INF523: Assurance in Cyberspace Applied to Information Security

Student Case Studies (Part A)

Prof. Clifford Neuman

Lecture 13A
17 November 2020

Extra Session: Tuesday 17 November 1:00 PM – 4:20 PM PST

- Process Control and Medical Devices (40 min)
  - Medical Devices – Jaynee Shah
  - Industrial Control Systems - Venkat Ramana Reddy Mareddy
- The Cloud and Storage/Database Infrastructure (80 min)
  - Database Servers – Di Rama
  - Cloud Security - Shagun Bhatia
  - FedRamp - Dewaine Reddish
  - Risk Management - Sarahzin Chowdhury
- Isolation and Key Management (40 min)
  - Identity Tokens and Yubikey - Arjun G. Raman
  - Isolation Technologies - Ayush Ambastha

Extra Session Thursday 19 November 1:00 PM – 4:20 PM PST

Mobile Devices
- Mobile OS - Chinmaya Pandit and Harshit Kothari
- Android - Mohammed Ababtain

Payment
- Apple Pay - Jairo Hernandez
- Apple Pay and Google Pay - MaryLiza Walker
- Apple Pay - Shanice Williams
- Apple Pay - Yang Xue

Assurance in Payment Systems - Uddipt Sharma
- (this may be at end of Friday Session)

Friday November 20

Operating Systems

- Linux Applications - Aditya Goindi
- Linux - Tejas Pandey
- Chrome OS - Malavika Prabhakar

Infrastructure and Vehicle Control Systems

- US Voting Infrastructure - Anthony Cassar
- Autonomous Vehicles - Chris Samayoa
- Autonomous Vehicles - Amarbir Singh
- Connected and Automated Vehicles - Abhishek Tatti
- Tesla - Dwayne Robinson
- Avionics - Pratyush Prakhar

INF523: Assurance in Cyberspace Applied to Information Security

Student Case Studies (Part A)

Prof. Clifford Neuman

Lecture 13A
17 November 2020

Extra Session: Tuesday 17 November 1:00 PM – 4:20 PM PST

- Process Control and Medical Devices (40 min)
  - Medical Devices – Jaynee Shah
  - Industrial Control Systems - Venkat Ramana Reddy Mareddy
- The Cloud and Storage/Database Infrastructure (80 min)
  - Database Servers – Di Rama
  - Cloud Security - Shagun Bhatia
  - FedRamp - Dewaine Reddish
  - Risk Management - Sarahzin Chowdhury
- Isolation and Key Management (40 min)
  - Identity Tokens and Yubikey - Arjun G. Raman
  - Isolation Technologies - Ayush Ambastha

NETWORKED MEDICAL DEVICES

JAYNEE SHAH

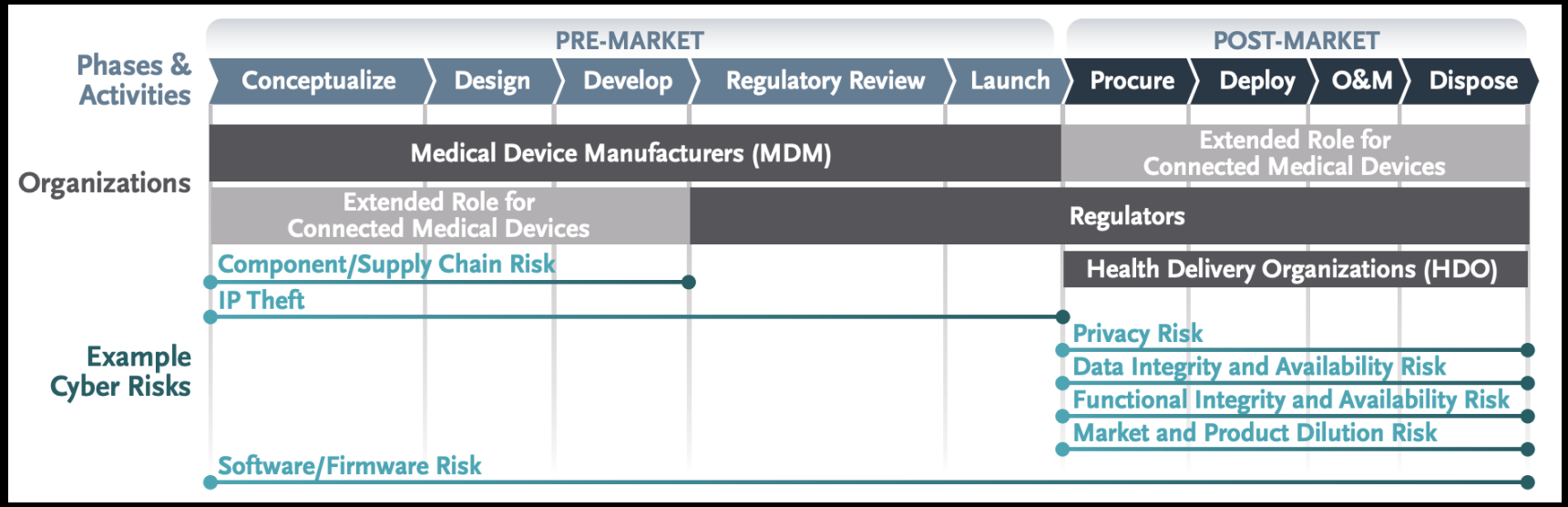
OUTLINE

- Introduction
- Regulations / Guidances
- Cybersecurity Measures
- OS in Healthcare Devices
- Securing Medical Devices
  - Reference Architecture - ISOSCELES
  - Platform Approach

INTRODUCTION

- A shared responsibility among healthcare facilities, patients, healthcare providers, and manufacturers of medical devices
- Attacker Goals:
  - Compromise healthcare network, Perform competitive analysis, Attack critical national infrastructure
- Major Security Problems and Challenges:
  - Malware, Secure updates, Passwords, Unauthorized access, Integrity, Privacy, Intellectual property (IP) protection
- Threats to Healthcare Sector and Medical Devices
  - Communication, Database injection, Replay, Spoofing or Impersonation, Social Engineering, Phishing, Malicious code, Denial of Service (DoS), Ransomware, Escalation of privileges, Physical destruction
- High assurance required for 'Protection of Human Life'

CONNECTED MEDICAL DEVICE LIFECYCLE



REGULATIONS

- FDA
  - FDA approval required to sell a medical device in the USA
  - Guidance:
    - Draft Guidance: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (Oct 2018)
    - Postmarket Management of Cybersecurity in Medical Devices (Dec 2016)
- UL 2900-2-1
  - Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems
  - Approved by ANSI (American National Standards Institute) and adopted by FDA
- AAMI TIR57: Principles for Medical Device Security - Risk Management (2016)
- Manufacturers Disclosure Statement for Medical Device Security (MDS2)
  - Manufacturers to disclose security related features of the medical device to healthcare providers
  - Required for any device that maintains or transmits data
- EU MDR 2017/745 - European Union Medical Device Regulation
- Common Concepts in all Regulations: Risk Management, Software Bill of Materials (SBOM), Monitoring, Communication, Total Product Lifecycle, Testing

FDA/UL GUIDANCE RECOMMENDATIONS

- Known Vulnerability Testing
  - National Vulnerability Database (NVD)
  - Testing software for vulnerabilities - product, third-party libraries, open-source libraries
- Malware Testing
  - Signature-based, behavior-based, anomaly-based approach
  - Testing for:
    - System/server on which software is deployed
    - Library or executable used
- Malformed Input Testing / Fuzzing
  - Fuzzing to test custom protocols
  - Mutational fuzzing - valid sample input, altering randomly
  - Generational fuzzing - use of state engine to generate input from scratch

FDA/UL GUIDANCE RECOMMENDATIONS

- Structured Penetration Testing
  - Manual, tool such as Burp
- Software Weakness Analysis
  - CWE Top 25, OWASP Top 10
- Static Source Code Analysis
  - Taint, data flow and control flow analysis
- Static Binary and Bytecode Analysis
  - Scanning compiler generated machine code
  - Scanning bytecode - computer object code
  - Deep binary analysis to catch backdoors, design flaws, implementation issues, configuration issues

CYBERSECURITY MEASURES

Secure by Design

- Build devices that are 'secure by design'
- Use of public key infrastructure (PKI) and digital certificates

Digital Certificates

- A unique digital certificate for each device
- Validates device authenticity
- Validates the integrity of messages sent to and from the device
- Client authentication certificate, Data encryption

Private key storage

- Store key hardware, use of Trusted Platform Module (TPM) or secure storage hardware
- TPM chip carries out cryptographic operations and secures keys/certificates

CYBERSECURITY MEASURES

Code Signing

- Code is digitally signed that validates its legitimate release
- Ensures code unchanged and uncorrupted since release
- Software or firmware update – verification of the signature using a digital certificate

Other

- Threat Modeling and Reducing Attack surface
- Secure Product Lifecycle
- Risk Management
  - Based on exploitability of vulnerability and severity of health impact to patients
  - Qualitative severity levels - Negligible / Minor / Serious / Critical / Catastrophic

OPERATING SYSTEM IN MEDICAL DEVICES

- What OS most medical devices use?
  - General purpose OS
    - Windows, Linux/Unix
  - RTOS
    - VxWorks, QNX, Windows Embedded Compact Edition (CE)
  - Microsoft Windows Embedded Standard
- Where is TCB?
  - Entire OS is trusted

Some Statistics

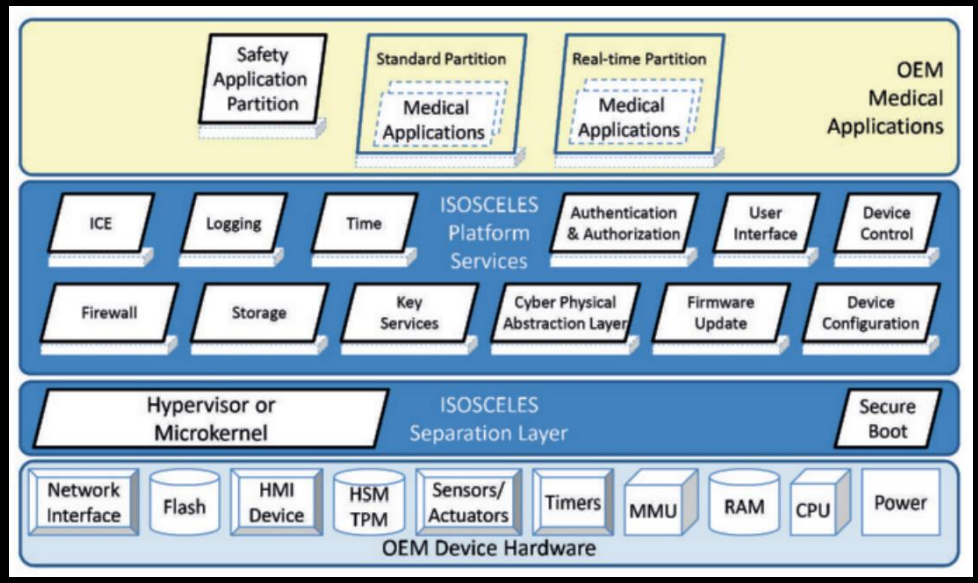
- Feb 2020, over 20% medical devices in the global clinical ecosystem runs Windows 7
- March 2020 - 83% medical imaging devices run on OS that are so old that no software updates are available
- 12% hospitals maintained a significant number of sub-networks to separate devices in 2017, increased to 44% in 2019

ISOSCELES

- A safe and secure reference architecture for medical devices
- ISOSCELES – Intrinsically Secure, Open, Safe Cyber-physically Enabled, Life-critical Essential Services
- Funded by DHS
- Open source
- Targeted for external devices with modern processors, communications and power supplies
- Not intended for power-constrained environments
- Manufacturers can select a hardware and separation approach based on their needs

ISOSCELES

- Hardware Layer
  - Processors and peripheral devices
- Separation Layer
  - Isolates software components
- Platform Layer
  - Services at this layer support common medical device needs
  - The design of a specific device to incorporate the required elements needed for that class of device



ISOSCELES – ARCHITECTURAL PRINCIPLES

Strong Time and Space Separation

- Each unit of separation is called a partition
- Partitions can run general purpose OSes
- Spatial separation - Provides memory region separation
- Temporal separation - One component can't affect or measure the time intervals during which another component access a resource
- Low level security kernel - small and simple
- One of the prototype uses seL4 microkernel and the Xen hypervisor for separation
  - Microkernel - strong separation of memory and processor time, minimizes interpartition communications
  - Hypervisor - components are running their own hardware
  - seL4 - formal proof on certain processor architectures

Minimize privilege

- A component granted only the privileges required to perform its mission
- Modern microprocessor at the hardware layer offer two modes, supervisory and user
  - Also applies to device drivers, file system devices, and protocol stacks
- Only separation layer runs in privileged mode, all other software components run in unprivileged mode and rely on separation layer to provide necessary privileges

ISOSCELES – ARCHITECTURAL PRINCIPLES

Minimize Complexity

- Construction of components as small and simple as possible
- Components can leverage service layer using interpartition communication (IPC) and avoid including service layer code in their own memory partitions

Manage Trust Relations

- Internal communications - restricted to predefined channels
- External communications - regulated by an integral firewall (default deny / whitelist)

Leverage Common Service

- Services: Logging, Time, Storage, Firewall, Update, Device control and configurations, Authentication/Authorization, Key, User Interface
- Cyber-physical abstraction layer

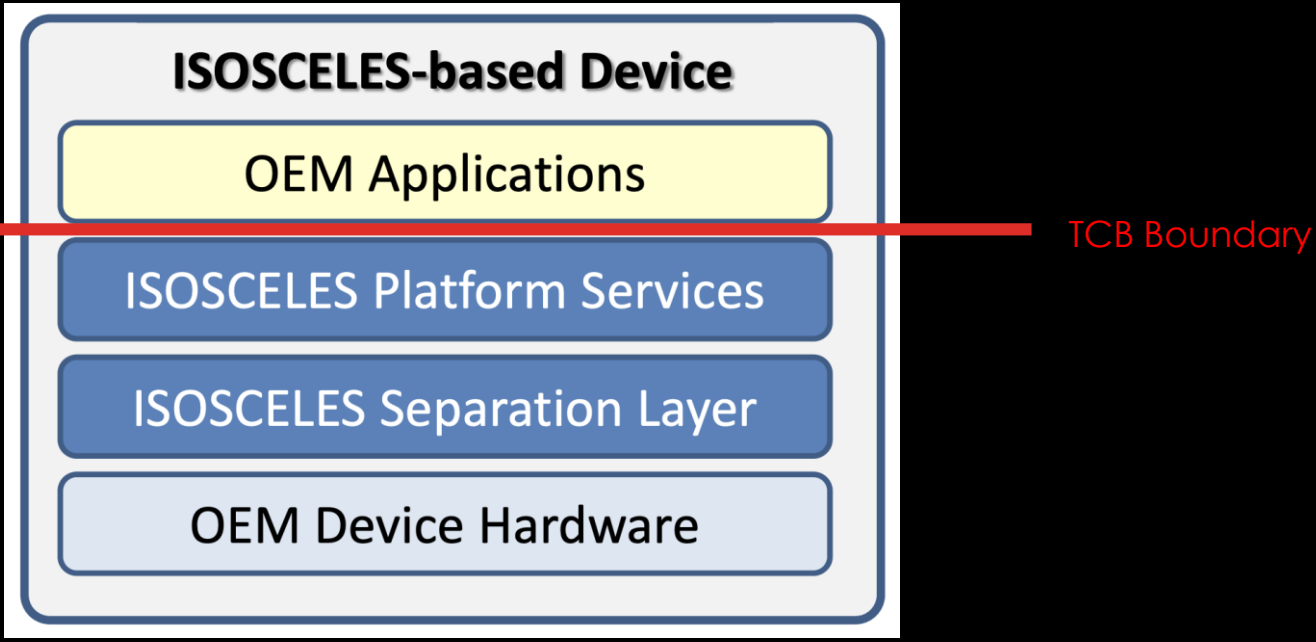
Leverage Cryptography for Confidentiality and Integrity

- Cryptographic Key Management Service (CKMS) - provides mechanism to control cryptographic materials such as keys, shared secrets, and certificates
  - Uses hardware security module if available such as TPM
- Verify software, Validate software updates, Transfer of sensitive data to/from, Communicating with external services

Leverage Models of Correctness

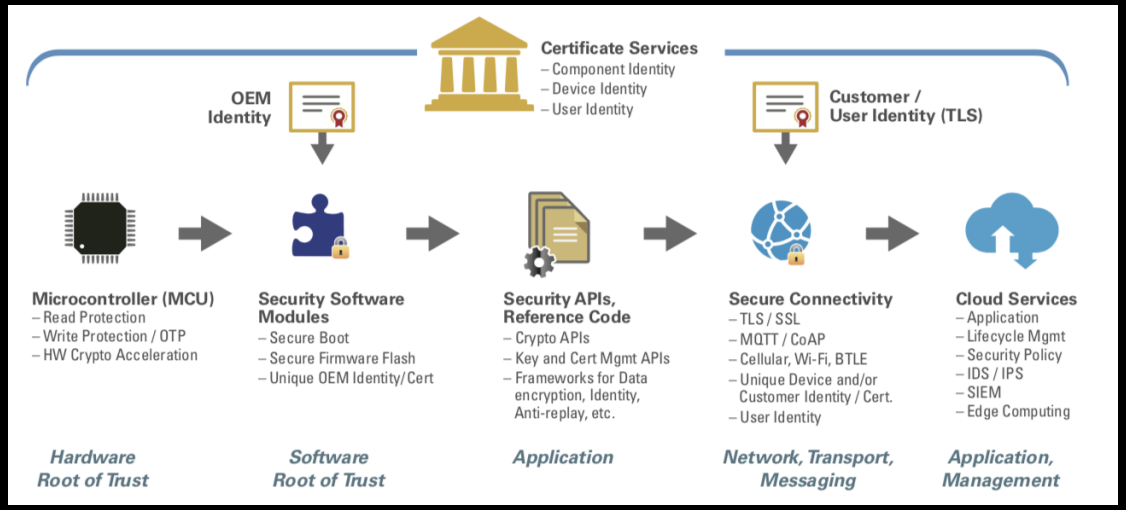
- Analytical proofs more valuable than system testing
- Represented in Architecture Analysis and Design Language (AADL) model
  - Flow annotations - what flows are allowed between different hardware and software components
- Tools convert modeled flows to runtime communication tables - provides tie between the model that was analyzed and the actual implementation

TCB IN ISOSCELES



A PLATFORM APPROACH TO SECURING MEDICAL DEVICES

- Technology security stack
- Security Architecture of a Medical Device Incorporating Multiple Protection Mechanisms
- Each part of the security architecture relates to the previous one



A PLATFORM APPROACH TO SECURING MEDICAL DEVICES

Microcontroller

- Code stored on the chip partitioned into non-secure/general and secure memory areas
- Small secure memory reduces firmware's attack surface
- OTP memory prevents the bootloader from being modified
- Root keys protected

Software Security Modules

- Bootloader verifies the validity of firmware
- Firmware checked every time upon device boot

Security APIs, Reference Code

- Crypto APIs take advantage of any hardware acceleration built into the device
- Protection functions isolate code that requires cryptographic operations
- Encryption while data at rest or shared with any other device
- Prevents unauthorized modifications, validates identities, and performs anti-replay tasks

A PLATFORM APPROACH TO SECURING MEDICAL DEVICES

Secure connectivity

- Third-party libraries - can be optimized for the specific microcontroller through a Hardware Abstraction Layer (HAL)

Cloud Services

- Healthcare applications link to the cloud
- The cloud-based software to incorporate medical device's protection mechanisms as well as provide its own set of security services

Certificate Services

- Provides identity to the medical device

REFERENCES

- Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, FDA-2018-D-3443, FDA.
- Postmarket Management of Cybersecurity in Medical Devices, FDA-2015-D-5105, FDA.
- Harp, S., Carpenter, T., & Hatcliff, J. (2018). A Reference Architecture for Secure Medical Devices. Biomedical instrumentation & technology, 52(5), 357–365. https://doi.org/10.2345/0899-8205-52.5.357
- Vora, K., & Schaeffer M. (2017). A Platform Approach to Securing Your Medical Devices, Renesas Electronics.
- How to build up cybersecurity for medical devices, Help Net Security, 2020.
- How to help your medical devices meet the UL (and FDA) standard, Synopsys, 2018.
- Cybersecurity of medical devices: Addressing patient safety and the security of patient health information, BSI, 2017.
- Principles and Practices for Medical Device Cybersecurity, Medical Device Cybersecurity Working Group, 2020.
- Medical Device Cybersecurity Guidance for Industry, Australian Government, Department of Health, 2019.
- 5 Principles for Creating Secure Healthcare IoT Devices, KeyFactor, 2019.
- How To Design Devices for FDA Cybersecurity Guidance, KeyFactor, 2019.
- Most Medical Imaging Devices Run Outdated Operating Systems, Wired, 2020.
- Tech Tips: Which Operating System For Which Medical Device, Why and How to Patch It?, TechNation, 2017.
- Securing Connected Medical Devices, Booz Allen Hamilton, 2019.

Industrial Control Systems Assurance

Venkat Ramana Reddy Mareddy

DSCI 523 Case Study

17 Nov 2020

Contents

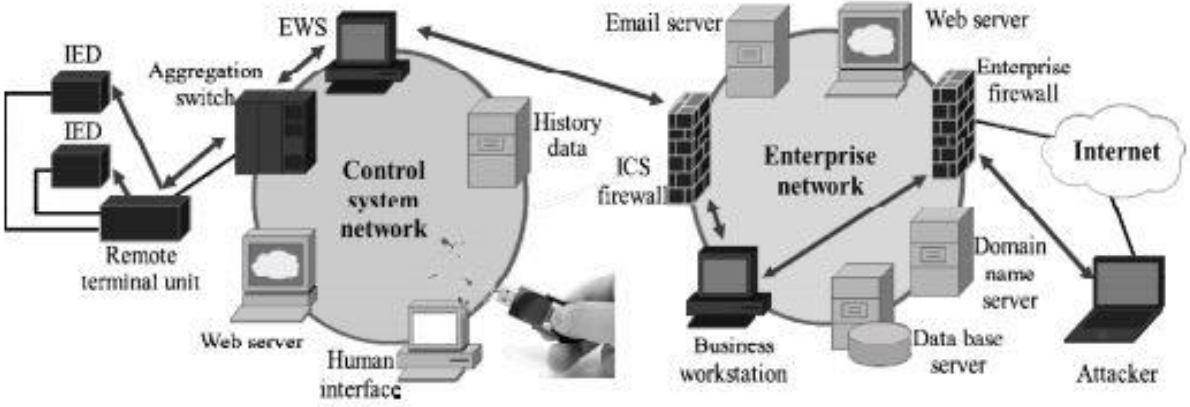
Industrial Control Systems

- Any system that gathers information on an Industrial process and modifies, regulates or manages the process to achieve a desired result.

