OWASP
AppSec Europe
London 2nd-6th July 2018

Current Research and Standards for Security Automation

An overview of US Government efforts to support and promote security automation

Charles Schmidt

Current Research and Standards for Security Automation

Charles Schmidt

About Me

- Charles Schmidt
  - 18 years at MITRE supporting cyber security research and development
    - Most supporting security automation standards (XCCDF, OCIL, TAXII, SCAP, etc.)
- The MITRE Corporation
  - MITRE is a not for profit organization chartered to work in the public interest

This technical data deliverable was developed using contract funds under Basic Contract No. W56KGU-17-C-0010.

MITRE

Current Research and Standards for Security Automation

Charles Schmidt

This Talk

1. Security Automation overview
2. Key Security Automation principles
3. Some current Security Automation efforts
4. Next steps

The Challenge

- The time of your cyber security team is valuable
  - There is more important work to do than resources will allow
  - Lots of this work is menial

- Solution: Security Automation

Current Research and Standards for Security Automation

Charles Schmidt

Security Automation

- It is not human-free security
- Instead use machines for tedious and manual activities
- Optimize your resources – humans for human tasks and machines for machine tasks

Why is the US Government involved?

- Self interest

Why pursue via international standards?

- Broad scope, specialized needs, and changing landscape requires a multi-vendor approach

- International standards are the solution
  - Enable multi-vendor solutions
  - International standards let vendors sell to bigger markets

Key Security Automation Principles

- Standardized, but extensible
- Modular design
- Data reuse via orchestration and data repositories
- Separate collection from evaluation
- Federated content creation

Security Automation Activities

- These are activities in which the US government is supporting participation
  - There are likely others – getting them connected would be great for all parties
- US Government does not own or run these activities – it is one of many participants/stakeholders

Current Research and Standards for Security Automation

Charles Schmidt

Integrated Adaptive Cyber Defense (IACD)

- Johns-Hopkins University Applied Physics Laboratory runs the Integrated Adaptive Cyber Defense program
  - JHU APL IACD
- "a strategy and framework to adopt an extensible, adaptive, commercial off-the-shelf (COTS)-based approach to cybersecurity operations."[1]

IACD logo from JHU APL IACD program (https://www.iacdautomate.org/)

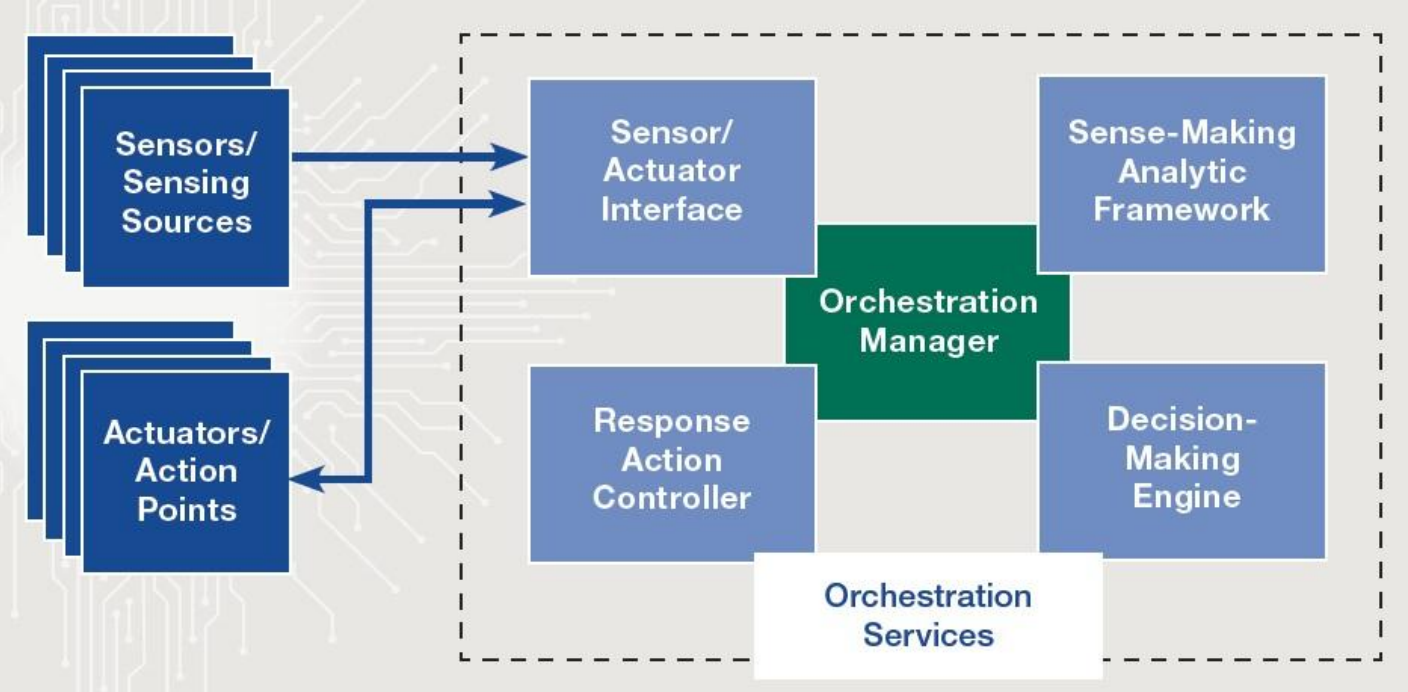
[1] https://www.iacdautomate.org/aboutiacd

