Dr. Ambedkar Memorial Institute of Information Technology & Management Science

LECTURE NOTES

ON

MCPE2022 MCA 4TH SEM

CYBER SECURITY & CYBER LAWS

Prepared By

Prof. Pujarani Nanda

Module I

Cyber Security Fundamentals:

Network and security concepts

Network security refers to the practices, policies, and hardware/software technologies designed to protect the integrity, confidentiality, and accessibility of computer networks and data. Managed primarily through multiple layers of defense, it prevents unauthorized access, malware propagation, and systemic cyberattacks.

Network Security is the measures taken by any enterprise or organization to secure its computer network and data using both hardware and software systems. This aims at securing the confidentiality and accessibility of the data and network. Every company or organization that handles a large amount of data, has a degree of solutions against many cyber threats.

Advantages of Network Security

- Network security provides protection against external threats like malware and hackers.
- It can improve the performance and reliability of a network by preventing bottlenecks and ensuring that resources are allocated appropriately.
- Network security measures can help organizations meet regulatory compliance requirements.

Disadvantages of Network Security

- Network security can be expensive to implement and maintain.
- It can be complex to configure and manage, requiring specialized knowledge and skills.
- Network security measures can sometimes slow down network performance or cause compatibility issues with other applications.

The CIA Triad: Core Objectives

The effectiveness of any network security framework is anchored on three pillars:

- **Confidentiality**: Assures that data remains hidden from unauthorized users via tools like encryption and multi-factor authentication (MFA).
- **Integrity**: Prevents unauthorized modifications, ensuring data remains accurate and trustworthy through cryptographic hashing and digital signatures.
- **Availability**: Guarantees dependable, uninterrupted access to network services for authorized users by mitigating downtime and DDoS attacks

Types of Network Attacks

Security administrators continually design defenses against two broad categories of threats:

- **Passive Attacks**: Intercepting or monitoring data traffic without altering its contents, such as port scanning or traffic sniffing.
- **Active Attacks**: Maliciously altering data payloads or disrupting data flows, such as data injection, malware transmission, and Denial of Service (DoS).

Information Assurance fundamentals

Information Assurance (IA) is the strategic practice of managing risks related to the use, processing, storage, and transmission of information and information systems. While closely related to information security, IA focuses more broadly on governance, organizational risk management, compliance, and data utility for business continuity.

The 5 Pillars of Information Assurance

At the core of IA are five fundamental principles designed to ensure comprehensive business and system level protection:

- **Confidentiality**: Restricting system access so data is seen only by authorized entities. For instance, implementing Role-Based Access Control (RBAC) ensures sensitive financial files remain hidden from staff outside the accounting department.
- **Integrity**: Guaranteeing that information remains accurate, complete, and un-tampered with across its entire lifecycle. Systems typically verify data integrity through cryptographic mechanisms like hashing.
- **Availability**: Providing reliable and constant access to data and resources for authorized users exactly when needed. Systems counter downtime by utilizing redundant server infrastructures and automated failovers.
- **Authentication**: Validating and proving the true identity of a user, device, or system trying to access data. Multi-Factor Authentication (MFA) is a standard modern practice used to achieve this verification.
- **Non-Repudiation**: Ensuring that a sender or receiver cannot deny having processed or transmitted specific data. Digital signatures and transactional logging create an indisputable audit trail to establish complete accountability.

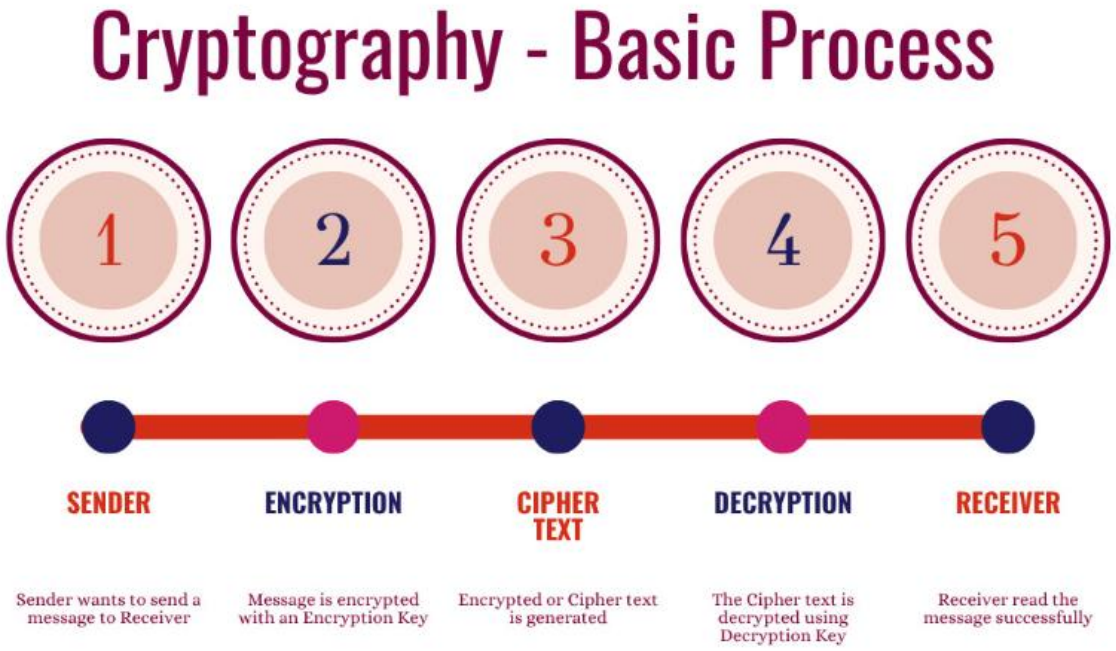
The 3 Information States

To protect information properly, IA frameworks monitor and apply policies across data in three distinct environments:

1. **Data at Rest**: Information stored securely on a physical medium, such as a database server or an encrypted hard drive.
2. **Data in Transit**: Information actively migrating through a public or private network, such as an email delivery or API traffic.
3. **Data in Process**: Active data sitting inside volatile memory (RAM) or being computed by a central processing unit (CPU).