Some important ICS:

- SCADA (Supervisory Control and Data Acquisition) Ex: Electricity, oil & gas
- DCS (Distributed Control System) Ex: Chemical plant, Food & Beverage Production
- PCS (Process Control System) Ex: Wastewater treatment plant
- EMS (Energy Management System) Ex: Electricity, Wind
- AS (Automated System) Ex: Staten Island - Amazon
- SIS (Safety Instrumented System) Ex: Refineries, nuclear and chemical.

ICS N/W Architecture



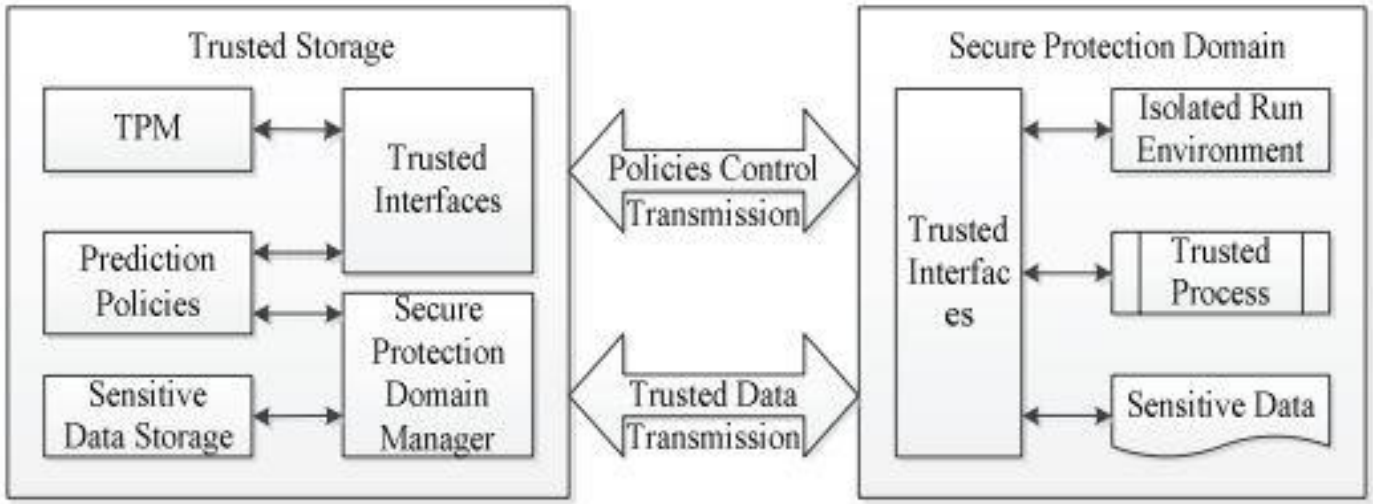
ICS Components

Control Component:

- Control Server
- Master Terminal Unit (MTU)
- Remote Terminal Unit (RTU)
- Programmable Logic Controller (PLC)
- Intelligent Electronic Devices (IED)
- Human-Machine Interface (HMI)
- Data Historian
- Input/Output (IO) Server

Network Component:

- Fieldbus Network
- Control Network
- Communications Routers
- Firewall
- Modems
- Remote Access Points


Trusted Storage
TPM
Prediction Policies
Sensitive Data Storage
Trusted Interfaces
Secure Protection Domain Manager
Policies Control Transmission
Trusted Data Transmission
Secure Protection Domain
Trusted Interfaces
Isolated Run Environment
Trusted Process
Sensitive Data

Trusted Computing Platform

- Trusted Platform Module (TPM) is embedded in trusted computing platform.
- TPM takes password and authentication technologies as a trusted chain
- The trusted chain transfers from the chip, motherboard, BIOS, operating system sequentially to ensure the integrity, credibility and security of the control computing platform, along with the trusted software protocol stack.
- The TPM checks all the operations between the field devices and the monitoring network.
- Trusted computing platform is resistance to various attacks, i.e. fabrication, falsification, illegal read, and can prevent leakage of sensitive data in the platform.
- Trusted computing platform is mainly used in prior monitoring, legality certification of system to ensure computing platform controlled, and refusal of unintended control of device system after security incidents.

Trusted Data Protection

- Trusted Data Protection mechanism in the field device layer and production monitoring layer helps to protect core data of industrial control system.
- Core data include production data in field equipment, control data of transmission, stored sensitive data.
- Isolated communication environment like VPN dynamically in the field device layer, ensuring data used for device control being not leaked.
- Combining with trusted computing and virtualization technology, build a virtual machine system in production monitor layer, and establish a secure protection domain (SPD) for sensitive data
- Sensitive data are bounded in SPD
- Security domain is a virtual isolated environment

Continued..

- File access, network access and communications are filtered by the security domain.
- The operation of writing the data to an un-trusted storage area or sending to untrusted processes is prohibited.
- SPD is encrypted and packaged by the TPM.
- The policies of using data are set in advance.
- SPD tests the related environment of data, authenticate the user or process, and ensure that the access of data and its operation are in the trusted environment.
- Untrusted process or clues to malicious code detection server, inspects malicious intrusions.
- Trusted virtual data protection mechanism is mainly used in the prior monitoring, security isolation, intrusion detection and post-audit

Trusted Network Management

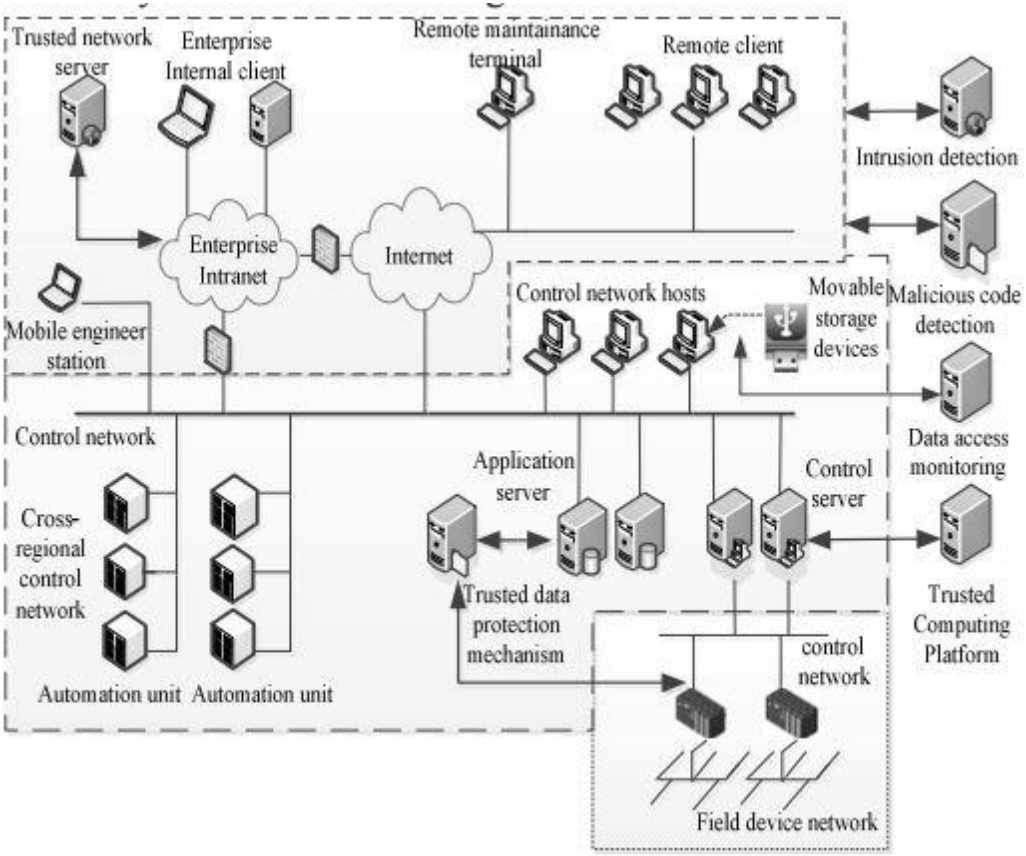
- Architecture of a trusted network: Trusted terminal set, Security gateway, Trusted agent layer and Application access layer.
- Security of trusted terminal is the core factor for a trusted network.
- In static evaluation, the security of trusted terminal is proved by trusted computing module.
- In dynamic evaluation, the trusted nodes have certain intelligence, the credibility are related to their actions and behaviors.
- Based on the trust values, a node is assigned one of the three possible states: 1) trusted, 2) un-trusted, 3) uncertain to other member nodes.
- Trusted network is mainly used to detect behavioral attacks, protect the ICS coordinating with intrusion prevention, malicious code defense and post-audit.

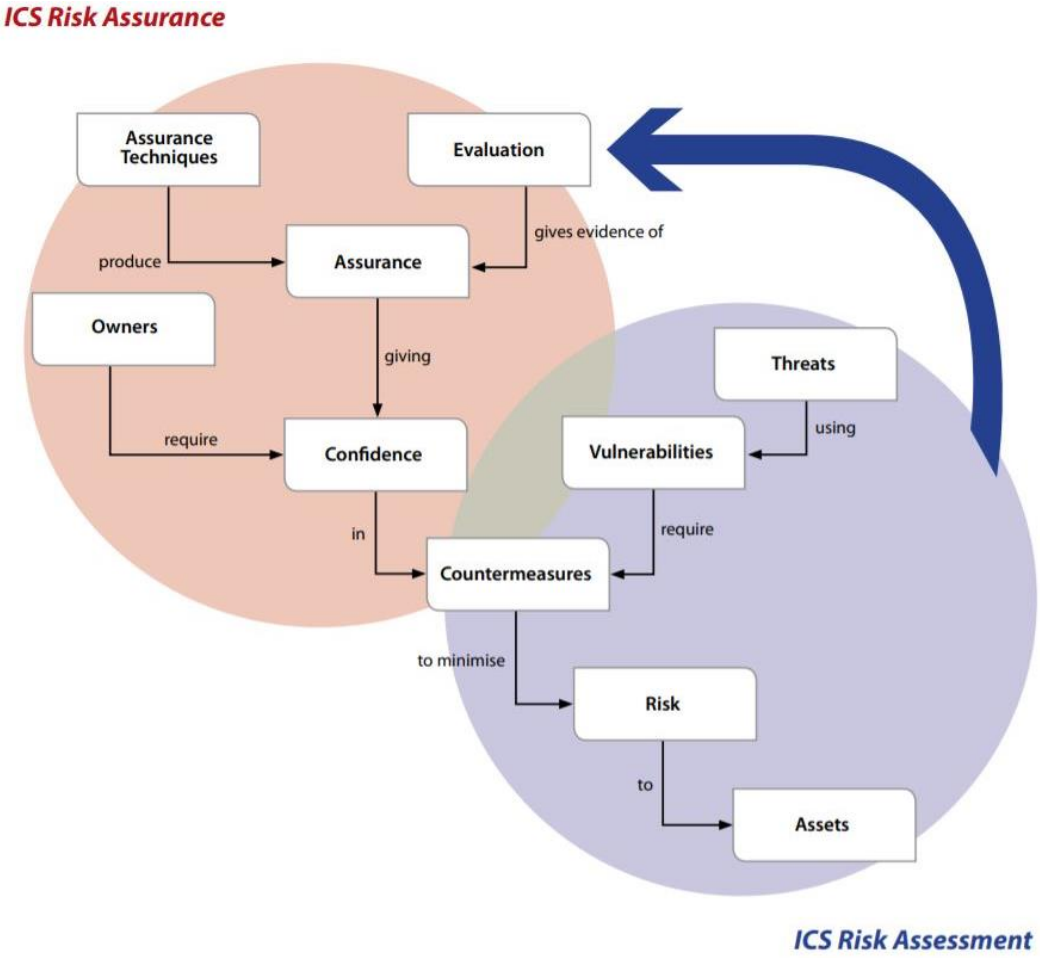
Trusted Protection Model

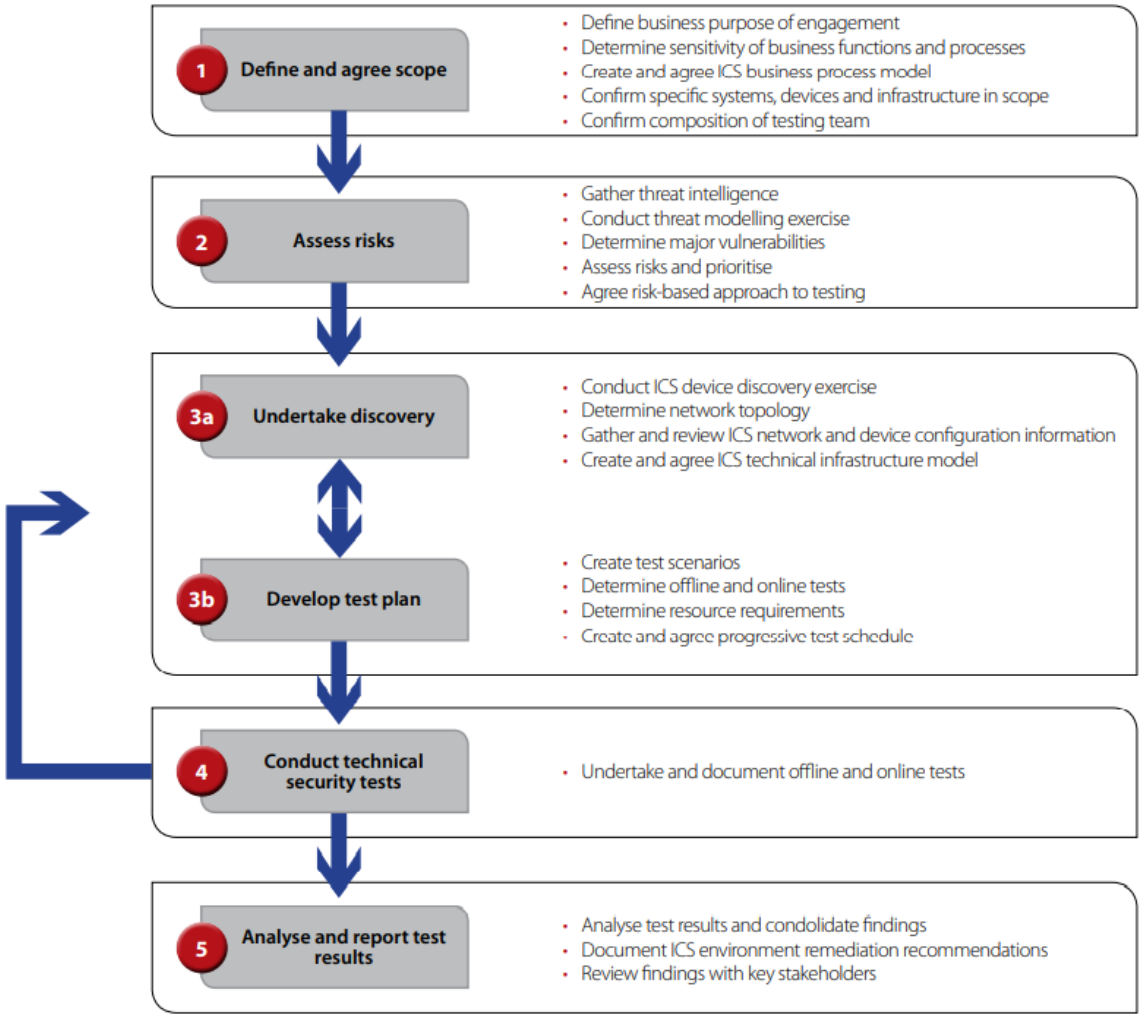
- The model is deployed in the layers of field devices network, production monitoring, and enterprise management.
- Trusted computing modules are embedded in the core control network of the industrial control system to perform access control.
- Trusted data protection mechanisms are embedded in operation monitoring module and field devices network of the industrial control system to achieve real and credible data management.
- Trusted Network Management model is embedded in enterprise management network module of the industrial control system to realize dynamic trust management of nodes.
- Trusted Protection Model analyze the data stream (i.e. network routing information, read and write information, data transmission information) of industrial control system from dimension of node and network
- We determine its credibility, the results of which can be used for real-time or post auditing.

ICS Security Policies and Procedures

- Policies and Procedures should be integrated with existing operational/management policies.
- Transparency between the Policy and Procedure is necessary.
- Policies and procedures help to ensure security is both consistent and current to protect against evolving threats.
- Examine existing security policies to see if they adequately address the risks to the ICS.
- If needed, existing policies should be revised or new policies created to address desktop and business systems as well as the ICS.
- Development of the security policies, based on a risk assessment that will set the security priorities and goals for the organization so that the risks posed by the threats are mitigated sufficiently
- Procedures that support the policies need to be developed so that the policies are implemented fully and properly for the ICS
- Security procedures should be documented, tested, and updated periodically in response to policy and technology changes


Trusted network server
Enterprise Internal client
Remote maintainance terminal
Remote client
Intrusion detection
Enterprise Intranet
Internet
Malicious code detection
Mobile engineer station
Control network hosts
Movable storage devices
Data access monitoring
Control network
Application server
Control server
Cross-regional control network
Trusted Computing Platform
Trusted data protection mechanism
control network
Automation unit
Automation unit
Field device network


ICS Risk Assurance
Assurance Techniques
Evaluation
gives evidence of
produce
Assurance
Owners
giving
Threats
using
require
Confidence
Vulnerabilities
require
in
Countermeasures
to minimise
Risk
to
Assets
ICS Risk Assessment


1
Define and agree scope
Define business purpose of engagement
Determine sensitivity of business functions and processes
Create and agree ICS business process model
Confirm specific systems, devices and infrastructure in scope
Confirm composition of testing team
2
Assess risks
Gather threat intelligence
Conduct threat modelling exercise
Determine major vulnerabilities
Assess risks and prioritise
Agree risk-based approach to testing
3a
Undertake discovery
Conduct ICS device discovery exercise
Determine network topology
Gather and review ICS network and device configuration information
Create and agree ICS technical infrastructure model
3b
Develop test plan
Create test scenarios
Determine offline and online tests
Determine resource requirements
Create and agree progressive test schedule
4
Conduct technical security tests
Undertake and document offline and online tests
5
Analyse and report test results
Analyse test results and condolidate findings
Document ICS environment remediation recommendations
Review findings with key stakeholders

Assurance Issues

- Changing nature of ICS environments
- Merging IT and OT
- Cultural Barriers and Resistance to change
- Technical Complexity
- Large Attack Surface
- Difficulty in conducting Security tests
- Need for ICS Risk Assurance
- Adoption of standardized protocols and technologies with known vulnerabilities
- Connectivity of the control systems to other networks
- Insecure and rogue connections
- Widespread availability of technical information about control systems.

ICS vs IT Systems

- Performance Requirements
- Availability Requirements
- Risk Management Requirements
- Architecture Security Focus
- Physical Interaction
- Time-Critical Responses
- System Operation
- Resource Constraints.
- Communications
- Change Management.
- Managed Support.
- Component Lifetime.
- Access to Components.

Adversarial Threats to ICS

- Attackers
- Bot-network operators
- Criminal groups
- Foreign intelligence services
- Insiders
- Phishers
- Spammers
- Spyware/malware authors
- Terrorists
- Industrial spies

Common ICS Vulnerabilities

- Plain text traffic and open protocols
- System susceptible to Denial of Service
- Susceptible to Buffer Overflows
- Weak or known passwords
- Absence of Embedded Counter Measures
- Dependent on Underlying Operating System
- Advanced features expands vulnerabilities
- Contemporary IT countermeasures are not always best fit
- Default configurations are used
- Undocumented assets

Policy Importance

- Incomplete, inappropriate, or nonexistent security documentation, including policy and implementation guides (procedures) can result in vulnerabilities.
- Corporate security policy can reduce vulnerabilities by mandating conduct such as password usage and maintenance or requirements for connecting modems to ICS.

Some vulnerabilities:

- Inadequate security policy for the ICS
- No formal ICS security training and awareness program
- Lack of administrative mechanisms for security enforcement
- Absent or deficient ICS equipment implementation guidelines
- No documented security procedures were developed from the security policy for the ICS
- Inadequate security architecture and design

Attacks on ICS

- Triton, 2017 – petrochemical facilities safety systems
- Black Energy, 2014 - Ukraine’s power grid
- Stuxnet, 2010 – Iranian Centrifuges

References

- https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
- https://www.crest-approved.org/wp-content/uploads/CREST-Industrial-Control-Systems-Technical-Security-Assurance-Position-Paper.pdf
- https://www.redteamsecure.com/blog/5-key-lessons-learned-critical-infrastructure-cyber-attacks/
- https://eprints.lancs.ac.uk/id/eprint/77348/1/AT_ICS.pdf
- F. Kargl F, dHRW. Van, H Konig, A Valdes, MC Dacier, “Insights on the Security and Dependability of Industrial Control Systems,” IEEE Security & Privacy, vol. 12, pp. 75-78, December 2014.
- https://ieeexplore.ieee.org/document/7423278
- https://dl.acm.org/doi/pdf/10.1145/2808705.2808710 Assurance Techniques for Industrial Control Systems (ICS)
- https://www.wired.com/story/russian-hackers-us-power-grid-attacks/

Thank you!

Cloud Database Assurance

Oracle 12C Family - Exadata

Review

Topic: Cloud Database

Assurance issues to addressed:

- Protect Data from accidental loss (at rest/in transit)
- Protect Data from corruption (at rest/in transit)
- Protect Data from unauthorized altercation (at rest/in transit)
- Protect data from unauthorize access (at rest/in transit)
- Ensure accurate data is available for access as required
- Ensure compliances with company policies (at rest/in transit)

  (Physical & Administrative)
- Ensure compliance with rules and regulations (at rest/in transit)
- Consequences of not addressing these matters
- Where to look for answers

Today's Attraction

TOE: Oracle Exadata DB 12c -19c (Autonomous Database)

Model: Traditional or Dbaas

Certified Assurance Level

- Common Criteria for Information Technology Security Evaluation
- Federal Information Processing Standard

Assurance Techniques Applied

- How does the system utilize minimization

Where is the TCB

Possible Improvements

Database:

A large collection of data and a set of rules that organizes that data by specifying their relationships and is stored **electronically on a computer** that can be accessed in multiple ways by multiple users concurrently.

