Information Security And IT Laws

PG DIPLOMA IN WEB DESIGNING

Lecture 1

Introduction And Security Trends

सुरक्षा की आवश्यकता (Need for Security)

आज के डिजिटल युग में, लगभग सभी कार्य कंप्यूटर और इंटरनेट के माध्यम से होते हैं। ऐसे में डेटा और सिस्टम की सुरक्षा अत्यंत महत्वपूर्ण हो जाती है।

सुरक्षा की आवश्यकता के प्रमुख कारण:

1. **डेटा की गोपनीयता (Confidentiality):** निजी और संवेदनशील जानकारी को अनधिकृत उपयोगकर्ताओं से सुरक्षित रखना।
2. **डेटा की अखंडता (Integrity):** सुनिश्चित करना कि डेटा बिना अनुमति के बदला या नष्ट न हो।
3. **उपलब्धता (Availability):** अधिकृत उपयोगकर्ता जब चाहें तब सिस्टम या डेटा तक पहुंच सकें।
4. **अनाधिकृत पहुँच से बचाव:** हैकिंग, वायरस, मैलवेयर आदि से बचाव।
5. **व्यवसाय की निरंतरता:** किसी भी सुरक्षा उल्लंघन से व्यवसाय को भारी नुकसान हो सकता है।

सुरक्षा सिद्धांत (Security Principles)

सूचना सुरक्षा के कुछ मूलभूत सिद्धांत होते हैं जिन्हें CIA ट्रायएड (CIA Triad) कहा जाता है:

1. **गोपनीयता (Confidentiality):**
    - केवल अधिकृत व्यक्ति ही डेटा देख या उपयोग कर सके।
    - उदाहरण: पासवर्ड, एन्क्रिप्शन आदि।
2. **अखंडता (Integrity):**
    - डेटा पूरा, सही और विश्वसनीय बना रहे।
    - उदाहरण: हैशिंग तकनीक, डिजिटल सिग्नेचर।
3. **उपलब्धता (Availability):**
    - जब जरूरत हो, डेटा या सेवा उपलब्ध हो।
    - उदाहरण: बैकअप सिस्टम, फायरवॉल, डीडीओएस सुरक्षा।

इन तीनों के अतिरिक्त और सिद्धांत भी होते हैं:

4. **पहुंच नियंत्रण (Access Control):** यह तय करता है कि कौन क्या उपयोग कर सकता है।
5. **उत्तरदायित्व (Accountability):** कौन क्या कर रहा है, इसका रिकॉर्ड रखना (जैसे लॉगिंग)।

प्रमाणीकरण (Authentication)

Authentication का अर्थ है किसी उपयोगकर्ता की पहचान की पुष्टि करना। यह निर्धारित करता है कि उपयोगकर्ता वही है जो वह दावा करता है।

Authentication के प्रकार:

1. **कुछ जो आप जानते हैं (Something you know):**
    - पासवर्ड, पिन, उत्तर वाले प्रश्न
2. **कुछ जो आपके पास है (Something you have):**
    - स्मार्ट कार्ड, ओटीपी (One Time Password), टोकन
3. **कुछ जो आप हैं (Something you are):**
    - बायोमेट्रिक पहचान जैसे फिंगरप्रिंट, रेटिना स्कैन, फेस आईडी

उदाहरण: जब आप बैंक ऐप में लॉग इन करते हैं और OTP डालते हैं – तो यह एक प्रमाणीकरण प्रक्रिया है।

पहुंच नियंत्रण (Access Control)

Access Control यह निर्धारित करता है कि कौन उपयोगकर्ता कौन से संसाधनों तक पहुंच सकता है और क्या कार्य कर सकता है।

Access Control के प्रकार:

1. **DAC (Discretionary Access Control):**
    - स्वामित्व आधारित नियंत्रण। उपयोगकर्ता अपने डेटा की अनुमति तय कर सकता है।
2. **MAC (Mandatory Access Control):**
    - सख्त नीति आधारित नियंत्रण, जैसे सरकारी सिस्टम में।
3. **RBAC (Role-Based Access Control):**
    - उपयोगकर्ता की भूमिका के आधार पर अनुमति मिलती है।
    - जैसे – टीचर, स्टूडेंट, एडमिन आदि।
4. **ABAC (Attribute-Based Access Control):**
    - उपयोगकर्ता के गुणों, समय, स्थान आदि के आधार पर अनुमति।

उदाहरण: एक स्टूडेंट केवल अपना रिजल्ट देख सकता है, किसी और का नहीं – यह एक प्रकार का RBAC है

सुरक्षा के खतरे (Threats to Security)

सुरक्षा के खतरे वे सभी संभावनाएँ हैं जो किसी सिस्टम, नेटवर्क, डेटा या सेवा को नुकसान पहुँचा सकती हैं। ये खतरे बाहरी (External) या आंतरिक (Internal) हो सकते हैं।

1. वायरस और वॉर्म्स (Viruses and Worms)

वायरस (Virus):

- यह एक **हानिकारक प्रोग्राम** होता है जो खुद को किसी अन्य प्रोग्राम या फाइल के साथ जोड़ लेता है।
- यह जब तक सक्रिय नहीं होता जब तक वह प्रोग्राम नहीं चलता जिसमें वायरस जुड़ा है।
- वायरस फाइल्स को भ्रष्ट कर सकते हैं, डेटा को नष्ट कर सकते हैं, सिस्टम को स्लो कर सकते हैं।

उदाहरण: Michelangelo Virus, ILOVEYOU Virus

वॉर्म (Worm):

- वॉर्म खुद को नेटवर्क में फैलाता है और इसकी **स्वतंत्र कार्यक्षमता** होती है (इसके लिए किसी फाइल की ज़रूरत नहीं)।
- यह तेजी से नेटवर्क में फैल सकता है और सर्वर को धीमा कर सकता है या क्रैश कर सकता है।

उदाहरण: Code Red Worm, MyDoom

2. घुसपैठिए (Intruders)

घुसपैठिए वे व्यक्ति होते हैं जो अनधिकृत तरीके से सिस्टम में प्रवेश करते हैं। दो प्रकार होते हैं:

1. **असत्यापित घुसपैठिए (External Intruders):**
    - वे जो सिस्टम से बाहर होते हैं, जैसे हैकर्स।
2. **सत्यापित लेकिन दुर्भावनापूर्ण (Internal Intruders):**
    - वे लोग जो अधिकृत उपयोगकर्ता होते हैं लेकिन अंदर से नुकसान पहुँचाते हैं।

3. अंदरूनी लोग (Insiders)

- ये वे कर्मचारी या उपयोगकर्ता होते हैं जो सिस्टम तक **वैध पहुँच** रखते हैं लेकिन जानबूझकर या अनजाने में सुरक्षा को खतरा पहुँचाते हैं।
- अक्सर सबसे बड़ा खतरा अंदरूनी लोगों से होता है क्योंकि उनके पास डेटा, पासवर्ड आदि की सीधी पहुँच होती है।

उदाहरण: कोई कर्मचारी कंपनी का गोपनीय डेटा चुरा कर प्रतियोगी को बेच देता है।

4. आपराधिक संगठन (Criminal Organizations)