Basic cryptography

Cryptography is the practice and study of techniques used to secure communication and data protection in the presence of adversaries. It uses mathematical concepts and algorithms to transform readable information into an unreadable format, ensuring that only the intended recipient can access and understand it.



The Four Pillars of Cryptography

1. **Confidentiality**: Ensuring that only authorized individuals can access and read the data.
2. **Integrity**: Verifying that the data has not been modified or tampered with during transmission.
3. **Authentication**: Confirming the identities of both the sender and the receiver.
4. **Non-repudiation**: Preventing a sender from denying that they sent a specific message.

Symmetric and Asymmetric encryption

The primary difference between symmetric and asymmetric encryption lies in the number of keys used: symmetric encryption uses a single, shared key to both encrypt and decrypt data, whereas asymmetric encryption uses a mathematically linked pair of keys—a public key for encryption and a private key for decryption.

Symmetric Encryption

Symmetric encryption acts like a physical safe with a single key. Anyone who needs to lock or unlock the safe must possess the exact same key.

Core Challenge: The "Key Distribution Problem". Sharing the secret key safely across an insecure network without it being intercepted is highly complex.
Primary Use Cases: Used extensively for protecting bulk data storage, local hard drive encryption, database security, and cloud file archives

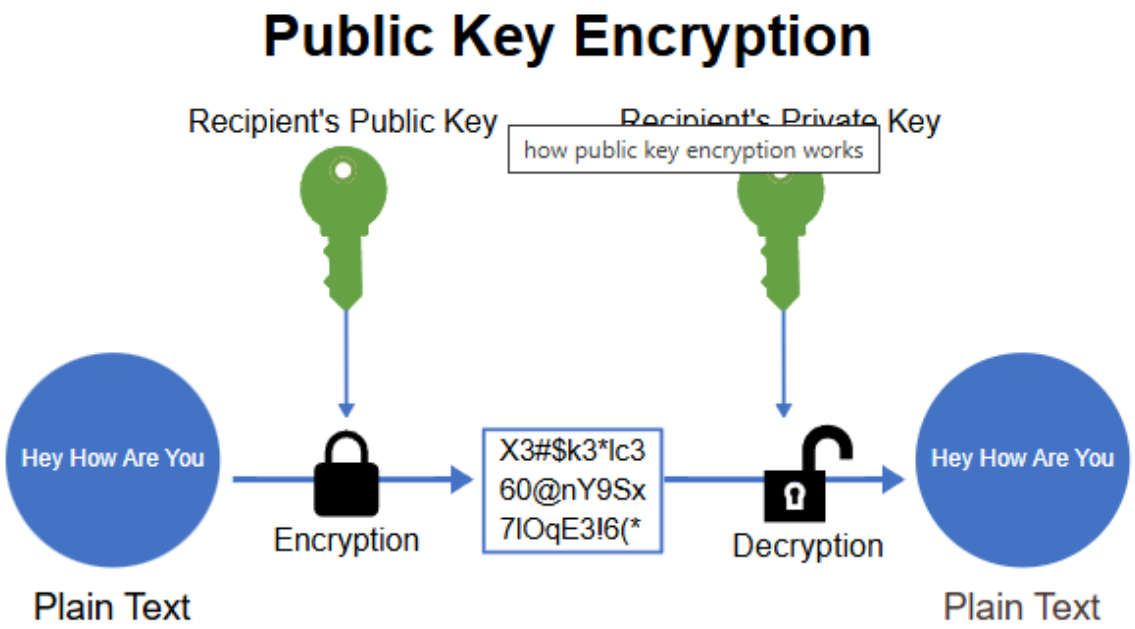
Asymmetric Encryption

Also known as public-key cryptography, asymmetric encryption provides every user with a unique pair of keys:

1. **Public Key**: Shared openly with anyone who wants to send you encrypted messages.
2. **Private Key**: Kept entirely secret and used only by you to decrypt those incoming messages

Public key encryption

Public key encryption, also known as asymmetric cryptography, is a security method that uses a mathematically linked pair of keys—a public key to encrypt data and a private key to decrypt it. This system eliminates the need to securely share a single password or key before communicating, serving as a core foundation for modern internet security.



Public Key: This key is distributed openly to anyone. It functions like a mailbox slot where anybody can drop a letter in, but they cannot look inside.
Private Key: This key is kept completely secret by the owner. It functions like the physical key to the mailbox, allowing only the owner to read the dropped messages.
Mathematical Bond: The keys are built on complex mathematical problems, like factoring massive prime numbers. It is computationally impossible to guess the private key using only the public key.

Domain Name System (DNS)

The Domain Name System (DNS) is the phonebook of the Internet. It translates human-readable domain names (like google.com) into machine-readable IP addresses (like 142.250.190.46) so browsers can load internet resources.

Common DNS Record Types

DNS servers use specific text records to direct traffic and manage services:

- **A Record**: Maps a domain directly to an IPv4 address.
- **AAAA Record**: Maps a domain directly to an IPv6 address.