Cloud Database:

Database access through the internet.

Cloud Models:

Traditional:

Purchase from cloud provider. Managed by the organization and their personnel

DBaaS:

Fee based subscription service

Outsourced.

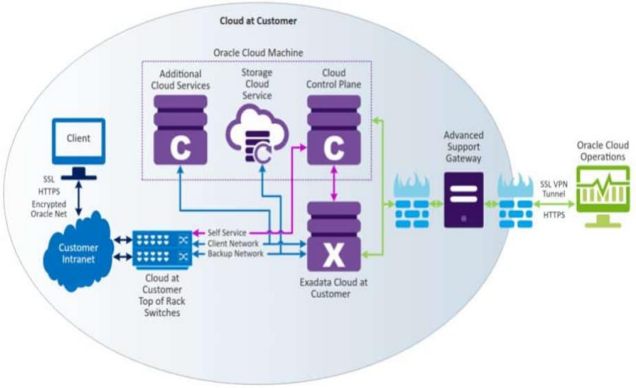
Oracle Exadata:

Computing platform “in a box” optimized for running oracle database on the cloud. Allows for OLAP and OLTP

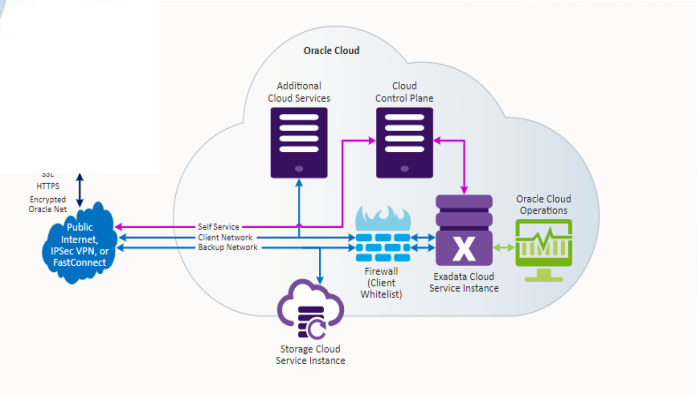
Components: Hardware, Software, Intra-network connections.

Oracle Exadata Models:

Cloud @ Customer:

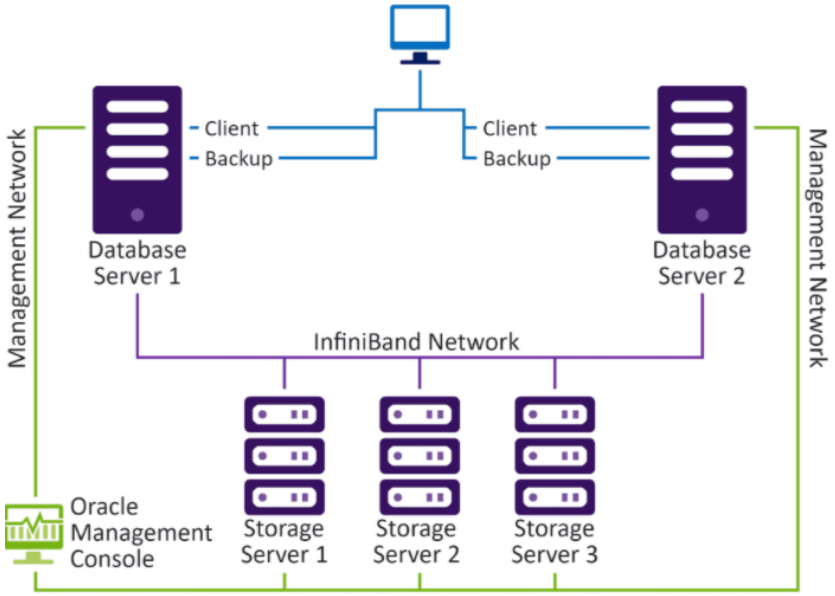


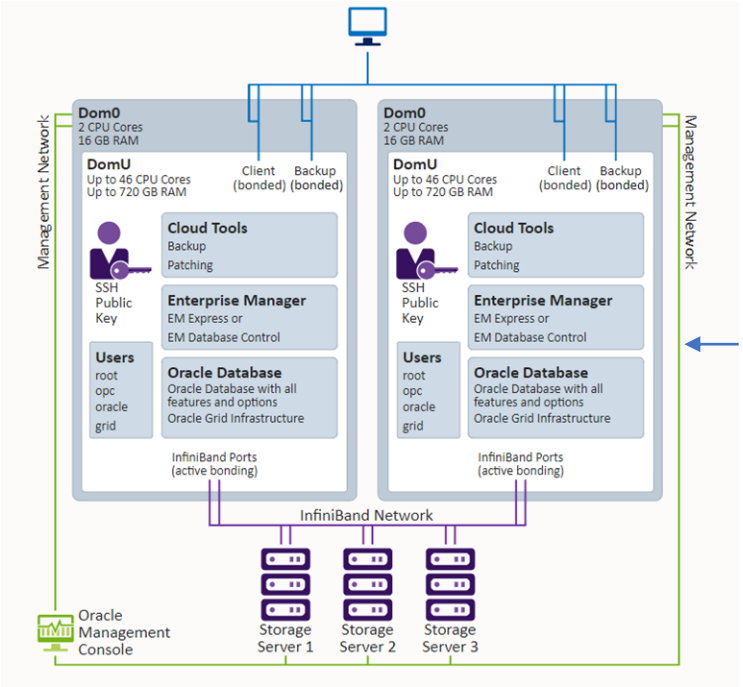
Cloud @ Oracle



Oracle.com

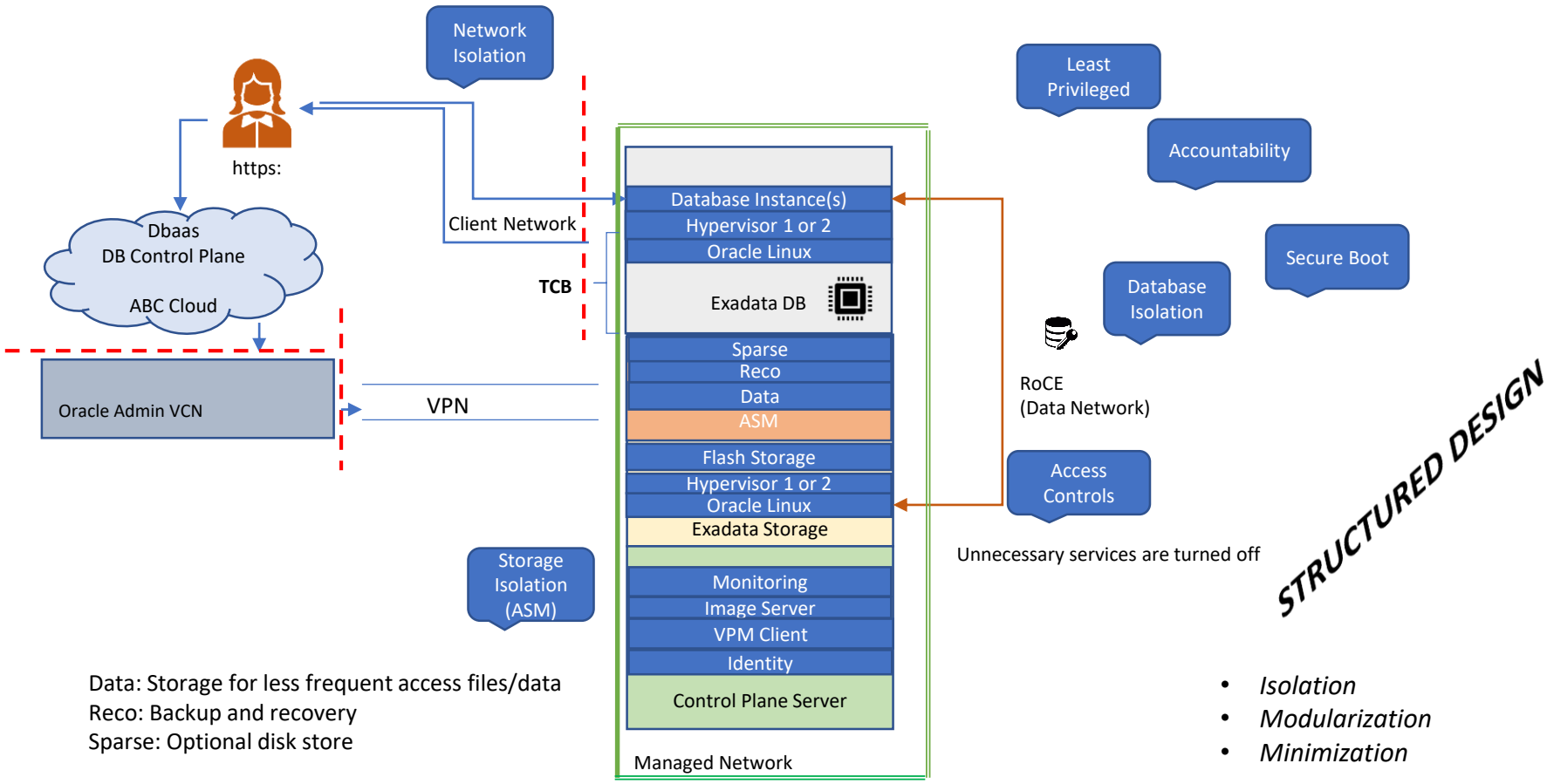
Exadata Components





Database Server

Oracle.com

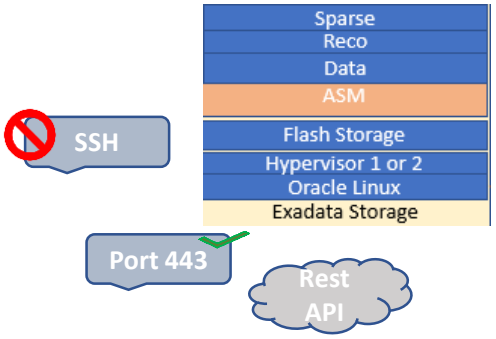


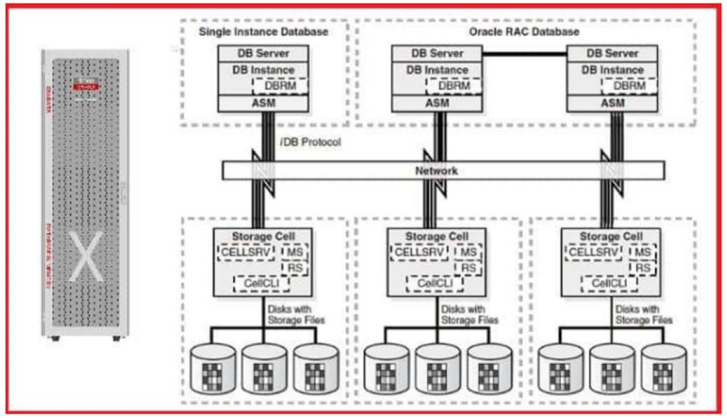
Data: Storage for less frequent access files/data
Reco: Backup and recovery
Sparse: Optional disk store

- *Isolation*
- *Modularization*
- *Minimization*

RoCE = RDMA over Converged Ethernet

Database & Storage Separation



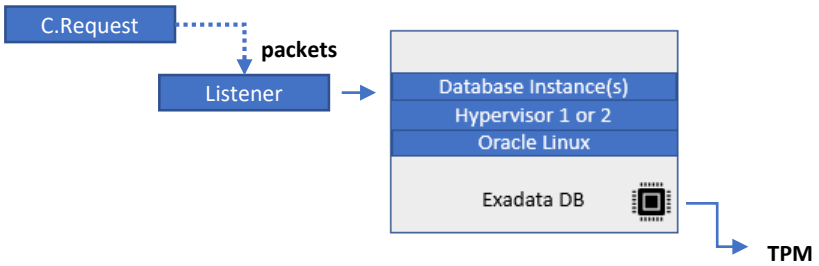


Open Security

DB Scope Security

ASM Security

TDE for Data at REST



STRUCTURED DESIGN

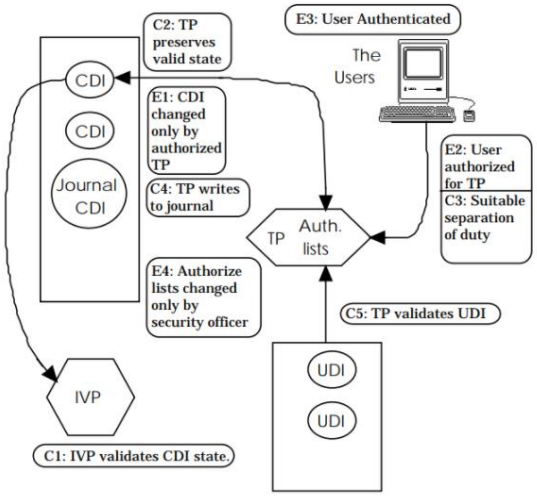
- *Isolation*
- *Modularization*
- *Minimization*

Oracle.com

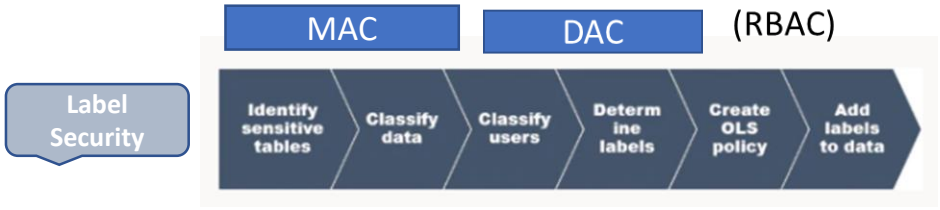
Clark Wilson Security Model

Certification Rule (CR) – integrity monitoring
C1: All IVPs must properly ensure that all CDIs are in a valid state.
C2: All TPs must be certified to be valid. For each TP and each set of CDI that it may manipulate, the security officer must specify a "relation" of the form: (TP, {CDI}).
C3: (Separation of Duty Certification) The list of relation in E2 must be certified to meet the separation of duty requirement.
C4: (Journal Certification) All TPs must be certified to write to an append-only CDI (the log) all information necessary to permit the nature of the operation to be reconstructed.
C5: Any TP that takes a UDI as an input value must be certified to perform only valid transformations, or no transformations, for any possible value of the UDI. The transformation should take the input from a UDI to a CDI, or the UDI is rejected.

Enforcement Rule (ER) – integrity preserving
E1: (Basic: Enforcement of Validity) The system must maintain the list of relation specified in C2 and must ensure that only TPs certified to run on a CDI manipulate that CDI.
E2: (Enforcement of Separation of Duty) The system must associate a user with each TP and set of CDIs in a list of relations of the form: (User, TP, {CDI}). It must ensure that only executions described in one of the relations are performed.
E3: (User Identity) The system must authenticate the identity of each user attempting to execute a TP.
E4: (Initiation) Only the agent permitted to certify entities may change the list of such entities associated with other entities, specifically the one associated with a TP. An agent that can certify an entity may not have any execute rights concerning that entity.



Edk2.doc.gitbooks (Lee)



Assurance Evaluation

Common Criteria

TOE:

Oracle 12c with DB Vault and Multitenant

Oracle 19c (In Process)

Oracle Linux 7.3 and UEK (unbreakable enterprise kernel.)

Oracle Linux 7 Open SSH

(Server & Client Cryptographical Modules)

Oracle IAM

Note: Many Others

Documentation and Testing

CSEC

Swedish Certification Body for IT Security

COMMON CRITERIA CERTIFICATE

Oracle Linux 7.3

Certification/Validation Identification: CSEC2017013
Type of Product: Operating system
Product Name: Oracle Linux 7.3
Version and Release Numbers: Version 7 Release 3
Evaluation Platform of Target of Evaluation: x86 64-bit Intel Xeon processors: Oracle Server X7-2a
Product Manufacturer: Oracle America, Inc.
Assurance Package: EAL1 + ALC_FLR.3
Name of IT Security Evaluation Facility: atsec information security AB
Certification/Validation Report Identifier: Certification Report - Oracle Linux 7.3, CSEC, 2019-02-14, 17FMV7413-52:1

is through decision

14th of February 2019

certified in accordance with Common Criteria and the Swedish Certification Scheme

Dag Ströman
Head of CSEC

CSEC

Swedish Certification Body for IT Security

COMMON CRITERIA CERTIFICATE

Oracle Database 12c Release 2 Enterprise Edition
(with Database Vault and Multitenant)

is through decision

18th of December 2018

certified in accordance with Common Criteria and the Swedish Certification Scheme

Dag Ströman
Head of CSEC

FMV

ational Information Assurance Partnership

Common Criteria Certificate

is awarded to

Oracle Corporation

for

Oracle Access Manager Suite 11g Release 2

identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodolog
ation (Version 3.1) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1). This certifica
o the specific version and release of the product in its evaluated configuration. The product's functional and assurance
ifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of t
ion Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical
t with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Govern
nty of the IT product is either expressed or implied.

2017-07-24

eport Number: CCEVS-VR-VID10812-2017

Allen Hamilton Common Criteria Testing Laboratory

Assurance Level: PP Compliant

Protection Profile Identifier:
Protection Profile for Enterprise Security Management-Access Control Version 2.1
Protection Profile for Enterprise Security Management - Poli Management Version 2.1

iginal Signed By
e Evaluation and Validation Scheme
n Assurance Partnership

Original Signed By
Deputy National Manager National Secu
National Security Agenc

https://www.commoncriteriaportal.org/

Assurance Evaluation

Federal Information Processing Standards

- FIPs 140-2 level 1
- Cryptographic Module Validation Program
- Cryptographic Algorithm Validation Program

“ Absence of Evidence of Errors is not an Evidence for Absence of Error.”

FIPS 140-2 Consolidated Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

March 2019

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the cryptographic modules listed below in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting Sensitive Information (United States) or Protected Information (Canada) within computer and telecommunications systems (including voice systems).

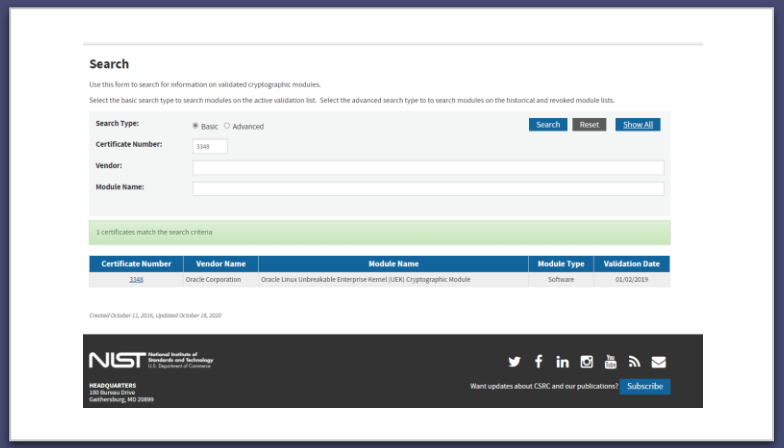
Products which use a cryptographic module identified below may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life-cycle, continues to use the validated version of the cryptographic module as specified in this consolidated certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module.

The scope of conformance achieved by the cryptographic modules as tested are identified and listed on the Cryptographic Module Validation Program website. The website listing is the official list of validated cryptographic modules. Each validation entry corresponds to a uniquely assigned certificate number. Associated with each certificate number is the module name(s), module versioning information, applicable caveats, module type, date of initial validation and applicable revisions, Overall Level, individual Levels if different than the Overall Level, FIPS-approved and other algorithms, vendor contact information, a vendor provided description and the accredited Cryptographic Module Testing laboratory which performed the testing.

Signed on behalf of the Government of the United States
Signature:
Dated: 4/4/2018
Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada
Signature:
Dated: 4/4/2018
Director, Security Architecture and Risk Mgmt
Communications Security Establishment



Search

Use this form to search for information on validated cryptographic modules.

Select the basic search type to search modules on the active validation list. Select the advanced search type to to search modules on the historical and revoked module lists.

Search Type: Basic Advanced — Search | Reset | Show All

Certificate Number: 3348

Vendor:

Module Name:

1 certificates match the search criteria

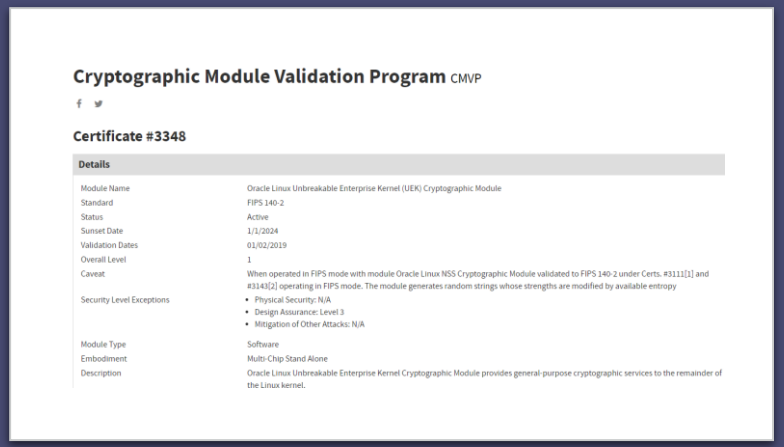
Certificate Number	Vendor Name	Module Name	Module Type	Validation Date
3348	Oracle Corporation	Oracle Linux Unbreakable Enterprise Kernel (UEK) Cryptographic Module	Software	01/02/2019

Created October 11, 2016, Updated October 16, 2020

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

HEADQUARTERS
100 Bureau Drive
Gaithersburg, MD 20899

Want updates about CSRC and our publications? Subscribe



Cryptographic Module Validation Program CMVP

Certificate #3348

Details

Module Name	Oracle Linux Unbreakable Enterprise Kernel (UEK) Cryptographic Module
Standard	FIPS 140-2
Status	Active
Sunset Date	1/1/2024
Validation Dates	01/02/2019
Overall Level	1
Caveat	When operated in FIPS mode with module Oracle Linux NSS Cryptographic Module validated to FIPS 140-2 under Certs. #3111[1] and #3143[2] operating in FIPS mode. The module generates random strings whose strengths are modified by available entropy
Security Level Exceptions	• Physical Security: N/A • Design Assurance: Level 3 • Mitigation of Other Attacks: N/A
Module Type	Software
Embodiment	Multi-Chip Stand Alone
Description	Oracle Linux Unbreakable Enterprise Kernel Cryptographic Module provides general-purpose cryptographic services to the remainder of the Linux kernel.

