Hardware CWE™ Special Interest Group (SIG)

Gananand Kini, Bob Heinemann, Luke Malinowski, Gage Hackford, Chris Lathrop, Steve Christey Coley, Alec Summers

MITRE

June 9, 2023

Agenda

REMINDER: This meeting is being recorded.

- **Housekeeping and Announcements**
- **Working Items for this meeting:**

1	D3FEND and Hardware Coverage	Peter K	20 min
2	CVE QWG Hardware and Software Tagging	Jason F	20 min
3	HW CWE DEMOX's from Student Competitions		
4	Becoming a CNA (if time permits)	Alec S	10 min

Housekeeping

- **Schedule:**
  - **Next Meeting:**
    - **Scheduled for July 14**
    - **12:30 – 1:30 PM EST (16:30 – 17:30 UTC)**
    - **Microsoft Teams**
- **Contact: cwe@mitre.org**
- **Mailing List:** *hw-cwe-special-interest-group-sig-list@mitre.org*
- **Minutes from previous meetings available on our GitHub site:**
  - **https://github.com/CWE-CAPEC/hw-cwe-sig**

Announcements

- **Top 25 Release June 13**
- **CWE/CAPEC Board Meeting Occurred on June 2**
- **Tentative: CISA strategy around Secure By Design/Secure By Default for July SIG**

D3FEND and Hardware Coverage

Peter K

D3FEND

A knowledge graph of cybersecurity countermeasures

Peter Kaloroumakis

Principal, D3FEND Lead

pk@mitre.org

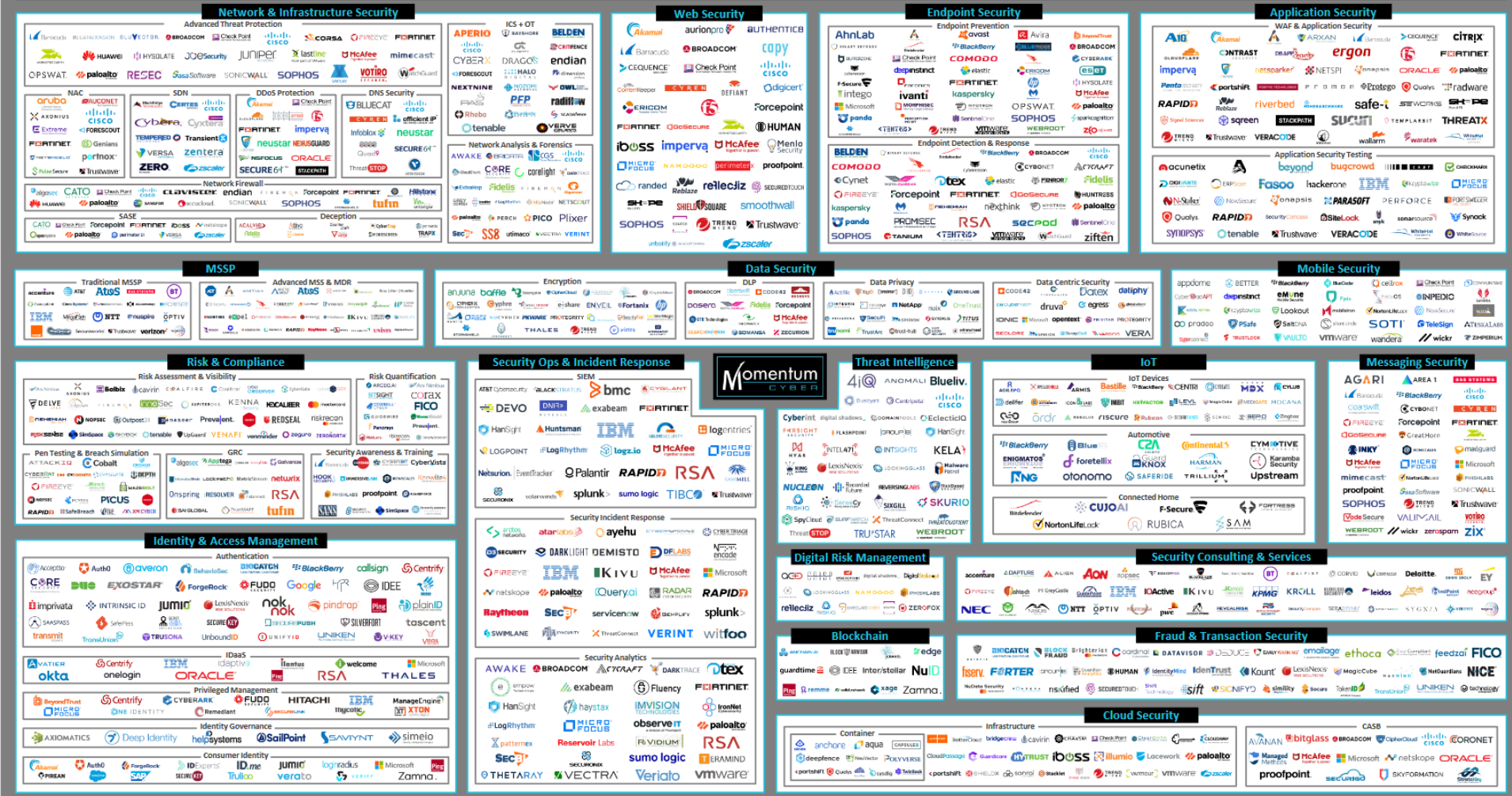
MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

APPROVED FOR PUBLIC RELEASE;
DISTRIBUTION UNLIMITED #21-1750

DEFEND™

MITRE

CYBER SCAPE 2021



Cyber Security & Information Systems Information Analysis Center

Build and Operate a Trusted DoDIN

Cybersecurity-Related Policies and Issuances

Developed by the DoD Deputy CIO for Cybersecurity

Last Updated: November 29, 2021

Send questions/suggestions to **contact@csiac.org**

ORGANIZE

Lead and Govern

- Interim National Security Strategic Guidance
- United States Intelligence Community Information Sharing Strategy
- 2019 National Intelligence Strategy
- U.S. Int'l Strategy for Cyberspace
- National Cyber Strategy
- National Strategy to Secure 5G
- NIST Framework for Improving Critical Infrastructure Cybersecurity
- National Defense Strategy (NDS)
- National Military Strategy (NMS)
- 2018 DoD Cyber Strategy
- DoD Digital Modernization Strategy
- *DoD Cybersecurity Risk Reduction Strategy*
- Summary of the 2018 DoD Artificial Intelligence Strategy
- DoD Cloud Strategy
- DoD Data Strategy
- DoD Identity, Credential, and Access Management (ICAM) Strategy
- DoD 5G Strategy
- DoD Information Sharing Strategy

ORGANIZE

Design for the Fight

- NIST SP 800-119 Guidelines for the Secure Deployment of IPv6
- CNSSP-11 Nat'l Policy Governing the Acquisition of IA and IA-Enabled IT
- CNSS National Secret Fabric Architecture Recommendations
- DFARS Subpart 208.74, Enterprise Software Agreements
- DoDD 5000.01 The Defense Acquisition System
- DoDD O-5100.19 (CAC req'd) Critical Information Communications (CRITCOM) System
- DoDD 7045.20 Capability Portfolio Management
- DoDD 8115.01 IT Portfolio Management
- DoDI 5000.02T Operation of the Defense Acquisition System
- DoDI 5000.67 Operation of the Software Acquisition Pathway
- DoDI 5200.44 Protection of Mission Critical Functions to Achieve TSN
- DoDI 7000.14 Financial Management Policy and Procedures (FPPE)
- DoDI 8115.02 IT Portfolio Management Implementation
- DoDI 8310.01 Information Technology Standards in the DoD
- DoDI 8330.01 Interoperability of IT and National Security Systems (NSS)
- DoDI 8510.01 Risk Management Framework for DoD IT
- DoDI 8580.1 Information Assurance (IA) in the Defense Acquisition System
- *RMF Knowledge Service*
- MOA between DoD CIO and ODNI CIO Establishing Net-Centric Software Licensing Agreements
- DODAF (Version 2.02) DoD Architecture Framework
- DTM 20-004 Enabling Cyberspace Accountability of DoD Components and Information Systems
- Common Criteria Evaluation and Validation Scheme (CCEVS)
- CJCSI 5123.01H Charter of the JROC and Implementation of the JCID
- Joint Publication 6-0 Joint Communications System

Develop the Workforce

- NIST SP 800-181 R1 Workforce Framework for Cybersecurity
- CNSSD-500 Information Assurance (IA) Education, Training, and Awareness
- NSTISSD-501 National Training Program for INFOSEC Professionals
- CNSSD-504 Protecting National Security Systems from Insider Threat
- CNSSI-4000 Maintenance of Communications Security (COMSEC) Equipment
- NSTISSI-4011 National Training Standard for INFOSEC Professionals
- CNSSI-4012 National IA Training Standard for Senior Systems Managers
- CNSSI-4013 National IA Training Standard For System Administrators (SA)
- CNSSI-4014 National IA Training Standard For Information Systems Security Officers
- NSTISSI-4015 National Training Standard for System Certifiers
- CNSSI-4016 National IA Training Standard For Risk Analysts
- DoDD 8140.01 Cyberspace Workforce Management
- DoDM 8570.09 Cryptologic Accreditation and Certification
- DoD 8570.01-M Information Assurance Workforce Improvement Program

Partner for Strength

- NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing
- NIST SP 800-171, R2 Protecting CUI in Nonfederal Systems and Organizations
- NIST SP 800-172 Enhanced Security Requirements for Protecting CUI
- CNSSP-14 National Policy Governing the Release of IA Products/Services...
- CNSSI-4008 Program for the Mgt and Use of Nat'l Reserve IA Security Equipment
- DoDI 5205.13 Defense Industrial Base (DIB) Cyber Security (CS) / IA Activities
- *DoDM O-5205.13 DIB CS/IA Program Security Classification Manual*
- DoD 5220.22-M, Ch. 2 National Industrial Security Program Operating Manual (NISPOM)
- Cybersecurity Maturity Model Certification (CMMC)
- MOA Between DoD and DHS (Jan. 19, 2017)

ENABLE

Secure Data in Transit

- FIPS 140-3 Security Requirements for Cryptographic Modules
- NIST SP 800-153 Guidelines for Securing Wireless Local Area Networks
- CNSSP-1 National Policy for Safeguarding and Control of COMSEC Material
- CNSSP-15 Use of Pub Standards for Secure Sharing of Info Among NSS
- CNSSP-17 Policy on Wireless Communications: Protecting Nat'l Security Info
- CNSSP-19 National Policy Governing the Use of HAIPE Products
- CNSSP-25 National Policy for PKI in National Security Systems
- NSTISSP-101 National Policy on Securing Voice Communications
- *NACSI-2005 Communications Security (COMSEC) End Item Modification*
- CNSSI-5000 Voice Over Internet Protocol (VoIP) Computer Telephony (Annex I, VoSIP)
- CNSSI-5001 Type-Acceptance Program for VoIP Telephones
- NACSI-6002 Nat'l COMSEC Instruction Protection of Gov't Contractor Telecomm's
- CNSSI-7003 Protected Distribution Systems (PDS)
- DoDD 8100.02 Use of Commercial Wireless Devices, Services, and Tech in the DoD GIG
- DoDD 8521.01E Department of Defense Biometrics
- DoDI 4650.01 Policy and Procedures for Mgt and Use of the Electromagnetic Spectrum
- DoDI 8100.04 DoD Unified Capabilities (UC)
- DoDI 8420.01 Commercial WLAN Devices, Systems, and Technologies
- DoDI 8523.01 Communications Security (COMSEC)
- DoDI S-5200.16 Objectives and Min Stds for COMSEC Measures used in NC2 Comms
- *CJCSI 6510.02E Cryptographic Modernization Plan*
- *CJCSI 6510.06C Communications Security Releases to Foreign Nations*