- **CNAME Record**: Forwards one domain name to another domain name (an alias).
- **MX Record**: Directs email traffic to the domain's email server.
- **TXT Record**: Holds text information for security checks like SPF or domain ownership verification.

DNS Caching

To speed up the internet, DNS responses are temporarily saved closer to the user.

- **Browser Caching**: Your web browser saves recently visited IP addresses.
- **OS Caching**: Your computer's operating system checks its local cache before sending a request to the internet.
- **Router Caching**: Your home router maintains its own DNS memory to serve local devices quickly.

Firewalls

A firewall is a network security device or software that monitors, filters, and controls incoming and outgoing network traffic. Acting as a barrier between a trusted internal network and an untrusted external network (like the internet), it blocks malicious threats and unauthorized access based on predetermined security rules.

Types of Firewalls

- **Hardware Firewalls:** Physical devices installed between your network and the internet gateway (like your office router).
- **Software Firewalls:** Programs installed on individual devices (like Windows Defender or macOS firewall) to inspect local data.
- **Cloud Firewalls:** Hosted in the cloud (FWaaS), offering scalable, perimeter-less protection often used for remote workers and distributed cloud environments

Firewalls act like a security guard checking IDs. They examine data packets and decide to allow, block, or drop them based on specific rules:

- **Packet Filtering:** Inspects packets individually against a set of rules (IP, port, protocol).
- **Stateful Inspection:** Remembers the state of active connections and makes decisions based on the context of the traffic.
- **Proxy Service:** Filters traffic at the application level to shield the actual network from direct connections

Virtualization, and Radio-Frequency Identification (RFID)

Radio-Frequency Identification (RFID) uses electromagnetic radio waves to wirelessly track and identify tagged objects, animals, or people. It serves as an advanced alternative to traditional barcodes by eliminating the need for line-of-sight and allowing multiple items to be scanned simultaneously from a distance.

Every standard RFID system is comprised of three core elements:

- **RFID Tags (Transponders):** Consist of a microchip that stores data and an antenna. They come in three forms:

- **Passive:** Do not have an internal battery; they harvest energy from the reader's radio waves to transmit data.
- **Active:** Contain their own power source (battery), allowing for a longer read range and larger memory.
- **Semi-Passive:** Utilize a battery to run the microchip's circuitry but rely on the reader to transmit the response.
- **RFID Readers (Interrogators):** Devices equipped with an antenna and transceiver that emit radio waves and receive signals back from the tags. They can be portable or mounted in fixed positions.
- **Antennas:** Facilitate the scanning functions by capturing the radio waves and translating them into usable data to be sent to a database.

Primary Applications

- **Supply Chain & Inventory Management:** Enables retailers to track stock at the item level from the warehouse to the sales floor, dramatically improving order accuracy.
- **Access Control:** Used in secure buildings, parking garages, and ski resorts.
- **Asset Tracking:** Healthcare facilities use RFID to locate expensive medical equipment instantly.
- **Transportation & Logistics:** Powers electronic toll systems (like FASTag) and baggage tracking in airports.

Module II

Threats and Vulnerabilities

Types of threats:

Malware (short for *malicious software*) is any program intentionally designed to harm, exploit, or gain unauthorized access to a computer, network, or device. Its primary goal is to steal sensitive data, spy on users, or extort money for financial gain.

Common Types of Malware

- **Ransomware:** Encrypts your files or locks your system, demanding payment (ransom) to restore access.
- **Trojans:** Disguise themselves as legitimate software or files to trick you into downloading and executing them.
- **Spyware:** Secretly monitors your activity (e.g., keystrokes or passwords) and sends the data to a remote attacker.
- **Adware:** Displays unwanted, intrusive pop-up advertisements and redirects your browser, often slowing down your device.
- **Worms:** Standalone programs that replicate themselves and spread across networks without needing you to click or open anything.

Phishing

Phishing is a social engineering cyberattack where scammers trick individuals into revealing sensitive information—such as passwords, credit card numbers, or bank details—or installing malware. Attackers masquerade as trusted entities (e.g., banks, tech companies, or personal contacts) via email, SMS, or social media to execute the fraud.

Common Types of Phishing

- **Email Phishing:** The most common form, often involving urgent alerts (e.g., "Account suspended") urging you to click a fake link.
- **Smishing & Vishing:** Phishing conducted via SMS/text messages or phone calls, respectively.
- **Spear Phishing:** Highly targeted attacks directed at specific individuals or employees within a company.
- **Clone Phishing:** Scammers copy a legitimate, previously delivered email and change the link or attachment to a malicious one.

Man-in-the-Middle attacks

A Man-in-the-Middle (MitM) attack is a cybersecurity breach where an attacker secretly intercepts, relays, or alters communications between two unsuspecting parties. The goal is to covertly harvest sensitive data—such as login credentials, credit card details, or personal messages—or to hijack sessions and impersonate one of the parties.

MitM attacks typically involve two main phases:

1. **Interception:** The attacker positions themselves between the user and the intended destination (e.g., a web application, server, or another user). This is often done by exploiting weaknesses in network protocols or using compromised routers.
2. **Decryption/Manipulation:** The attacker reads or modifies the traffic. If the connection lacks encryption, the data is visible instantly. If the connection is encrypted, they may use sophisticated techniques to bypass or trick the encryption protocols before sending the data on its way.