Current Research and Standards for Security Automation

Charles Schmidt

IACD Overview

- Series of prototyping efforts to solve specific problems using existing products
- Focuses on data orchestration

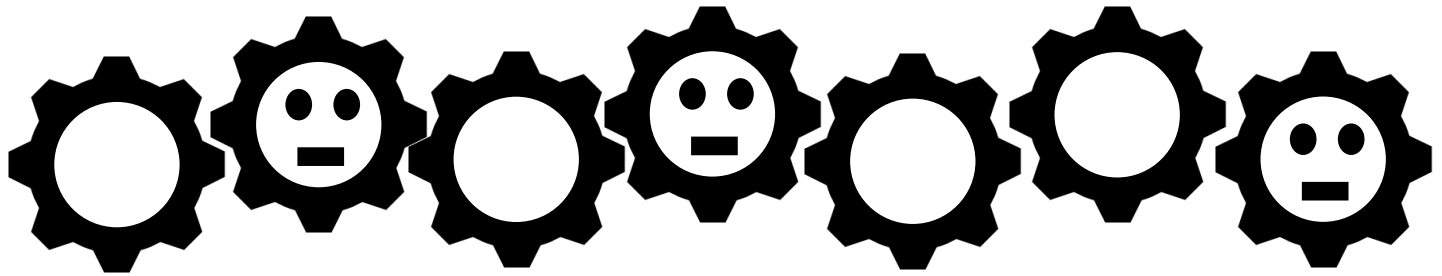


[1] Image from "IACD Baseline Architecture"

IACD Outcomes

- "IACD moves human defenders outside the response loop into a response planning and approval role 'on the loop' of cyber defense"[1]

- In multi-tool environments, humans often end up being the connective tissue between tools



[1] "IACD 101", https://www.iacdautomate.org/iacd101

IACD Products

- IACD defines a framework - including reference architectures, use cases, standard playbooks, specifications, and implementation examples

- Not seeking to invent standards; rather an attempt to identify the possible and key enablers

Current Research and Standards for Security Automation

Charles Schmidt

OASIS Open Command and Control (OpenC2)

- OASIS Open Command and Control (OpenC2)
  - "a common language for machine-to-machine communication" for security tools
  - OpenC2 converges on a common language and abstract commands
    - 'atomic actions', 'generic steps', 'Schema' …
- Decouple functional blocks in security architecture through standardized interfaces

OpenC2 Scope

- OpenC2 assumes the following has been done:
  - Sensing; 'What' triggers the action
  - Analytics; 'Why'
  - Decision; 'Which' action
  - Message Fabric; 'Transport' and 'Assurance'
- Focuses on 'Acting' portion of cyber-defense
  - The "make it so" part of the process

Current Research and Standards for Security Automation

Charles Schmidt

OpenC2 Subcommittee Foci

- Language Specification
  - Actions
  - Default Target namespace
  - Semantics, syntax
  - Minimum to implement
- Actuator Profiles
  - Scope and applicability
  - Required and optional Actions/ Target Pairs in the context of the Actuator
  - Specifiers and options for a class of actuators
- Implementation Guides
  - All other integration aspects
  - Use of other standards to address ‘External Dependencies’

