DSci523: Computer Systems Assurance

Case Study Proposals

http://ccss.usc.edu/523

Prof. Clifford Neuman

Lecture 5
25 September 2020
OHE 120

NETWORKED MEDICAL DEVICES

JAYNEE SHAH

INTRODUCTION

- New innovations leading to more sophisticated medical devices
  - Wireless, internet- and network-connected
- Uses hardware, software and networks to monitor patient's medical status, and transmits and receives data over wired or wireless networks
- Advantages:
  - Improved treatments and precise diagnostics
  - Better patient monitoring and improved patient compliance
  - Automated control
  - Central collection, reporting and monitoring of data, leads to more personalized care
  - Detection of device failures before they become serious
- Example Medical Devices:
  - Pacemakers, Insulin pumps, Wireless heart monitors, Insulin dispensers, Dialysis machines, Radiology systems, Medication dispensing systems
- Medical Devices Companies
  - Medtronic, Johnson & Johnson, GE Healthcare, Abbott, Stryker, Siemens, 3M, Cardinal Health, any many more

- HIPAA Security Rule / HITECH Act - protects electronic health information
- Manufacturers Disclosure Statement for Medical Device Security (MDS2) form - manufacturers to disclose security related features of the medical devices to healthcare providers

SECURITY ISSUES

- Medical Device Hijack (MedJack) - hospital's weakest link in the chain
- Hospital networks are usually behind the firewalls and the internal network runs AntiVirus and other intrusion prevention and security mechanisms
- However, most medical devices lack basic firewalls or security protocols, often rely on simple password authentication, and many times store or transmit unencrypted data
- Built based on the assumption that these are not attractive targets for hackers
- Medical devices companies lack security expertise and resources to ensure that high levels of security are built into these products
- Platforms and solutions are not thoroughly vetted for security issues, making it easily compromisable by attackers
- Many medical devices are fixed function devices and can not be upgraded or patched easily
- Long lifecycle of the devices, sometimes up to 15-20 years - hard to manufacture devices with future security innovations in mind
- Many times, these devices are deployed outside of hospital networks, e.g. in homes, not protected

CONSEQUENCES OF SECURITY FAILURES

- Compromise allows hackers to gain unauthorized access to the wider hospital network
- Puts protected health information (PHI), personally identifiable information (PII) and patient safety at risk
- A malware can be introduced into medical equipment and configuration settings can be changed on the devices
  - At a hospital, blood gas analyzers were infected with malware that enabled backdoors into the hospital network
  - At another hospital, backdoor was found installed in one of the hospital X-ray systems
- Many ransomware attacks targeting hospitals and medical providers in recent years
  - Hackers can compromise the system, encrypt the data, thus blocking normal functionality of these medical devices, and then ask for ransom to to restore the system back to its normal functionality
  - Per a report, Wannacry Ransomware has affected more than 40% healthcare organizations
- FDA warnings and recalls:
  - FDA warning on 'hackers could compromise insulin pumps'
    - An unauthorized person can connect the pump to WiFi and change settings to under- or over- deliver insulin or stop insulin altogether
    - These insulin pumps can also be controlled remotely
    - Certain Medtronics pump were recalled due to this vulnerability
  - Similarly, FDA announced Abbott pacemakers recall in 2017 due to software vulnerability
  - Hospital drug pumps can be remotely exploited where an attacker can up the dose
- Adverse health consequences and danger to patient safety and life

ASSURANCE CONCERNS

- High assurance required for ‘Protection of Human Life’
- Restricting unauthorized access to medical devices
- Monitoring for unauthorized use
- Minimization
- Malware / Rootkits
- Ransomware attacks
- Denial of service attacks, mainly on hospital networks
- Physical security of the devices
- Environmental factors

ASSURANCE QUESTIONS TO CONSIDER

- What do medical device manufacturers currently do? What can be improved upon?
  - Do manufacturers design, develop, and support devices that are securable throughout the product lifecycle?
  - Cybersecurity risk analysis?
  - Third party evaluations?
- What are the assurance components? What level of assurance is provided by these components?
- Security Options
  - Authentication methods
  - Access control mechanisms - DAC / MAC / RBAC
  - Encryption - at rest / in transit
- Where is the TCB in the device? Where is TCB boundary? What about TCB for the overall hospital network? Do they implement the defined security policy?
- How can an attack on one medical device have minimal impact on the other hospital network components? How can we stop the attacker moving laterally through the hospital network?
- What are attack surfaces? - Physical access, remote access (open ports), insiders
- What OS do most manufacturers use? How is OS integrity achieved? What about supply chain subversions?
- Are there any regulations around medical devices manufacturing, distribution, and support?
  - US Food and Drug Administration (FDA)
  - European Union Regulation
  - Other countries
- Pick 2 or 3 medical devices companies (from Medtronic, Johnson & Johnson, GE Healthcare, Abbott, Stryker) and research on what security and assurance practices they implement

RESOURCES

- FDA cybersecurity guidelines
  - https://www.fda.gov/medical-devices/digital-health/cybersecurity
- Security and privacy issues in implantable medical devices: A comprehensive survey
  - https://www.sciencedirect.com/science/article/pii/S153204641500074X?via%3Dihub
- Cybersecurity for Medical Device Manufacturers: Ensuring Safety and Functionality
  - https://go-gale-com.libproxy1.usc.edu/ps/i.do?p=HRCA&u=usocal_main&id=GALE|A497861240&v=2.1&it=r
- Cybersecurity of medical devices: Addressing patient safety and the security of patient health information
  - https://www.bsigroup.com/LocalFiles/EN-AU/ISO%2013485%20Medical%20Devices/Whitepapers/White_Paper___Cybersecurity_of_medical_devices.pdf
- Research papers by Anita Finnegan, Fergal Mccaffery, and Gerry Coleman
  - A Security Assurance Framework for Networked Medical Devices
  - A Process Assessment Model for Security Assurance of Networked Medical Devices
  - A Security Argument Pattern for Medical Device Assurance Cases
  - Framework to Assist Healthcare Delivery Organisations and Medical Device Manufacturers Establish Security Assurance for Networked Medical Devices
- Holding the Line: Events that Shaped Healthcare Cybersecurity
  - https://search-proquest-com.libproxy1.usc.edu/docview/1967813225/fulltextPDF/36AB2E3AA4684BC7PQ/1?accountid=14749

FEEDBACK / QUESTIONS ?

Assurance Techniques for Industrial Control Systems

By: Venkat Ramana Reddy Mareddy

Content

- ICS Definition
- Assurance Issues
- Common ICS Vulnerabilities
- Attacks on ICS
- References

Industrial Control System

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

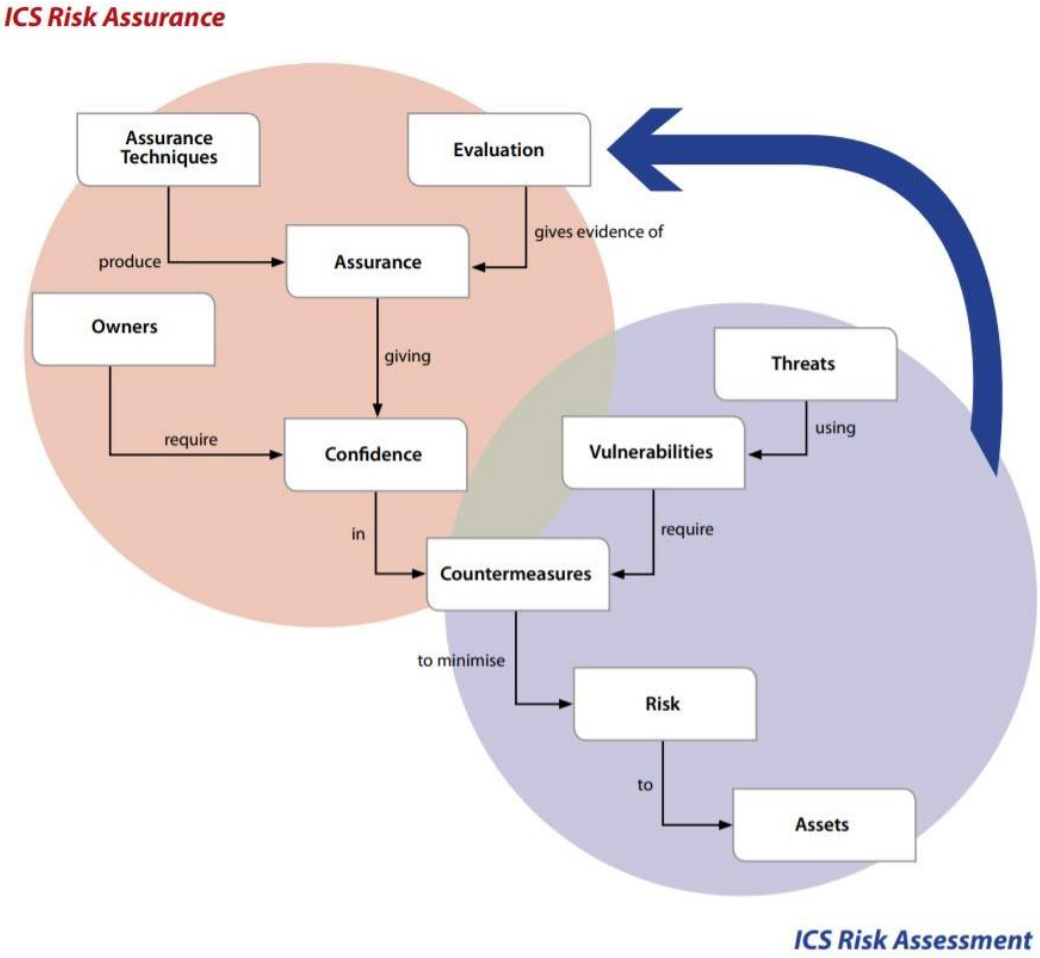
DCS (Distributed Control System) Ex: Chemical plant, Food & Beverage Production

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 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

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

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

Attacks on ICS

- TRITON Attack
- Ukraine power grid
- US power grid

References

- https://www.crest-approved.org/wp-content/uploads/CREST-Industrial-Control-Systems-Technical-Security-Assurance-Position-Paper.pdf
- https://dl.acm.org/doi/pdf/10.1145/2808705.2808710 Assurance Techniques for Industrial Control Systems (ICS)
- https://www.redteamsecure.com/blog/5-key-lessons-learned-critical-infrastructure-cyber-attacks/
- https://www.wired.com/story/russian-hackers-us-power-grid-attacks/

Thank You

Questions?

Assurance

Database Server

DI Rama

Assurance Issues that needs to be met

Database for Cloud Environment in the HealthCare Industry by tenancy model

- **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…

- Data Loss, corruption, unauthorized altercation, unauthorized access
- Violation of company policies and procedures
- Violation of legal obligations
- Lose $$$$ (Fines or Ransom)
- Theft of intellectual property
- Operations temporary shutdown
- Company closures
- Sensitive Information stolen
- Steal Trade Secrets, Research and Development
- Decline in business sales due to competition

Guidance Resources

- CFR21
- NIST (DB Security Checklist)
- NIST (800-53)
- ISO2700 family
- HIPAA – Encryption for data at rest
- HITECH
- HHS.Gov
- Database Harden Best Practices
- GDPR
- CCPA

Cloud Security Assurance

DSCI 523 Computer Security Assurance

Shagun Bhatia

Why Cloud is Used

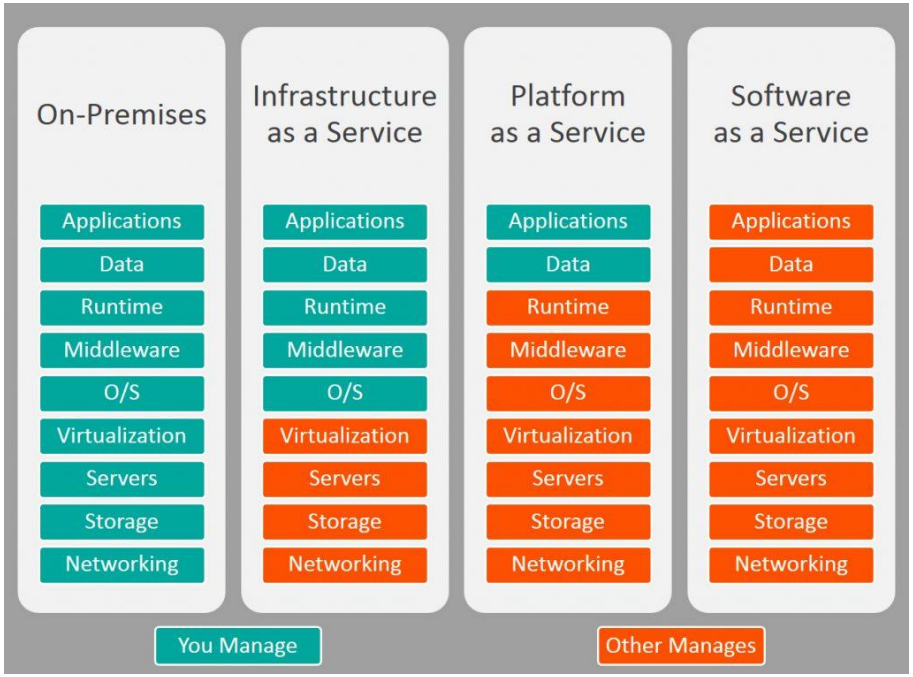
Cloud provides 3 benefits

- Flexibility: It provides features such as Scalability, Control choice(SaaS, PaaS, IaaS), Storage option(public, hybrid, private storage options)
- Efficiency: features like accessibility, speed to market, a pay structure, Saving on server and components, Data security provided by redundancy in real time.
- Strategic Value: Regular updates. Low investment in new countries to setup business, increased collaboration, Streamlined work

Types of Cloud Services

Shared Responsibility Model

- SaaS- Software as a Service e.g. Salesforce
- PaaS- Platform as a Service e.g. Heroku
- IaaS- Infrastructure as a Service e.g. AWS, GCP, Azure



Cloud Components

- NLB(Network Load Balancer)
- Proxy
- Gateway
- Computing servers
- Virtual Private Cloud
- Secrets Manager
- Vault
- IAM systems
- Detection and monitoring
- Content Delivery network
- Storage servers

What is Cloud Security

- It is the protection of data and applications in the cloud environment against attacks against confidentiality, integrity availability.
- There is no defined parameters and boundary in the cloud environment
- With Cloud computing all the components are now software's, IaC is a technology which pushes all the components towards software
- There are a lot new threat landscape and vectors for which stricter and new defenses are developed
- Various methods and standard exist to secure the cloud which include firewall, security assessment, penetration testing, Red Team assessment, VPN, tokenization

Cloud Security Standards

- FEDRAMP
- NIST SP 800-144
- NIST SP 800- 53
- ISO 27017
- ISO/IEC 27002

These Standards are mandatory if the customer is Government example DHS, FBI, NSA, etc

- AWS GovCloud
- Azure Government
- Government - Google Cloud

FEDRAMP (The Federal Risk and Authorization Management Program)

This is a government wide program which aims to provide actionable and standardized approach toward making cloud more secure by defining security assessment and cloud monitoring process.

