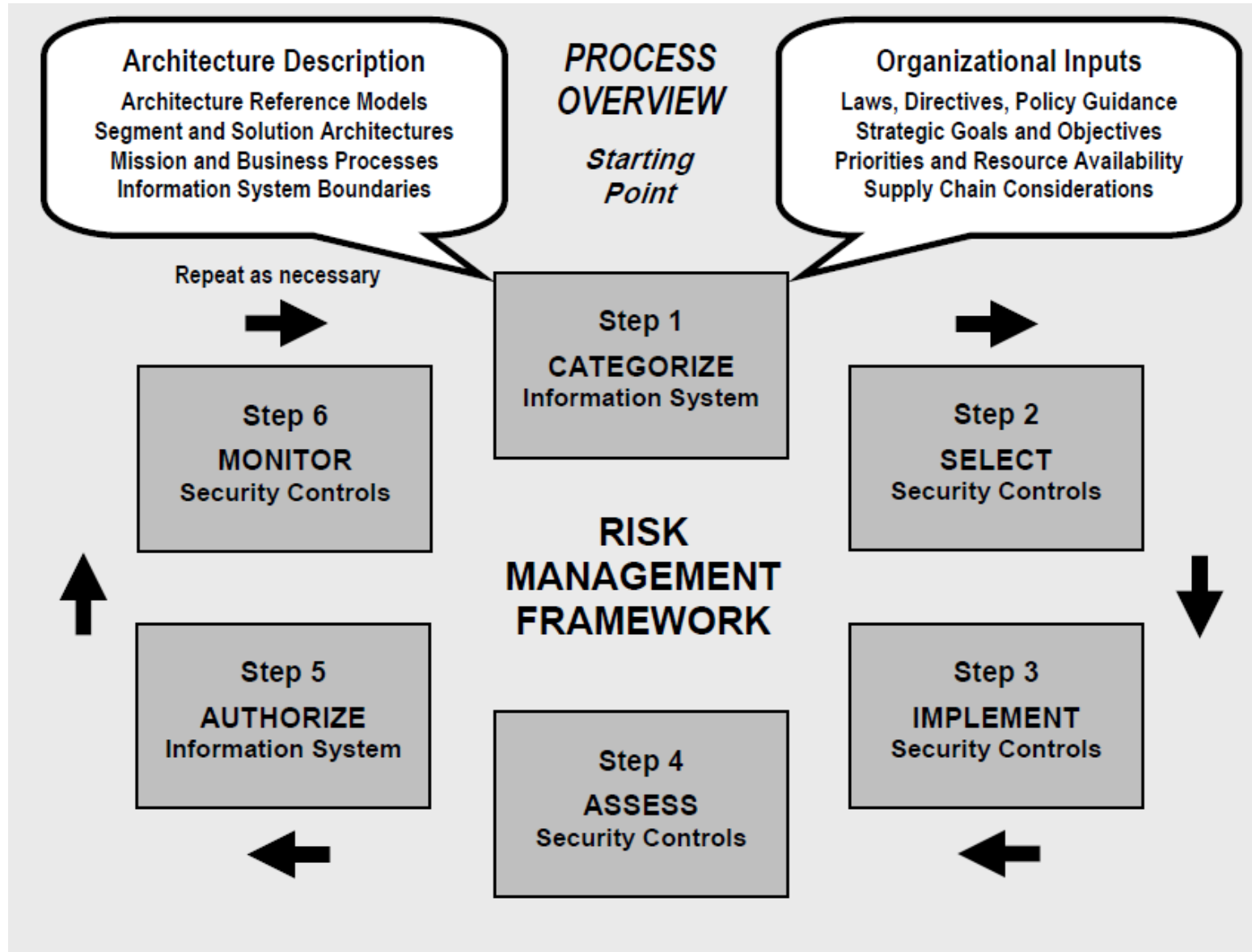
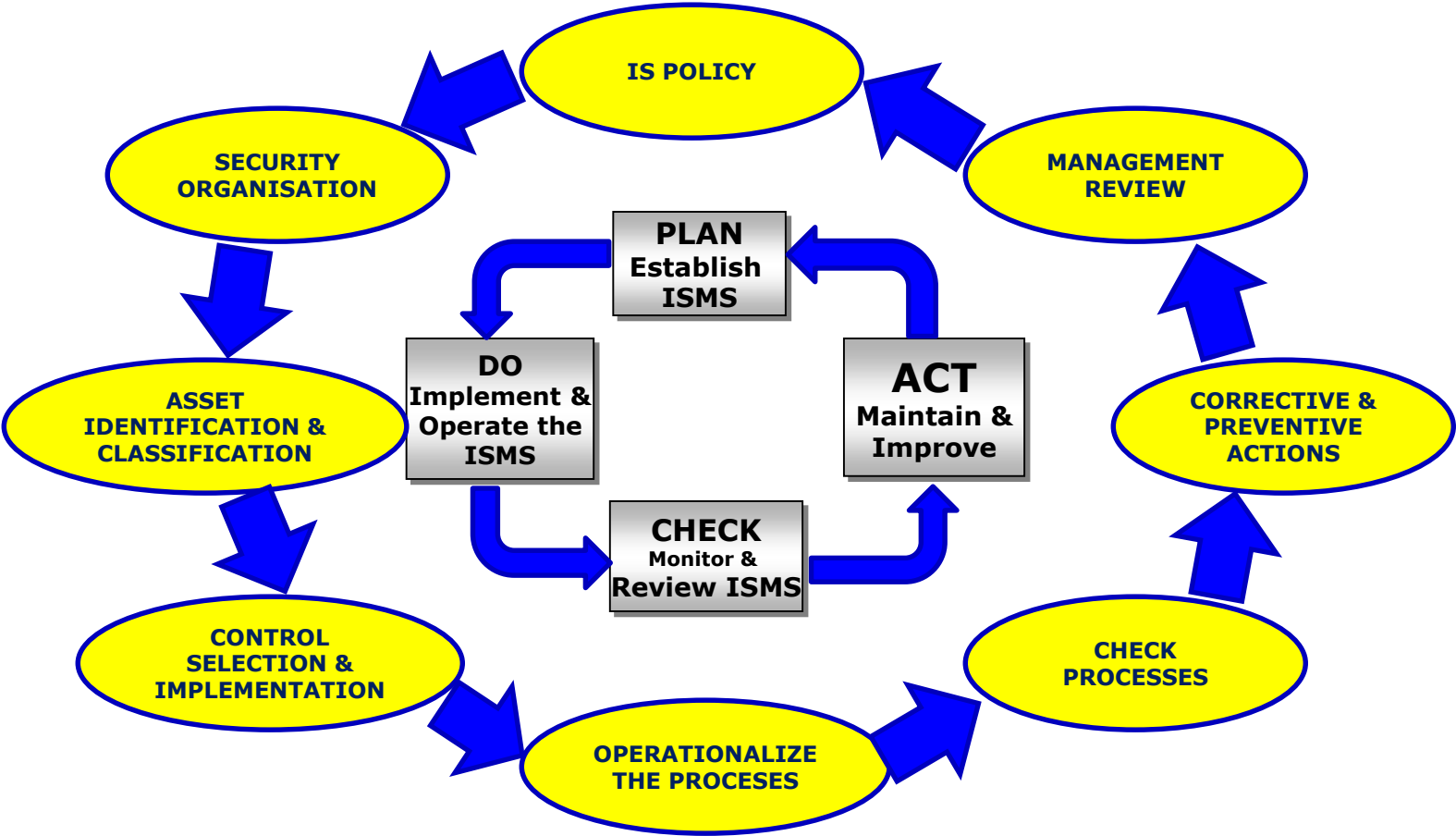
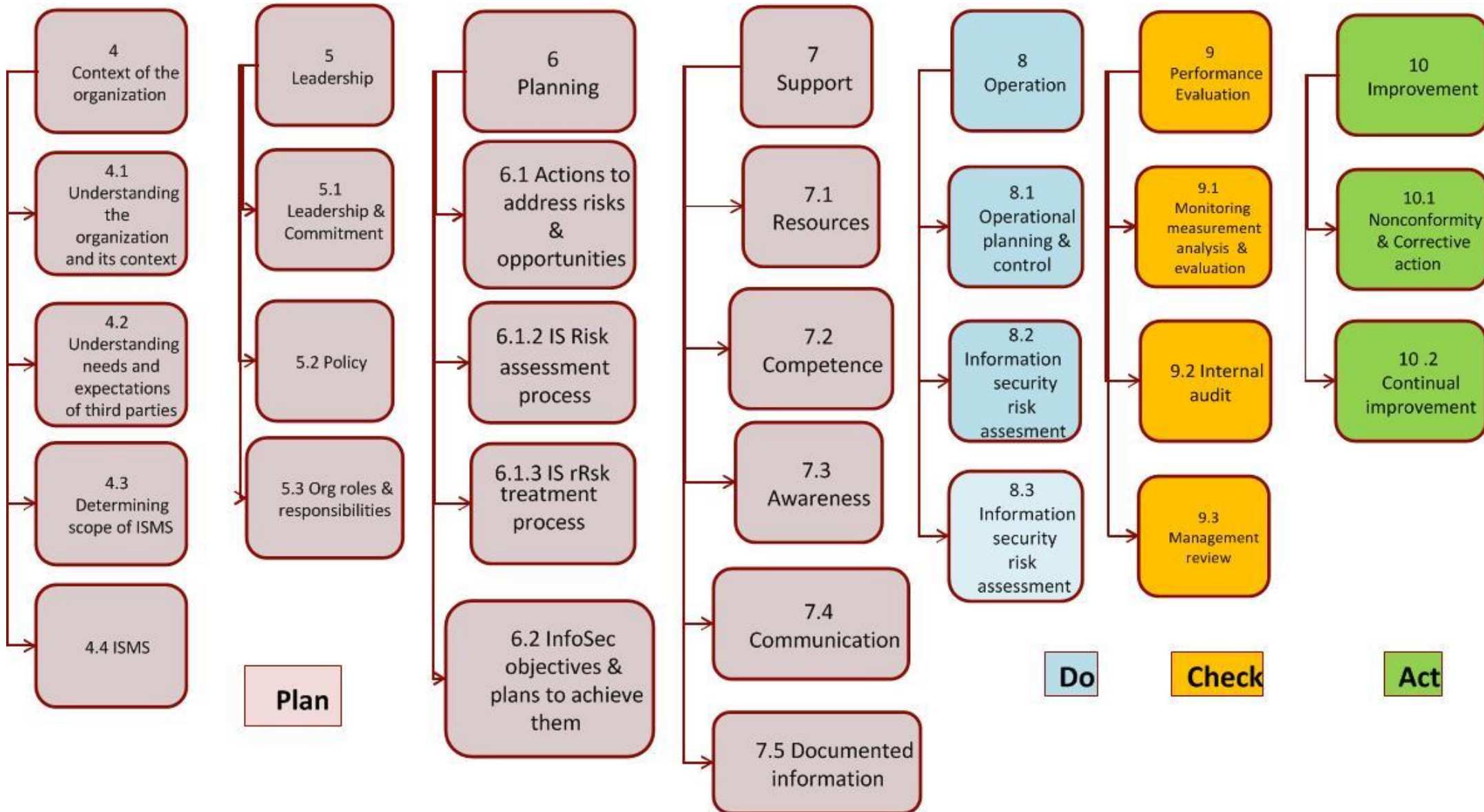


