

Notes n Hindi

SUBJECT

INFORMATION SECURITY

PREPARED BY

TEAM NOTESINHINDI

Notesinhindi.com

2026 Edition

INFORMATION SECURITY

Unit 1: Basics of Information Security

Introduction to Information Security, Security Terminologies, Security Features of Operating Systems, aur Anti-Virus Software

Syllabus — Unit 1: Basics of Information Security

Unit	Topics and Sub-topics
Unit 1: Basics of Informa tion security	• Introduction to Information Security - Need of Security, Types of Security, Security Principles, CIA Triad (Confidentiality, Integrity and Authentication) • Security Terminologies: Threat, Vulnerability, Risk, Active Attacks, Passive Attacks • Security Features of Operating Systems – Authentication, Logs, Audit Features, File System Protection, User Privileges • Anti-Virus Software

Table of Contents

1. Introduction to Information Security

1. Need of Security
2. Types of Security
3. Security Principles
4. CIA Triad

2. Security Terminologies

1. Threat
2. Vulnerability
3. Risk
4. Active Attacks
5. Passive Attacks

3. Security Features of Operating Systems

1. Authentication
2. Logs
3. Audit Features
4. File System Protection
5. User Privileges

4. Anti-Virus Software

1. Introduction to Information Security

Information Security एक ऐसी practice है जिसमें digital information (data) को **unauthorized access, use, disclosure, modification, ya destruction** से बचाया जाता है। आसान भाषा में कहें तो, यह एक तरीका है जिससे हमारे important data, systems और networks को hackers, viruses aur अन्य खतरों से सुरक्षित रखा जाता है।

- आज के digital युग में data ही सबसे बड़ा asset है — बैंक details, personal information, company records — इन सबको protect करना बहुत ज़रूरी है, इसीलिए Information Security की ज़रूरत पड़ती है।
- Information Security सिर्फ computer viruses से बचाव तक सीमित नहीं है, बल्कि इसमें physical security, network security, aur policies/procedures भी शामिल होती हैं।

1.1 Need of Security

Need of Security का मतलब है यह समझना कि आखिर information security इतनी ज़रूरी क्यों है — बिना security के, डेटा aur systems को कई तरह के गंभीर नुकसान का सामना करना पड़ सकता है।

- **Data Protection** — Sensitive data (जैसे passwords, bank details, personal records) को unauthorized लोगों से बचाने के लिए security ज़रूरी है।
- **Cyber Attacks से बचाव** — Hacking, malware, phishing जैसे cyber attacks से systems aur networks को सुरक्षित रखने के लिए security ज़रूरी है।
- **Business Reputation बनाए रखना** — Data breach से company की reputation aur customer का trust खराब हो सकता है, security इसे बचाती है।
- **Legal Compliance** — कई कानून (जैसे data protection laws) organizations को अपने users का data सुरक्षित रखने के लिए बाध्य करते हैं।
- **Financial Losses से बचाव** — Data breach से बहुत बड़ा monetary नुकसान हो सकता है, जिसे अच्छी security practices रोक सकती हैं।

1.2 Types of Security

Information Security को उसके focus area के आधार पर कई types में divide किया जाता है, क्योंकि अलग-अलग तरह के assets को अलग-अलग तरीकों से सुरक्षित रखना पड़ता है।

- कोई भी एक security measure अकेले पूरी सुरक्षा नहीं दे सकता — इसीलिए organizations को अपने network, applications, devices, aur physical infrastructure — सभी को अलग-अलग तरीकों से सुरक्षित करना पड़ता है।
- यह अलग-अलग types अक्सर एक साथ, एक-दूसरे के complement के रूप में इस्तेमाल होती हैं, ताकि हर संभावित entry point (जहाँ से attacker घुस सकता है) सुरक्षित रहे।

Type	Description
Network Security	Network से गुज़रने वाले data aur traffic को unauthorized access से सुरक्षित रखना (जैसे firewalls, IDS/IPS का उपयोग)
Application Security	Software applications में मौजूद vulnerabilities को ठीक करके उन्हें attacks से सुरक्षित बनाना
Endpoint Security	Individual devices (laptops, mobiles, servers) को malware aur unauthorized access से सुरक्षित रखना
Cloud Security	Cloud पर store किए गए data aur applications को सुरक्षित रखना
Operational Security	Data को handle करने aur store करने से जुड़ी processes aur decisions को सुरक्षित बनाना
Physical Security	Hardware, servers aur equipment को physical नुकसान (जैसे चोरी, आग) से बचाना

Example: किसी bank में सिर्फ network security काफी नहीं है — अगर कोई चोर server room में physically घुसकर hard disk चुरा ले (physical security की कमी), तो network security का कोई फायदा नहीं होगा। इसीलिए सभी types साथ में लागू करनी पड़ती हैं।

1.3 Security Principles

Security Principles वे fundamental (बुनियादी) guidelines हैं, जिन्हें follow करके कोई भी system या organization एक मज़बूत security foundation बना सकती है।

- यह principles किसी specific tool या technology से जुड़े नहीं होते, बल्कि यह एक **सोचने का तरीका (design philosophy)** हैं, जो हर तरह के security decisions में लागू होते हैं।
- Security architects aur developers इन principles को system design करते समय शुरुआत से ही ध्यान में रखते हैं, ताकि बाद में security को अलग से "patch" न करना पड़े।