All the cloud provider and services that are FEDRAMP authorized can be found at

https://marketplace.fedramp.gov/#!/products?sort=productName

The FedRAMP Security Controls and baseline https://www.fedramp.gov/documents/

FedRAMP follows NIST SP 800-53 standard which provides guidelines on how the US government should setup and establish architecture, implement and manage their information security systems .

Family of controls that are implemented

- Access Control
- Awareness and Training
- Audit and Accounting
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incidence Response
- Maintenance
- Physical and environmental protection
- Risk Assessment
- System and Information Integrity

NIST SP 800-144

- NIST has a guideline for maintaining security and privacy in public cloud The document can be found at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf
- This guideline talks about various principles that need to be looked while performing a security assessment
  - Governance
  - Compliance
  - Trust
  - Identity Access Management
  - Software Isolation
  - Data Protection
  - Availability
  - Incidence Response

ISO/IEC 27017:2015

- The standard was revised in 2015 and mentions security controls for cloud services
- These are the 7 security controls which are needed in addition to 18 sections mentioned in ISO 27002
  - Who is responsible for what between the cloud service provider and the cloud customer.
  - The removal or return of assets at the end of a contract.
  - Protection and separation of the customer's virtual environment.
  - Virtual machine configuration.
  - Administrative operations and procedures associated with the cloud environment.
  - Cloud customer monitoring of activity.
  - Virtual and cloud network environment alignment

ISO/IEC 27002

- Scope
- Normative References
- Definitions and abbreviations
- Cloud sector-specific concepts
- Information security policies
- Organization of information security
- Human resource security
- Asset management
- Compliance
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management

ASSURANCE CHALLENGES WITH FEDRAMP

DSCI 523

DEWAINE REDDISH

9/25/2020

USC University of Southern California

USC University of Southern California

CONTENTS

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

USC University of Southern California

ASSURANCE ISSUES & CONSEQUENCES

- Not unlike assurance with any other system; organizations must have an adequate level of certainty that controls sufficiently enforce policy
- 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.
- Some assurance issues with FedRAMP are systemic; others stem from a difference in agency/organizational policy that makes assurance claims difficult to transfer.
- Loss of information that might enable adversaries to gain classified information (FOUO/CUI data)
- Loss of personally identifiable information and/or protected health information

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, security authorizations, or granting ATOs for cloud services

Intended to allow/force agencies to accept ATO's outside of their organization

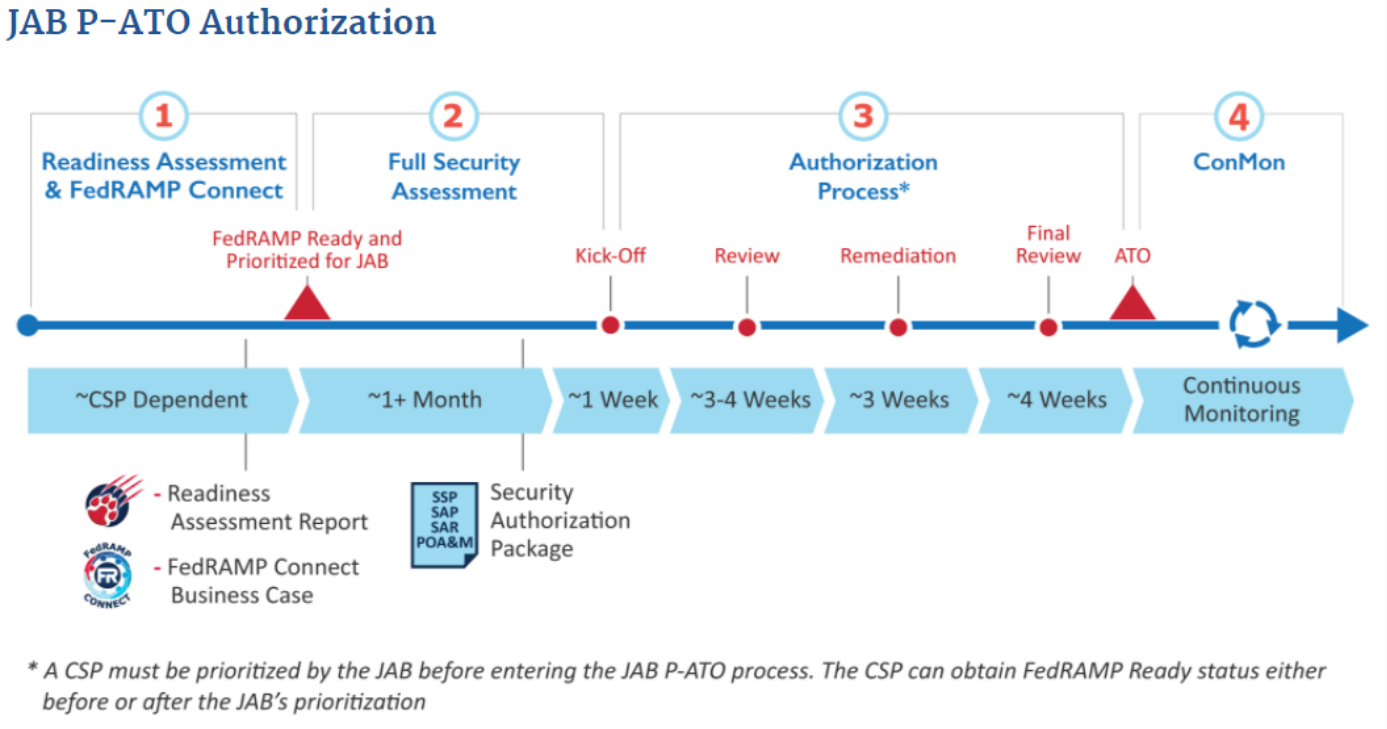
Costs cloud offering providers $250k – $5M for an authorization decision

Marketplace for agency organizations to find approved cloud service offerings that are already 'secure'.

Sounds promising! This is a huge challenge for the federal government.

FEDRAMP ASSURANCE CHALLENGES

Cost: $250k - $5M



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

USC University of Southern California

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, providing agencies with little or no protection against subversion performed after the initial authorization decision.

FEDRAMP ASSURANCE CHALLENGES

Control SI-12

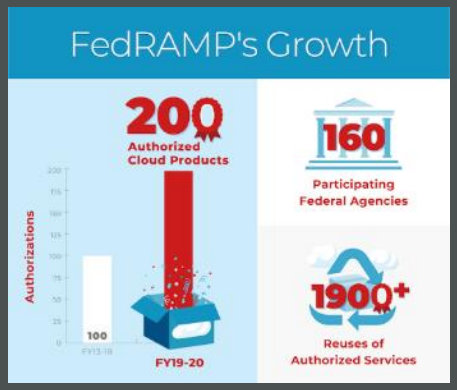
The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

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.



amazon web services™

Amazon - AWS US East/West

Akamai

Akamai - Content Delivery Services

TROJAN FAMILY

WE FIGHT AS ONE

USC University of Southern California

RISK MANAGEMENT FRAMEWORK (RMF) AND NATIONAL SECURITY SYSTEMS

SARAHZIN CHOWDHURY

DSCI 523

SEPTEMBER 25, 2020

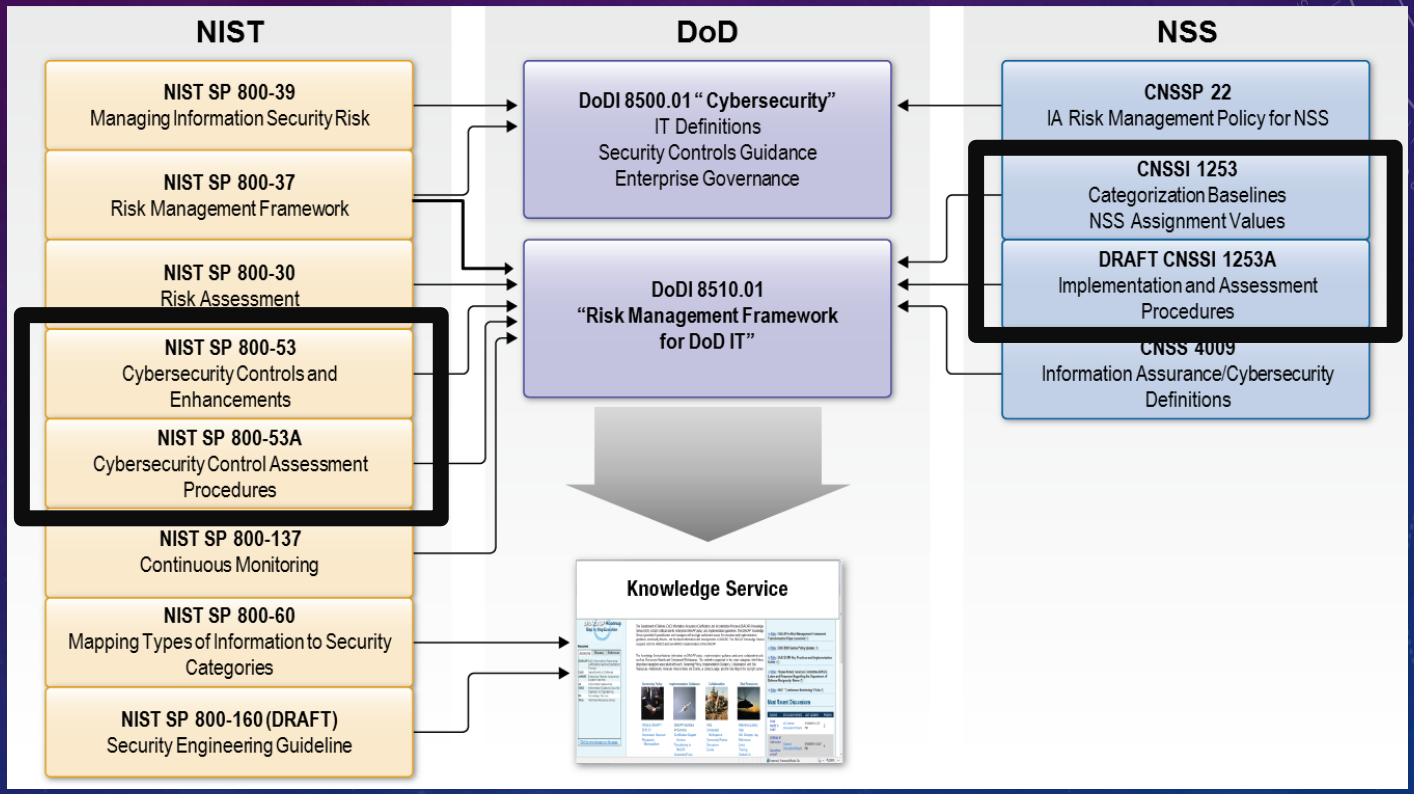
AGENDA

- 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

SECURITY CONTROL BASELINE

Table D-1: NSS Security Control Baselines

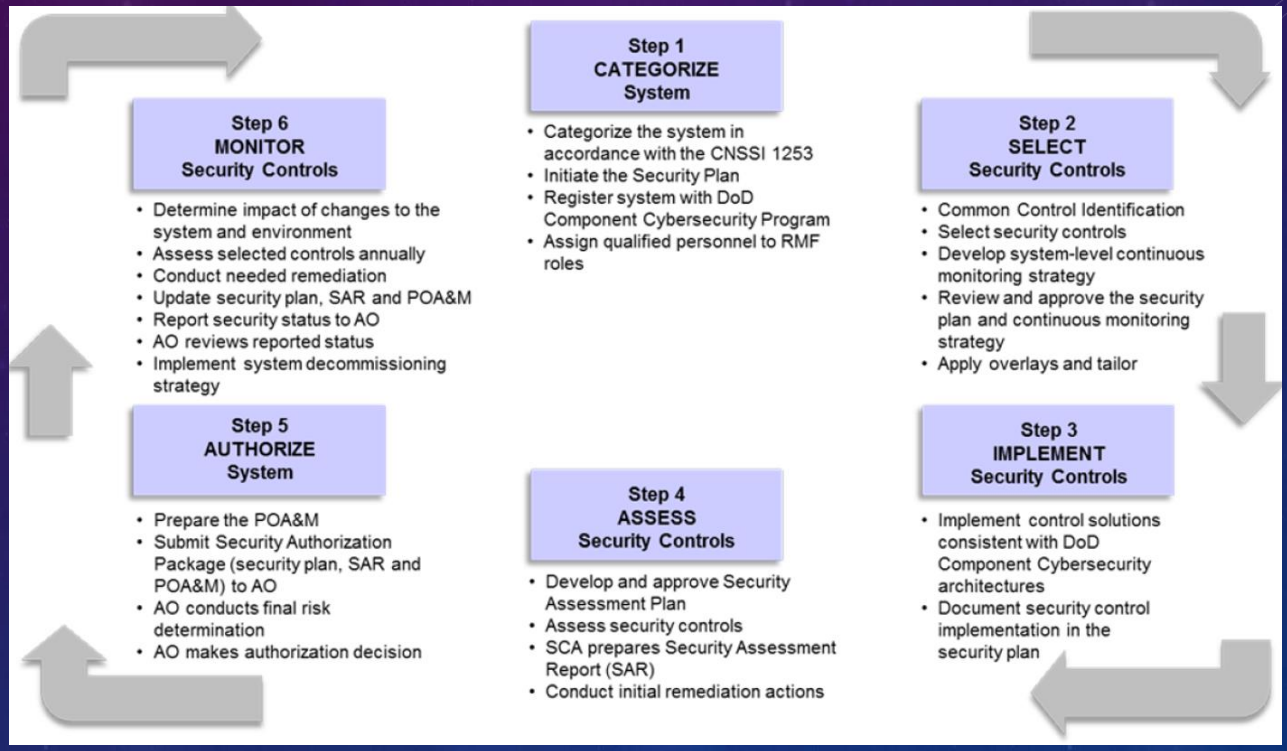
ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X
AC-2	Account Management	X	X	X	X	X	X			
AC-2(1)	Account Management | Automated System Account Management		X	X		X	X			
AC-2(2)	Account Management | Removal of Temporary / 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

RMF STEPS

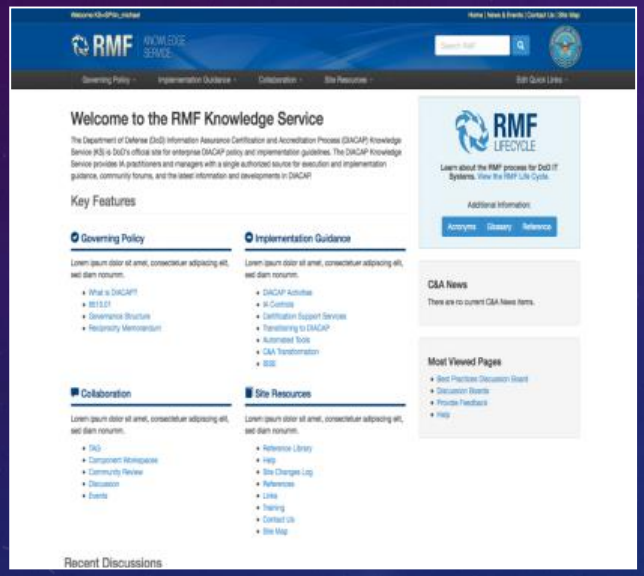

Step 1
CATEGORIZE
System
• Categorize the system in accordance with the CNSSI 1253
• Initiate the Security Plan
• Register system with DoD Component Cybersecurity Program
• Assign qualified personnel to RMF roles
Step 2
SELECT
Security Controls
• Common Control Identification
• Select security controls
• 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 AND IMPACT?