Assurance Evaluation Levels

Common Criteria

EAL 1: Functionally Tested
- **Requires confidence in a product's correct operation, but threats to security are not considered serious. EAL 1 provide evidence that the TOE of evaluation functions in a manner consistent with its documentation and that it provides useful protection against identified threats.**
- **Independent testing and review of functional and interface specifications.**

EAL 2: Structurally Tested
- **Low to moderate independently assured security but the complete development record is not readily available. Independent testing, analysis of security function and review of developer testing.**

EAL 3: Methodically Tested and Checked
- **Applies when developers or users require a moderate level of independently assured security and require a thorough investigation of the target of evaluation and its development, without substantial reengineering.**
- **More testing, Some dev. environment controls;**

EAL 4: **Methodically Designed, Tested, Reviewed**
- **Applies when developers or users require moderate to high independently assured security in conventional commodity products and are prepared to incur additional security-specific engineering costs. More design description, improved confidence that TOE will not be tampered is required.**

EAL 5: Semi formally Designed and Tested
- Require high, independently assured security in a planned development, formal model, modular design and a rigorous development approach that does not incur unreasonable costs from specialist security engineering techniques. Included are vulnerability search, covert channel analysis, etc.
- Vulnerability search, covert channel analysis

EAL 6: Semi formally Verified Design and Tested
- Applies when developing security targets of evaluation for application in high-risk situations, using structured development processes, where the value of the protected assets justifies the additional costs.

EAL 7: Formally Verified Design and Tested
- Applies to the development of security targets of evaluation for application in extremely high-risk situations, as well as when the high value of the assets justifies the higher costs Formal presentation of functional specification
- Product or system design must be simple
- Independent confirmation of developer tests

https://us-cert.cisa.gov/bsi/articles/best-practices/requirements-engineering/the-common-criteria

Highlights

- A higher EAL = Evaluation completed a more stringent set of quality assurance requirements
- It is presupposed that a system that achieves a high EAL = more attested security features; however, there is little to none evidence produced to support this assumption
- Anything below EAL4 is useless
- Anything above EAL4 is extremely difficult for complex systems to achieve
- Evaluation is done for environments predefined by vendors *(Cheating?)*
- Evaluation is a costly process and center predominately on assessing the documentation set, instead of the product
- Effort and time to prepare evaluation-related documentation is extremely cumbersome lengthy time to complete = Evaluation obsolete

https://www.commoncriteriaportal.org

Additions…

Add software firewall to the DB server, Storage Server, VM

Automation for archive of log files to remote SEIM

Focus more on security testing and not functionality testing

Proper resource training and vetting

Humans are the weakest link

Proper Policies .. Longer and more difficult =! Better

*** Assess RISK vs Benefits .. EXPENSIVE ***

References

https://www.researchgate.net/publication/220803268_A_new_Access_Control_model_based_on_the_Chinese_Wall_Security_Policy_Model

https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7316.pdf

https://www.giac.org/paper/gsec/835/clark-wilson-security-model/101747

https://us-cert.cisa.gov/bsi/articles/best-practices/requirements-engineering/the-common-criteria

https://www.commoncriteriaportal.org/communities/database_management_systems.cfm

https://www.commoncriteriaportal.org/communities/CCP%20DBMS_WG_ESR%201.1.pdf

https://blogs.oracle.com/multitenant/oracle-multitenant-receives-common-criteria-certification

https://www.oracle.com/database/multitenant/

https://www.commoncriteriaportal.org/products/#DB

https://edk2-docs.gitbook.io/understanding-the-uefi-secure-boot-chain/overview/integrity-models

https://www.semanticscholar.org/paper/A-Comparison-of-the-trusted-Computing-Group-Model-Smith/fa82426d99b86d1040f80b8bd8e0ac4f785b29a6

https://www.cl.cam.ac.uk/~mgk25/lee-essays.pdf

https://www.oracle.com/engineered-systems/exadata/

https://www.stigviewer.com/stig/oracle_database_12c/

https://www.oracle.com/database/technologies/

https://edk2-docs.gitbook.io/understanding-the-uefi-secure-boot-chain/overview/integrity-models

https://docs.oracle.com/cd/B28359_01/server.111/b28318/intro.htm#CNCPT924

https://blogs.oracle.com/cloud-infrastructure/oracle-iaas-and-seven-pillars-of-trusted-computing-platform-part-1-of-4

Cloud Security Assurance

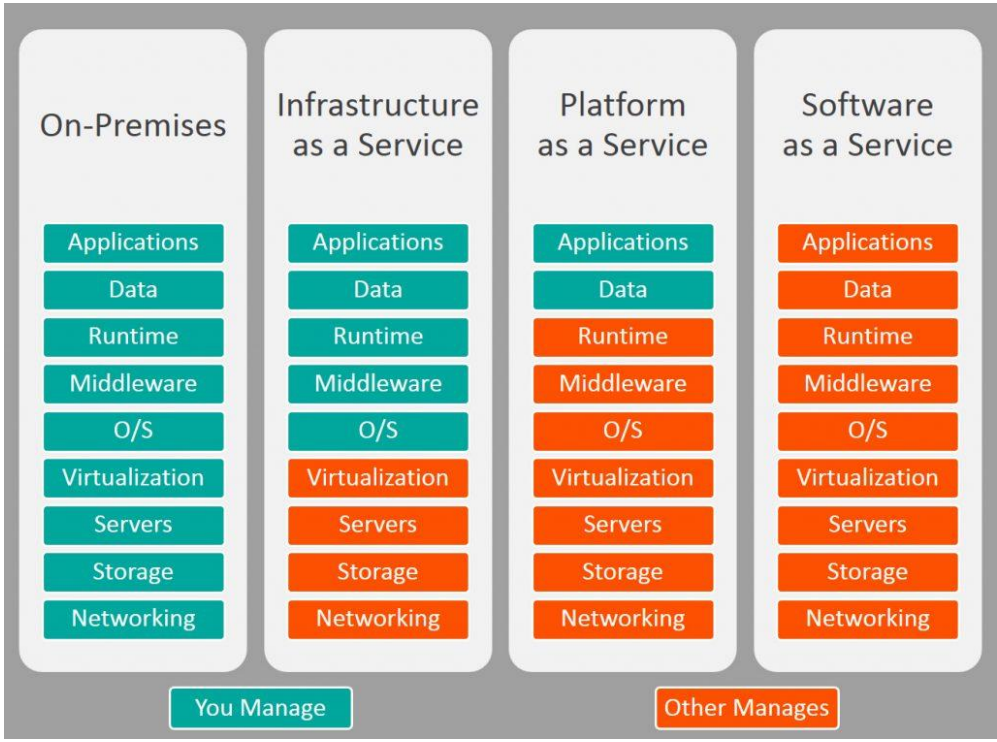
Shagun Bhatia

(Share Screen)

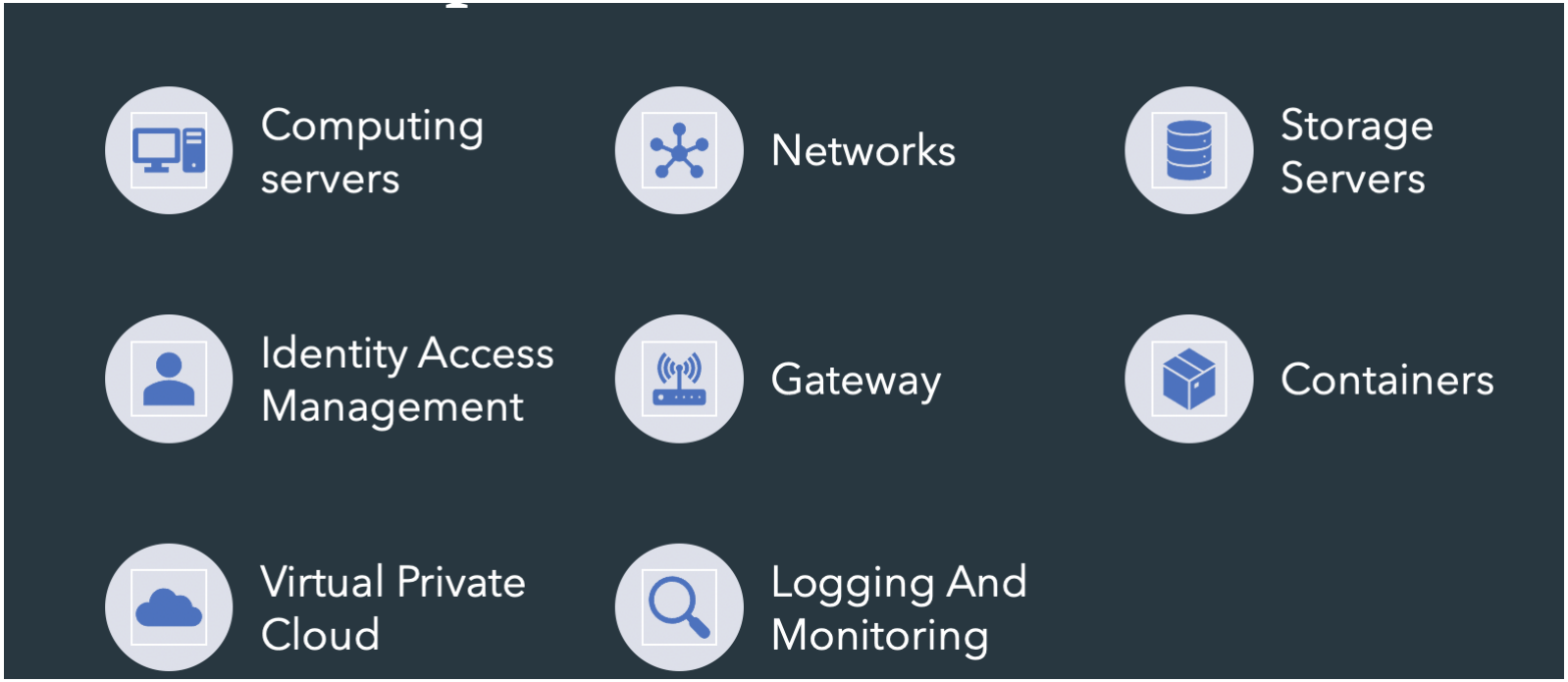

Flexibility
Scalability
Efficiency
Investment and
Maintenance costs

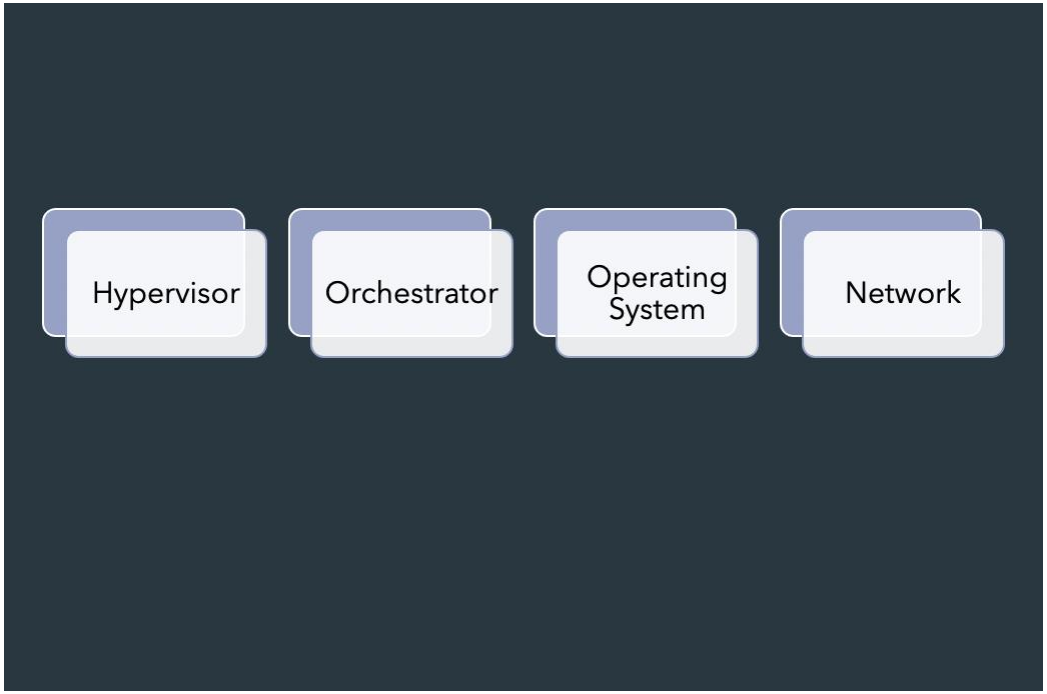
Types of Cloud Services

- Software as a Service
- Platform as a Service
- Infrastructure as a Service



Cloud Components




Hypervisor
Orchestrator
Operating System
Network

Hypervisor Security Assurance

- VM Process Isolation
- Devices Emulation and Access Control
- Execution of Privileged Operations by Hypervisor for Guest VMs
- VM Lifecycle Management
- Management of Hypervisor

VM Process Isolation

- Hardware-based assistance is provided for virtualization whether its for memory or instruction set.
- The hypervisor are configured to give physical RAM for every VM and to also to set an upper limit to stop the excessive use by one application or party
- The hypervisor also has features to specify a lower and upper bound for CPU clock cycles needed for every deployed VM
- The hypervisor is configured to provision virtual resources to all hosted VMs such that it does not exceed a key physical resource such as number of CPU cores.

Devices Emulation and Access Control

- All device drivers installed as part of Hypervisor are configured to run in user mode than the kernel mode
- Access Control List (ACL) are set to restrict access of each VM process to only the resources assigned to that VM.
- Resource limits are set for network bandwidth and I/O bandwidth (e.g., disk read/write speeds) for each VM

VM Lifecycle Management

- A standard is defined for VMs of all types and VM Images not conforming to the standard are not stored in the Image library. Further images in the VM Image library are periodically scanned for OS versions and patches which are out of date and not according to the standard
- Every VM Image stored in the image server has a digital signature attached to it as a mark of authenticity and integrity, signed using trustworthy, robust cryptographic keys.
- Checking in and out images from VM Image library are enforced through robust access control mechanism and limited to an authorized admins.
- Access to the server storing VM images is done using a secure protocol such as TLS.

Management of Hypervisor

- The administration of all hypervisor installations is performed centrally using an enterprise virtualization management system (EVMS). Further Standard hypervisor configurations for different types of workloads and clusters are also managed (enforced) through EVMS. The standard configurations cover the following aspects – CPU, Memory, Storage, Network bandwidth and Host OS hardening

Orchestrator Security

- Infrastructure security
- Cluster Security
- Pod Security

Infrastructure Security

- All access to the Kubernetes control plane is not allowed publicly on the internet and is controlled by network access control lists restricted to the set of IP addresses needed to administer the cluster
- Access to etcd is limited to the control plane only can be done only over TLS.
- All drives are encrypted at rest, specially etcd since it holds the state of the entire cluster (including Secrets) its disk should especially be encrypted at rest

Cluster Security

- All API clients are authenticated, even those that are part of the infrastructure like nodes, proxies, the scheduler, and volume plugins. These clients are typically service accounts or use x509 client certificates, and they are created automatically at cluster startup or are setup as part of the cluster installation
- Kubernetes ships an RBAC component that matches an incoming user or group to a set of permissions bundled into roles. These permissions combine verbs (get, create, delete) with resources (pods, services, nodes) and are generally namespace or cluster scoped

Recommendation for improvement

- Kubelets expose HTTPS endpoints which grant powerful control over the node and containers. By default Kubelets allow unauthenticated access to this API. Production clusters should enable Kubelet authentication and authorization
- Resource quota limits the capacity of resources granted to a namespace. This is used to limit the amount of CPU, memory, or persistent disk a namespace can allocate, but can also control how many pods, services, or volumes exist in each namespace
- Limit range restrict the size of some of the resources to prevent users from requesting unreasonably high or low values for commonly reserved resources like memory

Pod Security

- Security settings for Pods are typically applied by using security context. Security Contexts allow for the definition of privilege and access controls on a per-Pod basis.
- A *Pod Security Policy* is a cluster-level resource that controls security sensitive aspects of the Pod specification.
- There are 3 type of policy types
  - ***Privileged*** - Unrestricted policy, providing the widest possible level of permissions. This policy allows for known privilege escalations.
  - ***Baseline/Default*** - Minimally restrictive policy while preventing known privilege escalations. Allows the default (minimally specified) Pod configuration.
  - ***Restricted*** - Heavily restricted policy, following current Pod hardening best practice

Privileged Policy

- The Privileged policy is purposely-open, and entirely unrestricted. This type of policy is typically aimed at system- and infrastructure-level workloads managed by privileged, trusted users
- The privileged policy is defined by an absence of restrictions. It uses allow-by-default enforcement mechanisms

Baseline/Default Policy

The Baseline/Default policy is aimed at ease of adoption for common containerized workloads while preventing known privilege escalations

- Sharing the host namespaces is not allowed
- Privileged Pods are disallowed because they disable most security mechanism
- No additional capabilities beyond the default is allowed
- HostPath volumes is forbidden
- Setting custom SELinux options is not allowed.

Restricted Policy

- The Restricted policy is aimed at enforcing current Pod hardening best practices. It is targeted at operators and developers of security-critical applications, as well as lower-trust users.
  - Containers are required to run as non-root users.
  - Privilege escalation (such as via set-user-ID or set-group-ID file mode) is not allowed
  - The restricted profile limits usage of non-core volume(GitRepo, nfs, EBS)

Container

- The Monolithic architecture has now been substituted by microservices architecture which believes in deploying each service components in containers and interconnecting them.
- These containers are run and managed by an orchestrator.
- Containers are based on use and throw model. They are not patched instead a new container is spun up when old one is to be removed

Container Security

- The most important aspect of container security is its base image(linux, SELinux, GRSEC)
- The attack surface of the Docker daemon which runs the container
- Another component is how the containers are configured namespaces, control groups

Improve Security

Software As A Service Security

- SAAS provider are responsible almost all of the security for the cloud application
- Customers are responsible for the security of customer data and access to the data.
- By 2022, Gartner projects that 95% of cloud security failures will be the customer's fault

Security For Customer

- Detect Rogue services and accounts: A customer should do perform a regular audits to detect compromised or accounts that are not needed and remove them. They should also have an Inventory of cloud services they use to avoid unnecessary risk.
- Apply Identity Access Management systems: this ensures end user do not access more resources than they should
- Encrypt Cloud Data: SaaS providers provide some type of encryption but customer can opt for higher level encryption

Security For Customer

- Enable Data Loss Prevention(DLP): Software detects and prevent sensitive data to be downloaded on personal devices ad also blocks malwares
- Monitor collaborative sharing of the data: employee may inadvertently share confidential document through email
- Check SaaS providers security: if the provider meets the security requirement defined in various standards.

Platform As A Service Security

- Cloud Provider is responsible for security of the underlying cloud infrastructure such as servers, network, operating systems and storages
- Customer is responsible for securing the application that they are hosting on the platform and the data.

Security For Customer

- Threat modeling: Apply on all the application that you want to host on the platform to know about all the vulnerabilities
- Check for inherited software vulnerabilities: A lot of application use 3rd party modules or dependencies.
- Implement role-based access control: This helps provide a resources to a user only for the time they require it on a time basis and level basis

Security For Customer

- Manage inactive accounts
- Use the services of the provider: Take advantage of the solutions that the cloud provider can give to make the application and data more secure
- Research on platforms security standard: If they follow standards like HIPAA, PCI and also the strength of the security measure they follow.

Infrastructure As A Service Security

- Customers are responsible for securing data, application, operating system, virtual network traffic.
- The vendor is responsible for the physical security of the hardware and datacenters. They are also responsible for making the services available all the time.

Security For Customer

- Encrypt data: encryption should be done on both data in transit and rest.
- Avoid making configuration mistakes: Customer can use IaC for defining the configuration and making a standardized server.
- Make a contingency plan and backups

Security For Customer

- Network Security and Visibility: Implement Logging and monitoring, use IDS and IPS software and set gateway and firewall rules
- OS Security: Use a secure base image for making containers
- Use the services of the provider: Take advantage of the solutions that the cloud provider can give to make the application and data more secure

Cloud Security Alliance (CSA)

- It is a non-profit organization who aim to promote the best practices that should be used in cloud environments.
- They focus on a lot of areas in the field of cloud security
  - *Top Threats to Cloud Computing*. Helps organizations make educated risk management decisions regarding their cloud adoption strategies
  - *Cloud Controls Matrix (CCM)*. Security controls framework for cloud provider and cloud consumers. There are 133 controls across 16 domains
  - *Security Guidance for Critical Areas of Focus in Cloud Computing*. Foundational best practices for securing cloud computing

CSA's Cloud Control Matrix Framework

- Application & interface security
- Audit Assurance and Compliance
- Business Continuity Management & Operational Resilience
- Change Control & Configuration Management
- Data Security & Information Lifecycle Management
- Datacenter Security (DCS)
- Encryption & Key Management
- Governance & Risk Management

Security Controls in Cloud

- Human Resources
- Identity & Access Management
- Infrastructure & Virtualization Security
- Interoperability & Portability
- Mobile Security
- Security Incident Management, E-Discovery, & Cloud Forensics
- Supply Chain Management, Transparency, and Accountability
- Threat & Vulnerability Management

Application & interface security

- API that are developed should be developed and tested according to industry standard OWAP for web and mobile
- Identify all the security, compliance and contractual requirements for customer access before granting access to data and assets
- Data input and output integrity checks should be implemented on application interfaces and databases to prevent data corruption or errors

Audit Assurance and Compliance

- Audit plans, Contingency plan, and operational action items focusing on data redundancy, access, and data boundary limitations shall be designed to minimize the risk of business process disruption.
- Independent reviews and assessments shall be performed at regular interval. Keep logs and data records for PCI and HIPAA audit
- An inventory of the organization's external legal, statutory, and regulatory compliance obligations should be maintained with respect to any scope whether its data localization or mapping to virtual or physical servers.

Encryption & Key Management

- Strong encryption in standard algorithms shall be required. Keys shall be maintained by the cloud consumer or trusted key management provider
- Keys must have identifiable owners (binding keys to identities) and there shall be key management policies. These shall be managed in a corporate identity management system.
- Policies should be established for lifecycle of key from key generation, key rotation, revocation

Governance & Risk Management

- Risk assessments associated with data governance requirements shall be conducted at planned intervals
- An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction.
- Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and executive approval

Identity & Access Management

- Access to audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.
- User access to diagnostic and configuration ports should be secured and restricted to authorized individuals
- Timely de-provisioning of user access to data and organizationally-owned or managed applications, infrastructure systems, and network components, shall be implemented as per established policies

Infrastructure & Virtualization Security

- The provider should ensure that integrity of all virtual machine images are maintained all the time. Any changes made to VM images must be logged and an alert raised regardless of their running state
- Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls
- Multi-tenant owned or managed applications, and infrastructure system and network components, shall be designed, developed, deployed and configured such that provider and customer user access is appropriately segmented from other tenant users

Interoperability & Portability

- All unstructured data should be available to the customer and provided to them upon request in an industry-standard forma
- The provider should use an industry-recognized virtualization platform and standard virtualization formats
- The provider should use secure standardized network protocols for the import and export of data and to manage the service and make a document for the consumers detailing the relevant interoperability and portability standards that are involved.