FIGURE 2-2: RISK MANAGEMENT FRAMEWORK

# ISMS PROCESS CYCLE

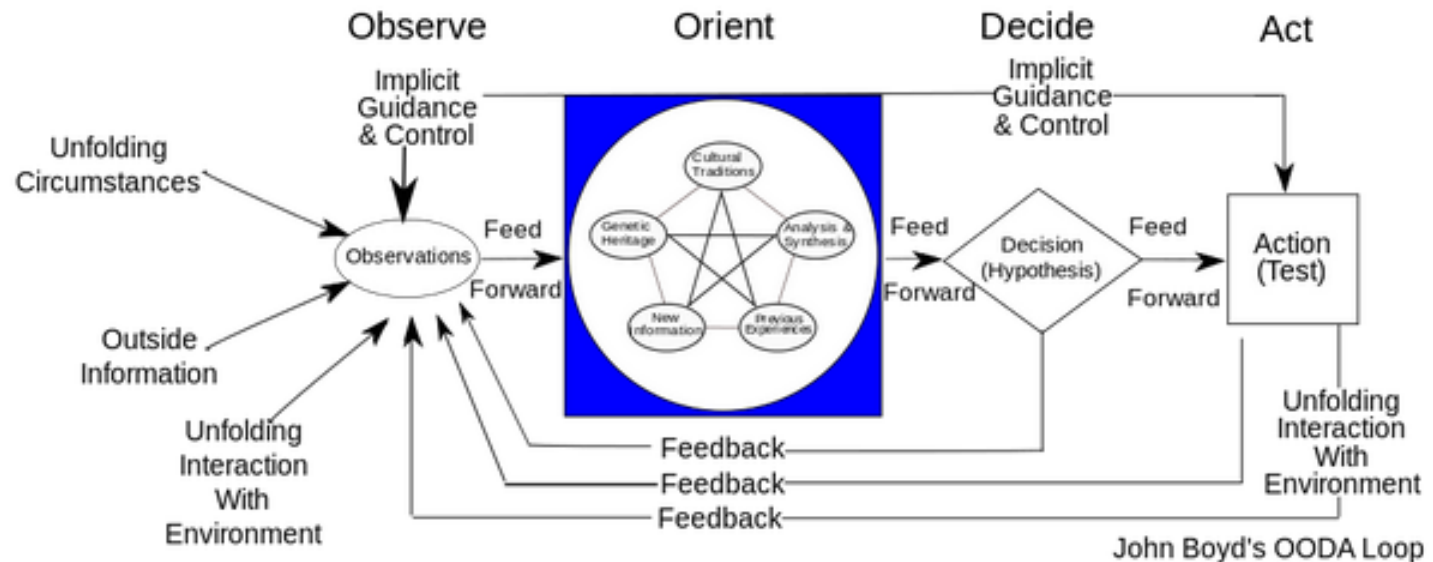
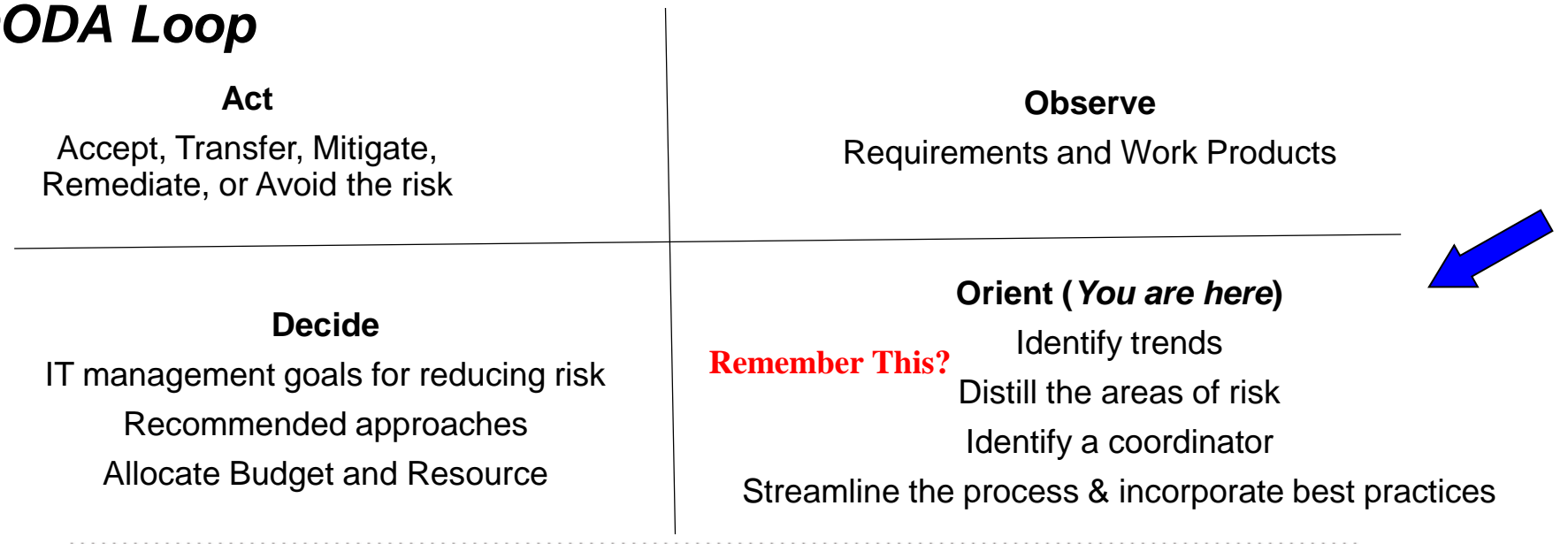


# Plan Do Check Act

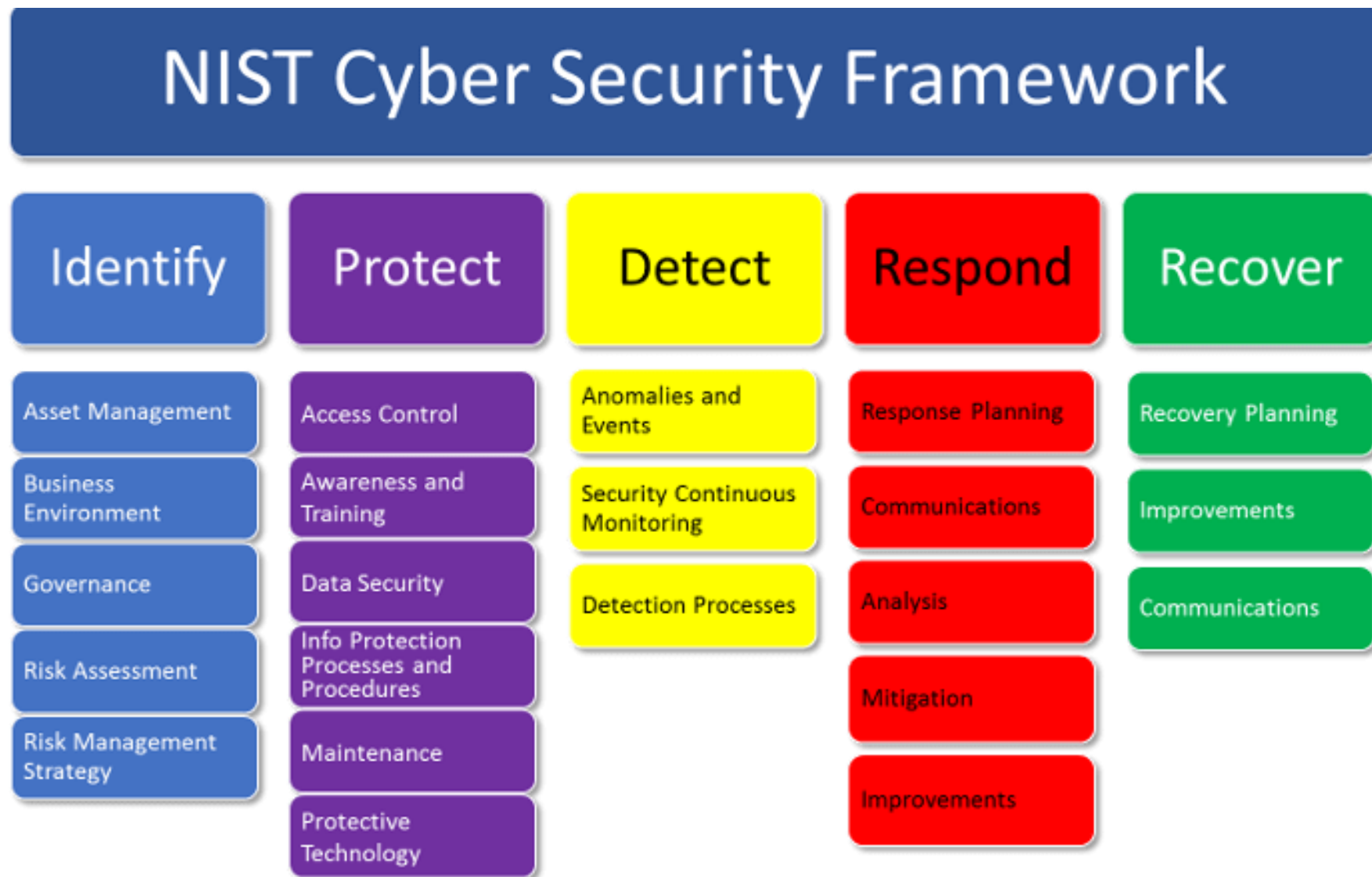


# Risk Management - OODA Loop

On the surface – and how many people still interpret the OODA model – it seems to be a simple step-by-step loop. For our purposes here, in this series, we could reframe ‘**Observe**’ as ‘**sense**’ – the process of sensing out what seems to be happening in our world – and ‘**Orient**’ as ‘**make-sense**’ – literally ‘sensemaking’ from what we’ve observed – which leads us onward to **decide and act**, at which point we loop back to sense and make-sense again.



# NIST Cybersecurity Framework (CSF)

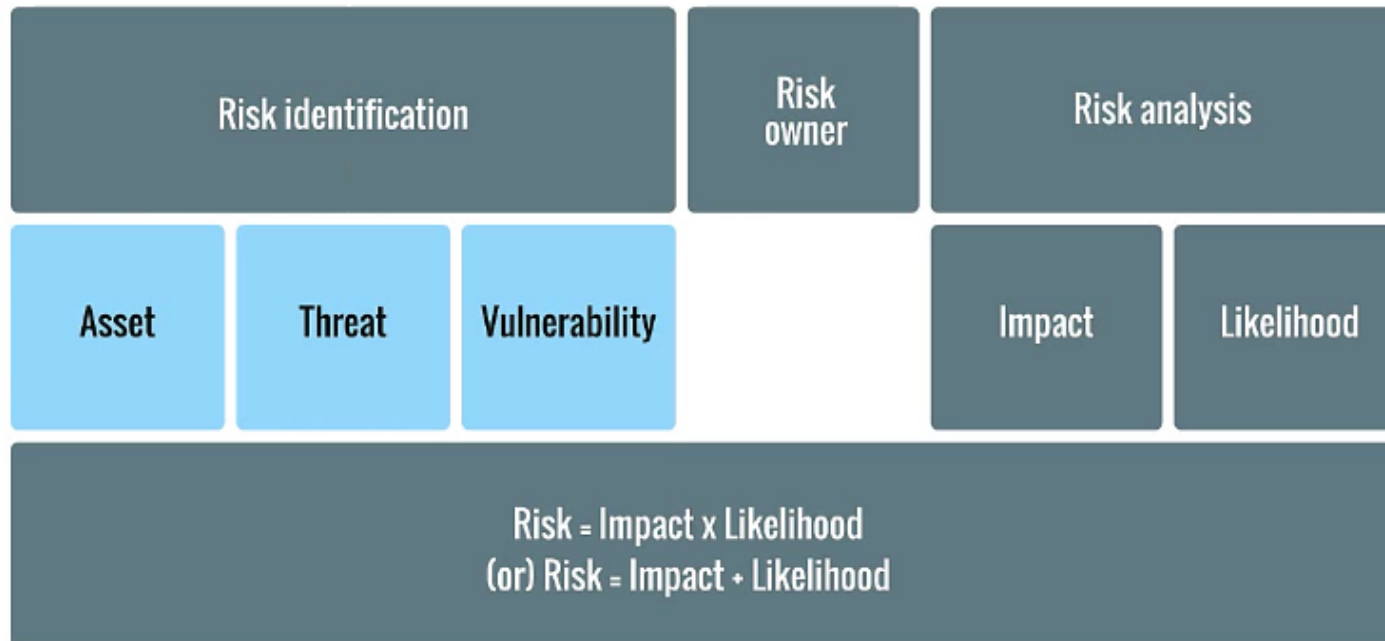




# Risk Management Principles (IT Risk Foundation)



## Elements of risk assessment



# Risk Assessments for Cloud Applications – where to get started?

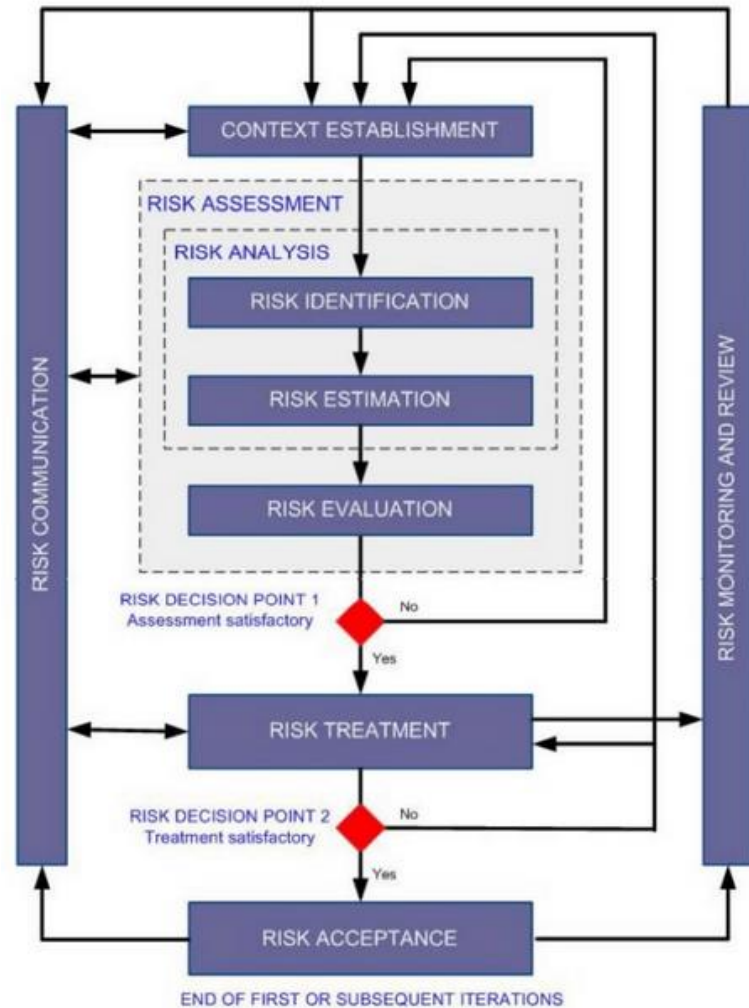
ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)

IJCST VOL. 4, ISSUE 1, JAN - MARCH 2013

## Cloud Security Risk Assessment using FAIR

<sup>1</sup>Ishan Rastogi, <sup>2</sup>Adesh Chandra, <sup>3</sup>Anurag Singh

<sup>1,2,3</sup>Dept. of Cyber Law and Information Security, IIT Allahabad, India



### Abstract

Cloud computing is a very powerful concept but with it comes various security scares which are enough to keep most of the perspective users at bay. This paper tries to calculate the additional risk which an organization might have to face when shifting to cloud computing, by performing cloud security risk assessment using the FAIR model.

### Keywords

Cloud Computing, Security, FAIR, Risk Assessment, Risk, Impact

### I. Introduction

Cloud computing is the next step in the evolution of computing. It aims at delivering computing resources as a service over a network by using virtualization and distributed computing techniques, thus providing computation power to the users at low costs by employing a pay as you go model for bill payment, i.e., a user pays only for the resources she has used.