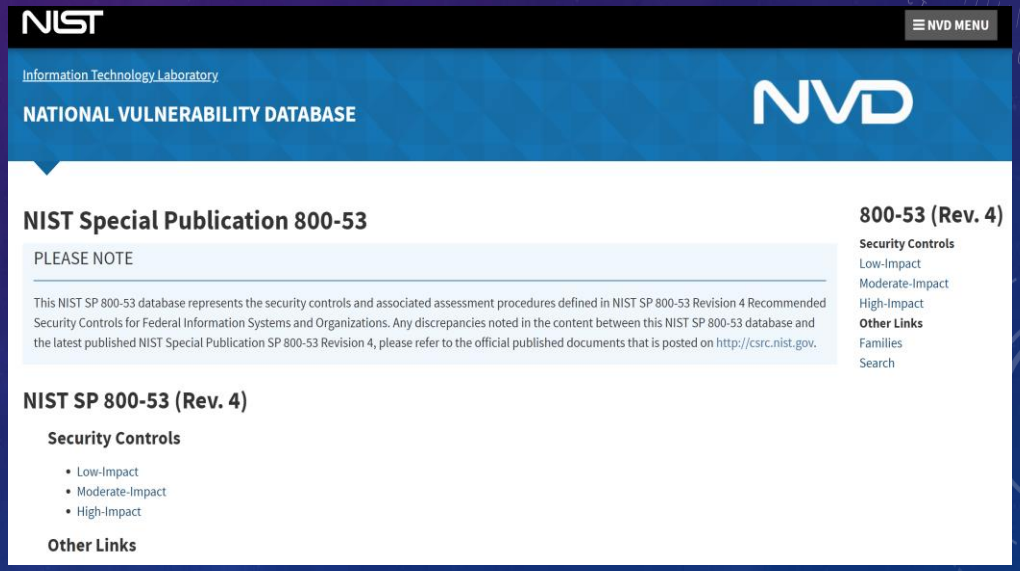
- Authorization to Operate (ATO)
  - Without ATO, system will be decommissioned and/or have high risk
- Impact Examples
  - Top Secret
    - "Top Secret shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause **'exceptionally grave damage'** to the 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."

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

QUESTIONS?

9/24/2020

Identity Tokens & Yubikey

DSCI523 –CASE STUDY– FALL 2020

SEPTEMBER 24, 2020

AUTHOR: ARJUN G. RAMAN

CONTACT: ARJUN.RAMAN@USC.EDU

Objectives & Contents of Presentation

Objectives

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

- Explain (though not necessarily answer) the assurance issues that need to be met by the identified system.
- Identify the consequences of security failure in such systems.
- Discuss where one will look to answer those questions.
- Engage students to discuss in a question and answer format

Contents

- What is an Identity Token? What is Yubikey?
- Assurance issues or requirements to be met by the system
- Consequences
- Exploratory areas and sources
- Q&A

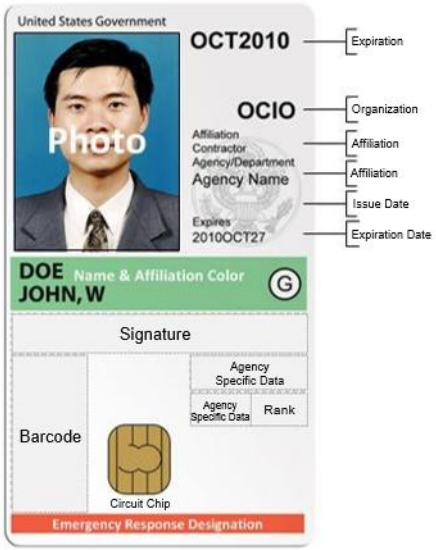
Identity Token?

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)

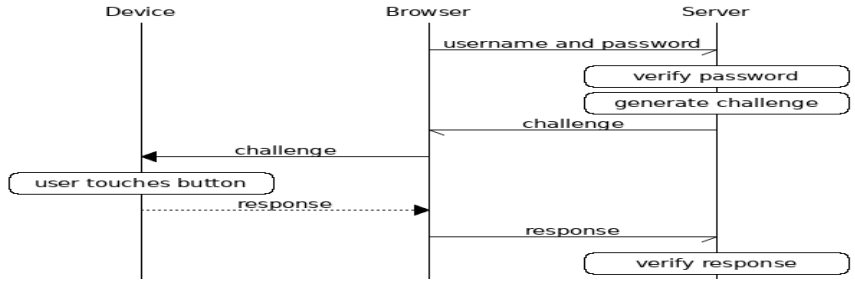
What is an Identity Token?

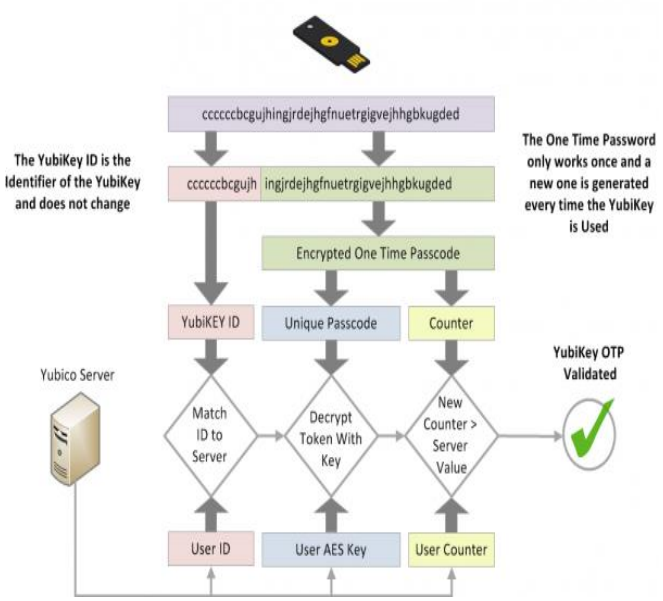
- An identity token is a portable piece of hardware that a user carries and uses to access a network. The token aids in proving the user's identity and authenticating that user for the use of a service.
- Other Examples: security token or an authentication token.



What is Yubico? Yubikey?

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





Assurance Issues for Class of System/Product

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).
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.
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

Consequences of Failure

Loss of Access / Limitations of Access – Tedious for the user if key is tampered with or protocol does not sync/work

With potential for biometric, the focus on how that data is protected will be critical if attacker understands key location and password

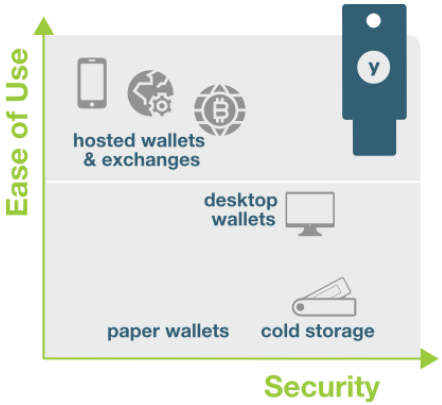
Forgetfulness – Forgetting your token if inputted into the device

Malicious Code Injection / Trojans from USB Port

Planned Areas and Sources of Exploration – Look Deeper at Use Cases

Mobile

Yubikey Bio – Supporting Fingerprints



Digital Assets / Tokens or Currency

Thank You

Q&A + DISCUSSION

Security Assurance for Isolation Technologies

- Ayush Ambastha

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.

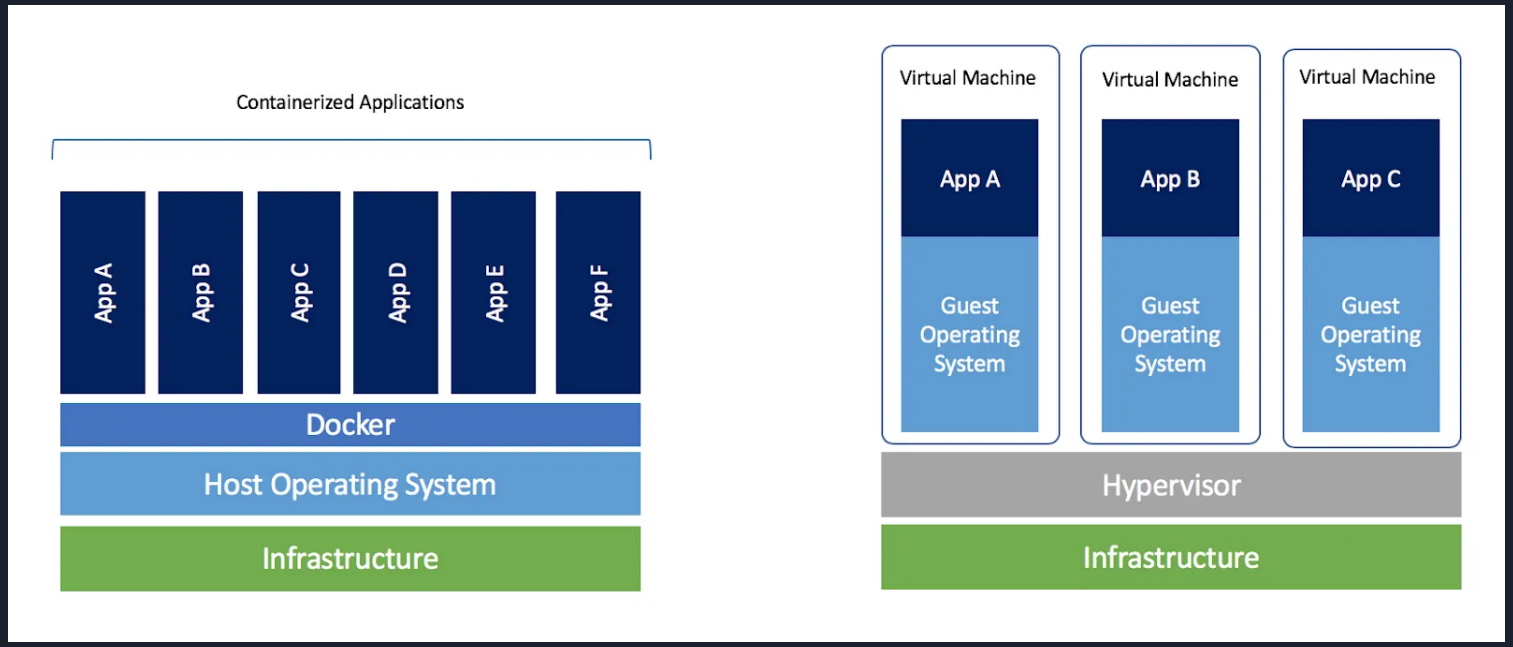
What are Containers?

- 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.
- Its 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

- Denial of Service attacks - A process/container can use all the resources of the system and starve other processes and containers on the host.
- 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.
- All containers should be protected from other containers on the host.
- 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

Assurance Issues

- Prevent illegitimate access to filesystem objects from one container to another and from any container to the host.
- If a non-root process creates a user namespace, applications that needed root access can do so from within this namespace.
- Device Isolation - Since most kernels do not support device namespaces, how do we protect the device drivers?
- An attacker modifies the container image from the registry?

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!

Apple and Google Pay

By: MaryLiza Walker

Agenda

- Assurance Issues that need to be met
- Identify the consequences of security failures in such systems
- How to find the answers to more question from above
- Questions?!

Assurances

- Apple and the device does not store any card information that could lead to the owner of the card
- Near-Field Communications

Identify Consequences of Security Failures

- Attacker being able to access Owner Card information
- Initialization of Credit card information

Where to look for answers

- Google Pay Contract
- Apple Pay Contract

Feedback and Questions
Please be honest but nice
and I do take email feedback
marywalk@usc.edu

Security Assurance in Linux Application

Aditya Goindi

Assurance Requirements for Linux Application Container Deployments

- The focus is on application containers on a Linux platform.
- Linux and its various distributions form the predominant host OS component of the deployed container platforms.