- ये पेशेवर अपराधी समूह होते हैं जो फ़ायदे के लिए:
    - डेटा चोरी करते हैं,
    - फिरौती माँगते हैं (Ransomware),
    - वित्तीय धोखाधड़ी करते हैं,
    - पहचान चोरी करते हैं।

उदाहरण: बैंकिंग ट्रोजन द्वारा बैंक अकाउंट से पैसा निकाल लेना।

5. आतंकवादी (Terrorists)

- साइबर आतंकवादी इंटरनेट और डिजिटल नेटवर्क का उपयोग करके:
    - किसी देश की सुरक्षा प्रणालियों को ठप कर सकते हैं,
    - महत्वपूर्ण सेवाओं जैसे बिजली, पानी, संचार को निशाना बना सकते हैं,
    - दहशत फैलाने का काम कर सकते हैं।

6. सूचना युद्ध (Information Warfare - IW)

- **सूचना युद्ध** का अर्थ है किसी देश, संस्था या संगठन की सूचनाओं और सूचना प्रणालियों पर हमला करना।
- इसका उद्देश्य:
    - गलत सूचना फैलाना (Disinformation)
    - महत्वपूर्ण सूचना चुराना (Cyber Espionage)
    - जनता की सोच प्रभावित करना
    - सैन्य या राजनीतिक नुकसान पहुँचाना

उदाहरण: किसी देश का चुनाव प्रभावित करने के लिए सोशल मीडिया में झूठी खबरें फैलाना।

7. हमला करने के रास्ते (Avenues of Attack)

हमले करने के कई रास्ते या तरीके होते हैं, जैसे:

1. **नेटवर्क अटैक:** DDoS, IP Spoofing, Packet Sniffing
2. **सिस्टम अटैक:** वायरस, रूटकिट्स, बैकडोर्स
3. **वेब अटैक:** SQL Injection, XSS, CSRF
4. **सामाजिक इंजीनियरिंग:** फिशिंग, प्रीटेक्स्टिंग, बाइटिंग
5. **फिजिकल अटैक:** हार्डवेयर चोरी, अनधिकृत प्रवेश

8. हमले के चरण (Steps in Attack)

एक सामान्य साइबर हमला इन चरणों में किया जाता है:

1. **Reconnaissance (जासूसी):**
    - लक्ष्य के बारे में जानकारी इकट्ठा करना (IP, सिस्टम आदि)
2. **Scanning (स्कैनिंग):**
    - कमजोरियों को स्कैन करना, जैसे कौन से पोर्ट खुले हैं
3. **Gaining Access (पहुंच प्राप्त करना):**
    - हैकिंग करके सिस्टम में प्रवेश करना

4. **Maintaining Access (पहुँच बनाए रखना):**
    - बैकडोर या रूटकिट इंस्टॉल करना ताकि बार-बार प्रवेश किया जा सके
5. **Covering Tracks (साक्ष्य मिटाना):**
    - लॉग फाइल्स मिटाना, ट्रेस को छुपाना

हमलों के प्रकार (Types of Attacks)

साइबर अटैक्स को आमतौर पर दो मुख्य श्रेणियों में बाँटा जाता है:

1. सक्रिय हमले (Active Attacks)

इन हमलों में **डेटा को बदला जाता है, रोका जाता है, या नष्ट किया जाता है।** हमलावर सिस्टम या नेटवर्क में हस्तक्षेप करता है।

उदाहरण:

- Man-in-the-Middle Attack
- Spoofing
- Denial of Service (DoS)
- Replay Attack

2. निष्क्रिय हमले (Passive Attacks)

इसमें हमलावर केवल **डेटा को सुनता (monitor) या देखता (observe)** है लेकिन कोई बदलाव नहीं करता। यह हमला जानकारी चुराने के लिए होता है।

उदाहरण:

- ईमेल या डेटा की निगरानी (eavesdropping)
- ट्रैफिक एनालिसिस

Denial of Service (DoS) Attack

- इसका उद्देश्य होता है कि कोई **सेवा (service)** या वेबसाइट **उपयोगकर्ता के लिए उपलब्ध न रहे।**
- हमलावर एक साथ बहुत सारे रिक्वेस्ट भेजता है जिससे सिस्टम या सर्वर क्रैश हो जाता है।

उदाहरण: किसी वेबसाइट पर इतना ट्रैफिक भेजना कि वह डाउन हो जाए।

DoS का उन्नत रूप **Distributed Denial of Service (DDoS)** है, जो कई कंप्यूटरों से एक साथ हमला करता है।

Backdoors और Trapdoors

Backdoor:

- यह एक **गुप्त रास्ता** होता है जिससे हमलावर सिस्टम तक पहुँच सकता है, बायपास करते हुए सामान्य सुरक्षा।
- सॉफ़्टवेयर में जानबूझकर या अनजाने में छुपा हो सकता है।

Trapdoor:

- यह एक **प्रोग्राम के अंदर छिपा कोड** होता है जो कुछ विशेष शर्तों पर सक्रिय होता है।
- प्रोग्रामर इसे परीक्षण या बाद में उपयोग के लिए छोड़ता है, लेकिन हमलावर इसका दुरुपयोग कर सकते हैं।

Spoofing Attack

- इसमें हमलावर किसी वैध सिस्टम, डिवाइस, या व्यक्ति की **नक़ल (pretend)** करता है।
- **प्रकार:**
    - IP Spoofing
    - Email Spoofing
    - Website Spoofing
    - DNS Spoofing

उदाहरण: एक नकली वेबसाइट जो दिखती असली बैंक की तरह है।

Man-in-the-Middle (MITM) Attack

- हमलावर दो लोगों या सिस्टम के **बीच में बैठकर उनकी बातचीत सुनता या बदलता है।**
- दोनों पक्षों को लगता है कि वे सीधे एक-दूसरे से बात कर रहे हैं, जबकि बीच में कोई है।

उदाहरण: इंटरनेट कैफे में कोई Wi-Fi पर डेटा कैप्चर कर ले।

Replay Attack

- इसमें हमलावर एक वैध डेटा ट्रांसमिशन को **कैप्चर करके उसे बाद में फिर से भेजता है** ताकि सिस्टम को धोखा दिया जा सके।

उदाहरण: एक वैध लॉगिन सत्र को कैप्चर करके दोबारा उपयोग करना।

TCP/IP Hacking

- TCP/IP प्रोटोकॉल में कमजोरी का फायदा उठाकर हमलावर नेटवर्क कम्युनिकेशन को बाधित या नियंत्रित करता है।
- **उदाहरण:**

- IP Spoofing
- Session Hijacking
- Packet Sniffing

Encryption Attacks

- एन्क्रिप्शन तकनीकों को तोड़ने या चुराने का प्रयास।

प्रकार:

1. **Brute Force Attack:** सभी संभावित कुंजियों को आज़माना।
2. **Cryptanalysis:** एन्क्रिप्शन एल्गोरिथ्म की कमजोरी को खोजना।
3. **Side-channel Attack:** हार्डवेयर से संकेत (जैसे समय या ऊर्जा) लेकर कुंजी निकालना।

मैलवेयर (Malware)

1. वायरस (Virus):