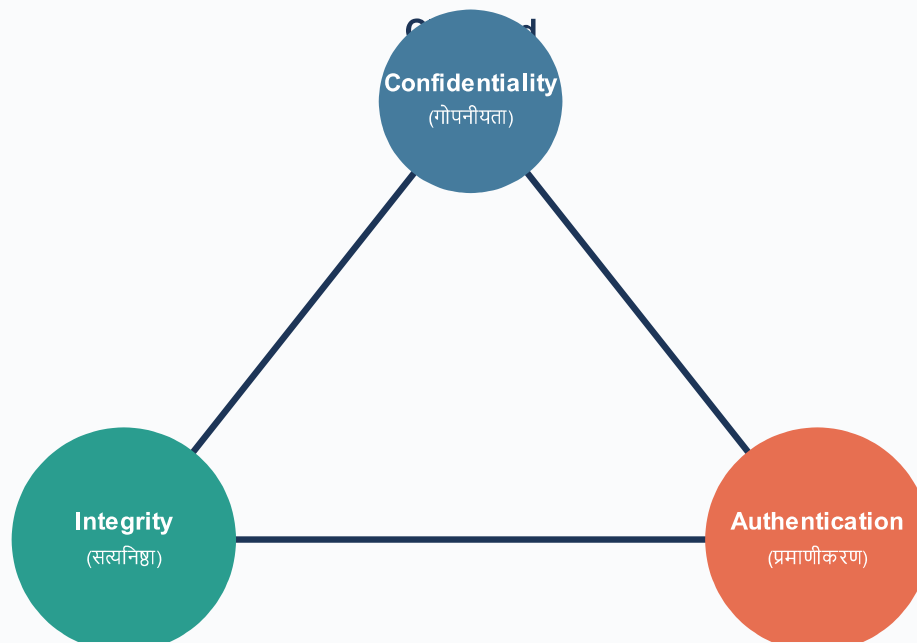
Principle	Description
Principle of Least Privilege	हर user या process को सिर्फ उतनी ही access दी जाए जितनी उसे अपना काम करने के लिए ज़रूरी है, न कम न ज़्यादा
Defense in Depth	Security की कई layers (जैसे firewall + antivirus + encryption) एक साथ इस्तेमाल करना, ताकि एक layer fail होने पर भी बाकी layers सुरक्षा दें
Separation of Duties	किसी critical काम को पूरा करने के लिए एक से ज़्यादा लोगों की ज़रूरत हो, ताकि कोई एक व्यक्ति अकेले misuse न कर सके

Fail-Safe Defaults	Default रूप से सब कुछ deny (मना) रहना चाहिए, aur सिर्फ specifically allowed चीज़ों को ही access मिलना चाहिए
Economy of Mechanism	Security design को जितना हो सके simple रखना चाहिए, ताकि उसे समझना, test करना, aur secure रखना आसान हो

Example: किसी bank locker को खोलने के लिए दो अलग employees की चाबियाँ चाहिए होती हैं (Separation of Duties), aur एक normal employee को सिर्फ अपने department के records दिखते हैं, पूरे bank के नहीं (Least Privilege) — यह दोनों principles साथ में असली दुनिया में लागू होते हैं।

1.4 CIA Triad (Confidentiality, Integrity, aur Authentication)

CIA Triad Information Security के तीन सबसे मूल (core) objectives को मिलाकर बनता है — **Confidentiality, Integrity, aur Authentication**। यह किसी भी security system को design करते समय foundation की तरह काम करता है।



चित्र 1.1 — CIA Triad के तीनों components मिलकर information को हर तरह से सुरक्षित बनाते हैं।

Confidentiality (गोपनीयता)

यह ensure करती है कि data सिर्फ **authorized लोग ही access** कर पाएँ, बाकी किसी को उसे देखने की permission न हो। इसे encryption, access control, aur passwords के through achieve किया जाता है।

Integrity (सत्यनिष्ठा)

यह ensure करती है कि data transmission या storage के दौरान बिना अनुमति के **बदला (modify) न जाए**। Hashing algorithms (जैसे SHA) का उपयोग करके यह check किया जाता है कि data में कोई छेड़छाड़ तो नहीं हुई।

Authentication (प्रमाणीकरण)

यह verify करती है कि कोई व्यक्ति या system वाकई वही है जो वह होने का दावा कर रहा है। Username-password, biometric, या OTP जैसे तरीकों से authentication किया जाता है।

Real-life Example: जब आप अपने bank के mobile app में login करते हैं, तो आपका password (Confidentiality के लिए) encrypt होता है, OTP verification (Authentication के लिए) होता है, aur आपकी transaction history बिना छेड़छाड़ के (Integrity के साथ) store होती है।

2. Security Terminologies

Information Security को अच्छे से समझने के लिए कुछ core terminologies (शब्दावली) को जानना ज़रूरी है — **Threat, Vulnerability, Risk, Active Attacks, aur Passive Attacks**। यह terms अक्सर आपस में जुड़ी होती हैं, इसलिए इन्हें एक साथ समझना बेहतर होता है।