**FAIR – Factor Analysis of Information Risk.** The **Open FAIR Cookbook** uses ISO/IEC 27005 as the example risk assessment framework. FAIR is complementary to all other risk assessment models/frameworks, including COSO, ITIL, ISO/IEC 27002, COBIT, OCTAVE, etc. It provides an engine that can be used in other risk models to improve the quality of the risk assessment results.

Online available - <https://publications.opengroup.org/c103>

### A. Loss of Governance

since all the data is with the cloud provider and SLAs may not cover all the points, a client may feel lack of control over her data.

### B. Lock-in

The lack of current availability of portability may cause difficulties to users who wish to migrate to different cloud provider, or bring the entire data back to in-house environment, or outsource the services to a third-party.

### C. Isolation Failure

Multi-tenancy and resource sharing may cause security concerns to the user if the isolation mechanisms are not appropriate.

### D. Compliance Risks

An organization may lose some of its security certifications if it decides to migrate to cloud.

ISO 27005 Information Security Risk Management Process

# Table of Contents

- ▶ Introduction – IT Pro SI on Cyberthreats and Security
- ▶ Information Security Management Models for Risk Management
- ▶ Featured Articles
- ▶ VPKI Hits the Highway
- ▶ AI and Machine Learning – Risk Management for Finance Industry
- ▶ References + Q&A

## Article Summaries

- ▶ **“Advancing Cybersecurity: The Growing Need for a Cyber-Resiliency Workforce,”** authors **Logan O. Mailloux and Michael R. Grimaila** address the topic of preparing the next generation of cybersecurity professionals who must focus on cyber resiliency—bouncing back from computing faults, networking failures, cyberattacks, and unpredictable events—especially as the world becomes more connected via cyber-physical systems. They uniquely detail several key responsibilities, work roles, and expertise areas for the future cyber-resiliency workforce.
- ▶ **“Experiments with Ocular Biometric Datasets: A Practitioner’s Guideline”** by **Zahid Akhtar, Gautam Kumar, Sambit Bakshi, and Hugo Proenca** deals with ocular biometrics, where an individual is recognized via iris, retina, sclera, periocular region, or eye movements. This biometric trait is gaining more popularity in applications ranging from international border crossings to unlocking smart devices due to its ease of use and few user-cooperation requirements. The authors provide a review of ocular databases available in the literature, discuss diversities among these databases, and outline how to choose the proper database for experimentation.
- ▶ **“The Evolving Cyberthreat to Privacy,”** **A.J. Burns and Eric Johnson** analyze breaches of personally identifiable information and find that they are significantly larger than other types of breaches. This shows that past breaches can be useful for predicting and mitigating future breaches. Considering the basic principles involved can spur creative thinking about how to improve cyber defenses.

# Advancing Cybersecurity: The Growing Need for a Cyber-Resiliency Workforce

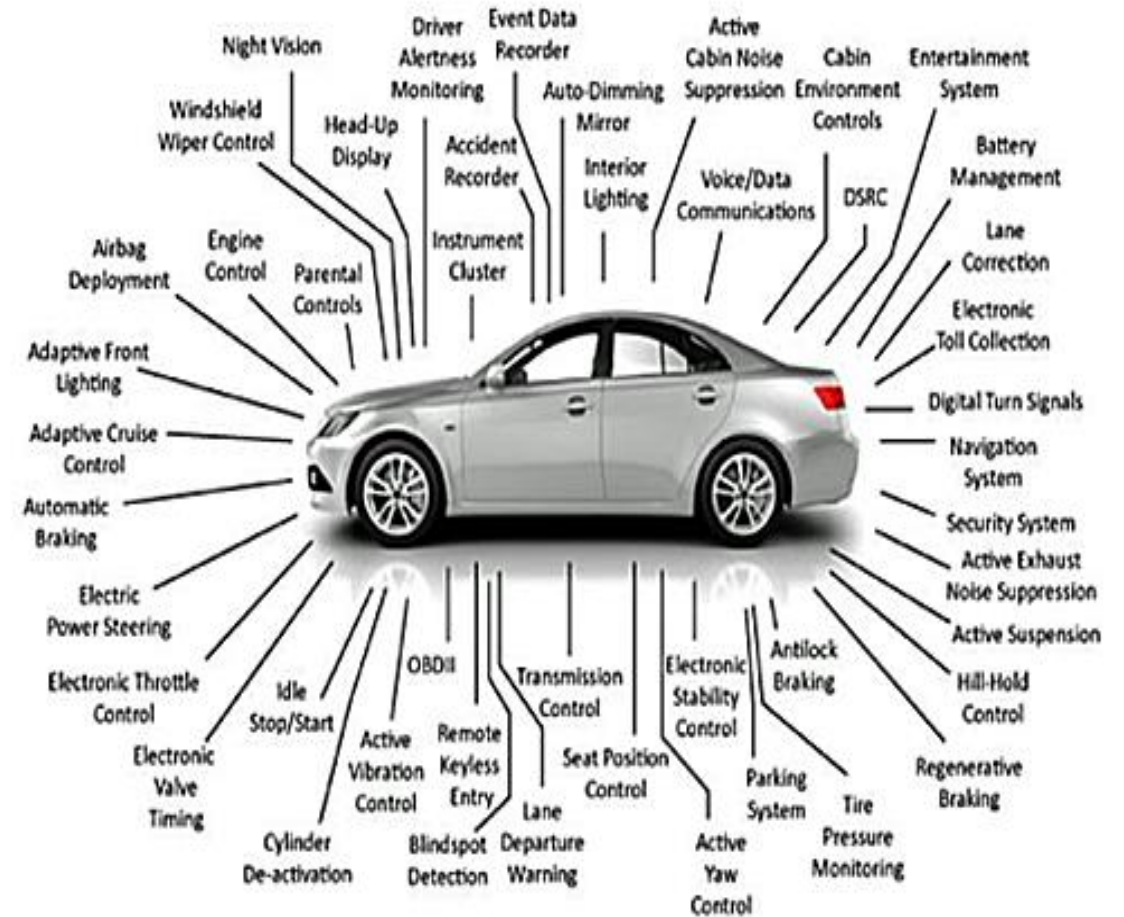
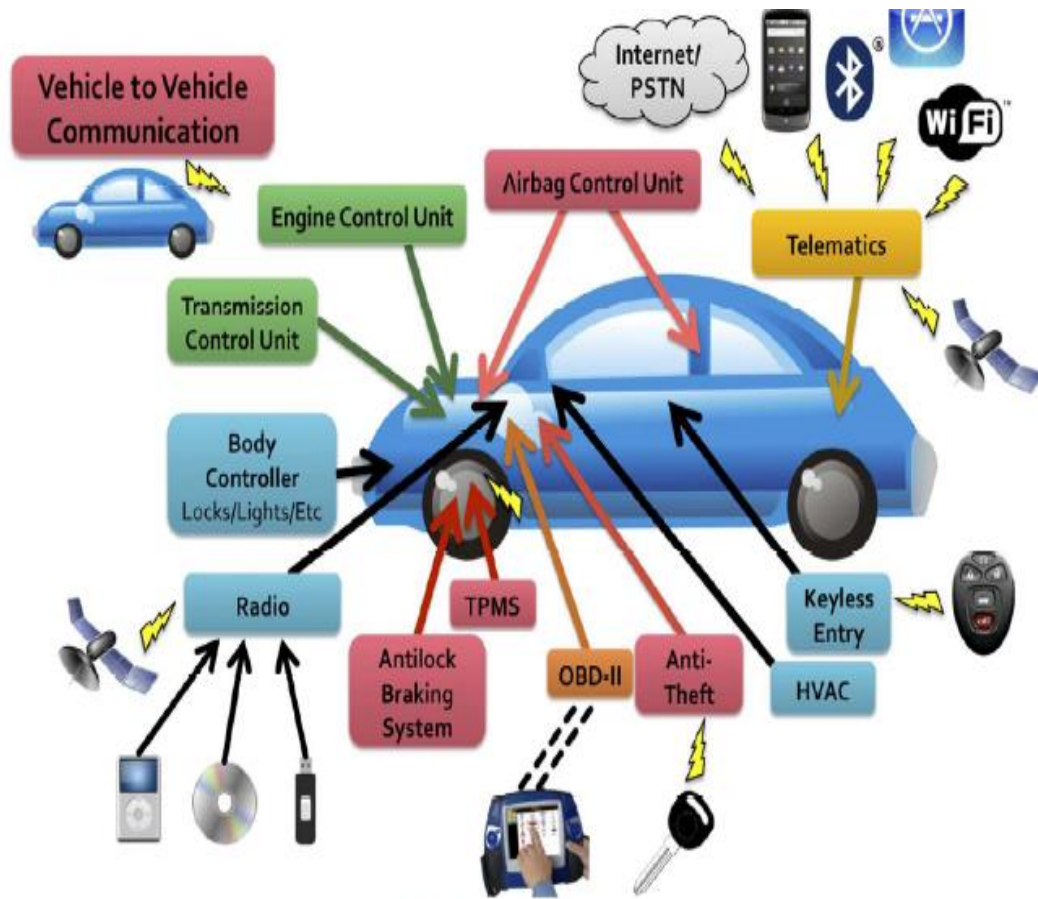


Figure 1. Checkoway *et al*'s work demonstrates the many attack paths available against automotive vehicles [7].  
(Reprinted with permission from Checkoway).

Smart vehicle are *unsecure robots*

# Advancing Cybersecurity: The Growing Need for a Cyber-Resiliency Workforce

## Understanding the Cybersecurity Resiliency Problem

The fact that cyber-physical systems require more cybersecurity attention has been brought to light through several initiatives across industry, academia, and even the United States Department of Defense [8]. For example, in May 2017, SANS hosted their first ever Automotive Cybersecurity Training Summit [9]. Likewise, a five-year collaboration between the National Institute for Standards and Technology (NIST), the National Security Agency (NSA), and MITRE Corporation with backing from several industry partners culminated in the recent publication of NIST SP 800-160 which brings new life to the specialty domain of systems security engineering [10]. Although the science of cyber resiliency has been slow to develop, MITRE's Cyber Resiliency Engineering Framework provides an excellent baseline and is complemented by a number of related efforts towards effective implementation [11]. Before diving further into the topic of cyber resiliency, let's consider for a moment: *What is cyber resiliency, and how is cyber resiliency different from cybersecurity?*

At its essence, cyber resiliency is focused on "fighting through" or "bouncing back" from computing faults, networking failures, cyber attacks, and unpredictable events [12]. This means cyber-physical systems are required to maintain essential operational capabilities regardless of the threats they face (malicious or non-malicious) or where they originate (natural or man-made) [13]. Thus, the

Table 1: Definition and attributes of resiliency for cyber-physical systems. Derived from [11], [15].