Current Research and Standards for Security Automation

Charles Schmidt

Trusted Computing Group's Trusted Network Communications

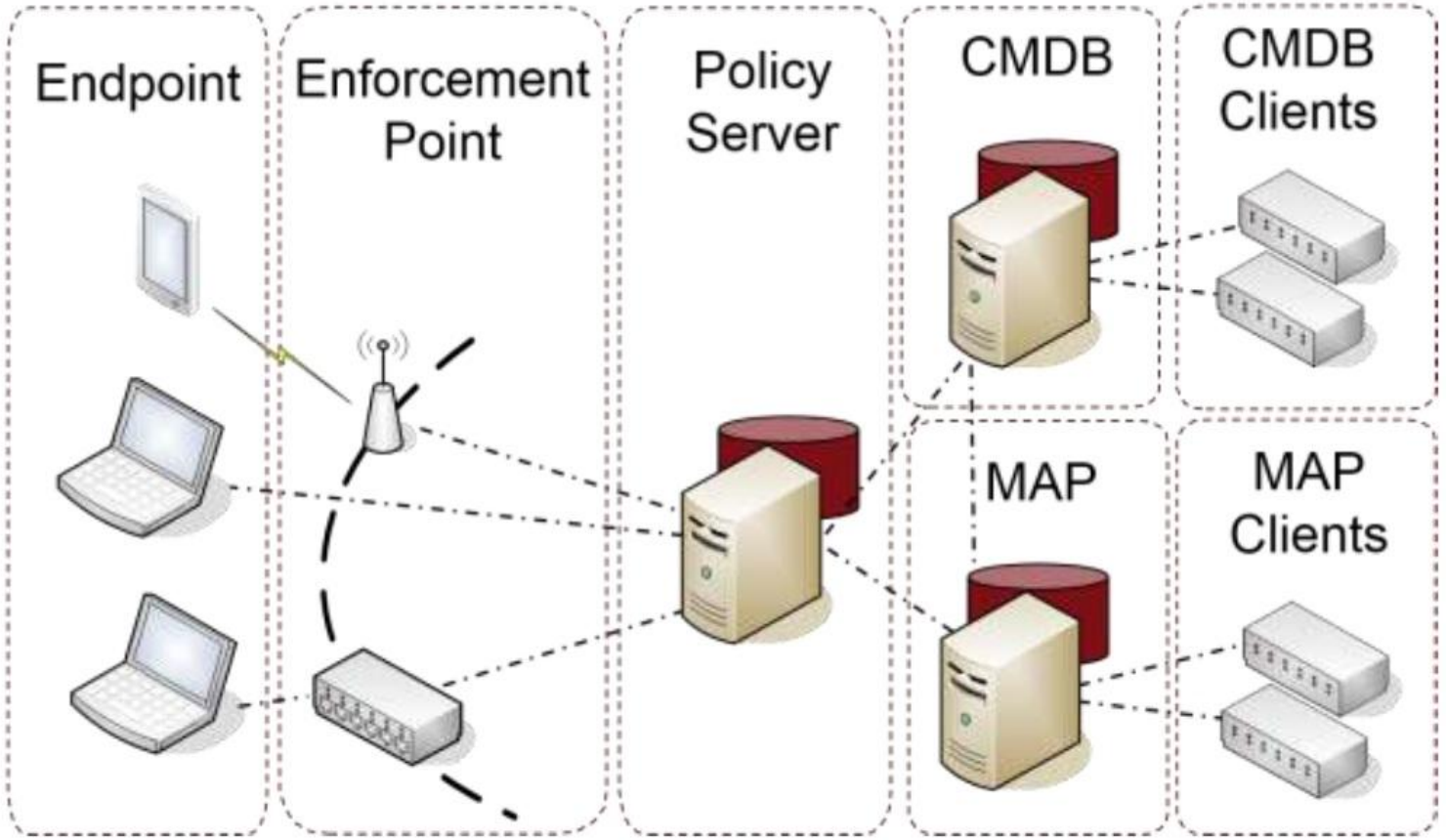
- Trusted Computing Group (TCG) Trusted Network Communications (TNC)
  - "provide network and endpoint visibility"[1]
  - "enable context-based access control enforcement"[1]
- An architecture for collecting, evaluating, acting on, and sharing security information
- Designed to be extensible and modular

[1] "TCG Trusted Network Communications Architecture for Interoperability" Version 2.0 October 2017

