Introductory Webinar
NIST Automotive Cybersecurity Community of Interest

February 7, 2023

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

Agenda

- Introduction and the AutoSec COI

  Suzanne Lightman
- NIST AV Project

  Craig Schlenoff
- Supply Chain Project

  Jon Boyens
- Code Signing NISTIR and Post-Quantum Cryptography

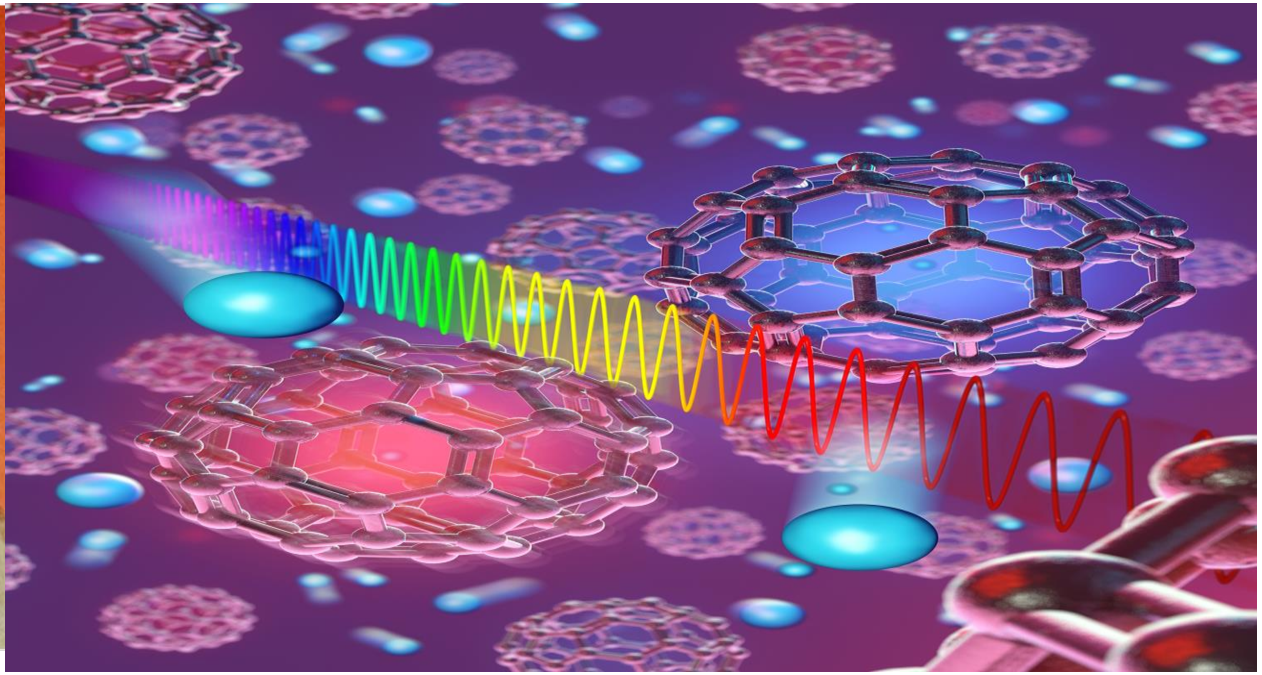
  Andrew Regenscheid
- NIST AI Project

  Elham Tabassi
- AI Attack Taxonomy

  Apostol Vassilev
- Dioptra

  Harold Booth
- EVSE Project

  James McCarthy



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

NIST INFORMATION TECHNOLOGY LABORATORY

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

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

NIST's Automated Vehicle Effort

2/07/2023

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

Scope and Process (FY22)

- Scope The Effort:
  - Focus on on-road (e.g., personal vehicles, long-haul trucking, service vehicles such as Uber/Lyft) automated vehicles
- Don't Step on Other's Toes:
  - Landscape document lists and describes major AV efforts in other Federal agencies
- Leverage NIST's Strengths:
  - NIST AV efforts document lists and describes NIST AV efforts broken down into AI, cybersecurity, communications, perception, and safety
- Hear From Our Stakeholders!

Department	Proposed areas of collaboration
US DOT/NHTSA	• Assistance with SRI development for sensors • Safety-related measures development • Cybersecurity metrics and measurement • Communication system evaluation • AI/ML implementation and measurement • Provision of additional expertise
NSF	• Assistance with tech transfer • Publicizing NSF-supported research by integration with NIST work
DHS	• Provide expertise
GSA	• Assistance with operational guidelines
DOD	• Provide expertise • Collaborative research in relevant areas ○ AI/ML ○ Supply chain ○ Cybersecurity measures ○ Workforce

SERI FY 2022 – Autonomous Vehicle Measurement Science, Standards, and Test Methods Program Ongoing Efforts at NIST

Milestone task: Map recommended efforts in on-road autonomous vehicles to existing NIST efforts to identify opportunity areas as well as existing areas that are not of high priority to our stakeholders.

Approach: Compare the challenges/opportunities uncovered at the NIST workshop with existing autonomous vehicle efforts at NIST.

Purpose

This document summarizes key priority areas from our stakeholders in the development of on-road autonomous vehicles (referred to as AVs throughout this document), as extracted from Deliverable #3. This document then maps ongoing NIST efforts in on-road autonomous vehicles with respect to the key priorities identified by our stakeholders.

Identification of high priority areas to our stakeholders

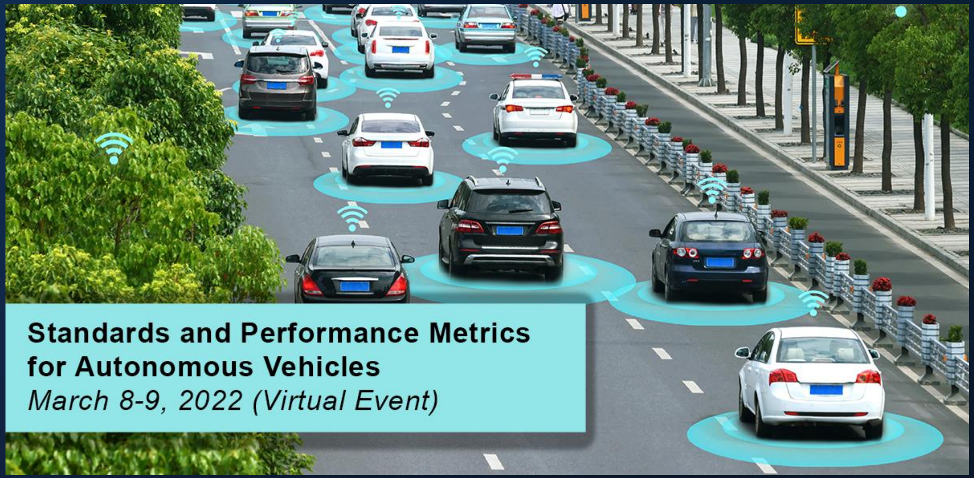
During the workshop, focus groups, and individual interviews conducted by NIST, the following five areas were highlighted by several stakeholders: a) Artificial Intelligence (AI), b) Cybersecurity, c) Communication, d) Sensor Perception, and e) Safety. The topics of high priority areas to address in AVs that were highlighted by the participants are listed below:

1. **Artificial Intelligence:**
   a. Gaps in standards and metrology (including tests) for trustworthy AI for AVs, including:
      i. Accuracy: This trustworthiness attribute captures the broad notion of whether the machine learning model is correctly capturing a relationship that exists within training data. False positive and false negative rates are often used to measure (aggregate) accuracy for tasks such as recognition, detection, or estimation. There is a need to measure the likelihood of failures and their system-level vehicle and driving environment impact.

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

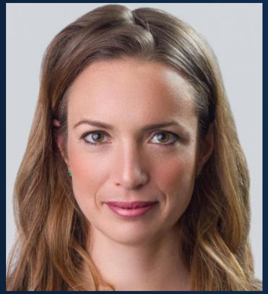
To answer this question, NIST conducted the following:

- Conducted 65 one-on-one stakeholder interviews
- Facilitated 4 focus group meetings with 36 domain experts
- Hosted an automated vehicles workshop (811 attendees)
  - Workshop web site: https://www.nist.gov/news-events/events/2022/03/standards-and-performance-metrics-road-autonomous-vehicles
  - Workshop report: https://www.nist.gov/system/files/documents/noindex/2022/05/24/AV%20Workshop%20Summary_Draft.pdf



Workshop Speakers and Attendees

Kyle Davis and Andrew Beasley
Biden-Appointed Strategic Policy Fellows
Office of Science and Technology Policy



Nellie Abernathy
Director
Office of Policy and Strategic Planning
Department of Commerce

Tim Kurth
Chief Counsel (R)
Commerce of the House Committee on Energy & Commerce

Robyn Robertson
President & CEO of Traffic Injury Research Foundation

Edward Straub
Executive Director of Automated Vehicle Safety Consortium
SAE

Jack Weast
CTO, Corporate Strategy Office
Intel

Bert Kaufman
Head of Public Policy and Regulatory Affairs
Zoox

Scott McCormick
President
Teleoperation Consortium

Hussein Mehanna
Vice President of AI/ML
Cruise

Alberto Lacaze
CEO
Robotic Research

Dr. Trent Victor
Director of Safety Research and Best Practices
Waymo

Katherine McClaskey
Program Lead for Advanced Threats Security
CISA

Dr. Adam Campbell
Senior Manager Safety Innovation and Impact
Gatik AI

Organizations

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

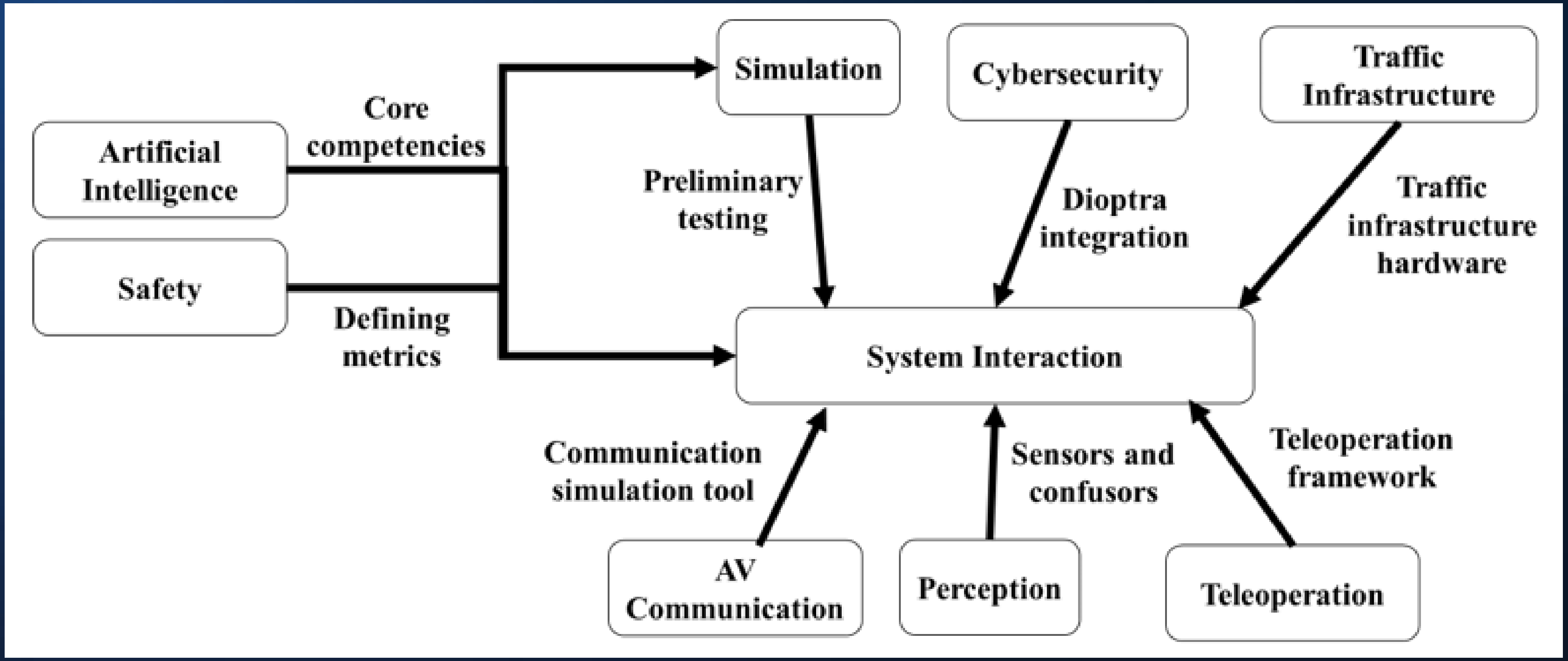
Not within NIST scope
Within NIST scope and expertise/infrastructure is lacking (NIST can support agencies)
Within NIST scope and expertise/infrastructure is available

What did stakeholders request that NIST can help with?