Security Incident Management, E-Discovery, & Cloud Forensics

- Mechanisms should be there to monitor and quantify the types, volumes, and costs of information security incidents.
- Policies and procedures should be put in place along with supporting business processes and technical measures implemented to triage security-related events.
- In the event an action concerning a person or organization after an information security incident requires legal action, proper forensic procedures, including chain of custody, shall be required for the preservation and presentation of evidence to support potential legal action subject to the relevant jurisdiction

Threat & Vulnerability Management

- Policies and procedures should be in place along with technical measures to prevent the execution of malware on organizationally-owned or managed user end-point devices
- Policies and procedures should be in place along with technical measures for timely detection of vulnerabilities within owned or managed applications and infrastructure network and system component
- Policies and procedures should be in place along with technical measures to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system

Thank you

ASSURANCE CHALLENGES WITH FEDRAMP

DSCI 523

DEWAINE REDDISH

10/17/2020

USC University of Southern California

USC University of Southern California

CONTENTS

System Class: Cloud Services for U.S. Federal Government

ASSURANCE ISSUES & CONSEQUENCES OF FEDERAL CLOUD USE

- For government, the problems start at policy. Policies vary by agency, customer, use-case and data sensitivity
- All federal agencies are "required" to use FedRAMP
- Federal agencies looking to use cloud offerings on the FedRAMP marketplace are effectively being asked to trust other agencies and the 3PAO selected by FedRAMP
  - Federal agencies tend to be siloed and untrusting of other agencies
- Loss of Protected Health Information [PHI] (Accenture – healthcare.gov)
- General Controlled Unclassified Information [CUI – Formerly FOUO] (Google – G Suite)
- Federal Tax Information [FTI] (IRS.gov)
- Access to all sorts of data and systems (GSA – Login.gov)
- Personally Identifiable Information [PII] (Social Security Administration "Agency Cloud Initiative-Amazon Web")
  - 22 systems to external cloud environments hosted by 11 different providers as of August 2019

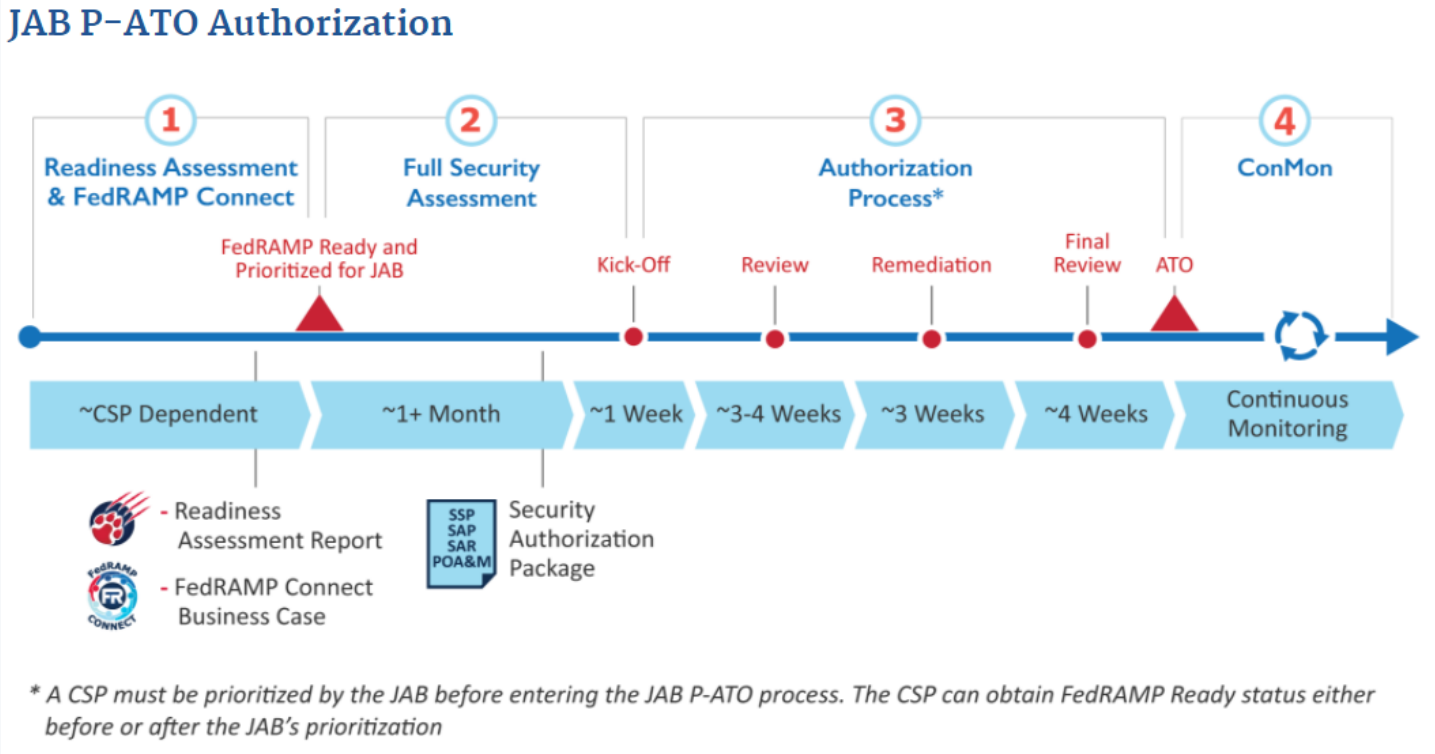
Federal systems are diverse, storing and processing data from a wide array of classes and sensitivity levels

FEDRAMP INTRODUCTION

- FedRAMP is the Federal Risk and Authorization Management Program
- Mandatory for all federal government agencies who need to perform risk assessments or grant ATOs for cloud services
- Intended to enable agencies to leverage previously issued ATOs from other agencies
- Costs cloud offering providers $250k – $5M for an authorization decision (FedRAMP only provides a Provisional ATO (P-ATO); full ATO must still be issued by a customer Federal Agency)
- Marketplace for agency organizations to find approved cloud service offerings that are already 'secure'.

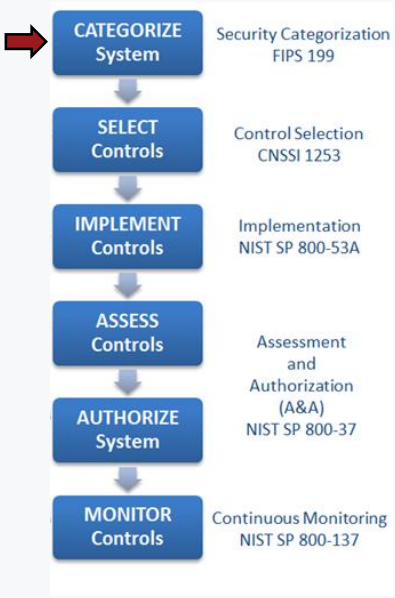
ATO Reuse Could Save Hundreds of Millions of Dollars for the Federal Government Each Year

FEDRAMP INTRODUCTION



System Design / Development > "Policy" Creation > Security Assessment/Authorization > Customer Gets Involved

FEDRAMP ATO PROCESS



The potential impact is high if—

- The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
- A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Table 2-2. Sensitivity Categorization of Information Types

Information Type (Use only information types from NIST SP 800-60, Volumes I and II as amended)	NIST 800-60 identifier for Associated Information Type	Confidentiality	Integrity	Availability
<Enter Information Type>	<Enter NIST Identifier>	Choose level.	Choose level.	Choose level.
<Enter Information Type>	<Enter NIST Identifier>	Choose level.	Choose level.	Choose level.
<Enter Information Type>	<Enter NIST Identifier>	Choose level.	Choose level.	Choose level.

2.2. Security Objectives Categorization (FIPS 199)

Based on the information provided in Table 2-2. Sensitivity Categorization of Information Types, for the Enter Information System Abbreviation, default to the high-water mark for the Information Types as identified in Table 2-3. Security Impact Level below.

Table 2-3. Security Impact Level

Security Objective	Low, Moderate or High
Confidentiality	Choose level.
Integrity	Choose level.
Availability	Choose level.

Categorization is essentially identical to generic Risk Management Framework process

FEDRAMP ATO PROCESS

FedRAMP *Tailored* LI-SAAS Baseline - Details

No.	Control ID	Control Name	Tailoring Action	Additional Tailoring Comments
55	IA-5 (11)	Authenticator Management | Hardware Token-Based Authentication	FED, Document and Assess (Conditional)	FED - for Federal privileged users. Condition - Must document and assess for privileged users. May attest to this control for non-privileged users.
56	IA-6	Authenticator Feedback	Document and Assess	
57	IA-7	Cryptographic Module Authentication	Attest	
58	IA-8	Identification and Authentication (Non-Organizational Users)	Attest	
59	IA-8 (1)	Identification and Authentication (Non-Organizational Users) | Acceptance of PIV Credentials from Other Agencies	Document and Assess (Conditional)	Condition: Must document and assess for privileged users. May attest to this control for non-privileged users. FedRAMP requires a minimum of multi-factor authentication for all Federal privileged users, if acceptance of PIV credentials is not supported. The implementation status and details of how this control is implemented must be clearly defined by the CSP.
60	IA-8 (2)	Identification and Authentication (Non-Organizational Users) | Acceptance of Third-Party Credentials	Document and Assess (Conditional)	Condition: Must docume users. May attest to this users. FedRAMP require authentication for all Fe acceptance of PIV creder implementation status a control is implemented CSP.
61	IA-8 (3)	Identification and Authentication (Non-Organizational Users) | Acceptance of FICAM-Approved Products	Attest	
62	IA-8 (4)	Identification and Authentication (Non-Organizational Users) | Use of U.S. Federal Identity, Credential and Access Management (FICAM)-Issued Profiles	Attest	

Tailoring Symbol	Tailoring Criteria
FED	The control is typically the responsibility of the Federal Government, not the CSP.
NSO	FedRAMP has determined the control does not impact the security of the Cloud SaaS.
Document and Assess	The control must be documented in Appendix B, and independently assessed. This does not mean that a vendor will necessarily have each control fully implemented or implemented as stated. A vendor must address how they meet (or don't meet) the intent of the control so that it can be independently assessed and detail any risks associated with the implementation.
Document and Assess (Conditional)	If the condition exists, the control must be documented in Appendix B and independently assessed as above. If the condition does not exist, the CSP must attest to this in Appendix E.
Attest	The control must exist; however, the CSP may attest to its existence in Appendix E. (No documentation or independent assessment is required.)

Control selection baselines are tailored for cloud offerings by FedRAMP

FEDRAMP ATO PROCESS

2) Control Origination

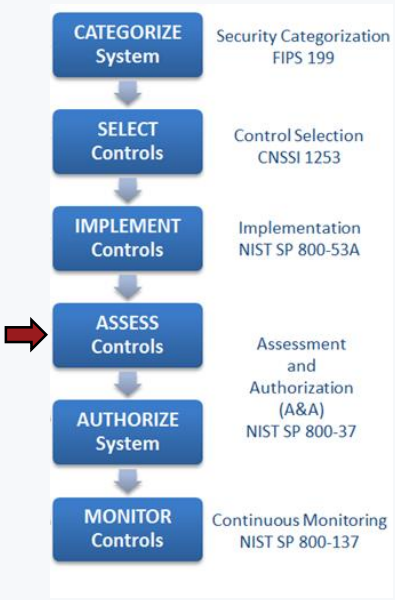
"Control Origination" refers to which entity has responsibility for implementing the control. The following table defines the control origination options.

Control Origination and Definition

Control Origination	Definition	Example
Service Provider Corporate	A control that originates from the CSP's corporate network.	Domain Name System (DNS) from the corporate network provides address resolution services for the information system and the service offering.
Service Provider System Specific	A control specific to a particular CSP system and the control is not part of the service provider corporate controls.	A unique host-based intrusion detection system (HIDS) is available on the service offering platform that is separate from the corporate network and dedicated to the service offering.
Service Provider Hybrid (Corporate and System Specific)	A control that makes use of both corporate controls and additional controls specific to a particular CSP system.	Corporate may provide scanning of the CSP's service offering utilizing the corporate network infrastructure, databases, or web-based applications.
Configured by Customer (Customer System Specific)	A control where the customer needs to apply a configuration to meet the control requirement.	User profiles, policy/audit configurations, enabling/disabling key switches (e.g., enable/disable http or https, etc.), entering an IP range specific to their organization that are configurable by the customer.
Provided by Customer (Customer System Specific)	A control where the customer needs to provide additional hardware or software to meet the control requirement.	The customer provides a Security Assertion Markup Language (SAML) Single Sign On (SSO) solution to implement two-factor authentication.
Shared (Service Provider and Customer Responsibility)	A control that is managed and implemented partially by the CSP and partially by the customer.	Security awareness training must be conducted by both the CSP and customer.
Inherited from Pre-Existing Authorization	A control that is inherited (by the CSP service offering) from another CSP system that has already received a FedRAMP Authorization.	A Platform as a Service (PaaS) or Software as a Service (SaaS) provider inherits Physical and Environmental Protection (PE) controls from an Infrastructure as a Service (IaaS) provider.

CSP Performs Control Implementation for Most Controls

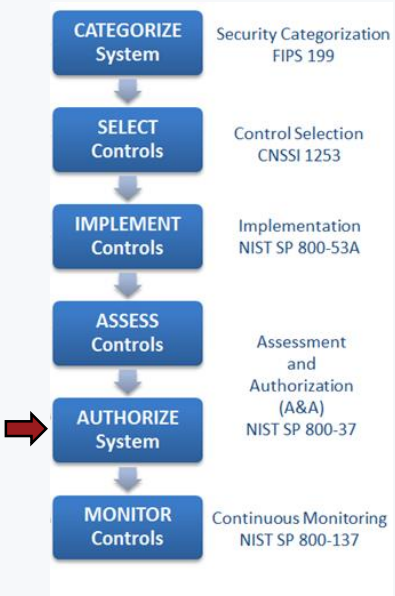
FEDRAMP ATO PROCESS



- FedRAMP assigns 3rd party assessors from their list of available and qualified companies.
- *Third party assessors may have undisclosed relationships with the Cloud Service Provider*
- Classified system control assessment:
  - DoD Collateral
    - Controls assessed by thee Defense Counterintelligence and Security Agency using the DCSA Assessment and Authorization Process Manual (DAAPM)
  - USAF Special Access Program Systems
    - Controls assessed by the Air Force Office of Special Investigations (AFOSI) using the JSIG

Control Assessment Performed by 3rd Party Assessor Selected by FedRamp

FEDRAMP ATO PROCESS



- P-ATO (Provisional Authority to Operate) granted by FedRAMP
  - P-ATO authorizes the cloud service provider to do nothing; authorizes federal agencies to do nothing… this is just a FedRAMP 'thumbs up'
- Real ATO must be granted by the customer / Federal Agency

--

FEDRAMP ATO PROCESS

5. Think of FedRAMP as a continuous program, rather than just a project with a start and end date.

The initial authorization represents a major milestone, but only represents a system's risk posture at a single point in time. Security applies throughout the lifecycle of a system; cloud services must be continuously monitored and kept up to date to ensure the appropriate risk posture is maintained.

FedRAMP Marketplace Participation Requires Continuous Monitoring

FEDRAMP ASSURANCE CHALLENGES

Control SI-02

The organization:
a. Identifies, reports, and corrects information system flaws;
b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Installs security-relevant software and firmware updates within [Assignment: organization- defined time period] of the release of the updates; and
…

- **This control effectively enables cloud service providers to change functionality of their SW without oversight**
  - **Agencies likely need additional assurance measures on system updates to protect against bad actors within the CSO or supply chain attacks on the CSO**

Not inherently a FedRAMP problem; but this problem is compounded by multi-customer cloud offering model.

FEDRAMP ASSURANCE CHALLENGES

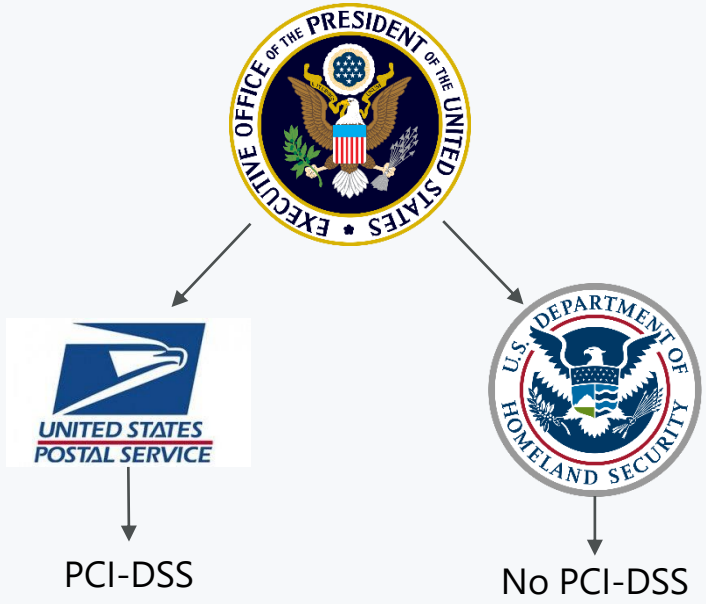
Control SI-12

The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Supplemental Guidance: Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems. The National Archives and Records Administration provides guidance on records retention. Related controls: AC-16, AU-5, AU-11, MP-2, MP-4.

Control Enhancements: None.

References: None.



Different use cases require different policies. Different policies require different controls.
Changing policy or security controls means previous assurance work is no longer valid/complete.

FEDRAMP ASSURANCE CHALLENGES

Control SI-12 Continued…

Binding Operational Directive 17-01

September 13, 2017

Removal of Kaspersky-branded Products

This page contains a web-friendly version of the Department of Homeland Security's Binding Operational Directive 17-01, "*Removal of Kaspersky-branded Products*".

A binding operational directive is a compulsory direction to federal, executive branch, departments and agencies for purposes of safeguarding federal information and information systems.

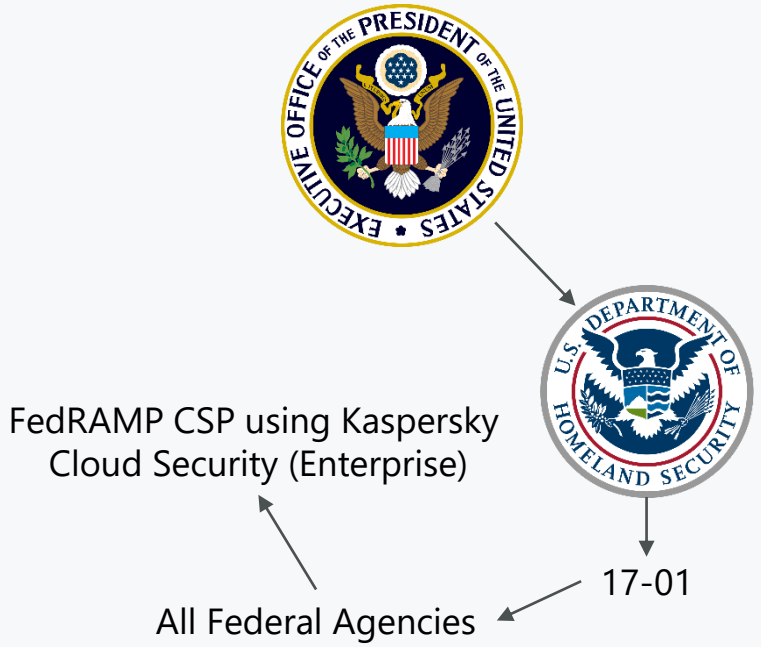
The Department of Homeland Security (DHS) develops and oversees the implementation of binding operational directives pursuant to the Federal Information Security Modernization Act of 2014.

Federal agencies are required to comply with DHS-developed directives.

DHS binding operational directives do not apply to statutorily defined "National Security Systems" nor to certain systems operated by the Department of Defense or the Intelligence Community. Id. § 3553(d)-(e).

Background

DHS, in consultation with interagency partners, has determined that the risks presented by Kaspersky-branded products justify issuance of this Binding Operational Directive.



Different use cases require different policies. Different policies require different controls.
Changing policy or security controls means previous assurance work is no longer valid/complete.