Common Attack Techniques

- **IP and ARP Spoofing:** Attackers link their own MAC address to a legitimate IP address on a local area network (LAN), causing traffic intended for a router or server to be routed through the attacker's machine first.
- **DNS Spoofing (Cache Poisoning):** Attackers manipulate DNS records to redirect users from a legitimate website URL to a malicious, fraudulent site that looks identical to the real one.
- **Rogue Access Points:** Threat actors set up fake, unsecured Wi-Fi networks in public spaces (e.g., airports or coffee shops) that mimic legitimate hotspots. When users connect, the attacker controls the gateway and sees all unencrypted traffic.
- **Session Hijacking:** Attackers steal a user's session token after the initial login, allowing them to impersonate the user and access the application without needing credentials.

Scareware

Scareware is a malicious social engineering tactic that uses fake, alarming warnings to trick you into thinking your device is infected. The goal is to panic you into downloading useless "antivirus" software, handing over credit card details, or granting hackers access to your personal information.

A common scareware definition is a cyberattack tactic that scares people into visiting spoofed or infected websites or downloading malicious software (**malware**). Scareware can come in the form of pop-up ads that appear on a user's computer or spread through spam email attacks.

A scareware attack is often launched through pop-ups that appear on a user's screen, warning them that their computer or files have been infected and then offering a solution. This social engineering tactic aims to scare people into paying for software that purportedly provides a quick fix to the "problem." However, rather than fix an issue, scareware actually contains malware programmed to steal the user's personal data from their device.

Scareware can also be distributed by spam email, through messages that trick people into buying worthless items or services. Hackers then use the details they successfully steal to widen their criminal enterprise that is mostly based on identity theft.

Scareware Ads And Pop-ups

So how is scareware used? Typically through pop-up ads from rogue security providers that may sound legitimate but are fake. For example, rogue scareware or fake software names to watch out for include Advanced Cleaner, System Defender, and Ultimate Cleaner.

Scareware ads, which pop up in front of open applications and browsers, aim to scare computer users into thinking they have a major problem with their device. The hacker uses pop-up warnings to tell them their computer has been infected with dangerous viruses that could cause it to malfunction or crash. Some scareware ads also purport to be scanning the user's device, then showing them hundreds of viruses that are supposedly present but are actually fake results. Typically, the more menacing or shocking an ad pop-up sounds, the more likely the claims being made are scareware.

Another key feature of scareware is urgency. Hackers attempt to convince users that the supposed device problem requires immediate action and then prompt them to install the program as quickly as possible. Therefore, always be careful with any ad that demands the user to act immediately. It is most likely scareware.

Even more concerningly, scareware ad pop-ups can be particularly difficult for users to remove from their device. Hackers want the fake software to linger on a user's screen, so they make the close button difficult to find and show even more fake warnings when the user manages to locate and click on it.

Distributed Denial-of-Service (DDoS) attacks

A Distributed Denial of Service (DDoS) attack floods a server, website, or network with malicious internet traffic. By overwhelming the target's resources with fake connection requests, the system crashes or slows to a crawl, denying access to legitimate users.

Attacks are generally classified by the specific layer of the network they target:

- **Volumetric Attacks:** The most common type. The goal is simple congestion; attackers saturate the available bandwidth to create a massive "traffic jam".
- **Protocol Attacks:** These target firewalls, load balancers, or the servers themselves by exhausting their processing capacity with malformed or incomplete connection requests (e.g., SYN floods).
- **Application-Layer Attacks:** The most sophisticated type. These target the web page itself, sending seemingly legitimate HTTP requests to exhaust memory or compute cycles, effectively crashing the server

Rootkits, and Click-fraud. Vulnerabilities-Shellcode

These three cyber security concepts form an interconnected attack chain: vulnerabilities are the entry point, shellcode is the exploit vehicle, and rootkits provide the stealthy, persistent control to execute malicious tasks like click-fraud.

1. Vulnerabilities

A vulnerability is a flaw, weakness, or misconfiguration in a system's software, hardware, or operating system code. If left unpatched, attackers can exploit these weaknesses to bypass security controls and execute unauthorized commands.

2. Shellcode

Shellcode is a small, lightweight payload, typically written in machine code (like assembly), used by attackers to capitalize on a vulnerability.

- **The Mechanism:** When an attacker exploits a flaw, they inject this custom shellcode into the application's memory.
- **The Goal:** The shellcode executes directly to perform a specific action, such as opening a remote command line, downloading larger malicious payloads (like Trojans), or escalating user privileges.

3. Rootkits

Once the shellcode has successfully dropped the main malware, a rootkit is often deployed to secure the attacker's foothold.

- **Stealth:** Rootkits are designed to conceal their presence and the presence of other malicious programs (like click-fraud bots) from the operating system, users, and antivirus software.
- **Persistence:** They achieve this by modifying core system processes, replacing system drivers, or even operating at the kernel level (before the main OS fully boots), allowing the attacker to maintain administrative, root-level control over the machine indefinitely.

4. Click-fraud

Click-fraud is the malicious outcome of such infections. It is a type of cyber-fraud where an infected computer (often working as part of a botnet) secretly and artificially interacts with online advertisements or links.

- **The Attack:** Hidden malware or rootkits running on the compromised machine generate automated, fake clicks on pay-per-click (PPC) ads.
- **The Motive:** This diverts advertising revenue into the pockets of the cybercriminals while draining the advertising budgets of legitimate businesses.

- **Essential Defenses**

- **Vulnerability Management:** Routinely patch operating systems and applications to eliminate the flaws that shellcode relies on.
- **Endpoint Detection and Response (EDR):** Utilize advanced, AI-powered endpoint security platforms to detect anomalous behaviors and rootkit manipulations hidden deep in the system.
- **Network Monitoring:** Monitor outbound network traffic for the abnormal, repeated spikes in connections required to execute click-fraud

  Buffer overflows, and SQL injection.