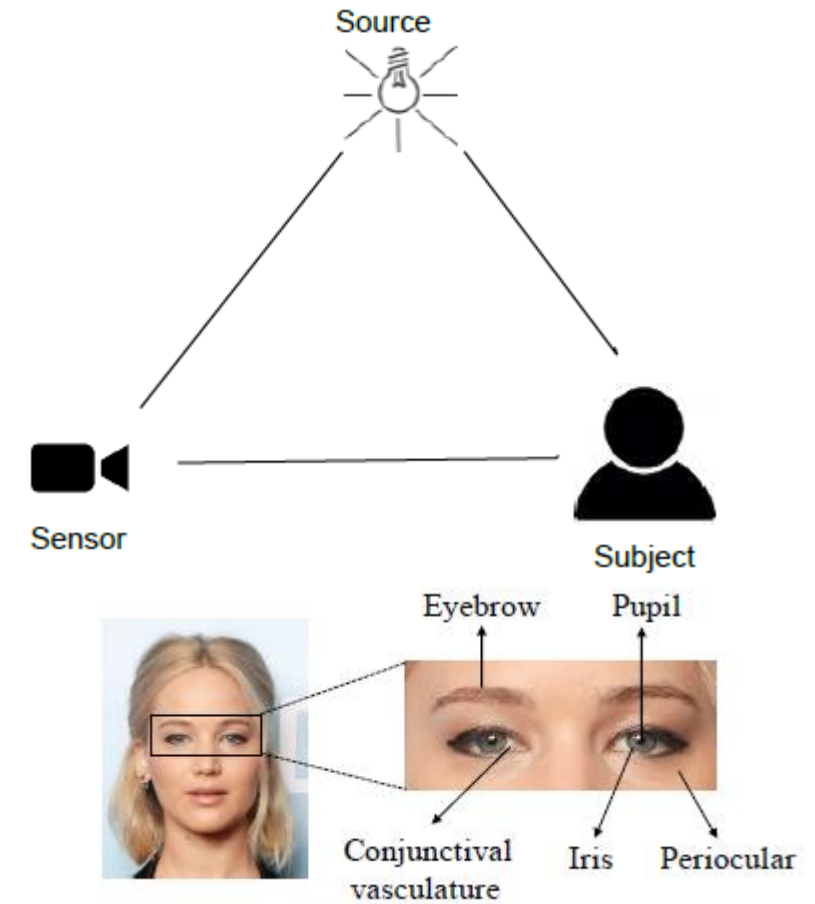
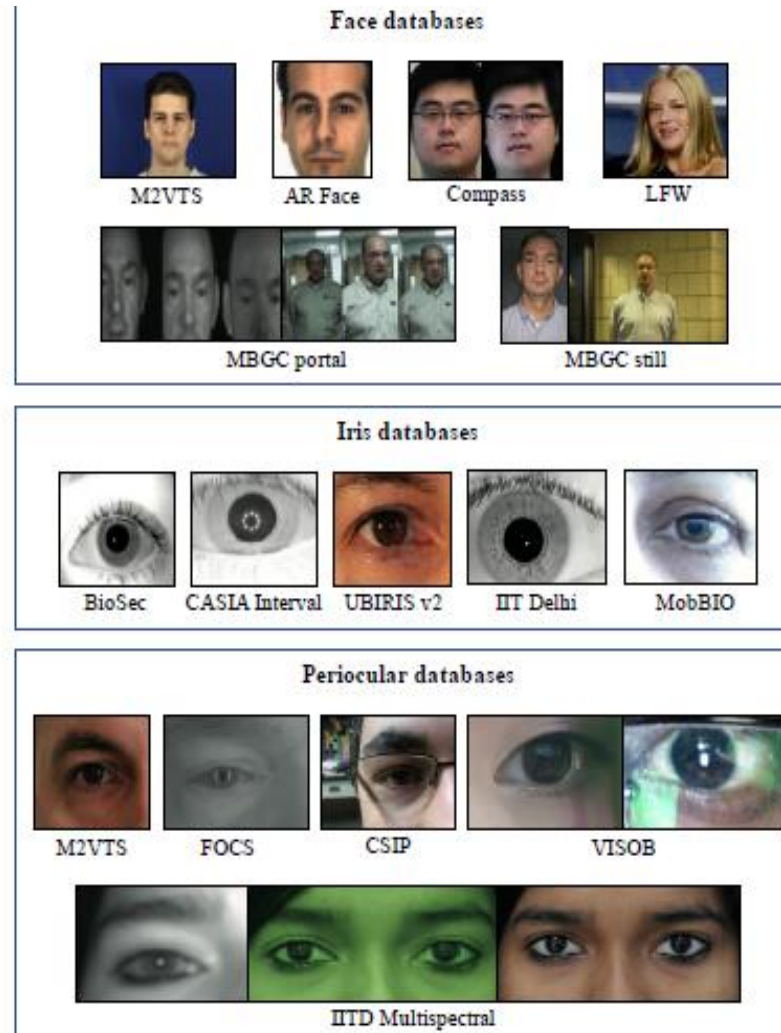
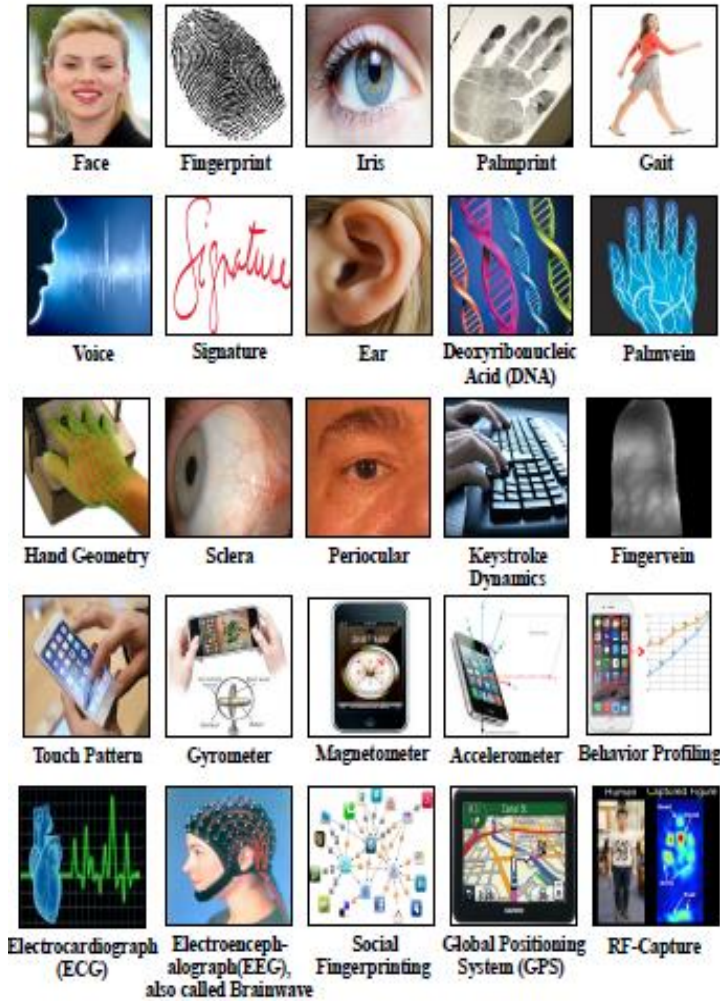
Term	Definition
Resiliency	The ability of a cyber-physical system to anticipate, withstand, and recover from actual and potential adverse events.
Attribute	Description
Anticipate	Planning and/or preparation for known, predicated, and even unknown adverse events to include changes in the operational environment, modes of operation, business/mission functions, emerging threats, integration of novel technologies, and other necessary changes.
Withstand	To absorb or survive the negative impacts of adverse events such as system faults, user errors, software bugs, hardware failures, and cyber attacks.
Recover	To restore business/mission operations (and more specifically desired functionality) to an acceptable level within specified time and performance requirements. Ideally, recovery also includes the ability of the system to

Table 2: Comparison of cyber-physical systems and traditional cyber attributes.

		Cyber-Physical	Traditional Cyber
Comparative Attributes	Business Advantage	Focused on real-time operations, assuring the system is successful – considers what the business does to make a profit	Focused primarily on protecting assets, mostly preventative with intense moments of reaction – considers what valuable business assets need to be protected
	Prioritization of the C-I-A Triad*	Focused on availability with assumed integrity and little regard for confidentiality	Focused on retaining confidentiality of data along with integrity, and less priority on availability
	Scale of the Complexity Challenge	Complex Interactions lead to poorly understood, emergent behaviors	Interactions may be complicated but are mostly linear, leading to well-understood behaviors
	Systems View: People, Processes, and Technology	These "Socio-Technical" systems require nearly constant inputs from users and sensors to monitor and control	Mostly focused on technical security solutions and data security

\*C-I-A Triad: Confidentiality, Integrity, and Availability.

# Experiments with Ocular Biometric Datasets: A Practitioner's Guideline



# Experiments with Ocular Biometric Datasets: A Practitioner's Guideline

Database	Research Lab	Version	Acquisition Device	Images	Subjects	Resolution	Color Model
UBIRIS	Soft Computing and Image Analysis (SOCIA) Group, Department of Computer Science, University of Beira Interior, Portugal	v1 [6]	Nikon E5700	1,877	241	800 × 600	RGB
		v2 [5]	Canon EOS 5D	11,102	261	400 × 300	sRGB
CASIA	Iris Recognition Research Group, Center for Biometrics and Security Research, National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences Beijing, China	TestV1	IrisGuard AD100	10,000	1,000	640 × 480	Grayscale
		IRISv1	Self-developed	756	108	320 × 280	Grayscale
		IRISv2	OKI IRISPASS-h	1,200	60	640 × 480	Grayscale
			CASIA-IrisCamV2	1,200	60	640 × 480	Grayscale
		IRISv3-Interval	Close-up iris camera	2,639	249	320 × 280	Grayscale
		IRISv3-Lamp	OKI IRISPASS-h	16,212	411	640 × 480	Grayscale
		IRISv3-Twins	OKI IRISPASS-h	3,183	200	640 × 480	Grayscale
		IRISv4-Interval	Close-up iris camera	2,639	249	320 × 280	Grayscale
		IRISv4-Lamp	OKI IRISPASS-h	16,212	411	640 × 480	Grayscale
		IRISv4-Twins	OKI IRISPASS-h	3,183	200	640 × 480	Grayscale
		IRISv4-Distance	Long range iris camera	2,567	142	2352 × 1728	Grayscale
IRISv4-Thousand	Irisking IKEMB-100	20,000	1,000	640 × 480	Grayscale		
IRISv4-Syn	By image synthesis	10,000	1,000	640 × 480	Grayscale		
ND-IRIS	Department of Computer Science & Engineering, University of Norte Dame, USA	-	Iridian LG EOU2200	64,980	356	640 × 480	Grayscale
MMU	Multimedia University Malaysia	v1	LG IrisAccess2200	450	100	320 × 280	Grayscale
		v2	Panasonic BM - ET100US Authenticam	995	100	320 × 280	Grayscale
BATH	University of Bath Bath United Kingdom	Iris DB 400		8,000	200	1280 × 960	Grayscale
		Iris DB 800	IrisGuard AD-100 Dual-Eye Autofocus Camera	16,000	400	1280 × 960	Grayscale
		Iris DB 1600		32,000	800	1280 × 960	Grayscale



# The Evolving Cyberthreat to Privacy

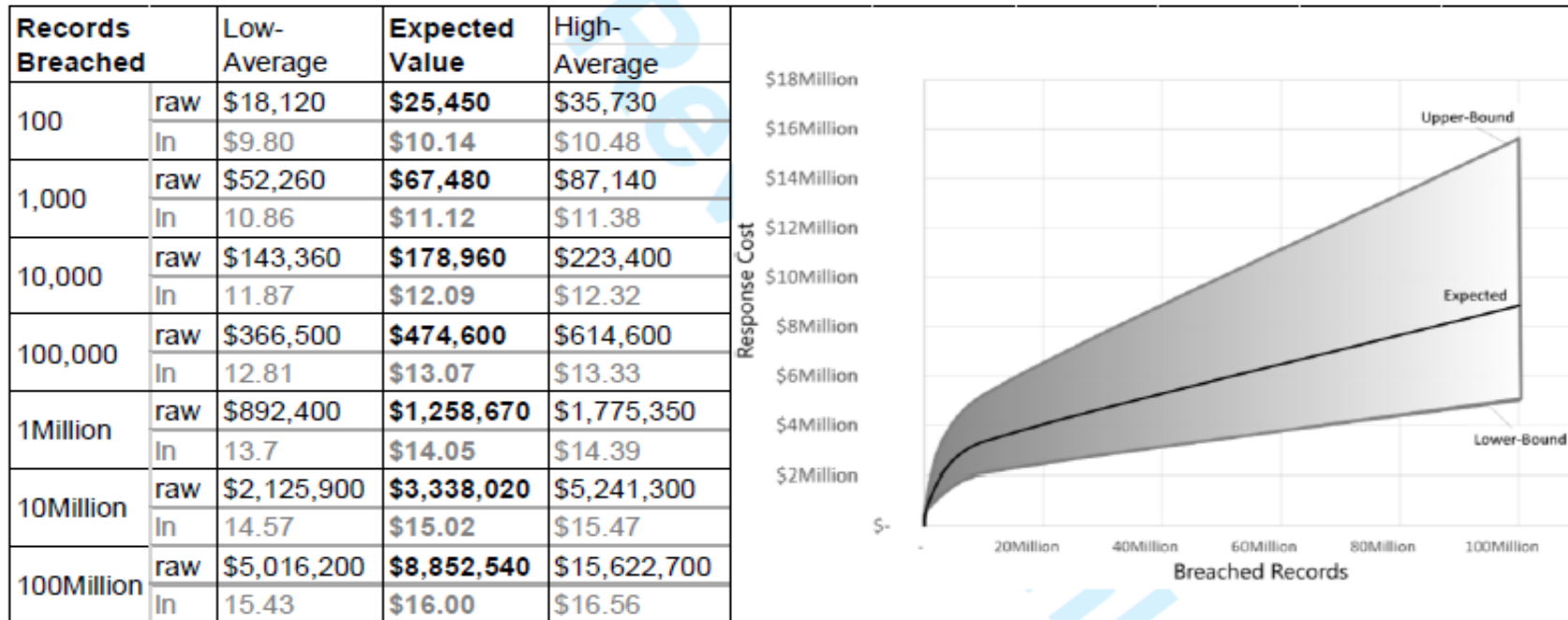


Figure 4. Verizon Breach Cost Estimates.

Deriving the cost function shown in figure 10 yields  $y=3618x^{0.4236}$  ( $R^2=1.0$ ) where  $y$  is the cost estimate (in raw dollars) and  $x$  is the (raw) number of records breached. Therefore, the log-log relationship can also be written as the linear function  $y=0.4236x+8.1938$  where  $y$  is  $\ln(\text{cost})$  and  $x$  is  $\ln(\text{records})$ . Adding the error term to our previous cost function results in a cost model of the form

# The Evolving Cyberthreat to Privacy

**Table 1. Simulated Cost Estimates**

Records	Size	Minimum	Mean	Maximum
100 ( $\pm 0.5$ )	n=21	\$18,564.38	\$25,241.88	\$32,630.41
1,000 ( $\pm 1$ )	n=18	\$53,852.28	\$72,998.20	\$96,374.80
10,000 ( $\pm 10$ )	n=24	\$125,847.00	\$165,034.97	\$252,470.13
100,000 ( $\pm 100$ )	n=29	\$286,184.29	\$454,642.24	\$698,069.66
1,000,000 ( $\pm 1,000$ )	n=11	\$898,846.81	\$1,221,412.41	\$1,584,211.05
10,000,000 ( $\pm 10,0000$ )	n=29	\$2,258,982.48	\$3,313,083.69	\$4,745,512.73
100,000,000 ( $\pm 100,0000$ )	n=1	\$9,241,390.96	\$9,241,390.96	\$9,241,390.96

## Cost of Hacking

Based on our derived cost model and the CDF of non-zero record hacks, we examined the cost of hacking incidents for 2014, 2015, and our projected 2015 estimates from above. To do this, we applied a Monte Carlo approach to simulate three datasets of 100,000 observations based on our derived breach distributions and the cost model. We generated three sets of simulated breach costs in the form

$$y=0.4236x_{abb'}+8.1938+\varepsilon,$$

where  $y$  is  $\ln(\text{cost})$ ,  $x$  is  $\ln(\text{records})$ , and  $\varepsilon$  is the cost variance ( $\mu = 0$ ;  $\sigma=0.178$ ) [ $x_a = 2014_{\text{actual}}$ ;  $x_b = 2015_{\text{actual}}$ ;  $x_{b'} = 2015_{\text{Projected}}$ ; max of  $x_{abb'} = 18.683$ [observed overall maximum in the PRCH dataset]; min of  $x_{abb'} = 0.69$ [observed overall minimum in the PRCH dataset].