Manage Access

- HSPD-12 Policy for a Common ID Standard for Federal Employees and Contractors
- FIPS 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors
- NIST SP 800-207 Zero Trust Architecture
- NIST SP 800-210 General Access Control Guidance for Cloud Systems
- NIST SP 1800-16 Securing Web Transactions: TLS Server Certificate Management
- CNSSP-3 National Policy for Granting Access to Classified Cryptographic Information
- CNSSP-10 Nat'l Policy Gov. Use of Approved Sec. Containers in Info Security Applications
- CNSSP-16 National Policy for the Destruction of COMSEC Paper Material
- CNSSD-507 National Directive for ICAM Capabilities
- CNSSD-506 National Directive to Implement PKI on Secret Networks
- CNSSI-1300 Instructions for NSS PKI X.509
- NSTISSI-3028 Operational Security Doctrine for the FORTEZZA User PCMCIA Card
- CNSSI-4001 Controlled Cryptographic Items
- CNSSI-4003 Reporting and Evaluating COMSEC Incidents
- CNSSI-4005 Safeguarding COMSEC Facilities and Materials, amended by CNSS-008-14
- CNSSI-4006 Controlling Authorities for COMSEC Material
- DoDI 1000.25 DoD Personnel Identity Protection (PIP) Program
- DoDI 5200.01 DoD Information Security Program and Protection of SCI
- DoDI 5200.08 Security of DoD Installations and Resources and the DoD PSRB
- DoDI 5200.48 Controlled Unclassified Information(CUI)
- DoDI 8520.02 Public Key Infrastructure (PKI) and Public Key (PK) Enabling
- DoDI 8520.03 Identity Authentication for Information Systems
- DoDM 1000.13, Vol. 1 DoD ID Cards: ID Card Life-cycle
- DoDM 5205.02 DoD Operations Security (OPSEC) Program Manual

Assure Information Sharing

- CNSSP-24 Policy on Assured Info Sharing (AIS) for National Security Systems(NSS)
- DoDI 8170.01 Online Information Management and Electronic Messaging
- DoDI 8320.02 Sharing Data, Info, and IT Services in the DoD
- DoDI 8582.01 Security of Non-DoD Info Sys Processing Unclassified Nonpublic DoD Information
- CJCSI 3213.01D, Joint Operations Security
- CJCSI 6211.02D Defense Information System Network: (DISN) Responsibilities

ANTICIPATE

Understand the Battlespace

- FIPS 199 Standards for Security Categorization of Federal Info. and Info. Systems
- NIST SP 800-59 Guideline for Identifying an Information System as a NSS
- NIST SP 800-60, Vol 1, R1 Guide for Mapping Types of Info and Info Systems to Security Categories
- NIST SP 800-92 Guide to Computer Security Log Management
- NISTIR 7693 Specification for Asset Identification 1.1
- CNSSD-520 Use of Mobile Devices to Process Nat'l Sec.Info Outside Secure Spaces
- CNSSP-28 Cybersecurity of Unmanned National Security Systems
- DoDI S-5240.23 Counterintelligence (CI) Activities in Cyberspace

Prevent and Delay Attackers and Prevent Attackers from Staying

- FIPS 200 Minimum Security Requirements for Federal Information Systems
- NIST SP 800-37 R2 Guide for Applying the Risk Mgt Framework to Fed. Info. Systems
- NIST SP 800-53 R5 Security & Privacy Controls for Federal Information Systems
- NIST SP 800-53A R4 Assessing Security & Privacy Controls in Fed. Info. Systems & Orgs.
- NIST SP 800-61, R2 Computer Security Incident Handling Guide
- NIST SP 800-124, R1 Guidelines for Managing the Security of Mobile Devices in the Enterprise
- NIST SP 800-128 Guide for Security-Focused Configuration Mgt of Info Systems
- NIST SP 800-163, R1 Vetting the Security of Mobile Applications
- NIST SP 1800-26 Data Integrity: Detecting & Responding to Ransomware
- CNSSI-1011 Implementing Host-Based Security Capabilities on NSS
- CNSSI-1013 Network Intrusion Detection Sys & Intrusion Prevention Sys (IDS/IPS)
- CNSSI-1253 Security Categorization and Control Selection for Nat'l Security Systems
- CNSSI-1253F, Atchs 1-5 Security Overlays
- CNSSAM IA 1-10, Reducing Risk of Removable Media in NSS
- DoDI 5200.39 CPI Identification and Protection within RDT&E
- DoDI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations
- DoDI 8551.01 Ports, Protocols, and Services Management (PPSM)
- DoDM 5105.21V1, SCI Admin Security Manual: Info and Info Sys Security
- CJCSI 6510.01F Information Assurance (IA) and Computer Network Defense (CND)
- *CJCSM 6510.02 IA Vulnerability Mgt Program*
- DTM 17-007, Ch. 2, Defense Support to Cyber Incident Response
- CJCSM 6510.01B Cyber Incident Handling Program

ABOUT THIS CHART

- This chart organizes cybersecurity policies and guidance by Strategic Goal and Office of Primary Responsibility (see Color Key). Double-clicking" on the box directs users to the most authoritative publicly accessible source.
- *Policies in italics indicate the document is marked for limited distribution or no authoritative public-facing hyperlink is currently available.*
- The linked sites are not controlled by the developers of this chart. We regularly check the integrity of the links, but you may occasionally experience an error message due to problems at the source site or the site's decision to move the document. Please let us know if you believe the link is no longer valid.
- CNSS policies link only to the CNSS site.
- Boxes with red borders reflect recent updates.
- "Note: It is best to open this PDF directly in a browser. However, if you are unable to open the links directly from this PDF document, place your cursor over the target box and right-click to copy the link location. Open a web browser and paste the copied link into the address bar.
- For the latest version of this chart or email alerts to updates go to https://dodiac.dtic.mil/dod-cybersecurity-policy-chart/

PREPARE

Develop and Maintain Trust

- CNSSP-12 National IA Policy for Space Systems Used to Support NSS
- CNSSP-21 National IA Policy on Enterprise Architecture for NSS
- NIST 800-160, vol.1, Systems Security Engineering: ... Engineering of Trustworthy Secure Systems
- CNSSI-5002, Telephony Isolation Used for Unified Comms. Implementations w/ in Physically Protected Spaces
- DoDD 3020.40 Mission Assurance
- DoDD 3100.10 Space Policy

Strengthen Cyber Readiness

- NIST SP 800-18, R1 Guide for Developing Security Plans for Federal Information Systems
- NIST SP 800-30, R1 Guide for Conducting Risk Assessments
- NIST SP 800-126, R3 SCAP Ver. 1.3
- NIST SP 800-137 Continuous Monitoring
- NIST SP 800-39 Managing Information Security Risk
- NIST SP 1800-25 Data Integrity: Identifying and Protecting Assets Against Ransomware
- CNSSD-505 Supply Chain Risk Management
- CNSSD-520 The Use of Mobile Devices to Process National Security Information Outside...
- DoDD 3700.01 DoD Command and Control (C2) Enabling Capabilities
- *DoDD S-3710.01 National Leadership Command Capability*
- DoDD 5101.21E Unified Platform and Joint Cyber Command and Control (JOC2)
- DoDI 8500.01 Cybersecurity
- DoDI 8560.01 COMSEC Monitoring
- Joint Special Access Program (SAP) Implementation Guide (JSIG)

Sustain Missions

- NIST SP 800-34, R1 Contingency Planning Guide for Federal Information Systems
- NIST SP 800-82, R2 Guide to Industrial Control Systems (ICS) Security
- *CNSSP-18 National Policy on Classified Information Spillage*
- CNSSP-22, IA Risk Management Policy for National Security Systems
- *CNSSP-300 National Policy on Control of Compromising Emanations*
- *CNSSI-1001 National Instruction on Classified Information Spillage*
- *CNSSI-4004.1, Destruction and Emergency Protection Procedures for COMSEC and Class. Material*
- CNSSI-4007 Communications Security (COMSEC) Utility Program
- *CNSSI-7000 TEMPEST Countermeasures for Facilities*
- *NSTISSI-7001 NONSTOP Countermeasures*
- DoDD 3020.26 DoD Continuity Policy
- DoDD 3020.44 Defense Crisis Management
- DoDD 5144.02 DoD Chief Information Officer
- DoDD 8000.01 Management of the DOD Information Enterprise
- DoDD 5000.83 Technology & Program Protection to Maintain Technological Advantage
- DoDI 8410.02 NetOps for the Global Information Grid (GIG)
- ICD 503 IT Systems Security Risk Management and C&A
- UFC 4-010-06, Cybersecurity of Facility-Related Control Systems
- *NSA IA Directorate (IAD) Management Directive MD-110 Cryptographic Key Protection*
- Defense Acquisition Guidebook Program Protection

Color Key - OPRs

- ASD(NII)/ASD(C3I)/DOD CIO
- NIST
- USD(I&S)
- CNSS/NSTISS
- NSA
- USD(P)
- DISA
- OSD
- USD(P&R)
- DNI
- CYBERCOM
- Other Agencies
- JCS
- USD(A&S)
- Recently updated policy and/or link Expired; Update pending
- NIAP
- USD(C)

AUTHORITIES

- Title 10, US Code Armed Forces (§§2224, 3013(b), 5013(b), 8013(b))
- Title 14, US Code Cooperation With Other Agencies (Ch. 7)
- Title 32, US Code National Guard (§102)
- Title 40, US Code Public Buildings, Property, and Works (Ch. 113: §§11302, 11315, 11331)
- Title 44, US Code Federal Information Security Mod. Act, (Chapter 35)
- Title 50. US Code War and National Defense (§§3002, 1801)
- Clinger-Cohen Act, Pub. L. 104-106
- UCP Unified Command Plan (US Constitution Art II, Title 10 & 50)

NATIONAL / FEDERAL

- Computer Fraud and Abuse Act Title 18 (§1030)
- Federal Wiretap Act Title 18 (§2510 et seq.)
- Stored Communications Act Title 18 (§2701 et seq.)
- Pen Registers and Trap and Trace Devices Title 18 (§3121 et seq.)
- Foreign Intelligence Surveillance Act Title 50 (§1801 et seq)
- Executive Order 13231 as Amended by EO 13286 - Critical Infrastructure Protection in the Info Age
- Executive Order 13526 Classified National Security Information
- Executive Order 13587 Structural Reforms To Improve Classified Nets
- Executive Order 13691 Promoting Private Sector Cybersecurity Information Sharing
- EO 13636: Improving Critical Infrastructure Cybersecurity
- EO 13800: Strengthening Cybersecurity of Fed Nets and CI
- NSD 42, National Policy for the Security of Nat'l Security Telecom and Information Systems
- EO 13873: Securing the Information and Communications Technology and Services Supply Chain
- Executive Order on Improving the Nation's Cybersecurity
- *NSPD 54 / HSPD 23 Computer Security and Monitoring*
- PPD 21: Critical Infrastructure Security and Resilience
- PPD 41: United States Cyber Incident Coordination
- PPD 28, Signals Intelligence Activities
- FAR Federal Acquisition Regulation
- A-130, Management of Fed Info Resources
- National Strategy to Secure Cyberspace
- Ethics Regulations
- NIST Special Publication 800-Series
- NIST SP 800-63 series Digital Identity Guidelines
- NIST SP 800-88, R1,Guidelines for Media Sanitization
- NIST SP 800-101, R1 Guidelines on Mobile Device Forensics
- NIST SP 800-125A, R1, Security Recommendations for Hypervisor Platforms
- NIST SP 800-209 Security Guidelines for Storage Infrastructure
- NISTIR 7298, R3, Glossary of Key Information Security Terms
- CNSSD-502 National Directive On Security of National Security Systems
- CNSSD-900, Governing Procedures of the Committee on National Security Systems
- CNSSD-901 Nat'l Security Telecomm and Info Sys Security (CNSS) Issuance System
- CNSSI-4009 Cmte on National Security Systems Glossary
- DoD Information Technology Environment Strategic Plan