Current Research and Standards for Security Automation

Charles Schmidt

TNC Architecture



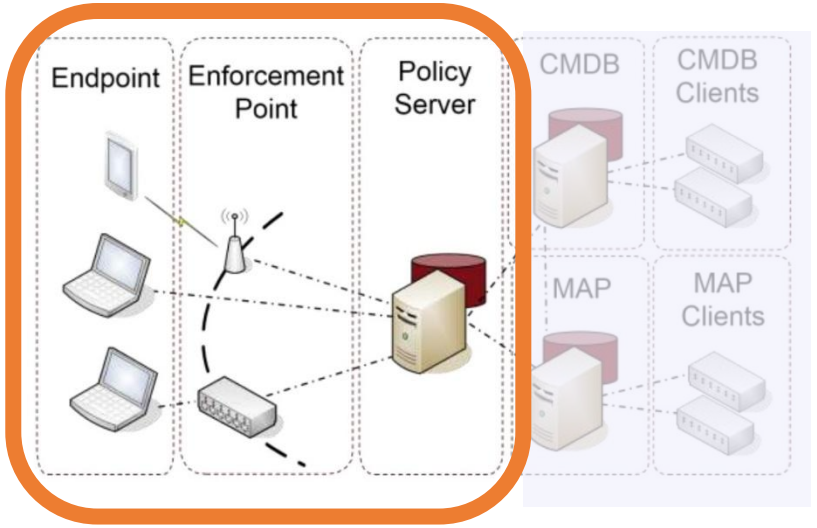
"TCG Trusted Network Communications Architecture for Interoperability" Version 2.0 October 2017

Current Research and Standards for Security Automation

Charles Schmidt

IETF NEA

- TCG offered the TNC specifications to the IETF for adoption as RFCs
  - Produced the Network Endpoint Assessment standards (RFCs 5209, 5792, 5793, 6876, & 7171)
- The same as the data collection portion of TNC
  - Efforts are compatible
  - Technical components given new names



Current Research and Standards for Security Automation

Charles Schmidt

IETF SACM

- IETF Security Automation and Continuous Monitoring (SACM) workgroup
- Develop "Standardized protocols and models aiding collection and evaluation of endpoint elements"[1]
- Effort focuses on standards for:
  - Collection of data elements from endpoints
  - Evaluation of collected data elements
  - Orchestration and Communication

IETF Logo is a registered trademark of the IETF (https://www.ietf.org/)

[1] SACM Charter (https://datatracker.ietf.org/wg/sacm/about/)

Current Research and Standards for Security Automation

Charles Schmidt

Key SACM Efforts

- Incorporation and extension of NEA protocols to enable collection
  - Software Inventory Message and Attributes (SWIMA)
    - "allow endpoints to report their installed software inventory information to a NEA server"[1]
- Concise Software Identifiers (CoSWID)
  - "concise representation of ISO/IEC 19770-2:2015 Software Identification (SWID) tags"[2]
- Other efforts are also ongoing in SACM

[1] "Software Inventory Message and Attributes (SWIMA) for PA-TNC" – draft-ietf-sacm-nea-swima-patnc-05
[2] "Concise Software Identifiers" – draft-ietf-sacm-coswid-05

Current Research and Standards for Security Automation

Charles Schmidt

IETF MILE

- IETF Managed Incident Lightweight Exchange (MILE)
  - "support computer and network security incident management"[1]
- Resource-Oriented Lightweight Information Exchange (ROLIE) (RFC 8322 and extensions)
  - Supports "security automation information publication, discovery, and sharing"[2]
  - Extension of the Atom Publishing Protocol focused on security automation data

IETF Logo is a registered trademark of the IETF (https://www.ietf.org/)

[1] MILE Charter (https://datatracker.ietf.org/wg/mile/about/)

[2] RFC 8322

Current Research and Standards for Security Automation

Charles Schmidt

SCAP

- Security Content Automation Protocol (SCAP)
  - A “synthesis of interoperable specifications” supporting security automation

- The SCAP specification (NIST Interagency Report 800-126) contains:
  - A list of supported specifications
  - Standardization of how these specification can be used together

Current Research and Standards for Security Automation

Charles Schmidt

SCAP 1.3

- Focused on data standardization
  - Languages (standardizing syntax and semantics for instructions and data)
  - Naming (common names to allow correlation)
  - Metrics (for help prioritizing issues)

- First released 2011; latest release (1.3) released this February

- SCAP 1.* has seen significant market uptake

SCAP 2.0

- SCAP 1.3 facilitated interoperable data, but not interoperable tools
  - Need standardized interfaces for that

- SCAP 2.0 – a new effort to build on SCAP 1.3 to create an interoperable security automation architecture
  - Currently in early phase – have developed an initial design to kick-start conversations; public conversations will begin later this year