Solution for Linux Container Application Stack

- Linux kernel features:
  - Namespaces
  - Cgroups
  - Capabilities
  - Kernel Modules

Hardware based Solutions

- Trusted Platform Module
  - In OS kernel
  - In a standalone container
  - Trusted Execution Support

Assurance for host OS Protection

- Generic OS host protection
- OS protection for container escape

Will be covering

- Providing authenticity and attestation of integrity to containers
- Hardware-based protection for shielding one container from another
- Protection measures for container runtime, images and registry
- Linux kernel features

Security Assurance in Linux

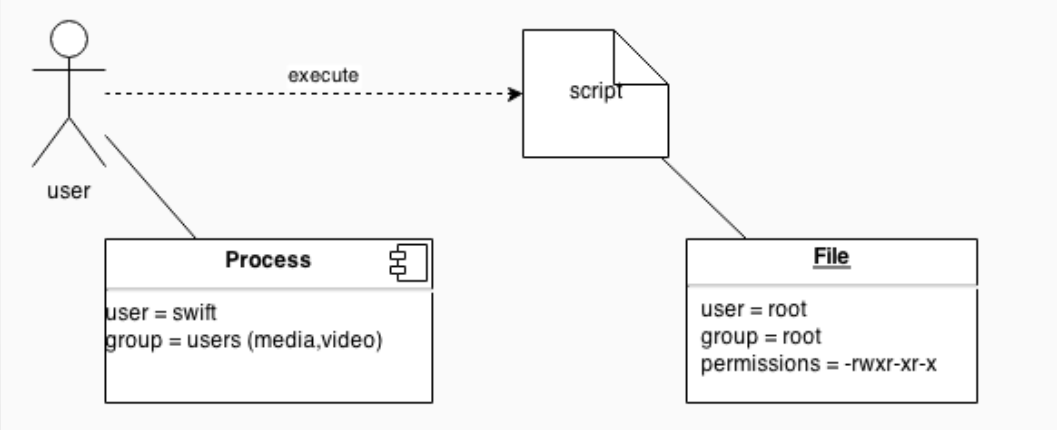
Tejas Pandey

Operating System Security

- Applications can be subverted.
- Security mechanisms can be circumvented.
- Secure end-to-end transactions require secure end systems
- Human the weakest link (deliberate/unintentional).

Linux Access Control

- User wants to read/write/execute file,
  - Linux DAC checks process user is running (shell).
  - Compares with that of file to make decision.
  -



Discretionary Access Control

- Permissions identified by “OGO” (owner, group, other).
- Is existing control mechanism among all Linux flavours.
- Limited in its scope, based on identity and ownership that defines access to files, processes, sockets etc.
- Only differentiates between admin and regular user.
- Subject to admin/user’s whim; subverted by malware.
- Additional security features (ACL) still DAC in nature.

Case for SELinux

- Provides MAC governed through security policy.
- Restrict program execution and privileges.
  - Service may listen on a port and write to syslog, but does it need to access /home?
- Separation of different security domains based on confidentiality and integrity requirements.
- MAC checks happen after DAC.

SELinux Policy Engine

- Implements a combination of:
  - Type Enforcement
  - Role-based Access Control
  - Multi-Level Security

Type Enforcement Access Control

- Access specified between:
  - Subject type: process or a domain.
  - Object type: file, dir, socket etc.
- Four elements that define allowed access:
  - Source type: domains
  - Target type: objects to which access is allowed.
  - Object Classes: classes to which access applies.
  - Permissions: type of access allowed.

Object Classes and Permissions

- SELinux defines ~50 object classes, each with their own permissions:

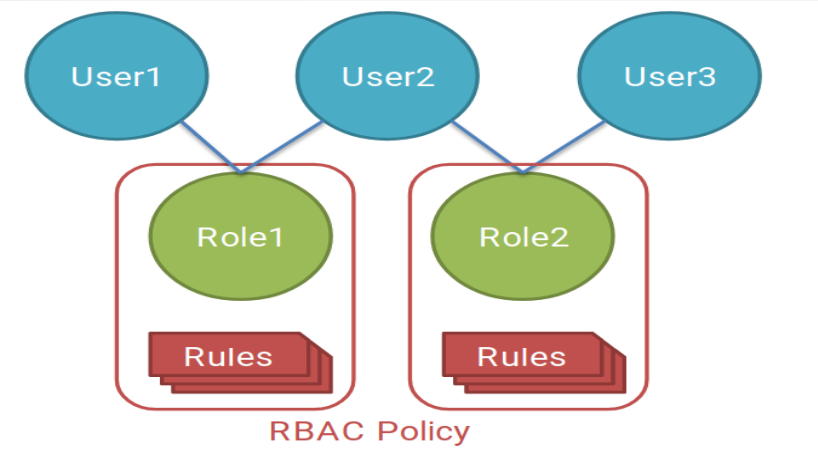
Object Class	Description
blk_file	Block files
file	Regular files
sock_file	Unix sockets
dir	Regular directories
tcp_socket	A TCP socket

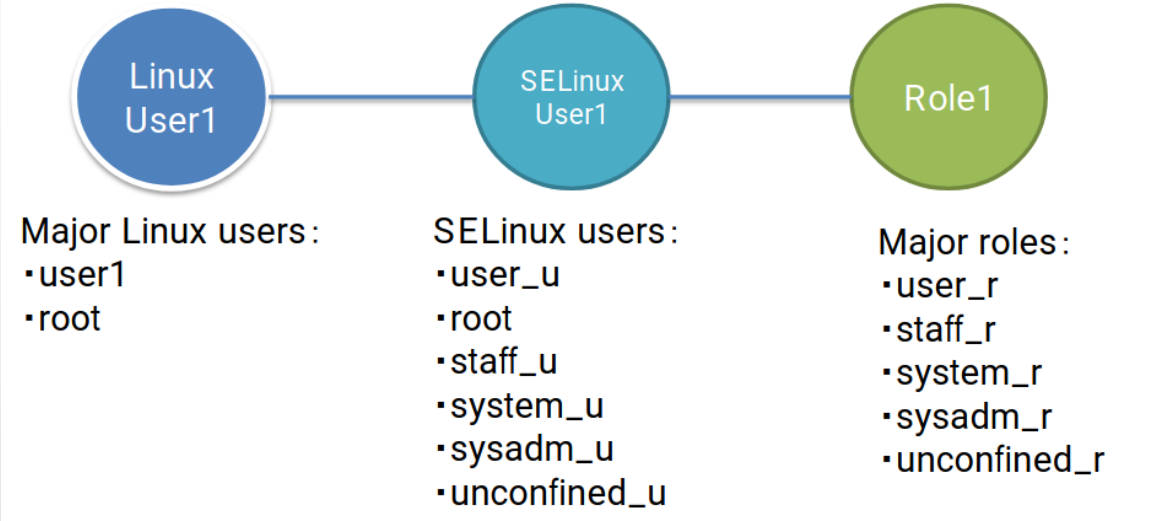
Permissions on “file” object class
create, append, rename, read, execute, write setattr etc

Role-based Access Control

- Users are assigned roles.
- Role is granted permission to access.
- SELinux maps Linux users to SELinux users.
- Further maps SELinux users to SELinux roles.
- Roles can be switched if policy allows
  - Unprivileged user is assigned role “user_r”, administrator is assigned “staff_r” for regular operations, and “sysadm_r” for system administration tasks.
  - Other roles include developer, dba etc.

Role-based Access Control





Security Goals of TE, RBAC and MLS

- Controlled execution domains.
  - Isolation of untrusted code (sandboxing).
  - Limited inter-process communication.
- System Hardening
  - Confinement of error propagation (privilege escalation).
- Integrity/Confidentiality constraints based on RBAC policies.
- Information flow policies.
  - Multi-level security and multiple security levels (BLP).

CHROME OPERATING SYSTEM – CASE STUDY PROPOSAL

MALAVIKA PRABHAKAR

DSCI-523

SEPT 25, 2020

WHAT IS CHROME OS?

- Chrome OS is a Gentoo Linux–based operating system designed by Google.
- It is derived from the open-source project Chromium OS and uses the Google Chrome web browser as its principal user interface.
- It aims to provide a fast, simple, and more secure computing experience for people who spend most of their time on the web.
- Chrome OS is available primarily on Chromebooks.

ASSURANCE ISSUES THAT NEED TO BE MET BY CHROME OS

Remote System Compromise

- Attack vectors through which an adversary might try to compromise a Chrome OS device remotely include:
  - an exploit that gives them control of browser processes
  - an exploit in a plugin
  - tricking the user into giving a malicious web app unwarranted access to HTML5/Extension APIs
  - trying to subvert the auto-update process in order to get some malicious code onto the device.

Device Theft

- The challenges involved here are:
  - Wanting to protect user data while also enabling users to opt-in to auto-login.
  - Wanting to protect user data while also allowing users to share the device.
  - Wanting to protect user credentials without giving up offline login, auto-login, and device sharing.
  - Wanting to provide disk encryption with only minimal impact on battery life and performance speed.
  - The attacker can remove the hard drive to circumvent OS-level protections.
  - The attacker can boot the device from a USB device.

CONSEQUENCES OF SECURITY FAILURE

- Manipulation of data
- Loss of data
- Disclosure of personal information / breach of privacy
  - Could lead to identity theft, credit card fraud, coercion, etc.
- Denial of service
- Elevation of privilege resulting in future exploits

CHROME OS VS OTHER OPERATING SYSTEMS

- This case study will also involve contrasting Chrome OS to other operating systems, including:
- Google's Android OS
- Microsoft Windows
- Apple's Mac OS
- Apple's iOS
- Other Linux-based operating systems

RESOURCES TO BE USED GOING FORWARD

- https://www.chromium.org/chromium-os
- http://www.chromium.org/chromium-os/chromiumos-design-docs
- https://www.chromium.org/chromium-os/chromiumos-design-docs/security-overview
- http://www.chromium.org/developers/design-documents/tpm-usage
- https://chromium.googlesource.com/chromiumos/docs/+/refs/heads/factory-grunt-11164.B/security_severity_guidelines.md
- https://www.google.com/chromebook/chrome-os/#secure
- https://support.google.com/chromebook/answer/3438631?hl=en
- https://www.forbes.com/sites/kevinmurnane/2019/04/21/a-chromebooks-superb-security-is-another-good-reason-to-leave-windows-10s-update-failures-behind/#138fbd3a9a97

THANK YOU

Assurance in Mobile OS

Presented by:

Chinmaya Pandit
Harshit Kothari

Overview

- Assurance in mobile operating systems like Android and iOS.
- Assurance issues exploited by vulnerabilities like Strandhogg 2.0 and jailbreak vulnerability.
- Consequences of security failure like privilege escalation, access to confidential data
- Actions taken to rectify the vulnerabilities.

Key Attributes

- Android’s Trusted Execution Environment.
- Design goals and objectives.
- Trade off’s:
  - Security vs. Performance
  - Fault tolerance vs. Testability

Reference Links

- Android Enterprise Security White Paper
- Apple iOS : List of security vulnerabilities
- Android Vulnerabilities

Questions and recommendations?

Android Assurance

Mohammed Ababtain

9/25/2020

About Android

- Owned By Google
- Open source based on modified Linux kernel
- Released on September 2008
- 87% market share of the global market in 2019
- Around 50% market share of US market
- 2.5 billion active users
- Runs on ARM and x86 architectures

Android Assurance Mechanisms

- TCB
  - Linux Kernel is the lowest layer in the Android software stack
  - Abstraction between the hardware and the software
- Verified boot
  - Verifies the integrity and authenticity of the OS
- Encryption
  - Full disk encryption
  - File-based encryption
- Sandboxing
  - Each application runs on private directory
- Application Signing
  - Each application needs to be signed by the developer

Consequences of Security Failure

- Confidentiality
  - Allows unauthorized access to sensitive information such as Personal and Financial (Emails, Google Pay, Passwords)
- Integrity
  - Allows unauthorized modification to the device (Malwares)
- Availability
  - Device shutdown
  - Allows unauthorized uses of resources

    - Reputational damage and further confidence loss

Thank You ..
Questions/ Suggestions ?

Resources

- https://source.android.com/security/reports/Google_Android_Enterprise_Security_Whitepaper_2018.pdf
- https://www.statista.com/statistics/272307/market-share-forecast-for-smartphone-operating-systems/#:~:text=Smartphones%20running%20the%20Android%20operating,percent%20share%20of%20the%20market
- https://www.e-consystems.com/blog/system-on-module-SOM/android-hal-and-device-driver-architecture/
- https://source.android.com/security

APPLE PAY

SHANICE WILLIAMS
USC
DSCI523

TABLE OF CONTENTS

WHAT IS APPLY PAY?

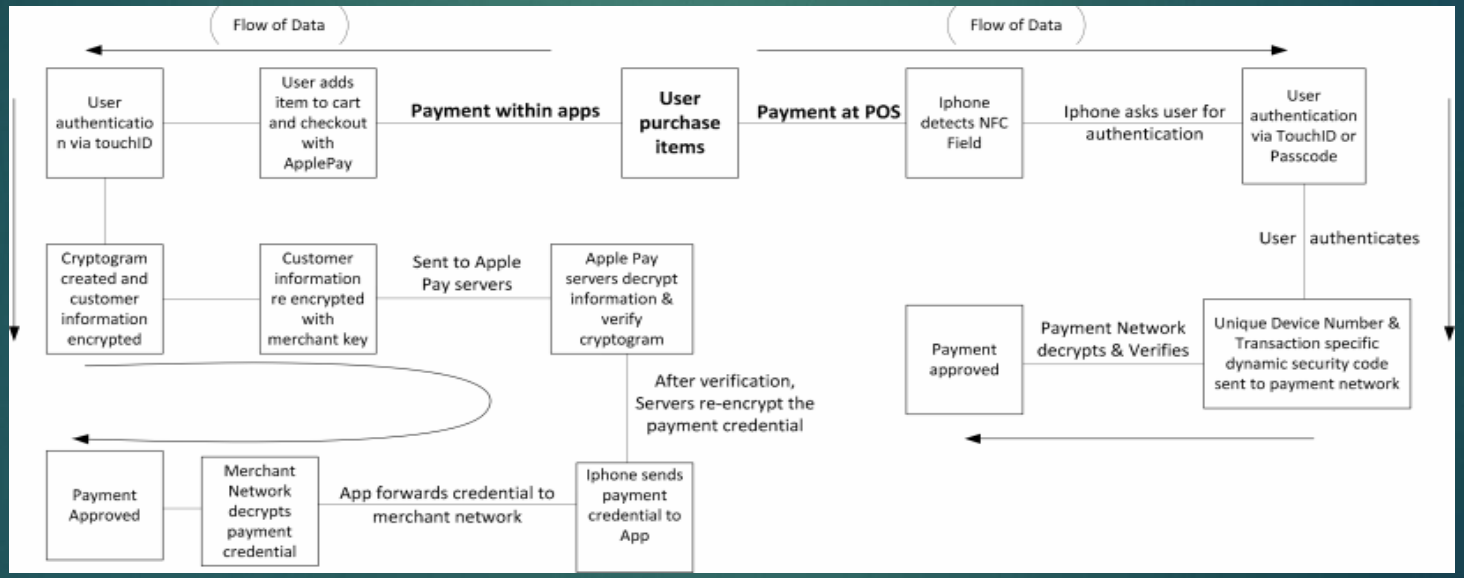
- Apple Pay is a contactless payment system designed by Apple; and used only on Apple devices
- It allows you to authorize payments via your personal device biometrics systems when linking your debit/ credit cards to it.
- Apple Pay can be used locally on devices via apps or at retail stores who accept Near Field Communications, or NFC for short.
- Per Apple, your actual card data is never transmitted/ stored locally on the device nor on its server

HOW DOES IT WORK?