OPERATIONAL

- *CYBERCOM Orders*
- *JFHQ-DODIN Orders*

SUBORDINATE POLICY

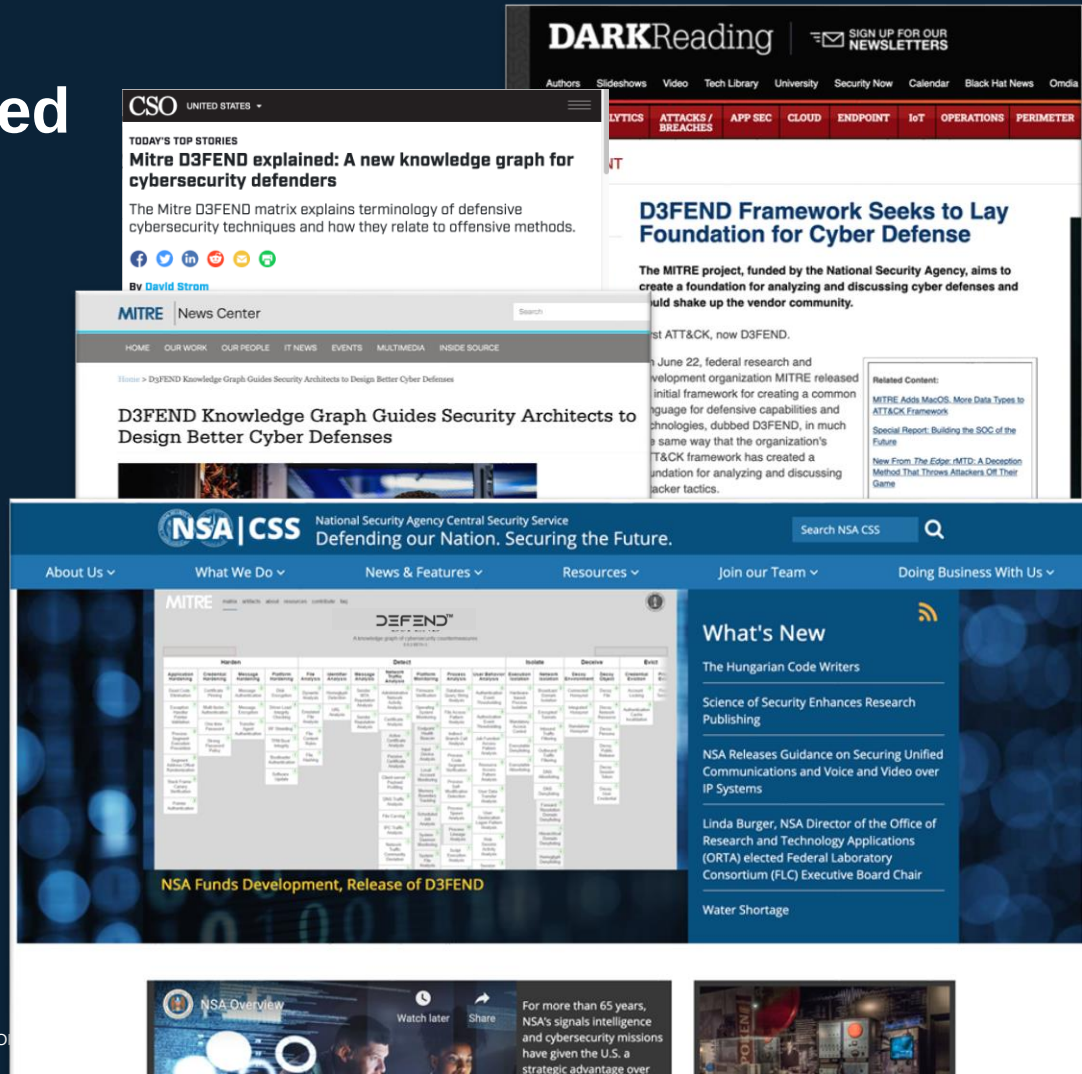
- Security Configuration Guides (SCGs)
- *Component-level Policy (Directives, Instructions, Publications, Memoranda)*
- NSA IA Guidance
- Security Technical Implementation Guides (STIGs)

D3FEND Publicly Released

- MITRE & NSA launch D3FEND
- https://d3fend.mitre.org
- Picked up by numerous media outlets
- 50K+ unique visitors to website in first week
- *Strong positive response to ontological modeling approach*

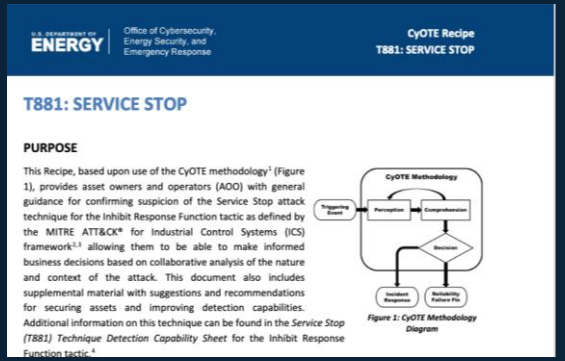
Links:

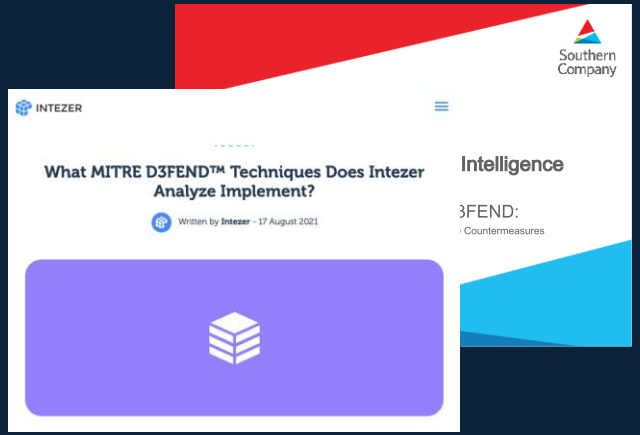
- nsa.gov article
- mitre.org article

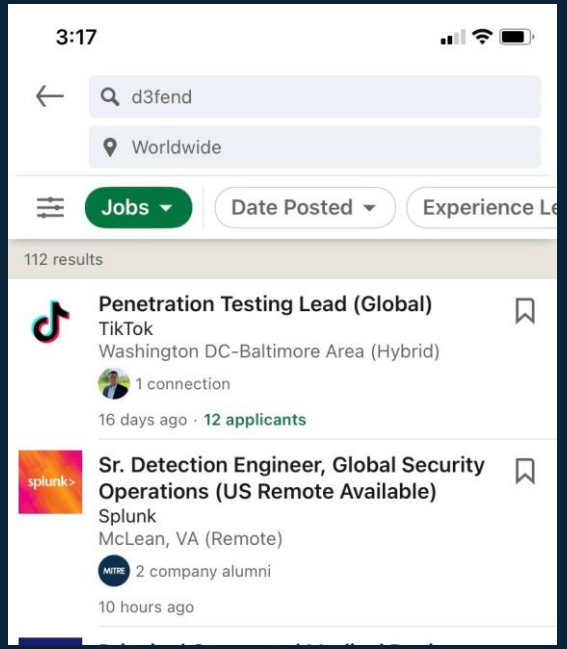


Impact

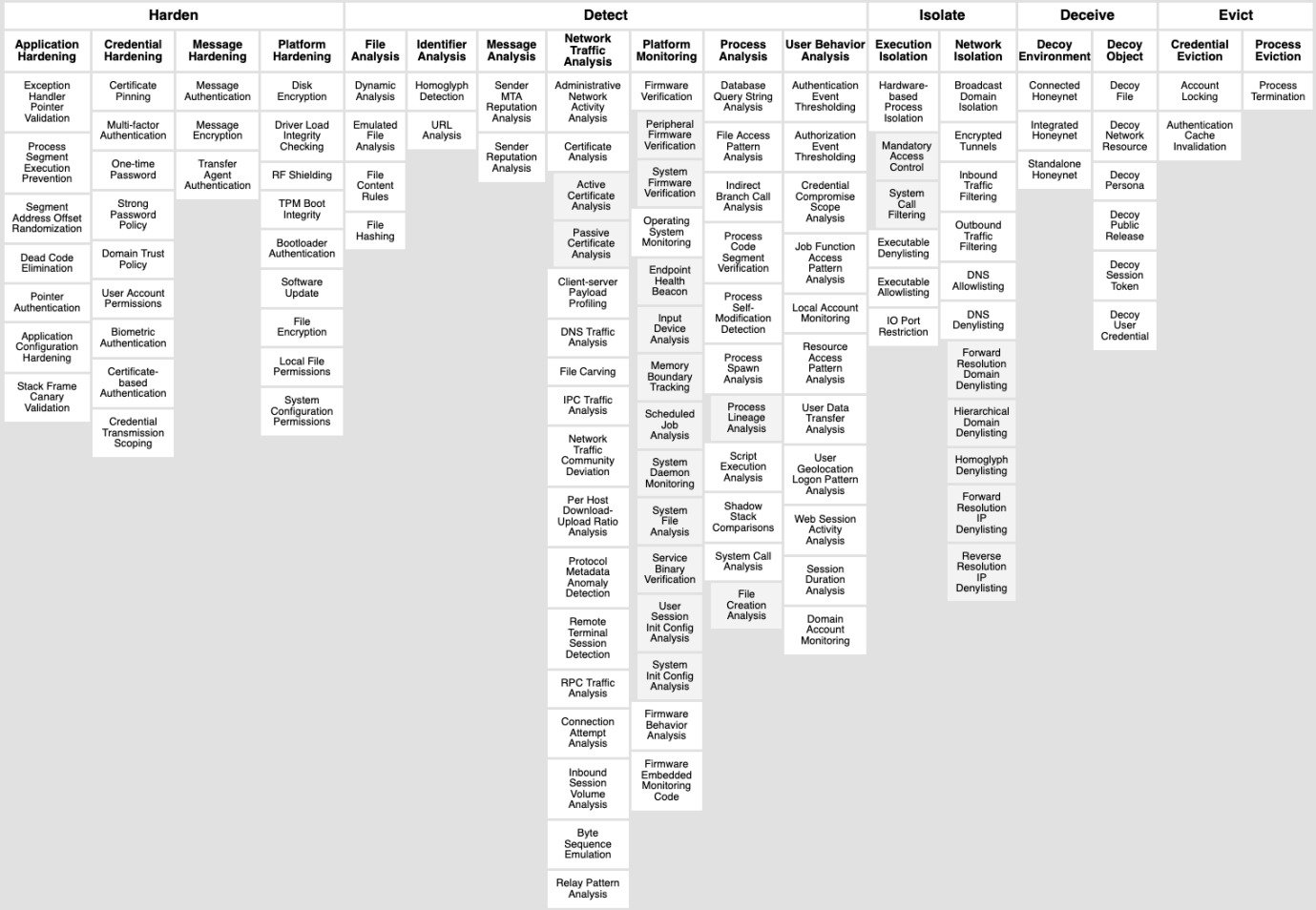
- NSA using D3FEND in public reporting to prescribe defenses against China's cyber attacks
- NSA TBCS transition improved capability analysis efficiency
- Advanced modeling applications for USAF; 50% improvement in threat coverage
- DOE CyOTE project recommends countermeasures
- Critical infrastructure commercial companies identified gaps in their security capabilities
- Vendors beginning to map to D3FEND
- D3FEND Paper Cited by over 13 academic papers in less than one year
- > 100 Job postings want D3FEND familiarity & knowledge



