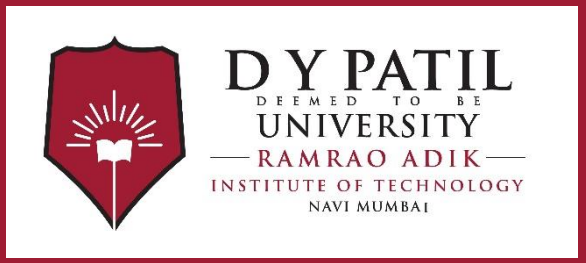


Information Security

Module: 5

•Faculty: Mrs. Bhavana Alte
• Mr. Prathmesh Gunjgur

Contents

Module 5:

Lecture 31: Data Privacy

Data Privacy

- Data privacy is a discipline intended to keep data safe against improper access, theft or loss. It's vital to keep data confidential and secure by exercising sound data management and preventing unauthorized access that might result in data loss, alteration or theft.

Importance of Data Privacy

- Business Asset Management: Data is perhaps the most important asset a business owns. We live in a data economy where companies find enormous value in collecting, sharing and using data about customers or users, especially from social media. Transparency in how businesses request consent to keep personal data, abide by their privacy policies, and manage the data that they've collected, is vital to building trust with customers who naturally expect privacy as a human right.
- Regulatory Compliance: Managing data to ensure regulatory compliance is arguably even more important. A business may have to meet legal responsibilities about how they collect, store, and process personal data, and non-compliance could lead to a huge fine. If the business becomes the victim to a hack or ransomware, the consequences in terms of lost revenue and lost customer trust could be even worse.

Data Privacy

Data privacy is generally composed of the following six elements:

- Legal framework. Prevailing legislation enacted and applied to data issues, such as data privacy laws.
- Policies. Established business rules and policies to protect employees and user data privacy.
- Practices. Best-practices put in place to guide IT infrastructure, data privacy and protection.
- Third-party associations. Any third-party organizations, such as cloud service providers, that interact with data.
- Data governance. Standards and practices used to store, secure, retain and access data.
- Global requirements. Any differences or variations of data privacy and compliance requirements among legal jurisdictions around the world such as the U.S. and European Union (EU).

Data Privacy Laws

- Children's Online Privacy Protection Act (COPPA) gives parents control over what information websites can collect from their kids.
- Health Insurance Portability and Accountability Act (HIPAA) ensures patient confidentiality for all healthcare-related data.
- Electronic Communications Privacy Act (ECPA) extends government restrictions on wire taps to include transmission of electronic data.
- Video Privacy Protection Act (VPPA) prevents the wrongful disclosure of an individual's PII stemming from their rental or purchase of audiovisual material.
- Gramm-Leach-Bliley Act (GLBA) mandates how financial institutions must deal with the individual's private information.
- Fair Credit Reporting Act (FCRA) regulates the collection and use of credit information.

Data Privacy Vs Data Security

Data privacy and data security are closely related ideas, but they aren't interchangeable.

- Data privacy focuses on issues related to collecting, storing and retaining data, as well as data transfers within applicable regulations and laws, such as GDPR and HIPAA.
- Data security is the protection of data against unauthorized access, loss or corruption throughout the data lifecycle. Data security can involve processes and practices, along with a variety of tools such as encryption, hashing and tokenization to guard data at rest and in motion.

Module 5:

Lecture 32: Digital Forensics

Digital Forensics

- Digital forensic science is a branch of forensic science that focuses on the recovery and investigation of material found in digital devices related to cybercrime. The term digital forensics was first used as a synonym for computer forensics.
- Digital forensics is the process of identifying, preserving, analyzing, and documenting digital evidence. This is done in order to present evidence in a court of law when required.