Threat, Vulnerability, aur Risk का Relationship

Threat
(संभावित खतरा)

+

Vulnerability
(कमज़ोरी)

=

Risk
(नुक़सान की संभावना)

अगर कोई Threat exist करता है aur system में उससे related Vulnerability भी है, तभी Risk बनता है

चित्र 2.1 — Threat aur Vulnerability मिलकर Risk बनाते हैं। अगर Vulnerability न हो, तो Threat होने के बावजूद असल नुक़सान (Risk) कम हो जाता है।

2.1 Threat

Threat कोई भी ऐसी संभावित (potential) घटना, व्यक्ति, या चीज़ है जो किसी system, network, या data को नुक़सान पहुँचा सकती है। यह अभी हुआ नहीं है, लेकिन होने की संभावना है।

Type of Threat	Description
----------------	-------------

Natural Threats	प्राकृतिक आपदाएँ, जैसे भूकंप, बाढ़, जो data centers/hardware को नुकसान पहुँचा सकती हैं
Human Intentional Threats	Hackers या malicious insiders द्वारा जानबूझकर किए गए attacks
Human Unintentional Threats	Employees की गलतियों से होने वाला नुकसान, जैसे गलती से sensitive file delete करना
Environmental Threats	Power failure, hardware overheating जैसी technical/environmental समस्याएँ

(a) Natural Threats

यह वे threats हैं जो प्रकृति (nature) की वजह से पैदा होते हैं aur इंसानों के control में नहीं होते — जैसे भूकंप, बाढ़, आग, या तूफान। यह threats physical infrastructure (servers, buildings, cables) को सीधे नुकसान पहुँचा सकते हैं, इसीलिए organizations अक्सर अपने data centers को geographically अलग-अलग locations पर बनाती हैं, ताकि एक जगह आपदा आने पर भी data सुरक्षित रहे।

(b) Human Intentional Threats

यह वे threats हैं जो कोई व्यक्ति जानबूझकर, बुरे इरादे (malicious intent) से करता है — जैसे hackers, disgruntled (नाराज़) employees, या organized cyber-criminal groups। यह सबसे common aur खतरनाक category है, क्योंकि attacker सोच-समझकर, targeted तरीके से नुकसान पहुँचाने की कोशिश करता है, aur नए-नए तरीके भी ढूँढता रहता है।

(c) Human Unintentional Threats

यह threats किसी की जानबूझकर की गई गलती नहीं, बल्कि लापरवाही (carelessness) या गलती (mistake) से पैदा होते हैं — जैसे कोई employee गलती से important email किसी गलत व्यक्ति को भेज दे, या गलती से database की table delete कर दे। Awareness training से इस तरह के threats को काफी हद तक कम किया जा सकता है।

(d) Environmental Threats

यह technical/environmental कारणों से पैदा होने वाले threats हैं — जैसे power supply का अचानक चले जाना, hardware का ज़्यादा गर्म (overheat) हो जाना, या cooling system का fail हो जाना। इनसे बचने के लिए organizations backup power (UPS, generators) aur proper cooling systems में invest करती हैं।

Example: कोई hacker किसी company के network को hack करने की कोशिश करे, यह एक threat है — चाहे वह सफल हो या न हो।

2.2 Vulnerability

Vulnerability किसी system, software, या process में मौजूद वह कमज़ोरी (weakness) है, जिसका फायदा उठाकर कोई threat असल नुकसान पहुँचा सकता है।

Type of Vulnerability	Description
Software Vulnerability	Software में मौजूद bugs या coding errors, जैसे outdated software में patch न होना
Hardware Vulnerability	Physical devices में design flaws, जो attacker द्वारा exploit की जा सकती हैं

Network Vulnerability	Network configuration में कमियाँ, जैसे weak encryption या open ports
Human/Procedural Vulnerability	Weak passwords, security awareness की कमी, या गलत प्रक्रियाएँ (processes)

(a) Software Vulnerability

यह किसी software (operating system या application) के code में मौजूद bugs, coding errors, या design flaws होते हैं। जैसे अगर कोई software पुराना (outdated) है aur उसके ज्ञात (known) bugs को patch नहीं किया गया, तो attacker उन bugs को exploit करके unauthorized access पा सकता है। इसीलिए software को हमेशा updated रखना बहुत ज़रूरी होता है।

(b) Hardware Vulnerability

यह physical devices (जैसे routers, processors) के design में मौजूद कमज़ोरियाँ होती हैं। कभी-कभी hardware manufacturing के समय ही कोई design flaw रह जाता है, जिसे बाद में attackers discover करके उसका फायदा उठा सकते हैं — इन्हें ठीक करना software vulnerabilities से ज़्यादा मुश्किल होता है, क्योंकि इसके लिए hardware ही बदलना पड़ सकता है।

(c) Network Vulnerability

यह network की configuration में मौजूद कमियाँ होती हैं — जैसे weak/outdated encryption algorithms का इस्तेमाल, ज़रूरत से ज़्यादा open ports रखना, या firewall rules ठीक से set न करना। इस तरह की vulnerabilities से attacker network traffic को intercept कर सकता है या unauthorized तरीके से network में घुस सकता है।