- खुद को किसी फाइल में जोड़ता है और फैलता है। फाइल्स को नुकसान पहुंचा सकता है।

2. लॉजिक बम (Logic Bomb):

- एक छुपा हुआ प्रोग्राम जो किसी **विशेष स्थिति या तारीख** पर सक्रिय होता है।
- **उदाहरण:** जैसे ही कोई फाइल डिलीट की जाए, सिस्टम खुद-ब-खुद फॉर्मेट हो जाए।

Lecture 2

Organizational/Operational Security

सुरक्षा में लोगों की भूमिका

कंप्यूटर सुरक्षा या साइबर सुरक्षा केवल तकनीकी उपायों तक ही सीमित नहीं होती, बल्कि इसमें **लोगों की जागरूकता और जिम्मेदारी** भी महत्वपूर्ण भूमिका निभाती है। एक असावधान व्यक्ति लाखों की सुरक्षा प्रणाली को कमजोर बना सकता है। नीचे सुरक्षा से संबंधित विभिन्न गतिविधियों और लोगों की जिम्मेदारियों का विवरण दिया गया है:

1. पासवर्ड चयन (Password Selection)

- मजबूत पासवर्ड का चयन करना प्रत्येक उपयोगकर्ता की जिम्मेदारी होती है।
- आसान या सामान्य पासवर्ड जैसे "123456", "password", "admin" सुरक्षा के लिए खतरा होते हैं।
- **मजबूत पासवर्ड** में छोटे-बड़े अक्षर, संख्याएँ और विशेष चिन्ह जैसे @, #, $ शामिल होने चाहिए।
- पासवर्ड को नियमित रूप से बदलना और किसी के साथ साझा न करना आवश्यक है।

2. पिग्गीबैकिंग (Piggybacking)

- जब कोई व्यक्ति किसी अधिकृत व्यक्ति के साथ या उसके पीछे बिना अनुमति के सुरक्षा क्षेत्र में प्रवेश करता है, तो इसे पिग्गीबैकिंग कहा जाता है।
- जैसे कोई बिना ID कार्ड के ऑफिस में उस व्यक्ति के साथ घुस जाए जो ID दिखाकर अंदर जा रहा है।
- इससे अनधिकृत पहुंच संभव होती है, जो सुरक्षा के लिए खतरा है।
- उपाय: दरवाजे पर ऑटोमैटिक लॉक सिस्टम, और "टेलगेटिंग" रोकने के लिए कर्मचारियों को सचेत किया जाना चाहिए।

3. शोल्डर सर्फिंग (Shoulder Surfing)

- यह तब होता है जब कोई व्यक्ति किसी अन्य के कंधे के ऊपर से देख कर उसका पासवर्ड, पिन या अन्य संवेदनशील जानकारी चुरा लेता है।
- सार्वजनिक स्थानों पर कंप्यूटर या मोबाइल फोन का उपयोग करते समय सावधानी बरतनी चाहिए।
- स्क्रीन प्राइवेसी गार्ड का उपयोग किया जा सकता है।

4. डंपस्टर डाइविंग (Dumpster Diving)

- जब कोई व्यक्ति कूड़ेदान (डस्टबिन) से पुराने कागज़, रिपोर्ट, या अन्य दस्तावेज़ ढूँढकर संवेदनशील जानकारी निकालने की कोशिश करता है, तो इसे डंपस्टर डाइविंग कहा जाता है।
- समाधान: पुराने दस्तावेज़ों को फाड़ना या शेडर मशीन से नष्ट करना।

5. अनधिकृत सॉफ्टवेयर/हार्डवेयर इंस्टॉल करना (Installing Unauthorized Software/Hardware)

- कर्मचारी यदि बिना अनुमति के सॉफ़्टवेयर या हार्डवेयर इंस्टॉल करते हैं, तो इससे वायरस, मालवेयर या डेटा चोरी हो सकती है।
- IT नीति के अंतर्गत केवल अनुमोदित सॉफ्टवेयर और उपकरणों का ही उपयोग किया जाना चाहिए।
- कंपनी को ऐसे मामलों में सख्त नीति अपनानी चाहिए।

6. गैर-कर्मचारी व्यक्तियों द्वारा पहुँच (Access by Non-employees)

- यदि कोई बाहरी व्यक्ति कंपनी के सिस्टम या परिसर तक पहुँच जाता है, तो यह सुरक्षा जोखिम होता है।
- उदाहरण: क्लीनर, विज़िटर, कूरियर बॉय आदि का सिस्टम एरिया में पहुँच।
- उपाय: विजिटर पास सिस्टम, CCTV निगरानी और सीमित पहुंच (Restricted Access) लागू करना।

7. सुरक्षा जागरूकता (Security Awareness)

- सुरक्षा जागरूकता सभी कर्मचारियों के लिए अनिवार्य है।
- समय-समय पर प्रशिक्षण (training) देना चाहिए जिससे वे फिशिंग, स्पैम, वायरस, और अन्य खतरों को पहचान सकें।
- एक जागरूक कर्मचारी ही पहली सुरक्षा दीवार होता है।

8. व्यक्तिगत उपयोगकर्ताओं की जिम्मेदारी (Individual User Responsibilities)

- हर उपयोगकर्ता को निम्नलिखित जिम्मेदारियाँ निभानी चाहिए:
    - पासवर्ड गोपनीय रखना
    - संदिग्ध लिंक या ईमेल पर क्लिक न करना
    - ऑफिस सिस्टम का व्यक्तिगत उपयोग न करना
    - स्क्रीन लॉक करके सिस्टम छोड़ना
    - सॉफ़्टवेयर अपडेट्स को नजरअंदाज न करना

भौतिक सुरक्षा (Physical Security)

भौतिक सुरक्षा (Physical Security) का तात्पर्य उन उपायों और साधनों से है जो किसी संगठन, संसाधन या उपकरण को **शारीरिक रूप से पहुँच से बचाने** के लिए किए जाते हैं। इसका उद्देश्य है अवांछित व्यक्तियों, चोरी, तोड़फोड़, प्राकृतिक आपदाओं आदि से सुरक्षा प्रदान करना।

प्रवेश नियंत्रण (Access Controls)

प्रवेश नियंत्रण यह सुनिश्चित करता है कि केवल अधिकृत व्यक्ति ही किसी विशेष क्षेत्र, उपकरण या सिस्टम तक पहुँच सकें। इसमें निम्नलिखित शामिल हो सकते हैं:

- ID कार्ड / स्मार्ट कार्ड
- पिन कोड / पासवर्ड
- बायोमेट्रिक पहचान प्रणाली
- सिक्योरिटी गार्ड द्वारा मैन्युअल जांच
- ऑटोमेटेड दरवाजे और लॉक सिस्टम

बायोमेट्रिक्स (Biometrics)

बायोमेट्रिक प्रणाली इंसानों की **शारीरिक या व्यवहारिक विशेषताओं** को पहचान कर सुरक्षा प्रदान करती है। यह प्रणाली अत्यधिक सुरक्षित मानी जाती है क्योंकि ये विशेषताएं व्यक्ति विशेष के लिए अद्वितीय होती हैं।

बायोमेट्रिक पहचान के प्रकार:

1. फिंगरप्रिंट्स (Fingerprints - अंगुलियों के निशान)

- प्रत्येक व्यक्ति के फिंगरप्रिंट अद्वितीय होते हैं।
- अंगुलियों की लकीरों के पैटर्न को स्कैन करके पहचान की जाती है।
- यह सबसे सामान्य और प्रचलित बायोमेट्रिक विधि है।

2. हैंड प्रिंट्स (Hand Prints - हाथों के निशान)

- पूरे हाथ की बनावट, लंबाई और उंगलियों की स्थिति की जाँच होती है।
- इसका उपयोग उच्च-सुरक्षा क्षेत्रों में किया जाता है।

3. रेटिना स्कैन (Retina Scan - नेत्र की रेटिना का स्कैन)

- आँख की रेटिना में रक्त धमनियों की संरचना को स्कैन किया जाता है।
- यह बेहद सटीक और सुरक्षित तरीका है लेकिन महंगा होता है।

4. आईरिस पैटर्न (Iris Pattern - आंखों की पुतली के पैटर्न)

- रेटिना के बजाय आईरिस (पुतली) के पैटर्न को स्कैन किया जाता है।
- संपर्क रहित प्रक्रिया होती है, जिससे सुविधाजनक होती है।

5. वॉयस पैटर्न्स (Voice Patterns - आवाज़ की पहचान)

- व्यक्ति की आवाज़ की टोन, गति, लय आदि की पहचान करके एक्सेस दी जाती है।

- कॉल सेंटर या वॉयस असिस्टेंट सिस्टम में उपयोगी।

6. हस्ताक्षर और लेखन शैली (Signature and Writing Patterns)

- व्यक्ति के हस्ताक्षर की गति, दबाव, दिशा और पैटर्न को विश्लेषित किया जाता है।
- बैंकिंग और दस्तावेज़ सत्यापन में इसका उपयोग होता है।

7. कीस्ट्रोक्स (Keystrokes - टाइपिंग पैटर्न)

- व्यक्ति किस तरह से टाइप करता है – गति, अक्षरों का क्रम, दबाव – यह सब विश्लेषण किया जाता है।
- यह एक व्यवहारिक बायोमेट्रिक तरीका है।

भौतिक अवरोध (Physical Barriers)

इनका उद्देश्य अनधिकृत व्यक्तियों को भौतिक रूप से किसी क्षेत्र में प्रवेश करने से रोकना है:

- **दीवारें और गेट्स**: सीमाओं की रक्षा करते हैं।
- **सीसीटीवी कैमरे**: निगरानी के लिए।
- **सुरक्षा गार्ड**: मैन्युअल जांच और निगरानी।
- **बायोमेट्रिक दरवाजे**: एक्सेस कंट्रोल के लिए।
- **मेटल डिटेक्टर और स्कैनर**: हथियार या अवैध वस्तुओं की जांच।

नेटवर्क सुरक्षा का परिचय (Introduction to Network Security)

नेटवर्क सुरक्षा (Network Security) का उद्देश्य कंप्यूटर नेटवर्क और उससे जुड़ी जानकारी को **अनधिकृत पहुंच, दुरुपयोग, संशोधन, या विनाश** से बचाना है। यह एक ऐसा ढाँचा है जो हार्डवेयर, सॉफ्टवेयर, नीतियों और प्रक्रियाओं का उपयोग कर नेटवर्क को सुरक्षित बनाता है।

नेटवर्क सुरक्षा के मूल तत्व (Network Security Basics)

नेटवर्क सुरक्षा में कुछ प्रमुख बुनियादी सिद्धांत होते हैं, जो किसी भी सुरक्षा प्रणाली की नींव होते हैं:

1. गोपनीयता (Confidentiality)

- केवल अधिकृत व्यक्ति ही डेटा तक पहुँच सकें।
- एन्क्रिप्शन (Encryption) का उपयोग कर डेटा को सुरक्षित रखा जाता है।

2. अखंडता (Integrity)

- डेटा को ट्रांसमिट या स्टोर करते समय बिना किसी अनधिकृत बदलाव के बनाए रखना।
- हैशिंग तकनीकों और चेकसम का उपयोग किया जाता है।

3. उपलब्धता (Availability)

- आवश्यक जानकारी और सेवाएं अधिकृत उपयोगकर्ताओं को समय पर उपलब्ध हों।
- डिनायल-ऑफ-सर्विस (DoS) हमलों से सुरक्षा प्रदान की जाती है।

4. प्रमाणीकरण (Authentication)

- सुनिश्चित करना कि उपयोगकर्ता वही है जो वह कहता है।
- पासवर्ड, बायोमेट्रिक, OTP, आदि का उपयोग।

5. अनुमति (Authorization)

- उपयोगकर्ता को केवल उन्हीं संसाधनों तक पहुँच मिले, जिनकी उसे अनुमति हो।

6. गणनशीलता (Accountability)

- सभी गतिविधियों की निगरानी और लॉग रखना ताकि बाद में उसका विश्लेषण किया जा सके।

नेटवर्क सुरक्षा का मॉडल (Model for Network Security)

नेटवर्क सुरक्षा का एक मानक मॉडल होता है जो संचार प्रक्रिया को **सुरक्षित** बनाने में मदद करता है।

मॉडल की मुख्य इकाइयाँ:

1. प्रेषक (Sender)

- वह उपयोगकर्ता या सिस्टम जो संदेश भेज रहा है।

2. संदेश (Message / Data)

- वह सूचना जो प्रेषक द्वारा भेजी जा रही है।

3. एन्क्रिप्शन (Encryption)

- डेटा को कोड में बदलना ताकि कोई अनधिकृत व्यक्ति उसे न पढ़ सके।

4. संप्रेषण माध्यम (Transmission Medium)

- जैसे: इंटरनेट, लोकल एरिया नेटवर्क (LAN), वाई-फाई आदि।

5. हमलावर (Attacker / Intruder)

- ऐसा व्यक्ति जो नेटवर्क में घुसपैठ कर डेटा चोरी या नुकसान पहुँचाना चाहता है।

6. डिक्रिप्शन (Decryption)

- एन्क्रिप्टेड डेटा को फिर से मूल रूप में बदलना ताकि रिसीवर उसे समझ सके।

7. प्राप्तकर्ता (Receiver)

- वह उपयोगकर्ता या सिस्टम जो संदेश प्राप्त करता है।

नेटवर्क सुरक्षा मॉडल का सरलीकृत चित्रात्मक प्रतिनिधित्व:

प्रेषक → [एन्क्रिप्शन] → [संचार माध्यम] → [हमले की संभावना] → [डिक्रिप्शन] → प्राप्तकर्ता

नेटवर्क सुरक्षा में प्रयुक्त तकनीकें (Technologies Used in Network Security)

तकनीक	विवरण
Firewall	अनधिकृत एक्सेस को रोकने के लिए नेटवर्क के बीच सुरक्षा दीवार
Antivirus/Anti-malware	हानिकारक सॉफ़्टवेयर से सुरक्षा
Intrusion Detection System (IDS)	संदिग्ध गतिविधियों की पहचान
Virtual Private Network (VPN)	डेटा को एन्क्रिप्ट कर निजी नेटवर्क जैसा अनुभव
Access Control List (ACL)	उपयोगकर्ताओं की पहुँच को नियंत्रित करना
Encryption (AES, RSA)	डेटा को सुरक्षित बनाने के लिए कोडिंग