- “Digital forensics is the process of uncovering and interpreting electronic data. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying, and validating the digital information to reconstruct past events. The context is most often for the usage of data in a court of law, though digital forensics can be used in other instances.” - Techopedia

Digital Forensics

- Identifying the cause and possible intent of a cyberattack
- Safeguarding digital evidence used in the attack before it becomes obsolete
- Increasing security hygiene, retracing hacker steps, and finding hacker tools
- Searching for data access/exfiltration
- Identifying the duration of unauthorized access on the network
- Geolocating the logins and mapping them

Objectives of Digital Forensic

- To identify the evidences associated with a malicious activity.
- To recover and analysis the evidence and related materials from computers and other ECDs.
- To present the collected evidence in a court of law.
- To estimate the potential impact of the malicious activity.
- To estimate the potential impact of the malicious activity.
- To assess the intention and identity of the offender.

Rules of Digital Forensic

- Rule 1: An examination should never be performed on the original media.
- Rule 2: A copy is made onto forensically sterile media.New media should always be used if available.
- Rule 3: The copy of the evidence must be an exact, bit-by-bit copy (Sometimes referred to as a bit-stream copy).
- Rule4: The computer and the data on it must be protected during the acquisition of the media to ensure that the data is not modified (Use a write blocking device when possible).
- Rule 5: The examination must be conducted in such a way as to prevent any modification of the evidence.
- Rule 6: The chain of the custody of all evidence must be clearly maintained to provide an audit log of whom might have accessed the evidence and at what time.

Types of Digital Forensic

- Computer Forensics – the identification, preservation, collection, analysis and reporting on evidence found on computers, laptops, and storage media in support of investigations and legal proceedings.

- Network Forensics – the monitoring, capture, storing, and analysis of network activities or events in order to discover the source of security attacks, intrusions or other problem incidents, that is, worms, virus, or malware attacks, abnormal network traffic and security breaches.

- Mobile Devices Forensics – the recovery of electronic evidence from mobile phones, smart phones, SIM cards, PDAs, GPS devices, tablets, and game consoles. Mobile device forensics involves the recovery of digital evidence or data from mobile devices.

Types of Digital Forensic

- Digital Image Forensics – the extraction and analysis of digitally acquired photographic images to validate their authenticity by recovering the metadata of the image file to ascertain its history

- Digital Video/Audio Forensics – the collection, analysis, and evaluation of sound and video recordings. The science is the establishment of authenticity as to whether a recording is original and whether it has been tampered with, either maliciously or accidentally.

- Memory forensics – the recovery of evidence from the RAM of a running computer, also called live acquisition.

Role of Digital Forensic Investigator

- Protect victim's from any damage.
- Determines the extent of damage.
- Gather evidences in a forensically sound manner.
- Analyse the evidences data and protect those evidences.
- Prepare the analysis report.
- Prepare acceptable evidences in court.