Both buffer overflows and SQL injection are critical security vulnerabilities caused by a failure to properly validate and sanitize user input. However, they target entirely different layers of the technology stack

1. Buffer Overflows

A buffer overflow occurs when an application receives more data than it is allocated to hold in its temporary memory space (the buffer).

- **The Mechanism:** The excess data "overflows" into adjacent memory space, overwriting and corrupting the data or executable code in those neighboring blocks.
- **The Impact:** It can cause the program to crash (causing a Denial of Service) or allow attackers to hijack the application's execution path, granting them full system control.
- **Where It Happens:** These are low-level flaws prevalent in memory-unsafe languages like C and C++.
- **Prevention:** Use memory-safe languages or functions that enforce boundary checks, and enable modern compiler protections like Address Space Layout Randomization (ASLR).

2. SQL Injection (SQLi)

SQL injection occurs when user-provided data is directly concatenated into a backend database query, turning ordinary input into executable code.

- **The Mechanism:** An attacker enters malicious SQL commands (e.g., ' OR 1=1 --) into web application input fields like login forms or search bars. The application unknowingly passes these commands to the database for execution.
- **The Impact:** This allows attackers to bypass authentication, steal sensitive data, modify/delete database entries, or deface the website.
- **Where It Happens:** This occurs in the application and database layers of web applications.
- **Prevention:** Never concatenate user input directly into SQL queries. Use **Parameterized Queries (Prepared Statements)** and Stored Procedures.

Defense and Mitigation Measures

Anti-virus scanners

Antivirus (AV) scanners are core cybersecurity tools designed to detect, quarantine, and eliminate malicious software (malware) such as viruses, worms, Trojans, and ransomware. They act as a digital shield, continuously monitoring devices and networks to safeguard your data from being compromised or damaged.

Types of Scans

Quick/Smart Scan: Targets only the most vulnerable areas of your system (e.g., temporary folders, system memory, registry keys) to detect active threats quickly.
Full System Scan: Thoroughly analyzes every file, folder, and drive connected to your device.

Custom/Scheduled Scan: Allows you to select specific directories or set a specific time (e.g., overnight) for automated scanning.

Static and dynamic analysis methods

Static and dynamic analysis are complementary evaluation methods used across software engineering, cybersecurity, and structural mechanics. Static analysis assesses systems without executing or disturbing them, whereas dynamic analysis evaluates systems during actual operation or runtime to capture behavioral and performance characteristics.

In software engineering and cybersecurity, these methods are used for debugging, testing, and malware analysis.

- **Static Analysis:** Examines source code, binaries, or documentation without executing the program.
  - **Techniques:** Code reviews, data flow analysis, and syntax checking.
  - **Use Cases:** Early vulnerability detection, checking compliance with coding standards, and identifying dead code.
  - **Tools:** Platforms like SonarQube identify code-level security and quality defects.

- **Dynamic Analysis:** Evaluates the application while it is running.
  - **Techniques:** Sandboxing, behavioral analysis, and memory inspection.
  - **Use Cases:** Detecting runtime errors, memory leaks, buffer overflows, and zero-day threats that static tools miss.
  - **Tools:** Instrumentation frameworks like Parasoft are used to combine runtime testing with code analysis.

Detecting and preventing obfuscation, and identifying run-time attacks

Detecting and preventing code obfuscation alongside identifying run-time attacks requires shifting from static, signature-based defenses to dynamic, behavior-first strategies. Modern security relies on behavioral baselines, sandboxing, and Runtime Application Self-Protection (RASP) to identify hidden payloads and block active exploits.

1. Detecting Obfuscation

Because obfuscation intentionally breaks static signatures, detection relies on recognizing structural and behavioral anomalies:

- **Entropy Analysis:** Packed or heavily encrypted code exhibits high randomness. Files or memory sections with unusually high entropy often indicate obfuscated payloads.
- **Command-Line Telemetry:** Monitoring tools like Sysmon or EDR capture suspicious command arguments, such as excessive Base64 encoding or unusual parent-child process chains (e.g., an office document spawning PowerShell).
- **Machine Learning:** ML algorithms evaluate binary structures and control flows to detect the subtle patterns typical of obfuscators like UPX.

2. Preventing Obfuscation

Prevention involves early detection within the development pipeline and controlling how programs execute on host systems:

- **Static Application Security Testing (SAST):** Integrate SAST into your CI/CD pipelines to scan source code for malicious packages and restricted execution paths before compiling.
- **Constrained Environments:** Limit what scripts (e.g., PowerShell) are permitted to run. Tools like Microsoft's Constrained Language Mode (CLM) prevent attackers from using advanced obfuscation techniques.
- **Hardened Infrastructure:** Prevent initial access and limit lateral movement by enforcing strict credential management and Zero Trust policies.

3. Identifying Run-Time Attacks

Run-time attacks (e.g., memory injection, fileless malware, or malicious tampering) evade disk-based scanners by operating only in volatile memory. They are identified using the following tools and methods:

- **Memory Forensics:** Examining process memory spaces helps find injected shellcode and hidden payloads executing invisibly on the host.
- **Extended Sandboxing:** Run suspicious files in Sandbox environments set for 30 minutes or more, which circumvents time-based evasion tactics used by advanced threats.
- **RASP (Runtime Application Self-Protection):** RASP embeds security directly into an application's runtime, allowing the software to continuously monitor its own execution, recognize tampering, and immediately block threats.
- **Anomaly Detection:** Utilize platforms to detect deviations from normal application behavior and unusual network traffic patterns.