Lecture 3

Cryptography And Public Key Infrastructure

1. परिचय (Introduction)

क्रिप्टोग्राफी (Cryptography)

क्रिप्टोग्राफी एक ऐसी तकनीक है जिसमें **जानकारी को गुप्त (सीक्रेट)** बनाया जाता है ताकि केवल अधिकृत व्यक्ति ही उसे पढ़ सके। इसमें डेटा को **एनक्रिप्ट (Encrypt)** और **डिक्रिप्ट (Decrypt)** किया जाता है।

> उद्देश्य: **गोपनीयता (Confidentiality), अखंडता (Integrity), प्रमाणीकरण (Authentication)** और **अस्वीकरण से रोकथाम (Non-repudiation)**।

क्रिप्टएनालिसिस (Cryptanalysis)

क्रिप्टएनालिसिस वह प्रक्रिया है जिसमें कोड या एन्क्रिप्टेड डेटा को बिना कुंजी (key) के डिकोड करने की कोशिश की जाती है।

> यह क्रिप्टोग्राफी के विरुद्ध कार्य करता है।

क्रिप्टोलॉजी (Cryptology)

क्रिप्टोलॉजी एक व्यापक क्षेत्र है, जो क्रिप्टोग्राफी और क्रिप्टएनालिसिस दोनों को सम्मिलित करता है।

> मतलब: **क्रिप्टोग्राफी** + **क्रिप्टएनालिसिस** = **क्रिप्टोलॉजी**

2. सब्स्टीट्यूशन तकनीकें (Substitution Techniques)

इसमें मूल अक्षरों को दूसरे अक्षरों या प्रतीकों से **बदल दिया जाता है (substitute)**। इसके अंतर्गत निम्नलिखित तकनीकें आती हैं:

2.1. सीज़र सिफर (Caesar Cipher)

- यह सबसे प्राचीन सब्स्टीट्यूशन सिफर है।
- हर अक्षर को **निश्चित स्थान (जैसे 3 स्थान)** आगे खिसका दिया जाता है।

उदाहरण:

Plain Text: HELLO
Key: 3
Cipher Text: KHOOR
(A को D, B को E, ... Z को C)

2.2. मोनोअल्फाबेटिक सिफर (Monoalphabetic Cipher)

- प्रत्येक अक्षर को किसी *एक अन्य अक्षर* से बदला जाता है।
- यह स्थिर मैपिंग होती है, लेकिन ज़्यादा सुरक्षित नहीं क्योंकि फ्रिक्वेंसी एनालिसिस से तोड़ी जा सकती है।

उदाहरण:

A → M, B → Q, C → L, ...

2.3. पॉलीअल्फाबेटिक सिफर (Polyalphabetic Cipher)

- इसमें **कई अल्फाबेट मैपिंग** का प्रयोग होता है, जिससे एक ही अक्षर को अलग-अलग जगहों पर अलग तरीके से बदला जाता है।

सबसे प्रसिद्ध: Vigenère Cipher

3. ट्रांसपोजिशन तकनीकें (Transposition Techniques)

इसमें अक्षरों की **स्थिति (Position) बदली जाती है**, लेकिन अक्षर वही रहते हैं।

3.1. रेल फेंस तकनीक (Rail Fence Technique)

- अक्षरों को "रेल" जैसी लहर में लिखा जाता है और फिर पढ़ा जाता है।

उदाहरण:

Plain Text: HELLO WORLD
2-रेल:

```
H . L . O . W . R . D
. E . L .   . O . L
```

Cipher Text: HLOWRD EL OL

3.2. सिंपल कॉलमर ट्रांसपोजिशन (Simple Columnar Transposition)

- एक की (Key) दी जाती है, और टेक्स्ट को कॉलम में लिखा जाता है। फिर की के क्रम के अनुसार कॉलम पढ़े जाते हैं।

उदाहरण:

Key: 3 1 4 2
Plain Text: WEAREDISCOVERED

```
W E A R
E D I S
```

```
C O V E
R E D X
```

Cipher Text (Columns rearranged by key): E D R A W I S X C O V E

4. स्टेगनोग्राफी (Steganography)

स्टेगनोग्राफी वह तकनीक है जिसमें संदेश को **छिपाकर** भेजा जाता है, ताकि किसी को पता भी न चले कि कोई जानकारी भेजी गई है।

उदाहरण:

- चित्र या ऑडियो फाइल में गुप्त संदेश छिपाना
- एक ईमेल के बीच में अदृश्य टेक्स्ट
- श्रोत कोड की टिप्पणियों में संदेश

यह क्रिप्टोग्राफी से अलग है क्योंकि इसमें डेटा **छिपाया जाता है**, न कि सिर्फ एनक्रिप्ट किया जाता है।

हैशिंग की संकल्पना (Concept of Hashing in Hindi)

परिभाषा (Definition)

हैशिंग एक प्रक्रिया है जिसमें किसी भी इनपुट (डेटा) को एक **फिक्स्ड साइज वैल्यू या कोड** में परिवर्तित किया जाता है, जिसे **हैश वैल्यू (Hash Value)** या **हैश कोड** कहा जाता है।

यह वैल्यू एक विशेष **हैश फंक्शन (Hash Function)** द्वारा उत्पन्न होती है।

उद्देश्य (Purpose of Hashing)

- डेटा की **सत्यता और अखंडता (Integrity)** को सुनिश्चित करना
- पासवर्ड को सुरक्षित रूप में संग्रहीत करना
- तेज़ सर्च और डेटा एक्सेस में मदद करना
- डिजिटल सिग्नेचर और मैसेज ऑथेंटिकेशन

हैश फंक्शन क्या होता है?

हैश फंक्शन वह गणितीय एल्गोरिदम होता है जो इनपुट डेटा को लेकर उसे एक निश्चित लंबाई के आउटपुट (हैश वैल्यू) में बदल देता है।

उदाहरण:

```
Input: "hello"
Hash Function: SHA-256
Output (Hash Value): 2cf24dba5fb0a... (64-character hex string)
```

हैशिंग की विशेषताएँ (Properties of Hashing)

गुण (Property)	विवरण (Description)
Deterministic	एक ही इनपुट के लिए हमेशा एक ही आउटपुट मिलेगा।
Fast Computation	हैश वैल्यू जल्दी और आसानी से निकाली जा सकती है।
Pre-image Resistance	हैश वैल्यू से ओरिजिनल इनपुट पता करना लगभग असंभव होता है।
Collision Resistance	दो अलग इनपुट का एक जैसा हैश वैल्यू आना बहुत ही मुश्किल है।
Avalanche Effect	इनपुट में थोड़ा सा भी बदलाव, आउटपुट को पूरी तरह बदल देता है।

हैशिंग बनाम एन्क्रिप्शन

बिंदु	हैशिंग	एन्क्रिप्शन
रूपांतरण	एकतरफा (One-way)	दोतरफा (Two-way)
उद्देश्य	सत्यता और पहचान	गोपनीयता
डिक्रिप्शन संभव?	नहीं	हाँ
आउटपुट	फिक्स्ड साइज	वेरिएबल साइज