General Ethics Norms for Investigator in Digital Forensic Field

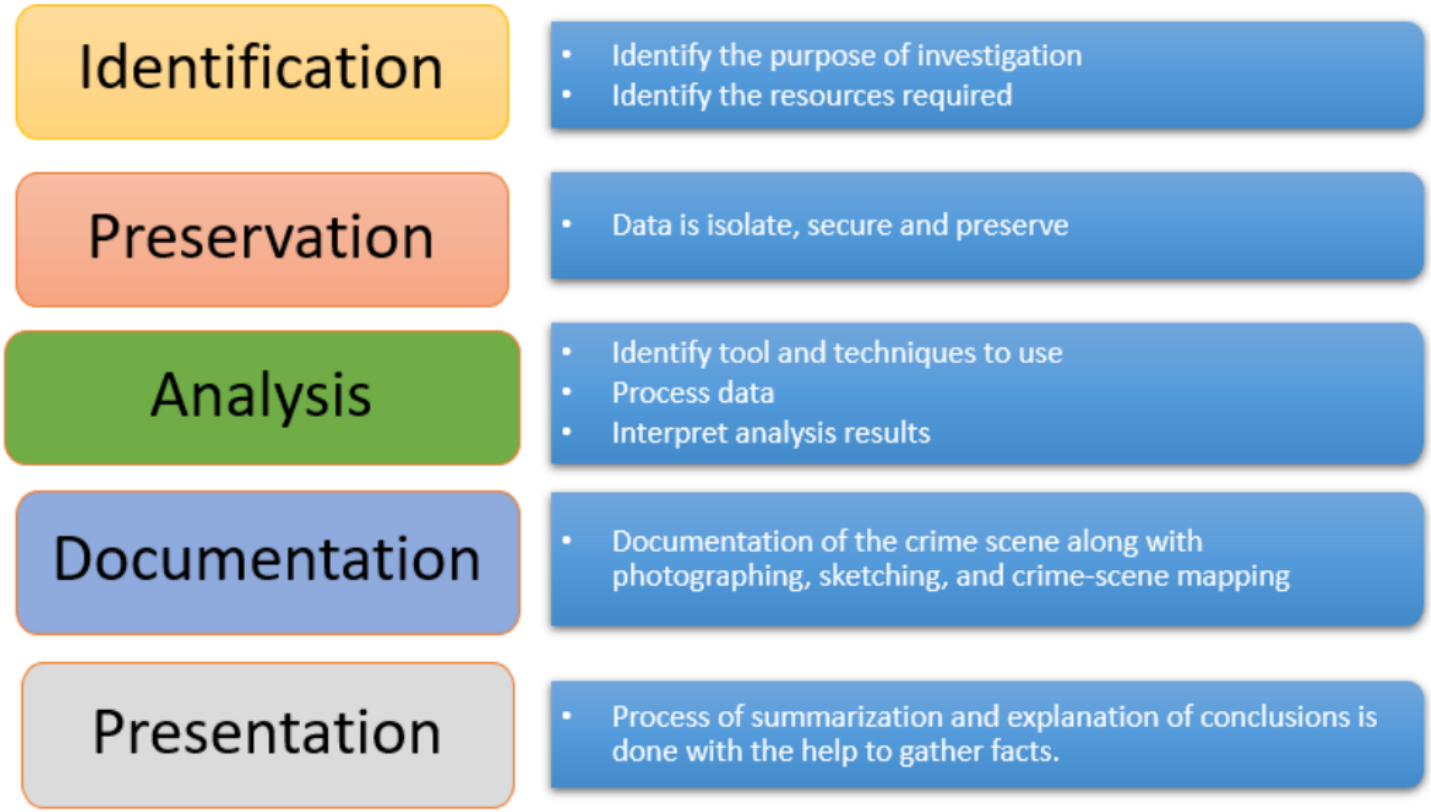
- Before starting the investigation in the digital forensic field, the investigator should satisfy the following points.
- Should contribute to the society and human being.
- Should avoid harm to others
- Should be honest and trustworthy.
- Should be fair and take action not to discriminate.
- Should honor property rights, including copyrights and patents.
- Should give proper credit to intellectual property.
- Should respect the privacy of others.
- Should honor confidentiality.

Unethical Norms for Digital Forensic Investigation

The investigator should not:

- Uphold any relevant evidence.
- Declare any confidential matters or knowledge learned in an investigation without an order from a court of competent jurisdiction or without the client's consent.
- Express an opinion on the guilt or innocence belonging to any party.
- Engage or involve in any kind of unethical or illegal conduct.
- Deliberately or knowingly undertake an assignment beyond his or her capability.
- Distort or falsify education, training or credentials.
- Display bias or prejudice in findings or observations.
- Exceed or outpace authorization in conducting examinations.

Digital Forensic Phases



Process of Digital Forensics

Module 5:

Lecture 33: Enterprise Security Specification

Enterprise Security

- Enterprise Security includes the strategies, techniques, and process of securing information and IT assets against unauthorized access and risks that may infringe the confidentiality, integrity or availability of these systems. Building on the traditional cybersecurity premise of protecting digital assets at the local front, enterprise security extends to the security of data in transit across the connected network, servers, and end-users.

