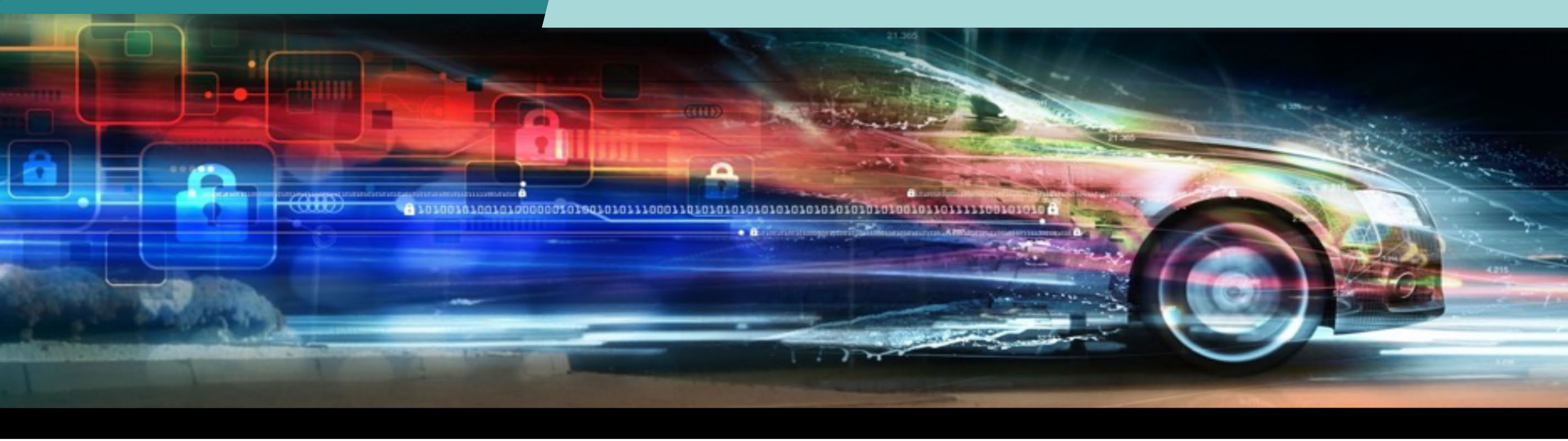


Welcome to Auto-ISAC!

Monthly Virtual Community Call

April 5th, 2023

This Session will be recorded.

TLP:CLEAR

AUTO-ISAC
Automotive Information Sharing and Analysis Center

DHS Traffic Light Protocol (TLP) 2.0 Chart

COLOR	WHEN SHOULD IT BE USED?	HOW MAY IT BE SHARED?
TLP:RED 🔴 ⚫ ⚫ Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only, no further.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER+STRICT ⚫ 🟡 ⚫ Limited disclosure, restricted to participants' and its organization.	Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization.	Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.
TLP:AMBER ⚫ 🟡 ⚫ Limited disclosure, restricted to participants' organization and its clients.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Note that TLP:AMBER+STRICT should be used to restrict sharing to the recipient organization only.	Recipients may share TLP:AMBER information with members of their own organization and its clients on a need-to-know basis to protect their organization and its clients and prevent further harm.
TLP:GREEN ⚫ ⚫ 🟢 Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.	Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. Unless otherwise specified, TLP:GREEN information may not be shared outside of the cybersecurity or cyber defense community.
TLP:CLEAR ⚪ ⚪ ⚪ Disclosure is not limited.	Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Recipients may share this information without restriction. Information is subject to standard copyright rules.

Agenda

Time (ET)	Topic
11:00	**Welcome** ➢ Why We're Here ➢ Expectations for This Community
11:05	**Auto-ISAC Update** ➢ Auto-ISAC Activities ➢ Heard Around the Community ➢ Intelligence Highlights
11:15	***DHS CISA Community Update*** ➢ **Jeff Terra, Consulting Support, Joint Cyber Defense Collaborative (JCDC), Cybersecurity and Infrastructure Security Agency (CISA)**
11:20	**Featured Speaker:** ➢ **Suzzanne Lightman, Senior Advisor, NIST; Nakia Grayson, IT Security Specialists, NIST** ➢ **Title: : NIST Auto Cybersecurity Community of Interest**
11:45	**Around the Room** ➢ Sharing Around the Virtual Room
11:55	**Closing Remarks**

Welcome - Auto-ISAC Community Call!

Purpose: These monthly Auto-ISAC Community Meetings are an opportunity for you, our Members & connected vehicle ecosystem Partners, to:

- ✓ ***Stay informed of Auto-ISAC activities***
- ✓ ***Share information on key vehicle cybersecurity topics***
- ✓ ***Learn about exciting initiatives within the automotive community from our featured speakers***

Participants: Auto-ISAC Members, Potential Members, Strategic Partners, Academia, Industry Stakeholders and Government – ***the whole of the automotive industry***

Classification Level: TLP:GREEN - May be shared within the Auto-ISAC Community and "off the record"

How to Connect: For further info, questions or to add other POCs to the invite, please contact us!

(sharmilakhadka@automotiveisac.com)

TLP:CLEAR

Engaging in the Auto-ISAC Community

AUTO-ISAC
Automotive Information Sharing and Analysis Center

❖ Join

- ❖ If your organization is eligible, apply for Auto-ISAC Membership
- ❖ If you aren’t eligible for Membership, connect with us as a Partner
- ❖ Get engaged – *“Cybersecurity is everyone’s responsibility!”*

❖ Participate

- ❖ Participate in monthly virtual conference calls (1st Wednesday of month)
- ❖ If you have a topic of interest, let us know!
- ❖ Engage & ask questions!

27
OEM Members

21
Navigator Partners

❖ Share – *“If you see something, say something!”*

- ❖ Submit threat intelligence or other relevant information
- ❖ Send us information on potential vulnerabilities
- ❖ Contribute incident reports and lessons learned
- ❖ Provide best practices around mitigation techniques

48 ***Supplier & Commercial Vehicle Members***

19
Innovator Partners

Membership represents **99%** ***of cars and trucks on the road in North America***

Coordination with **26** ***critical infrastructure ISACs through the National Council of ISACs (NCI)***

2023 Board of Directors

Thank you for your Leadership!

Josh Davis
Chair *of the*
Board of the Directors
Toyota

Kevin Tierney
Vice Chair *of the*
Board of the Directors
GM

Stephen Roberts
Secretary *of the*
Board of the Directors
Honda

Tim Geiger
Treasurer *of the*
Board of the Directors
Ford

Andreas Ebert
Chair *of the EuSC*
Volkswagen

Andrew Hillery
Chair *of the CAG*
Cummins

Ravi Puvvala
Chair *of the SAG*
Harman

Monica Mitchell
Polaris

Bob Kaster
Bosch

Brian Witten
Aptiv

AUTO-ISAC
Automotive Information Sharing and Analysis Center

TLP:CLEAR

Auto-ISAC Member Roster

As of April 1, 2023

Highlight = New Active Member

76 Members + 2 Pending

Aisin	Ferrari	LG Electronics	Panasonic (Ficosa-Affiliate)
Allison Transmission	Fleet Defender	Lucid Motors	Polaris
American Axle & Manufacturing	Flex	Luminar	Qualcomm
Aptiv	Ford	Magna	Renesas Electronics
AT&T	Garrett	MARELLI	Stellantis
AVL List GmbH	General Motors (Cruise-Affiliate)	Mazda	Subaru
Blackberry Limited	Geotab	Mercedes-Benz	Sumitomo Electric
BMW Group	Harman	Mitsubishi Electric	ThyssenKrupp
BorgWarner	Hitachi	Mitsubishi Motors	Tokai Rika
Bosch (ETAS-Affiliate)	Honda	Mobis	Toyota (Woven Planet-Affiliate)
Bose Automotive	Hyundai	Motional	Valeo
Canoo	Infineon	Navistar	Veoneer
ChargePoint	Intel	Nexteer Automotive Corp	Vitesco
CHN Industrial	John Deere Electronic	Nissan	Volkswagen
Continental (Argus-Affiliate)	JTEKT	Nuro	Volvo Cars
Cummins (Meritor-Affiliate)	Kia America, Inc.	Nuspire	Volvo Group
Denso	Knorr Bremse	NXP	Waymo
e:fs TechHub GmbH	KTM	Oshkosh Corp	Yamaha Motors
Faurecia	Lear	PACCAR	ZF

