Compliance & Security Framework

(Chapter -2 : DISSA Course)

Arijit Chakraborty

May 29, 2021

PCI DSS

- The Payment Card Industry Data Security Standard (PCI DSS) exists to protect **security of cardholder data.**
- Mandatory for organizations that process credit card data.
- For example, banks, merchants, processors and service providers
- **IS Auditor role**

✓ enforcing certain procedures and controls based on PCI DSS level,
✓ complete self-assessment questionnaires,
✓ quarterly network scans, and
✓ on-site independent security audits.

PCI COMPLIANCE

- **Payment card industry (PCI)** compliance
- mandated by credit card companies to help ensure security of credit card transactions in the payments industry.
- **Payment card industry compliance** refers : *technical and operational standards that businesses follow to secure and protect credit card data provided by cardholders and transmitted through card processing transactions.*
- PCI standards for compliance are developed and managed by the **PCI Security Standards Council**

SERVICE PROVIDERS AND OTHER THIRD PARTIES

- All **business partners, entities providing remote support services, and other service providers connected to CDE** or may have risk of potentially compromise an entity's CDE **are also considered in PCI DSS scope.**

- If an entity **outsources in-scope functions or facilities to a third party, or utilizes a third-party service that impacts how it meets PCI DSS requirements**, the entity will **need to work with the third party to ensure the applicable aspects of the service are included in scope for PCI DSS.**

- As per PCI DSS standard, "System components" include **network devices, servers, computing devices, and applications**.

- A system component being in scope **does not mean** that all PCI DSS requirements apply to it.

- The applicable PCI DSS requirements depend on the function and/or location of the system component.

PCI DSS Scope- Process flow

Activity	Description
Identify how and where the organization receives cardholder data (CHD)	1**. Identify all payment channels** and methods for accepting CHD, from the point where the CHD is received through to the point of destruction, disposal or transfer.
Locate and document where account data is stored, processed, and transmitted	2. **Document all CHD flows**, and identify PPT involved in storing, processing, and/or transmitting of CHD. These people, processes, and technologies are all part of the CDE.
Identify all other system components, processes, and personnel that are in scope.	3. **Identify all processes (**both business and technical), system components, and personnel with the ability to interact with or influence the CDE (as identified in 2, above). These PPT are all in scope, as they have connectivity to the CDE or could otherwise impact the security of CHD.
Implement controls to minimize scope to necessary components, processes, and personnel.	4. **Implement controls** to limit connectivity between CDE and other in-scope systems to only that which is necessary. 5.Implement controls to segment the CDE from people, processes, and technologies that do not need to interact with or influence the CDE.
Implement all applicable PCI DSS requirements.	5**. Identify and implement** PCI DSS requirements as applicable to the in-scope system components, processes, and personnel.
Maintain and monitor.	6. **Implement processes** to ensure PCI DSS controls remain effective day after day. 7.Ensure PPT included in scope are accurately identified when changes are made

12 REQUIREMENTS OF PCI DSS

- Requirements by the **PCI SSC** : both operational and technical,
- **Core focus** = always to **protect cardholder data.**

1. **Install and maintain a firewall configuration to protect cardholder data** -

Configuration rules to be **reviewed bi-annually** & ensure **no insecure access rules** which can allow access to CDE.

2. **Do not use vendor-supplied defaults for system passwords and other security parameters-**

Most of O/S & devices come with **factory default setting such as usernames, passwords**, & insecure configuration parameters. Default usernames and passwords **simple to guess,** even published on Internet. Such default passwords & security parameters **are not permissible per this requirement**

3. **Protect stored cardholder data**

4. **Encrypt transmission of cardholder data across open, public networks-**

secure card data when it is transmitted over open or public network (e.g. Internet, Bluetooth, GSM, CDMA, GPRS).

PCI DSS

5. **Use and regularly update anti-virus software or programs-**

anti-virus or anti-malware programs , anti-virus mechanisms to be always active, generating auditable logs.

- 6. **Develop and maintain secure systems and applications** = areas :
  - Operating systems
  - Firewalls, Routers, Switches
  - Application software
  - Databases
  - POS terminals

7. **Restrict access to cardholder data by business need to know**

8. **Assign a unique ID to each person with computer access-** should not use shared/group user and passwords

9. **Restrict physical access to cardholder data-**

*use of **video cameras/electronic access control to monitor entry** and exit doors of physical locations such as data centre. Recordings or access logs of personnel movement to be **detailed for minimum 90 days***

10. **Track and monitor all access to network resources and cardholder data-** *all the systems must have **correct audit policy set** & **send logs to centralized syslog server,** logs must be reviewed **at least daily to look for anomalies**, & suspicious activities*.