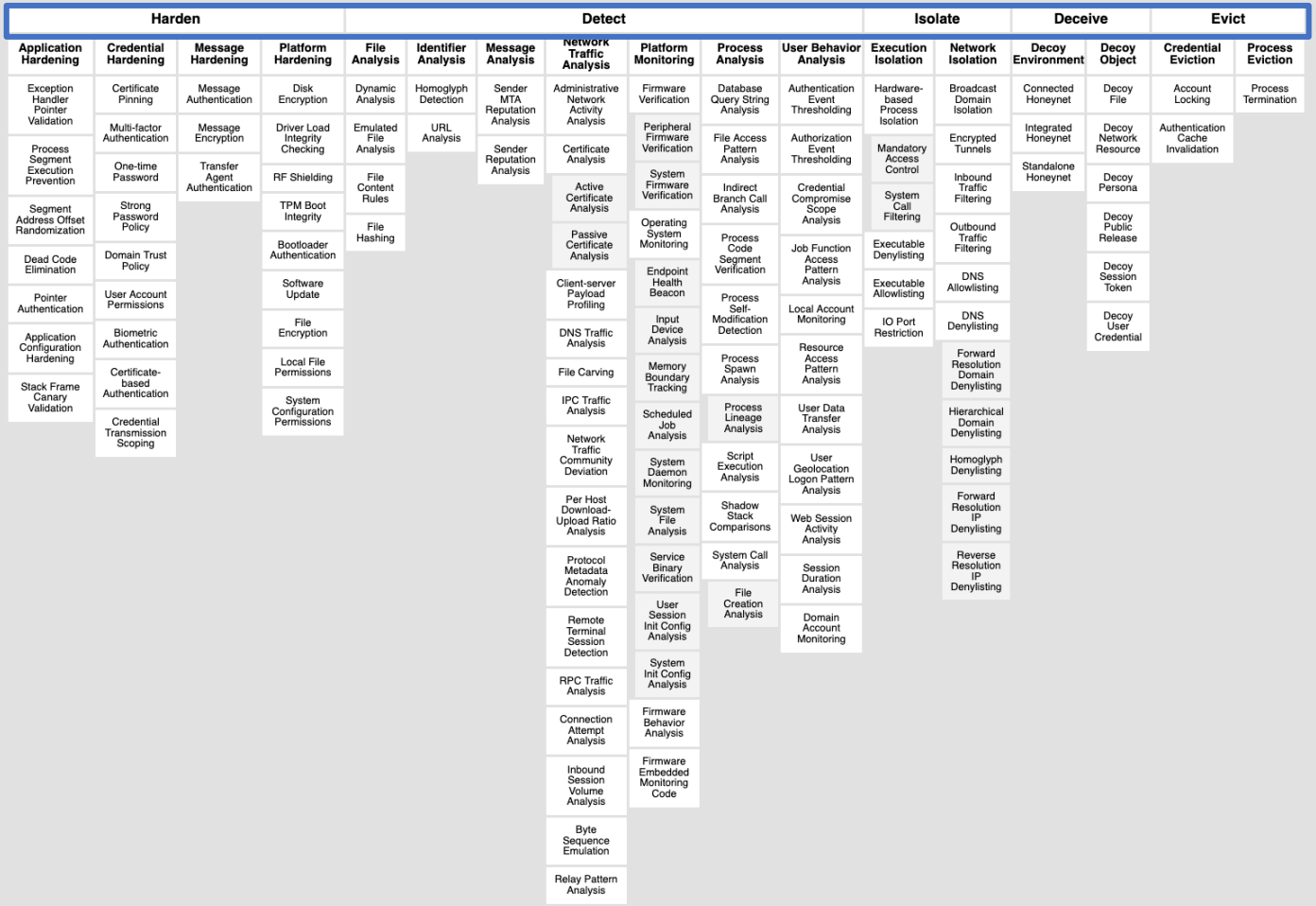




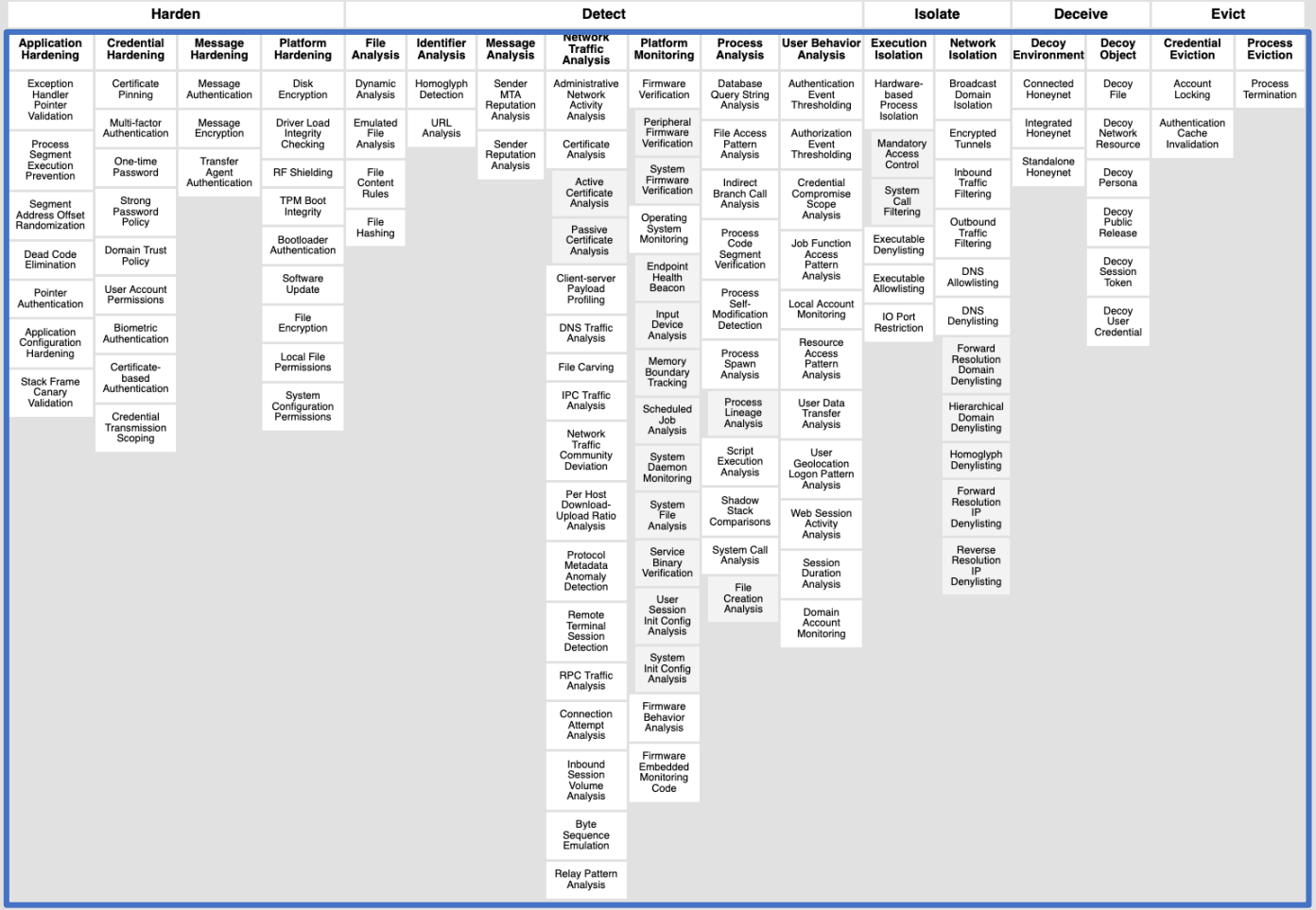
DEFEND™

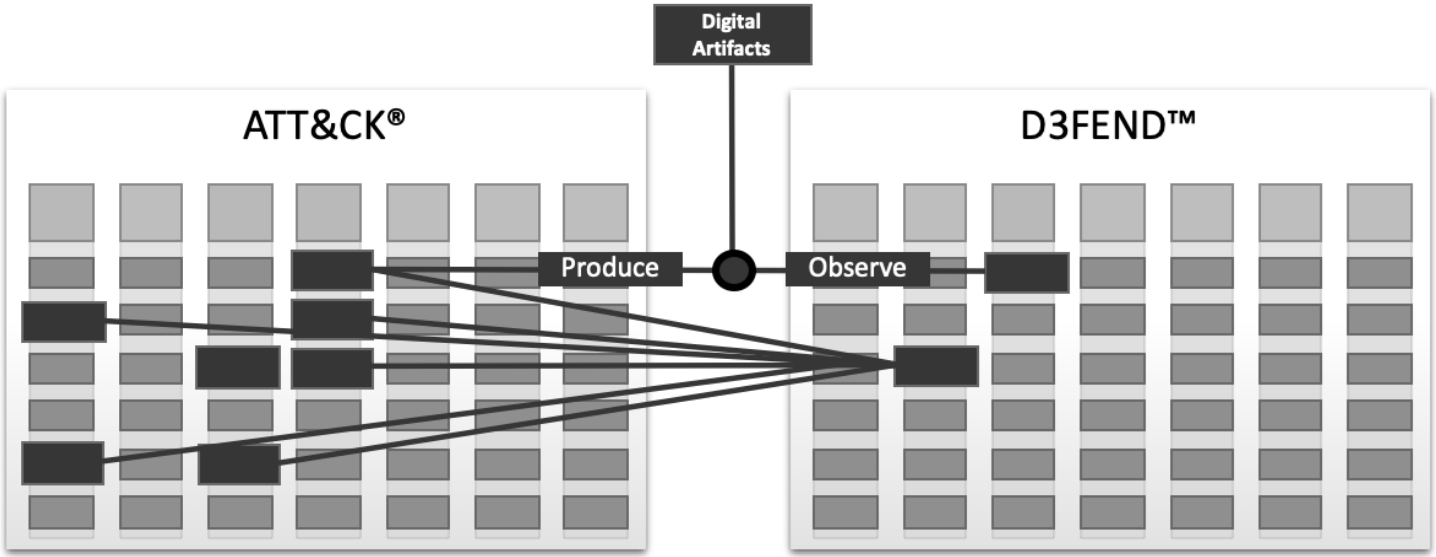

Harden
Application Hardening
Exception Handler Pointer Validation
Process Segment Execution Prevention
Segment Address Offset Randomization
Dead Code Elimination
Pointer Authentication
Application Configuration Hardening
Stack Frame Canary Validation
Credential Hardening
Certificate Pinning
Multi-factor Authentication
One-time Password
Strong Password Policy
Domain Trust Policy
User Account Permissions
Biometric Authentication
Certificate-based Authentication
Credential Transmission Scoping
Message Hardening
Message Authentication
Message Encryption
Transfer Agent Authentication
Platform Hardening
Disk Encryption
Driver Load Integrity Checking
RF Shielding
TPM Boot Integrity
Bootloader Authentication
Software Update
File Encryption
Local File Permissions
System Configuration Permissions
Detect
File Analysis
Dynamic Analysis
Emulated File Analysis
File Content Rules
File Hashing
Identifier Analysis
Homoglyph Detection
URL Analysis
Message Analysis
Sender MTA Reputation Analysis
Sender Reputation Analysis
Network Traffic Analysis
Administrative Network Activity Analysis
Certificate Analysis
Active Certificate Analysis
Passive Certificate Analysis
Client-server Payload Profiling
DNS Traffic Analysis
File Carving
IPC Traffic Analysis
Network Traffic Community Deviation
Per Host Download-Upload Ratio Analysis
Protocol Metadata Anomaly Detection
Remote Terminal Session Detection
RPC Traffic Analysis
Connection Attempt Analysis
Inbound Session Volume Analysis
Byte Sequence Emulation
Relay Pattern Analysis
Platform Monitoring
Firmware Verification
Peripheral Firmware Verification
System Firmware Verification
Operating System Monitoring
Endpoint Health Beacon
Input Device Analysis
Memory Boundary Tracking
Scheduled Job Analysis
System Daemon Monitoring
System File Analysis
Service Binary Verification
User Session Init Config Analysis
System Init Config Analysis
Firmware Behavior Analysis
Firmware Embedded Monitoring Code
Process Analysis
Database Query String Analysis
File Access Pattern Analysis
Indirect Branch Call Analysis
Process Code Segment Verification
Process Self-Modification Detection
Process Spawn Analysis
Process Lineage Analysis
Script Execution Analysis
Shadow Stack Comparisons
System Call Analysis
File Creation Analysis
User Behavior Analysis
Authentication Event Thresholding
Authorization Event Thresholding
Credential Compromise Scope Analysis
Job Function Access Pattern Analysis
Local Account Monitoring
Resource Access Pattern Analysis
User Data Transfer Analysis
User Geolocation Logon Pattern Analysis
Web Session Activity Analysis
Session Duration Analysis
Domain Account Monitoring
Isolate
Execution Isolation
Hardware-based Process Isolation
Mandatory Access Control
System Call Filtering
Executable Denylisting
Executable Allowlisting
IO Port Restriction
Network Isolation
Broadcast Domain Isolation
Encrypted Tunnels
Inbound Traffic Filtering
Outbound Traffic Filtering
DNS Allowlisting
DNS Denylisting
Forward Resolution Domain Denylisting
Hierarchical Domain Denylisting
Homoglyph Denylisting
Forward Resolution IP Denylisting
Reverse Resolution IP Denylisting
Deceive
Decoy Environment
Connected Honeynet
Integrated Honeynet
Standalone Honeynet
Decoy Object
Decoy File
Decoy Network Resource
Decoy Persona
Decoy Public Release
Decoy Session Token
Decoy User Credential
Evict
Credential Eviction
Account Locking
Authentication Cache Invalidation
Process Eviction
Process Termination

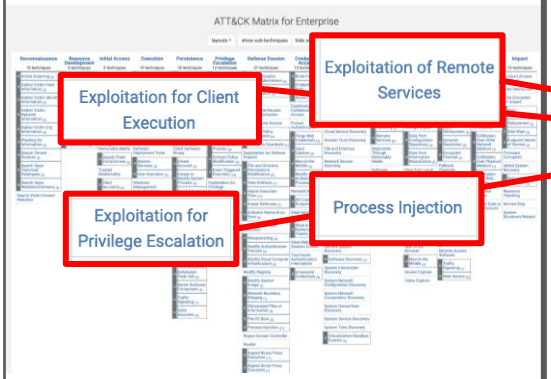
D3FEND™


Harden
Application Hardening
Exception Handler Pointer Validation
Process Segment Execution Prevention
Segment Address Offset Randomization
Dead Code Elimination
Pointer Authentication
Application Configuration Hardening
Stack Frame Canary Validation
Credential Hardening
Certificate Pinning
Multi-factor Authentication
One-time Password
Strong Password Policy
Domain Trust Policy
User Account Permissions
Biometric Authentication
Certificate-based Authentication
Credential Transmission Scoping
Message Hardening
Message Authentication
Message Encryption
Transfer Agent Authentication
Platform Hardening
Disk Encryption
Driver Load Integrity Checking
RF Shielding
TPM Boot Integrity
Bootloader Authentication
Software Update
File Encryption
Local File Permissions
System Configuration Permissions
Detect
File Analysis
Dynamic Analysis
Emulated File Analysis
File Content Rules
File Hashing
Identifier Analysis
Homoglyph Detection
URL Analysis
Message Analysis
Sender MTA Reputation Analysis
Sender Reputation Analysis
Network Traffic Analysis
Administrative Network Activity Analysis
Certificate Analysis
Active Certificate Analysis
Passive Certificate Analysis
Client-server Payload Profiling
DNS Traffic Analysis
File Carving
IPC Traffic Analysis
Network Traffic Community Deviation
Per Host Download-Upload Ratio Analysis
Protocol Metadata Anomaly Detection
Remote Terminal Session Detection
RPC Traffic Analysis
Connection Attempt Analysis
Inbound Session Volume Analysis
Byte Sequence Emulation
Relay Pattern Analysis
Platform Monitoring
Firmware Verification
Peripheral Firmware Verification
System Firmware Verification
Operating System Monitoring