- Create and enforce a baseline for AV safety systems testing
- Enforce sensor specs that should be used in AVs
- Create regulation on periodic testing and updating
- Define the data that should be **measured** before, during, and after operation of automated vehicles
- Provide **reference materials** for what infrastructure investment state and local governments should invest in
- Collect **standardized** data from the DoT from accidents to develop representative testing environments
- Provide classification and levels for AV components
- Develop novel individual and fused sensor **measurement science** solutions for vehicles
- Help define **testing** guidance for stakeholders to meet regulatory agency requirements
- Develop mitigation **standards** for adversarial AI
- Develop AV simulation-based **measurement science**
- Advance **standards** with SAE, 3GP, and Teleoperation Consortium
- Develop **measurement science** for traffic infrastructure that can support AVs
- Develop **metrics** to identify what aspects of AVs should be measured to ensure safety
- Create **test models** and **measurement science** for AV communications
- Foster a community of stakeholders to agree on common **taxonomies** and **standards**
- Be a one-stop-shop for pointers to relevant autonomous vehicle **standards**
- **Measure** how different parts of an AV work together
- "Do you know that NIST cybersecurity framework? Just do that for autonomous 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



NIST Strategic and Emerging Research Initiatives (SERI) Project
October 2022 – September 2024

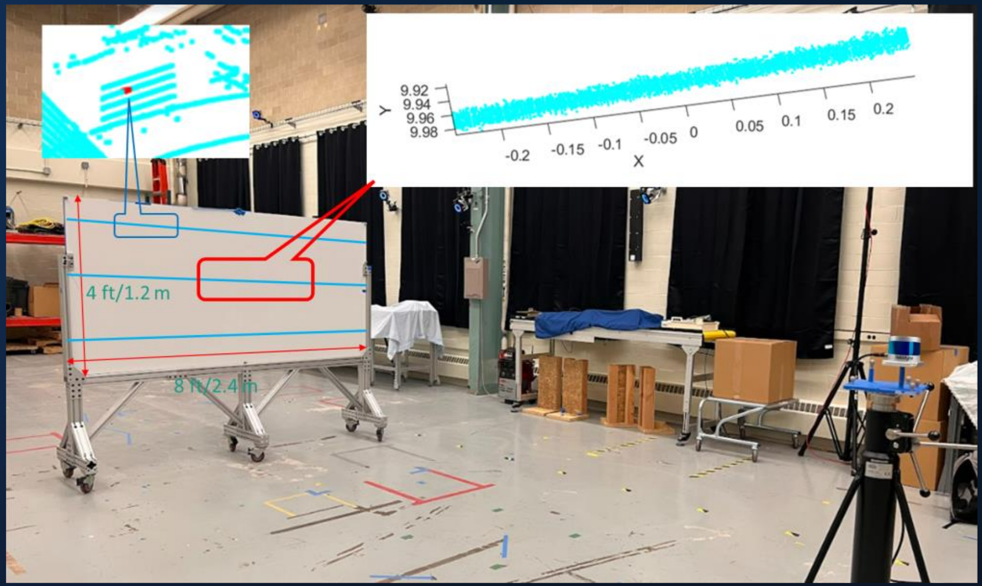
System Level Testing

a) **Assessing Automotive Sensor Perception**
Develop a sensor testbed facility that stakeholders can use for characterization of their automotive sensors.

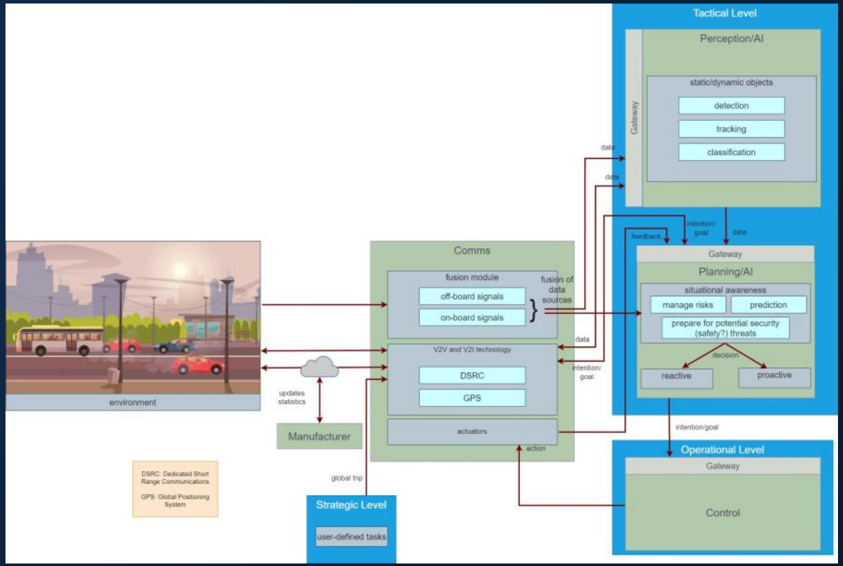
b) **Minimizing Risk in AI**
Develop a simulation testbed for testing and minimizing risk for AI algorithms used in on-road automated vehicles.

c) **Measuring Cybersecurity**
Develop a testbed for measuring adversarial machine learning and defensive mitigations.

d) **Evaluating Communication Technologies**
Develop a simulation tool for stakeholders to validate testing methods that assess vehicle communications

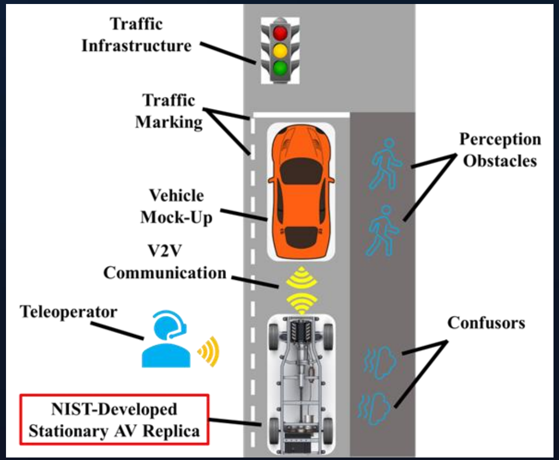


NIST Strategic and Emerging Research Initiatives (SERI) Project
October 2022 – September 2024



Complete Vehicle Behavior Based on System Interaction

- Develop a testbed to evaluate system interaction in automated vehicles in a subset of SAE's behavioral competencies.
  - Maintaining a lane
  - Changing lanes
  - Navigating intersection
  - Navigating unstructured roadways
  - Navigating parking
  - Responding to other vehicles
- Perturb the system at points and determine the effect on the overall AV performance. For example:
  - Degrade communications between the test vehicle and the environment
  - Simulate a cybersecurity attack on some portion of the system
  - Introduce compromised sensor input
- Planning a workshop for the September 2023 timeframe to discuss progress.



Testing Approach

Simulation

Structured Environment

Test Track

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

Join our Google Group to stay up to date!

Email autonomousvehicles+subscribe@list.nist.gov from the email address that you would like to have added to the mailing list

OR

Go to https://groups.google.com/a/list.nist.gov/g/autonomousvehicles and click the "Ask To Join" button

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

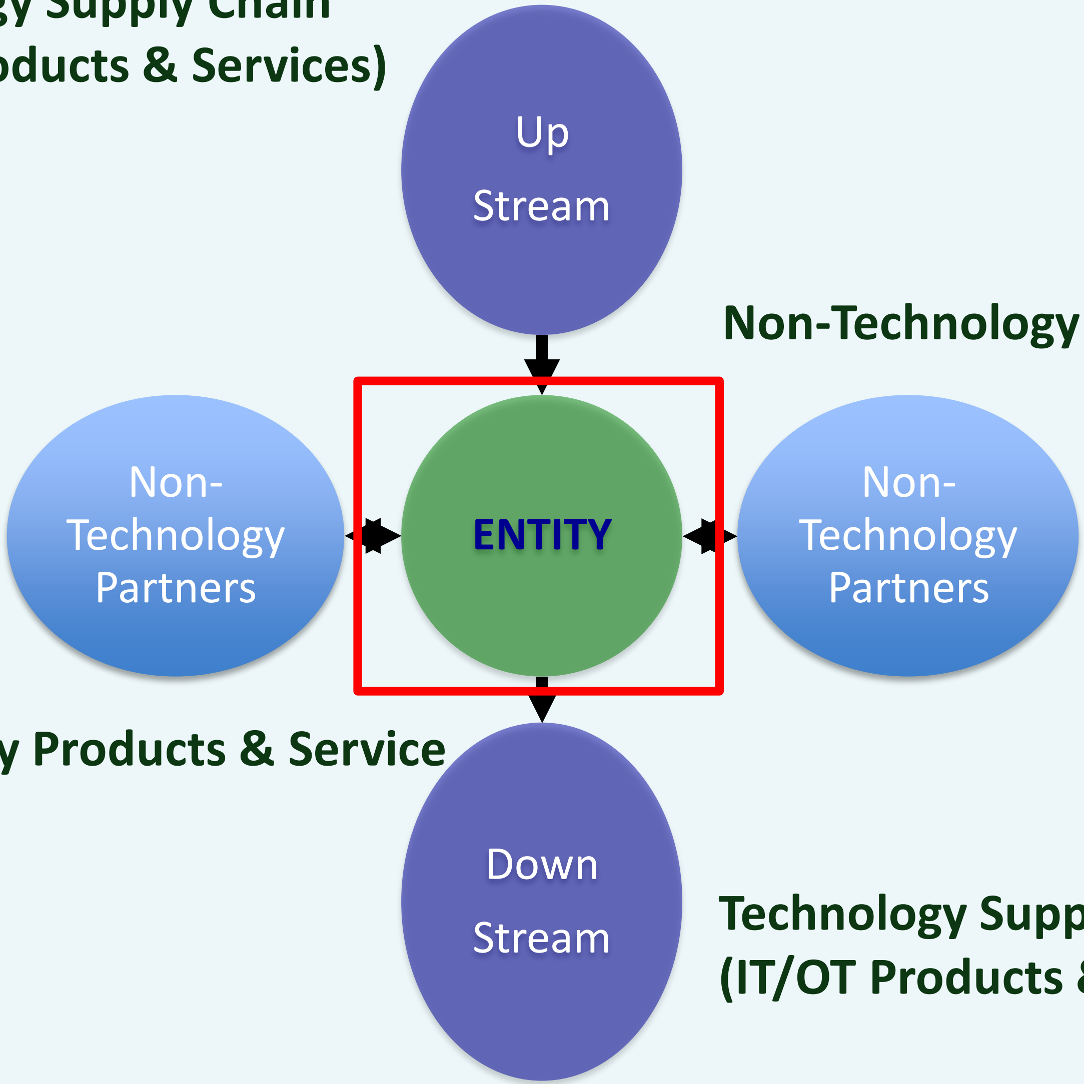
Technology and Non-Technology Dependencies

TRUST
-Organization
-Process
-Products/Service

Technology Supply Chain
(IT/OT Products & Services)

But Verify
-Due Diligence
-Standards/Audits
-Testing

Non-Technology Products & Service



Non-Technology Products & Service

Technology Supply Chain
(IT/OT Products & Services)

Cybersecurity Risks in Supply Chains

- Counterfeit products
- Hardware or software delivered with vulnerabilities, malware or inserted post-delivery
- Third and Nth Party - Vulnerabilities in systems and networks used by supply chain partners
- Insider Threat (including non-adversarial)
- Poor quality manufacturing, development, maintenance, or disposal practices
- Cybersecurity risks in NON-technology products and services

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

EO 14028 Section 4 Tasks and Timelines

Day 0 – May 12, 2021
EO 14028 issued

Day 30 – June 11, 2021
Solicit input from stakeholders (4b)

Day 45 – June 26, 2021
Publish definition of “critical software” (4g)

Day 60 – July 11, 2021
Publish guidance outlining security measures for critical software (4i)
Publish guidelines recommending minimum standards for vendor testing of SW source code (4r)