Pending: Micron, Rivian

AUTO-ISAC BUSINESS UPDATES AND EVENTS

**All times are in ET

Upcoming Meetings:

- **Community Call:**
  - **Wednesday, May 3rd– Time: *11:00am – 12:00 p.m.* TLP:GREEN; Speaker: Nalindrani Malimage, Cybersecurity Consultant, Burns and McDonnell**
  - **Title: *"Cybersecurity Challenges in the in Electric Vehicle Market"***

- **Auto-ISAC Member Advisory Forum (MAF) April 13th, 11:00 – 2:00 PM ET, *In person (Novi, MI) & Virtual***

- **Auto-ISAC Partner's Week Event May 22nd – May 26th 11-1 pm ET, *Virtual***

- **Auto-ISAC's first European Summit will be June 13th-14th, 2023 with June 12th having Members-only activities. https://automotiveisac.com/2023-europe-summit**

- **Auto-ISAC Summit will be Tuesday, October 17th-18th, 2023 in Redondo Beach, California. Registration information and complementary passes will be coming soon.**

AUTO-ISAC
Automotive Information Sharing and Analysis Center

TLP:CLEAR

Auto-ISAC Europe Cybersecurity Summit

12-14 June 2023 | The Peugeot Adventure Museum, Sochaux, France

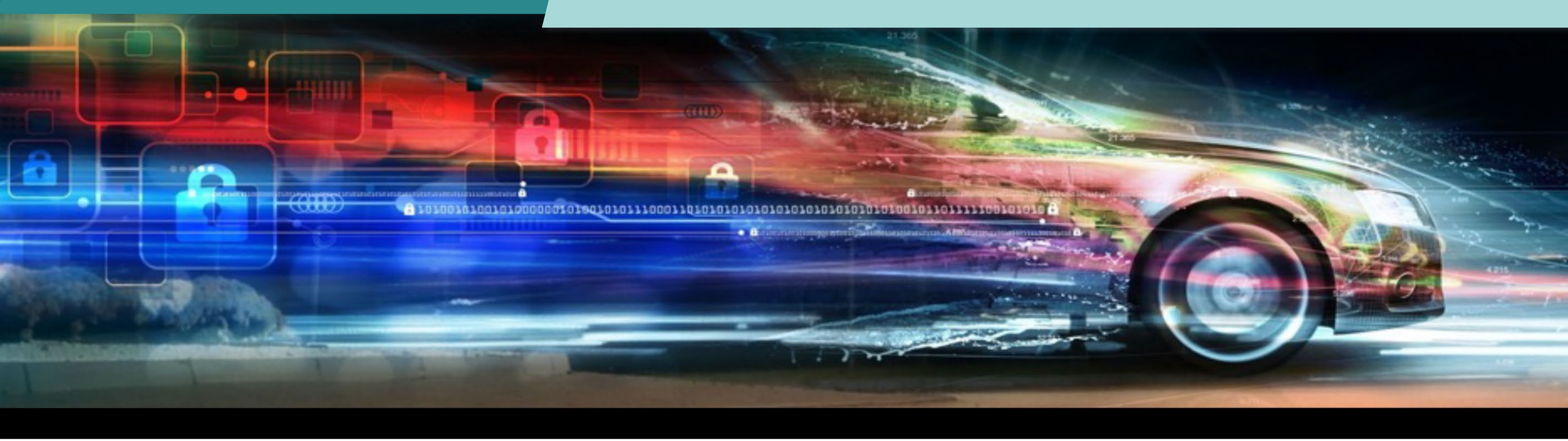
REGISTRATION IS LIMITED!

June 12 Members Only: TLP:AMBER
Monday, June 12: 11:00 – 20:00 CET

Open to Auto-ISAC Members only

June 13-14 Open to Public: TLP:CLEAR
Tuesday, June 13: 8:00 – 20:00 CET
Wednesday, June 14: 8:00 – 16:00 CET

Open to Auto-ISAC Members and External Partners



Auto-ISAC Intelligence Highlight

TLP:CLEAR

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Auto-ISAC Intelligence

- **Know what we track daily: subscribe to the DRIVEN; TLP:GREEN Auto-ISAC 2022 Threat Assessment released with Auto-ISAC Automotive Cyber Threat Ecosystem (1st Iteration) included.**
  - **Send feedback, contributions, or questions to analyst@automotiveisac.com**

- **Intelligence Notes**
  - **Geopolitical tensions involving Russia, China, North Korea, and Iran remain high with Russia-Ukraine in crisis. Threat of cyberattack spillover increases if: (1) the Russia-Ukraine war leads to kinetic clashes with the West (possible but unlikely), and (2) if any of the other hotspots escalate into crises (Russia-Ukraine, China [1], North Korea [2], Iran [3]).**
  - **Ransomware [4] Groups Targeting Automotive: AlphV/BlackCat, BianLian, Stormous, Everest, Snatch, Medusa, Black Basta, LockBit 3.0 [5] Royal, Cl0p, AvosLocker.**
  - **Multiple incidents of threat actors selling access to automotive organizations' stolen data. Notable Forums: Exploit, BreachForum (reportedly taken down by LE). Notable Dark Web Marketplace: MetaVerse Market (Dark Web Market Lists in Reddit here – use with caution)**
  - **Notable TTPs and Tools: Scan-V (The Guardian); Dbatloader/ModiLoader (ZScaler); GoBruteforcer (Unit42) Exploitation of Adobe ColdFusion (CISA); Microsoft Outlook Privilege Escalation via Email (Talos); Exploitation of GoAnywhere Zero-Day (Rubrik); Exploitation of High-Severity, LastPass-related Plex Vulnerability (BleepingComputer); Exploited CVEs Reportedly not in CISA KEV (VulnCheck).**

AUTO-ISAC COMMUNITY MEETING

Why Do We Feature Speakers?

- ❖ These calls are an opportunity for information exchange & learning
- ❖ Goal is to educate & provide awareness around cybersecurity for the *connected vehicle*

What Does it Mean to Be Featured?

- ❖ Perspectives across our ecosystem are shared from Members, government, academia, researchers, industry, associations and others.
- ❖ Goal is to showcase a rich & balanced variety of topics and viewpoints
- ❖ *Featured speakers are not endorsed by Auto-ISAC nor do the speakers speak on behalf of Auto-ISAC*

30+ ***Featured Speakers to date***

How Can I Be Featured?

- ❖ If you have a topic of interest you would like to share with the broader Auto-ISAC Community, then we encourage you to contact us!