FEDRAMP ASSURANCE CHALLENGES

Control PE-3.a.2.1

The organization:
a. Enforces physical access authorizations at organization-defined entry/exit points to the facility where the information system resides by: verifying individual access authorizations before granting access to the facility"

- **In an environment where the Federal Government is implementing the IS/service (non-cloud), federal assessors and agencies have authority to directly assess these controls.**
- **Agencies must trust both the CSP and the 3PAO on their level of rigor in enforcing many of these non-digital controls.**

- **Many federal agencies will desire only US citizens who pass a background check have physical access; CSP may stand to benefit financially by having non-US citizens or those without background checks perform maintenance functions.**

Not inherently a FedRAMP problem; but this problem is compounded by multi-customer cloud offering model

FEDRAMP ASSURANCE CHALLENGES

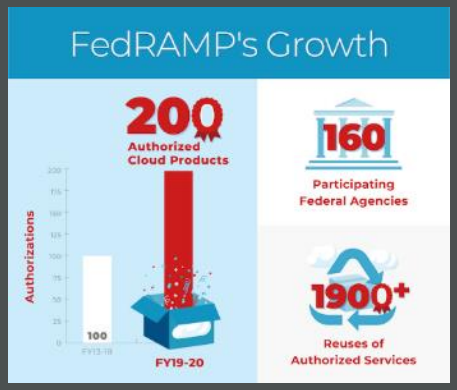
Control PS-7.a

The organization:
a. Establishes personnel security requirements, including security roles and responsibilities, for third-party providers

- **Effectively requires a CSP renegotiate their physical access policies with EACH federal customer prior to changing their own sub-contractor/supplier relationships and agreements.**

- **Despite the fact that the Risk Management Framework documentation necessitates certain agreements, the practicality of consistently enforcing certain controls brings into question how much assurance agencies have that the CSP is actually adhering to the stated policy over the long run.**

Documentation ≠ Assurance



amazon web services™

Amazon - AWS US East/West

Akamai

Akamai - Content Delivery Services

TROJAN FAMILY

WE FIGHT AS ONE

USC University of Southern California

THE RISK MANAGEMENT FRAMEWORK (RMF) AND NATIONAL SECURITY SYSTEMS

SARAHZIN CHOWDHURY

DSCI 523

NOVEMBER 17, 2020

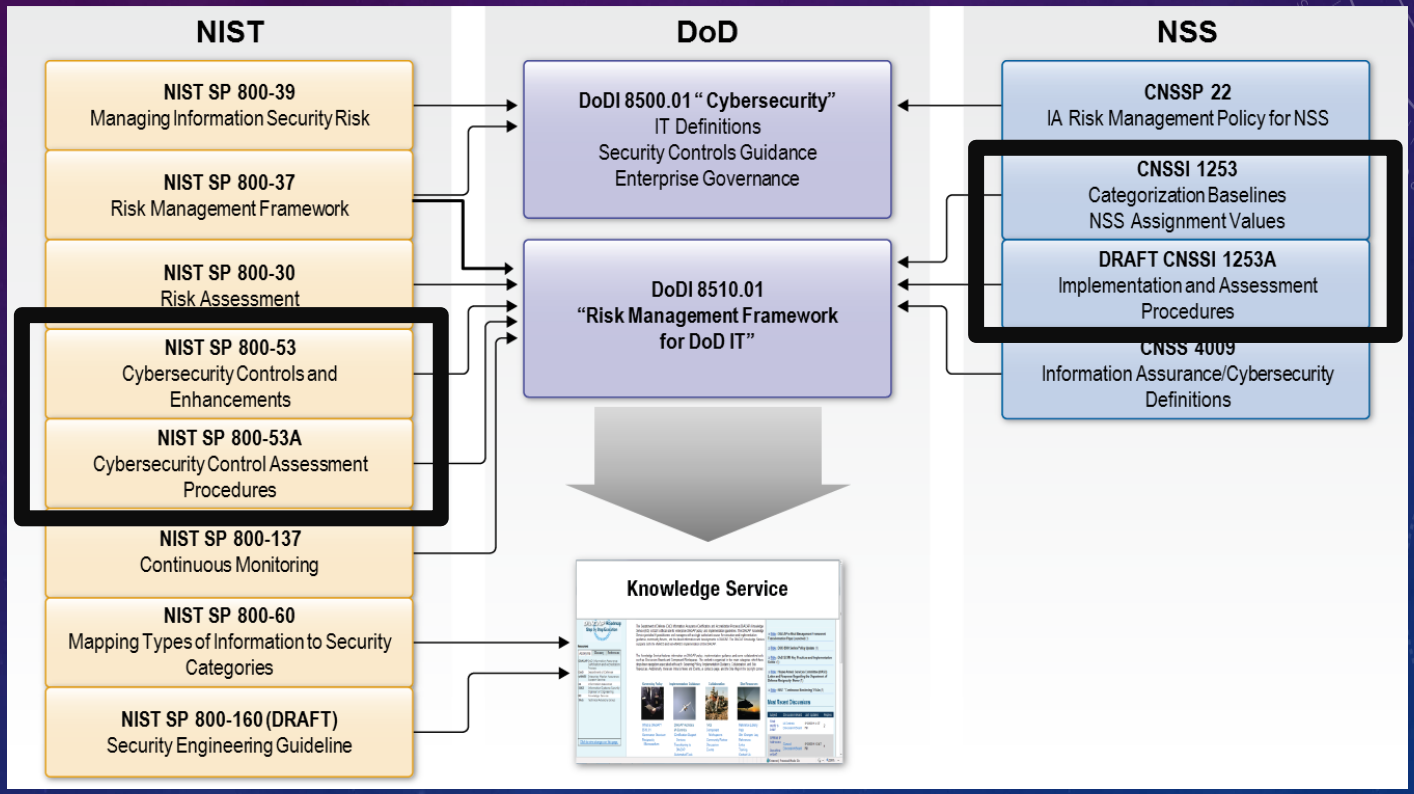
AGENDA

- Overview
- Background
- Questions

OVERVIEW

- Federal Information Security Management Act (FISMA) requires government agencies to implement an information security program that effectively manages risk
- National Institute of Standards and Technology (NIST) is a non-regulatory agency that has issued specific guidance for complying with FISMA
- NIST SP 800-53 represents the security controls and associated assessment procedures defined in NIST SP 800-53 Revision
- Department of Defense (DoD) Instruction (DoDI) 8510.01, “Risk Management Framework (RMF) for DoD Information Technology (IT)”
  - Establishes the associated cybersecurity policy and assigns responsibilities for executing and maintaining the DoD RMF
- RMF is the “common information security framework” for the federal government and its contractors
  - To improve information security
  - To strengthen risk management processes
  - To encourage reciprocity among federal agencies

STANDARDS


NIST
NIST SP 800-39
Managing Information Security Risk
NIST SP 800-37
Risk Management Framework
NIST SP 800-30
Risk Assessment
NIST SP 800-53
Cybersecurity Controls and Enhancements
NIST SP 800-53A
Cybersecurity Control Assessment Procedures
NIST SP 800-137
Continuous Monitoring
NIST SP 800-60
Mapping Types of Information to Security Categories
NIST SP 800-160 (DRAFT)
Security Engineering Guideline
DoD
DoDI 8500.01 " Cybersecurity"
IT Definitions
Security Controls Guidance
Enterprise Governance
DoDI 8510.01
"Risk Management Framework for DoD IT"
Knowledge Service
NSS
CNSSP 22
IA Risk Management Policy for NSS
CNSSI 1253
Categorization Baselines
NSS Assignment Values
DRAFT CNSSI 1253A
Implementation and Assessment Procedures
CNSS 4009
Information Assurance/Cybersecurity Definitions

CIA TRIAD

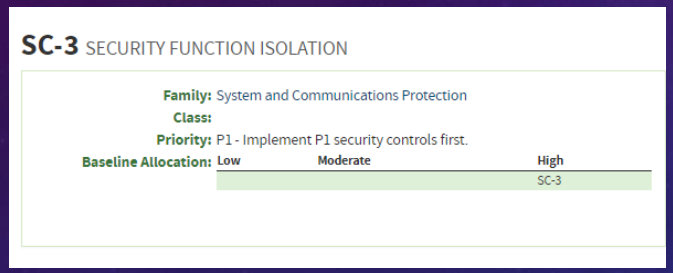
Table 1: Information and Information System Security Objectives

Security Objectives	FISMA Definition [44 U.S.C., Sec. 3542]	FIPS 199 Definition
Confidentiality	"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…"	A loss of *confidentiality* is the unauthorized disclosure of information.
Integrity	"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…"	A loss of *integrity* is the unauthorized modification or destruction of information.
Availability	"Ensuring timely and reliable access to and use of information…"	A loss of *availability* is the disruption of access to or use of information or an information system.

CONTROL FAMILIES

- Risk Assessment
- Certification, Accreditation and Security Assessments
- System Services and Acquisition
- Security Planning
- Configuration Management
- System and Communications Protection
- Personnel Security
- Awareness and Training
- System and Information Integrity
- Incident Response
- Identification and Authentication
- Access Control
- Accountability and Audit
- Physical and Environmental Protection
- Media Protection
- Contingency Planning

CONTROL EXAMPLE



SC-3 SECURITY FUNCTION ISOLATION

Family: System and Communications Protection
Class:
Priority: P1 - Implement P1 security controls first.
Baseline Allocation:

Low	Moderate	High
		SC-3

Control Description

The information system isolates security functions from nonsecurity functions.

Supplemental Guidance

The information system isolates security functions from nonsecurity functions by means of an isolation boundary (implemented via partitions and domains). Such isolation controls access to and protects the integrity of the hardware, software, and firmware that perform those security functions. Information systems implement code separation (i.e., separation of security functions from nonsecurity functions) in a number of ways, including, for example, through the provision of security kernels via processor rings or processor modes. For non-kernel code, security function isolation is often achieved through file system protections that serve to protect the code on disk, and address space protections that protect executing code. Information systems restrict access to security functions through the use of access control mechanisms and by implementing least privilege capabilities. While the ideal is for all of the code within the security function isolation boundary to only contain security-relevant code, it is sometimes necessary to include nonsecurity functions within the isolation boundary as an exception.

Related to: AC-3 , AC-6 , SA-4 , SA-5 , SA-8 , SA-13 , SC-2 , SC-7 , SC-39

Control Enhancements

SC-3 (1) SECURITY FUNCTION ISOLATION | HARDWARE SEPARATION
The information system utilizes underlying hardware separation mechanisms to implement security function isolation.

Supplemental Guidance: Underlying hardware separation mechanisms include, for example, hardware ring architectures, commonly implemented within microprocessors, and hardware-enforced address segmentation used to support logically distinct storage objects with separate attributes (i.e., readable, writeable).

SC-3 (2) SECURITY FUNCTION ISOLATION | ACCESS / FLOW CONTROL FUNCTIONS
The information system isolates security functions enforcing access and information flow control from nonsecurity functions and from other security functions.

Supplemental Guidance: Security function isolation occurs as a result of implementation; the functions can still be scanned and monitored. Security functions that are potentially isolated from access and flow control enforcement functions include, for example, auditing, intrusion detection, and anti-virus functions.

SECURITY CONTROL BASELINE

Table D-1: NSS Security Control Baselines

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X
AC-2	Account Management	X	X	X	X	X	X			
AC-2(1)	Account Management | Automated System Account Management		X	X		X	X			
AC-2(2)	Account Management | Removal of Temporary / Emergency Accounts		X	X		X	X			
AC-2(3)	Account Management | Disable Inactive Accounts		X	X		X	X			
AC-2(4)	Account Management | Automated Audit Actions	+	X	X	+	X	X			
AC-2(5)	Account Management | Inactivity Logout							+	+	X
AC-2(6)	Account Management | Dynamic Privilege Management									
AC-2(7)	Account Management | Role-Based Schemes	+	+	+	+	+	+			
AC-2(8)	Account Management | Dynamic Account Creation									
AC-2(9)	Account Management | Restrictions on Use of Shared Groups / Accounts	+	+	+	+	+	+			
AC-2(10)	Account Management | Shared / Group Account Credential Termination	+	+	+	+	+	+			
AC-2(11)	Account Management | Usage Conditions									
AC-2(12)	Account Management | Account Monitoring / Atypical Usage	+	+	X	+	+	X			
AC-2(13)	Account Management | Disable Accounts For High-Risk Individuals	+	+	X	+	+	X			
AC-3	Access Enforcement	X	X	X	X	X	X			

"X" = Security Controls from NIST Baselines

"+" = Security Controls Added for Protection of NSS

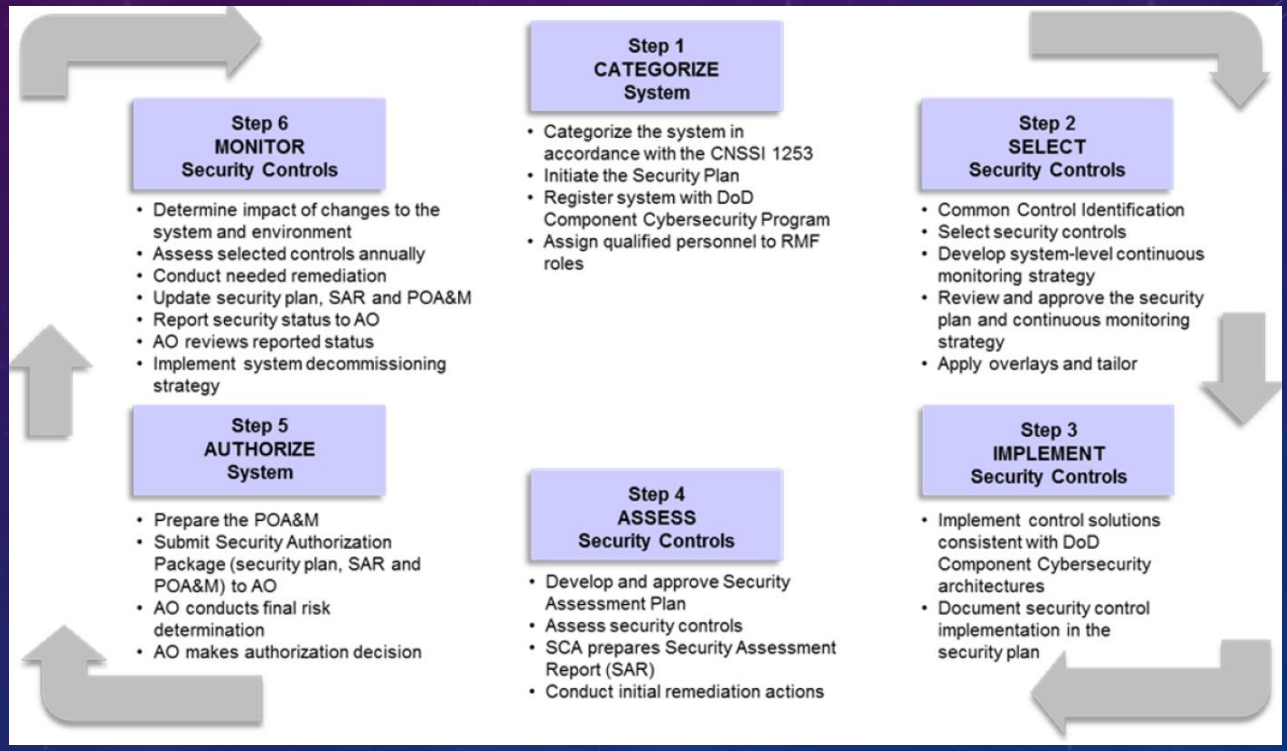
Not all DoD ISs are NSS, however, the same standards and processes under the RMF also apply to ISs that are not NSSs

DOD OVERLAYS

Approved

- **Space Platforms**
- **Cross Domain Solutions**
- **Classified Information**
- **Privacy Information**
- **Industrial Control Systems**
- **Supply Chain**
- **Email**

RMF STEPS

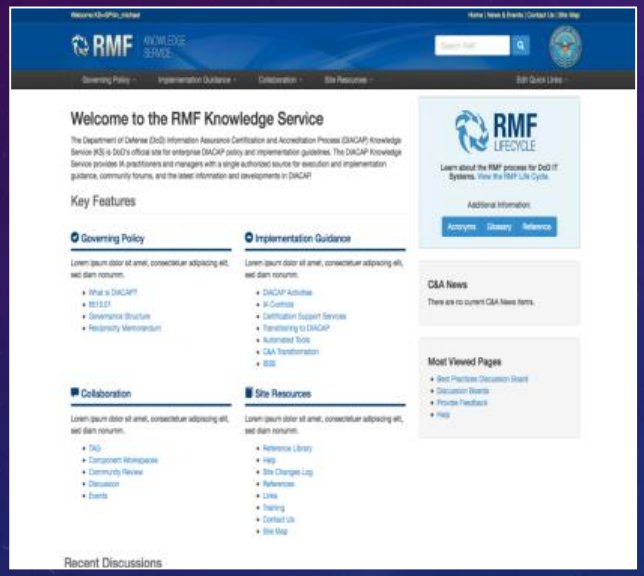

Step 1
CATEGORIZE
System
• Categorize the system in accordance with the CNSSI 1253
• Initiate the Security Plan
• Register system with DoD Component Cybersecurity Program
• Assign qualified personnel to RMF roles
Step 2
SELECT
Security Controls
• Common Control Identification
• Select security controls
• Develop system-level continuous monitoring strategy
• Review and approve the security plan and continuous monitoring strategy
• Apply overlays and tailor
Step 3
IMPLEMENT
Security Controls
• Implement control solutions consistent with DoD Component Cybersecurity architectures
• Document security control implementation in the security plan
Step 4
ASSESS
Security Controls
• Develop and approve Security Assessment Plan
• Assess security controls
• SCA prepares Security Assessment Report (SAR)
• Conduct initial remediation actions
Step 5
AUTHORIZE
System
• Prepare the POA&M
• Submit Security Authorization Package (security plan, SAR and POA&M) to AO
• AO conducts final risk determination
• AO makes authorization decision
Step 6
MONITOR
Security Controls
• Determine impact of changes to the system and environment
• Assess selected controls annually
• Conduct needed remediation
• Update security plan, SAR and POA&M
• Report security status to AO
• AO reviews reported status
• Implement system decommissioning strategy

GOAL

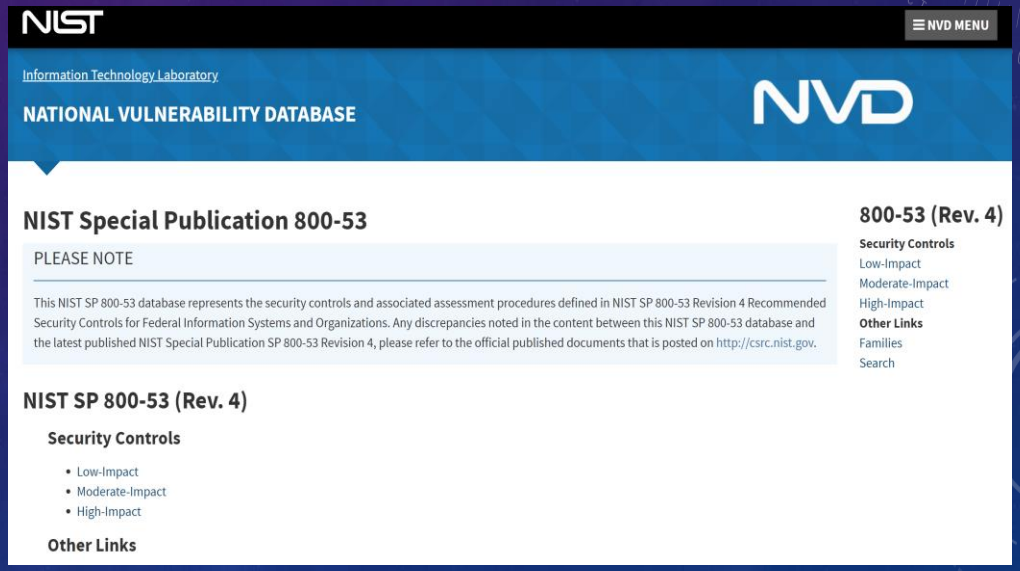
The purpose of RMF is to achieve an authorization to operate (ATO).

RMF KNOWLEDGE SERVICE AND NVD

- The Knowledge Service is the authoritative source for information, guidance, procedures, and templates on how to execute the Risk Management Framework



URL for RMF KS: https://rmfks.osd.mil



https://nvd.nist.gov/800-53

Step 1: Categorize System

STEP 1 – CATEGORIZE SYSTEM

- Assign the three security objectives (confidentiality, integrity, and availability: CIA) with one impact value (low, moderate, or high)
- Document results in the System Security Plan (SSP)
- Describe the system and document description in the SSP
- Register the system in Enterprise Mission Assurance Support Service (eMASS)
- Information System Security Engineer (ISSE) assigns qualified personnel to RMF roles and document team member assignments in the SSP

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Step 2: Select Security Controls

STEP 2 – SELECT SECURITY CONTROLS

- Security Control Selection
- Tailor baseline controls IAW system scope
- Apply overlays: address additional factors beyond impact; Space, Cross Domain Solution, Classified
- Document resulting security controls, supporting selection rationale, and system use limitation in the security plan
- Applicable versus Not-Applicable; goal is for ATO
- ISSE coordinates with stakeholders

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X
AC-2	Account Management	X	X	X	X	X	X			
AC-2(1)	Account Management | Automated System Account Management		X	X		X	X			
AC-2(2)	Account Management | Removal of Temporary / Emergency Accounts		X	X		X	X			
AC-2(3)	Account Management | Disable Inactive Accounts		X	X		X	X			
AC-2(4)	Account Management | Automated Audit Actions	+	X	X	+	X	X			

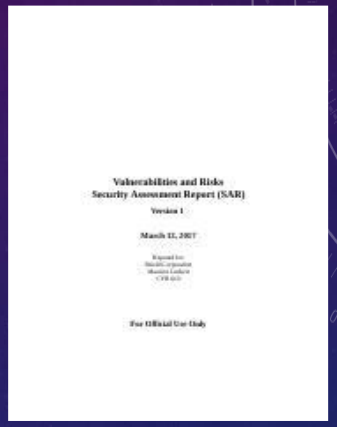
Step 3: Implement Security Controls

STEP 3 – IMPLEMENT SECURITY CONTROLS

- Implementation of Security Controls
- Specified in the SSP
- Document Security Control implementation IAW guidance contained in the RMF Knowledge Service
- Typically done by developing contractor or operations and maintenance contractor
- Ensure compliance during step 4 for ATO

Step 4: Assess Security Controls

STEP 4 – ASSESS SECURITY CONTROLS


Vulnerabilities and Risks
Security Assessment Report (SAR)
Version 1
March 15, 2017
For Official Use Only

- Assessing Security Controls
- Agent of the Security Control Assessor (ASCA) leads step
- Develop, review, and approve a plan to assess the security controls
- Prepare the security assessment report (SAR) documenting the issues, findings, and recommendations from the security control assessment
- ASCA must determine and document in the SAR an assessment of overall system level of risk
- Moderate or below required for ATO