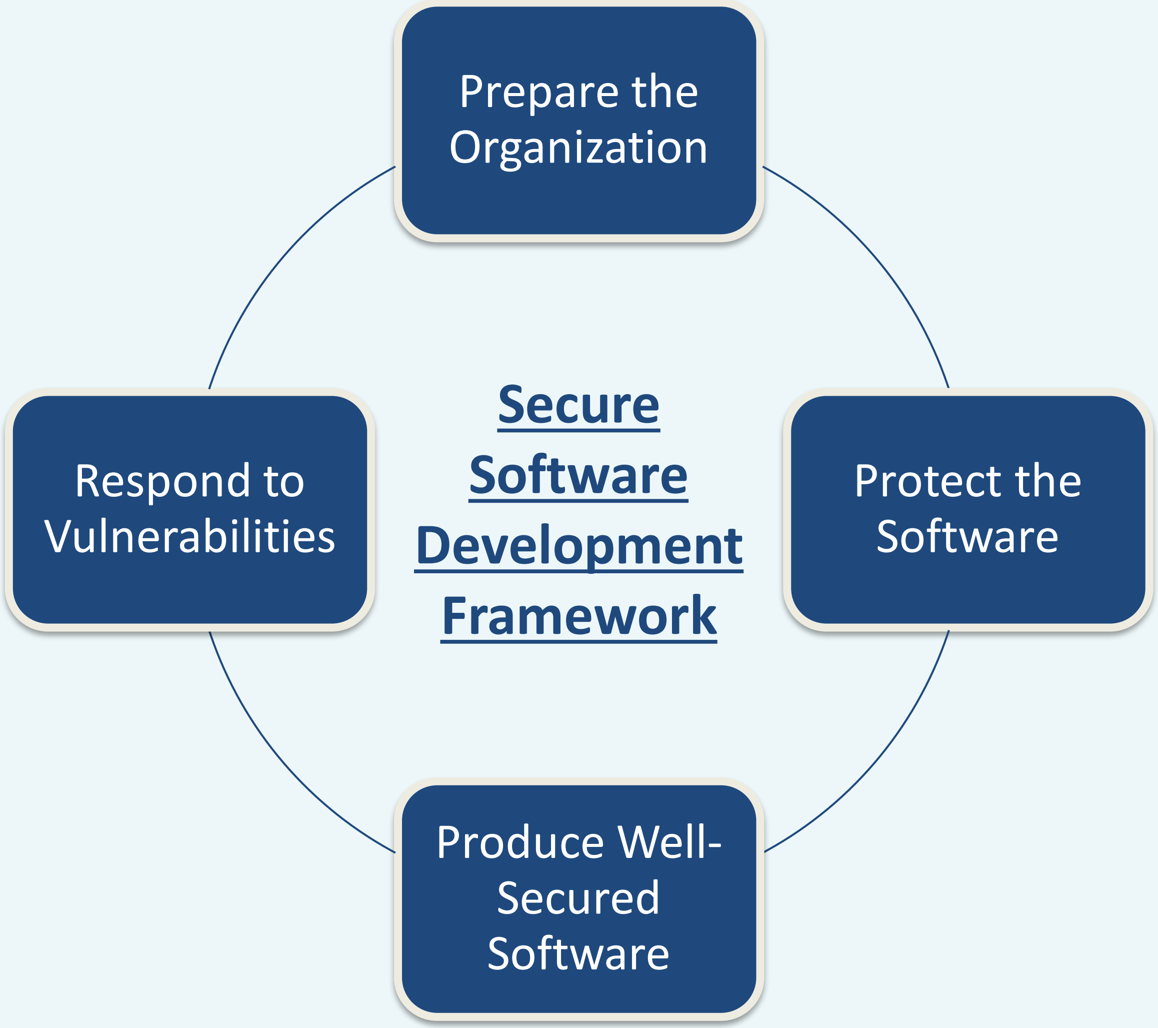
Day 180 – Nov 8, 2021
Publish preliminary guidelines for enhancing SW SC security (4c)

Day 270 – Feb 6, 2022
Issue guidance identifying practices that enhance security of SW SC (4e)
Initiate pilot programs, identifying IoT cyber & secure SW development practices or criteria for consumer labeling programs (4s, 4t, 4u)

Day 360 – May 8, 2022
Publish additional guidelines, including review/update procedures (4d)

Day 365 – May 13, 2022
Review & submit summary report of pilot programs (4w)

NIST SP 800-218, Secure Software Development Framework (SSDF) Practice Groups



Elements of an SSDF Practice

Practices	Tasks	Notional Implementation Examples	References
Identify and Confirm Vulnerabilities on an Ongoing Basis (RV.1): Help ensure that vulnerabilities are identified more quickly so that they can be remediated more quickly in accordance with risk, reducing the window of opportunity for attackers.	**RV.1.1**: Gather information from software acquirers, users, and public sources on potential vulnerabilities in the software and third-party components that the software uses, and investigate all credible reports.	**Example 1**: Monitor vulnerability databases[9], security mailing lists, and other sources of vulnerability reports through manual or automated means. **Example 2**: Use threat intelligence sources to better understand how vulnerabilities in general are being exploited. **Example 3**: Automatically review provenance and software composition data for all software components to identify any new vulnerabilities they have.	**BSAFSS**: VM.1-3, VM.3 **BSIMM**: AM1.5, CMVM1.2, CMVM2.1, CMVM3.4, CMVM3.7 **CNCFSSCP**: Securing Materials—Verification **EO14028**: 4e(iv), 4e(vi), 4e(viii), 4e(ix) **IEC62443**: DM-1, DM-2, DM-3 **ISO29147**: 6.2.1, 6.2.2, 6.2.4, 6.3, 6.5 **ISO30111**: 7.1.3 **OWASPSAMM**: IM1-A, IM2-B, EH1-B **OWASPSCVS**: 4 **PCISSLC**: 3.4, 4.1, 9.1 **SCAGILE**: Operational Security Task 5 **SCFPSSD**: Vulnerability Response and Disclosure **SCTPC**: MONITOR1 **SP80053**: SA-10, SR-3, SR-4 **SP800161**: SA-10, SR-3, SR-4 **SP800181**: K0009, K0038, K0040, K0070, K0161, K0362; S0078

Task: An individual action (or actions) needed to accomplish a practice

Implementation Example: An example of a type of tool, process, or other method that could be used to implement this task

Reference: An established secure development practice document and its mappings to this task

Secure Software Attestation Guidance

- The EO directs NIST to issue guidance identifying practices that enhance the security of the software supply chain for producers and purchasers and then directs OMB to require federal agencies to comply with NIST guidelines with respect to software procured after the date of the order. NIST has guidance for attesting to conformity with SSDF and related guidance.

1. Use the SSDF terminology

Enables all software producers to use the same lexicon when attesting to conformity for federal agencies

2. Require attestation

Focus on processes and procedures vs. how things were done for a specific release

3. Accept first-party attestation

First party-attestation is recommended, depending on the risk

4. Request high-level artifacts.

Producer should be able to trace the practices summarized in high-level artifacts to low-level artifacts

SP 800-161 Revision 1, Appendix F
EO 14028 Sections 4(c)/(d) Response
Guidance for Software Supply Chain Security

Software supply chain security concepts are a critical sub-discipline within C-SCRM

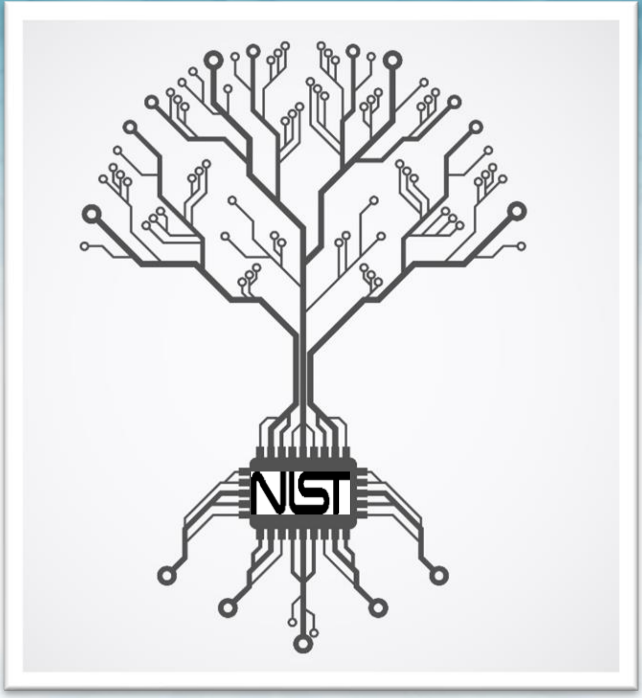
Available online to allow for update to guidance.

EO through the lens of 800-161

- EO Critical Software & Measures
- Software Verification
- SSDF & Attestations

Emerging Concepts

- Software Bill of Materials (SBOM)
- Enhanced Vendor Risk Assessments
- Open Source Software Controls
- Vulnerability Management



Email: scrm-nist@nist.gov

Visit: http://scrm.nist.gov

CRYPTOGRAPHIC TECHNOLOGIES:

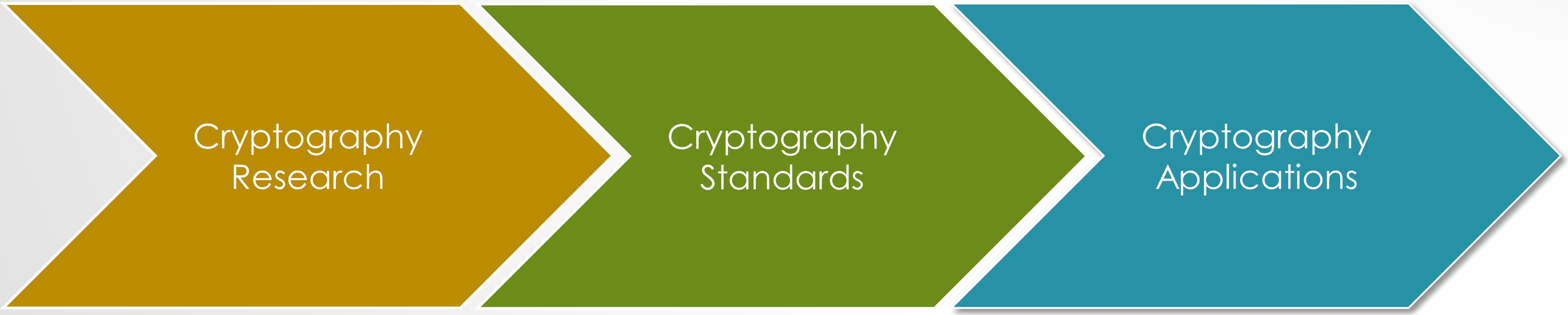
Quantum-Resistant Algorithms and Code Signing

Andrew Regenscheid
Cryptographic Technology Group

Murugiah Souppaya
Computer Security Division

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

NIST CRYPTOGRAPHY PROGRAM



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

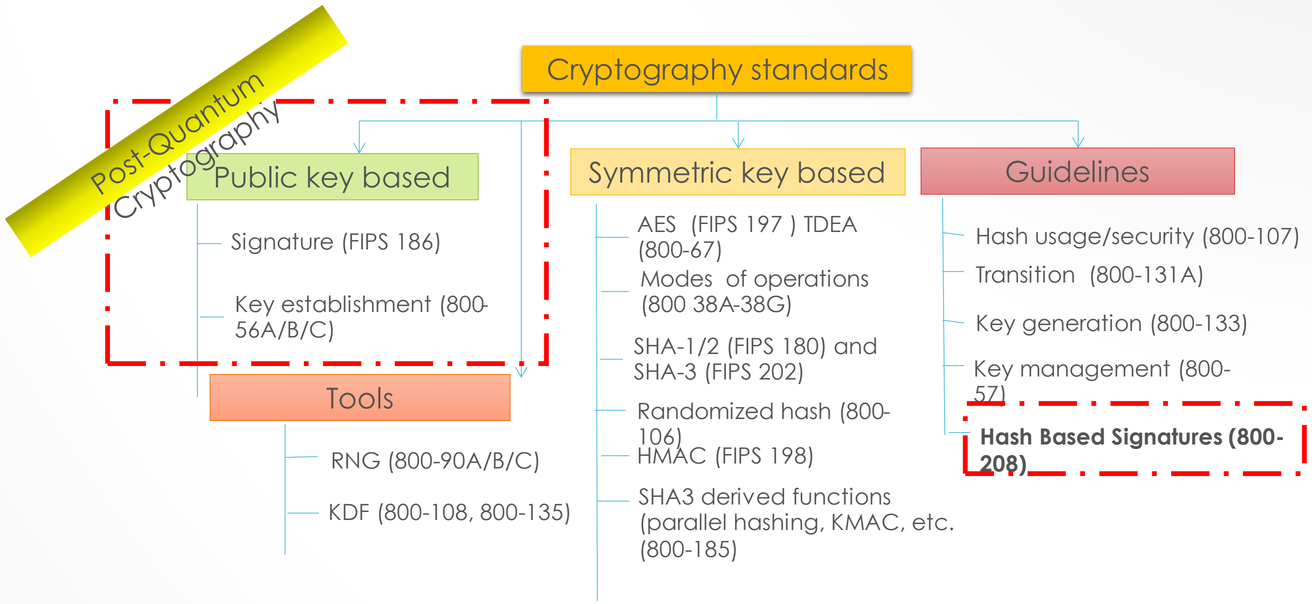
- AES (FIPS 197)
- Modes of operations (SP800 38A-38G)
- SHA-1/2 (FIPS 180) and SHA-3 (FIPS 202)
- HMAC (FIPS 196)
- Hash-Based Signatures (SP800-208)

Guidelines

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

CRYPTOGRAPHY STANDARDS

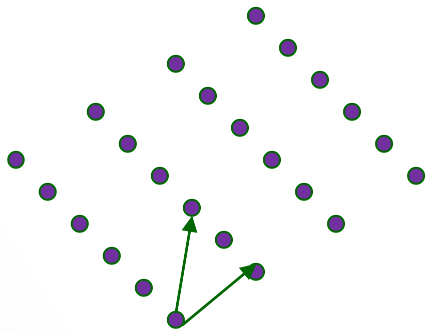
- **Shor's Algorithm–** Efficiently (polynomial-time) solve problems underpinning current public key cryptosystems
  - *Factorization*– RSA
  - *Discrete Logarithms*– ECDSA, Diffie-Hellman
- The well-deployed key establishment and digital signature algorithms will need to be replaced to prepare for quantum era
- Quantum computing also impacted security strength of symmetric key based cryptography algorithms – manageable by increasing key size