7 ***Best Practice Guides available on website***

2000+ ***Community Participants***

TLP:CLEAR

CISA Resource Highlights

- Joint Cyber Defense Collaborative

JOINT CYBER DEFENSE COLLABORATIVE

Jeff Terra
4/4/2023

Supply Chain Attack Against 3CXDesktopApp

- CISA is aware of open-source reports describing a supply chain attack against 3CX software and their customers.
- According to the reports, 3CXDesktopApp — a voice and video conferencing app — was trojanized, potentially leading to multi-staged attacks against users employing the vulnerable app.
- CISA urges users and organizations to review the following reports for more information, and hunt for the listed indicators of compromise (IOCs) for potential malicious activity:

CrowdStrike: Falcon Platform Detects and Prevents Active Intrusion Campaign Targeting 3CXDesktopApp Customers

SentinelOne: SmoothOperator | Ongoing Campaign Trojanizes 3CXDesktopApp in Supply Chain Attack

DesktopApp: 3CX DesktopApp Security Alert

- Please note all information provided is TLP Amber

CISA and NSA Release Enduring Security Framework Guidance on Identity and Access Management

- As part of the Enduring Security Framework (ESF), the Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA) has released Identity and Access Management Recommended Best Practices Guide for Administrators.
- These recommended best practices provide system administrators with actionable recommendations to better secure their systems from threats to Identity and Access Management (IAM).
- IAM ensures that users only gain access to data when they have the appropriate credentials.

Untitled Goose Tool Aids Hunt and Incident Response in Azure, Azure Active Directory, and Microsoft 365 Environments

- CISA released the Untitled Goose Tool to help network defenders detect potentially malicious activity in Microsoft Azure, Azure Active Directory (AAD), and Microsoft 365 (M365) environments.

- The Untitled Goose Tool offers novel authentication and data gathering methods for network defenders to use as they interrogate and analyze their Microsoft cloud services.

- Goose, developed by CISA with Sandia National Laboratories, is available on the CISA GitHub Repository.

- Please note all information provided is TLP Amber

Security/Software Updates

As of March 1, 2023:

- Drupal Releases Security Update: Drupal Core
- CISCO Releases Security Advisories: Multiple products
- Samba Releases Security Updates: Multiple versions of Samba
- Apple Releases Security Updates: Multiple products
- Microsoft Releases Security Updates: Multiple products
- Mozilla Releases Security Updates: Firefox 111 and ESR 102.9 and Thunderbird 102.9
- Adobe Releases Security Updates: Multiple products
- Fortinet Releases Security Updates: Multiple products

- **Best practices:**
  - Leverage automatic updates for all operating systems and third-party software
  - Implement security configurations for all hardware and software assets
  - Remove unsupported or unauthorized hardware and software from systems

Please note all information provided is TLP Amber

CISA Releases Industrial Control Advisories

- These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS.
- CISA encourages users and administrators to review the newly released ICS advisories for technical details and mitigations
- Since 3/1/23 approximately 36 advisories have been issued
- The advisories span the following sectors: Information Technology, Critical Manufacturing, Energy and Multiple Sectors
- Cybersecurity Alerts & Advisories | CISA

Please note all information provided is TLP Amber

KEVs Catalogue

CISA strongly urges all organizations to reduce their exposure to cyberattacks by prioritizing timely remediation of Catalog vulnerabilities as part of their vulnerability management practice.

CISA added 19 new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog in the month of March. These types of vulnerabilities are a frequent attack vector for malicious cyber actors and pose significant risk to the federal enterprise.

Please note all information provided is TLP Amber

Additional Resources from CISA

- ❑CISA Homepage - https://www.cisa.gov/
- ❑CISA NCAS – https://cisa.gov/resources-tools/all-resources-tools
- ❑CISA Shields Up - https://www.cisa.gov/shields-up
- ❑Free Cybersecurity Services and Tools - https://www.cisa.gov/free-cybersecurity-services-and-tools
- ❑CISA News Room - https://www.cisa.gov/cisa/newsroom
- ❑CISA Blog - https://www.cisa.gov/blog-list
- ❑CISA Publications Library - https://www.cisa.gov/publications-library
- ❑CISA Cyber Resource Hub - https://www.cisa.gov/cyber-resource-hub
- ❑CISA Cybersecurity Directives - https://cyber.dhs.gov/directives/

JOINT CYBER DEFENSE
COLLABORATIVE

For more information:

cisa.gov

Questions?

Central@cisa.dhs.gov

1-888-282-0870

Jeff Terra
4/4/2023

Featured Speaker

TLP:CLEAR

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Suzanne Lightman

Senior Advisor, Computer Security, NIST

Suzanne Lightman is a Senior Advisor at the Computer Security Division of the Information Technology Lab at the National Institute of Standards and Technology (NIST). In that position, she serves as the main point for cybersecurity and transportation systems as well as cybersecurity of industrial systems.

Ms. Lightman has been involved with a diverse portfolio of topics including development of the NIST Cybersecurity Framework, cybersecurity in cyber-physical systems, identity management, IoT cybersecurity and cybersecurity & privacy policy. Her standards work includes automotive cybersecurity engineering (SAE/ISO 21434, ISO 24089) and industrial cybersecurity (IEC 62443).

Suzanne Lightman has two decades of experience in cybersecurity policy and implementation in positions all over the government, as well as in the private sector. She has held positions in both the legislative and executive branches which gives her a unique perspective on the development and implementation of government policy. In addition, she has worked on ethical hacking teams as well as led in-depth audits and reviews of cybersecurity.

Nakia Grayson

IT Security Specialist/Project Manager, NIST

Nakia Grayson is an IT Security Specialist/Project Manager who leads the Healthcare Sector & Supply Chain Assurance, and Autonomous Vehicle cybersecurity research project efforts at the National Cybersecurity Center of Excellence (NCCoE), which is part of the National Institute of Standards and Technology (NIST).

Ms. Grayson is also a part of the Privacy Engineering Program at NIST, where she supports the development of privacy risk management best practices, guidance, and communications efforts. She serves as the Contracting Officer Representative (COR) for NIST cybersecurity contracts.

Overview of NIST Auto-related Projects

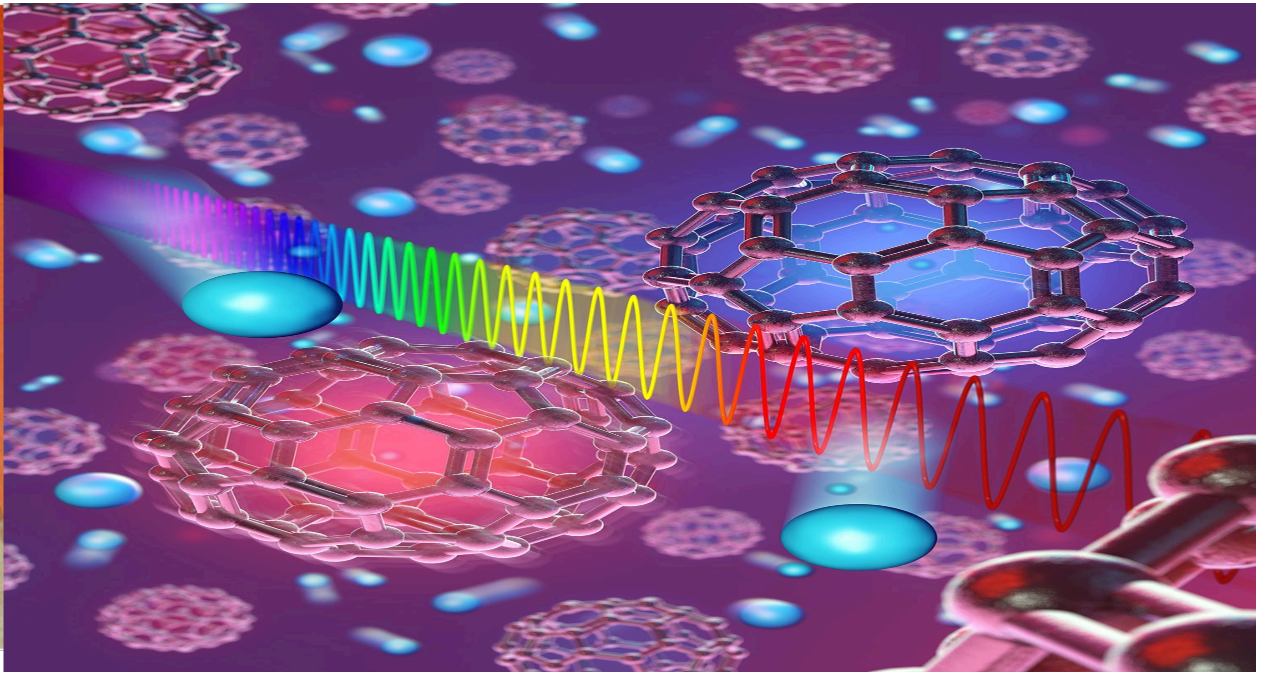
Suzanne Lightman

April 5, 2023

Auto –ISAC Monthly Community Call

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

STANDARD REFERENCE MATERIAL®
2387
Peanut Butter
www.nist.gov/srm
NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce



ABOUT US

NIST Mission

To promote U.S. innovation and industrial competitiveness by advancing *measurement science*, *standards*, and *technology* in ways that enhance economic security and improve our quality of life

List of NIST Projects

Automotive Cybersecurity Community of Interest (COI)

Automated Vehicle Effort

Cybersecurity Supply Chain Risk Management (C-SCRM)

Cryptographic Technologies: Quantum-Resistant Algorithms and Code Signing

Artificial Intelligence (AI) Risk Management Framework (RMF)

A Taxonomy of Attacks and Mitigations

Dipotra

Electric Vehicle (EV) Fast Charging Vehicle (XFC) Cybersecurity Framework Profile

Automotive Cybersecurity Community of Interest (AutoSec COI)

- Provide a communication channel to the industry for NIST work
- Allow industry participants to engage with NIST on work that they find relevant
- Assist NIST in identifying possible areas of work that would enhance the cybersecurity of vehicles and the transportation sector

COI Website Link: https://csrc.nist.gov/projects/auto-cybersecurity-coi

Procedures for NIST AutoSec COI

- Periodic webinars on NIST work of interest to the community
- Announcements of events and activities
- Updates on on-going projects

April AutoSec COI Call

Cherilyn Pascoe, Senior Technology Policy Advisor at NIST, will present on the Cybersecurity Framework 2.0.

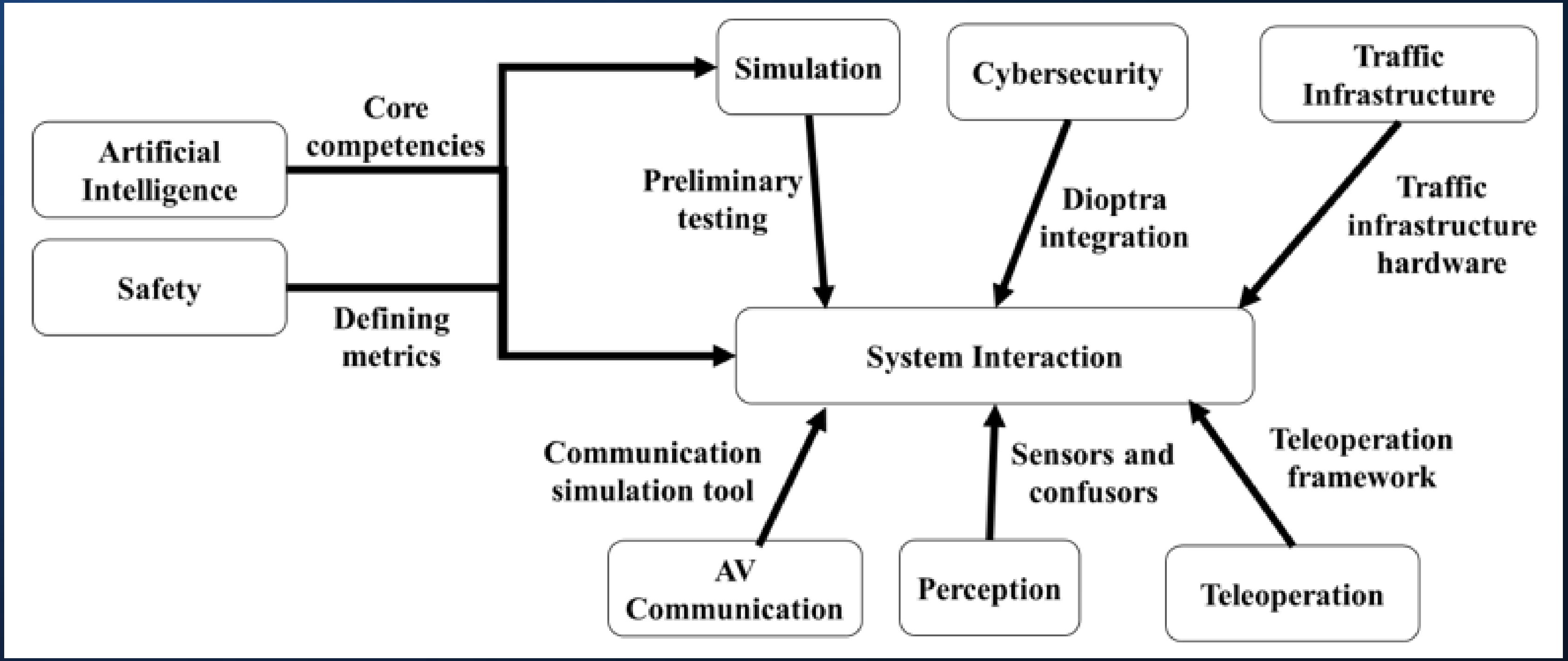
Cheri is leading the work at NIST for the first major update to the NIST CSF since its release in 2013.

NIST's Automated Vehicle Effort

Core Question: How Can NIST Advanced Standards and Support the Measurement of Automated Vehicles?

The NIST AV Program/Implementation Plan

- Developed a 44-page Program Plan for possible NIST AV focused efforts
- Specific efforts include:
  - Systems Interaction
  - Artificial Intelligence
  - Communications
  - Cybersecurity
  - Perception
  - Safety Quantification
  - Simulation
  - Teleoperation
  - Traffic Infrastructure



National Institute of
Standards and Technology
U.S. Department of Commerce

Cybersecurity Supply Chain Risk Management (C-SCRM)

Jon Boyens
Computer Security Division
IT Laboratory

C-SCRM Resources

- Draft SP 1800-34a/b/c: Validating the Integrity of Computing Devices (NCCoE Public-Private Collaboration)
- SP 800-161 Revision 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (May 2022)
  - Includes guidance stemming from EO 14028, e.g. SBOMs, OSS, Vulnerability Management, Enhanced Vendor Risk Assessments
- SP 800-218, *Secure Software Development Framework*. (February 2022)
- NISTIR 8276, *Key Practices in Cyber Supply Chain Risk Management* (February 2021)
- Integrate C-SCRM into other NIST guidance, e.g. NIST SPs 800-53r5 and 800-37r2, NIST Cybersecurity Framework
- Software and Supply Chain Assurance (SSCA) Forum: bringing industry, academia, and government together since 2003

CRYPTOGRAPHIC TECHNOLOGIES:

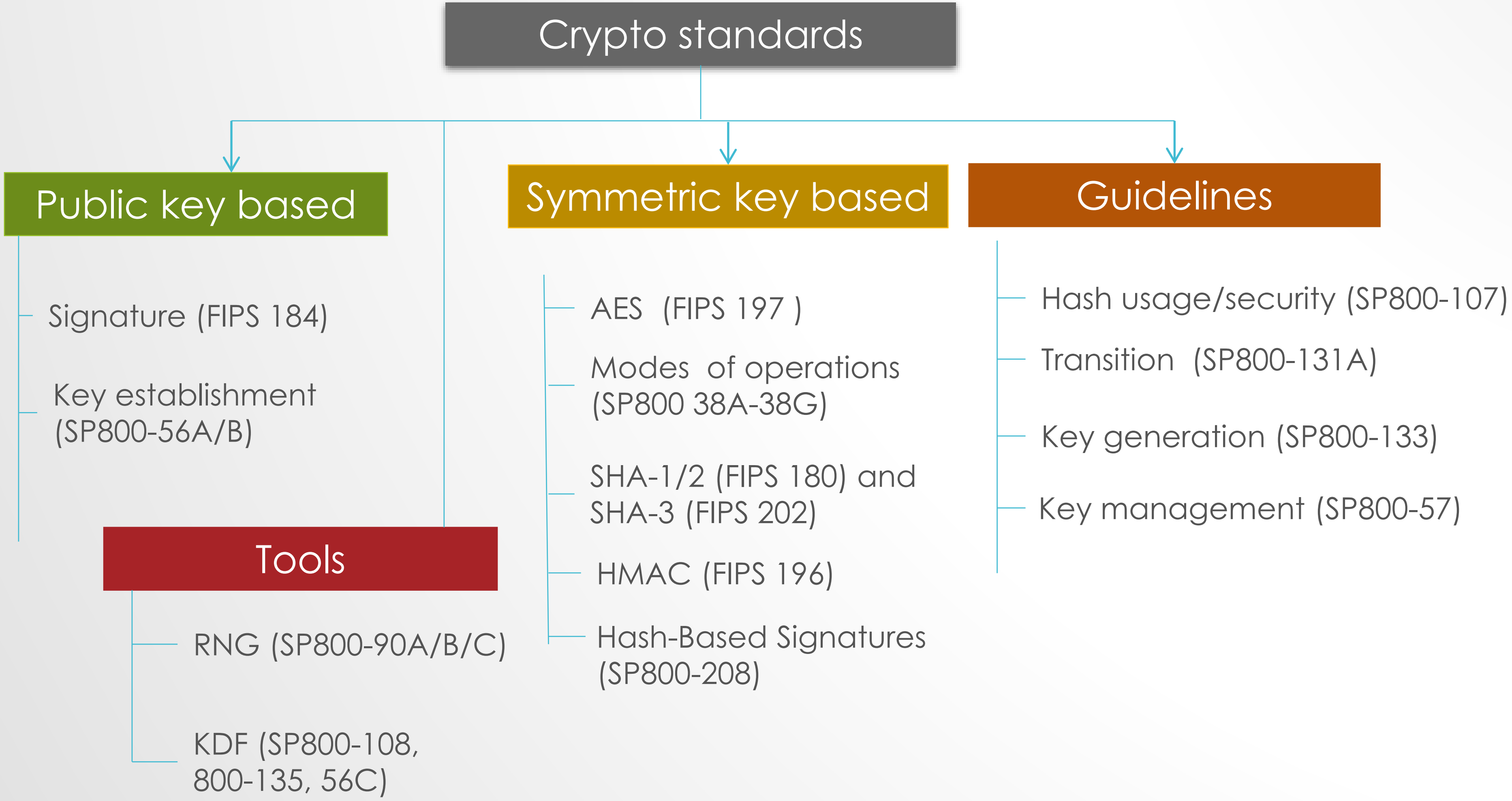
Quantum-Resistant Algorithms and Code Signing

Andrew Regenscheid
Cryptographic Technology Group

Murugiah Souppaya
Computer Security Division

National Institute of
Standards and Technology
U.S. Department of Commerce

CRYPTOGRAPHY STANDARDS



Crypto standards

Public key based

- Signature (FIPS 184)
- Key establishment (SP800-56A/B)

Tools

- RNG (SP800-90A/B/C)
- KDF (SP800-108, 800-135, 56C)

Symmetric key based

- AES (FIPS 197)
- Modes of operations (SP800 38A-38G)
- SHA-1/2 (FIPS 180) and SHA-3 (FIPS 202)
- HMAC (FIPS 196)
- Hash-Based Signatures (SP800-208)

Guidelines

- Hash usage/security (SP800-107)
- Transition (SP800-131A)
- Key generation (SP800-133)
- Key management (SP800-57)

PQC MIGRATION

- **National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems**
  - *"Mitigating the Risks to Encryption. … To mitigate this risk, the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by 2035."*
- NIST will provide transition guidelines to PQC standards
- NIST National Center of Cybersecurity Excellence *Migration to Post-Quantum Cryptography Project*

CODE SIGNING SYSTEMS

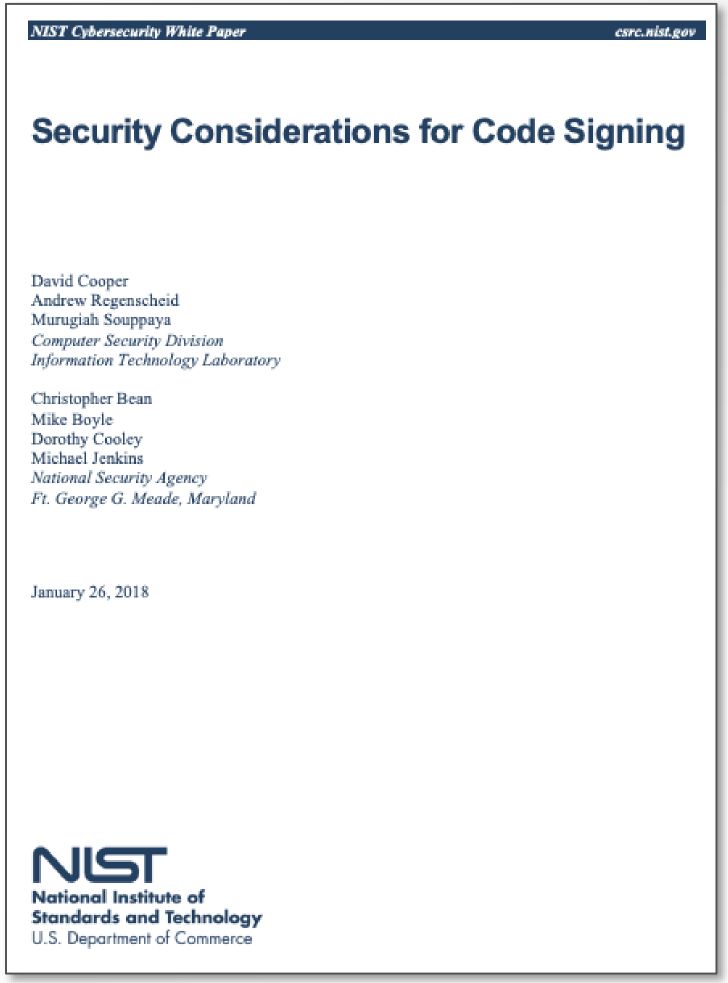
NIST Whitepaper:

Security Considerations for Code Signing

Topics:

- Code signing overview
- Architectures and use cases
- Description of roles
- Major Threats
- Recommended security practices

https://doi.org/10.6028/NIST.CSWP.01262018



NIST Cybersecurity White Paper *csrc.nist.gov*

Security Considerations for Code Signing

David Cooper
Andrew Regenscheid
Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

Christopher Bean
Mike Boyle
Dorothy Cooley
Michael Jenkins
National Security Agency
Ft. George G. Meade, Maryland

January 26, 2018

National Institute of
Standards and Technology
U.S. Department of Commerce

WRAP UP

Post-Quantum Cryptography

- Prepare for future migration to quantum-resistant cryptography
- Identify current algorithms/schemes used
- Assess suitability of emerging standards

Code Signing Systems

- Tailor guidelines for automotive use cases
- Software supply chain – code development through software updates

NIST Artificial Intelligence (AI) Risk Management Framework (RMF)