# Table of Contents

- ▶ Introduction – IT Pro SI on Cyberthreats and Security
- ▶ Information Security Management Models for Risk Management
- ▶ Featured Articles
- ▶ VPKI Hits the Highway
- ▶ AI and Machine Learning – Risk Management for Finance Industry
- ▶ References + Q&A



**Software Technology Conference Tutorial – Part II**

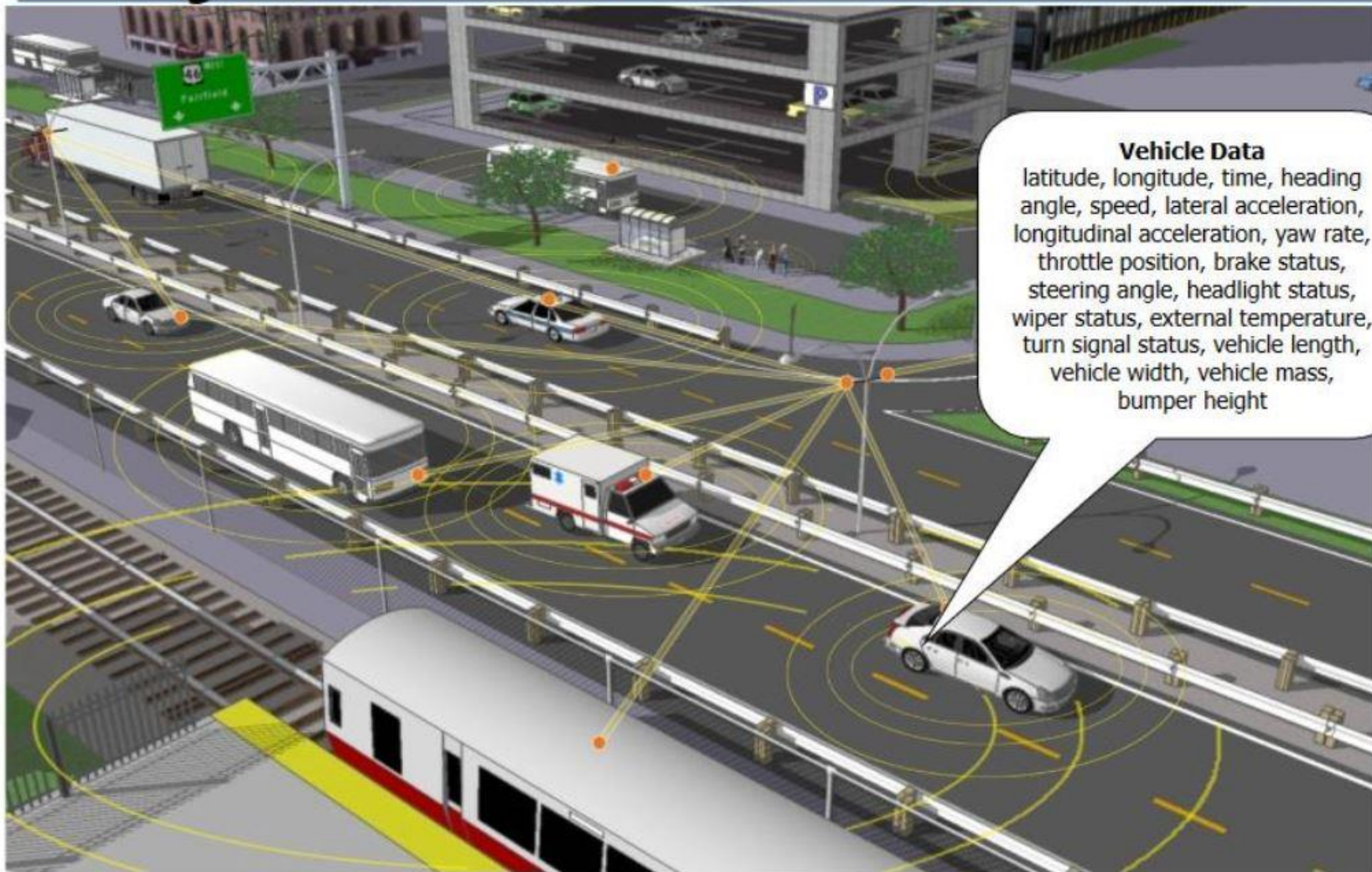
# **VPKI Hits the Highway – Security and Privacy Models**

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

NIST  
Gaithersburg, MD  
25 September 2017

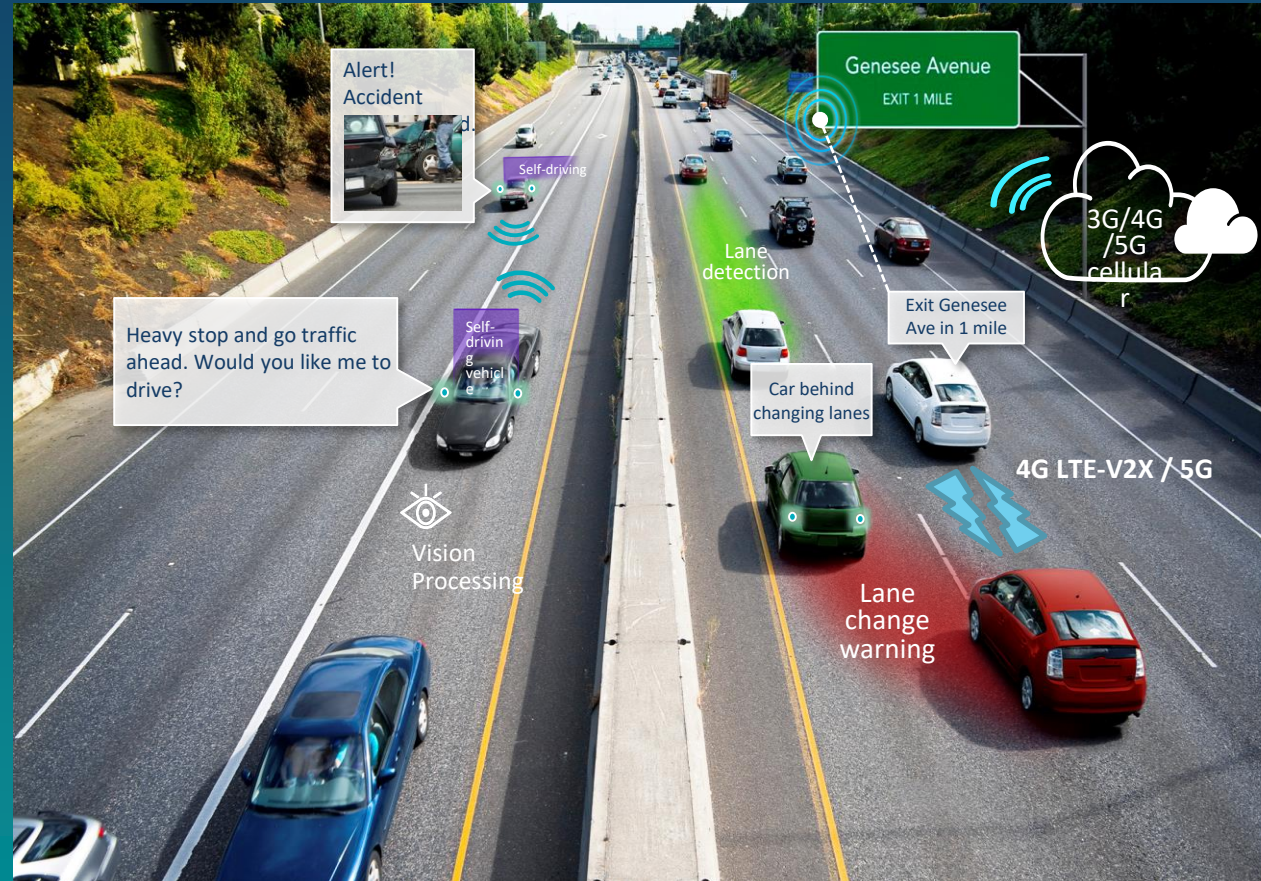


# Fully Connected Vehicle



**Vehicle Data**  
latitude, longitude, time, heading angle, speed, lateral acceleration, longitudinal acceleration, yaw rate, throttle position, brake status, steering angle, headlight status, wiper status, external temperature, turn signal status, vehicle length, vehicle width, vehicle mass, bumper height

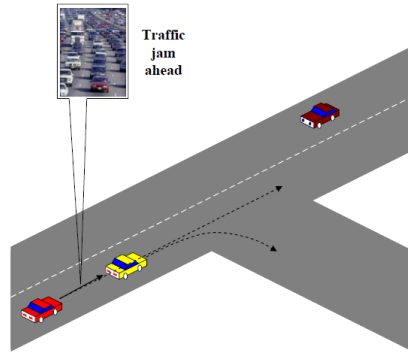
# A New Era of Connected Car Capabilities



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

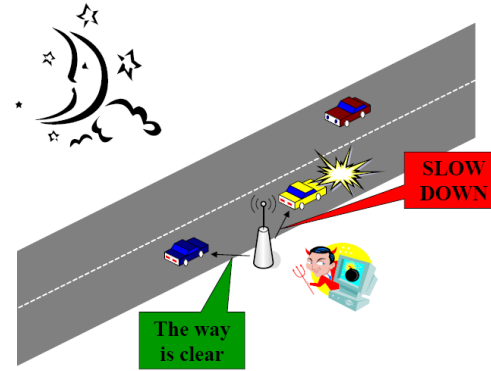
# Security Architecture for VANETS ([EPFL V-PKI – J.Hubaux et. al.](#)) - 2004

Attack 1 : Bogus traffic information



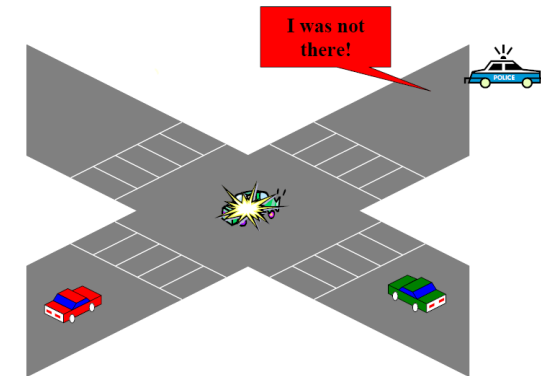
■ Attacker: **insider, rational, active**