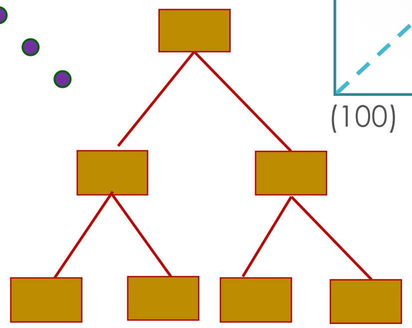


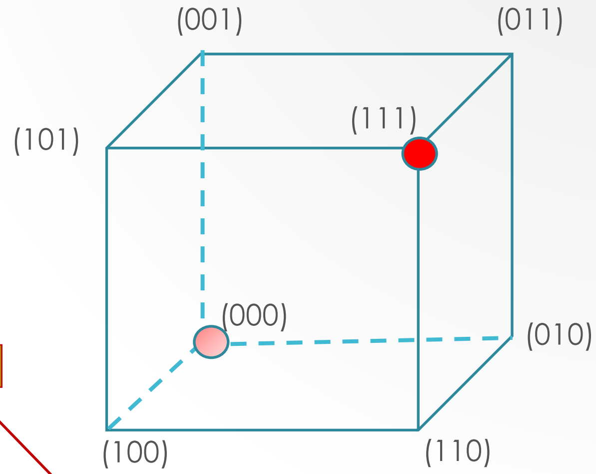
POST-QUANTUM CRYPTOGRAPHY

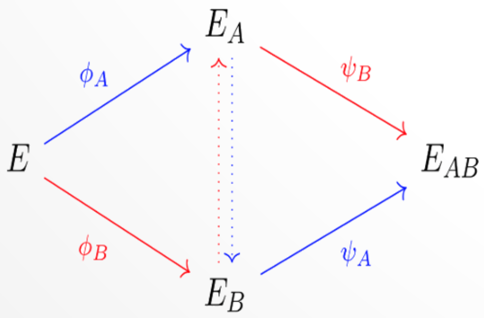
NIST

- PQC has been a very active research area in the past decade
- Some actively researched PQC categories include
  - Lattice-based
  - Code-based
  - Multivariate
  - Hash/Symmetric key -based signatures
  - Isogeny-based schemes









$$p^{(1)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)} \cdot x_i x_j \;+\; \sum_{i=1}^{n} p_i^{(1)} \cdot x_i + p_0^{(1)}$$

$$p^{(2)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)} \cdot x_i x_j \;+\; \sum_{i=1}^{n} p_i^{(2)} \cdot x_i + p_0^{(2)}$$

$$\vdots$$

$$p^{(m)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(m)} \cdot x_i x_j \;+\; \sum_{i=1}^{n} p_i^{(m)} \cdot x_i + p_0^{(m)}$$

SELECTED PQC ALGORITHMS

Key Encapsulation	Digital Signatures
Lattice-Based: • CRYSTALS-Kyber	*Lattice-Based* • CRYSTALS-Dilithium • Falcon *Hash-Based* • SPHINCS+

4th round KEMs

- Classic McEliece
- BIKE
- HQC
- SIKE

Onramp signatures

New call for additional signatures– preferably for signatures based on non-lattice problems.

Due: June 1, 2023

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*

NCCOE OVERVIEW

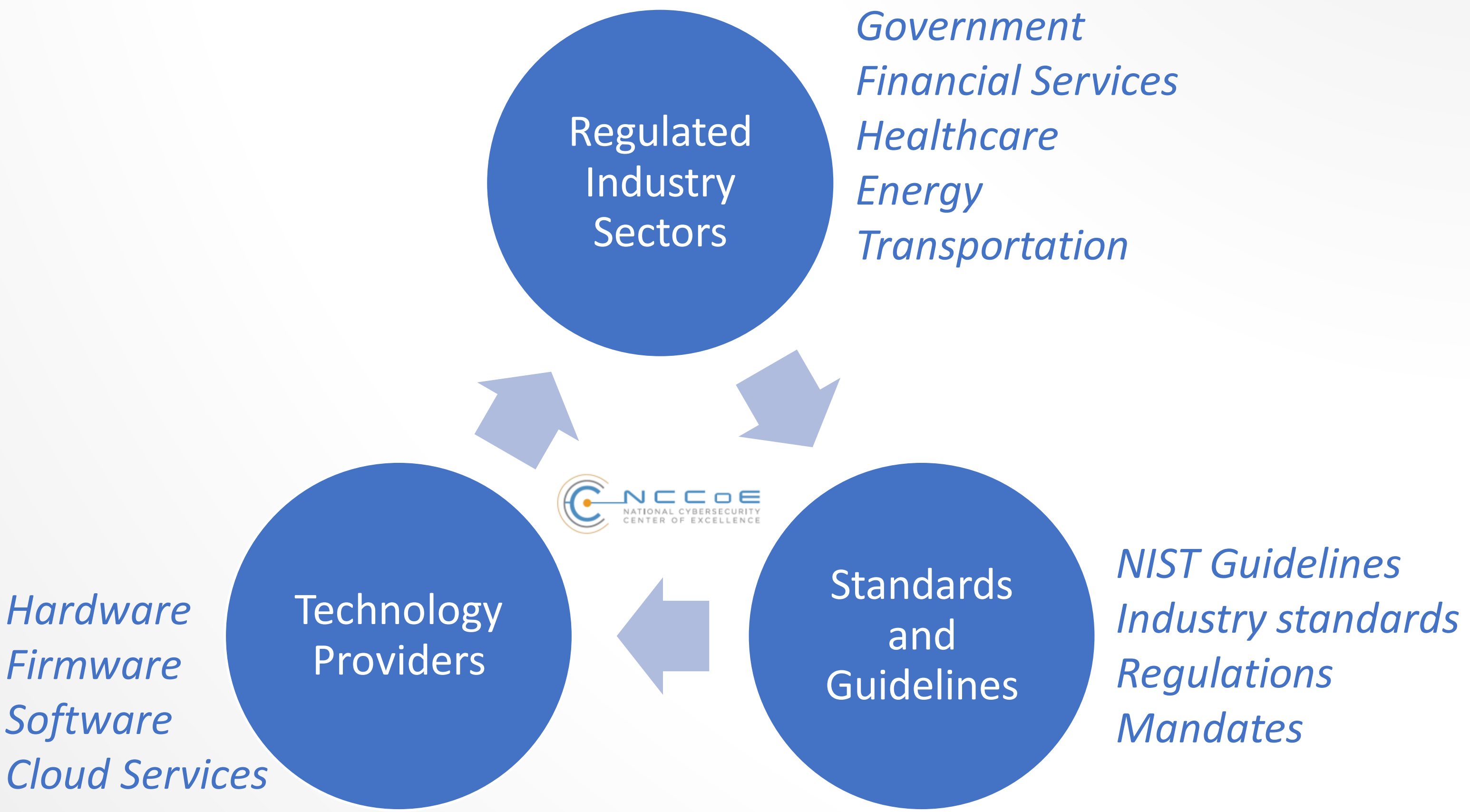
National Cybersecurity Center of Excellence (NCCoE)

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

- DEFINE
- ASSEMBLE
- BUILD
- ADVOCATE

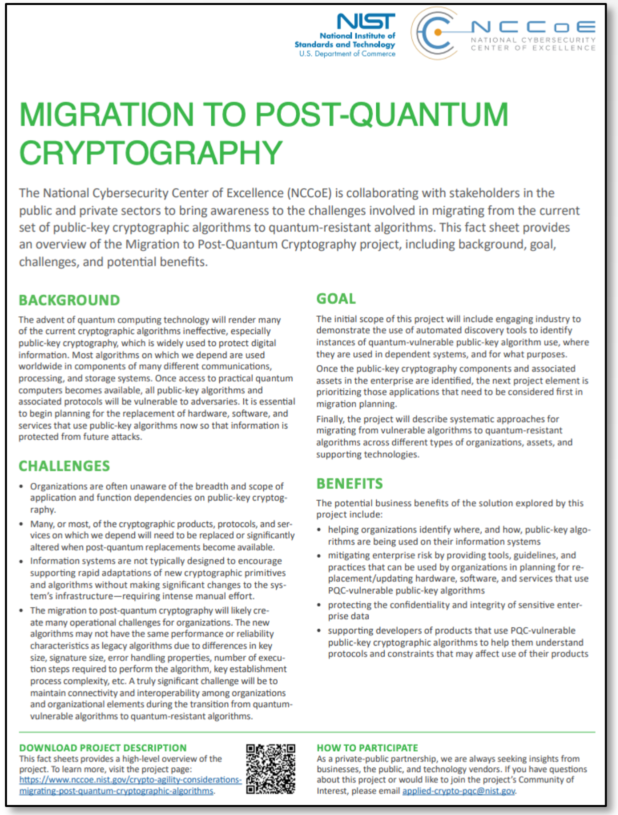
Practice Guide SP 1800

Engagement Model



NCCOE– MIGRATION TO PQC PROJECT

- Complement NIST PQC standardization effort
- Tackle challenges with adoption, implementation, and deployment of PQC
- Engage with the community including industry collaborators and across government to bring awareness to the issues involved in migrating to post-quantum algorithms
- Coordinate with standard developing organization and government and industry sectors community to develop guidance to accelerate the migration
- Leverage automated tools to discover use of quantum vulnerable cryptography within an organization in hardware, firmware, software, protocols, and services and use a risk-based approach to prioritize their replacement
- Perform interoperability and performance tests across different technology and protocols to include TLS, QUIC, code signing, public key certificates, hardware security modules, etc.



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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

MIGRATION TO POST-QUANTUM CRYPTOGRAPHY

The National Cybersecurity Center of Excellence (NCCoE) is collaborating with stakeholders in the public and private sectors to bring awareness to the challenges involved in migrating from the current set of public-key cryptographic algorithms to quantum-resistant algorithms. This fact sheet provides an overview of the Migration to Post-Quantum Cryptography project, including background, goal, challenges, and potential benefits.

BACKGROUND

The advent of quantum computing technology will render many of the current cryptographic algorithms ineffective, especially public-key cryptography, which is widely used to protect digital information. Most algorithms on which we depend are used worldwide in components of many different communications, processing, and storage systems. Once access to practical quantum computers becomes available, all public-key algorithms and associated protocols will be vulnerable to adversaries. It is essential to begin planning for the replacement of hardware, software, and services that use public-key algorithms now so that information is protected from future attacks.

CHALLENGES

- Organizations are often unaware of the breadth and scope of application and function dependencies on public-key cryptography.
- Many, or most, of the cryptographic products, protocols, and services on which we depend will need to be replaced or significantly altered when post-quantum replacements become available.
- Information systems are not typically designed to encourage supporting rapid adaptations of new cryptographic primitives and algorithms without making significant changes to the system's infrastructure—requiring intense manual effort.
- The migration to post-quantum cryptography will likely create many operational challenges for organizations. The new algorithms may not have the same performance or reliability characteristics as legacy algorithms due to differences in key size, signature size, error handling properties, number of execution steps required to perform the algorithm, key establishment process complexity, etc. A truly significant challenge will be to maintain connectivity and interoperability among organizations and organizational elements during the transition from quantum-vulnerable algorithms to quantum-resistant algorithms.

GOAL

The initial scope of this project will include engaging industry to demonstrate the use of automated discovery tools to identify instances of quantum-vulnerable public-key algorithm use, where they are used in dependent systems, and for what purposes.

Once the public-key cryptography components and associated assets in the enterprise are identified, the next project element is prioritizing those applications that need to be considered first in migration planning.

Finally, the project will describe systematic approaches for migrating from vulnerable algorithms to quantum-resistant algorithms across different types of organizations, assets, and supporting technologies.

BENEFITS

The potential business benefits of the solution explored by this project include:

- helping organizations identify where, and how, public-key algorithms are being used on their information systems
- mitigating enterprise risk by providing tools, guidelines, and practices that can be used by organizations in planning for replacement/updating hardware, software, and services that use PQC-vulnerable public-key algorithms
- protecting the confidentiality and integrity of sensitive enterprise data
- supporting developers of products that use PQC-vulnerable public-key cryptographic algorithms to help them understand protocols and constraints that may affect use of their products

DOWNLOAD PROJECT DESCRIPTION
This fact sheets provides a high-level overview of the project. To learn more, visit the project page: https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms.