प्रमुख हैशिंग एल्गोरिदम (Popular Hashing Algorithms)

- **MD5 (Message Digest 5)** – अब पुराना और असुरक्षित
- **SHA-1 (Secure Hash Algorithm 1)** – अब क्रैक हो चुका
- **SHA-256, SHA-512 (Secure Hash Algorithm 2)** – सुरक्षित और आधुनिक
- **SHA-3** – नवीनतम वर्जन

हैशिंग का उपयोग (Applications of Hashing)

1. **पासवर्ड स्टोरेज** – पासवर्ड को plain text की बजाय hashed रूप में स्टोर करना
2. **डेटा इंटीग्रिटी चेक** – फ़ाइल ट्रांसफर के दौरान डेटा के साथ हैश भेजा जाता है, जिससे यह पता चलता है कि डेटा बदला नहीं गया।
3. **डिजिटल सिग्नेचर** – दस्तावेजों को सत्यापित करने के लिए
4. **ब्लॉकचेन** – हर ब्लॉक में हैश वैल्यू शामिल होती है
5. **डेटा स्ट्रक्चर** – जैसे हैश टेबल, मैप्स आदि

कोलिज़न (Collision) क्या है?

जब दो अलग-अलग इनपुट्स एक ही हैश वैल्यू प्रदान करते हैं, तो उसे **कोलिज़न** कहते हैं।

उदाहरण:
```
H("Data1") = H("Data2")
```
ऐसी स्थिति दुर्लभ होनी चाहिए – इसे **Collision Resistance** कहते हैं।

Symmetric और Asymmetric Cryptography (सममित एवं असममित क्रिप्टोग्राफी)

परिचय (Introduction)

Cryptography (कूटलेखन) एक तकनीक है जिसके द्वारा डेटा को इस प्रकार बदला जाता है कि वह केवल अधिकृत व्यक्ति द्वारा ही समझा जा सके।

क्रिप्टोग्राफी मुख्यतः दो प्रकार की होती है:

1. **Symmetric Key Cryptography (सममित कुंजी कूटलेखन)**
2. **Asymmetric Key Cryptography (असममित कुंजी कूटलेखन)**

Symmetric Key Cryptography (सममित कुंजी कूटलेखन)

इस पद्धति में **एक ही कुंजी** का प्रयोग **डेटा को एन्क्रिप्ट और डिक्रिप्ट** करने के लिए किया जाता है।

विशेषताएँ:

- **एक कुंजी (Single key)** होती है।
- कुंजी का **गोपनीय रहना जरूरी** होता है।
- तेज़ और संसाधन-क्षम (Fast and efficient) होती है।
- लेकिन **कुंजी वितरण (Key Distribution)** में समस्या होती है।

DES (Data Encryption Standard)

DES एक पुरानी और लोकप्रिय symmetric encryption तकनीक है।

मुख्य बातें:

- ब्लॉक साइज़: 64-बिट
- कुंजी साइज़: 56-बिट (प्रभावी)
- राउंड्स: 16
- कार्य प्रणाली: Feistel Network पर आधारित

कार्यप्रणाली:

1. Plaintext को 64-बिट ब्लॉक्स में बांटा जाता है।
2. 16 राउंड्स में substitution और permutation के जरिए डेटा को बदला जाता है।
3. अंत में Ciphertext प्राप्त होता है।

नोट: आजकल DES को असुरक्षित माना जाता है और इसके स्थान पर AES, 3DES का उपयोग होता है।

Diffie-Hellman Algorithm

यह एक **Key Exchange Algorithm** है, जिसका उपयोग दो पक्षों के बीच **सुरक्षित कुंजी साझा** करने के लिए किया जाता है।

उद्देश्य:

एक सामान्य सीक्रेट कुंजी तैयार करना, जिसे बाद में symmetric encryption के लिए प्रयोग किया जा सकता है।

कार्यविधि:

1. दोनों पार्टियाँ एक सार्वजनिक प्राइम नंबर (p) और बेस (g) पर सहमत होती हैं।
2. हर कोई अपना प्राइवेट नंबर चुनता है और उससे एक पब्लिक वैल्यू बनाता है।
3. पार्टियाँ अपनी पब्लिक वैल्यू एक-दूसरे को भेजती हैं।
4. वे अपनी निजी कुंजी और प्राप्त पब्लिक वैल्यू से साझा कुंजी बनाते हैं।

लेकिन:

यह स्वयं डेटा एन्क्रिप्ट नहीं करता, बल्कि **सिर्फ कुंजी साझा** करने के लिए प्रयोग होता है।

Key Distribution Problem (कुंजी वितरण की समस्या)

Symmetric cryptography में **कुंजी** को **सुरक्षित रूप से भेजना** एक बहुत बड़ी चुनौती होती है।

- यदि कोई कुंजी ट्रांसमिशन के दौरान लीक हो जाए, तो संपूर्ण सुरक्षा प्रणाली नष्ट हो जाती है।
- यही कारण है कि Asymmetric Cryptography की जरूरत पड़ी।

Asymmetric Key Cryptography (असममित कुंजी कूटलेखन)

इसमें **दो कुंजी** होती हैं:

- **Public Key (सार्वजनिक कुंजी)** – सभी को ज्ञात हो सकती है
- **Private Key (निजी कुंजी)** – केवल उपयोगकर्ता को ज्ञात होती है

विशेषताएँ:

- धीमी लेकिन अधिक सुरक्षित
- कोई कुंजी वितरण की समस्या नहीं
- उपयोग: डिजिटल सिग्नेचर, SSL, एन्क्रिप्शन, आदि में

Digital Signature (डिजिटल हस्ताक्षर)

डिजिटल सिग्नेचर किसी इलेक्ट्रॉनिक दस्तावेज़ की **प्रामाणिकता (Authenticity)** और **सत्यता (Integrity)** सुनिश्चित करता है।

कैसे काम करता है?

1. डॉक्युमेंट का हैश निकाला जाता है।
2. इस हैश को प्राइवेट कुंजी से एन्क्रिप्ट किया जाता है – यही होता है डिजिटल सिग्नेचर।
3. रिसीवर, पब्लिक कुंजी से सिग्नेचर को डिक्रिप्ट करके हैश प्राप्त करता है और डॉक्युमेंट का हैश से मिलान करता है।

उपयोग: सरकारी ई-सेवा, ईमेल सत्यापन, अनुबंधों की वैधता आदि

Key Escrow (कुंजी गुप्त रखाव)

Key Escrow वह व्यवस्था है जिसमें एन्क्रिप्शन की कुंजी को **एक विश्वसनीय थर्ड पार्टी** के पास सुरक्षित रखा जाता है।

उद्देश्य:

- यदि कोई उपयोगकर्ता अपनी कुंजी खो देता है, तो थर्ड पार्टी उसे पुनः प्राप्त करवा सकती है।
- राष्ट्रीय सुरक्षा या जांच के लिए सरकार को एक्सेस मिल सकता है।

चिंता:
इसका दुरुपयोग हो सकता है यदि थर्ड पार्टी भरोसेमंद न हो।

निष्कर्ष (Conclusion)