- Cards can be manually inputted into the phone or it uses the camera to capture a picture of the cards data
  - Banks authorize how their cards get added to devices
- Apple uses NFC technology, along with security biometrics to allow users to securely make payment transactions using their mobile devices
- Apple uses a tokenized infrastructure, that replaces the details from your credit card with a randomized token ID, that is then encrypted and stored securely on the Secure Element.
  - This is known as the Device Account Number

HOW DOES IT WORK?

- Apple Pay can be used for purchases two ways
  1. Via device applications
  2. Via POS devices at Certified NFC retail stores



INTENDED USE?

- Apple pay intended use is to provide a contactless payment system users can use to make transactions securely via their own devices.
  - Devices uses it own biometrics security system to authorize payments.
- Apple states that they never store any credit card information
  - This allows for more secure transactions as no CC data is being transferred to merchants, etc.
- Convenience

ASSURANCE ISSUES & CONSEQUENCES

- Biometrics may become spoofed
  - Allows for unauthorized purchases
- Malicious malware installed on devices
  - May use keylogger to capture CC data before it becomes a randomized number
- Lax banking authentications for Apple Pay setup
  - Adversaries can set up apple pay on their own devices using others stolen CC info and social engineering

MORE INFO….

- Will search for articles on more technically details of Apple Pay system
- Explore the different types of attacks that can occur to the current system
- What we can do to help improve the assurance issues in the system

REFERENCES

- Brewster, Thomas. "Millions Are Being Lost To Apple Pay Fraud—Will Apple Card Come To The Rescue?" *Forbes*, 27 Mar. 2019, www.forbes.com/sites/thomasbrewster/2019/03/27/millions-are-being-lost-to-apple-pay-fraudwill-apple-card-come-to-the-rescue/#421fde00622f. Accessed 24 Sept. 2020.
- Jawale, Ashay, and Joon Park. *A Security Analysis on Apple Pay*. IEEE, 17 Aug. 2016.
- PYMNTS. "Apple Pay's Security Problems." *PYMNTS.Com*, 4 Mar. 2016, pymnts.com/apple-pay-CB%20tracker/2016/apple-pays-low-tech-security-problem/. Accessed 24 Sept. 2020.
- Schwartz, Mathew J. "Payment Fraud: Criminals Enroll Stolen Cards on Apple Pay." *Www.Bankinfosecurity.Com*, 15 July 2019, www.bankinfosecurity.com/payment-fraud-criminals-enroll-stolen-cards-on-apple-pay-a-12779. Accessed 24 Sept. 2020.

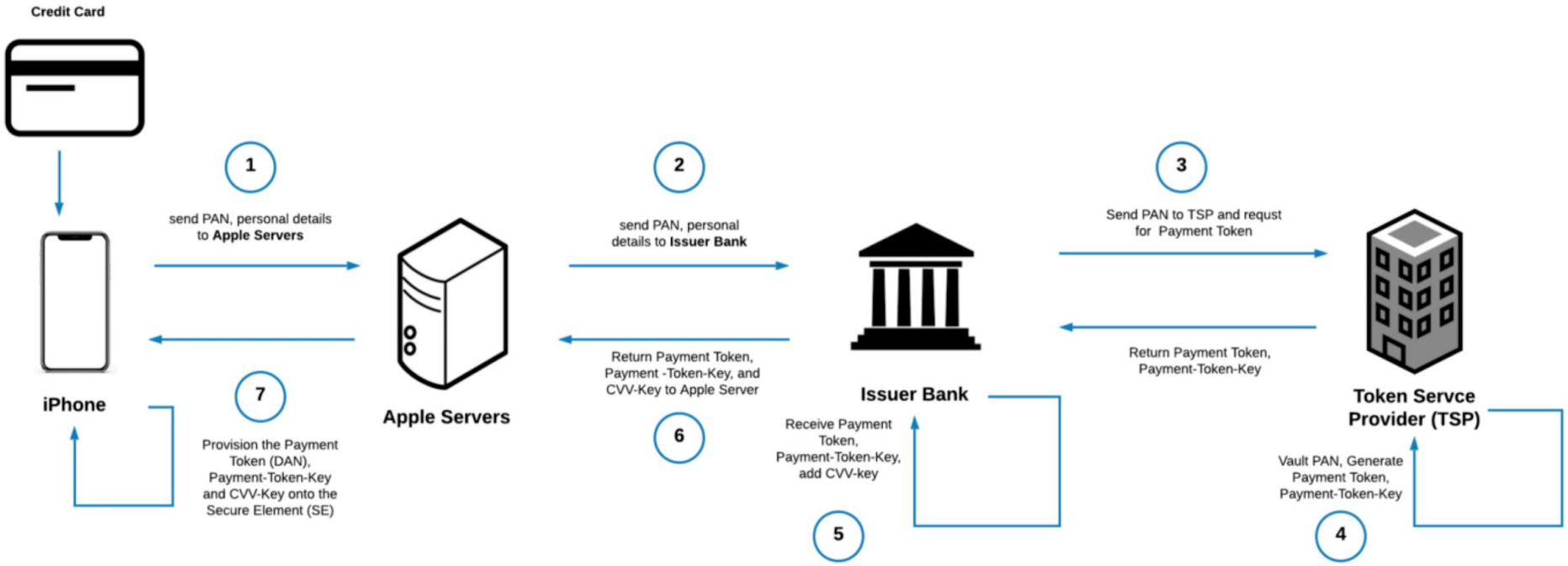
THANK YOU!!!!!

Apple Pay

DSCI 523 proposal

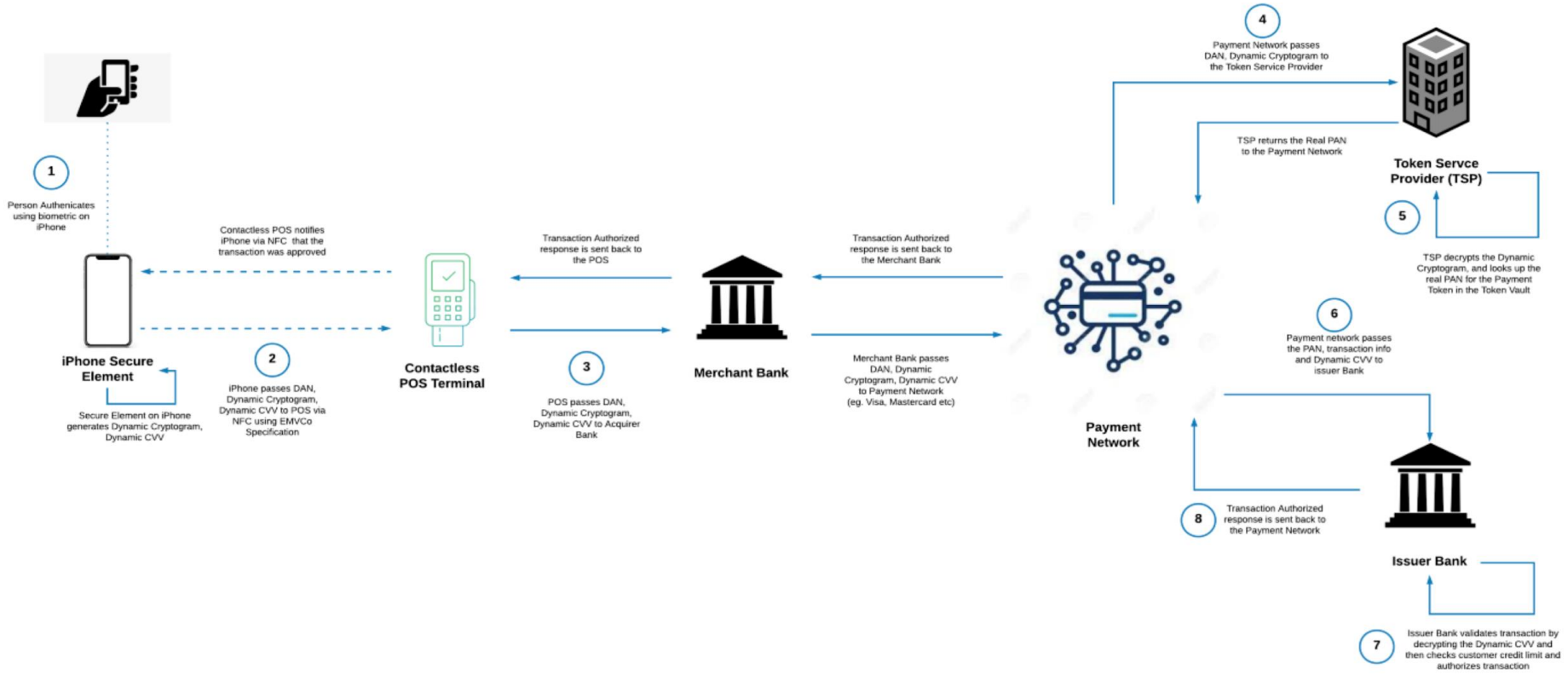
Yang Xue

Process phase 1 add card to apple pay



(Payment Token i.e. DAN, only resides on the Secure Element (SE) on the

Process phase 2 pay with apple pay



Assurance issue

1, Authentication

“One possible weak point involves using Apple's Touch ID fingerprint recognition system to authenticate that you are the owner of the device making the payment. It's a possible weak point because Touch ID can be bypassed relatively easily using fingerprints lifted from glass.

The biometrics hacking team of the Chaos Computer Club (CCC) has successfully bypassed the biometric security of Apple's TouchID using easy everyday means.[4]”

Assurance issue

2, card information stealing

“The exception to this is when you first enroll a credit card into the system. This is done by taking a photograph of the card or entering the card details manually. This is a weak point in the process because this is the one time you interact with your card data.

Credit card information could be harvested as it is entered by hackers using malware or exploiting misconfigurations or aws in the iOS software. "Apple is certainly not immune to bugs, and it's really almost inevitable that there are some in there[3].”

Assurance issue

3, Spoof

“ In 2016, researchers from the anti-fraud company PinDrop warned that crooks could benefit from Apple Pay by adding stolen credit cards from so-called “carding” sites where such information is sold for as little as $2 per card.”

“When using a mobile wallet, the fraudster can instantly receive their stolen goods from the store without providing additional identification or delivery address, Online, many retailers use verification applications, such as Verified by Visa or other mechanisms, to ensure the person making the purchase is the person whose credit card is used.[1]”

Assurance issue

4, Replay

“the thieves were probably in control of a payment terminal and had the ability to manipulate data fields for transactions put through that terminal. After capturing traffic from a real EMV-based chip card transaction, the thieves could insert stolen card data into the transaction stream, while modifying the merchant and acquirer bank account on the fly. [2]”

Bad Consequence

1, “the Department of Justice quietly announced the four-year sentence of a 23-year-old Miami resident who the government claimed was involved in a gang that loaded stolen Capital One credit cards onto their iPhones. Between 2015 and 2016, they spent more than **$1.5 million** on fraudulent purchases via Apple Pay.”

2, “the U.S. government alleged that a group of 30-year-old friends loaded Apple Pay accounts and other digital wallets with stolen JPMorgan credit cards purchased from dark Web trading sites. They then made **$600,000** in fraudulent purposes, splurging on a range of expensive gadgets—from a Rolex watch costing **$35,000** to MacBook Pros and iPhones costing thousands of dollars—in stores in Washington State, according to the government.”

reference

1,https://www.forbes.com/sites/thomasbrewster/2019/03/27/millions-are-being-lost-to-apple-pay-fraudwill-apple-card-come-to-the-rescue/#138d1b50622f

2, https://krebsonsecurity.com/2014/10/replay-attacks-spoof-chip-card-charges/

3, https://www.esecurityplanet.com/mobile-security/apple-pay-how-secure-is-it.html

4, https://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid

5, https://codeburst.io/how-does-apple-pay-actually-work-f52f7d9348b7

6, https://support.apple.com/en-us/HT203027

Case Study: Apple Pay

Proposal Presentation

Jairo Hernandez

DSCI523 – Fall 2020

What is Apple Pay?

Apple's proprietary digital wallet service

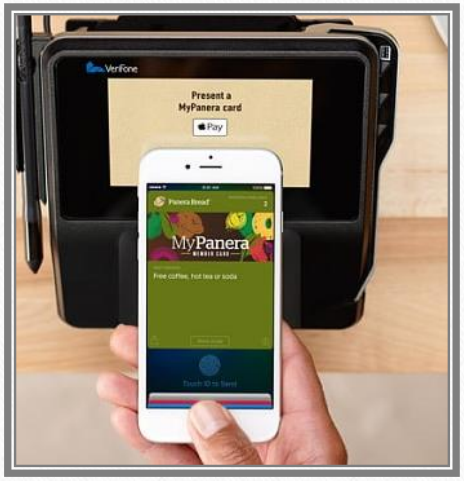
Allows you to store membership and credit cards, event tickets, and more, but the focus of this project is going to be on contactless payment

First introduced October 20, 2014 on the iPhone 6 (iOS 8.1)

Now available on iPhones, iPads, Macs, and Apple Watches

Retailers started to accept Apple Pay in 2016

Rollout to the rest of the world still on-going



What assurances do I plan on tackling?

My plan is to tackle three major points:

1. The viability and trustworthiness of NFC/EMV technology that makes contactless payments work
   - What are some pros and cons of this method?
   - What are consequences or drawbacks of this method?
2. The security of the device holding the information
   - iPhones are touting privacy and security as a major selling point. What evidence do t to trust them?
   - How secure is Apply Pay compared to physical credit cards?
3. The security of the device that is processing the paym
   - How secure are the standard Point of Sale (PoS) systems?
   - How can they prevent or help protect against a breach like Target's?

What are the consequences of failure?