HOW TO PARTICIPATE
As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you have questions about this project or would like to join the project's Community of Interest, please email applied-crypto-pqc@nist.gov.

https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

MUCH WORK REMAINS

NIST

- Operations
- Infrastructure Modernization
- PQC Adoption in Software/Systems
- Hardware Acceleration/Support
- Implementation in Cryptographic Libraries
- Protocol/Application Standards
- $\mathbb{Z}_q[X]$ Algorithm Standards

CODE SIGNING SYSTEMS

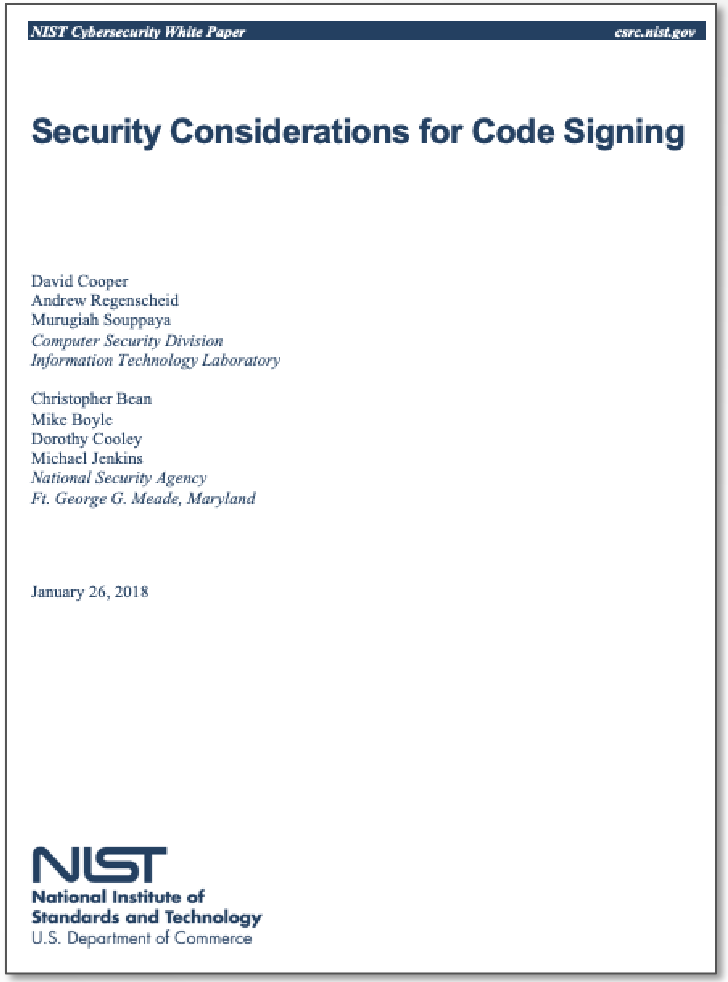
NIST Whitepaper:

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

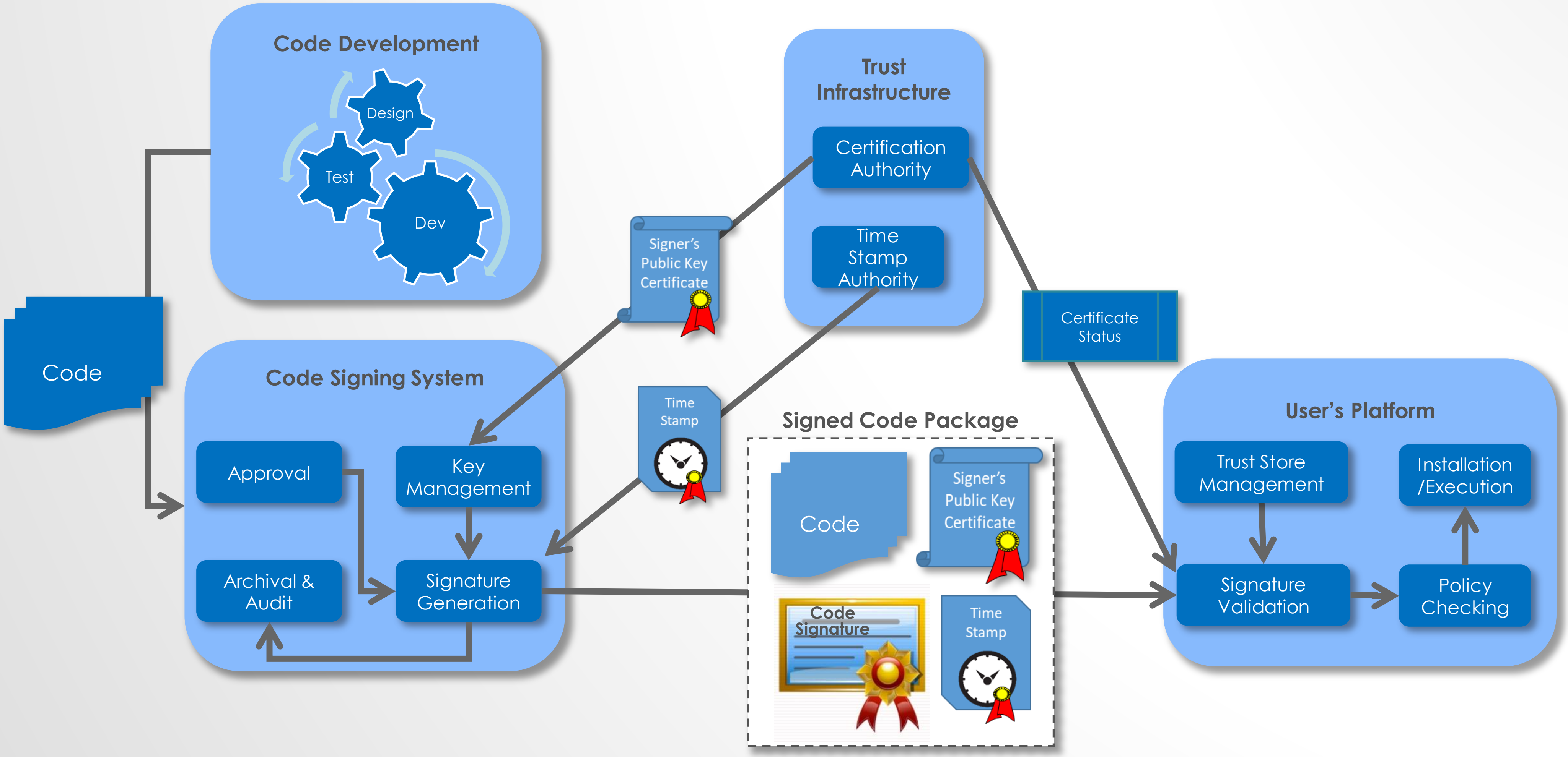
David Cooper
Andrew Regenscheid
Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

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

January 26, 2018

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

CODE SIGNING

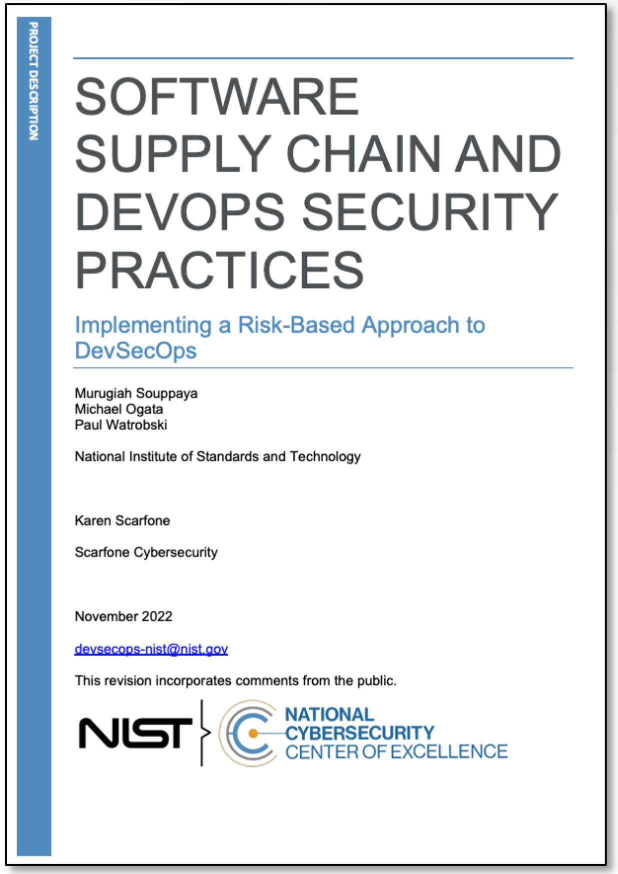


CODE SIGNING RECOMMENDATIONS

- Identify and authenticate trusted users
- Separate roles and require two-party control
- Establish policies and procedures for reviewing, vetting and approving code
- Isolate and protect the Code Signing System
- Separate development, testing, and production infrastructures
- Utilize auditing and periodically review logs
- Develop revocation/recovery mechanisms for cases of key compromise or unauthorized signing

NCCoE– DevSecOps Project

- Develop an applied risk-based approach and recommendations for secure DevOps and software supply chain practices consistent with the Secure Software Development Framework (SSDF), Cybersecurity Supply Chain Risk Management (C-SCRM), and other NIST, government, and industry guidance
- Apply these DevSecOps practices in proof-of-concept use case scenarios that will each be specific to a technology, programming language, and industry sector to produce practical and actionable guidelines that meaningfully integrate security practices into development methodologies
- Integrate automated security tools into the DevOps pipeline (development, integration, testing, build, and distribution)


PROJECT DESCRIPTION

SOFTWARE SUPPLY CHAIN AND DEVOPS SECURITY PRACTICES

Implementing a Risk-Based Approach to DevSecOps

Murugiah Souppaya
Michael Ogata
Paul Watrobski

National Institute of Standards and Technology

Karen Scarfone

Scarfone Cybersecurity

November 2022

devsecops-nist@nist.gov

This revision incorporates comments from the public.

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices

WRAP UP

Post-Quantum Cryptography

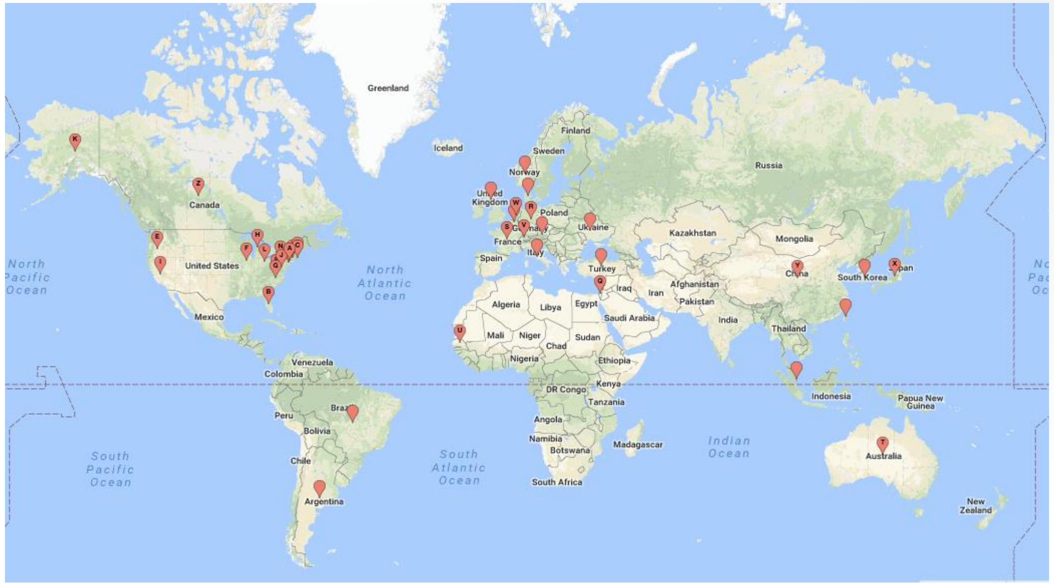
- Prepare for future migration to quantum-resistant cryptography
- Identify current algorithms/schemes used
- Assess suitability of emerging standards

Code Signing Systems

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

PQC STANDARDIZATION PROJECT

2010-2015
NIST PQC project team builds
First PQC conference



2016
Determined criteria and requirements, published NISTIR 8105
Announced call for proposals

2017
Received 82 submissions
Announced 69 1st round candidates

2018
Held the 1st NIST PQC standardization Conference

2019
Announced 26 2nd round candidates, NISTIR 8240
Held the 2nd NIST PQC Standardization Conference

2020
Announced 3rd round 7 finalists and 8 alternate candidates. NISTIR 8309

2021
Hold the 3rd NIST PQC Standardization Conference

2022 Make 3rd round selection and draft standards
2023 Release draft standards and call for public comments

FIRMWARE UPDATES

NIST SP 800-193, *Platform Firmware Resiliency Guidelines* & NIST SP 800-147, *BIOS Protection Guidelines*

Protection

- *Firmware* updates are authenticated using digital signatures
- *Critical data* only updated through authorized channels and checked for validity

Detection

- Verify integrity of *firmware* during boot
- Validate *critical data* via inspection before use (where possible), or detect signs of boot failures (e.g., watch dog timers)

Recovery

- Capability to restore code/data through automated or manual means
- Firmware recovery images verified through digital signatures (like an update)
- Capability to backup known-good copies of critical data

NIST AI project

Elham Tabassi

Adobe Acrobat
Document

A Taxonomy of Attacks and Mitigations

Apostol Vassilev
Computer Security Division
02/07/2023

NIST INFORMATION TECHNOLOGY LABORATORY

Adversarial ML

Machine Learning is Risky

The NIST AI RMF identifies many different sources of risk:

- Inherent: e.g., unwanted bias, errors in the data, implementation flaws in the model, cybersecurity flaws in the platform on which the ML models is deployed.
- Adversarial: deliberate actions by motivated experienced adversaries aiming to disrupt/evade/compromise the operation of the model or its output.