विशेषता	Symmetric	Asymmetric
कुंजी की संख्या	1	2 (Public + Private)
गति	तेज	धीमी
सुरक्षा	कम	अधिक
उपयोग	डेटा एन्क्रिप्शन	डिजिटल सिग्नेचर, कुंजी वितरण
कुंजी वितरण	बड़ी समस्या	सरल

Public Key Encryption (सार्वजनिक कुंजी एन्क्रिप्शन)

मूल बातें (Basics)

Public Key Encryption एक प्रकार का **Asymmetric Encryption** है जिसमें दो अलग-अलग कुंजियाँ उपयोग होती हैं:

1. **Public Key (सार्वजनिक कुंजी)** – जिसे सभी के साथ साझा किया जा सकता है।
2. **Private Key (निजी कुंजी)** – जो केवल मालिक के पास रहती है।

कार्यविधि:

- Sender, receiver की **Public Key** से डेटा एन्क्रिप्ट करता है।
- Receiver अपनी **Private Key** से उस डेटा को डिक्रिप्ट करता है।

इससे कुंजी साझा करने की कोई समस्या नहीं होती और सुरक्षा भी उच्च स्तर की होती है।

Digital Certificates (डिजिटल प्रमाणपत्र)

डिजिटल सर्टिफिकेट एक इलेक्ट्रॉनिक दस्तावेज़ है जो प्रमाणित करता है कि कोई **Public Key** वास्तव में संबंधित व्यक्ति या संगठन की है।

डिजिटल प्रमाणपत्र में होता है:

- मालिक का नाम
- सार्वजनिक कुंजी (Public Key)
- प्रमाणपत्र जारी करने वाली संस्था (Certificate Authority)
- प्रमाणपत्र की वैधता अवधि
- डिजिटल हस्ताक्षर

Certificate Authorities (प्रमाणपत्र प्राधिकरण - CA)

CA एक विश्वसनीय संगठन होता है जो डिजिटल प्रमाणपत्र जारी करता है। यह यह सुनिश्चित करता है कि जिस व्यक्ति या संस्था के नाम पर प्रमाणपत्र जारी हुआ है, वही उसका वास्तविक मालिक है।

उदाहरण:

- **DigiCert**, **GoDaddy**, **GlobalSign**, **Let's Encrypt**

Registration Authorities (पंजीकरण प्राधिकरण - RA)

RA एक मध्यस्थ संस्था होती है जो उपयोगकर्ताओं की पहचान को प्रमाणित करती है और फिर CA को प्रमाणपत्र जारी करने के लिए अनुशंसा करती है।

- CA = प्रमाणपत्र जारी करता है
- RA = पहचान की पुष्टि करता है

डिजिटल प्रमाणपत्र प्राप्त करने की प्रक्रिया (Steps to Obtain a Digital Certificate)

1. **CSR (Certificate Signing Request) तैयार करना**
   उपयोगकर्ता अपनी जानकारी और सार्वजनिक कुंजी के साथ CSR तैयार करता है।
2. **RA द्वारा पहचान सत्यापन**
   RA उपयोगकर्ता की पहचान की जांच करता है।
3. **CA को CSR भेजना**
   सत्यापन के बाद, CSR को CA को भेजा जाता है।
4. **CA द्वारा प्रमाणपत्र जारी करना**
   CA प्रमाणपत्र तैयार कर उसे डिजिटल रूप से साइन करता है और उपयोगकर्ता को भेजता है।

5. **प्रमाणपत्र को इंस्टॉल करना**
   उपयोगकर्ता इसे अपने सर्वर/ब्राउज़र/सिस्टम में इंस्टॉल करता है।

प्रमाणपत्र की सत्यता और अखंडता की जांच कैसे करें?

(Steps for Verifying Authenticity and Integrity)

1. **प्रमाणपत्र की वैधता जांचें**
   - क्या यह वर्तमान तिथि में वैध है?
   - समाप्ति तिथि से पहले है?
2. **Issuer की जानकारी जांचें**
   - क्या यह किसी विश्वसनीय CA द्वारा जारी किया गया है?
3. **डिजिटल हस्ताक्षर की पुष्टि करें**
   - प्रमाणपत्र में डिजिटल हस्ताक्षर को उस CA की Public Key से वेरिफाई करें।
4. **Certificate Revocation List (CRL) देखें**
   - यह देखें कि क्या प्रमाणपत्र वापस ले लिया गया है या नहीं।
5. **Certificate Chain की जांच करें**
   - प्रमाणपत्र की CA तक की पूरी चेन वैध और अप्रकाशित होनी चाहिए।

निष्कर्ष (Conclusion)

विषय	विवरण
Public Key Encryption	दो कुंजियाँ: एक सार्वजनिक, एक निजी
Digital Certificate	Public key का प्रमाणित दस्तावेज
CA	प्रमाणपत्र जारी करने वाला विश्वसनीय संगठन
RA	उपयोगकर्ता की पहचान की पुष्टि करता है
प्रमाणपत्र प्राप्त करने की प्रक्रिया	CSR → RA → CA → Certificate जारी
सत्यापन	तारीख, डिजिटल सिग्नेचर, CRL और Chain की जांच

Lecture 4

Network Security

Firewall (फायरवॉल)

परिभाषा (Definition):

Firewall एक नेटवर्क सुरक्षा प्रणाली है जो नेटवर्क ट्रैफिक को नियंत्रित करती है। यह यह तय करती है कि कौन-सा डेटा अंदर (इनकमिंग) या बाहर (आउटगोइंग) नेटवर्क से गुजर सकता है।

Firewall का कार्य:

- अनधिकृत एक्सेस को रोकना
- नेटवर्क ट्रैफिक को मॉनिटर करना
- हानिकारक सॉफ़्टवेयर और हमलों से सुरक्षा प्रदान करना

Firewall Design (डिज़ाइन)

आम प्रकार के फायरवॉल:

1. **Packet Filtering Firewall** – पैकेट की हेडर जानकारी को चेक करता है।
2. **Stateful Inspection Firewall** – कनेक्शन की स्थिति को ट्रैक करता है।
3. **Proxy Firewall** – नेटवर्क ट्रैफिक को एक मध्यवर्ती सिस्टम से होकर गुजरवाता है।
4. **Next-Gen Firewall (NGFW)** – पारंपरिक firewall + deep inspection + antivirus + IDS/IPS

Firewall Principles (सिद्धांत)

1. **Default Deny Rule** – अनजान या अस्वीकृत ट्रैफिक को ब्लॉक किया जाता है।
2. **Least Privilege** – केवल वही ट्रैफिक जिसकी आवश्यकता है, उसे अनुमति दी जाती है।
3. **Rule-based Access** – ट्रैफिक को नियमों (rules) के आधार पर अनुमति दी जाती है।
4. **Auditing and Logging** – हर ट्रांजैक्शन को रिकॉर्ड किया जाता है।

Limitations of Firewall (सीमाएं)