- Money
- Time
- Information
- Branding

Possible Comparisons

- Google Pay (formally known as Android Pay)
- Physical Credit Cards

Resources

DuckDuckGo (Google)

Company Websites

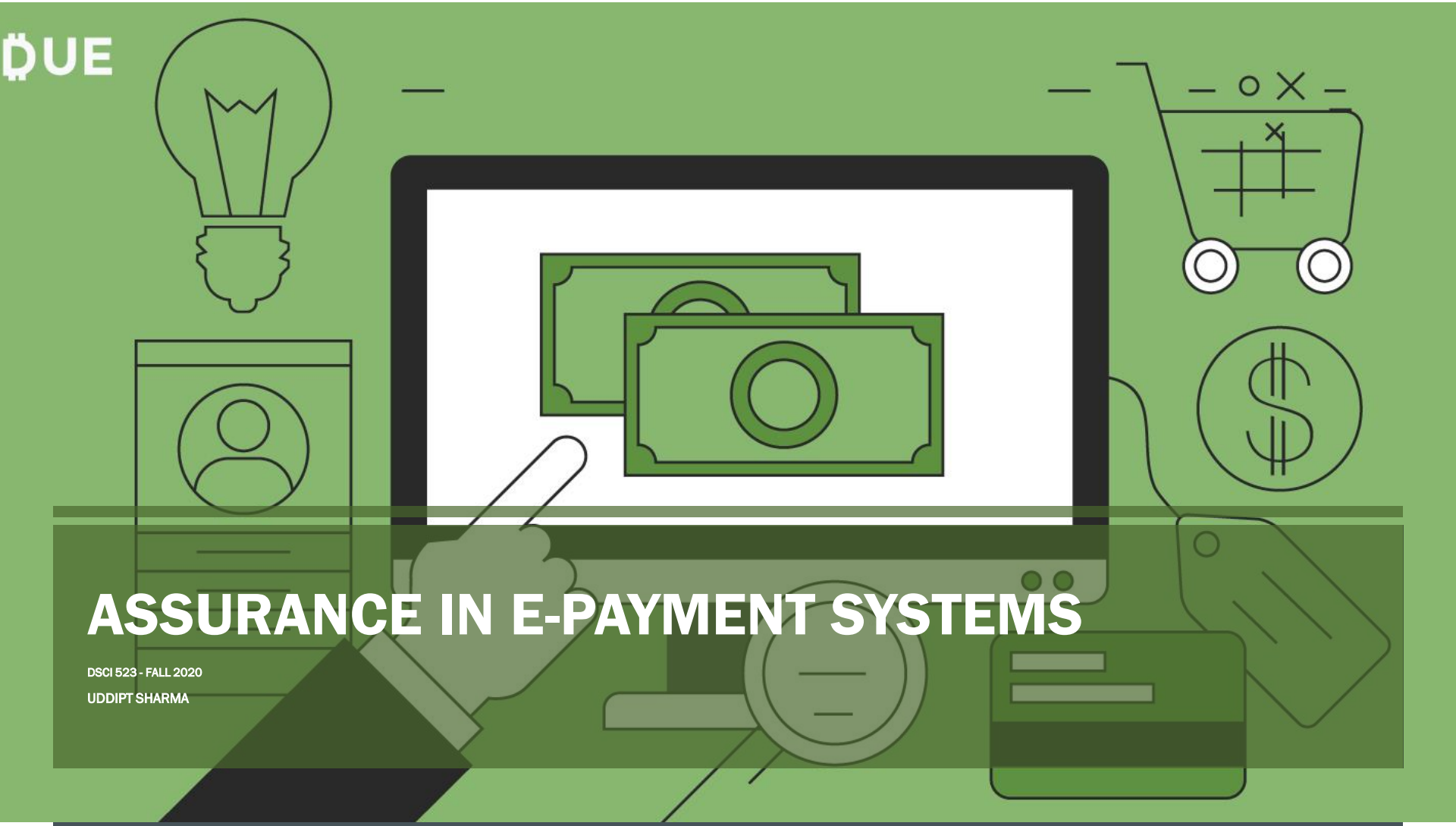
- https://www.apple.com/apple-pay/
- https://squareup.com/us/en/point-of-sale
- https://www.verifone.com/en/mobile

Tech forums

- https://nfc-forum.org

Thoughts or Additions

- Is there anything you'd like to see covered?



ASSURANCE IN E-PAYMENT SYSTEMS

DSCI 523 - FALL 2020

UDDIPT SHARMA

WHAT ARE ELECTRONIC PAYMENT SYSTEMS?

- An e-payment system is a way of making transactions or paying for goods and services through an electronic medium, without the use of checks or cash. It's also called an electronic payment system or online payment system
- E-payment methods could be classified into two areas, credit payment systems and cash payment systems
- Credit Payment System- Includes Credit Card, E-wallet and Smart Card
- Cash Payment System- Includes Debit Card, E-check, Prepaid Cards and E-cash

SOUNDS GREAT, SO ARE THERE ANY DRAWBACKS?

- E-commerce **fraud** is growing at 30% per year. If you follow the security rules, there shouldn't be such problems, but when a merchant chooses a payment system which is not highly secure, there is a risk of sensitive data breach which may cause identity theft.
- **The lack of anonymity** — For most, it's not a problem at all, but you need to remember that some of your personal data is stored in the database of the payment system.
- **The need for internet access** — As you may guess, if the internet connection fails, it's impossible to complete a transaction, get to your online account, etc.

UNDERSTANDING THE PAYMENT GATEWAY

- Payment gateways facilitate communication and transmit transaction information between a payment portal (such as a website, mobile phone or interactive voice response service) and front-end processor of the acquiring bank
- It encrypts payment information, and then proceeds to authorizing payment and securely passing the information between sender and receiver
- When an order is confirmed by both the customer's as well as merchant's web server, a request from the application is sent to the payment gateway for payment processing
- After completion of the processing, gateway sends a response to the application in terms of success or failure
- The key concern of millions of people across the Globe lies around – "Is my transaction safe?", "Is my information secure?

ASSURANCE IN E-PAYMENT SYSTEM

- The uttermost importance to a business or Bank is the security and integrity of their payment processing system
- These system are often developed by third parties and thus needs a formal assurance for its security
- Security and Functional testing plays an important role in safeguarding the interest of both the parties
- Payment gateway testing requires continuous planning and diligence since it involves testing of different aspects such as security, web service connectivity, authorization, and data encryption
- End-to-end testing is to be performed with dedication and accuracy as the application is to be used for sensitive purposes
  - Functional Testing
  - Integration Testing
  - Security Testing
  - Performance Testing

REGULATIONS AND STANDARDS

- The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements intended to ensure that all companies that process, store, or transmit credit card information maintain a secure environment
- It was launched on September 7, 2006, to manage PCI security standards and improve account security throughout the transaction process
- While the PCI SSC has no legal authority to compel compliance, it is a requirement for any business that processes credit or debit card transactions
- PCI certification ensures the security of card data at your business through a set of requirements established by the PCI SSC
- PCI-compliant security provides a valuable asset that informs customers that your business is safe to transact with and provide assurance

OVERVIEW OF PCI SSC DATA SECURITY STANDARDS

- Use and Maintain Firewalls
- Proper Password Protections
- Protect Cardholder Data
- Encrypt Transmitted Data
- Use and Maintain Anti-Virus
- Restrict Data Access
- Unique IDs for Access
- Restrict Physical Access
- Create and Maintain Access Logs
- Scan and Test for Vulnerabilities
- Document Policies

OTHER STANDARDS

- **Federal Financial Institutions Examination Council (FFIEC) has developed a Cybersecurity Assessment Tool** (CAT) helps institutions identify their risk level and determine the maturity of their **cybersecurity** programs inducing payment system
- **NIST Special Publication 800-63B, Special Publication (SP) 800-63, SP 800-63A, and SP 800-63C provide** technical guidelines to agencies for the implementation of digital authentication
- **ISO 20022** is an ISO standard for electronic data interchange between financial institutions.
- It describes a metadata repository containing descriptions of messages and business processes, and a maintenance process for the repository content
- It covers financial information transferred between financial institutions that includes payment transactions, securities trading and settlement information, credit and debit card transactions and other financial information

THANK YOU

U.S. Voting Machines

INITIAL ASSURANCE ANALYSIS

BY ANTHONY CASSAR

Voting machines in 2020?

(DRE)Voting Machines

- Importance of election security
- Lack of existing security
- Average people don't talk about it!
- Issues with funding?

Who are the Threat Actors?

- Entry Level
  - Hacktivists(Ex:Anonymous)
- Mid Level
  - Organized Crime(Ex:Cybercriminal Groups)
  - Why?
- High Level
  - APTS(Ex: Goverment Sponsored and Nation-state(Fancy Bear)
- Others
  - Don't exist on the attack surface

Initial Security Assessment

- Trusted Distribution
- Physical Area
- Administrative Flaws
- Technical Security Misconfigurations

Where does it come from?

- Voting Machines
  - Approximately 60 percent of voting machine components are made outside U.S.
    - Made in China(20 percent) and Russia
    - As of December 2019 according to Interos
    - Age of these Products(Up to 10 years)

Vendor and Accreditors

Many different kinds and why is this?

- Competition
- Affordability
- No standardized system
- Voluntary(in Some Cases)
- Election Security Act of 2019(No Specific Requirements)

TCB

- Lines of Code Generally(Couple Thousand)
- Uses(Focuses on Integrity not Confidentiality)
- Involves 4 layers(App's,Drivers,I/0,Compiler)
- Some Issues(Tamper Proof, ACl, Code)

Plan of Action

- Step#1 Research further about Security Assessments and Standards for voting machine
- Step#2 Implement improved assurance polices for a single standardized voting system.
- Step#3 Review the security polices and point out the weaknesses and strengths of each item.

Consequences

- Questioning the integrity of U.S. Elections
  - Rigged Systems
  - Foreign Control or Influence
  - Civil Conflict

References

- https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime-activities.html
- https://www.lexology.com/library/detail.aspx?g=8ca91844-7c49-4542-9a7a-f78530b616dc
- https://www.cisecurity.org/spotlight/cybersecurity-spotlight-cyber-threat-actors/
- https://www.securitymagazine.com/articles/91889-concerned-about-nation-state-cyberattacks-heres-how-to-protect-your-organization
- https://www.usenix.org/legacy/event/evt07/tech/full_papers/feldman/feldman_html/index.html
- https://www.brennancenter.org/sites/default/files/analysis/Fact_Sheet_Voting_System_Security.pdf
- https://link.springer.com/chapter/10.1007/978-3-642-14577-3_24
- https://crypto.stanford.edu/cs155old/cs155-spring11/papers/rubin-wallach-voting-paper.pdf
- http://www.cs.jhu.edu/~ryan/min_tcb_voting/ggr_min_tcb_voting-full.pdf
- https://www.ncsl.org/research/elections-and-campaigns/elections-technology-toolkit.aspx
- https://www.google.com/search?q=hacker+picture&client=firefox-b-1-d&sxsrf=ALeKk01kJn2_96QvryeyDcJjyipMdCYEmA:1600740136266&tbm=isch&source=iu&ictx=1&fir=QkKIq2YDs1wetM%252CN4mIchtxLxyKIM%252C_&vet=1&usg=AI4_-kRuCL-BkY5ZOBa-ePyiMsdcIxgPHg&sa=X&ved=2ahUKEwjwlczZ1fvrAhX_HzQIHQ5ADAUQ9QF6BAgKEFU&biw=1440&bih=709#imgrc=QkKIq2YDs1wetM
- https://www.eac.gov/voting-equipment/registered-manufacturers
- https://www.eac.gov/sites/default/files/eac_assets/1/1/State%20Requirements%20and%20the%20Federal%20Voting%20System%20Testing%20and%20Certification%20Program.pdf
- **https://www.congress.gov/bill/116th-congress/senate-bill/1540/text#toc-HF25CFB6336F049508B0D6862239221FB**

Autonomous Vehicles

CHRIS SAMAYOA

SEPTEMBER 25, 2020

Technology Overview

Levels of Automation

None	Driver Assist	Partial Automation
Conditional Automation	High Automation	Full Automation

Traffic Efficiency

- Los Angeles / New York
- Growing population

Safety / Economics

- Vast reduction in accidents and insurance payouts

Convenience

Initial Assurance Issues

Network Segmentation

- Entertainment
- Vehicle telemetry
- Navigation and sensory

Trusted Computing Base

- Which components are critical for safety?
- Potential to root system for performance?

Software

- Design
- Code Review
- Updates

Data Centralization

Regulatory Agencies and Common Security Policies

Potential Consequences

Loss of Life

- System errors
- Targeted attacks

Manufacturer Liability

- Who is responsible for accidents?

Privacy Issues

- Potential to remotely track movements
- Legitimate / illegitimate

Vehicle Hijacking

Sources of Information

Vehicle Manufacturers
- Uber/Yandex
- Google
- Tesla

Analysis of wireless technologies (Bluetooth, Wi-Fi, etc.)

National Highway Traffic Safety Administration (NHTSA)

Past Assurance Issues
- Aviation
- Previous Automobiles

Uber

Questions?

Assurance in Autonomous Vehicles

Amarbir Singh

Class of System

- Advanced driver assist systems – Adaptive cruise control, lane assist
- Emergency driver assist systems – Emergency breaking, proximity sensors
- Partial/full self-driving systems – Autopilot, automated lane changes, traffic light recognition, smart-cars
- Driverless vehicles, futuristic Robotaxi
- Subset of IoT devices

Assurance Issues

- Assurance of software – Software running on cars, phone apps
- Assurance of Artificial Intelligence
- Assurance of hardware – Computers, sensors
- Assurance of OTA updates, upgrades
- Assurance of 3rd party software/hardware
- Assurance of wireless communication protocols

Consequences of Security Failures

- Consequences of Confidentiality and Integrity failures
- Consequences of Availability Failures – Natural and targeted
- Consequences of Authentication and Authorization failures
- Consequences of design flaws

- Theft, extortion, injury, or much worse

Answer these Questions

- Information and evidence provided by manufacturers
- Independent research findings
- Government agencies and regulations (domestic and international)
- Manufacturers of hardware and software
- Incidents of security failures in news

Suggestions!