Image credit: Pavel Vinnik, Shuttershock, Portswigger LTD.

Machine Learning
ATTACK TAXONOMY

Three main attacker goals/objectives:

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

Goals require different attack surfaces/capabilities to exploit

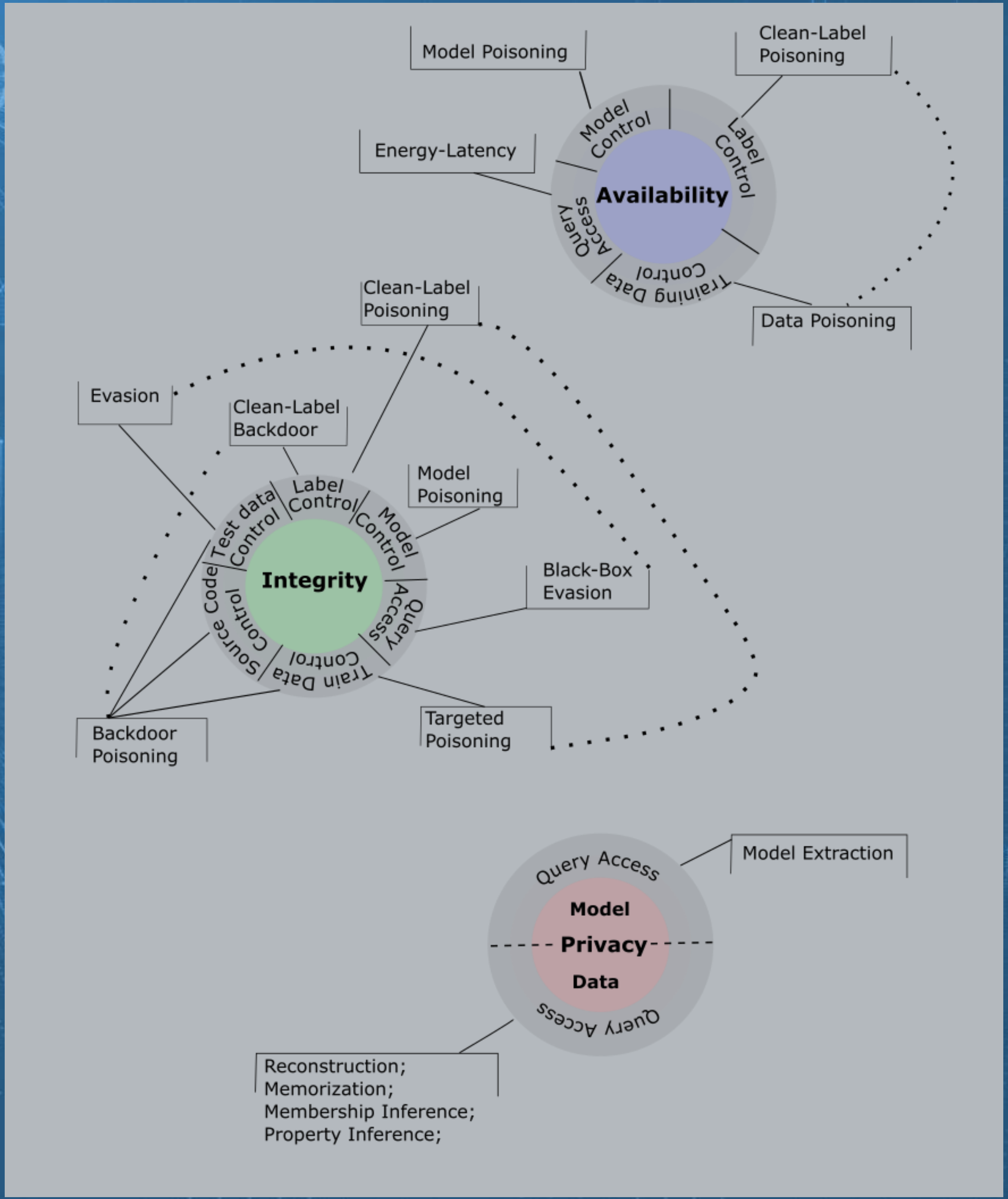
- *train data control,*
- *test data control,*
- *label control,*
- *source code control,*
- *model control,*
- *query access,*
- *etc.*

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*



Autonomous Vehicle
Physically-realizable attacks

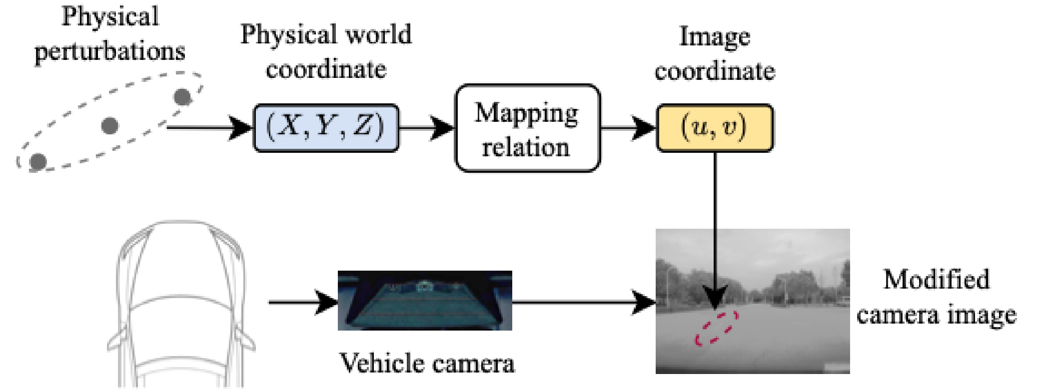
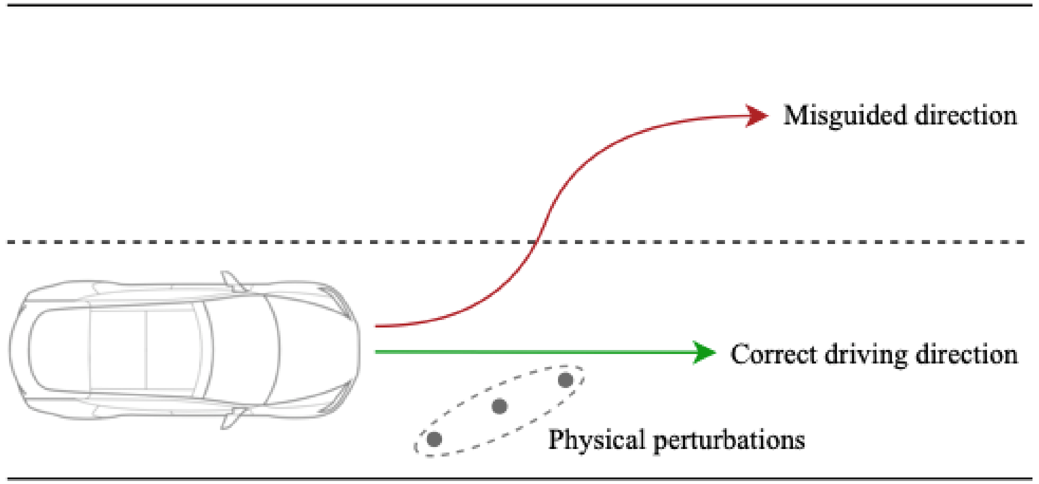


Figure 4: Mapping the coordinate of (X,Y,Z) on markings in physical world to the coordinate of (u,v) on perturbations in digital world.

Images credit: Pengfei Jing1, Qiyi Tang, Yuefeng Du, Lei Xue, Xiapu Luo, Ting Wang, Sen Nie, Shi Wu, [“Too Good to Be Safe: Tricking Lane Detection in Autonomous Driving with Crafted Perturbations”](), USENIX 2021.

Specifically designed perturbations of objects in the vision of the car that can evade vision classifiers in various physical environments



Human Eye Invisibale/Neglectible markings on road cause the vehicle the veer off into the opposite traffic lane

Potential Mitigations

Cognitive task automation!

≠

cognitive intelligence

No *information-theoretic* guarantees for mitigations !

Adversarial Training

The most robust approach

- Due to Goodfellow et al. in 2015
- Substantially improved by Madry et al. in 2018
- but costly, computationally & otherwise
- It may come at the cost of one accident at a time

Randomized smoothing

Provable L_2 ***robustness***

- robust smooth classifier based on most-likely predictions under Gaussian noise perturbation

Formal Verification

Good potential

Ongoing concerns

- Scalability
- Costs
- Restrictions on supported operations
- Reliance on assumptions that can be circumvented in practice

Machine Learning
INSIDER ATTACKS

<u>Backdoor poisoning:</u>

- *Train data control*
- *Test data control*
- *Source code control*

TROJANS

Some <u>computationally</u> undetectable

Shafi Goldwasser, Michael P. Kim, Vinod Vaikuntanathan and Or Zamir. Planting Undetectable Backdoors in Machine Learning Models, <u>arXiv</u>, 2022

Adversarial Machine Learning

A TAXONOMY OF ATTAKS AND MITIGATIONS

<u>Coming soon to the NIST AI Resource Center</u>

- *Joint effort with Prof. Alina Oprea*
- *Broad coverage, beyond automotive*
- *<u>Replaces</u> 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