Enterprise Security

Enterprise security architecture requirements for conceptual design include:

- Governance and policies – Robust and sustainable enterprise security architecture starts with managing the moving parts of IT infrastructure. Effective governance requires alignment between organization leadership, mission-specific objectives, and policies to support processes such as:
    - Compliance (regulatory or otherwise)
    - Threat and vulnerability management
    - Incident response protocols
- Operational risk management – Enterprise risks change frequently and require effective risk management to mitigate threats. Ongoing risk analysis helps identify and address any security gaps and vulnerabilities before materialization into threats.
- Information architecture – Any risks, gaps, or vulnerabilities that are not identified promptly can result in an attack. Implementing tools and processes to extract security information from critical systems, applications, or data improves enterprise security.

Enterprise Security

- Access controls – Without safeguards to access points, enterprises are at risk of malicious intrusion. Your organization needs access controls to secure sensitive data, applications, and systems from breach risks. Types of access controls include:
    - Passwords and passphrases
    - Personal Identification Numbers (PINs)
    - Access cards and cryptographic keys
    - Biometrics (e.g., facial scans, fingerprints)
    - Role-based access control (i.e., access by privilege)
- Incident response – Any threats or incidents must be addressed right away to minimize further damage and prevent any malicious intrusion. Examples of incident response are:
    - Threat detection and identification (e.g., monitoring and scanning tools)
    - Containment and eradication (e.g., isolation, escalation, malware removal)
    - System recovery to maintain business continuity
    - Learning and review to prepare for future incidents
    - System testing to ensure vulnerability and gap remediation

Enterprise Security

- Application security – The effectiveness of enterprise systems depends on application security, especially for the most commonly used applications, including but not limited to:
    - Web applications (e.g., browsers, eCommerce applications)
    - Email applications, web-based or on users' devices
    - Mobile applications (including on personal devices)

Enterprise Security

Physical enterprise security architecture requirements address risks to existing IT system components.

- Platforms – Enterprise security architecture must safeguard all assets used to host services or applications. Examples of platforms often at risk of threats include:
    - Computing platforms (e.g., cloud computing)
    - Integrations (e.g., Application Programming Interface (API))
    - Storage locations (e.g., shared cloud storage)
    - Media platforms (e.g., video streaming applications)
- Hardware – Any physical IT assets used to run systems, applications, or software must be protected from threat risks. Examples of hardware to incorporate in enterprise security architecture design include:
    - Physical servers and infrastructure
    - Workstations (shared and individual)
    - Computers (e.g., laptops, desktops)
    - Handheld devices (e.g., tablets, mobile devices)

Enterprise Security

- Networks – As one of the most frequently targeted assets, networks must be protected against threats. Specifically, enterprise security architecture design should address network security risks, the most common of which include:
    - Viruses spread via networked devices
    - Malware spread via email or web applications
    - Phishing launched via email, text, or phone calls
    - Rootkits, which use keyloggers to steal sensitive information
    - SQL injection, which use malicious code to steal sensitive data
- Operating systems – Your hardware and software run on operating systems (OS), which, if compromised, can affect business continuity–determining risks to enterprise operating systems is critical. The most common operating systems include:
    - Windows
    - macOS
    - Linux

Enterprise Security

- File storage – Regardless of your preferred file storage system, you should ensure that your enterprise security architecture contains robust access controls to protect:
    - Any files containing sensitive information
    - Digital file storage (i.e., on-site or cloud servers)
    - Hard copy storage (i.e., papers, filing cabinets)
- Databases – Enterprise security for databases should incorporate similar controls like those of file storage, except the safeguards should address the vast amounts of data collected over long periods, typically months or years. Essential components of databases include:
    - Sensitive data contained within databases
    - Database management system
    - Physical servers and access controls (for on-site databases)
    - Cloud servers and hosting networks (for cloud storage)
    - IT infrastructure used to support, manage, or run databases

operational processes for robust enterprise security architecture include:

- Implementation – When an enterprise creates a security policy to address threat risks, processes must be implemented to ensure cybersecurity. Considerations for implementing IT security include:
    - Designating roles and responsibilities to address specific tasks.
    - Compliance checklists to ensure adherence to regulatory frameworks
    - Periodic review of security goals, whether annually, bi-annually, or quarterly
- Administration – It is critical to establish administrative processes to help your personnel implement security controls. Administration helps simplify cumbersome processes in enterprise security architecture by:
    - Providing direction for new personnel (e.g., phishing training support)
    - Assisting personnel with troubleshooting controls (e.g., email access support)
    - Establishing processes for personnel to relay feedback on security processes

Enterprise Security

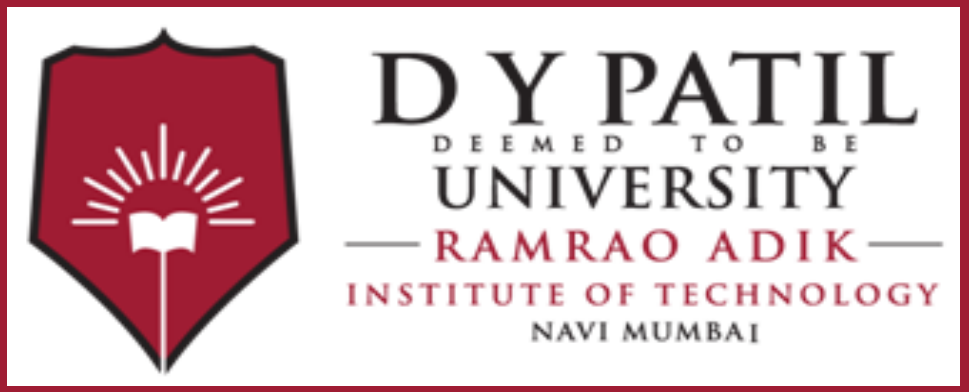
- Patch management – It is essential to deploy patches timely to mitigate any threats to IT security components, such as critical software. Designing enterprise security architecture for patch management must incorporate the following processes:
    - Identification of IT assets in need of security patches
    - Sorting assets based on level of vulnerability risk
    - Testing the stability of patches before deployment
    - Monitoring deployed patches to identify any issues
    - Backing up data and testing processes used for data backups
    - Deploying patches, either manually or automatically
    - Tracking the performance of patches following deployment
- Logging – Operational security design must also include processes for tracking security events or threats, which can help:
    - Provide insight into future threat attack vectors
    - Guide threat identification by eliminating false positives
    - Increase accuracy of machine learning-dependent threat detection

Enterprise Security

- Monitoring – Enterprise security architecture should include processes for monitoring systems, applications, and sensitive data environments for cybersecurity risks, including:
    - Sudden changes to IT environments (e.g., sensitive data storage)
    - Unusual network traffic, a common sign of malware threats
    - Higher than typical external data downloads or uploads
    - Unauthorized changes to access controls (e.g., the sudden elevation of privilege for user accounts)
    - User access events at odd times of day (e.g., late-night)
- Access management – As your enterprise grows, you could face multiple malicious actors attempting to gain unauthorized access to digital assets. Critical processes for access management, best implemented via an Identity and Access Management (IAM) system, include:
    - Authentication to verify the identity of users attempting to gain access to IT infrastructure
    - Authorization to provide access to authenticated users

Enterprise Security

- Penetration testing – One of the most effective methods for testing system, application, or data security is pen testing, also called “ethical hacking.” When added to enterprise security architecture operational design, pen-testing will help:
    - Identify vulnerabilities and gaps in security systems
    - Test new security processes (e.g., patches)
    - Comply with regulatory frameworks (e.g., PCI DSS, HIPAA)
- Change management – Many enterprises do not manage changes to their infrastructure, leaving room for security risks and vulnerabilities. Essential processes for change management include:
    - Scheduling changes to critical infrastructure to minimize risks to business continuity
    - Testing infrastructure changes before deployment (e.g., pen testing)
    - Monitoring changes to critical processes (e.g., tracking firewall performance)
    - Reviewing risks to any planned changes


D Y PATIL
DEEMED TO BE
UNIVERSITY
RAMRAO ADIK
INSTITUTE OF TECHNOLOGY
NAVI MUMBAI

Thank You