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

AI RMF

- Voluntary resource for designing, deploying and/or using AI systems
  - Facilitates the management of AI risks
  - Promotes trustworthy and responsible AI

AI RMF Website page:
https://www.nist.gov/itl/ai-risk-management-framework

Benefits of the AI Framework

Rights-preserving

Flexibly applied

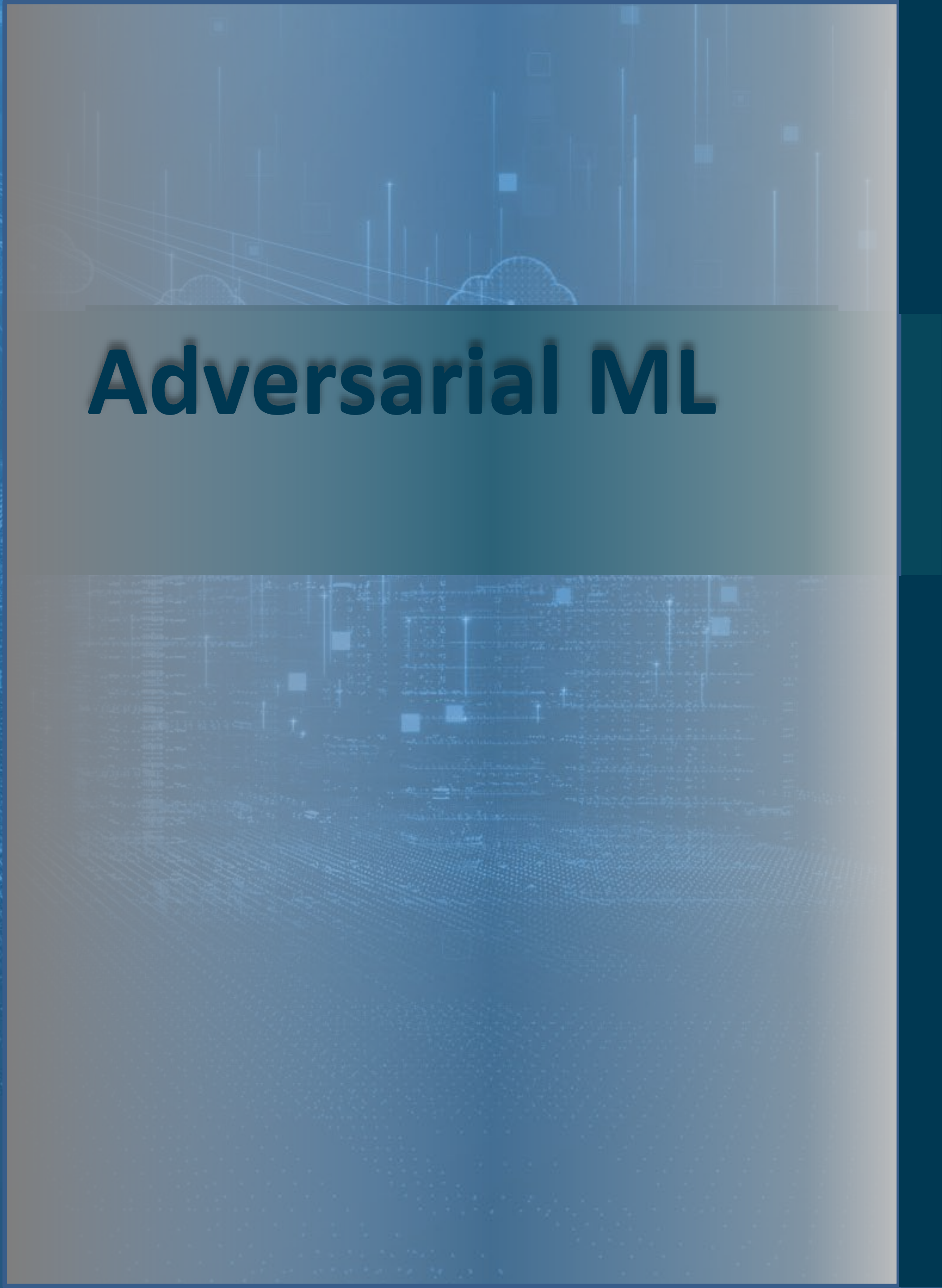
Measurable

A Taxonomy of Attacks and Mitigations

Apostol Vassilev

Computer Security Division

NIST INFORMATION TECHNOLOGY LABORATORY



Adversarial ML

Machine Learning
ATTACK TAXONOMY

Three main attacker goals/objectives:

- *Integrity violation*
- *Availability breakdown*
- *Privacy Compromise*

Goals require different attack surfaces/capabilities to exploit

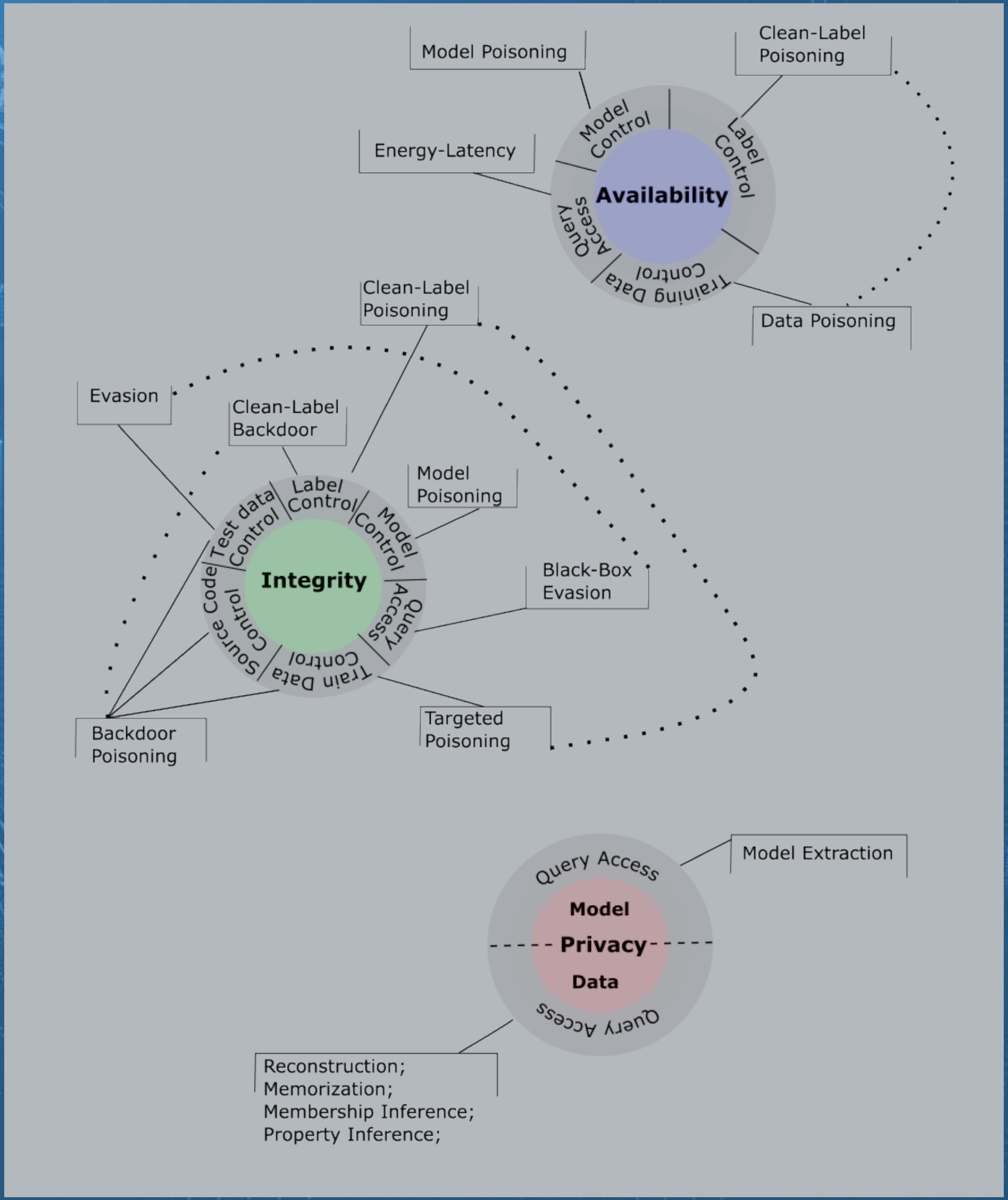
- *train data control,*
- *test data control,*
- *label control,*
- *source code control,*
- *model control,*
- *query access,*
- *etc.*