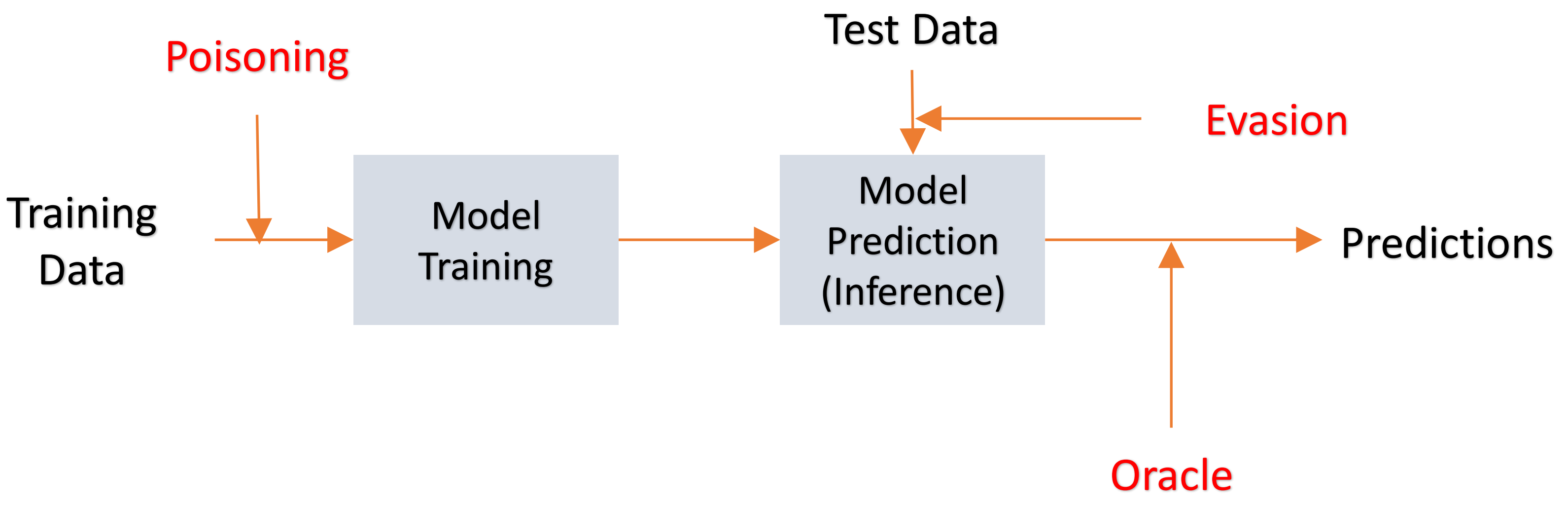
CONTACT US

ai-aml-ir@nist.gov

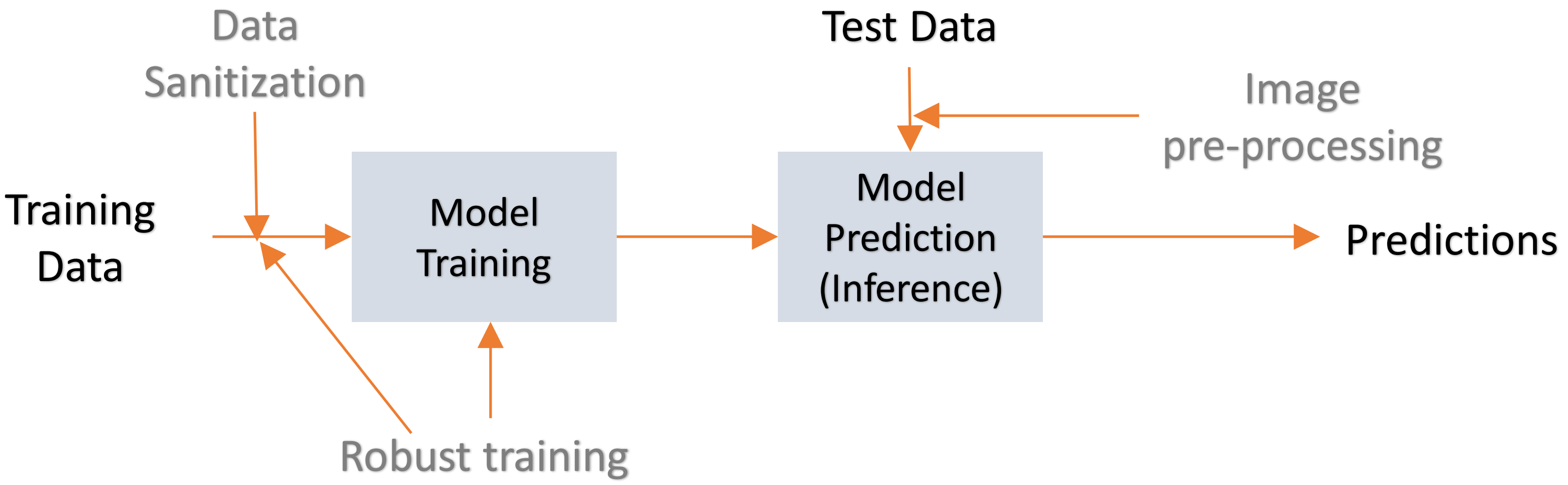
Dioptra

Test Platform for Machine Learning Systems

Attack and Mitigation Interfaces in the Model Lifecycle

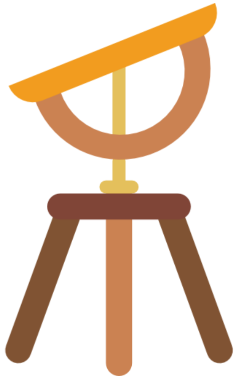


Sample of attack interfaces



Sample of mitigation interfaces

Scenario testing, Parameter Sweeping, Evaluation

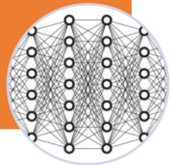


Dioptra

Image: Flaticon.com/Smashicons

- Shallow Net
- AlexNet
- LeNet
- ResNet50
- VGG16
- …

Training Architecture



- Patch augmentation
- Poison Frogs
- Adversarial training
- …

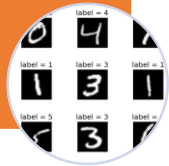
Data Augmentation

- Spatial smoothing
- Defensive distillation
- …

Inference pre-processing

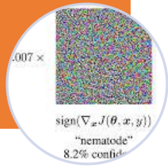
- MNIST
- Fruits360
- ImageNet
- …

Dataset



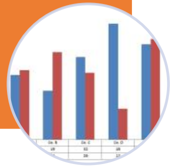
- Fast Gradient Method
- Pixel Threshold
- Patch
- Membership Inference
- …

Attack on trained model

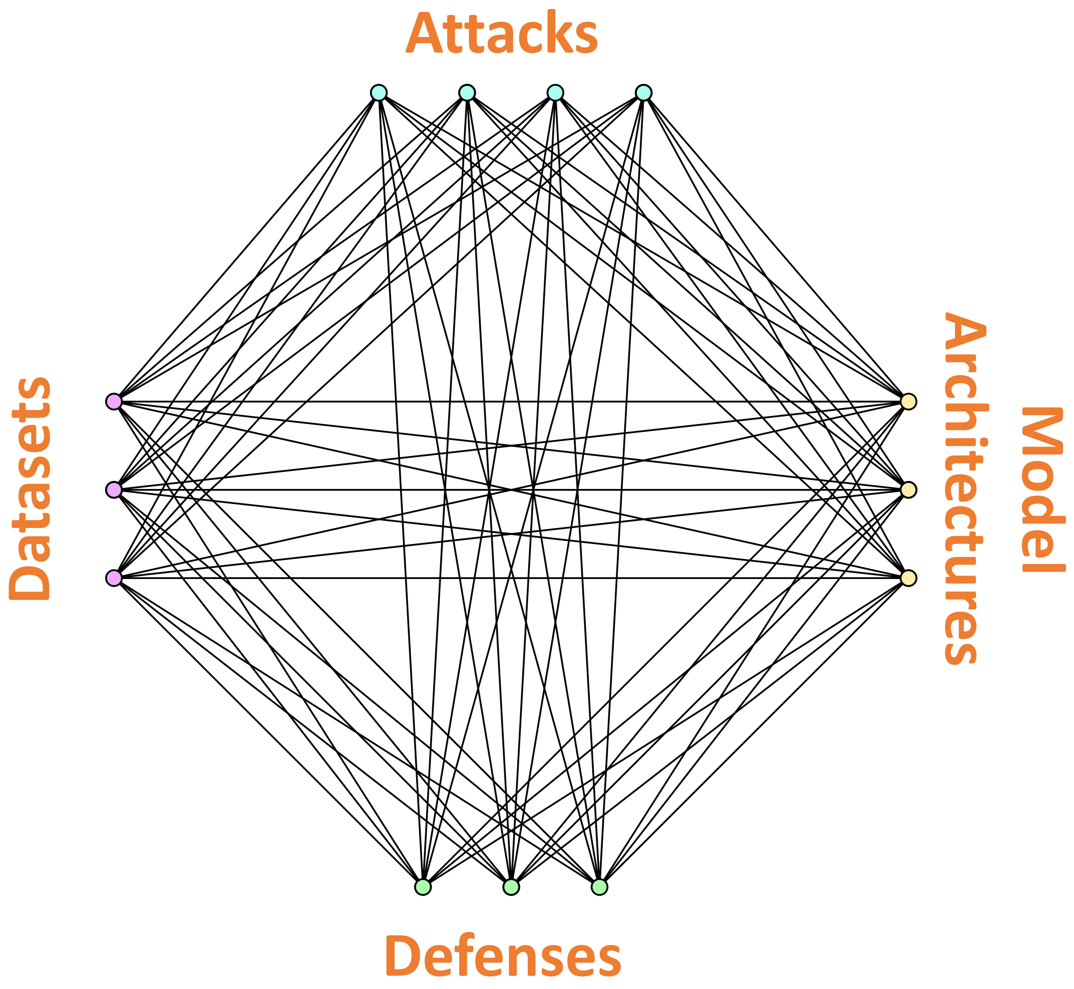


- Clean accuracy
- Adversarial accuracy
- Robustness radius
- …

Metric



Use Case Exploration



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)

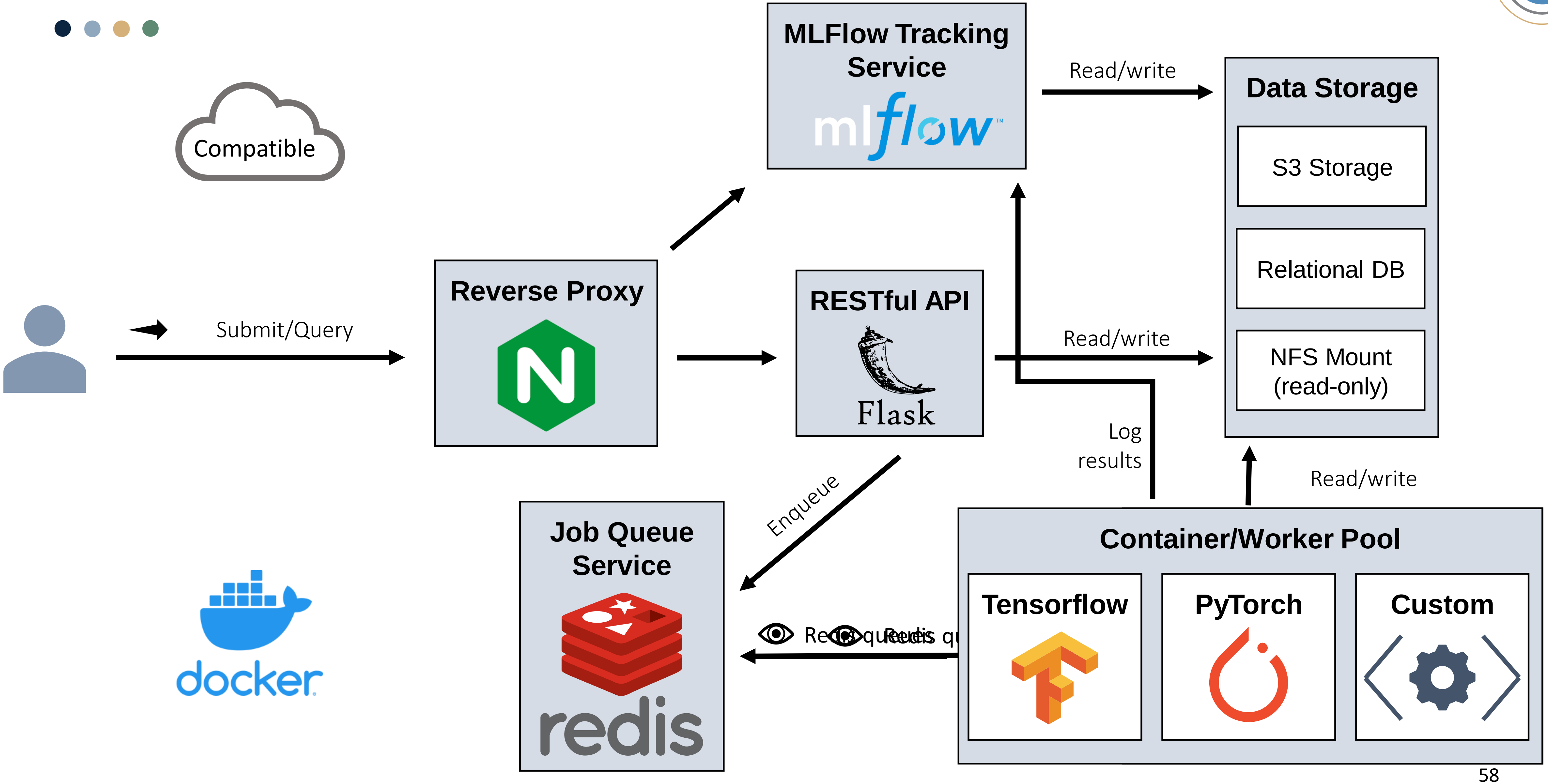
Examples / Demos

Docker Images

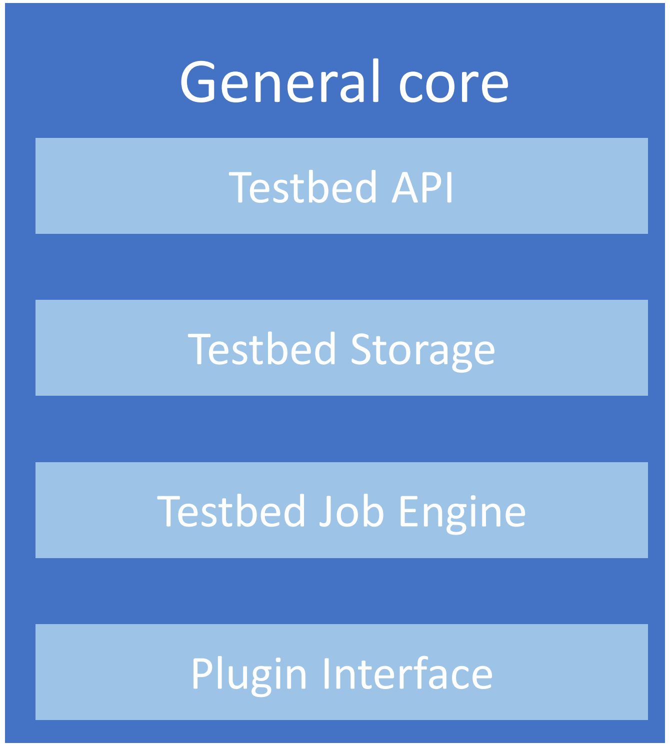
Built-in Task Plugins

Documentation

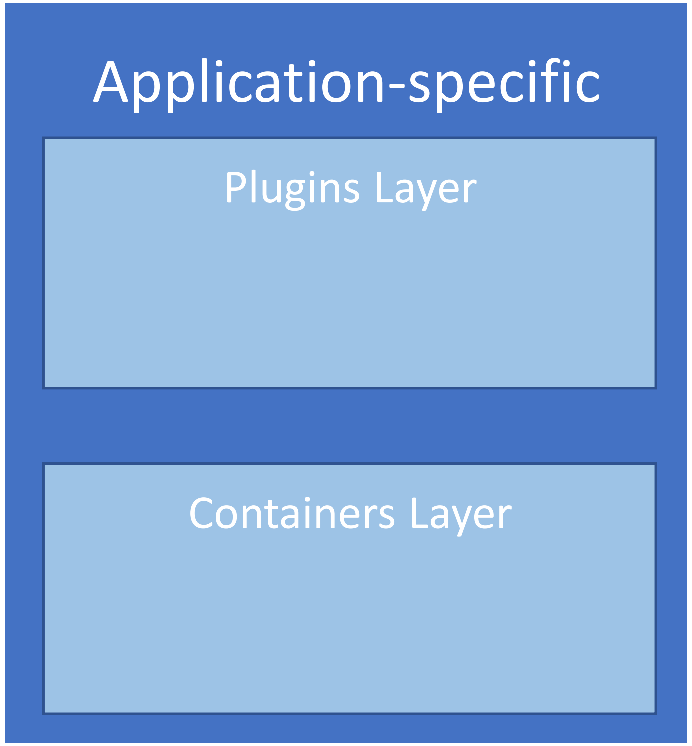
MICROSERVICES ARCHITECTURE ENABLES FLEXIBLE DEPLOYMENT