(d) Human/Procedural Vulnerability

यह लोगों के व्यवहार या organization की processes में मौजूद कमज़ोरियाँ होती हैं — जैसे employees का weak passwords इस्तेमाल करना, security awareness की कमी, या गलत तरीके से लिखी गई security policies। चूंकि यह technology से नहीं

बल्कि इंसानों से जुड़ी होती हैं, इसलिए इन्हें ठीक करने के लिए training aur awareness programs की ज़रूरत पड़ती है।

Example: अगर कोई software update न किया गया हो aur उसमें कोई known bug हो, तो वह bug एक vulnerability है, जिसका फायदा attacker उठा सकता है।

2.3 Risk

Risk वह संभावना (probability) है कि कोई threat किसी vulnerability का फायदा उठाकर actual नुकसान पहुँचाएगा। आसान भाषा में, Risk एक तरह से Threat aur Vulnerability के मिलने से पैदा होता है — अगर दोनों में से एक भी ना हो, तो असल में कोई खतरा नहीं रहता।

- Risk को अक्सर तीन factors से मिलाकर समझा जाता है — **Threat की संभावना** (कितनी बार/कितनी आसानी से attack हो सकता है), **Vulnerability की गंभीरता** (कमज़ोरी कितनी बड़ी है), aur **संभावित नुकसान** (अगर attack सफल हो जाए तो कितना बड़ा असर पड़ेगा)।
- Risk को पूरी तरह खत्म करना लगभग असंभव है — इसीलिए organizations "risk को zero करना" नहीं, बल्कि "risk को acceptable level तक कम करना" लक्ष्य रखती हैं।

Risk Management Process

1. **Risk Identification** — यह पता लगाना कि किन-किन assets (data, systems) को कौन-कौन से threats और vulnerabilities से खतरा है।
2. **Risk Assessment** — हर identified risk की गंभीरता (severity) aur होने की संभावना (likelihood) को measure करना, ताकि पता चले कि कौन सा risk सबसे ज़्यादा गंभीर है।

3. **Risk Prioritization** — सभी risks को उनकी गंभीरता के according रैंक करना, ताकि सबसे बड़े risks पर पहले ध्यान दिया जा सके।
4. **Risk Mitigation** — या तो threat को कम करना (जैसे firewall लगाना), या vulnerability को patch/fix करना, ताकि risk कम हो जाए।
5. **Monitoring aur Review** — समय-समय पर यह check करते रहना कि नए threats/vulnerabilities तो नहीं आए, aur mitigation measures अभी भी effective हैं या नहीं।



Features

- Risk हमेशा Threat aur Vulnerability, दोनों की मौजूदगी पर निर्भर करता है — दोनों में से एक भी हटा दें तो risk काफी कम हो जाता है।
- अलग-अलग assets का risk level अलग-अलग होता है — जैसे किसी company का customer database, उसकी office की photocopy machine से कहीं ज़्यादा high-risk asset होता है।
- Risk को कभी भी पूरी तरह zero नहीं किया जा सकता, सिर्फ एक acceptable level तक कम किया जा सकता है (इसे **Residual Risk** कहा जाता है)।

Example: अगर किसी server में एक known vulnerability है (outdated software) aur hackers उसे target कर रहे हैं (threat), तो उस server के hack होने का risk बहुत ज़्यादा है। इस risk को कम करने के लिए company या तो software को update (patch) कर सकती है (vulnerability कम करना), या server को firewall के पीछे रखकर hackers की पहुँच सीमित कर सकती है (threat कम करना)।

2.4 Active Attacks

Active Attack वह attack है जिसमें attacker data या system को **directly modify, alter, या नुकसान** पहुँचाने की कोशिश करता है। इस attack के दौरान system की normal working प्रभावित होती है, इसलिए इसे detect करना अपेक्षाकृत आसान होता है।

Type	Description
Masquerade	Attacker खुद को कोई authorized user दिखाकर system access करने की कोशिश करता है
Replay	पहले भेजे गए valid data को capture करके, उसे बाद में दोबारा भेजकर unauthorized access पाने की कोशिश करना
Modification of Message	Data को transmission के दौरान बदल देना, ताकि receiver को गलत जानकारी मिले

Denial of Service (DoS)	System या server को इतने requests से भर देना कि वह normal users के लिए काम करना बंद कर दे
-------------------------	---

(a) Masquerade

इसमें attacker अपनी असली identity छिपाकर खुद को किसी authorized user या system की तरह पेश करता है, ताकि वह unauthorized access पा सके। यह attack अक्सर उस समय शुरू होता है जब attacker किसी तरह किसी legitimate user के credentials चुरा लेता है, aur फिर उन्हीं credentials का इस्तेमाल करके system में घुसता है, ताकि उसे असली user ही समझा जाए।

(b) Replay Attack

इसमें attacker network पर भेजे जा रहे किसी valid data packet (जैसे login request) को बीच में capture कर लेता है, aur उसे बाद में hu-b-hu दोबारा भेज देता है, ताकि वह भी authenticate हो जाए — भले ही attacker को असली password पता न हो। यह attack तब कारगर होता है जब system यह check नहीं करता कि request "नई" है या "पुरानी दोहराई गई"।