Multitude of attacks

- *each specialized for particular targets and attack surface*

ML models can be attacked at all stages of their lifecycle

- *from design to learning to deployment and use*



Model Poisoning

Clean-Label Poisoning

Energy-Latency

Model Control

Label Control

Availability

Query Access

Training Data Control

Data Poisoning

Clean-Label Poisoning

Evasion

Clean-Label Backdoor

Model Poisoning

Test data Control

Label Control

Model Control

Integrity

Query Access

Source Code Control

Train Data Control

Black-Box Evasion

Targeted Poisoning

Backdoor Poisoning

Query Access

Model

Privacy

Data

Query Access

Model Extraction

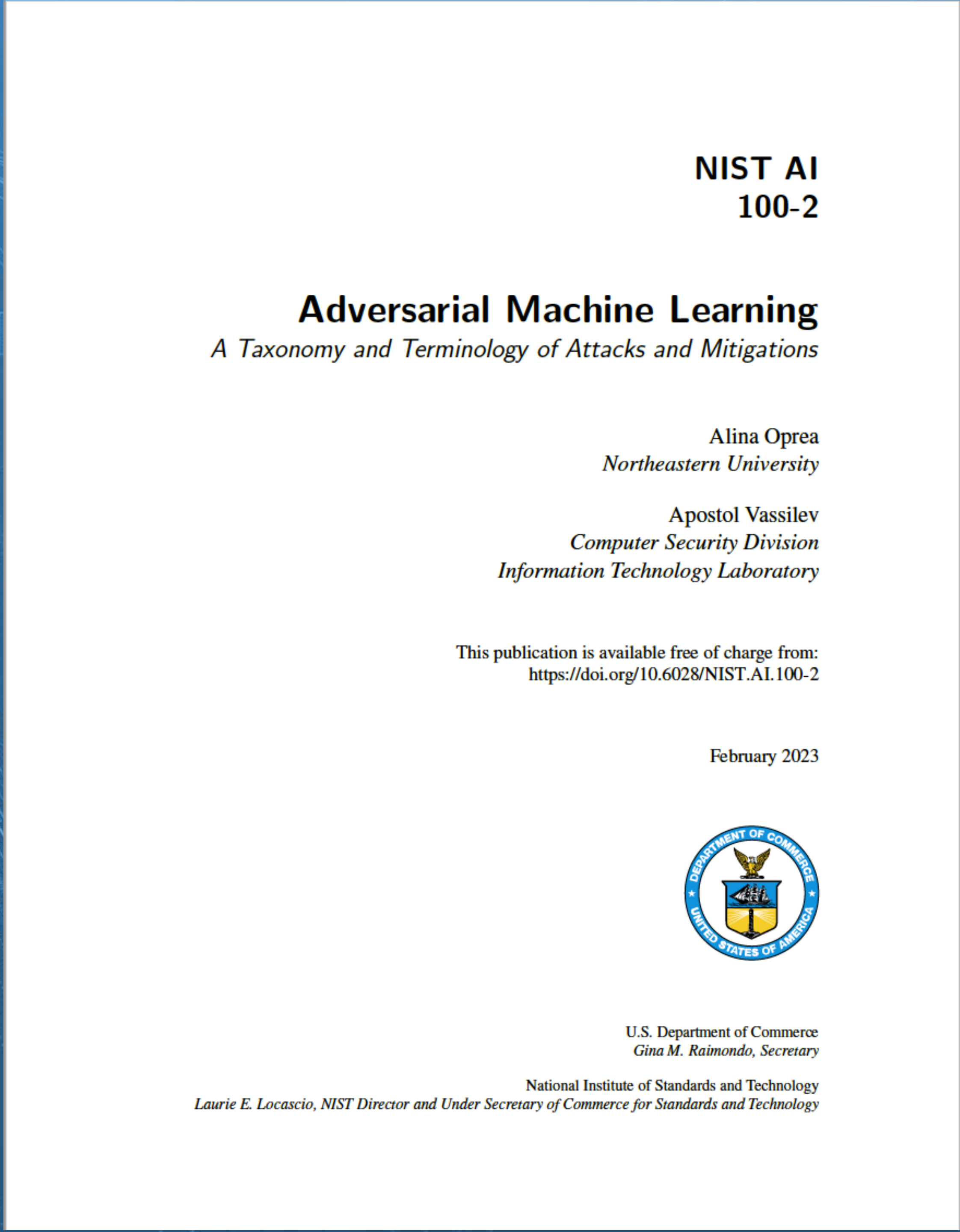
Reconstruction;
Memorization;
Membership Inference;
Property Inference;

Adversarial Machine Learning

A TAXONOMY OF ATTAKS AND MITIGATIONS

Coming soon to the NIST AI Resource Center

- *Joint effort with Prof. Alina Oprea*
- *Broad coverage, beyond automotive*
- *Replaces the old draft published in October 2019.*



NIST AI
100-2

Adversarial Machine Learning

A Taxonomy and Terminology of Attacks and Mitigations

Alina Oprea
Northeastern University

Apostol Vassilev
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.AI.100-2

February 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Dioptra

Test Platform for Machine Learning Systems

DIOPTRA IN A NUTSHELL

- Tool/application/testbed for creating, tracking and running machine learning experiments (jobs)
- Modular and extensible at both the architectural (microservices) and software (plugins) level

Flask

REST API

Software Development Kit (SDK)

Examples / Demos

docker

Docker Images

Built-in Task Plugins

Documentation

Repository:

https://github.com/usnistgov/dioptra

Questions: dioptra@nist.gov

Electric Vehicle (EV) Fast Charging Vehicle (XFC) Cybersecurity Framework Profile

Background & Purpose: The EV XFC infrastructure ecosystem relies on multiple connected subsystems including eXtreme Fast Charging, Electric Vehicle, XFC Cloud or Third-party Operator, and XFC and Utility-Building Networks. The U.S. Department of Energy's (DOE) Vehicle Technologies Office (VTO) and Office of Cybersecurity, Energy Security, and Emergency Response (CESER) have funded a collaborative project through the National Institute of Standards and Technology's (NIST) NCCoE to establish Cybersecurity Framework Profile for EV XFC infrastructure. The primary stakeholders initiating the effort include DOE, NIST, and the Electric Power Research Institute (EPRI). This effort will provide users with a national, risk-based approach to managing cybersecurity activities for EV XFC systems.

Ongoing activity:

- Meetings are held every Thursday from 2pm-3:30pm ET with the community to develop the Cybersecurity Framework Profile

How to participate and engage with us:

Join our community of interest by emailing us at Evxfc-nccoe@nist.gov

Website page:

https://www.nccoe.nist.gov/projects/cybersecurity-framework-profile-electric-vehicle-extreme-fast-charging-infrastructure

Open Discussion

Any questions about the Auto-ISAC or future topics for discussion?

How to Get Involved: Membership

If you are an OEM, supplier or commercial vehicle, Carrier or Fleet, please join the Auto-ISAC!