Attack 2 : Disruption of network operation



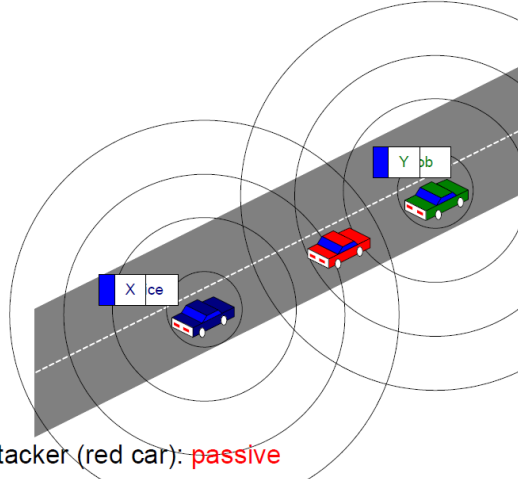
■ Attacker: **malicious, active**

Attack 3: Cheating with identity, position or speed



■ Attacker: **insider, rational, active**

Attack 4 : Uncovering the identities of other vehicles

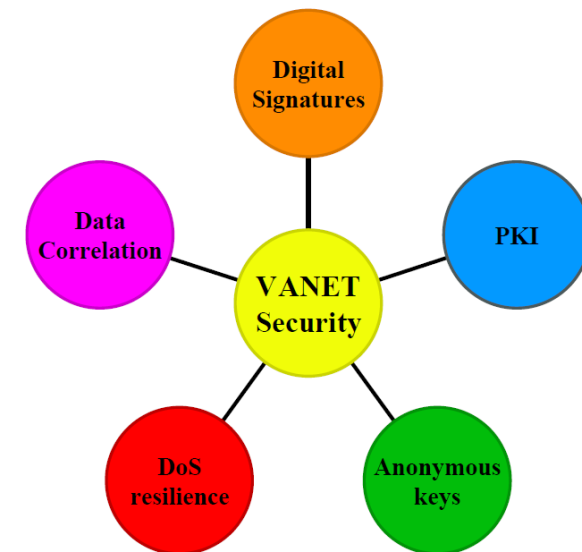


■ Attacker (red car): **passive**

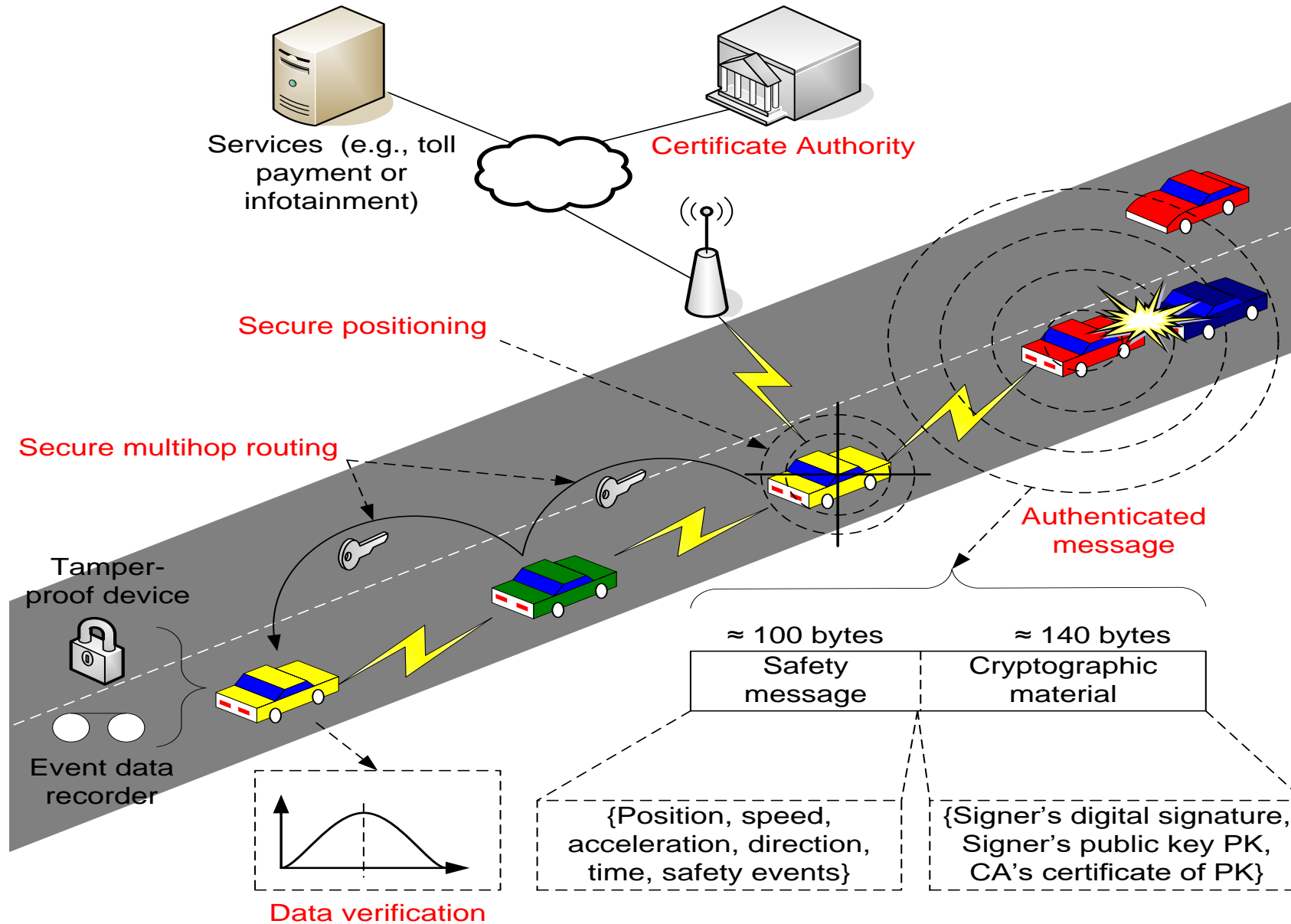
## Attacker's model in Vehicular Communications

- 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.)

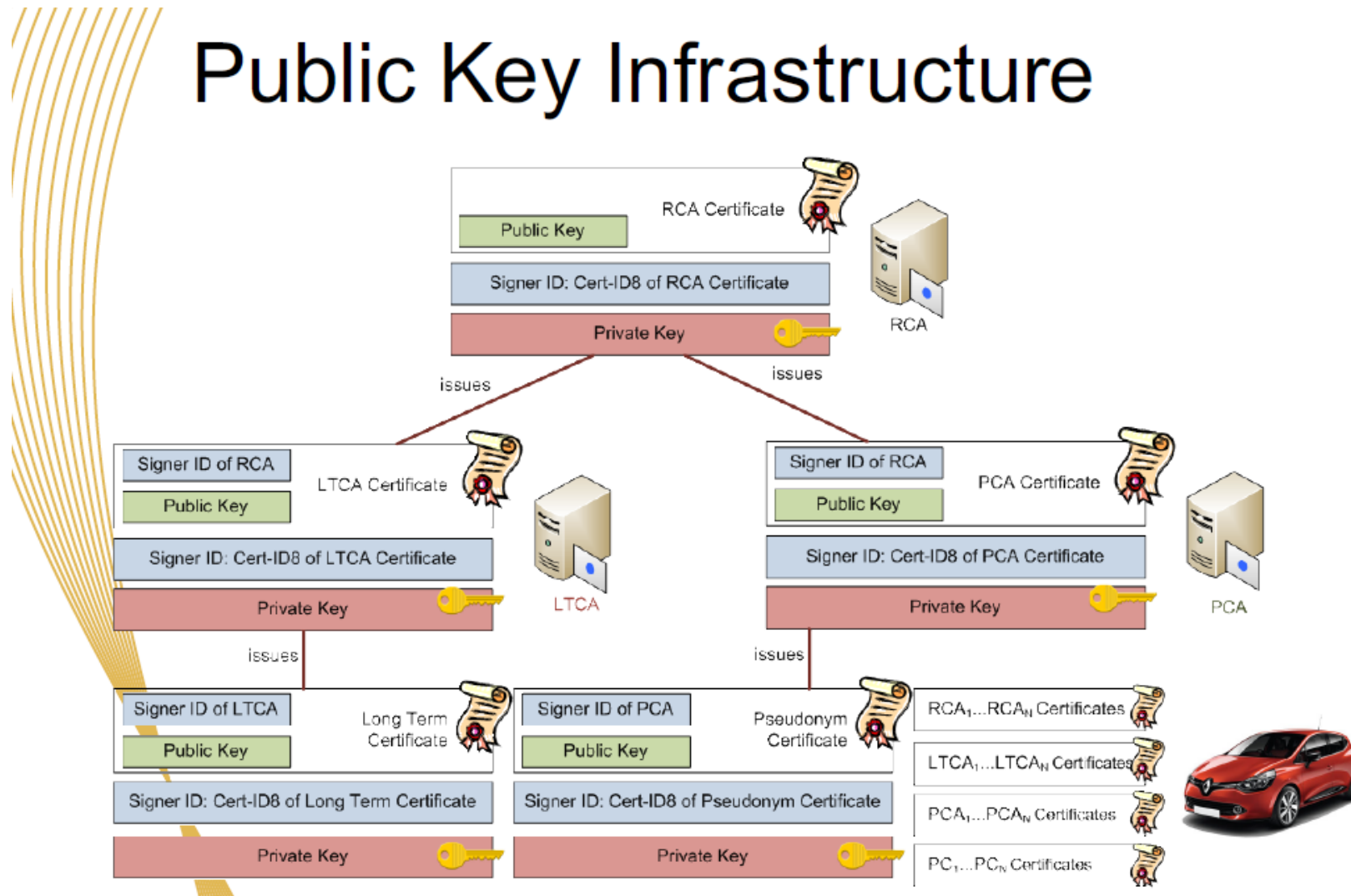




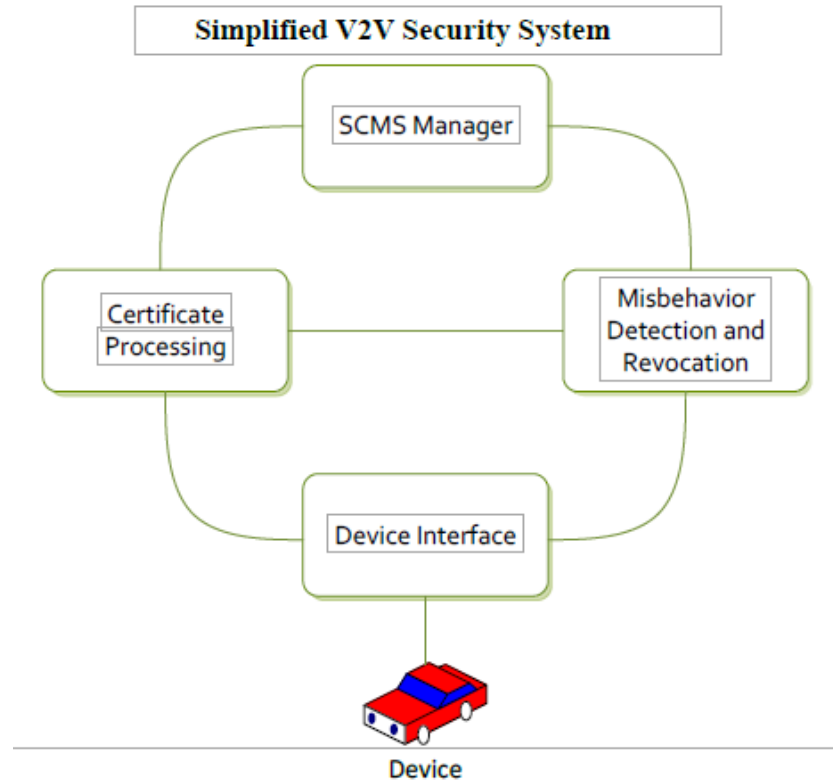


# PRESERVE V-PKI Infrastructure (EU)

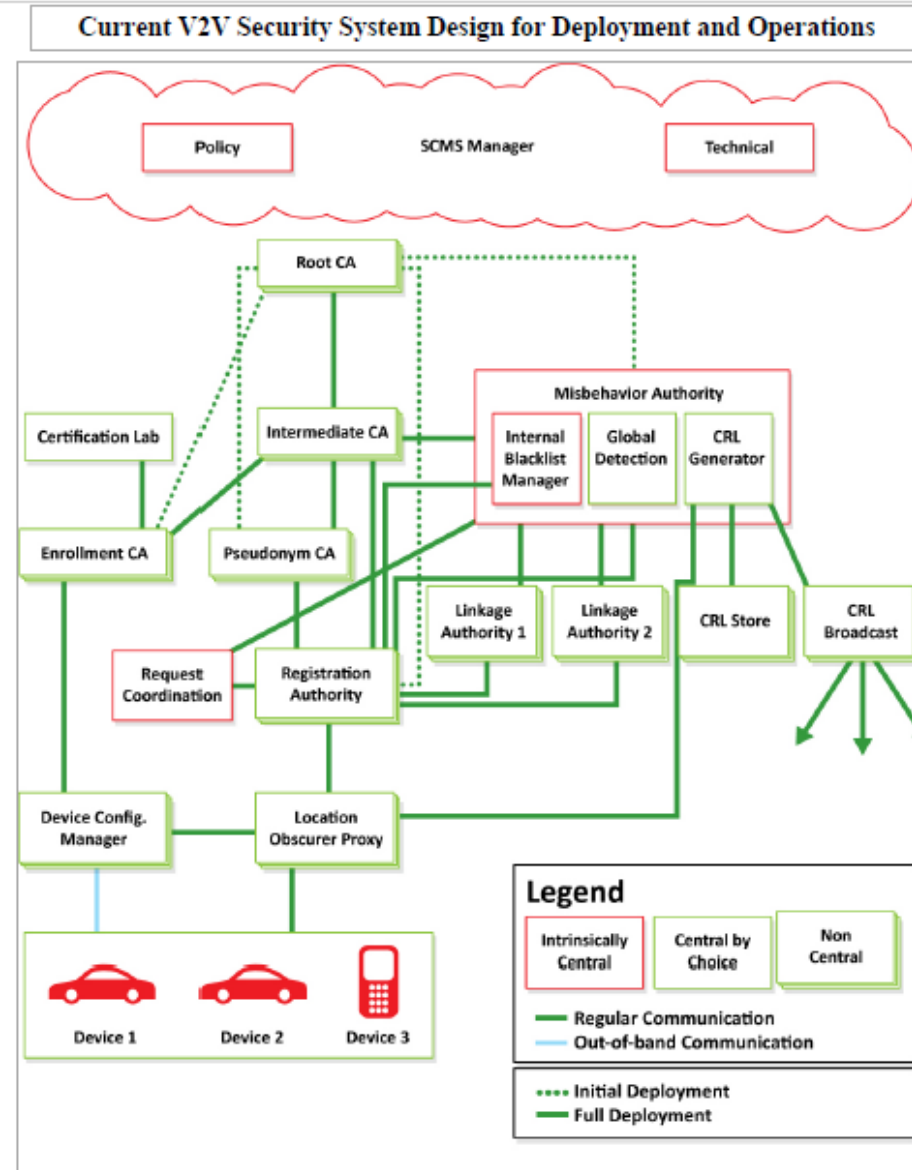
## Public Key Infrastructure



# 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](http://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

12/4/2018

36

# 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>

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

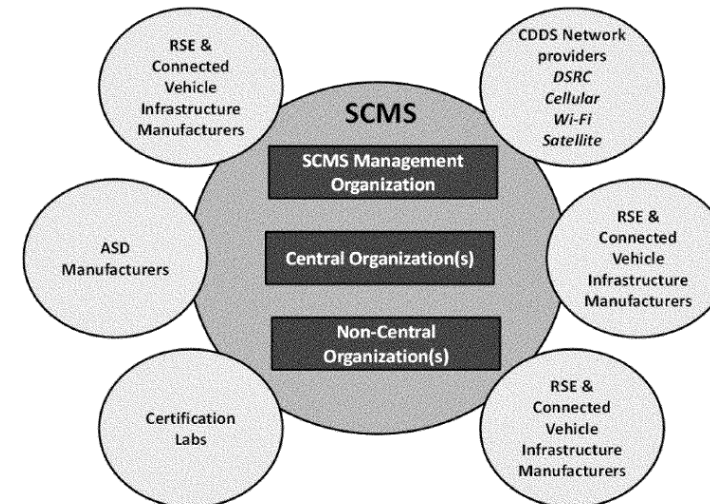
- A. V2V Communications Proposal
  - Overview
- B. Proposed V2V Mandate for New Light Vehicles, and Performance Requirement for Aftermarket for Existing Vehicles
- C. V2V Communication Devices That Would Be Subject to FMVSS No. 150
  - 1. Original Equipment (OE) Devices on New Motor Vehicles
  - 2. Aftermarket 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