(c) Modification of Message

इसमें attacker किसी data को transmission के दौरान बीच में पकड़कर उसकी content को बदल देता है, aur फिर उसे modified रूप में आगे भेज देता है, जिससे receiver को गलत जानकारी मिलती है। यह attack data की Integrity (सत्यनिष्ठा) को सीधे नुकसान पहुँचाता है।

(d) Denial of Service (DoS)

इसमें attacker किसी server या network को इतनी बड़ी संख्या में fake requests भेज देता है कि वह उन्हें handle नहीं कर पाता, aur normal, genuine users के लिए काम करना बंद कर देता है। जब यह attack एक साथ कई अलग-अलग computers से किया जाता है, तो इसे **Distributed Denial of Service (DDoS)** कहा जाता है, जो aur भी ज्यादा शक्तिशाली होता है।

Example: DDoS attack में attacker किसी website के server को इतना traffic भेजता है कि वह crash हो जाता है — यह एक active attack है।

2.5 Passive Attacks

Passive Attack वह attack है जिसमें attacker सिर्फ data को **secretly observe** या **sniff** करता है, बिना उसे modify या नुकसान पहुँचाए। चूँकि data में कोई बदलाव नहीं होता, इसलिए इसे detect करना बहुत मुश्किल होता है।

Type	Description
Eavesdropping (Release of Message Content)	Attacker network से गुज़र रहे data को secretly पढ़ लेता है, जैसे कोई unencrypted email पढ़ना
Traffic Analysis	Attacker actual data पढ़े बिना ही network traffic के pattern (कब, कितना data, किसके बीच) को analyze करके जानकारी निकालता है

(a) Eavesdropping (Release of Message Content)

इसमें attacker network से गुज़र रहे data को बिना किसी को बताए secretly पढ़ लेता है — जैसे कोई unencrypted email या message को बीच में capture करके पढ़ना। अगर data encrypted न हो, तो attacker सीधे उसकी पूरी content पढ़ सकता है, जिसमें passwords aur अन्य sensitive information भी शामिल हो सकती है।

(b) Traffic Analysis

इसमें attacker actual data (content) को पढ़ नहीं पाता (शायद क्योंकि वह encrypted है), लेकिन फिर भी network traffic के **pattern** को analyze करके काफी कुछ जानकारी निकाल लेता है — जैसे कब, किसके बीच, कितनी मात्रा में

communication हो रहा है। इससे भी sensitive जानकारी (जैसे कोई important meeting हो रही है) अंदाज़ा लगाई जा सकती है, भले ही actual message का पता न हो।

Example: किसी public WiFi पर attacker packet sniffing tool से बिना किसी को पता चले, दूसरों का data पढ़ लेता है — यह एक passive attack है।

2.6 Active vs Passive Attacks — Comparison

Active vs Passive Attack

Active Attack

Data को modify करता है

Detect करना आसान

जैसे: DoS, Replay

Passive Attack

सिर्फ Observe करता है

Detect करना मुश्किल

जैसे: Eavesdropping

चित्र 2.2 — Active Attack data को बदलता है aur नुकसान पहुँचाता है, जबकि Passive Attack सिर्फ चुपचाप data चुराता/observe करता है।

Basis	Active Attack	Passive Attack
Data पर असर	Data को modify/damage करता है	Data को सिर्फ पढ़ता/observe करता है, बदलता नहीं
Detection	आसानी से detect हो जाता है (system का असामान्य व्यवहार)	Detect करना बहुत मुश्किल होता है
Focus	Prevention (रोकना) पर focus होता है	Detection (पहचानना) पर focus होता है

Examples	DoS, Replay, Masquerade	Eavesdropping, Traffic Analysis
----------	----------------------------	------------------------------------

3. Security Features of Operating Systems

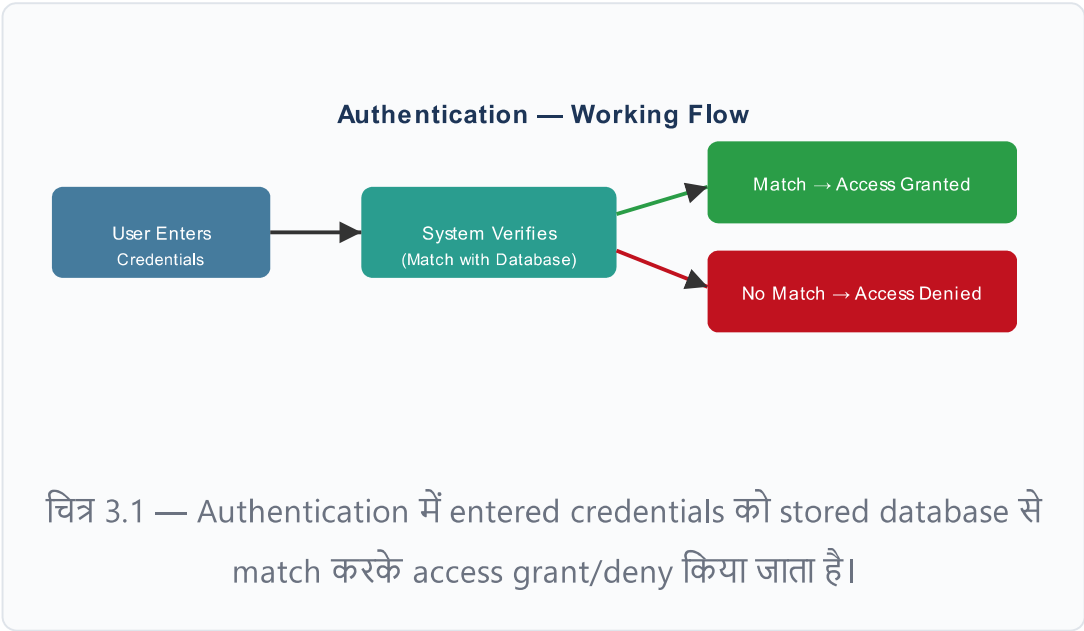
Operating System (OS) कंप्यूटर का वह core software है जो hardware aur user के बीच bridge का काम करता है, इसलिए इसकी security बहुत महत्वपूर्ण होती है। OS कई built-in security features देता है — Authentication, Logs, Audit Features, File System Protection, aur User Privileges।