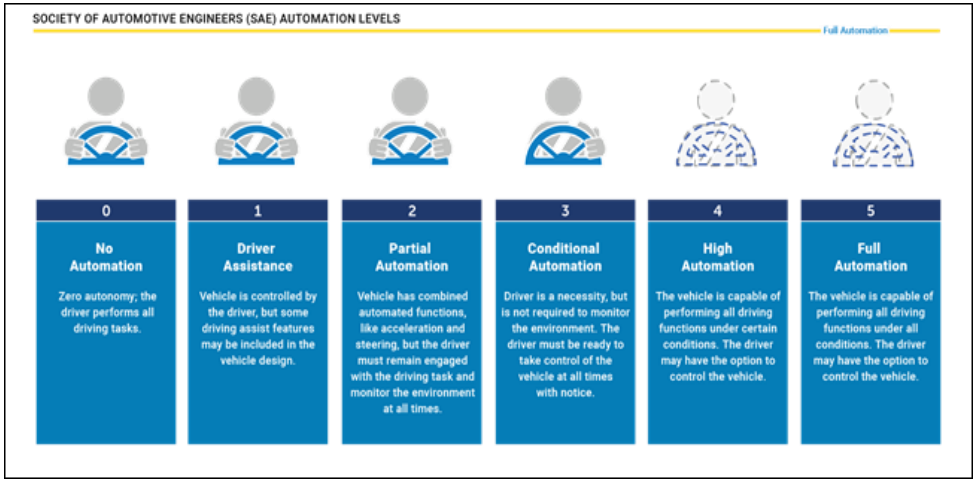
- Research regarding cybersecurity assurance of autonomous vehicles is sparse
- Similarities to other IoT devices

- Questions?

Security Assurance in Connected & Automated Vehicles

Abhishek Tatti
DSCI -523

Overview



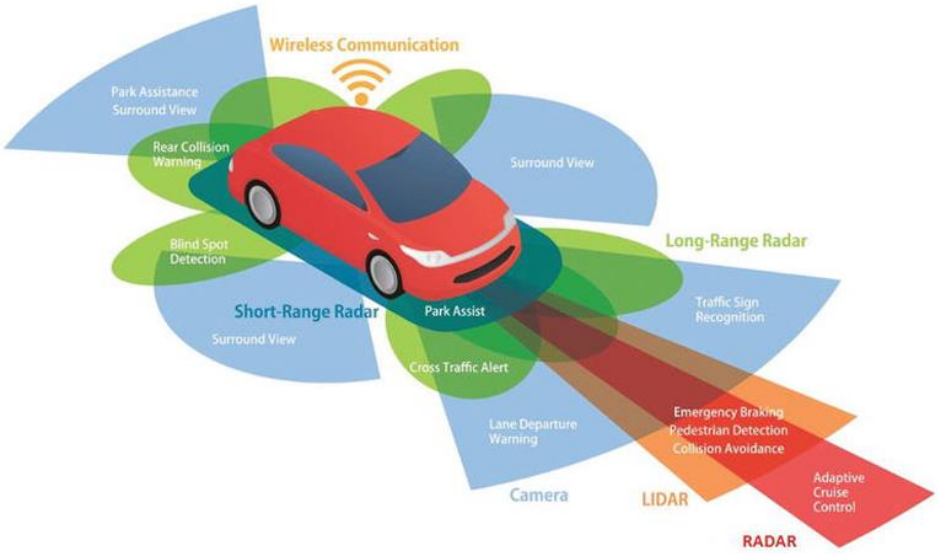
Autonomous vehicles are a reality - Waymo has racked up more than 10 million miles of running autonomous cars on public roads.

Laws and regulations to support CAVs - Arizona, California.

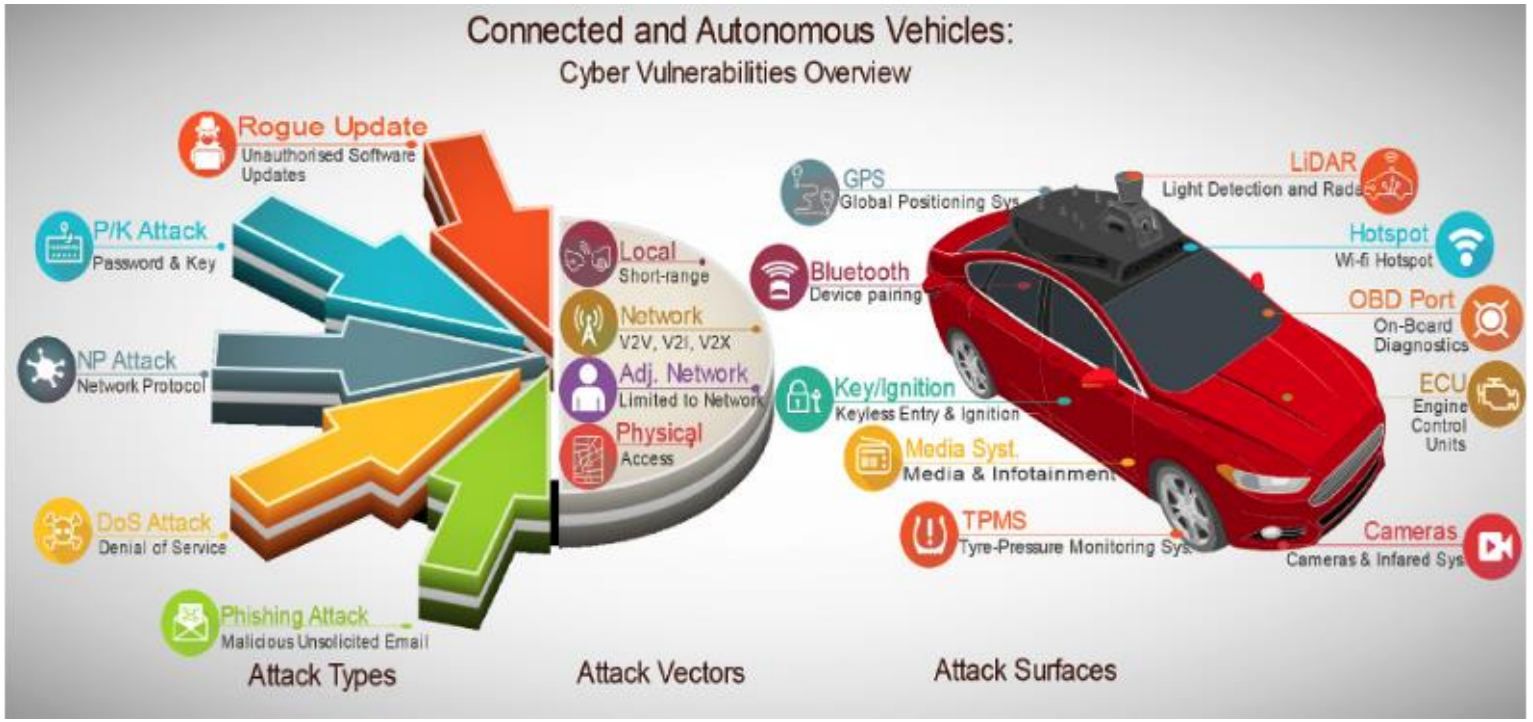
Key Players - Waymo, GM Cruise, AI Agro, Tesla, Uber and many more.

Challenges with Automotive security

- **Life of Vehicle is more** - More chance for hacker to find vulnerability
- **Assurance solutions are time consuming** - Encryption, authentication
- **ECU** (Memory & Computations constraints)
- **Privacy** - Location, Driving History
- **Cyber Physical** - Sensors, actuators - LIDAR, cameras, radar, light matrices, devices for sensing angular momentum of the wheels, & automated brake and steering control.
- **Computation and communication**- under hard real-time requirements



Vulnerabilities Overview:



Threats:

Long Distance (Remote Attacks)

- Attack a listening service in the communications module
- Attack against a remote assistance style feature. For example, Phantom Auto
- Attack again base devices on the base vehicle: telematics, infotainment, etc.
- Attacks against the infrastructure

Short Distance (Remote Attacks)

- Attack against Wi-Fi communications module
- Attack against Bluetooth
- Attack against Tire Pressure Monitoring System (TPMS)
- Attacks against the vehicle's sensors- general jamming attacks or more specific attacks to try to affect what a vehicle perceives in its environment.

Please find my resume attached to this email.

Threats

Physical Access Attacks

- Reprogramming an existing ECU to do something nefarious.
- Attack the Ethernet network in the vehicle - plugging a laptop into the ethernet network and attacking other Ethernet devices.
- An attacker may leave a rogue device on the Ethernet network that would affect the cars behavior at a later time.
- Tablets in the back of the vehicle.

Attacking the Base Vehicle

- Attacking the base vehicle on which the autonomous features are built i.e. attack the non-autonomous part of the stack.
- For example, attack the special firmware on the ECUs to allow complete computer control, or attack the built in TPMS functionality.

Non-Safety-Critical Attacks

- These attacks involve different types of theft, fraud, and personal information.

Assurance Issues:

- Code verifiability on system boot up
- Bootstrapping Cryptographic Keys
- Key Storage
- Code and Data Signing
- Attack Surface Reduction
- Encryption of data at rest
- Segregation
- Ethernet Switch
- Message Signing
- Tablets
- Remote Assistance
- Fleet Management
- Threat Detection
- External Communication
- Component Reduction
- Sensors

Consequences of Security Failure

- The most obvious consequence is the danger to the life of the passenger, bystanders, other vehicles, property or the environment in which the CAV runs.
- Vulnerability to Hacking & Remote Control
- Vehicle theft
- Accidents between Self-Driving and Manual Cars
- Privacy Issues - Owner and Passenger Information, Location tracking, Sensor data

Phase 2:

Use the following to identify assurance techniques:

- Understand general architecture and communication models for CAVs
- Analyzing CAV hacks in the recent past and identifying root cause and establishing a relation with assurance.
- Analyzing Security Architecture of major CAV companies – using whitepapers
- Security frameworks, standards and models to identify threat handling and assurance in CAVs - NHTSA (Cybersecurity Best Practices for Modern Vehicles)
- Quantitative and Risk Management Frameworks
- New method to prevent attacks – Deep learning, Machine learning, etc.

References:

- **The Fog Computing Paradigm Scenarios and Security Issues**
  - Ivan Stojmenovic, Sheng Wen
- **Connected and autonomous vehicles - A cyber-risk classification framework**
  - Barry Sheehan , Finbarr Murphy, Martin Mullins, Cian Ryan
- **Cyber Threats Facing Autonomous and Connected Vehicles - Future Challenges**
  - Simon Parkinson , Paul Ward , Kyle Wilson , Jonathan Miller
- **The Security of Autonomous Driving Threats, Defences, and Future Directions**
  - Kui Ren, Qian Wang, Cong Wang, Zhan Qin, and Xiaodong Lin
- **Certified Control: A New Safety Architecture for Autonomous Vehicles**
  - Jeff Chow, Valerie Richmond et all
- **The Role of Virtual Reality in Autonomous Vehicles Safety**
  - Alexandre M. Nascimento, Anna Carolina M. Queiroz et all
- **Security of Emergent Automotive Systems: A Tutorial Introduction and Perspectives on Practice**

Questions and Feedback

Tesla Motors
The Assurance Dilemma

Dwayne Robinson
DSCI523
University of Southern California
September 25, 2020

Company Statistics

- As of March 2020 Tesla has delivered 985,154 vehicles
- Vehicle delivery growth is increasing at an average of 2% per quarter with deliveries of 90,650 vehicles in the quarter ending June 2020
- CEO Elon Musk stated in the most recent earnings call that the company expects to deliver approximately 112,000 vehicles in the next quarter which is a 24% increase
- Tesla has a market cap valuation more than GM and Ford

Why do the company statistics matter?

- Tesla is rapidly becoming a data collection powerhouse
- Disruption of this automaker could have far reaching affects
  - Failure or modification of Tesla eco system could cause damage to the automotive company and industry advancements as a whole
- The average Tesla uploads between 50mb & 500mb of data per day to the Tesla Data Centers

  (Data is dependent on the amount of miles driven per the car)
- With an average of 100mb of data unloaded per vehicle per day, Telsa is collecting ~100tb of data per day fleet wide

  (this doesn't include data collection of their solar products)

Assurance Issues

- Tesla vehicles are mostly controlled by a computer, a device they call the MCU
- The vehicles have a collection of eight cameras that record a near 360° view around the vehicle constantly, a feature they are calling Sentry
- Tesla also has a feature called autopilot, which is in beta. This is an autonomous driving feature
  - With the advanced version the vehicle could detect stop signs and speed limits, detect the vehicle in front of your vehicle and suggest lane changes automatically
- Tesla also maintains logs for their autopilot offering and currently has logs for more than 3billion miles driven on their autopilot service

Assurance issues & Consequences

- Data breech
  - They amount of data maintained on +/- 1mm vehicles could be very valuable to a competitor or possibly foreign entity
  - Data obtained licitly could be used to compromise vehicles
- Vehicle hack
  - If the vehicle security if thwarted, unsuspected vehicle changes can happen such as acceleration which could cause potentially fatal accidents
  - Thwarting internal security could lead to modifications of the safety of the vehicle and could but the driver and pedestrians in danger

Assurance issues & Consequences (continued)

- Privacy
  - Unencrypted video that is stored on the vehicle accessible via a USB port
  - Additional unintended, possibly secret information could be determined from available information
- Special Feature Availably
  - A key component in their infrastructure, is over the air updates and ongoing features to the vehicle fleet
  - Maintaining the constant availability and assurance that the updates will not damage the vehicle paramount to maintaining the company's success

Identification of Assurance issues

- Local and Federal Government Safety Laws and Legislation
- The National Highway Traffic Safety Administration
- Various articles involving Tesla Data Breeches
- Published articles and excerpts of data updates regarding unauthorized vehicle modification
- Tesla’s public records to prevent vehicle / cyber hacks
- Tesla’s privacy and legal statements

TESLA

Questions / Discussion

Avionic Systems

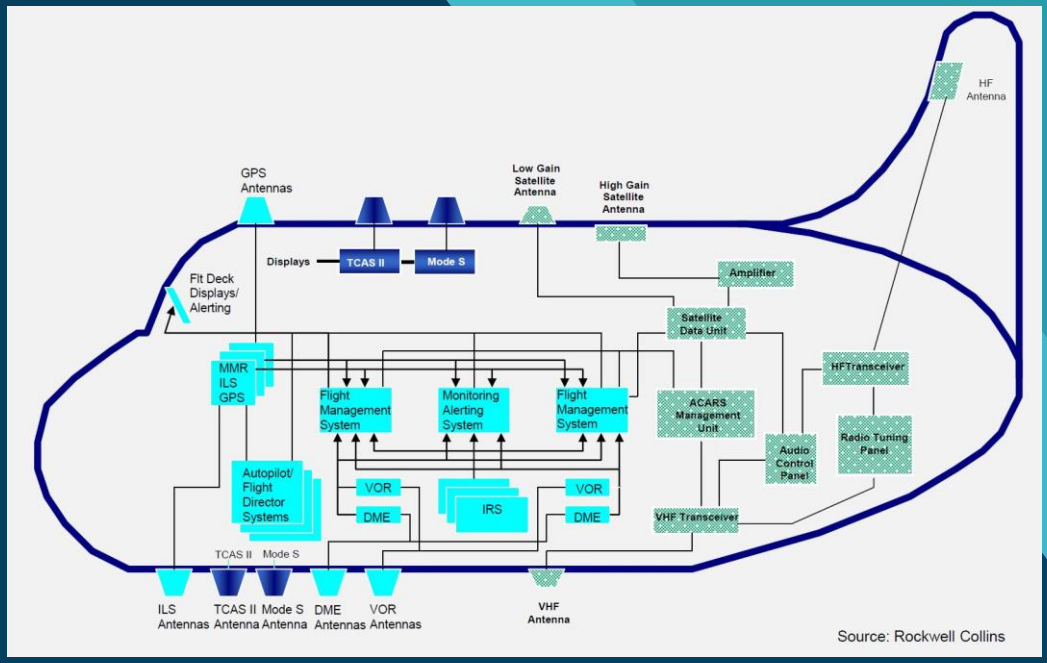
-A Cybersecurity Perspective

Pratyush Prakhar
Dsci523
2468183206

What do you mean by avionics ?