Endpoint Health Beacon
Input Device Analysis
Memory Boundary Tracking
Scheduled Job Analysis
System Daemon Monitoring
System File Analysis
Service Binary Verification
User Session Init Config Analysis
System Init Config Analysis
Firmware Behavior Analysis
Firmware Embedded Monitoring Code
Process Analysis
Database Query String Analysis
File Access Pattern Analysis
Indirect Branch Call Analysis
Process Code Segment Verification
Process Self-Modification Detection
Process Spawn Analysis
Process Lineage Analysis
Script Execution Analysis
Shadow Stack Comparisons
System Call Analysis
File Creation Analysis
User Behavior Analysis
Authentication Event Thresholding
Authorization Event Thresholding
Credential Compromise Scope Analysis
Job Function Access Pattern Analysis
Local Account Monitoring
Resource Access Pattern Analysis
User Data Transfer Analysis
User Geolocation Logon Pattern Analysis
Web Session Activity Analysis
Session Duration Analysis
Domain Account Monitoring
Isolate
Execution Isolation
Hardware-based Process Isolation
Mandatory Access Control
System Call Filtering
Executable Denylisting
Executable Allowlisting
IO Port Restriction
Network Isolation
Broadcast Domain Isolation
Encrypted Tunnels
Inbound Traffic Filtering
Outbound Traffic Filtering
DNS Allowlisting
DNS Denylisting
Forward Resolution Domain Denylisting
Hierarchical Domain Denylisting
Homoglyph Denylisting
Forward Resolution IP Denylisting
Reverse Resolution IP Denylisting
Deceive
Decoy Environment
Connected Honeynet
Integrated Honeynet
Standalone Honeynet
Decoy Object
Decoy File
Decoy Network Resource
Decoy Persona
Decoy Public Release
Decoy Session Token
Decoy User Credential
Evict
Credential Eviction
Account Locking
Authentication Cache Invalidation
Process Eviction
Process Termination

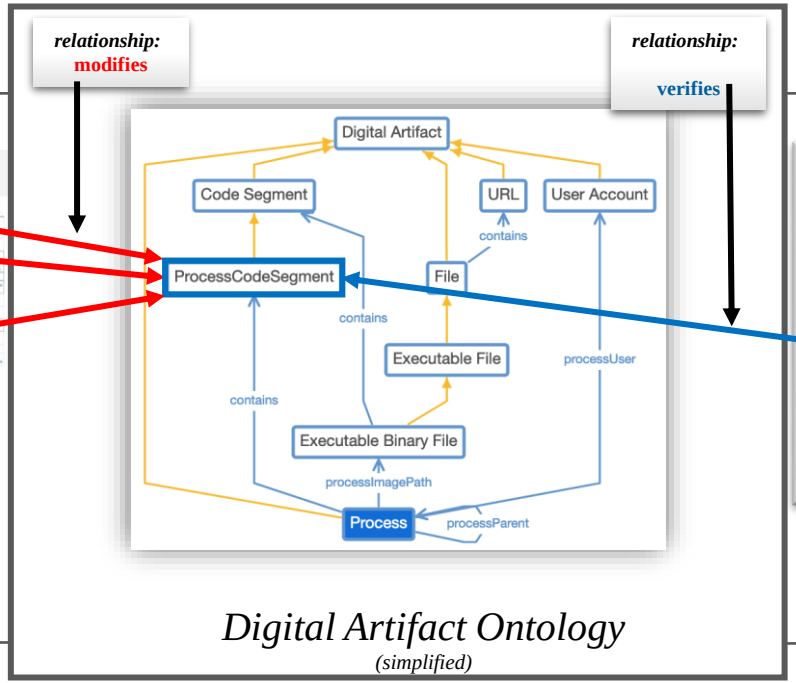
DEFEND™


Harden
Application Hardening
Exception Handler Pointer Validation
Process Segment Execution Prevention
Segment Address Offset Randomization
Dead Code Elimination
Pointer Authentication
Application Configuration Hardening
Stack Frame Canary Validation
Credential Hardening
Certificate Pinning
Multi-factor Authentication
One-time Password
Strong Password Policy
Domain Trust Policy
User Account Permissions
Biometric Authentication
Certificate-based Authentication
Credential Transmission Scoping
Message Hardening
Message Authentication
Message Encryption
Transfer Agent Authentication
Platform Hardening
Disk Encryption
Driver Load Integrity Checking
RF Shielding
TPM Boot Integrity
Bootloader Authentication
Software Update
File Encryption
Local File Permissions
System Configuration Permissions
Detect
File Analysis
Dynamic Analysis
Emulated File Analysis
File Content Rules
File Hashing
Identifier Analysis
Homoglyph Detection
URL Analysis
Message Analysis
Sender MTA Reputation Analysis
Sender Reputation Analysis
Network Traffic Analysis
Administrative Network Activity Analysis
Certificate Analysis
Active Certificate Analysis
Passive Certificate Analysis
Client-server Payload Profiling
DNS Traffic Analysis
File Carving
IPC Traffic Analysis
Network Traffic Community Deviation
Per Host Download-Upload Ratio Analysis
Protocol Metadata Anomaly Detection
Remote Terminal Session Detection
RPC Traffic Analysis
Connection Attempt Analysis
Inbound Session Volume Analysis
Byte Sequence Emulation
Relay Pattern Analysis
Platform Monitoring
Firmware Verification
Peripheral Firmware Verification
System Firmware Verification
Operating System Monitoring
Endpoint Health Beacon
Input Device Analysis
Memory Boundary Tracking
Scheduled Job Analysis
System Daemon Monitoring
System File Analysis
Service Binary Verification
User Session Init Config Analysis
System Init Config Analysis
Firmware Behavior Analysis
Firmware Embedded Monitoring Code
Process Analysis
Database Query String Analysis
File Access Pattern Analysis
Indirect Branch Call Analysis
Process Code Segment Verification
Process Self-Modification Detection
Process Spawn Analysis
Process Lineage Analysis
Script Execution Analysis
Shadow Stack Comparisons
System Call Analysis
File Creation Analysis
User Behavior Analysis
Authentication Event Thresholding
Authorization Event Thresholding
Credential Compromise Scope Analysis
Job Function Access Pattern Analysis
Local Account Monitoring
Resource Access Pattern Analysis
User Data Transfer Analysis
User Geolocation Logon Pattern Analysis
Web Session Activity Analysis
Session Duration Analysis
Domain Account Monitoring
Isolate
Execution Isolation
Hardware-based Process Isolation
Mandatory Access Control
System Call Filtering
Executable Denylisting
Executable Allowlisting
IO Port Restriction
Network Isolation
Broadcast Domain Isolation
Encrypted Tunnels
Inbound Traffic Filtering
Outbound Traffic Filtering
DNS Allowlisting
DNS Denylisting
Forward Resolution Domain Denylisting
Hierarchical Domain Denylisting
Homoglyph Denylisting
Forward Resolution IP Denylisting
Reverse Resolution IP Denylisting
Deceive
Decoy Environment
Connected Honeynet
Integrated Honeynet
Standalone Honeynet
Decoy Object
Decoy File
Decoy Network Resource
Decoy Persona
Decoy Public Release
Decoy Session Token
Decoy User Credential
Evict
Credential Eviction
Account Locking
Authentication Cache Invalidation
Process Eviction
Process Termination