Module III

Cyber Forensics:

Memory and network forensics for Windows and Linux internals

Memory and network forensics are critical in incident response, allowing analysts to extract volatile data—such as active network connections, injected code, and decrypted credentials—that traditional disk analysis misses.

While Windows forensics often focuses heavily on structured registry artifacts and NTFS metadata, investigating memory and network activity across both Windows and Linux requires a deep understanding of each operating system's kernel architecture.

Windows Internals & Forensics

- **Memory Management:** Windows utilizes a complex virtual memory model managed by structures like the EPROCESS (Executive Process) block for processes, ETHREAD for threads, and the Page Directory Base, which maps virtual addresses to physical RAM.
- **Network Artifacts:** In-memory network details can be extracted directly from RAM dumps using Volatility's connections or netscan plugins to trace active TCP/UDP endpoints.

Linux Internals & Forensics

- **Memory Management:** Linux memory is structured via the task_struct block, which resides in a doubly-linked list. Since the Linux kernel does not natively record process-specific DLLs in the same way Windows does (relying heavily on shared object .so files and dynamically linked execution), uncovering malicious processes requires traversing this structure.
- **Network Artifacts:** Network states in Linux are maintained by socket buffers (sk_buff). You can examine these by parsing ss or netstat commands, or directly from a memory dump using plugins like linux_netstat.
- **Acquisition Challenges:** Linux traditionally restricts /dev/mem access, making memory dumping harder. Investigators typically rely on specialized tools, such as **AVML** (Azure VM Memory Reader), **LiME** (Linux Memory Extractor), or **mquire** to bypass stale kernel debug requirements

OS hardening

Operating System (OS) hardening is the process of securing a computer's foundational software by minimizing its attack surface. This is achieved by patching vulnerabilities, removing unnecessary files and services, and enforcing strict access controls. It serves as a vital first layer of defense against cyberattacks.

Strategies & Techniques

1. **Patch Management:** Keeping the OS, drivers, and software updated with the latest security fixes is the most critical step to prevent exploitation of known bugs.

2. **Disable Unnecessary Services:** Uninstall or disable unused applications, background services, and legacy network protocols (e.g., stopping Telnet in favor of SSH).
3. **Principle of Least Privilege (PoLP):** Restrict user rights, ensure standard users don't have administrator access, and disable default root/administrator accounts where possible.
4. **Firewall & Network Configuration:** Configure host-based firewalls to block all inbound traffic except for explicitly allowed and necessary ports.
5. **File System Encryption:** Secure data at rest by enforcing full-disk encryption (e.g., BitLocker on Windows or LUKS on Linux).

RAM dump analysis

RAM dump analysis is the process of extracting and examining a snapshot of a computer's physical memory (RAM) to diagnose system crashes or uncover digital forensic artifacts like hidden processes, encryption keys, and network connections. It transforms volatile raw data into readable diagnostic insights.

The RAM dump process

- **Acquiring a RAM dump:** To perform a RAM dump, specialized tools or techniques are used to capture the contents of RAM. Common methods include physical access and utilizing software tools designed for memory acquisition. Physical access allows directly connecting to the computer's memory modules, while software tools can acquire RAM remotely or by creating a memory image from a hibernation file.

- **Preserving data integrity:** It is essential to ensure the integrity of the RAM dump during acquisition to maintain its evidentiary value. This involves utilizing write-blocking mechanisms, verifying the integrity of the acquired image, and documenting the entire process to establish a proper chain of custody.

- **Analyzing the RAM dump:** Once the RAM dump is acquired, it can be analyzed using specialized software tools designed for memory forensics. These tools enable investigators to extract information, identify running processes, recover artifacts, and search for patterns or indicators of compromise.

- **Extracting volatile data:** The RAM dump analysis involves extracting volatile data such as active network connections, running processes, loaded drivers, registry information, file handles, and other artifacts. This data can be used to reconstruct the system's state, identify malicious activities, or uncover hidden information.

- **Memory carving and artifacts recovery:** Memory carving techniques are employed to search for specific file types or artifacts within the RAM dump. This process involves identifying file headers or signatures and reconstructing files from the memory image. This can be particularly useful in recovering deleted or encrypted files.

Data acquisition and extraction

Data acquisition and extraction is the foundational first step in any data pipeline. It involves gathering raw, disparate information from various sources (such as sensors, web pages, or databases) and pulling it into a centralized system so it can be cleaned, transformed, and analyzed.

Data Extraction

Data extraction processes pull relevant information from files, websites, and documents for digital storage, analysis, and further processing. It extracts structured, unstructured, and semi-structured data from documents and converts them into a standardized format to integrate them easily into downstream applications for business operations.

Some real-life examples where data extraction is commonly employed:

1. **Banking and lending:** Banking professionals extract data from bank statements, payslips, cheques, mortgage documents, and identity proofs to streamline the account opening/closing and loan application processes
2. **Insurance:** Insurance agencies capture data from ACORD forms, submission emails, quotes, policies, and binders for accurate risk assessment, leading to precise claims processing and insurance underwriting

Benefits of Data Extraction

- **Improved accuracy:** Automated data extraction tools capture accurate data from documents using Optical Character Recognition (OCR), Artificial Intelligence (AI), and Machine Learning (ML) algorithms. Some advanced solutions, like Docsumo, validate the extracted data automatically to increase the accuracy rate to 99%+.
- **Quick turnaround time:** Automated data extraction allows businesses to process documents in batches so you can extract data in 30-60 seconds, allowing businesses to optimize business operations.
- **Security and Compliance:** Automated data capture ensures compliance with industry standards and regulations like SOC-2, HIPAA, and GDPR. Moreover, these tools provide features such as cloud storage and role-based access to enhance security.
- **Reduced operational costs:** By automating their end-to-end data processing workflows, businesses can reduce operational costs by 60-70%.