Security Information and Event Monitoring tools (SIEM), can help to log system and network activities, monitor logs and alert of suspicious activity

11. . **Regularly test security systems and processes**

- ✓ **Wireless analyser scan** to detect & identify **all authorized and unauthorized wireless access points on a quarterly basis.**

- ✓ **All external IPs and domains exposed in the CDE** are required to be scanned by a PCI **Approved Scanning Vendor** (ASV) at **least quarterly.**

- ✓ **Internal vulnerability scan** must be conducted **at least quarterly.**

- ✓ All external IPs and domains must go through exhaustive **Application penetration test** and **Network penetration test at least yearly or after any significant change.**

- ✓ **5. File monitoring is a necessity**. The system should perform file comparisons **each week to detect** changes that may have otherwise gone unnoticed.

12. **Maintain a policy that addresses information security for all personnel -** SOP:

- ✓ An annual, formal risk assessment that identifies critical assets, threats, and vulnerabilities.

- ✓ User awareness training

- ✓ Employee background checks

- ✓ Incident management

NIST Framework

- **NIST**
- **National Institute of Standards and Technology** -federal agency within Department of Commerce that spans manufacturing, quality control, and security,
- Collaborates with security industry experts, other government agencies, to establish **set of controls & balances** to help operators of critical infrastructure manage cybersecurity risk.
- For **IS team member of an organization that leverages NIST,**
- identifying, defining, and enforcing controls that are governed by the standard.
- For example, in VAPT / vulnerability scanning: NIST 800-53 Risk Assessment RA 5, which deals :
- frequency of scans,
- type of scanning that should be done,
- Reporting the results of these scans
- **What type of organizations leverage this framework?**
- large business enterprises and government agencies, but may be customized for SME

SSAE-16

- **Statement on Standards for Attestation Engagements** No. 16 (SSAE-16) monitors & enforces controls around applications and application infrastructure that impact financial reporting.

✓ covers business process controls & ITGC .

✓ Service Organization Controls (SOC) 1 reports, formerly known as SAS 70 reports, leverage the SSAE-16 framework.

✓ The SSAE-16 framework = best practices,

✓ mandatory part of SOX compliance process.

AT-101 Audit standard

- SOC 2 reports based on the AT-101 auditing standard. SOC 2 reports test the design or operating effectiveness of security, availability, processing integrity, confidentiality, and/or privacy controls.
- All SOC 2 reports need to cover security controls. Availability, processing integrity, confidentiality, and/or privacy controls
- **IS Auditor**
- To Review SOC 2 reports from other organizations can reveal how partnering with them could introduce risk into Organisation environment.
- **Organizations using AT 101 framework**
- Software as a Service (SaaS) providers,
- Cloud computing companies, and other technology-related services

FedRAMP

- FedRAMP = standardized way for government agencies to evaluate the risks of cloudbased solutions.
- ❑ It follows a “do it once, use it many times” approach, allowing existing security assessments and packages to be reused across multiple agencies.
- ❑ can improve real-time security visibility for organizations.
- In government agency, IS Auditor will use FedRAMP packages to decide whether it makes sense to leverage specific cloud-based solutions.

- Cloud solution providers interested in selling to federal government agencies will go through the FedRAMP certification process.

HIPAA / HITECH

- A. Health Insurance Portability and Accountability Act (HIPAA) signed into law in August 1996, updated by HIPAA Privacy Rule in 2003 & HIPAA Security Rule in 2005, amended - 2009
- HIPAA encompasses:

✓ Technical Safeguards
✓ Physical Safeguards
✓ Administrative Safeguards
✓ Privacy Rule
✓ Breach Notification Rule
✓ Enforcement Rule
✓ Data Encryption

- B. Health Information Technology for Economic and Clinical Health (HITECH) Act
- **HITECH** enforces **security to protect Personal Health Information (PHI).**
- **Applicability :** who is **collecting, storing or processing personal health information (PHI), including hospitals, medical providers, and insurance companies.**
- HITECH Act is to improve the quality, safety, and efficiency of healthcare by expanding the adoption of health information technology.

HITECH Audit

Coverage :

- ❑ Documentation
- ❑ Policies and Procedures
- ❑ Agreements of Business Associates
- ❑ Training and Awareness
- ❑ Data Security and Management

Data Protection, Identity theft & IS Controls

- **Personal Identifying information includes:**

✓ Name,

✓ Phone Number, Email-ID,

✓ Date of birth, Address,

✓ Identity card number, Permanent account number,

✓ Aadhaar card number,

✓ Voter ID,

✓ Credit/Debit card details,

✓ Medicare Number,

✓ Passport details, Travel details,

✓ Iris scan, Fingerprints, Voice sample etc.