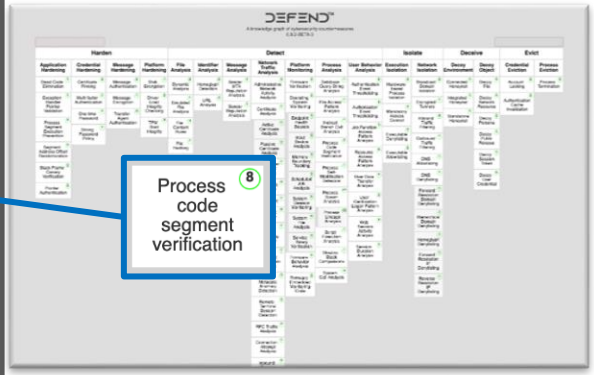




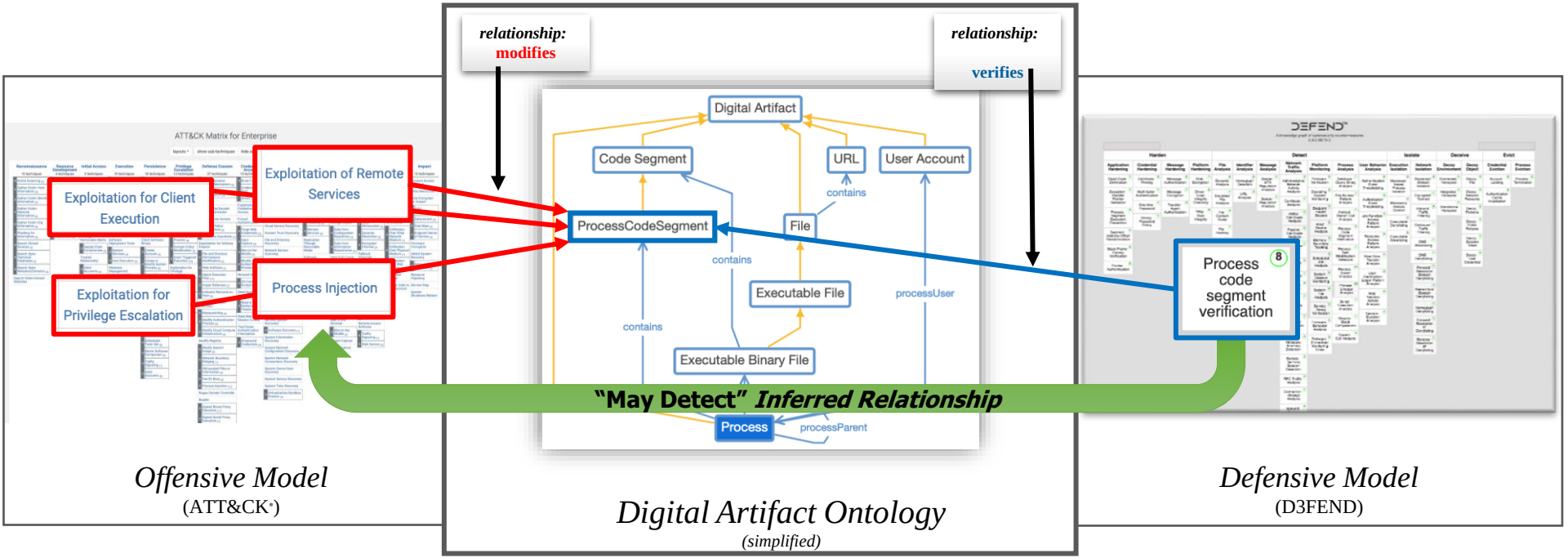
Offensive Model
(ATT&CK®)



Digital Artifact Ontology
(simplified)



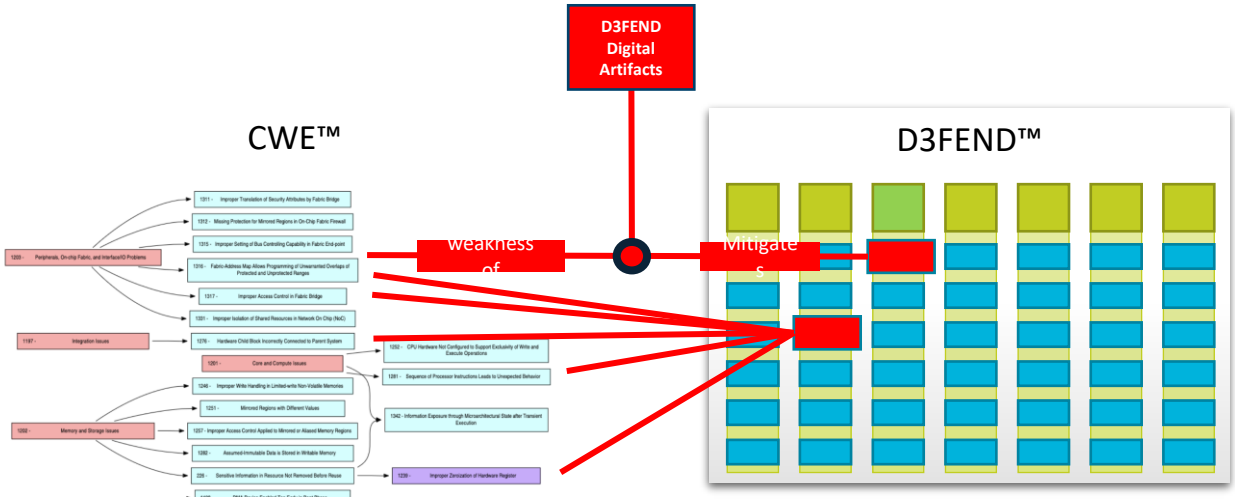
Defensive Model
(D3FEND)

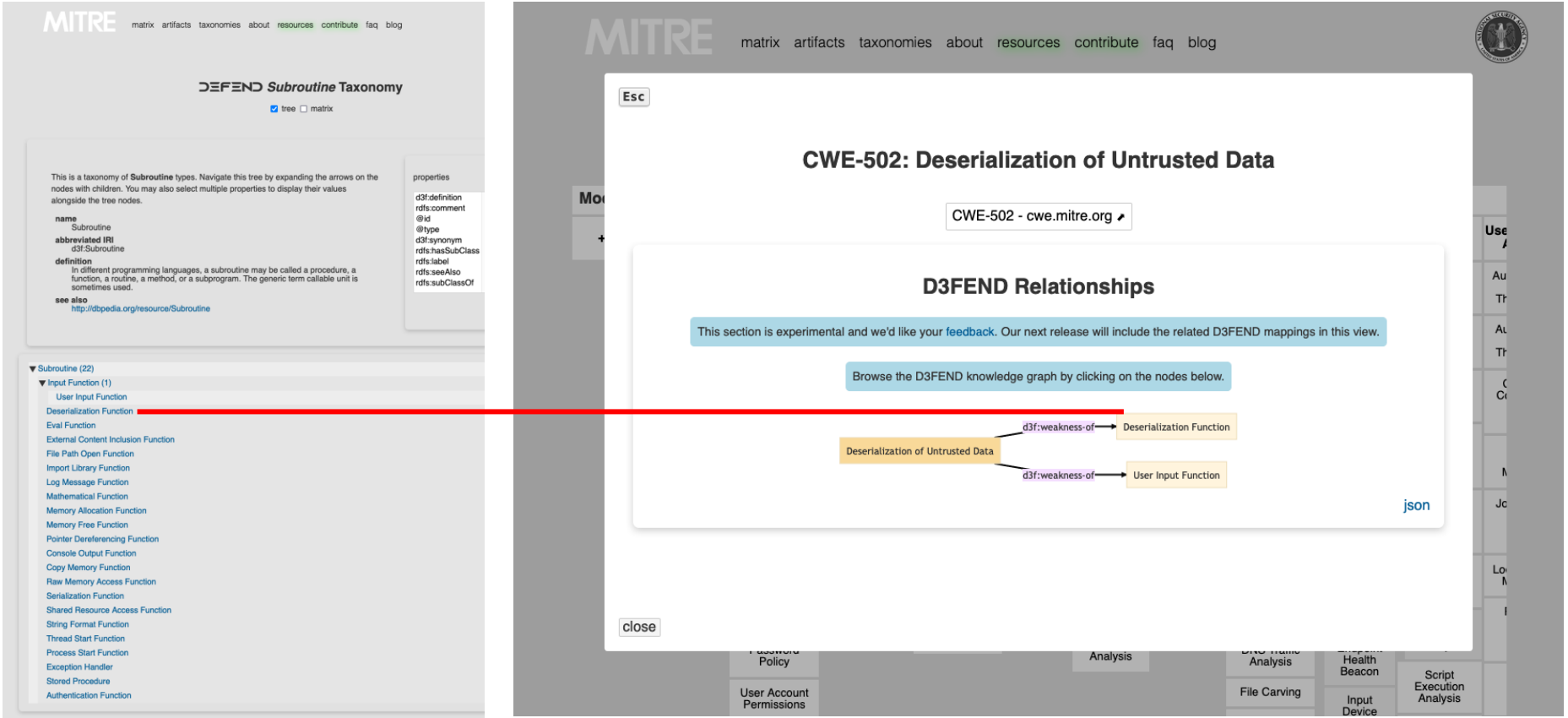


Offensive Model
(ATT&CK®)

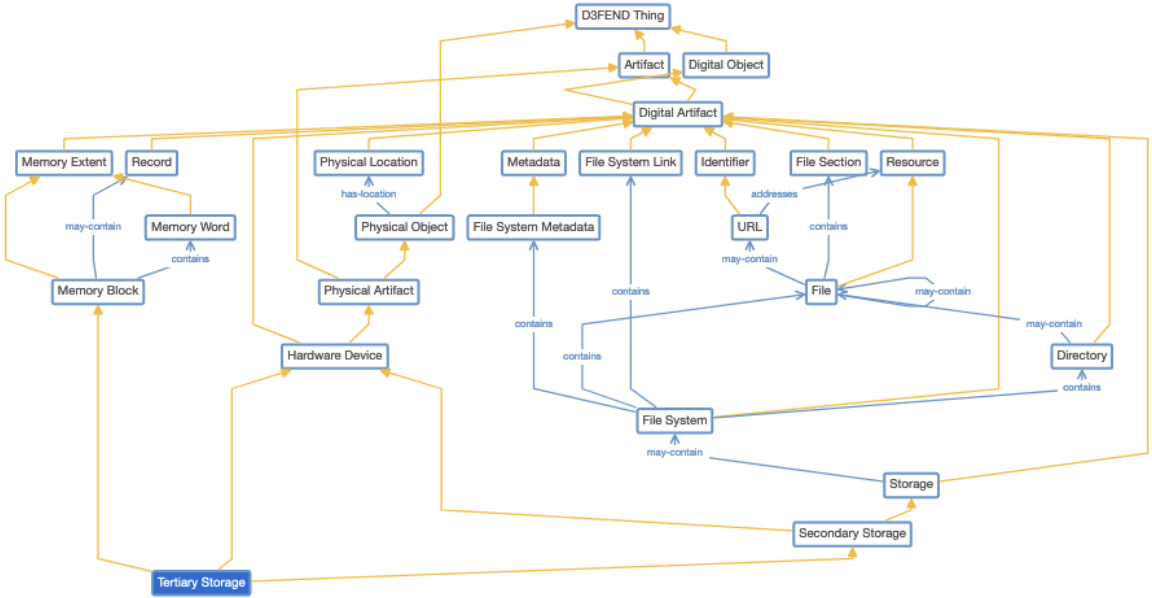
Digital Artifact Ontology
(simplified)

Defensive Model
(D3FEND)





Hardware Ontology



D3FEND Hardware Ontology GitHub Discussion:

https://github.com/d3fend/d3fend-ontology/discussions/181

MITRE

How to get involved

- Ask vendors what D3FEND techniques they support
- Think in terms of “Digital Artifacts” and “Defensive Verbs”
- Browse the knowledge base at https://d3fend.mitre.org
- If you are interested in the ontology, download Protégé to view the model
- Send ideas, and comments to d3fend@mitre.org
- Join our slack channel (link on D3FEND Resources page)
- Extend or contribute to D3FEND at https://github.com/d3fend/

MITRE

CVE QWG Hardware and Software Tagging
Jason F

HW CWE CONTENT ENHANCEMENT PROPOSALS

Jason M. Fung

June 9, 2023

CVE Root Cause Tagging Proposal

CVE Root Cause Tagging Proposal
Motivation

- Many CVEs filed every year; but current CVE schema does not offer a way to query those with hardware root causes
- Best if CVEs are tagged based on SW or HW root causes
- Potential Use Cases
  - **Correctness:** Monitor new CVEs with HW root causes and ensure correct CWEs are assigned
  - **Awareness:** Offer a data-driven approach to curate the next Most Important Hardware Weakness list
  - …

CVE Root Cause Tagging Proposal
Proposal Submitted to CVE Quality WG in March'21

- Proposal to add a tag to CVE schema for identifying the root cause
  - In collaboration with Chris Turner and Jason Oberg

We previously discussed including support for CVE level tags (which can be applied to the CNA or ADP containers) that assist in identification of root cause.