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



\*\* 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

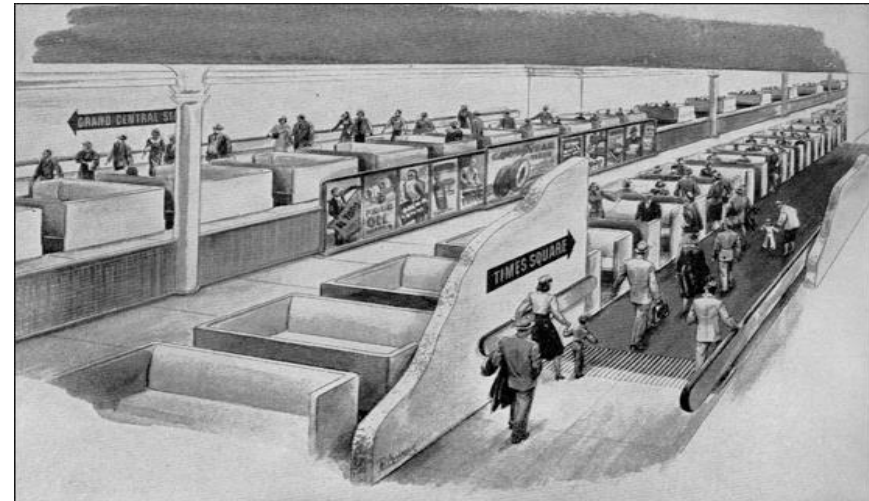
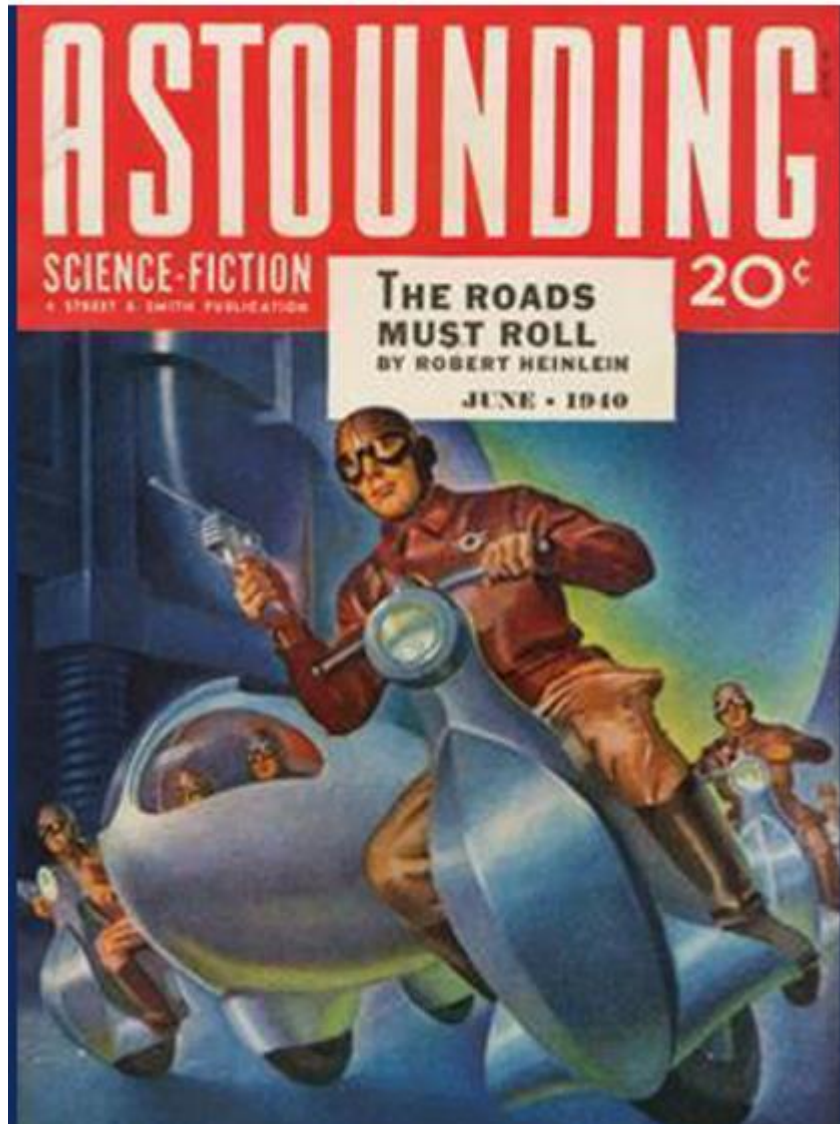
Greentech

Secure Automotive Networking

Press Release

Program Management

# The Roads Must Roll – Robert Heinlein





## Table of Contents

- ▶ Introduction – IT Pro SI on Cyberthreats and Security
- ▶ Information Security Management Models for Risk Management
- ▶ Featured Articles
- ▶ VPKI Hits the Highway
- ▶ AI and Machine Learning – Risk Management for Finance Industry
- ▶ References + Q&A

# AI and Machine Learning – Rick Management for Finance Industry

<https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-ai-risk-powers-performance.pdf>

**Deloitte.**



## Why artificial intelligence is a game changer for risk management

The idea of computers outsmarting and replacing humans has existed in movies and books for decades. Fortunately, that hasn't happened on a wide scale yet. But what has happened is the recent emergence of artificial intelligence concepts—specifically cognitive computing. These concepts involve advanced technology platforms that can address complex situations that are characterized by ambiguity and uncertainty. Cognitive computing has begun to augment business decisions and power performance right alongside human thought process and traditional analytics. In fact, the domain of risk management lends itself particularly well to cognitive computing capabilities, as typical risk issues often include unlikely and/or ambiguous events.

Companies and public sector organizations have progressed in terms of using massive amounts of internal and external data to take a more preventative risk stance, says **Samir Hans**, a Deloitte Advisory principal in the Forensics & Investigations practice of Deloitte Transactions and Business Analytics LLP. However, traditional methods of analysis have become increasingly incapable of handling this data volume. Instead, cognitive capabilities—including data mining, machine learning, and natural language processing—are supplanting traditional analytics and being applied against these massive data sets to help find indicators of known and unknown risks. ➔

“Given the increases in computational processing power and corresponding decreases in the costs of data storage, artificial intelligence in the business world is fast becoming a reality. These artificial intelligence or cognitive-based technologies help computers interact, reason, and learn like human beings.”

**Samir Hans**  
Deloitte Advisory principal  
Forensics & Investigations  
Deloitte Transactions and  
Business Analytics LLP

# AI and Machine Learning – Rick Management for Finance Industry

<http://www.rmmagazine.com/2018/09/17/artificial-intelligence-and-risk-management/>

**RISK MANAGEMENT**

**EMPOWER RESULTS**

Get the insights to empower your organization at [aon.com/fullpicture](http://aon.com/fullpicture)

AON Empower Results\*

Subscribe to RSS

Home Features Columns Topics Blog Digital Issue Subscribe RIMS.org

## Artificial Intelligence and Risk Management

by Daniel Wagner and Keith Furst | September 17, 2018 at 6:00 am

The cyber era heralded unparalleled opportunities for the advancement of science, technology and communication, and unleashed a range of new attack vectors for rogue elements, criminals and virtual terrorists. The era of machine learning is doing much the same, for the promise of advancement has gone hand in hand with a range of new perils and an expanded set of actors capable of carrying out attacks using artificial intelligence (AI) and machine learning systems.



This flows naturally from the efficiency, scalability and ease of diffusion of AI systems, which can increase the number of actors who can carry out attacks against civilian, business and military targets.

The typical character of threats derived from AI are likely to shift in some distinct ways in the future. Attacks supported and enabled by progress in AI will be especially effective, finely targeted, and difficult to attribute, as they have been in the cyber arena. Given that AI can, in a variety of respects, exceed human capabilities, attackers may be expected to conduct more effective attacks with greater frequency and on a larger scale. This is presenting new challenges for risk managers and promises to present even greater challenges in the decades to come.

Attackers often face a trade-off between how efficient and scalable their attacks will be, versus how finely targeted. AI systems may be able to avoid detection by using a learning model that automatically generates command and control domains that are indistinguishable from legitimate domains by human and machine observers. Such domains can be used by malware to “call home” and allow malicious actors to communicate with host machines. Attackers are likely to leverage the growing capabilities of reinforcement learning to benefit from experience in order to craft attacks that current technical systems and IT professionals are not

**RISK MANAGEMENT**

**RISK MONITOR**

LATEST HEADLINES

### RISK MANAGEMENT MONITOR

Q&A: Resiliency in India November 26, 2018

Eyes on the Road, Hands on the Wheel – Organizations Focused on Distracted Driving November 19, 2018

RIMS Risk Forum 2018 India Kicks Off In Mumbai November 14, 2018

Updates to PIPEDA, Canada's Own GDPR November 7, 2018

How to Use ODG Data to Improve Workers Comp Case Management November 6, 2018

RESILIENCE IS A CHOICE.

FM Global

> Learn more

# AI and Machine Learning – Rick Management for Finance Industry

<http://www.yogeshmalhotra.com/>

**Global Risk Management Network, LLC**, Cornell Business & Technology Park, Ithaca, New York 14852-4892.

**Griffiss Cyberspace**, Griffiss Business & Technology Park, Griffiss AFB, Rome, New York 13442-1155.

**World-Leading Hi-Tech R&D Leading Global AI, Machine Learning, and, Risk Management Practices™**

**Post-Doctoral R&D in AI & Machine Learning: Quant Finance, Computer Science, Cybersecurity.**

**PhD, MSQF, MSCS, MSNCS, MSAcc, MBAEco, BE, CEng, CISSP, CISA, CEH, CCP-CDP, CPA Education**

**Who's Who in America®**, **Who's Who in the World®**, **Who's Who in Finance & Industry®**, **Who's Who in Science & Engineering®**

---

[Griffiss Cyberspace™ & Griffiss Drones Network™ Ventures Advance AI-ML-Cyber Revolution in Mohawk Cyber Vall](#)

[JP Morgan Hedge Funds Quant : Princeton Quant Finance Expert : MIT AI-Machine Learning Expert : NYS CISO Exp](#)

[Impact: \[Computational Quant Finance : AI & Machine Learning : Cybersecurity & Cryptography : Digital Transform](#)

[FinRM™: \[Download our Research: Future Of Finance™ : Model Risk Arbitrage™ : Griffiss Cyberspace](#)

[AACSB: Research Impact among Finance Nobel Laureates Black-Scholes, Markowitz & Sharpe: Uncertainty & Risk Management](#)

[AFRL Commercialization Academy: Griffiss Cyberspace™ & Griffiss Drones Network™ Ventures in Spring 2019 Cohort.](#)

[MIT: AI & Machine Learning: Industry Expert: Deep Learning, NLP, Robots: Self-Driving Cars: Unmanned Ground Vehicles.](#)

[Princeton: Princeton Quant Finance & Trading Presentations: AI & Machine Learning: Sponsors: Goldman Sachs, Citadel, etc.](#)

[CFA Society: Invited Keynote: JP Morgan & Goldman Sachs Practices Case Studies: Model Risk Management with Auto-ML.](#)

[RISK.Net: Bridging Networks, Systems and Controls Frameworks for Cybersecurity Curriculums and Standards Development.](#)

[NAIC: National Association of Insurance Commissioners: Pre-empting the Forthcoming Global Cyber Risk Insurance Crisis.](#)

[AFCEA C4I & Cyber Conference: Cybersecurity Risk & Uncertainty Management: AI-ML and Risk Management Controls.](#)

[SSRN: AI-Machine Learning & Risk-Uncertainty Management:SSRN: 63 Top-10 Research Rankings: Top 2% Authors.](#)

[Editor-Referee: ACM, IEEE, Society of Actuaries, Society of Modeling & Simulation, 40+ Top-Tier Journals & Conferences.](#)

Building and Leading Worldwide CEO-CxO Digital practices for over 25-Years: Digital Transformation  
AI & Machine Learning; Analytics & Data Science; Cybersecurity & Cryptography; Quantitative Fin

CEO-CxO Teams AI-ML-Strategy Advisor. JP Morgan Quant: Wall Street Hedge Funds. NYS CIO-C  
Expert Panels: **National Science Foundation** Computer Scientists, **United Nations** Global Ec  
Advisor: **Big-4** Sr. Partners, \$100 B Hi-Tech Firms, **Silicon Valley** VCs-CEOs, US & World Gover  
Global Financial Systems Leader, **Big-3 Finance-IT**, **Wall Street Banks-Hedge Funds** \$1 Tril  
Pioneer: **Worldwide Digital Practices**: Clients-Patrons: Goldman Sachs, Google, IBM, Intel, O  
Founder: **Top Digital Site**, **Top-3 Search Engine**, **Top-10 Social Network**: Largest Finance-