Current Research and Standards for Security Automation

Charles Schmidt

SCAP 2.0 Architecture

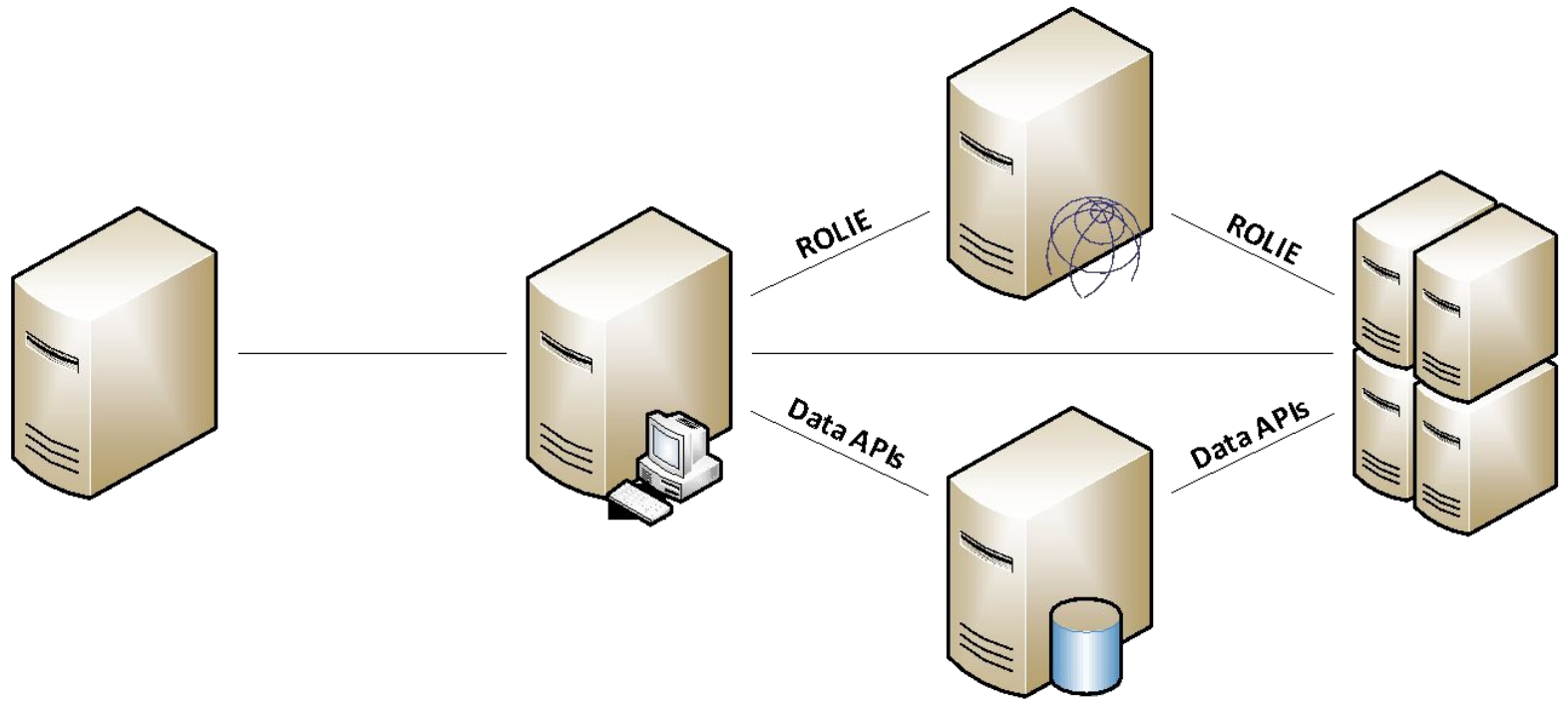
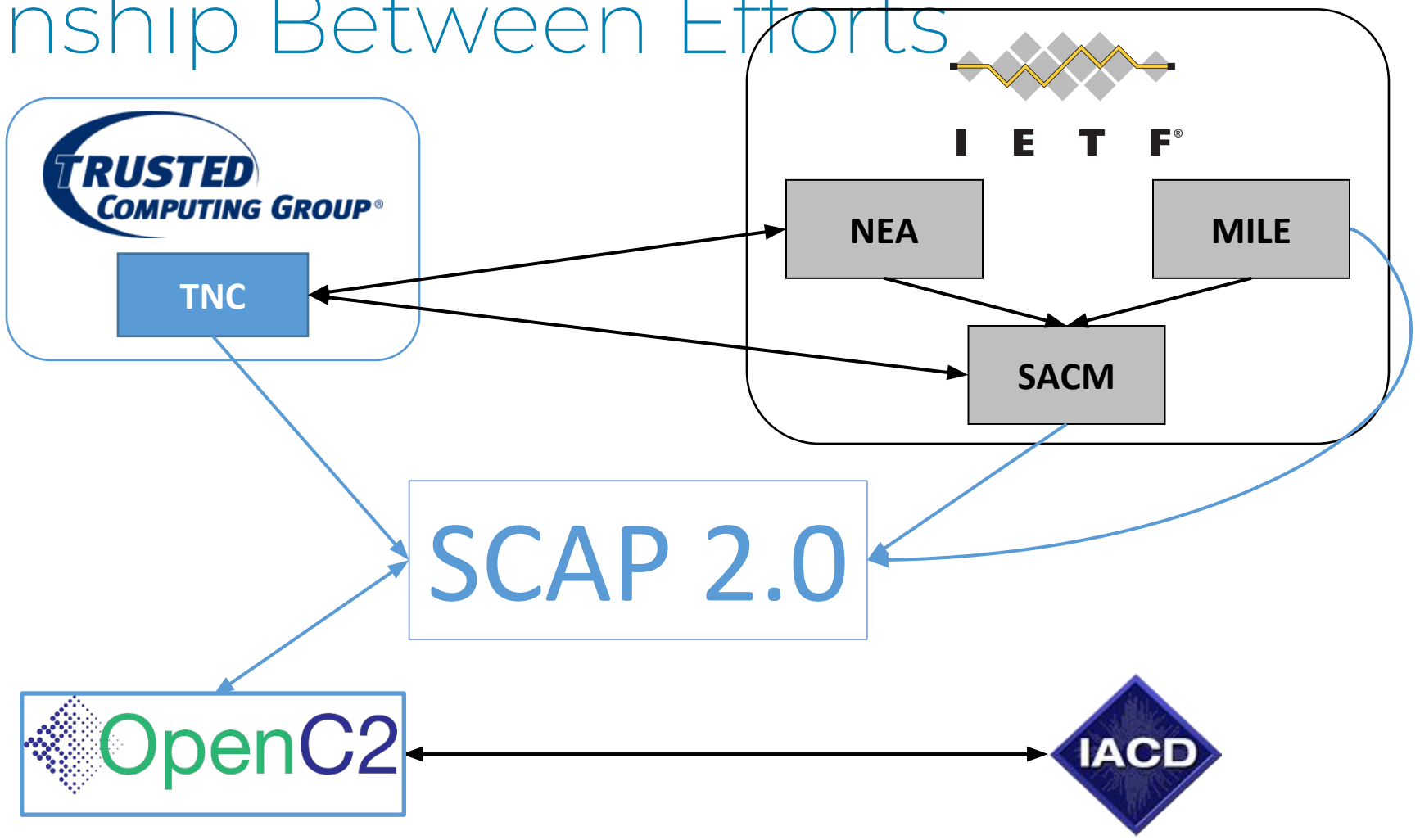