Tag	Definition
Hardware Root Cause	Tag this to a CVE if the primary root cause of the security vulnerability is originated from the hardware component of the affected product(s). The intent is to facilitate Hardware Designers to learn how to prevent similar weakness. Even when a hardware vulnerability can be addressed by a SW workaround, the "Hardware Root Cause" tag should still be applied, since the focus is on how the issue is introduced, not how it is remediated.
Software Root Cause	Tag this to a CVE if the primary root cause of the security vulnerability is originated from the software component of the affected product(s). The intent is to facilitate Software Developers to learn how to prevent similar weakness.

CVE Root Cause Tagging Proposal
Proposal Reviewed by CVE Quality WG in May'23

- CVE QWG agreed with the direction, but members initially had a difference in opinions on the implementation options
  - Should the tag be per CVE Record or per CWE?
    - Each CVE can support more than 1 "Problem Types" or CWE mappings
  - How to draw the line between HW vs. SW?
    - See next slide
- CVE QWG agreed to create a record-level experimental tag for root cause, and later promote to an official tag based on usage and feedback

CVE Root Cause Tagging Proposal
DISCUSSION: HOW TO DRAW THE LINE BETWEEN HW VS. SW?

- By position in the compute stack?
  - IP – SoC – Motherboard – BIOS – VM – OS – Driver – Apps
- By storage (anything in hard disk is SW)?
- By patchability?
  - HW = Circuit + Logic + BootROM
  - SW = Embedded FW and above
- By a fixed mapping/classification?
- By how it is implemented (C vs. RTL)?
- By security implications?
  - SW = FW with buffer overflow error
  - HW = FW misconfigures access control policy in HW
- …

Demonstrative Example Enhancement Proposal

Reusing Corpus from HACK@EVENT Hardware CTF Competitions

Demonstrative Example Enhancement Proposal OVERVIEW

- CWEs with demonstrative examples help readers better appreciate how design and implementation issues manifest in RTL
  - However, not many HW CWEs have code examples today
- HACK@EVENT is a series of Pre-Si HW capture-the-flag competitions created by Intel (Arun Kanuparthi, Hareesh Khattri), Texas A&M and TU Darmstadt in the past 6 years
  - We take a complex open source SoC, insert industry-like security features, and inject security vulnerabilities that mimic mistakes made by hardware designers to form a buggy SoC for the competition.
  - Participants have 48 hours to examine the buggy SoC to find as many vulnerabilities as they can. Through the process, participants get to realize how hardware vulnerabilities captured in HW CWE are being manifested in real hardware, and limitations of today's EDA tools to support robust product security assurance.
  - Through gamification, we inspire talents to contribute towards hardware security.
- Idea: Buggy code from past competitions can be reused to serve as Demonstrative Examples for HW CWE

Demonstrative Example Enhancement Proposal

CWE-1281: SEQUENCE OF PROCESSOR INSTRUCTIONS LEADS TO UNEXPECTED BEHAVIOR

HW CWE: CWE-1281
Example Language: SystemVerilog
CWE Issue Description (from Website):
Specific combinations of processor instructions lead to undesirable behavior such as locking the processor until a hard reset performed.
If the instruction set architecture (ISA) and processor logic are not designed carefully and tested thoroughly, certain combinations of instructions may lead to locking the processor or other unexpected and undesirable behavior. Upon encountering unimplemented instruction opcodes or illegal instruction operands, the processor should throw an exception and carry on without negatively impacting security. However, specific combinations of legal and illegal instructions may cause unexpected behavior with security implications such as allowing unprivileged programs to completely lock the CPU.

Example Description:
The example code is taken from the commit stage inside the processor core of the HACK@DAC'19 buggy CVA6 SoC. To ensure the correct execution of atomic instructions, the CPU must guarantee atomicity: no other device overwrites the memory location between the atomic read starts and the atomic write finishes. Another device may overwrite the memory location only before the read operation or after the write operation, but never between them, and finally, the content will still be consistent.
Atomicity is especially critical when the variable to be modified is a mutex, counting semaphore, or similar piece of data that controls access to shared resources. Failure to ensure atomicity may result in two processors accessing a shared resource simultaneously, permanent lock-up, or similar disastrous behavior.
The following vulnerable code check for CSR interrupts and give them precedence over any other exception. However, the interrupts should not occur when the processor runs a series of atomic instructions. In the following vulnerable code, the required check must be included to ensure the processor is not in the middle of a series of atomic instructions. For more info, please check the Fixed code example.

Vulnerable Code:

Example Language: SystemVerilog — bad code

```
if (csr_exception_i.valid && csr_exception_i.cause[63] && commit_instr_i[0].fu != CSR) begin
        exception_o = csr_exception_i;
        exception_o.tval = commit_instr_i[0].ex.tval;
end
```

Vulnerable Code Source:
https://github.com/PouyaMahmoody/hackdac_2019/blob/main/src/commit_stage.sv
line 287-290

Mitigation Description:
Refrain from interrupting if we are committing an atomic instruction that should not be interrupted. We can do that by adding a condition to check whether the current committing instruction is atomic.

Fixed code:

Example Language: SystemVerilog — good code

```
if (csr_exception_i.valid && csr_exception_i.cause[63] && !amo_valid_commit_o
&& commit_instr_i[0].fu != CSR) begin
        exception_o = csr_exception_i;
        exception_o.tval = commit_instr_i[0].ex.tval;
end
```

Fixed code Source:
https://github.com/openhwgroup/cva6/blob/7951802a0147aedb21e8f2f6dc1e1e9c4ee857a2/src/commit_stage.sv#L296:L301
line 296-301

Demonstrative Example Enhancement Proposal

CWE-1260: IMPROPER HANDLING OF OVERLAP BETWEEN PROTECTED MEMORY RANGES

HW CWE: CWE-1260
Example Language: SystemVerilog
CWE Issue Description (from Website):
The product allows address regions to overlap, which can result in the bypassing of intended memory protection.

Isolated memory regions and access control (read/write) policies are used by hardware to protect privileged software. Software components are often allowed to change or remap memory region definitions in order to enable flexible and dynamically changeable memory management by system software.

If a software component running at lower privilege can program a memory address region to overlap with other memory regions used by software running at higher privilege, privilege escalation may be available to attackers. The memory protection unit (MPU) logic can incorrectly handle such an address overlap and allow the lower-privilege software to read or write into the protected memory region, resulting in a privilege escalation attack. An address overlap weakness can also be used to launch a denial of service attack on the higher-privilege software memory regions.

Example Description:
The example code below is taken from the IOMMU controller module of the HACK@DAC'19 buggy CVA6 SoC. The static memory map is composed of a set of Memory-Mapped Input/Output (MMIO) regions covering different IP agents within the SoC. Each region is defined by two 64-bit variables representing the base address and size of the memory region (XXXBase and XXXLength). In this example (see the vulnerable code source), we have 12 IP agents, and only 4 of them are called out for illustration purposes in the code snippets. Access to the AES IP MMIO region is considered privileged as it provides access to AES secret key, internal states, or decrypted data. The vulnerable code allows the overlap between the protected MMIO region of the AES peripheral and the unprotected UART MMIO region. As a result, unprivileged users can access the protected region of the AES IP.
In the given vulnerable example UART MMIO region starts at address 64'h1000_0000 and ends at address 64'h1011_1000 (*UARTBase* is 64'h1000_0000, and the size of the region is provided by the *UARTLength* of 64'h0011_1000). On the other hand, the AES MMIO region starts at address 64'h1010_0000 and ends at address 64'h1010_1000, which implies an overlap between the two peripherals' memory regions. Thus, any user with access to the UART can read or write the AES MMIO region, e.g., the AES secret key.

Vulnerable Code:

Example Language: SystemVerilog — bad code

```
...
  localparam logic[63:0] PLICLength    = 64'h03FF_FFFF;
  localparam logic[63:0] UARTLength    = 64'h0011_1000;
  localparam logic[63:0] AESLength     = 64'h0000_1000;
  localparam logic[63:0] SPILength     = 64'h0080_0000;
...
  typedef enum logic [63:0] {
    ...
    PLICBase    = 64'h0C00_0000,
    UARTBase    = 64'h1000_0000,
    AESBase     = 64'h1010_0000,
    SPIBase     = 64'h2000_0000,
    ...
```

Vulnerable Code Source:
https://github.com/PouyaMahmoody/hackdac_2019/blob/main/tb/ariane_soc_pkg.sv
line 44-45, 61-62

Mitigation Description:
Remove the overlapping address regions by decreasing the size of the UART memory region (as shown in the good code example) or adjusting memory bases for all the remaining peripherals.

Fixed code:

Example Language: SystemVerilog — good code

```
...
  localparam logic[63:0] PLICLength    = 64'h03FF_FFFF;
  localparam logic[63:0] UARTLength    = 64'h0000_1000;
  localparam logic[63:0] AESLength     = 64'h0000_1000;
  localparam logic[63:0] SPILength     = 64'h0080_0000;
...
  typedef enum logic [63:0] {
    ...
    PLICBase    = 64'h0C00_0000,
    UARTBase    = 64'h1000_0000,
    AESBase     = 64'h1010_0000,
    SPIBase     = 64'h2000_0000,
    ...
```

Fixed code Source:
https://github.com/openhwgroup/cva6/blob/v4.2.0/tb/ariane_soc_pkg.sv
Line 45

Demonstrative Example Enhancement Proposal

HACK@DAC'19 OFFERS 21 EXAMPLES COVERING 13 UNIQUE HW CWES

Location	CWE-Description	# of Existing Prescriptive Examples	# of Existing Code Examples
ACC CTRL	CWE-1317: Improper Access Control in Fabric Bridge	1	0
AES	CWE-1262: Improper Access Control for Register Interface	1	0
ACC CTRL	CWE-1260: Improper Handling of Overlap Between Protected Memory Ranges	1	0
BOOTROM	CWE-1326: Missing Immutable Root of Trust in Hardware	1	0
JTAG	CWE-276: Incorrect Default Permissions	0	0
ACC CTRL	CWE-1262: Improper Access Control for Register Interface	1	0
CPU-Interrupt Controller	CWE-1220: Insufficient Granularity of Access Control	2	0
AES	CWE-1262: Improper Access Control for Register Interface	1	0
ACC CTRL	CWE-276: Incorrect Default Permissions	0	0
JTAG	CWE-1244: Internal Asset Exposed to Unsafe Debug Access Level or State	1	0
AES	CWE-1262: Improper Access Control for Register Interface	1	0
JTAG	CWE-1221: Incorrect Register Defaults or Module Parameters	0	1
AES	CWE-1241: Use of Predictable Algorithm in Random Number Generator	1	0
CPU-Interrupt Controller	CWE-1281: Sequence of Processor Instructions Leads to Unexpected Behavior	1	0
CPU-Commit Stage	CWE-1281: Sequence of Processor Instructions Leads to Unexpected Behavior	1	0
CPU-Comm			
CPU-Addr			
CPU-Address Translation	CWE-1262: Improper Access Control for Register Interface	1	0
CPU-Address Translation	CWE-226: Sensitive Information in Resource Not Removed Before Reuse	2 (not HW)	0
JTAG	CWE-1191: On-Chip Debug and Test Interface With Improper Access Control	1	0
JTAG	CWE-1243: Sensitive Non-Volatile Information Not Protected During Debug	1	0