Avionic Systems

- Avionic systems in simplest of words are a class of electronic systems that are specifically designed and utilized in aviation.
- An amalgam of aviation hardware and management software which is responsible for minutest of tasks in such a complex flight network.
- Commercial airliners, helicopters, military fighter jets, unmanned aerial vehicles (UAV), business jets, and spacecraft all use avionics in different capacity. They range from engine controls to flight control systems to navigation, communications and even performance monitors



Why I chose this topic ?

“ Good Night, MH370 ”

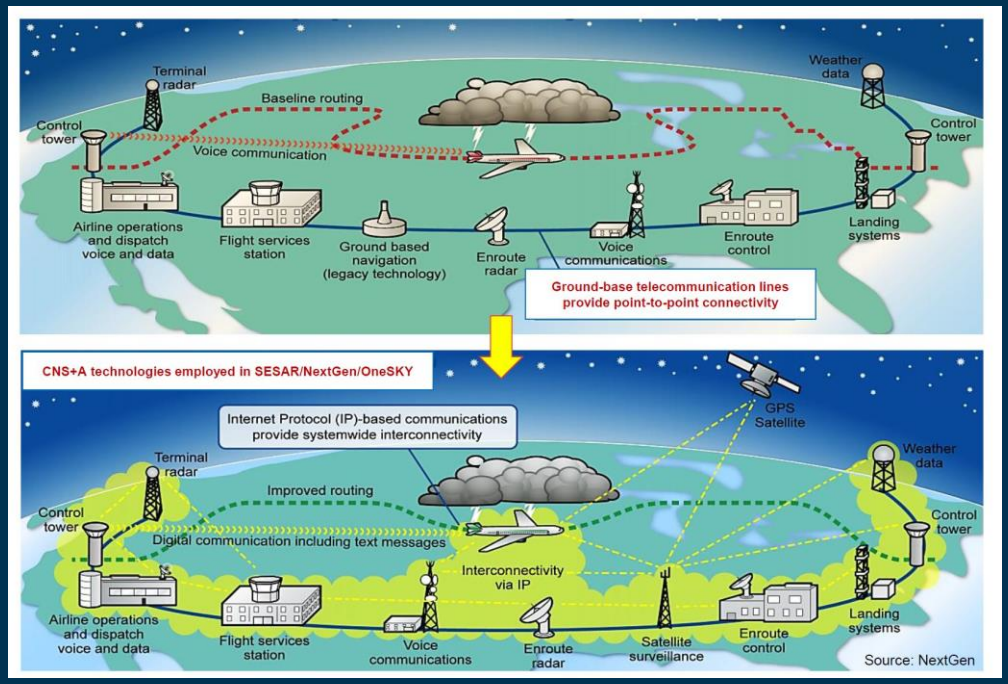
- Last message to Malaysian Airline flight MH370 before it’s disappearance

Best answer till date –
Cyber Security Hack into the plane’s avionic system.

Need of Cyber Security Assurance in Avionics

What changed?

- The avionics industry has gon through a rigorous evolution cycle in the last 50 years or so. They transitioned from individual task controlling systems to an integrated Intelligent Transport System (ITS).
- To accommodate with the growing air travel, the avionic system become more sophisticated by day. They are now an intricate system of navigation, communication and surveillance systems/sensors for airplane's automated applications and multi-platform networking. On top of that is the communication network which supports the hardware and software.
- Also, more and more aviation systems are based on commercial off-the-shelf products and solutions owing to the commercial airplane boom. The increased reliance on the vulnerable operating systems such as Linux, Windows and wireless protocols.
- The result of moving forward is moving backwards, as the widespread adoption of these technologies has unleashed increased vulnerabilities and greater risk to the avionics systems.



Key Issues

Cyber Security Policy

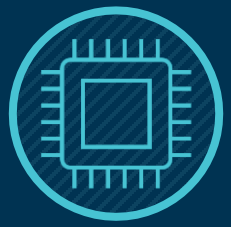
Multiple players in multi ecosystems

Commercial – AIA, ACI, A4A

Military – NIST, NSS, DoD

Drive Force

Economics have overtaken security in a commercial airline industry. Every resource dedicated to comfort.



Growth in Vulnerable Hardware Components

The integration of IoT sensors and entertainment system with core avionic system.

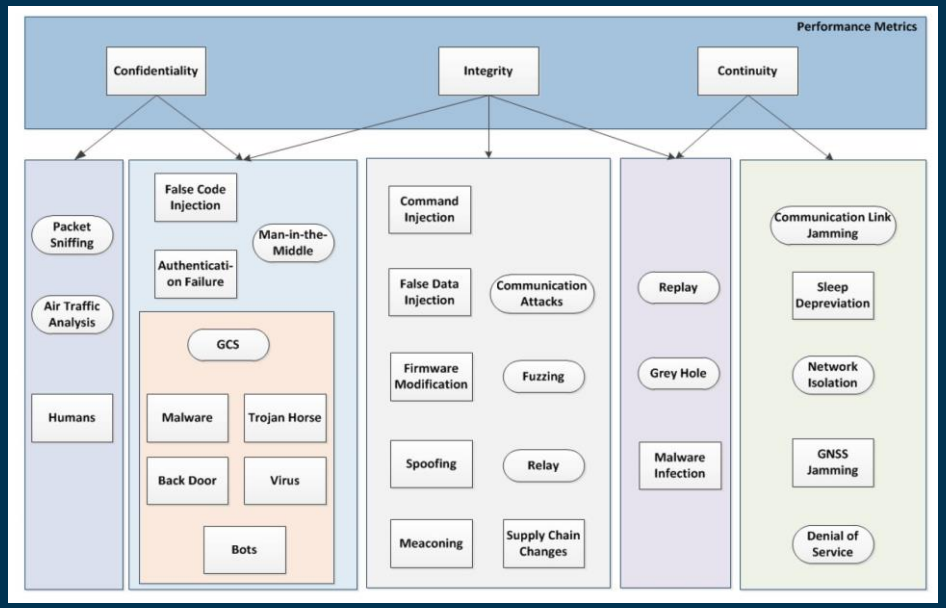
Malicious Software

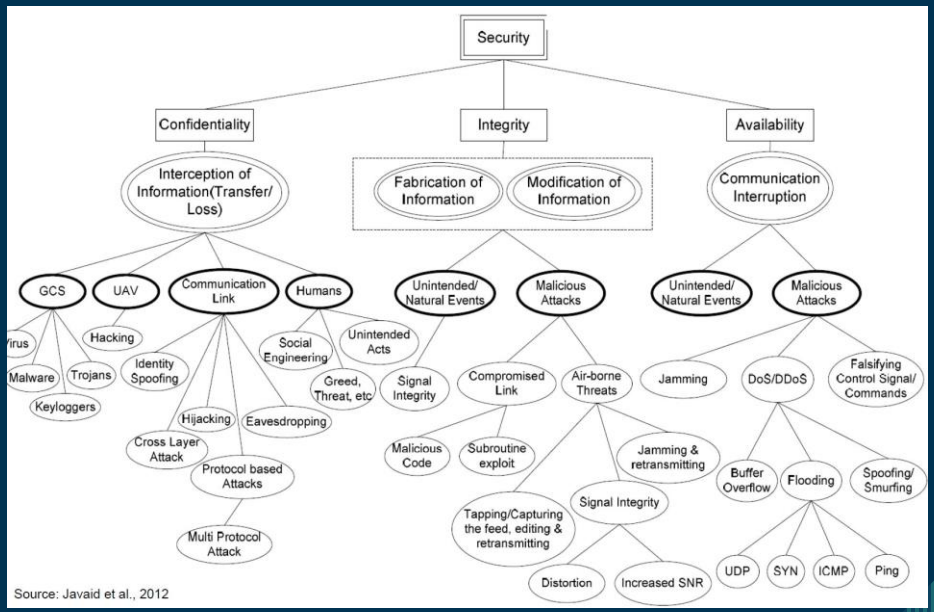
Although very hard task to obtain access to in flight systems. But again 99% secure is still insecure. Low standard commercial products add fuel to fire. Plus Huge.

NextGen Technology

Projects like Single European Sky ATM Research (SESAR) and the Next Generation Air Systems (NextGen) are modernizing Air Traffic Management but increased connectivity and information exchange comes increased cyber risk.

Known Vulnerabilities


Performance Metrics
Confidentiality
Integrity
Continuity
Packet Sniffing
Air Traffic Analysis
Humans
False Code Injection
Man-in-the-Middle
Authenticati-on Failure
GCS
Malware
Trojan Horse
Back Door
Virus
Bots
Command Injection
False Data Injection
Communication Attacks
Firmware Modification
Fuzzing
Spoofing
Relay
Meaconing
Supply Chain Changes
Replay
Grey Hole
Malware Infection
Communication Link Jamming
Sleep Depreviation
Network Isolation
GNSS Jamming
Denial of Service


Security
Confidentiality
Integrity
Availability
Interception of Information(Transfer/ Loss)
Fabrication of Information
Modification of Information
Communication Interruption
GCS
UAV
Communication Link
Humans
Unintended/ Natural Events
Malicious Attacks
Unintended/ Natural Events
Malicious Attacks
Hacking
Identity Spoofing
Malware
Trojans
Keyloggers
Social Engineering
Unintended Acts
Greed, Threat, etc
Signal Integrity
Hijacking
Eavesdropping
Cross Layer Attack
Protocol based Attacks
Multi Protocol Attack
Compromised Link
Air-borne Threats
Malicious Code
Subroutine exploit
Jamming & retransmitting
Signal Integrity
Tapping/Capturing the feed, editing & retransmitting
Distortion
Increased SNR
Jamming
DoS/DDoS
Falsifying Control Signal/ Commands
Buffer Overflow
Flooding
Spoofing/ Smurfing
UDP
SYN
ICMP
Ping
Source: Javaid et al., 2012

Impact

Human Life

There are multiple ‘ifs’ attached with the safest mode of transport. But we know better a small bug can bring down these complex systems. This pose immediate danger to travelling population.

Economy

2014 alone bought staggering $400 mil in loss due to cyber security breaches. A survey PWC places 85% CEOs in aviation industry fear cyber breaches in their avionic systems.

Also, the transport in question cost a handsome when it comes to mitigating the vulnerabilities.

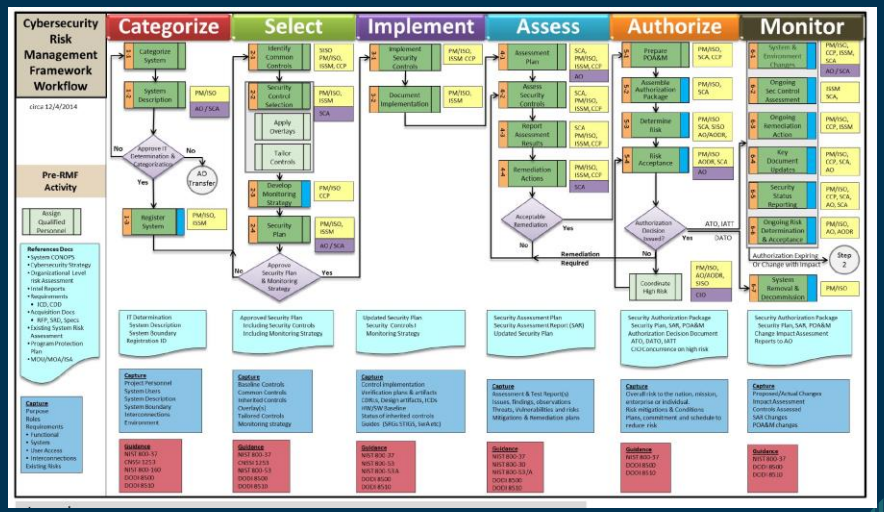
Where to look for Answers ?

Policy Framing

- Integration of multi ecosystem policies into one.
- Setting a higher standard of security systems involved. Commercial on-flight systems should have higher accountability.
- End-to-End Security Assessment.
- Proper Translation to actual mechanism with high assurance sue to the critical data involved.
- Taking a stance on vulnerable ITS components. Minimization.
- Secure interoperable communication systems.

Risk Management Framework

- Big player in this sector such as DoD and AIA both push for a higher cyber security risk management frameworks. This provide high assurance of implementation of cyber security policy concerning aviation with feedback mechanism.



Thank You

Reference

- https://www.baesystems.com/en-us/definition/what-is-avionics
- https://www.aia-aerospace.org/wp-content/uploads/2019/10/AIA-Civil-Aviation-Cybersecurity-Recommendations-Report-2019-Final-1.pdf
- http://mys5.org/Proceedings/2015/Day_3/2015-S5-Day3_1305_VanNorman.pdf
- https://www.pwc.com/us/en/industrial-products/publications/assets/pwc-airline-industry-perspectives-cybersecurity.pdf