- *Real-time Intelligence Sharing*
- *Intelligence Summaries*
- *Regular intelligence meetings*
- *Crisis Notifications*
- *Member Contact Directory*
- *Development of Best Practice Guides*
- *Exchanges and Workshops*
- *Tabletop exercises*
- *Webinars and Presentations*
- *Annual Auto-ISAC Summit Event*

To learn more about Auto-ISAC Membership, please contact melissacromack@automotiveisac.com.
For Partnership, please contact sharmilakhadka@automotiveisac.com.

AUTO-ISAC PARTNERSHIP PROGRAMS

Strategic Partnership

- **For-profit** companies such as “Solutions Providers” that sell connected vehicle cybersecurity products & services.
- **Examples:** *Hacker ONE, Upstream, IOActive, Karamba, Grimm*

1. **Must be approved** by Executive Director and the Membership & Benefit Standing Committee (MBSC).
2. Formal agreements: **NDA, SPA, SoW, CoC** required.
3. **In-kind contributions** allowed. Currently no fee.
4. **Does not** overtly sell or promote product or service.
5. Commits to **support the Auto-ISAC’s mission.**
6. Engages with the automotive ecosystem, **supporting & educating Auto-ISAC Members and its Community.**
7. **Develops value added Partnership Projects** to engage with the Auto-ISAC, its Member, and Community.
8. **Summit Sponsorship** allowed for promotion. Summit Booth **priority**.
9. Engagement **must provide Member awareness, education, training, and information sharing**
10. **Builds relationships, shares, and participates** in information sharing Auto-ISAC activities.
11. Supports our mission through **educational webinars and sharing of information.**

Community Partnership

- **Community Partners** are companies, individuals, or organizations with a complementary mission to the Auto-ISAC, with the interest in engaging with the automotive ecosystem, supporting, and educating Members and the community.
- Includes ***Industry Associations, Government Partners, Academia, Research Institution, Standards Organizations, Non- Profit, Technical Experts, Auto-ISAC Sponsors*.**
- **Examples:** *Autos Innovate, ATA, ACEA, JAMA, MEMA,CLEPA, CISA, DHS, FBI, NHTSA, NCI, UDM etc.*

1. **No formal agreement** required.
2. **No approval** required.
3. Added to **Auto-ISAC Community Distro** List to stay engaged in Community events and activities.
4. Participate in **Auto-ISAC Monthly Community Calls.**
5. Learn **what is trending** in the ISACs and hear from key leaders during the **special topic of interest** presentation.
6. Added to **Auto-ISAC DRIVEN** list to receive our **daily cyber automotive newsletter.**
7. Part of the Network with **Automotive Community and the extended automotive ecosystem.**
8. Invitation to **attend and support** our yearly Summit.

Current Partnerships

Many organizations engaging

Thanks for your Support to our Many Partners

Community Partners

INNOVATOR

Strategic Partnership (19)

ArmorText

BlockHarbor
Cybellum
Deloitte
FEV
GRIMM
HackerOne
Irdeto
Itemis
Karamba Security
KELA
Pen Testing Partners
Red Balloon Security
Regulus Cyber
Saferide
Security Scorecard
Trustonic
Upstream
Vultara

NAVIGATOR

Support Partnership

AAA
ACEA
ACM
American Trucking Associations (ATA)
ASC
ATIS
Auto Alliance
EMA
Global Automakers
IARA
IIC
JAMA
MEMA
NADA
NAFA
NMFTA
RVIA
SAE
TIA
Transport Canada

COLLABORATOR

Coordination Partnership

AUTOSAR
Billington Cybersecurity
Cal-CSIC
Computest
Cyber Truck Challenge
DHS CSVI
DHS HQ
DOT-PIF
FASTR
FBI
GAO
ISAO
Macomb Business/MADCAT
Merit (training, np)
MITRE
National White Collar Crime Center
NCFTA
NDIA
NHTSA
NIST
Northern California Regional Intelligence Center (NCRIC)
NTIA
OASIS
ODNI
Ohio Turnpike & Infrastructure Commission
SANS
The University of Warwick
TSA
University of Tulsa
USSC
VOLPE
W3C/MIT
Walsh College

BENEFACTOR

Sponsorship Partnership

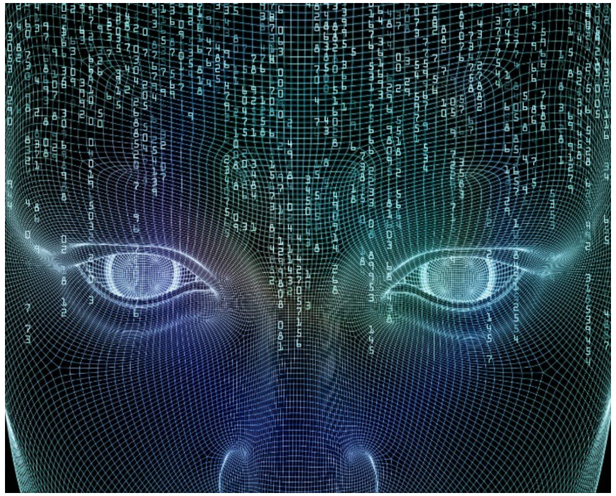
2022 Summit Sponsors-
Argus
BGNetworks
Bosch
Blackberry
Block Harbor
BlueVoyant
Booz Allen Hamilton
C2A
Cybellum
CyberGRX
Cyware
Deloitte
Denso
Finite State
Fortress
Itemis
Keysight Technologies
Micron
NXP
Okta
Sandia
Securonix
Tanium
UL
Upstream
VicOne

AUTO-ISAC
Automotive Information Sharing and Analysis Center

TLP:CLEAR

AUTO-ISAC BENEFITS

- Focused Intelligence Information/Briefings
- Cybersecurity intelligence sharing
- Vulnerability resolution
- Member to Member Sharing
- Distribute Information Gathering Costs across the Sector
- Non-attribution and Anonymity of Submissions
- Information source for the entire organization
- Risk mitigation for automotive industry
- Comparative advantage in risk mitigation
- Security and Resiliency



Building Resiliency Across the Auto Industry

Thank You!

SALAMAT
JUSPAXAR
OBRIGADO
MATONDO
KIITOS
KIA ORA
MULTUMESC
MAAKE
MOCHCHAKKERAM
TERMA KASIH
RAIBH MAITH AGAT
CHOKRANE
SALAMAT
CAM ON BAN
GRAZIE
MULTUMESC
MERCI
RAIBH MAITH AGAT
MERCI
MERCI
OBRIGADO
MOCHCHAKKERAM
MOCHCHAKKERAM
GRAZIE
THANK
ASANTE
CHOKRANE
UA TSAUG RAU KOJ
MATUR NUWUN
MOCHCHAKKERAM
MATONDO
WELALIN
YOU
KIITOS
CHOKRANE
UA TSAUG RAU KOJ
DANK JE
OBRIGADO
DANK JE
RAIBH MAITH AGAT
SPASIBO
SPASIBO
VINAKA
NIRRINGRAZZJAK
MAMANA
MAAKE
ARIGATO
KIITOS
MULTUMESC
DANKON
OBRIGADO
MOCHCHAKKERAM
NIRRINGRAZZJAK
MOCHCHAKKERAM
OBRIGADO
SPASIBO

Our Contact Info

Faye Francy
Executive Director

20 F Street NW, Suite 700
Washington, DC 20001
703-861-5417
fayefrancy@automotiveisac.com

Sharmila Khadka
Information Technology Executive
Coordinator

20 F Street NW, Suite 700
Washington, DC 20001
443-962-5663
sharmilakhadka@automotiveisac.com

AUTO-ISAC
Automotive Information Sharing and Analysis Center

www.automotiveisac.com
@auto-ISAC