Image from “Transitioning to SCAP Version 2”

Current Research and Standards for Security Automation

Charles Schmidt

Relationship Between Efforts



Next Steps

- The key objective of this talk:
  - **We need collaborators**
- USG is funding work in these groups but...
  - We need other user input so the standards address the full spectrum of operational challenges
  - We need vendor input so adoption is commercially viable
- Talk to us, engage with these efforts, and help us empower security practitioners everywhere

Current Research and Standards for Security Automation

Charles Schmidt

References

- JHU APL IACD
  - https://www.iacdautomate.org/
- OASIS OpenC2
  - https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=openc2
- TCG TNC
  - https://trustedcomputinggroup.org/work-groups/trusted-network-communications/
- IETF SACM/MILE
  - https://datatracker.ietf.org/wg/sacm/about/
  - https://datatracker.ietf.org/wg/mile/about/
- NIST SCAP
  - https://csrc.nist.gov/projects/security-content-automation-protocol

Charles Schmidt
cmschmidt@MITRE.org

Questions?

Current Research and Standards for Security Automation

Charles Schmidt

Wall of Acronyms

APL ARF CCE CCSS CEP CMDB CPE CVE
CVSS ECP IACD IETF IMC IMV ISO ITU
JHU MAP MILE NIST NSA OASIS OCIL
OVAL PDP PEP ROLIE SACM SCAP SDO
SWID SWIMA TCG TMSAD TNC
TNCC TNCCS TNCS USG XCCDF