Data Acquisition

Data acquisition means analyzing raw data to derive actionable insights, identify trends and patterns, and detect fraud, anomalies, and security threats. This deep data analysis helps businesses make informed decisions and gain a competitive edge by predicting outcomes.

Data acquisition processes include data collection, cleaning and preparation, mining, and interpretation. They blend statistical methodologies and machine learning algorithms to research data and predict results.

Benefits of Data Acquisition

Here are some benefits that data acquisition offers to businesses:

- **Access to real-time data:** Data acquisition enables analyzing real-time data and helps optimize business operations faster. With real-time data, you can quickly predict alarming situations, develop reports, finalize control measures, and mitigate risks.
- **Fraud detection:** Organizations can detect fraudulent activities and identify patterns and anomalies, which helps prevent losses related to data breaches and thefts.

Automated malicious code analysis

Automated malicious code analysis systems in cybersecurity are tools designed to rapidly scan, evaluate, and classify suspected malware without human intervention. They scale threat detection by utilizing static properties and dynamic execution to neutralize zero-day threats and extract critical indicators of compromise (IoCs).

1. Static Analysis

Static analysis examines the code and file structure without executing it. It is exceptionally fast and focuses on finding known threats and evaluating the raw file for suspicious attributes.

- **Signature Matching:** Compares file hashes against databases of known malware.
- **Heuristic Analysis:** Looks for suspicious code patterns or abnormal file structures (e.g., unusual imports or modified headers).
- **Machine Learning:** Scans codebase across the entire Software Development Life Cycle (SDLC) to identify anomalous features.

2. Dynamic Analysis

Dynamic analysis runs the suspected code in a secure, isolated environment known as a **sandbox**. By observing the file in action, these systems can understand its actual capabilities and intent.

- **Behavioral Monitoring:** Tracks actions like registry changes, file modifications, and network connections.
- **API Hooking:** Intercepts calls to the operating system to see if the malware is attempting to inject code or hijack processes.
- **Network Trace Analysis:** Monitors outgoing traffic to identify connections to Command and Control (C2) servers.

Module IV

Cyber Laws and Legal Framework

Cybercrime and the global legal landscape

The global legal landscape for cybercrime is characterized by highly decentralized and borderless threats that continually outpace traditional national legislations. To combat these complex jurisdictional and enforcement challenges, international bodies are increasingly prioritizing cross-border cooperation and standardized frameworks.

International Treaties & Frameworks

- **Budapest Convention:** Established by the Council of Europe, this remains the most prominent international treaty on cybercrime. It harmonizes national laws, improves investigative techniques, and fosters cooperation among member states.
- **UN Cyber Convention:** The United Nations General Assembly adopted a landmark legally binding convention aimed at strengthening international cooperation for preventing, investigating, and prosecuting cyber offenses (such as fraud and child exploitation) across borders.
- **INTERPOL and Europol:** These international agencies facilitate real-time communication, data sharing, and joint task forces to track down transnational cybercriminal networks.

Local and Regional Context (India)

In India, the primary legislation governing cybercrime and digital offenses is the Information Technology Act, 2000 (IT Act). This legislation—along with relevant sections of the Indian Penal Code (IPC)/Bharatiya Nyaya Sanhita (BNS)—covers offenses such as hacking, data privacy breaches, and identity theft. India also actively engages in international treaties and bilateral agreements to share intelligence and streamline cross-border investigations.

IT Act 2000 and its amendments

The Information Technology (IT) Act, 2000 is India's primary legislation governing cybercrime, digital transactions, and cybersecurity. To keep pace with evolving digital threats, it was significantly amended in 2008 to expand the definition of cybercrimes, strengthen corporate data privacy obligations, and introduce vital national security and interception measures.

The IT Act outlines multiple offenses and powers to regulate and mitigate digital risks.

- **Section 43A (Data Protection):** Holds corporate bodies liable to pay compensation if they fail to implement reasonable security practices to protect sensitive personal data.
- **Section 66 (Cybercrimes):** Penalizes various cyber offenses, including unauthorized access, data theft, identity theft, malware/virus attacks, and cheating by personation.
- **Section 69 (Interception & Decryption):** Empowers the Central or State Governments to intercept, monitor, or decrypt any computer resource if deemed necessary for national security, public order, or investigating a cognizable offense.
- **Section 69A (Content Blocking):** Allows the government to block public access to websites or information in the interest of India's sovereignty, defense, or public order.

- **Section 69B (Traffic Monitoring):** Authorizes designated agencies to monitor and collect traffic data or information generated or transmitted through any computer resource for cybersecurity purposes.
- **Section 70B (CERT-In):** Established the Indian Computer Emergency Response Team (CERT-In) as the national nodal agency to coordinate responses to cybersecurity incidents, issue alerts, and forecast vulnerabilities.

Major Amendments and Rules

- **The IT Amendment Act, 2008:** Shifted the legislative focus by adding provisions for corporate data protection (Section 43A), enhancing punishments for cyber terrorism, and introducing emergency surveillance and blocking powers.
- **Intermediary Guidelines Rules (2021):** Replaced older guidelines, imposing strict due diligence and grievance redressal mechanisms on social media and digital platforms to maintain their safe harbour protection.
- **DPDP Act (2023):** Superseded the data privacy provisions of the IT Act, establishing a comprehensive, standalone framework for processing and protecting digital personal data across the country.