HACK@DAC'19 and HACK@DAC'21 cover 38 unique HW CWEs

Becoming a CNA
Alec S

CVE Numbering Authority (CNA) Information and Requirements

June 9, 2023

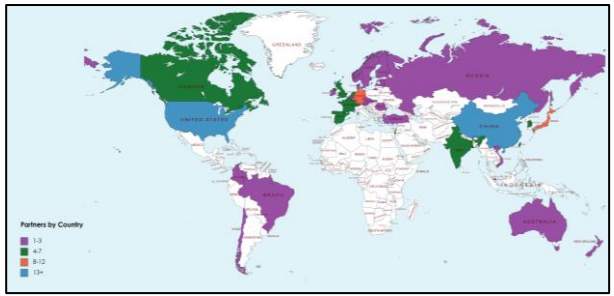
HSSEDI
Homeland Security Systems Engineering & Development Institute™

What is a CVE Numbering Authority (CNA)?

- **CVE Numbering Authority (CNA):** Organizations from around the world who are authorized by the CVE Program to assign CVE IDs and publish CVE Records for vulnerabilities within their distinct, agreed-upon scope.
  - Types of organizations include vendors, researchers, open source, CERTs, hosted services, bug bounty providers, and consortiums, but others are also welcome.

Strategy of Federation in Action

As of June 1, 2023:
295 Partners in 36 countries



Federated Growth Strategy Implemented

Federation Through Partnership: Impact by the Numbers

Year	Records Published	Number of CNAs
2016	6,457	24 (1 Int.)
2017	14,644	78
2018	16,510	90
2019	17,308	106
2020	18,364	144
2021	20,161	209 (100 Int.)
2022	25,059	263 (123 Int.)
2023	[illegible]5	295 (136 Int.)

*Note: 57 CNAs Added, to-date in FY 2023

Year	1999-2016	2017	2018	2019	2020	2021	2022	2023
All CNAs	0%	50%	53%	53%	58%	65%	68%	77%
CNA-LRs	100%	50%	47%	47%	42%	35%	32%	23%

*Note: CISA ICS became a Top-Level Root and CNA-LR in calendar year 2020

Benefits of Becoming a CNA

- **Demonstrate mature vulnerability management practices and commitment to cybersecurity**
- **Communicate value-added vulnerability information**
  - You are the subject matter experts and can provide the most accurate vulnerability description
- **Control the CVE publication release process for vulnerabilities within scope**
- **Assign CVE IDs without having to share embargoed information with another CNA**
- **Streamline vulnerability disclosure processes**

Cost of Being a CNA

- **There is no monetary fee; however, CVE Records are not free to produce (i.e., time and resource allocation)**
  - Estimated minimum Level of Effort: 8 hours per month (up to 10 CVE Records)
- **CNAs volunteer their own time for their own benefit**
- **No contract to sign**

Requirements for becoming a CNA

- **Have a public vulnerability disclosure policy* (e.g., Microsoft)**
- **Have a public advisory location (e.g., Apple)**
- **Agree to the CVE Program Terms of Use**

Please visit https://www.cve.org/PartnerInformation/ListofPartners for examples of other disclosure policies and advisory locations.

Process for Becoming a CNA (1 of 2)

- **Request information on how to become a CNA via the CVE Program webform here**
  - Select "Request information on the CVE Numbering Authority (CNA) Program" from the dropdown menu
- **Your request will be assigned to someone on the Program Coordination team, who will provide a link to the registration form and supplemental material**
  - CNA Rules
  - Onboarding videos
- **Once registration form is received, a one-hour onboarding session will be scheduled**
  - Public vulnerability disclosure policy is required (e.g., Microsoft)
  - Public source for vulnerability disclosures is required (e.g., Apple)
  - Choose Root (or Top-Level Root) based on scope
  - Define scope*

*Please visit https://www.cve.org/PartnerInformation/ListofPartners for examples of scopes.

Process for Becoming a CNA (2 of 2)

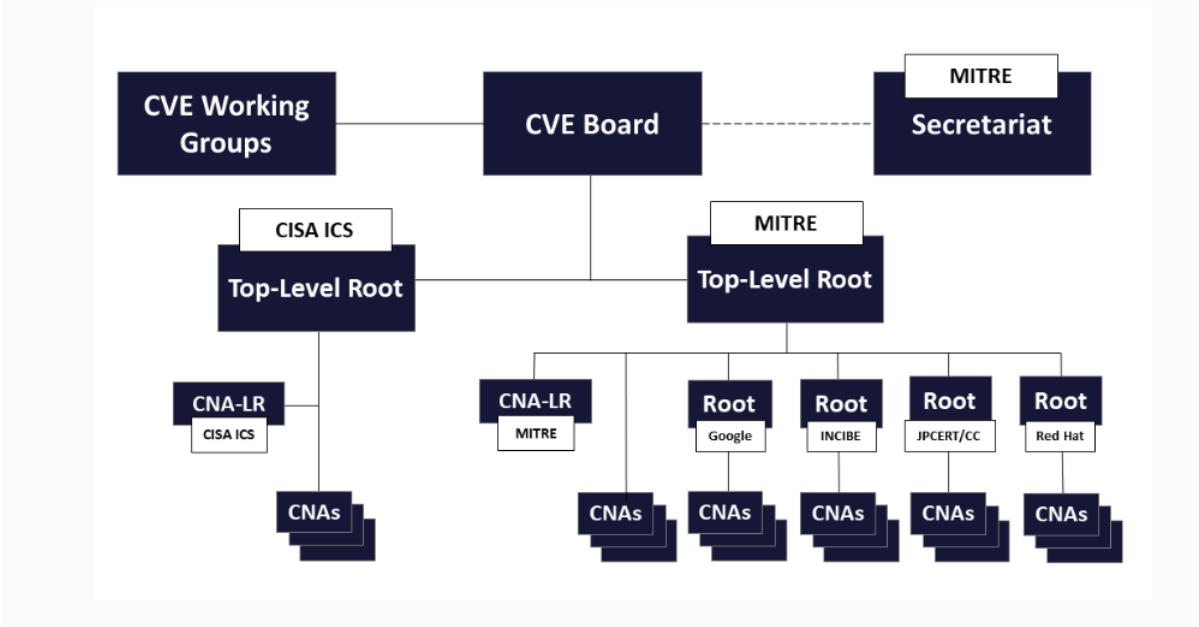
- **After onboarding session, you will be asked to complete and submit homework**
- **Once homework is submitted and approved, the CVE Program will work with you to select a date for announcement into the program**
- **After official announcement, CNA requests credentials to access CVE Services**
  - Request CVE IDs
  - Publish and update CVE Records

CVE Program Expectations of CNAs

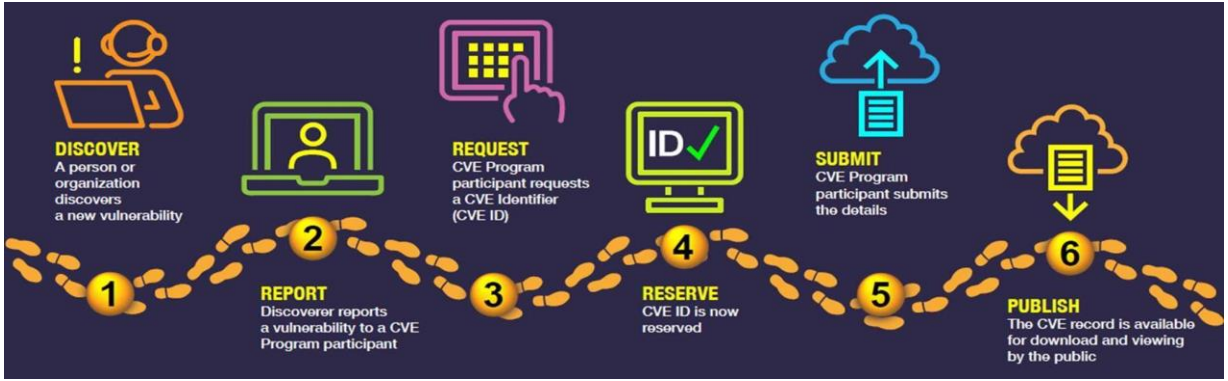
- **Follow the CNA Rules and the CVE Program Professional Code of Conduct**
- **Adhere to the CVE Program policies**
  - Record Dispute Policy
  - EOL Policy
- **Publish CVE Records in a timely manner once disclosure is made public**
  - Once the vulnerability (and associated CVE ID) is made **public** (via an advisory, Tweet, blog, etc.), CVE Records must be published to the CVE List within 5 business days
- **Respond to requests from Root (or Top-Level Root) in a timely manner**
- **Communicate any changes to CNA organization (POCs, mergers, change in scope) to Root or Top-Level Root**

Backup Slides

A Picture of CVE Program Organization



How CVE Works



- **Discover:** A person or organization discovers a new vulnerability (or a CNA finds a vulnerability in its own product)
- **Report:** Discoverer reports the vulnerability to a CVE Program participant (CNA)
  - CNA works with the discoverer and its internal security teams to validate and remediate the vulnerability
- **Request:** CNA requests a CVE Identifier (ID)
- **Reserve:** The ID is reserved (initial state of a CVE Record; not yet public)
- **Submit:** CNA submits the details
  - Details include, but are not limited to, affected product(s); affected or fixed product versions; vulnerability type, root cause, or impact; and at least one public reference
- **Publish:** Once the minimum required data elements are included in the CVE Record, and the vulnerability is publicly disclosed, it is published to the CVE List by the responsible CNA. The CVE Record is now available for download and viewing by the public.

Next Meeting (July 14)

CWE@MITRE.ORG

- **Mailing List:** *hw-cwe-special-interest-group-sig-list@mitre.org*
  - ***NOTE: All mailing list items are archived publicly at:***
    - *https://www.mail-archive.com/hw-cwe-special-interest-group-sig-list@mitre.org/*
- **What would members of this body like to see for the next HW SIG agenda?**
- **Questions, Requests to present? Please let us know.**

Backup

CWE-514: Covert Channel

Description

- A covert channel is a path that can be used to transfer information in a way not intended by the system's designers.

Extended Description

- Typically the system has not given authorization for the transmission and has no knowledge of its occurrence.

Covert Channels and Side Channels

- This is a discussion item on the GitHub
- Accidental transmission vs intentional transmission
- "A side channel is where information **leaks accidentally** via some medium that was not designed or intended for communication; a covert channel is where the **leak is deliberate**." – *Ross Anderson*
- Hardware view should have coverage in the hardware view –*Jason Oberg*
- CWE-514 is a class weakness for Covert Channels
- Covert Channels should be in the HW categories Security Flow Issues, General Circuit and Logic Design Concerns, or Debug and Test Problems. –*Paul Wortman*
- Should we place CWE-514 in the HW View? Or create a base of CWE-514 and put that into the HW view?