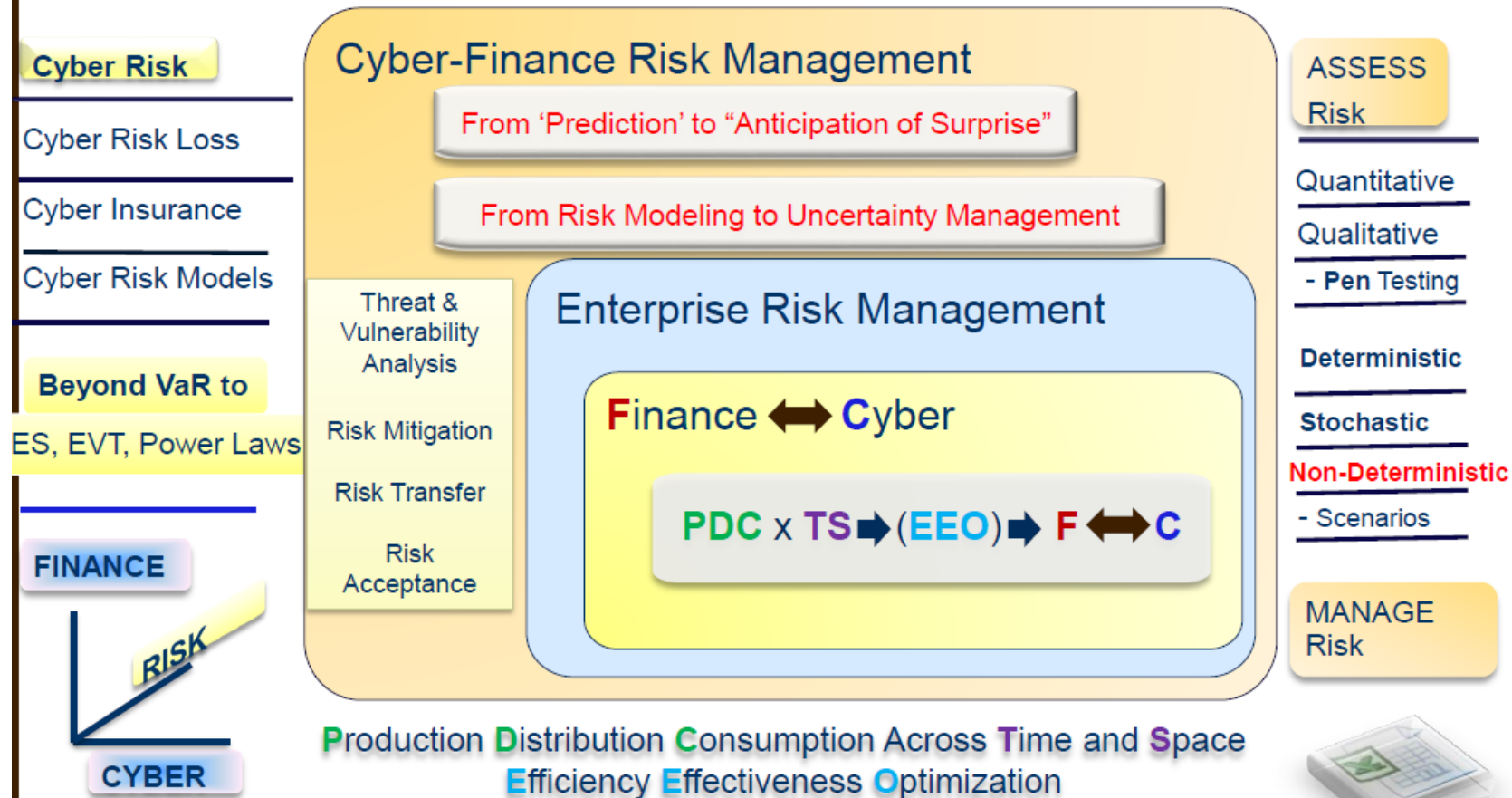


[LinkedIn](#)

# AI and Machine Learning – Risk Management for Finance Industry

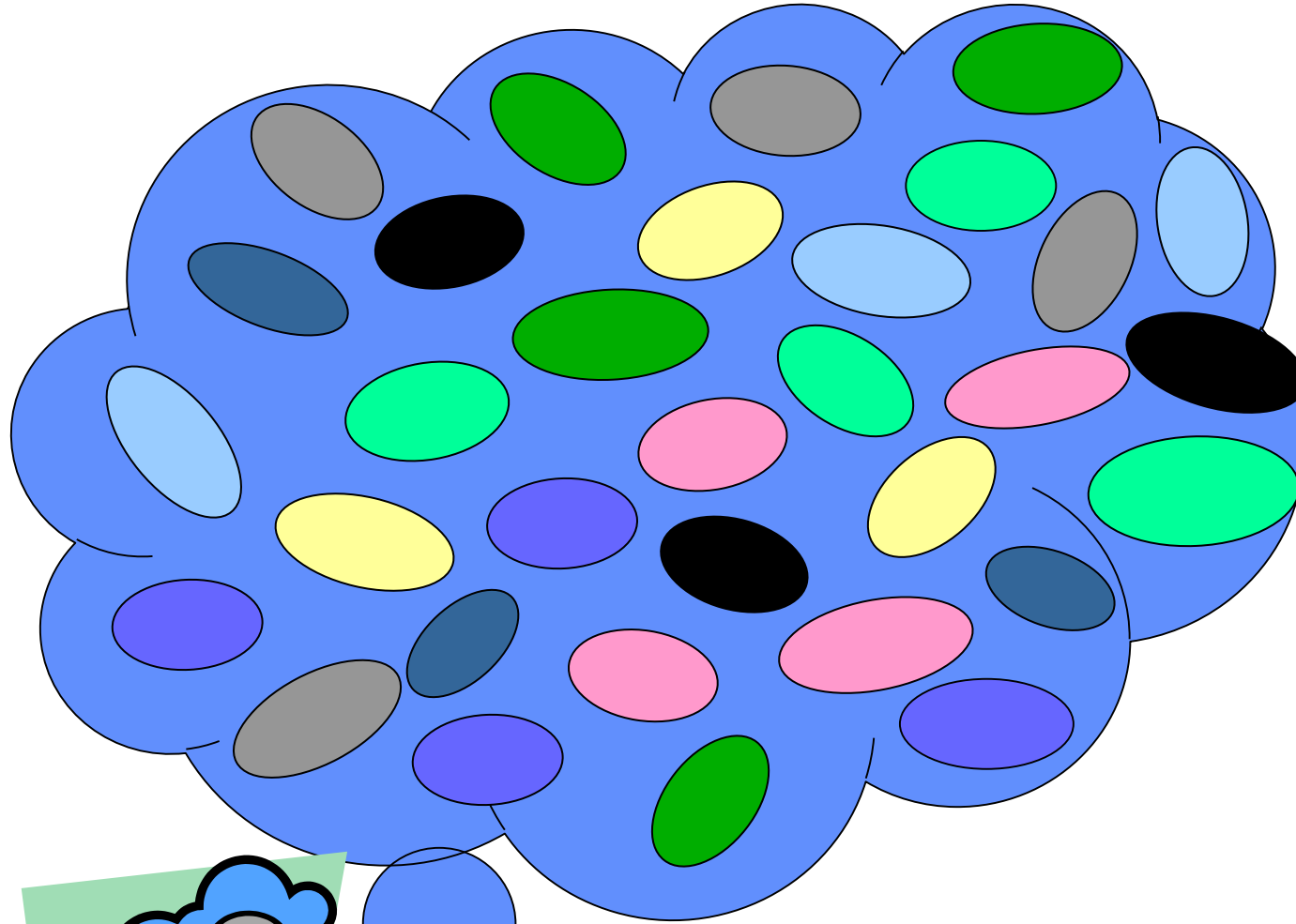
<http://www.yogeshmalhotra.com/>

## Cybersecurity & Cyber-Finance Risk Management Strategies, Tactics, Operations, & Intelligence Enterprise Risk Management to Model Risk Management Understanding Vulnerabilities, Threats, & Risk Mitigation



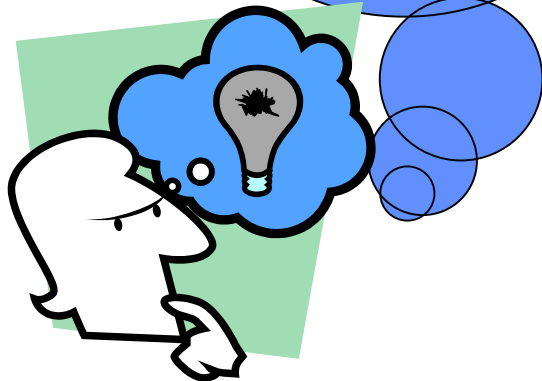
5/9/2018

# Managing Information Security Risk



IT 101 – What Problems Are We Trying to Solve?

- Identify 'Fix-It' areas in the program
- Understand Current State (Remediation)
- Improve 'ad hoc', 'not my problem' state
- Reduce Program Risk**
- Improve Continuous Monitoring Process



# Assessing Security and Privacy in the Cloud – Blue Sky or Rain?



5/9/2018

## Table of Contents

- ▶ Introduction – IT Pro SI on Cyberthreats and Security
- ▶ Information Security Management Models for Risk Management
- ▶ Featured Articles
- ▶ VPKI Hits the Highway
- AI and Machine Learning – Risk Management for Finance Industry
- ▶ References + Q&A



# The Failure of Asset-Based Risk Assessments (Walt Williams)

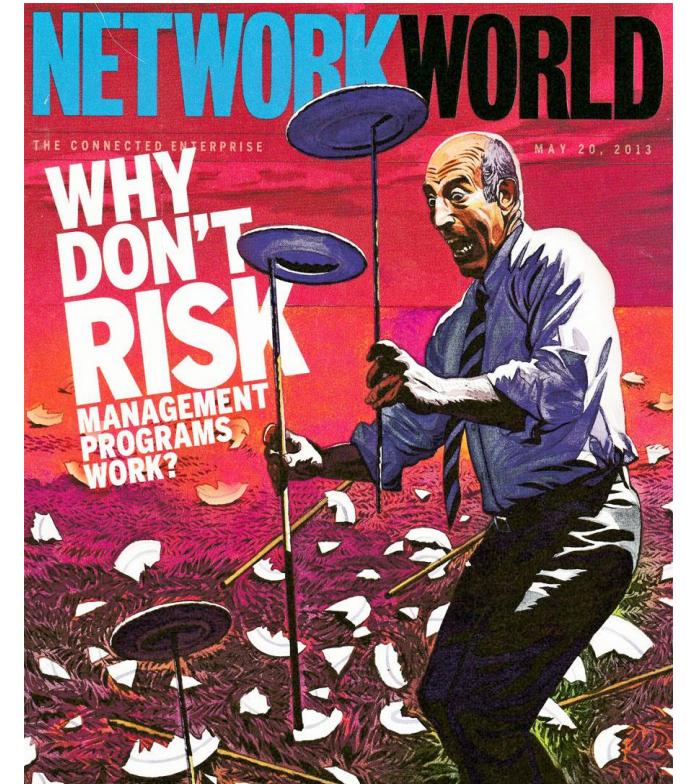
<https://infosecuritymetrics.wordpress.com/>

Most people don't understand that asset management risk Management Models for Risk Management have been failing us for years, and we're seeing the consequences of that failure in various laws and regulations. ***Assets are owned by an organization and have value. It makes sense to protect your assets, regardless of how you define what an asset is.***

The GDPR, and other data privacy laws have been introduced over the last decade precisely because the ***data that is in scope for the data privacy laws is not an asset for any organization. It is an asset for various individuals. This information doesn't bring the organization any value, and because of that, it is often not protected.***

Until the GDPR is enforced there is no incentive to protect name & email address. Organizations consider these data items to have no value. Individuals, on the other hand, expect that the value of the information is understood and properly protected by organizations that the data is entrusted to.

The data simply hasn't been an asset to the organization, not worth protecting. Until organizations cease using an asset based approach to risk management, you will see governments stepping with impactful regulations because ***asset based risk management frameworks don't lead to organizations protecting all the data. Just the data that drives business value. And this is why we fail.***



# SecurityFeeds Website - <http://securityfeeds.com/>

**SecurityFeeds**  
Your source for enterprise security management

Introduction Services About Resources Security Industry News Blog Contact Business Card

**Welcome to Security Feeds**

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. In the area of Program Management Mr. Weil has directed professional IA program teams in both the commercial and federal sectors. Professional expertise areas are listed here.

- IEEE IT Professional - (Securing IT - Editor)
- Management of Professional Services Organization
- Governance, Risk and Compliance (GRC) Program Development (IT Audit)
- Enterprise Risk Management and FISMA Compliance
- Cloud Security (FedRAMP) for federal and Cloud Service Providers (CSPs)
- ISO 27001 Accreditation for certifying organizations and commercial clients.
- IEEE-USA Professional Achievement Award for Individuals
- Certified Cloud Security Professional (ISC2)

**Professional Affiliations**

- ISACA 40
- PMI
- IEEE COMMUNICATIONS SOCIETY
- IEEE
- GLOBECOM
- (ISC)<sup>2</sup>

Connect on LinkedIn  
Tim Weil

**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"**

# References Used in This Presentation

- ▶ Scoping the Cyber Security Body of Knowledge” Awais Rashid et al, IEEE Security and Privacy Magazine, Volume 16, Issue 3, May, June 2018
- ▶ G. Hughson , “Architecture and OODA Loops - <https://genehughson.wordpress.com/2016/01/13/architecture-and-ooda-loops-fast-is-not-enough/>
- ▶ 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>
- ▶ W. Whyte, A. Weimerskirch et al, Crash Avoidance Metrics Partnership, Technical Design of the Security Credential Management System (Final Report), Cooperative Agreement Number DTFH61-05-H-01277, July 31, 2014 online available at - <https://www.regulations.gov/contentStreamer?documentId=NHTSA-2015-0060-0004&attachmentNumber=2&contentType=pdf>
- ▶ Y. Molhatra., Cybersecurity & Cyber-Finance Risk Management: Strategies, Tactics, Operations, & Intelligence: Enterprise Risk Management to Model Risk Management: Understanding Vulnerabilities, Threats, & Risk Mitigation, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2693886](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2693886)
- ▶ W. Whyte et al., “A Security Credential Management System for V2V Communications,” Proc. IEEE Vehicular Networking Conf. (VNC), 2013  
[https://www.researchgate.net/publication/271554151\\_A\\_security\\_credential\\_management\\_system\\_for\\_V2V\\_communications](https://www.researchgate.net/publication/271554151_A_security_credential_management_system_for_V2V_communications)

**Thank you for joining us!**