Step 5: Authorize System

STEP 5 – AUTHORIZE SYSTEM

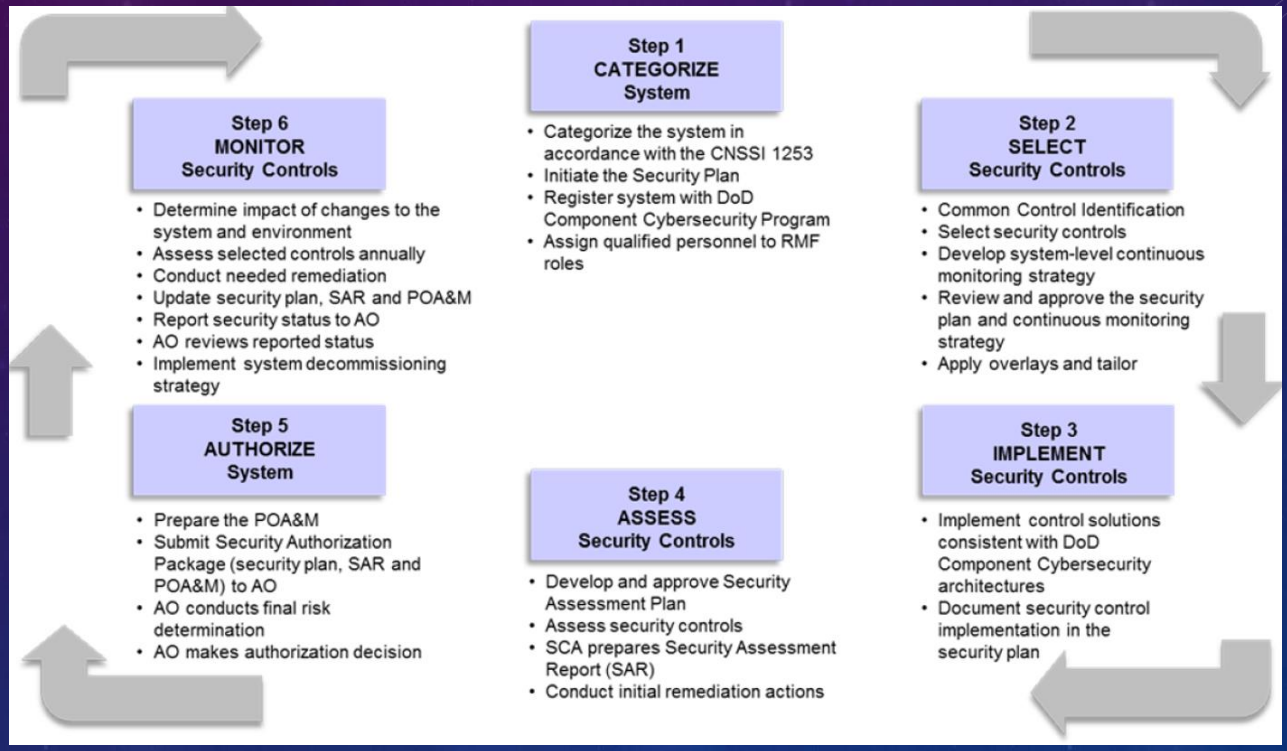
- Authorization of System
- ISSE prepares the plan of action and milestones based on the findings and recommendations of the SAR
- Submit SSP, SAR, and POAM to authorizing official (AO) for ATO

Step 6: Monitor Security Controls

STEP 6 – MONITOR SECURITY CONTROLS

- Monitor Security Controls
- Uncertain for DoD
- Security Information and Event management (SIEM) Solutions
- Cybersecurity Service Provider (CSSP)
- Process repetition
- POAM updates

RMF STEPS


Step 1
CATEGORIZE
System
• Categorize the system in accordance with the CNSSI 1253
• Initiate the Security Plan
• Register system with DoD Component Cybersecurity Program
• Assign qualified personnel to RMF roles
Step 2
SELECT
Security Controls
• Common Control Identification
• Select security controls
• Develop system-level continuous monitoring strategy
• Review and approve the security plan and continuous monitoring strategy
• Apply overlays and tailor
Step 3
IMPLEMENT
Security Controls
• Implement control solutions consistent with DoD Component Cybersecurity architectures
• Document security control implementation in the security plan
Step 4
ASSESS
Security Controls
• Develop and approve Security Assessment Plan
• Assess security controls
• SCA prepares Security Assessment Report (SAR)
• Conduct initial remediation actions
Step 5
AUTHORIZE
System
• Prepare the POA&M
• Submit Security Authorization Package (security plan, SAR and POA&M) to AO
• AO conducts final risk determination
• AO makes authorization decision
Step 6
MONITOR
Security Controls
• Determine impact of changes to the system and environment
• Assess selected controls annually
• Conduct needed remediation
• Update security plan, SAR and POA&M
• Report security status to AO
• AO reviews reported status
• Implement system decommissioning strategy

If these steps are met, this gives the DOD a baseline of an acceptable assurance.

It is important to remember one thing…

The purpose of RMF is to achieve an authorization to operate (ATO).

RISKS IF ATO FAILS

- Authorization to Operate (ATO)
  - Without ATO, system will be decommissioned and/or have high risk
- Impact Examples
  - Top Secret
    - "Top Secret shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause **'exceptionally grave damage'** to the National Security that the original classification authority is able to identify or describe."
  - Secret
    - "This is the second-highest classification. Information is classified Secret when its unauthorized disclosure would cause **'serious damage'** to national security."
  - Confidential
    - "This is the lowest classification level of information obtained by the government. It is defined as information that would **'damage'** national security if publicly disclosed, again, without the proper authorization."

QUESTIONS?

11/17/2020

Identity Tokens & Yubikey

DSCI523 –CASE STUDY– FALL 2020

NOVEMBER 17, 2020

AUTHOR: ARJUN G. RAMAN

CONTACT: ARJUN.RAMAN@USC.EDU

Agenda

Agenda

- What is an Identity Token?
- Yubikey – Physical Key to Digital Life
- Software (SW) & Hardware (HW) Overview
- Example Flows
- Assurance Considerations
- Product Scaling Factors
- Issues & Consequences
- Q&A

Objectives of Case Study

The presentation should identify the system or class of System to detail the following:

- Explain / Summarize the assurance issues that need to be met by the identified system.
- Identify the consequences of security failure in such systems.
- Engage students to discuss in a question-and-answer format

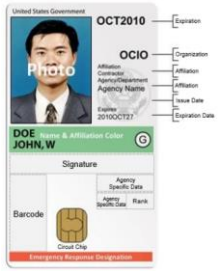
Identity Token?

Identification & Authentication – Who are you? / Prove who you are)

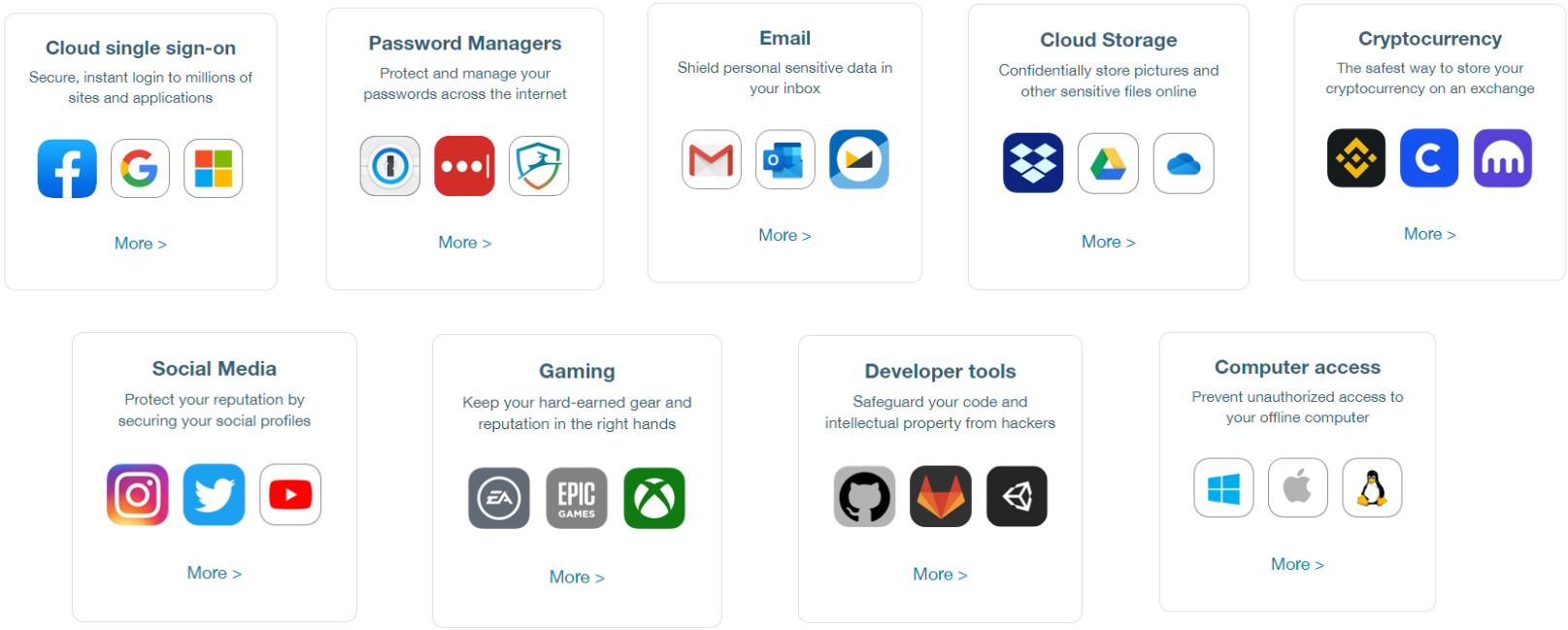
- Something you have (e.g., ID Badge/Key Fob)
- Something you know (PIN/ password)
- Something you are (biometric / voice)

What is an Identity Token?

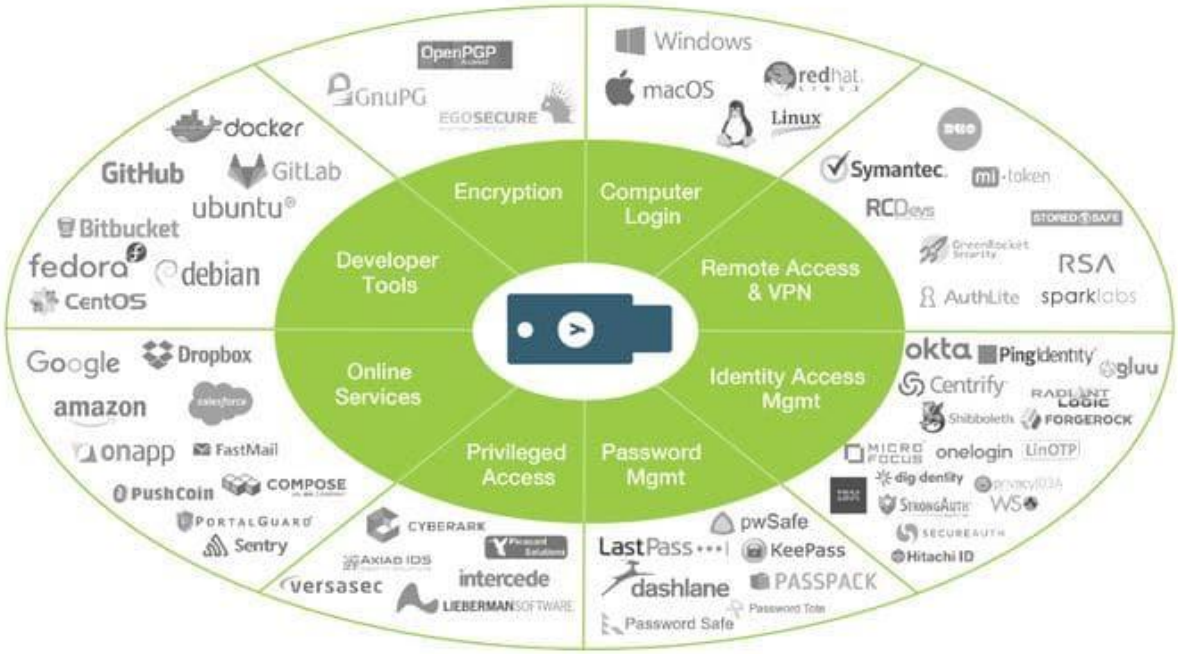
- An identity token is a portable piece of hardware that a user carries and uses to access a network. The token aids in proving the user's identity and authenticating that user for the use of a service.
- Other Examples: security token or an authentication token.



Yubikey – A physical key to digital life – Broad Use Cases

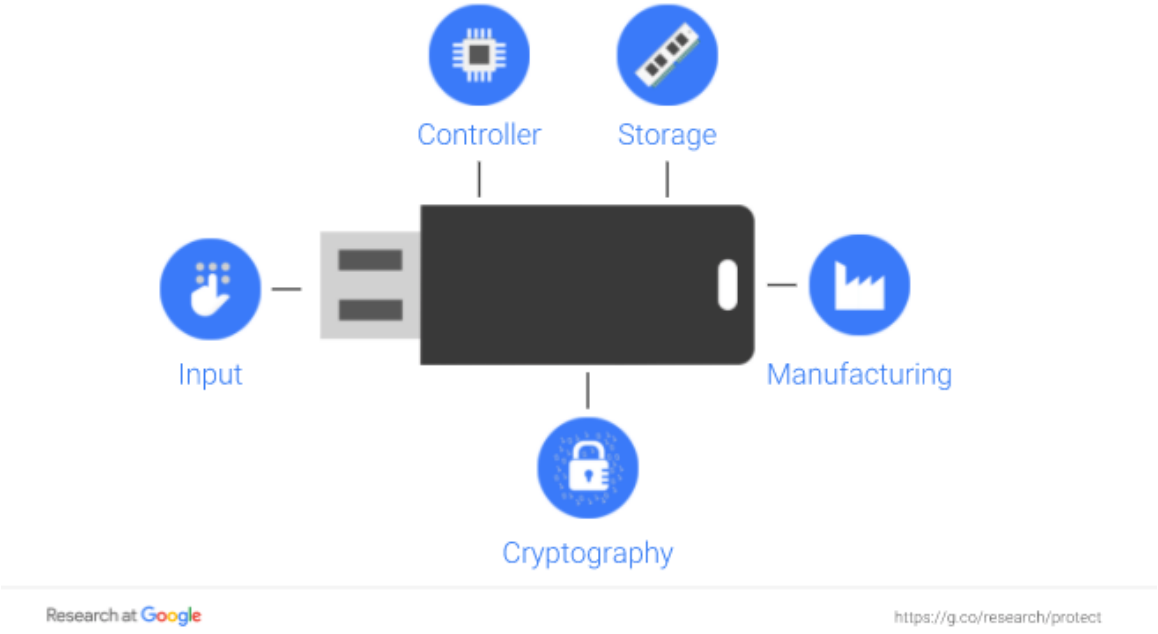


Yubikey – Looked at a Different Way – Being at the Center of It All



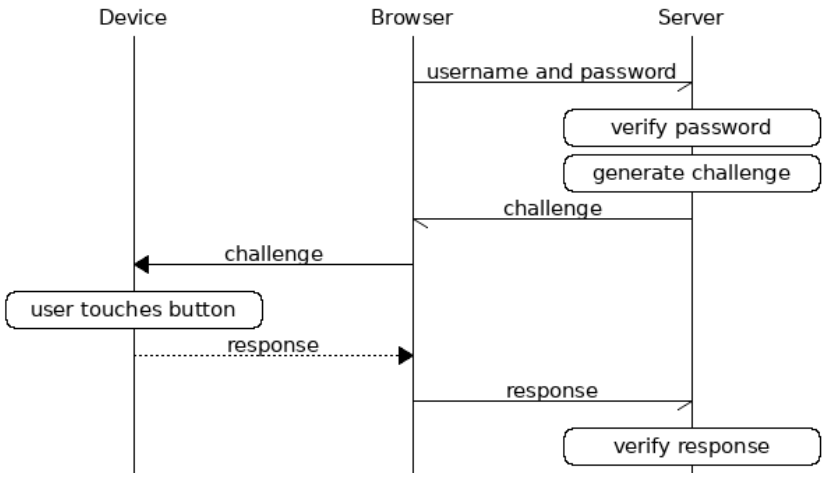
Example Interaction Flow

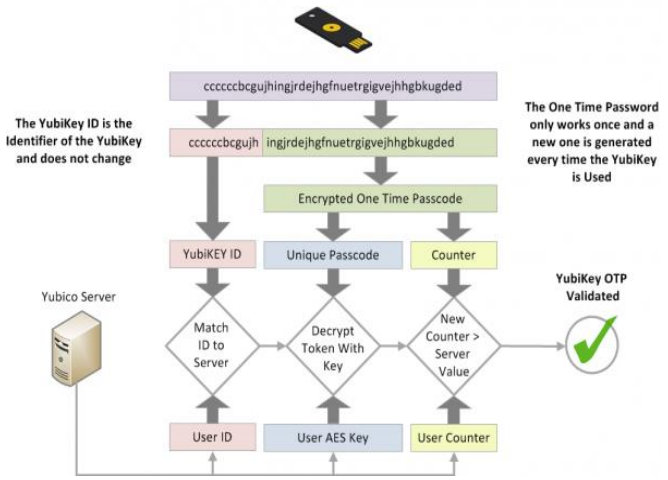
HW & SW come together



Software Overview

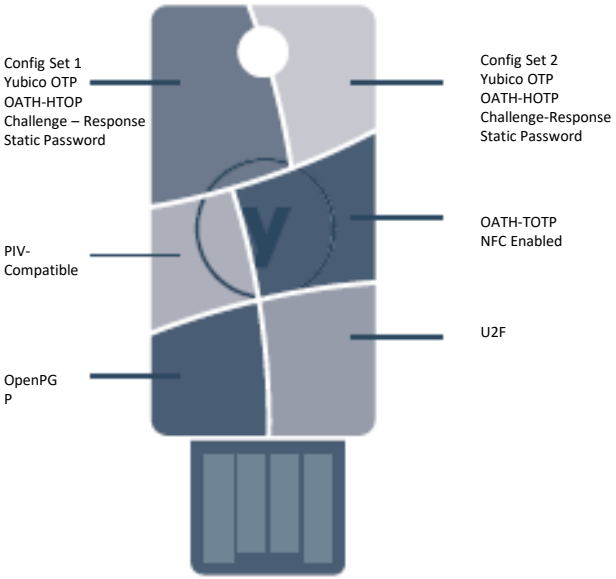
Universal 2nd Factor (U2F) protocol developed by the **FIDO Alliance**





The three authentication functions the YubiKey provides allow the user to authenticate with a smart card, one-time password, and/or a FIDO authenticator, at the same time and on the same device.

Hardware Overview



The YubiKey is a hardware token built using a mono-block design which is hermetically sealed in high quality resin.

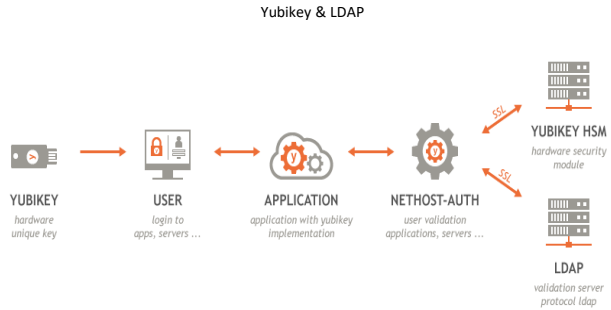
- IP67 class rating, as defined in international standard IEC 60529.
- Withstand 25 Nm of bending force, means the YubiKey easily resists common threats such as water, natural forces within reason, etc.
- One of the core components in the YubiKey is a secure element that protects the key material against hardware-based attacks.
- Meet the requirements FIPS 140-2 for physical security and is on the Process list.

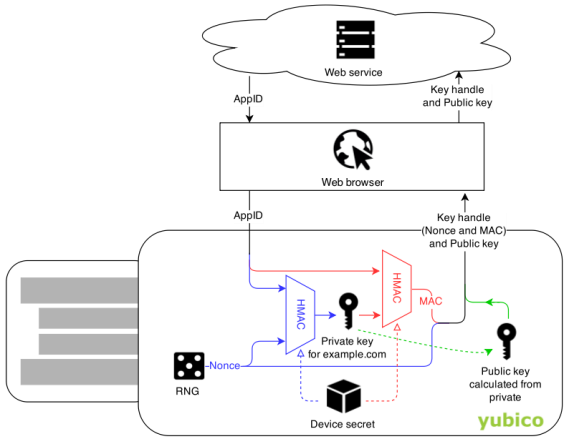
Yubikey-HSM Example:

The hardware security module (HSM) is a trusted network computer performing a variety of cryptographic operations: key management, key exchange, encryption etc.

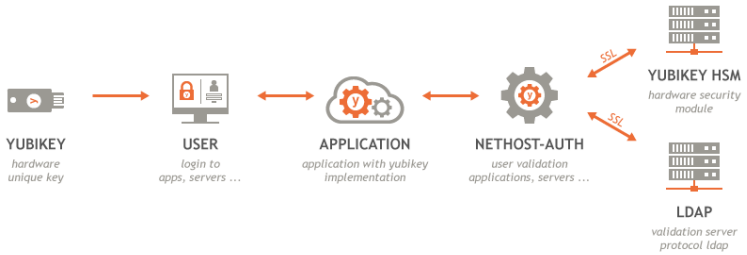
Key Aspects:

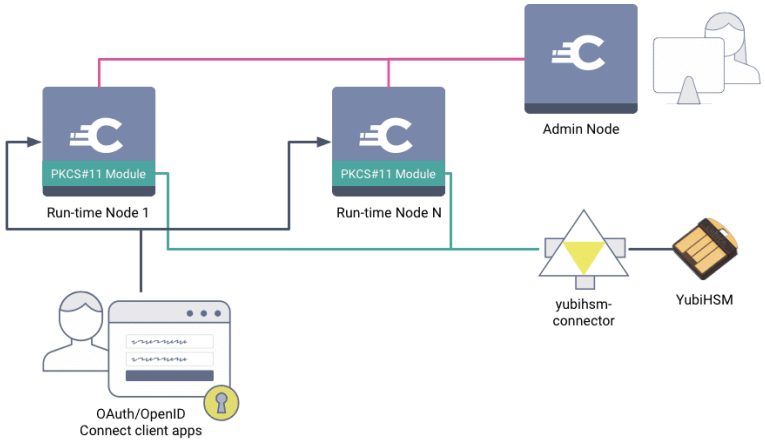
- Is built on top of specialized hardware. The hardware is well-tested and certified in special laboratories.
- Has a security-focused OS.
- Has limited access via a network interface that is strictly controlled by internal rules.
- Actively hides and protects cryptographic material.