3.1 Authentication

Operating System में **Authentication** वह security feature है जो यह verify करता है कि system को access करने वाला व्यक्ति वाकई वही है जो वह दावा कर रहा है, इसके बाद ही उसे login करने की अनुमति मिलती है।

Working / Steps

1. User अपना **identity claim** (जैसे username) enter करता है।
2. User एक **credential** (जैसे password, fingerprint, या OTP) provide करता है, जो यह prove करे कि वह वाकई वही व्यक्ति है।
3. System entered credential को अपने stored (encrypted) database की value से **match/verify** करता है।
4. अगर credential सही मिले, तो user को **access grant** कर दिया जाता है aur एक session शुरू होता है।
5. अगर credential गलत हो, तो access **deny** कर दिया जाता है, aur बार-बार गलत attempts होने पर account को temporarily lock भी किया जा सकता है।



Type	Description
Password-based Authentication	User एक secret password enter करता है जो पहले से system में set किया गया होता है
Biometric Authentication	Fingerprint, face recognition, या retina scan जैसी physical characteristics से identity verify की जाती है
Token-based Authentication	Smart card या security token के through authentication किया जाता है
Multi-Factor Authentication (MFA)	दो या ज़्यादा तरीकों (जैसे password + OTP) को मिलाकर authentication किया जाता है, जिससे security और मजबूत होती है

Features:

- Unauthorized users को system access करने से रोकता है।
- हर user का अलग account होता है, जिससे activities को track करना आसान हो जाता है।
- Failed login attempts को limit किया जा सकता है, ताकि brute-force attacks से बचा जा सके।
- Session timeout जैसे features अपने आप user को logout कर देते हैं, अगर वह लंबे समय तक inactive रहे।

Advantages

- System को unauthorized access से सुरक्षित रखता है।
- Multi-factor authentication से security और मजबूत होती है।

Disadvantages

- Password भूल जाने पर access में दिक्कत हो सकती है।
- Weak passwords use करने पर security कमजोर पड़ जाती है।

3.2 Logs

Logs वह records होते हैं जो operating system automatically generate करता है, जिनमें system में हुई सभी important activities (जैसे login, file access, errors) का detail होता है।

Working / Steps (Logs कैसे Generate होते हैं)

1. System में कोई **event** होता है (जैसे कोई user login करता है, या कोई file access होती है)।
2. OS का logging mechanism उस event को automatically **capture** कर लेता है।

3. Event की details (कौन, कब, क्या, किस result के साथ) को एक **timestamp** के साथ log file में **record/store** कर दिया जाता है।
4. यह logs एक centralized location (जैसे Windows में Event Viewer) में इकट्ठा होते रहते हैं, ताकि बाद में उन्हें review किया जा सके।

Type	Description
System Logs	OS की internal activities record करते हैं, जैसे startup, shutdown, hardware errors
Security Logs	Login attempts, authentication failures, aur access control से जुड़ी events record करते हैं
Application Logs	किसी specific software/application से related events record करते हैं

Features:

- Logs की मदद से यह पता चलता है कि system में कब, किसने, क्या किया।
- Security incident होने पर logs check करके पता लगाया जा सकता है कि क्या हुआ था।
- Logs troubleshooting में भी मदद करते हैं, जब system में कोई error आ रही हो।

Example: Windows का **Event Viewer** tool सभी system, security aur application logs दिखाता है, जिससे administrator यह track कर सकता है कि system में क्या-क्या हुआ।

3.3 Audit Features

Auditing एक ऐसी process है जिसमें system की activities को systematically review aur analyze किया जाता है, ताकि यह check किया जा सके कि सभी security policies सही से follow हो रही हैं या नहीं।

Process

1. सबसे पहले यह decide किया जाता है कि किन events को audit करना है (जैसे login attempts, file access)।
2. System उन events की logs collect करता रहता है।
3. Administrator या auditor उन logs को periodically review करता है।
4. अगर कोई suspicious activity मिलती है, तो उस पर आगे investigation की जाती है।

Features:

- यह पता लगाने में मदद करता है कि किसने, कब, कौन सा resource access किया।
- Compliance requirements को पूरा करने में मदद करता है।
- Unauthorized access attempts aur policy violations को पकड़ने में useful होता है।

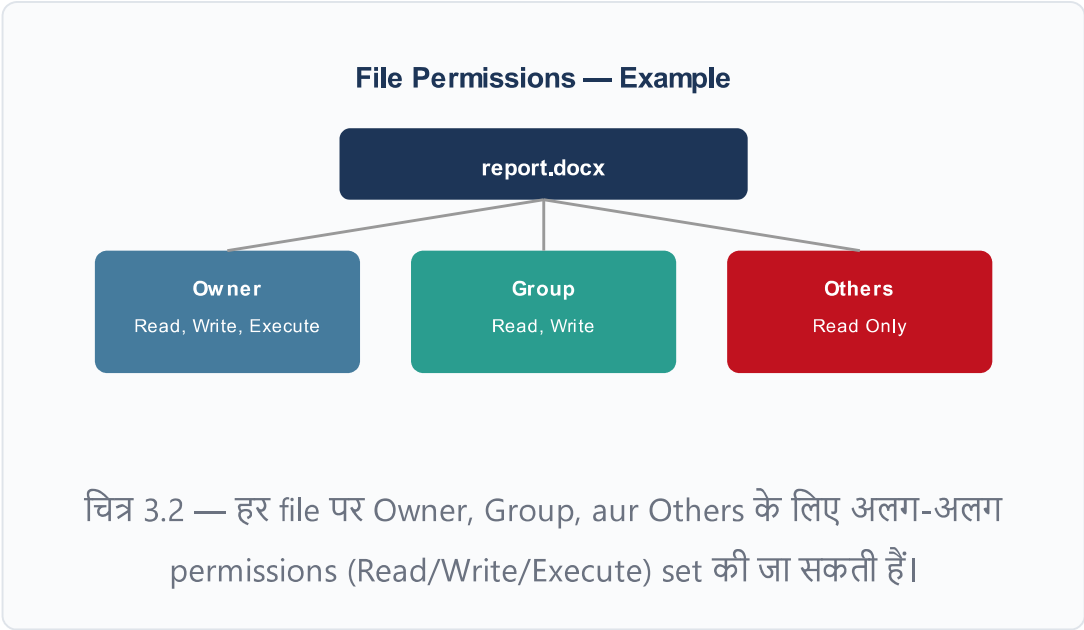
Example: किसी bank में employees किन-किन customer accounts को access कर रहे हैं, इसे audit करके यह ensure किया जाता है कि कोई भी employee बिना वजह किसी account की details न देखे।

3.4 File System Protection

File System Protection वह security feature है जो files aur folders को unauthorized access, modification, या deletion से बचाता है, ताकि सिर्फ authorized users ही उन्हें access कर सकें।

Working / Steps

- 1. हर file/folder बनने पर उसका एक **owner** तय होता है (आमतौर पर जिसने उसे बनाया)।
- 2. Owner (या administrator) उस file पर अलग-अलग users/groups के लिए **permissions set** करता है — Read, Write, या Execute।
- 3. जब भी कोई user उस file को access करने की कोशिश करता है, OS सबसे पहले यह **check** करता है कि उस user को उस specific permission (जैसे write) की अनुमति है या नहीं।
- 4. अगर permission मौजूद है, तो operation (पढ़ना/बदलना) होने दिया जाता है; अगर नहीं, तो **"Access Denied"** error दिखा दी जाती है।



Method	Description
--------	-------------

Permissions (Read, Write, Execute)	हर file/folder पर यह set किया जाता है कि कौन उसे read, write, या execute कर सकता है
Access Control List (ACL)	यह detailed list होती है जो बताती है कि कौन से specific users या groups को किस file पर कौन सी permission है
Encryption	Files को encrypt करके रखा जाता है, ताकि बिना सही key के कोई भी उन्हें पढ़ न सके

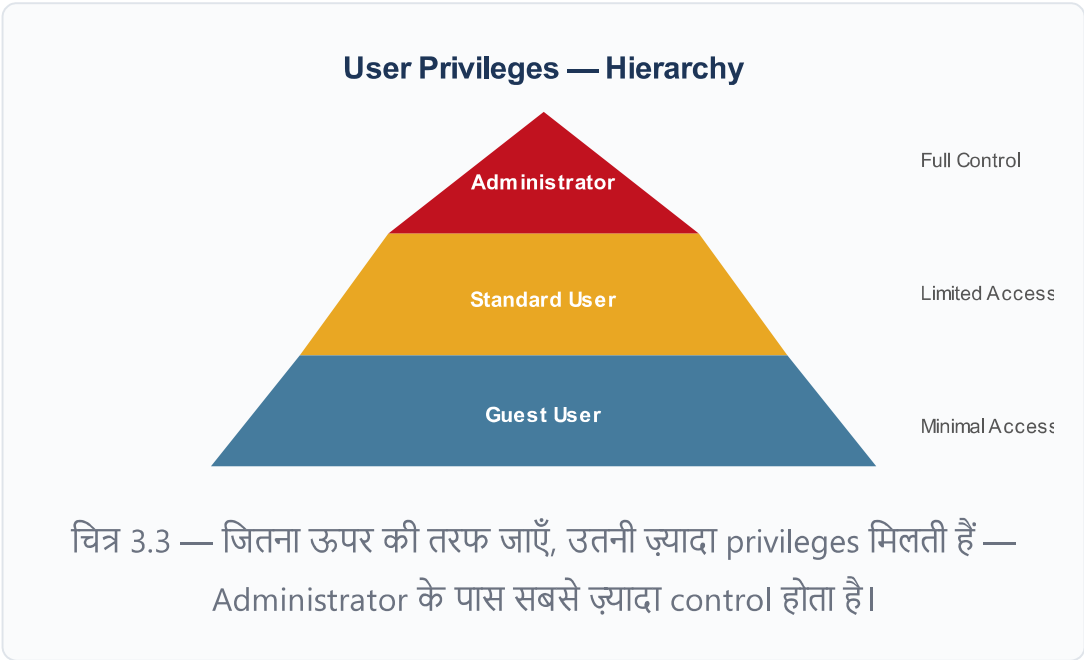
Features:

- Data को accidental या intentional नुकसान से बचाता है।
- अलग-अलग users को अलग-अलग level की access permissions दी जा सकती हैं।
- Sensitive files को unauthorized लोगों की पहुँच से दूर रखता है।

Example: Windows में किसी folder पर right-click करके "Properties → Security" में जाकर यह set किया जा सकता है कि कौन सा user उसे सिर्फ read कर सकता है aur कौन उसे edit भी कर सकता है।

3.5 User Privileges

User Privileges वह rights (अधिकार) होते हैं जो किसी user को system में दिए जाते हैं, यह decide करने के लिए कि वह user कौन-कौन से resources को access कर सकता है।



User Type	Privileges
Administrator (Root/Superuser)	पूरे system पर full control होता है — software install करना, settings बदलना, users manage करना
Standard User	Limited privileges होती हैं — अपनी files access कर सकता है, लेकिन system-wide settings नहीं बदल सकता
Guest User	सबसे कम privileges होती हैं — सिर्फ basic tasks कर सकता है

Principle of Least Privilege: हर user को सिर्फ उतनी ही privileges दी जानी चाहिए जितनी उसे अपना काम करने के लिए ज़रूरी हैं — इससे अगर किसी user का account compromise भी हो जाए, तो attacker को सीमित नुकसान ही पहुँचा पाएगा।

Example: किसी company में एक normal employee सिर्फ अपने department के software use कर सकता है, लेकिन IT administrator को पूरे network को manage करने की privilege होती है।

4. Anti-Virus Software

Anti-Virus Software एक ऐसा program है जो computer system में मौजूद viruses, malware, worms, trojans जैसे harmful software को detect करता है, उन्हें block करता है, aur ज़रूरत पड़ने पर system से remove भी कर देता है।

4.1 Types of Detection

Type	Description
Signature-based Detection	पहले से known viruses के unique "signatures" (patterns) की database से match करके उन्हें पहचानता है
Heuristic-based Detection	Files के behavior aur structure को analyze करके यह पता लगाता है कि क्या यह कोई नया, unknown virus हो सकता है
Cloud-based Detection	Cloud पर मौजूद बड़ी database का उपयोग करके real-time में नए threats को पहचानता है
Behavior-based Detection	किसी program के run होने के दौरान उसकी suspicious activities को monitor करता है

4.2 Working Process

Anti-Virus — Working Process

चित्र 4.1 — Anti-virus पहले files को scan करता है, signatures से compare करता है, infected files को quarantine/delete करता है, aur regularly अपनी database update करता रहता है।

Features:

- Real-time protection देता है, यानी नई files को download/open करते ही scan कर लेता है।
- Scheduled scans set किए जा सकते हैं, ताकि पूरा system periodically check होता रहे।
- Firewall aur email scanning जैसे additional security features भी अक्सर साथ में आते हैं।
- Automatic updates के through नए, हाल ही में discover हुए viruses की जानकारी भी database में जुड़ती रहती है।

Advantages

- System को viruses aur malware से सुरक्षित रखता है।
- Real-time monitoring से threats को नुकसान होने से पहले ही रोक देता है।
- Infected files को automatically detect करके quarantine कर देता है, जिससे manual effort कम लगता है।
- Regular scans से पुराने, छिपे हुए malware को भी ढूँढकर हटाया जा सकता है।

Disadvantages

- System के resources (RAM, CPU) थोड़ा ज़्यादा use करता है, जिससे system slow हो सकता है।
- अगर virus definitions update न हों, तो नए (latest) viruses को detect नहीं कर पाता।
- कभी-कभी genuine, safe files को भी गलती से virus समझ लेता है (false positive)।
- पूरी तरह free antivirus tools में advanced protection features (जैसे ransomware protection) की कमी हो सकती है।

Example: Windows Defender, Quick Heal, aur Norton जैसे anti-virus software आम तौर पर personal computers aur laptops में इस्तेमाल किए जाते हैं, ताकि internet से download की गई files या email attachments से आने वाले viruses से बचाव हो सके।