Cybercrimes and punishments

Major Cybercrimes and Their Penalties

- **Hacking & Unauthorized Access (Sec. 66 IT Act):** Modifying, destroying, or accessing a computer network without consent.
  - *Punishment:* Up to 3 years imprisonment, and/or a fine up to ₹5 lakh.
- **Identity Theft & Cheating by Personation (Sec. 66C & 66D IT Act):** Fraudulently using passwords, digital signatures, or deceiving someone for money.
  - *Punishment:* Up to 3 years imprisonment and a fine up to ₹1 lakh.
- **Publishing Obscene Content (Sec. 67 IT Act):** Transmitting sexually explicit content electronically.
  - *Punishment:* Up to 3 years imprisonment and a fine up to ₹5 lakh for the first conviction.
- **Child Sexual Abuse Material (CSAM) (Sec. 67B IT Act):** Publishing or transmitting material depicting children in sexually explicit acts.
  - *Punishment:* Up to 5 years imprisonment and a fine up to ₹10 lakh for the first offense.
- **Cyber Terrorism (Sec. 66F IT Act):** Threatening the unity, integrity, or security of India using electronic means.
  - *Punishment:* Imprisonment for life.
- **Cyber Stalking & Harassment (Sec. 354D IPC):** Unwanted digital tracking, monitoring, or repeatedly contacting an uninterested individual.
  - *Punishment:* Up to 3 years imprisonment (up to 5 years for subsequent offenses) and a fine

Legal and ethical aspects related to new technologies:

AI/ML

Artificial intelligence (AI) and machine learning (ML) are foundational to modern cybersecurity. They empower organizations to shift from reactive defense to proactive threat hunting by automating the detection, analysis, and containment of complex cyber threats at a scale that human analysts cannot achieve alone.

Machine Learning (ML): A subset of AI that uses algorithms and statistical models to parse vast datasets, recognize patterns, and identify subtle, abnormal attack signatures without needing explicit, pre-programmed rules.
Artificial Intelligence (AI): The broader concept of using software to simulate human logic and decision-making. AI takes the raw insights and patterns generated by ML and interprets them to recommend mitigation steps or automate incident response.

Internet of Things (IoT)

- **Legal Aspects:** Focuses on data breaches, consumer protection, and strict liability. Inadequately secured devices subject manufacturers to legal action for negligence. Legal frameworks like India's Information Technology Act, 2000 are adapting to penalize unauthorized access and data theft.
- **Ethical Aspects:** Revolves around consent and surveillance. IoT devices often collect sensitive, intimate data from households without clear, actionable user consent.
- **Case Study:** The *VTech Data Breach* (2015) involved a toy manufacturer whose internet-connected learning tablets were hacked, exposing the personal data and photos of millions of parents and children.

Blockchain and Cryptocurrencies

- **Legal Aspects:** Characterized by strict Anti-Money Laundering (AML) regulations and taxation frameworks. Because blockchain transactions are decentralized, establishing legal jurisdiction for disputes or financial fraud is inherently complex.
- **Ethical Aspects:** Centers on anonymity, the environmental impact of proof-of-work mining, and the risks of financial exploitation.
- **Case Study:** The collapse of the FTX Cryptocurrency Exchange in 2022 highlighted immense gaps in corporate governance, liquidity management, and international jurisdictional enforcement regarding digital assets, resulting in significant investor losses and fraud convictions.

The Darknet

- Legal Aspects: Involves combating the facilitation of illegal activities, including drug trafficking, arms sales, and child exploitation. The anonymity provided by onion routing inherently conflicts with law enforcement's investigative mandates, resulting in cross-border task force operations.

- Ethical Aspects: Debated as a dichotomy between preserving digital privacy/freedom of speech in oppressive regimes and preventing nefarious cybercrimes.
- Case Study: The Silk Road takedown (2013) by the FBI and global agencies demonstrated the limits of darknet anonymity. The site's operator, Ross Ulbricht, was convicted of multiple charges including money laundering and conspiracy to traffic narcotics, serving as a landmark case for digital forensics and server jurisdiction.

Social Media

- Legal Aspects: Governed by intermediary liability protections (e.g., Section 230 in the US), defamation laws, and data privacy regulations. Governments globally enforce compliance regarding content moderation and data localization.
- Ethical Aspects: Centers on misinformation, targeted political manipulation, algorithmic bias, and the psychological impacts of unchecked user engagement.
- Case Study: The Facebook-Cambridge Analytica Data Scandal (2018) involved the unauthorized harvesting of millions of users' personal data for political profiling. This forced a massive global reevaluation of platform accountability, resulting in multi-billion dollar fines (e.g., the US FTC settlement) and tighter enforcement of data privacy laws worldwide.

International Cyber Laws

Global legislative bodies have updated their frameworks to tackle emerging technologies:

- European Union: The General Data Protection Regulation (GDPR) enforces strict guidelines on how personal data—including IoT data and social media tracking—is collected and processed. Furthermore, the EU's Digital Services Act (DSA) mandates strict accountability for platforms regarding illegal content and disinformation.
- United States: State-level laws, such as the California Consumer Privacy Act (CCPA), establish baseline digital privacy and security parameters for modern technologies.
- India: The Digital Personal Data Protection Act (DPDPA), 2023 governs digital data processing, focusing on obtaining user consent and imposing significant financial penalties for corporate data breaches across connected networks and applications.