A MODULAR DESIGN AT THE ARCHITECTURAL AND SOFTWARE LEVEL

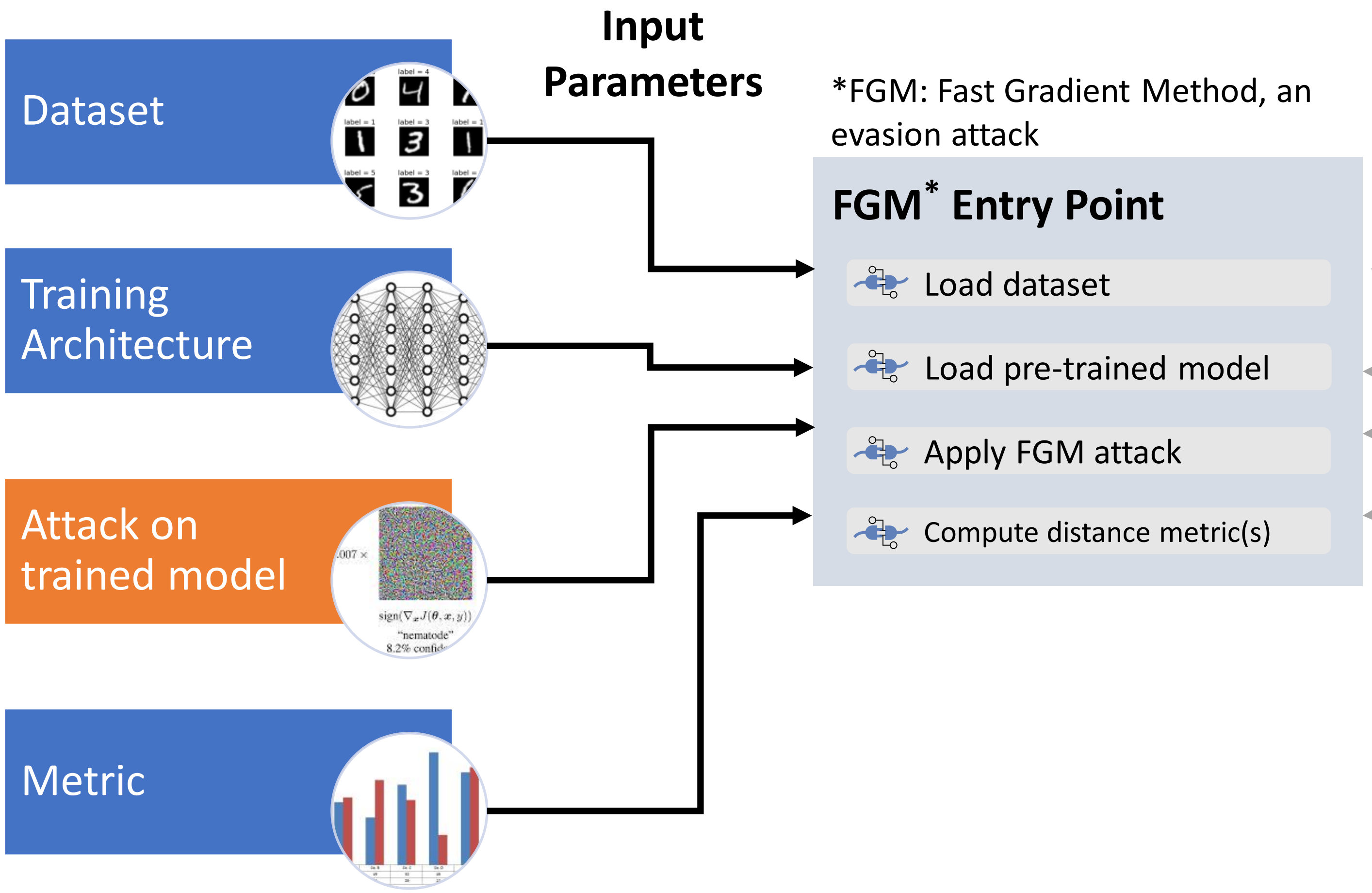


Flexible, able to be repurposed to meet needs in other projects



Specific use cases are implemented as plugins and customized containers

Running A Job

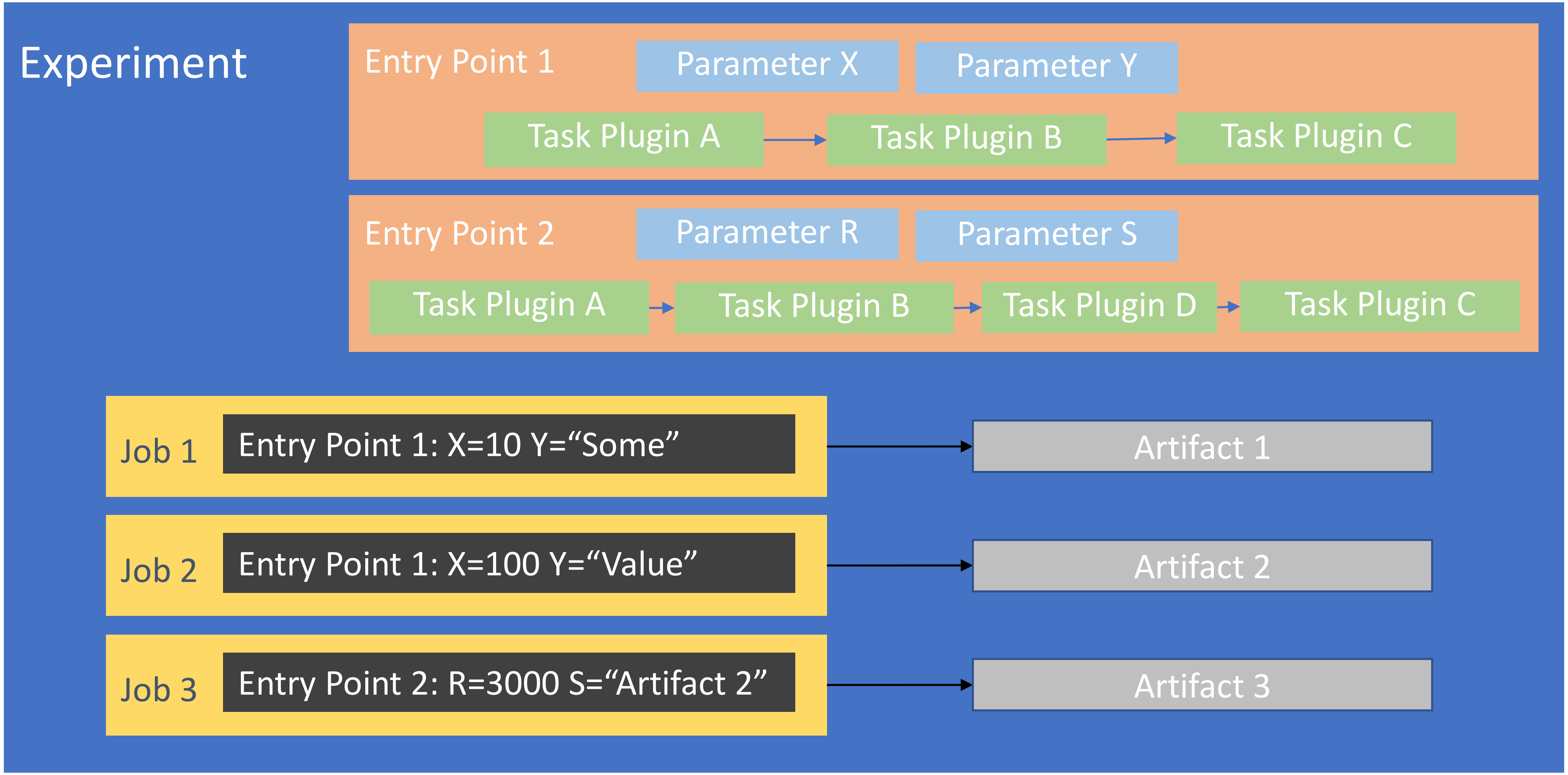


Task plugins

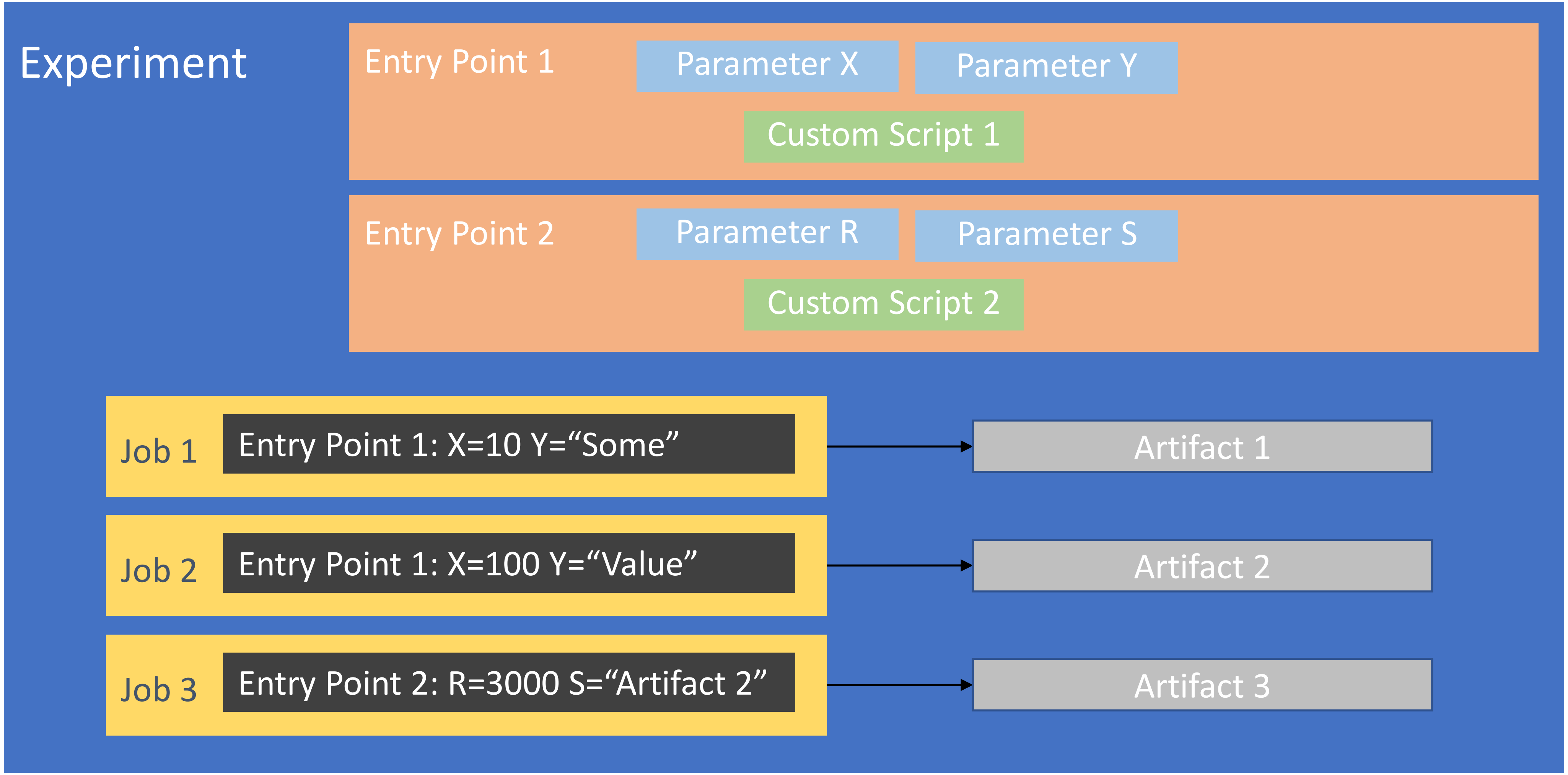
- Modular, reusable
- Building blocks

Entry Point = Script + Parameters

Anatomy of an Experiment



Anatomy of an Experiment



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.

Next Steps:

- Host EV XFC project kickoff on Thursday, February 16th from 2pm-3:30pm ET
  - Event link: https://www.nccoe.nist.gov/get-involved/attend-events/nccoe-learning-series-electric-vehicle-ev-extreme-fast-charging-xfc
- Begin meetings with the community to develop Cybersecurity Framework Profile on Thursday, February 23rd from 3pm-4pm ET
  - Invite will be sent to those on the community of interest email soon

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