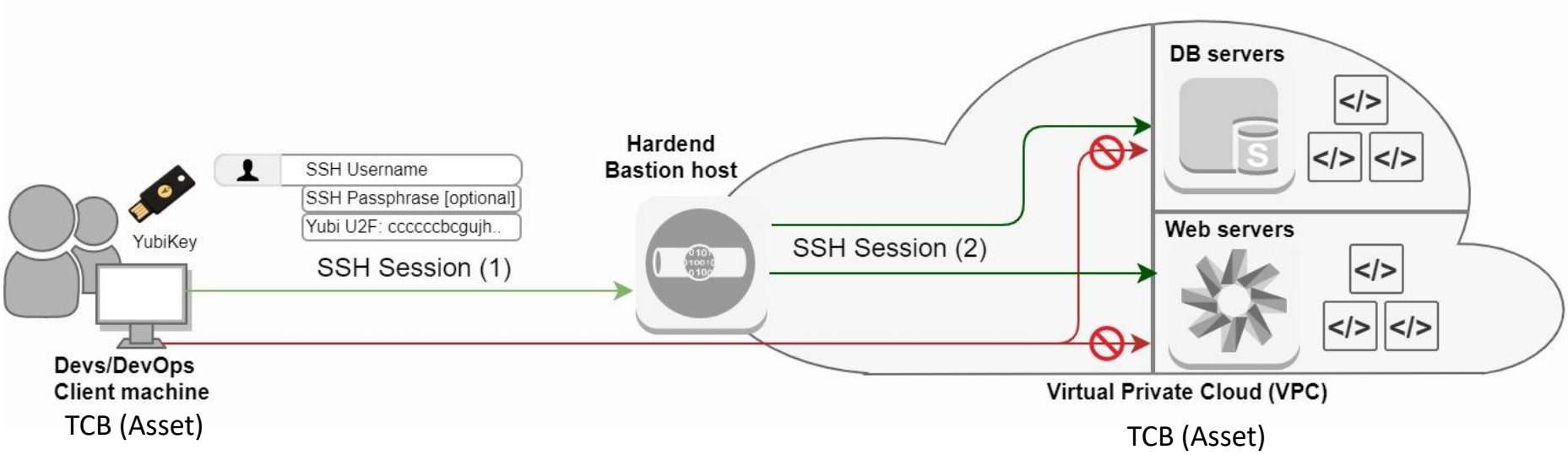
Source: https://www.yubico.com/blog/category/blog/page/3/





Concept – Example – Yubikey & LDAP & HSM

Concept – Example OpenSSH



Software Assurance Considerations

Assurance Item	Assurance Implementation Path for Yubikey
Challenge & Response	Relay Party has public Key of User U2F (Yubikey) has private key of user
Tamper Resistant / Virus Protected	Generating key pairs are in on device in tamper resistant environment. It is not a usb device, and cannot store malicious content.
Phishing & Man-in-the-Middle Protection	Client – Compiles items around HTTP connection (URI & TLS channel ID) U2F device signs and sends to RP Origin – Prevents Phishing; TLS Channel ID
Application Specific Keys	The U2F device generates a new key pair and key handle for each registration. The handle is stored by the RP and sent back to the device upon authentication. This way, the device knows which key to authenticate with (e.g. User1's key or User2's key).
Device Attestation	Attestation Certificate - Attestation gives relying parties the possibility to verify token properties, such as token model. It is implemented via an attestation certificate, signed by the device vendor, that the device sends to the RP upon registration.

Source: https://developers.yubico.com/U2F/Protocol_details/Overview.html

Hardware Assurance Considerations

Assurance Item	Assurance Implementation Path for Yubikey
Physical Contamination or Breaks	Complete protection against ingress of dust and airborne particles (IP67 rating). Withstand 25 Nm of bending force, means the YubiKey easily resists common threats such as water, natural forces within reason, etc.
Epoxy or resin mimicry	The YubiKey is a hardware token built using a mono-block design which is hermetically sealed in high quality resin. Its extremely hard to break the seal and then reseal it.
Theft of Hardware / Swap of Hardware	In cases of MFA tied to the authenticator, the authenticator app is linked to the trusted hardware of the individual (e.g., SmartPhone). Attacker would need to know UN and PW and hold possession of the key.
Cloning Detection	Cloning detection to U2F devices without tamper-resistant secure elements (e.g., software implementations) - The device increments the counter when authenticating, and the RP verifies that the counter is higher than last time.
Counterfeit YubiKey U2F token of an existing User	Malicious actor is able to retain the secret information that they burn into a fake YubiKey, and then convince a user that it's a legitimate YubiKey, they can later impersonate that token (so as long as the counter is synchronized). This is extremely hard to test.
Distributing Counterfeit Keys in mass	3D print a Yubikey replica that could hold their counterfeit circuit board. This attack could be implemented in the supply chain, by swapping out authentic YubiKeys for these fakes, but supply chain interference is always a difficult task. A more feasible scenario, if the attacker has specific targets, would be to hand them out as a "public service" at an infosec event.
Open Source vs. Closed Source.	Often, the notion of "open-source hardware" sounds like a great idea, except for the not-so-tiny complication of actually producing the hardware from the specifications. Recent advances in consumer-grade CNC machines have started to make homemade printed circuit boards (PCBs) feasible, but it's still time- and material-intensive to iterate. Yubikey is considered closed source hardware however can be mimicked such as in case of Field-programmable gate arrays (FPGAs).

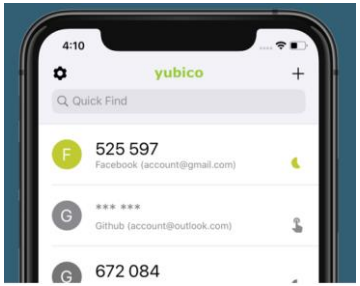
Product Scaling Factors in Context of Assurance

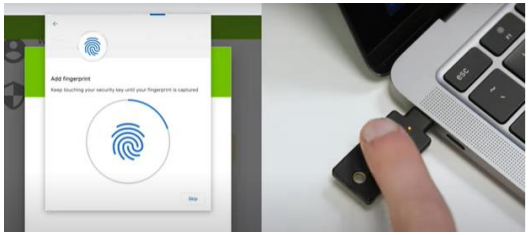
Blue-tooth NFC

Authenticator App

Biometric Enabled Key for Password less Login

Digital Assets





Issues & Consequences – Future Considerations

SW Issues

- Loss of Access / Limitations of Access – Tedious for the user if key is tampered with or protocol does not sync/work
- Forgetfulness – Forgetting your token if inputted into the device
- With potential for biometric, the focus on how that data is protected will be critical if attacker understands key structure.
- Malicious Code Injection / Trojans from USB Port

HW Issues

- Different security postures of hardware keys
- Partnerships – RSA + Yubikey
- Counterfeiting Security Tokens
- Hardware Transparency – Trusting Circuitry and firmware.

Thank You

Q&A + DISCUSSION

Open Source HW and Field-programmable gate arrays (FPGAs)

These attacks certainly serve to instill some distrust of “secure hardware,” which raises the question of: “What do we do when we don’t trust the circuitry and firmware?” One possible approach using open-source hardware was described by 0ctane in their DEF CON talk, “Untrustworthy Hardware and How To Fix It: Seeking Hardware Transparency”.

Often, the notion of “open-source hardware” sounds like a great idea, except for the not-so-tiny complication of actually producing the hardware from the specifications. Recent advances in consumer-grade CNC machines have started to make homemade printed circuit boards (PCBs) feasible, but it’s still time- and material-intensive to iterate.

Field-programmable gate arrays (FPGAs) are one option in this situation. An FPGA is a piece of hardware that can best be likened to software-defined microchip: the user sends a definition of the circuitry they want, and the FPGA configures itself to implement that hardware definition. They are usually used for prototyping, debugging hardware, or performing complex digital signal processing. The curious reader may be interested in taking a deeper dive into what FGPAs actually are, but that’s beyond the scope of this discussion.

0ctane proposes a cryptographic purpose: simulating a particular definition of a trusted CPU (in this case, OpenRISC), and running Linux and the desired cryptographic software on top of this simulated processor. The downside to using FPGAs is that the customizability comes at the cost of speed, when compared to silicon CPUs. Top-of-the-line FPGAs still run slower due to the need to buffer input and output between the cells, rather than the circuitry being optimally laid out, as is the case for a silicon chip.

For this application, however, that might be an entirely acceptable tradeoff: slower operation and computation in exchange for *knowing* that your code is running on a trusted stack, from the hardware up. In addition, there are some unanswered questions as to how sound this approach is. It’s unclear to the author whether an FPGA is harder for an attacker to surreptitiously insert malicious logic than it is with a CPU, since this approach requires trusting the FPGA and its programmer software (running on an untrusted CPU).

There’s also an assumption made that OpenRISC is itself more secure than an Intel or AMD x86 chip. As we’ve seen in case after case, just being open-source doesn’t mean that software is more secure. It does provide visibility that you don’t otherwise have, but you either have to read all the software and convince yourself of its security properties, or you have to also place trust in the OpenRISC project to make a secure processor. 0ctane’s proposal is an interesting one, but it needs more data and discussion to be a viable approach; we look forward to hearing more from them in the future.

FPGAs aren’t the solution to all of our concerns about hardware security, and you have to place your trust somewhere, unless you can oversee the entire design and supply chain. This approach could potentially be valuable in the future when trusted hardware is essential, such as a standalone code-signing computer with the keys in a hardware security module, which are designed to break before revealing their private information. There are definitely issues with this solution as it stands, though. Hardware hackers are a tenacious bunch, such as when Mikhail on our research team hacked our office doors. In reality, there doesn’t seem to be much of a supply-chain threat if you’re buying your hardware from a trusted supplier. However, you might want to think twice before using a YuibKey that somebody hands you at a crypto meetup…

Source: https://duo.com/decipher/dissecting-security-hardware-at-black-hat-and-def-con

Security Assurance for Isolation Technologies

- Ayush Ambastha

What is Assurance?

Security assurance is the guarantee provided with regard to access control, security privileges, and enforcement over time as users interact with an application.

It's the trust that a system correctly enforces a security policy. Also, these assurance techniques must be applied at all stages of the system life cycle.

For Hardware Isolation Technologies, we want to make sure that the authenticity of the platform, the OS, or even the component is attested, which in turn allows us to work in a trusted environment.

In the context on Software Isolation technologies, we want to make sure that an application running within a sandboxed environment is protected from illegitimate access to it and is independent of any other application on the system.

Hardware Isolation Technologies

Trusted Platform Module (TPM)

- A Trusted Platform Module (TPM) is a specialized chip on an endpoint device that stores RSA encryption keys specific to the host system for hardware authentication.
- Each TPM chip contains an RSA key pair called the Endorsement Key (EK), and it cannot be accessed by software. The Storage Root Key (SRK) is created when a user or administrator takes ownership of the system. This key pair is generated by the TPM based on the Endorsement Key and an owner-specified password.
- A second key, called an Attestation Identity Key (AIK) protects the device against unauthorized firmware and software modification by hashing critical sections of firmware and software before they are executed. When the system attempts to connect to the network, the hashes are sent to a server that verifies that they match expected values. If any of the hashed components has been modified since last started, the match will fail, and the system can not gain entry to the network.
- It has special registers called Platform Configuration Registers (PCRs) which hold various measurements in a shielded location in a manner that prevents spoofing.

Assurance Issues that TPMs combat

1. External software attacks
2. Protects data from adversaries that attempt to read data on the system without proper authentication. Example - If the device was stolen.
3. Protects data and secrets from unauthorized applications that are a result of a change in the server configuration.

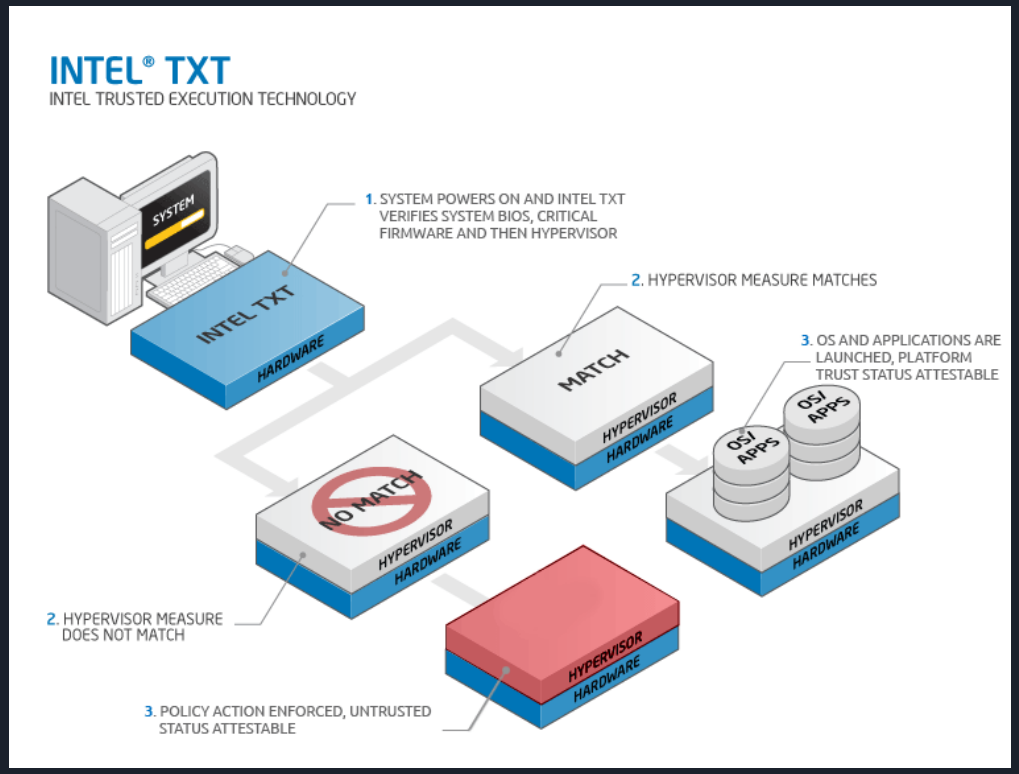
Drawbacks -

TPMs cannot control the software that is running on a PC. It can store pre-run time configuration parameters, but it is other applications that determine and implement policies associated with this information.

Intel TXT

Primary goals are:

- Attestation of the authenticity of a platform and its operating system.
- Assuring that an authentic operating system starts in a trusted environment, which can then be considered trusted.
- Providing of a trusted operating system with additional security capabilities not available to an unproven one.



TPMs in Cloud Computing

TPMs are now being used for establishing and maintaining trusted infrastructure in distributed system deployments.

In a Cloud based environment we use systems that are outside our trust boundary and we need a way to make sure that everything we use is trustworthy.

What many companies are currently working towards is incorporating the various cryptographic statements that the TPMs use to verify that the applications running on the remote machine, the machine's operating system, and everything down to the hardware have not been tampered with.

These cryptographic statements are also called Measurements that consist of a cryptographic hash using a Secure Hashing Algorithm (SHA); the TPM v1.0 specification uses the SHA-1 hashing algorithm.

Software Isolation Technologies

What are Virtual Machines?

- A virtual machine is a computer file, typically called an image, that behaves like an actual computer. In other words, creating a computer within a computer. It gives the end user the same experience on a virtual machine as they would have on the host operating system itself.
- Before VMs, businesses typically ran one application per server. This meant there would often be tons of idle CPUs on these servers, making it very inefficient .
- VMs make it possible to run many different types of operating system instances on a single machine. Also, VMs make it possible to run multiple applications on one server in a safe and secure manner making more efficient use of the computer's physical resources by converting the physical hardware into a shareable form.
- Each virtual machine provides its own virtual hardware, including CPUs, memory, hard drives, network interfaces, and other devices. The virtual hardware is then mapped to the real hardware on the physical machine which saves costs by reducing the need for physical hardware systems along with the associated maintenance costs that go with it, plus reduces power and cooling demand.
- These multiple operating systems run side-by-side with a piece of software called a hypervisor to manage them.

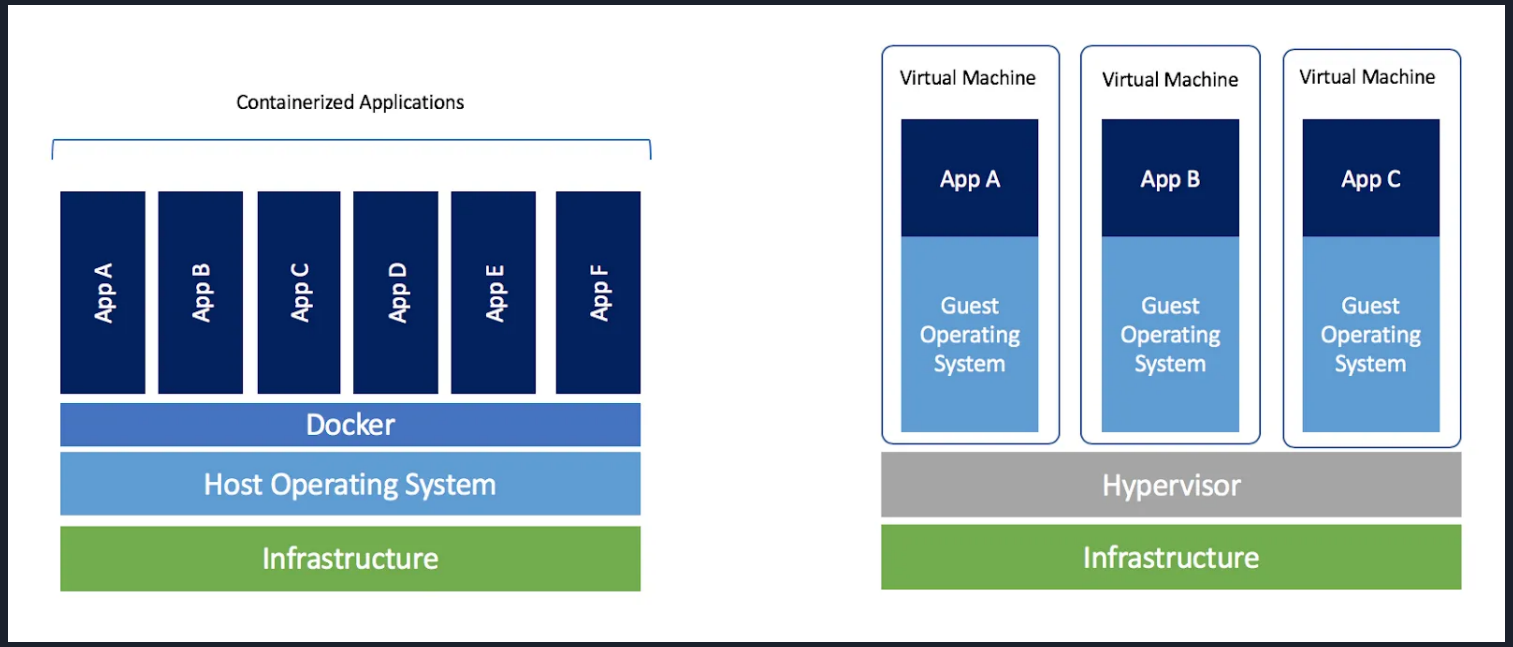
What are Containers?

- A container is a standard unit of software that packages up code and all its dependencies so the application runs quickly and reliably from one computing environment to another.
- Containers hold a microservice or app and everything it needs to run. Everything within a container is preserved on something called an image—a code-based file that includes all libraries and dependencies.
- It's a solution to problems that arise when the developer's testing environment is not similar to the production/use case environment. Different base Operating Systems, different package versions etc. are some of them.
- Not just different software versions can cause problems, the network topology might be different, or the security policies and storage might be different.
- By containerizing the application platform and its dependencies, differences in OS distributions and underlying infrastructure are abstracted away.
- Containers use the concept of namespace that wraps a global system resource in an abstraction that then appears to the running application as their own isolated instance of a global resource.

Architecture

- Software called a hypervisor separates resources from their physical machines so they can be partitioned and dedicated to VMs. When a user issues a VM instruction that requires additional resources from the physical environment, the hypervisor relays the request to the physical system and caches the changes.
- A physical server running three virtual machines would have a hypervisor and three separate operating systems running on top of it. By contrast a server running three containerized applications with Docker runs a single operating system, and each container shares the operating system kernel with the other containers.
- VMs take up a lot of system resources. Each VM runs not just a full copy of an operating system, but a virtual copy of all the hardware that the operating system needs to run.
- Containers' speed, agility, and portability make them yet another tool to help streamline software development.

Architecture



Assurance Issues and Solutions

- A: Denial of Service attacks - A process/container can use all the resources of the system and starve other processes and containers on the host.
- S: Control Groups - It is a kernel mechanism for specifying and enforcing hardware resource limits and access controls to a process or a group of processes. They isolate and limit a given resource over a group of processes to control performance or security

- A: Device Integrity Protection - If devices are accessed by users that shouldn’t be allowed to do so, it can compromise the integrity of the said device.
- S: Cgroups can be used to restrict access to devices using label-based access control by specifying a device whitelist.

Assurance Issues and Solutions

- A: If container is given root access to run commands, it can gain access to the host system. Sometimes the ‘ping’ binary is required by the containers and the developers end up giving full root access instead of a small subset of it.
- S: The Linux kernel has a feature called Capabilities that helps to partition the extensive set of privileges available to root so that processes can be allocated just the privileges needed to perform a specific function.

- A: All containers should be protected from other containers on the host.
- S: SELinux: Security Enhanced Linux can be used to assign labels (context) to processes and objects (e.g., files, sockets) and specify access restrictions based on certain combinations of categories. A specific SELinux label can be applied to a container to enforce a security policy.

SELinux

- Security-Enhanced Linux (SELinux) is a Linux kernel security module that provides a mechanism for supporting access control security policies, specifically mandatory access controls (MAC).
- It replaces user-based model with a policy-based model such that all actions reading and writing data are controlled by a security policy.
- It separates the applications and processes executing on the system which can isolate the attack and also limit the damage caused by the compromised application.
- SELinux users and roles do not have to be related to the actual system users and roles and the circumstances under which a process is allowed into a certain domain must be configured in the policies.
- Default-deny policy (anything not explicitly specified in the policy is disallowed)
- Access granted only if both DAC is allowed and appropriate label exists.

Assurance Issues and Solutions

- A: Provide Process Isolation - Ensure the integrity of various applications running in different containers as well as in the host.
  - Limiting cross-container process visibility
  - Ability to distinguish processes running in different containers from each other and from those running on the host
- S: Process ID (PID) namespace - It is a mechanism that groups processes and controls their ability to see and interact with one another.

- A: Prevent illegitimate access to filesystem objects from one container to another and from any container to the host.
- S: Mount namespace - Access to data for a container application is determined by its access to file systems through the filesystem mount points. Therefore, access to data can be restricted by making the list of filesystem mount points visible and accessible to a container application.

Resources

1. “Security Assurance Requirements for Linux Application Container Deployments”, Ramaswamy Chandramouli, October 2017, NISTIR 8176, National Institute of Standards and Technology
2. “Security Assurance of Docker Containers”, Stefan Winkle, November 2017, SANS Institute
3. “Application Container Security Guide”, Murugiah Souppaya, John Morello, Karen Scarfone, September 2017, NIST Special Publication 800-190, NIST
4. “Container Security: Issues, Challenges, and the Road Ahead”, Sari Sultan, Imtiaz Ahmad, Tassos Dimitriou, Kuwait University, IEEE April 2019

Thank you!