- *"identity theft is using another person's personal identifying information like name address etc., as well as financial information like credit/debit card details in order to make purchases or borrow money, open a new account or commit a crime without that person's permission"*

Part 1.Broadband

- *Broadband refers to high-speed network connection*
- *Traditional Internet services are accessed in "**dial-on-demand**" mode,*
- *broadband Internet is an "**always-on**" connection, therefore security risk is very high*
- **Types of modem in Broadband**

✓ Wireless Fidelity (Wi-Fi)

✓ • Digital Subscriber Line (DSL)

✓ Asynchronous Digital Subscriber Line (ADSL)

✓ Very high speed Digital Subscriber Line (VDSL)

✓ • Cable Modem

✓ • Satellite

✓ • Terminal Adapter Modem

✓ • Universal Serial Bus (USB)

Broadband security threats

- As broadband Internet connection is “Always On” , Threats :
- Trojans and backdoors
- Denial of Service
- Intermediary for another attack
- Hidden file extensions
- Chat clients
- Packet sniffing
- Default configurations are extremely vulnerable

Part 2. Smartphone - Checklist

- **STEP 1** : Read manufacturer's manual carefully & follow guidelines as specified to setup mobile phone.
- **STEP 2** : Record IMEI (International Mobile Equipment Identity) number for tracking mobile in case of loss.

- **Mobile Phone Security Threats Categories**
- **A. Mobile Device and Data Security Threats**
- Threats related to unauthorised or intentional physical access to mobile phone and Lost or Stolen mobile phones.
- **B. Mobile Connectivity Security Threats**
- Threats related to mobile phone connectivity to unknown systems, phones and networks using technologies like Bluetooth, WiFi, USB etc.
- **C. Mobile Application and Operating System Security Threats**
- Threats arising from vulnerabilities in Mobile Applications and Operating Systems .

Impact of Cyber attacks on smart Phones

1. • **Exposure or Loss of user's personal Information/Data**, stored/transmitted through mobile phone.
2. • **Monetary Loss** due to malicious software unknowingly utilizing premium and highly priced SMS and Call Services.
3. • **Privacy attacks** which includes tracing of **mobile phone location** along with **private SMSs and calls without** user's knowledge.
4. • **Losing control over mobile phone -** unknowingly becoming zombie for targeted attacks

2) Wi-Fi

- Wi-Fi = “Wireless Fidelity.”
- Wi-Fi : wireless networking technology that allows computers & devices to communicate over wireless signal.
- Connect only to **the trusted networks.**
- Use Wi-Fi **only when required.**
- Beware **while connecting to public networks**, as they may not be secure- Eg Airport , stations etc

Mobile as USB:

- Mobile phones can be used as USB memory devices when connected to computer. A USB cable is provided with the mobile phone to connect to computer.
- Mobile's phone memory and memory stick can be accessed as USB devices.
- ***Best practices :***
- When a mobile phone is connected to PC , **scan external phone memory and memory card using an updated anti virus.**
- Take regular **backup of your phone & external memory card** because if an event like a system crash or malware penetration occurs, at least your data is safe.
- Before transferring the data to Mobile from PC , **data to be scanned with latest Antivirus with all updates.**
- ***Risks:***
- Never keep **sensitive information like user names/passwords** on mobile phones.
- Never forward the **virus affected data to other Mobiles.**

1. UC Browser

- Developed by UCWeb, a subsidiary of Chinese tech giant, Alibaba, UC browser is one of the most downloaded in Android platform.
- may not adequately protect its data transmissions, which can leave personal data at risk of being intercepted by hackers
- Browser uses weak cryptography, sometimes no encryption at all, when it transmits keystrokes over the web.

2. **CLEANit**

- CLEANit claims to be junk file cleaner
- millions of downloads on Play Store.
- The app not only needs no of permissions,
- Also advertises services

3. **Virus Cleaner – Antivirus Free & Phone Cleaner**

- App with 14 million installs, Virus Cleaner – Antivirus Free and Phone Cleaner from Super Cleaner Studio
- promises - *“efficient security master, phone junk cleaner, WIFI security, super speed booster, battery saver, CPU cooler and notification cleaner”*
- **usually not possible by a single software**

4. Super VPN / Free VPN Client

- Criminals can also exploit vulnerabilities to hijack user's connection to malicious websites - endanger user privacy & security.
- potentially stealing personal info, including credit card details, photos & private chats

SIM Swapping

- **SIM Swapping** a.k.a SIM splitting, SIM jacking, SIM hijacking =taking over control of mobile operations from user's existing SIM to another SIM, in control of cyber fraudster.
- **Subscriber Identity Module (SIM)** = chip in mobile phone, which tells device which cellular network to connect to & which phone number to use.
- SIM, stores user data in Global System for Mobile (GSM) phones
- Without SIM card, GSM phone will not be authorized to use mobile network

SIM Cloning

- **SIM Cloning**
- creating a duplicate SIM from the original one.
- similar to SIM swapping.
- technically sophisticated technique, where software used to copy real SIM card.
- done to get access to victims International Mobile Subscriber Identity (IMSI) & encryption key, used to identify and authenticate subscribers on mobile telephony.
- Cloning SIM = enable fraudster to take control & track, monitor, listen to calls, make calls and send texts using mobile number.
- **IMSI**
- Mobile SIM card issued by Telecom Company has IMSI (International Mobile Subscriber Identity) number.
- IMSI number = 15 digit code that linked to that specific SIM, identifying & authenticating individual subscriber owning SIM card.
- Indicates : subscribers country, mobile network etc

Our identity is our responsibility

Thank You

Arijit Chakraborty