1. **Internal Attacks को नहीं रोकता**
   अगर अंदर से कोई हमला करता है, तो फायरवॉल बेबस होता है।
2. **Encrypted Traffic को Inspect नहीं कर सकता**
   SSL/TLS ट्रैफिक को समझना मुश्किल होता है।
3. **Social Engineering से सुरक्षा नहीं देता**
4. **Misconfiguration के कारण सुरक्षा खतरे में पड़ सकती है**

Trusted System (विश्वसनीय प्रणाली)

परिभाषा:

Trusted System ऐसा कंप्यूटर सिस्टम होता है जिसे सुरक्षा की दृष्टि से परखा और भरोसेमंद माना जाता है। यह सुरक्षा नीतियों को लागू करता है और डेटा को अवैध एक्सेस से बचाता है।

विशेषताएँ:

- Access Control Mechanism
- Identification and Authentication
- Security Audit Trails
- Data Encryption

Kerberos – Concept (केरबरोस की संकल्पना)

परिचय:

Kerberos एक नेटवर्क ऑथेंटिकेशन प्रोटोकॉल है जो यूज़र्स और सेवाओं के बीच **सुरक्षित पहचान (authentication)** सुनिश्चित करता है।

इसे **MIT (Massachusetts Institute of Technology)** द्वारा विकसित किया गया था।

मुख्य उद्देश्य:

- सुरक्षित लॉगिन सिस्टम प्रदान करना
- पासवर्ड को नेटवर्क पर ट्रांसमिट न करना
- ट्रस्टेड थर्ड पार्टी का उपयोग करना

Kerberos के घटक (Components):

1. **KDC (Key Distribution Center)**
   - दो भाग:

- **AS (Authentication Server)**
- **TGS (Ticket Granting Server)**

2. **Client (उपयोगकर्ता)**
3. **Service Server (सेवा प्रदाता)**

कार्यविधि (Working Steps):

1. उपयोगकर्ता लॉगिन करता है → **AS** से Authentication Ticket प्राप्त करता है
2. वह टिकट लेकर **TGS** से सेवा के लिए एक **Service Ticket** प्राप्त करता है
3. इस Service Ticket से वह उस सर्वर तक पहुंच पाता है

निष्कर्ष (Summary Table):

विषय	विवरण
Firewall	नेटवर्क ट्रैफिक को नियंत्रित करने वाला सुरक्षा सिस्टम
Design	Packet filtering, Proxy, Stateful inspection आदि
Principles	Default Deny, Least Privilege, Logging
Limitations	Internal attack, Encryption blind, Misconfiguration
Trusted System	विश्वसनीय सिस्टम जो सुरक्षा नीतियों को लागू करता है
Kerberos	सुरक्षित पहचान प्रणाली, जो ट्रस्टेड थर्ड पार्टी पर आधारित है
Kerberos Components	KDC, AS, TGS, Client, Service Server

Security Topologies (सुरक्षा संरचनाएं)

Security Topology वह संरचना होती है जिसमें एक नेटवर्क को इस तरह से डिजाइन किया जाता है कि सुरक्षा बेहतर बनाई जा सके। इसमें विभिन्न ज़ोन, नेटवर्क प्रकार और नियम होते हैं जो नेटवर्क एक्सेस को नियंत्रित करते हैं।

1. Security Zones (सुरक्षा क्षेत्र)

Security Zones नेटवर्क को अलग-अलग स्तरों पर विभाजित करने का तरीका है, ताकि संवेदनशील सिस्टम को बाहरी खतरों से अलग रखा जा सके।

सामान्य सुरक्षा ज़ोन:

ज़ोन	विवरण
Trusted Zone	पूरी तरह सुरक्षित, जैसे Intranet
Untrusted Zone	असुरक्षित, जैसे Internet
DMZ (Demilitarized Zone)	बीच का क्षेत्र – आंशिक रूप से सुरक्षित
Restricted Zone	बहुत ही संवेदनशील डेटा/सिस्टम के लिए

2. DMZ (Demilitarized Zone - निरस्त्रीकृत क्षेत्र)

परिभाषा:

DMZ एक नेटवर्क सबनेट होता है जो इंटरनल नेटवर्क और इंटरनेट के बीच स्थित होता है। इसमें वे सर्वर रखे जाते हैं जिन्हें बाहरी दुनिया से एक्सेस किया जाता है जैसे:

- वेब सर्वर
- मेल सर्वर
- FTP सर्वर

क्यों जरूरी है:

- इन सर्वरों को इंटरनेट से सीधे जोड़ने के बजाय DMZ में रखना अधिक सुरक्षित होता है।
- यदि कोई अटैकर DMZ में प्रवेश करता है तो वह सीधे Intranet तक नहीं पहुंच सकता।

3. Internet (इंटरनेट)

- यह एक **Untrusted Zone** है।
- पूरी दुनिया से जुड़ा हुआ नेटवर्क।
- इसमें कोई नियंत्रित एक्सेस नहीं होता।

4. Intranet (इंट्रानेट)

- संगठन के अंदर का निजी नेटवर्क।
- केवल कर्मचारियों या अधिकृत यूज़र्स के लिए।
- **Highly Trusted Zone** होता है।

5. VLAN (Virtual Local Area Network)

परिभाषा:

VLAN एक लॉजिकल नेटवर्क है जो एक ही फिजिकल नेटवर्क पर अलग-अलग सबनेट्स को अलग करता है।

सुरक्षा में उपयोग:

- अलग-अलग डिपार्टमेंट के लिए अलग VLAN बनाए जाते हैं जैसे HR, Finance, IT।
- इससे एक VLAN का ट्रैफिक दूसरे VLAN से अलग रहता है।
- सिक्योरिटी और मॉनिटरिंग बेहतर होती है।

6. Security Implications (सुरक्षा निहितार्थ)

नेटवर्क डिज़ाइन और टोपोलॉजी के आधार पर विभिन्न सुरक्षा खतरे उत्पन्न हो सकते हैं:

खतरा	विवरण
VLAN Hopping	एक VLAN से दूसरे VLAN में अनधिकृत ट्रैफिक भेजना
Misconfigured Firewalls	गलत कॉन्फ़िगरेशन से DMZ या Intranet असुरक्षित हो सकता है
Insider Threats	Trusted Zone में बैठा व्यक्ति नुकसान पहुंचा सकता है
Lack of Segmentation	सभी सिस्टम जुड़े हैं तो एक सिस्टम से सभी संक्रमित हो सकते हैं

7. Tunnelling (टनलिंग)

परिभाषा:

Tunneling वह तकनीक है जिसमें डेटा को एक प्रोटोकॉल के भीतर लपेटकर दूसरे नेटवर्क या इंटरनेट के ज़रिए सुरक्षित रूप से भेजा जाता है।

उपयोग:

- **VPN (Virtual Private Network)** का आधार यही है।
- टनलिंग डेटा को एन्क्रिप्ट कर एक सुरक्षित मार्ग से भेजता है।

लाभ:

- डेटा छिपा रहता है
- असुरक्षित नेटवर्क पर भी सुरक्षित ट्रांसमिशन होता है

निष्कर्ष (Summary Table):

टॉपिक	विवरण
Security Zones	नेटवर्क को ज़ोन में बाँटकर सुरक्षा बढ़ाना
DMZ	बाहरी और आंतरिक नेटवर्क के बीच का सुरक्षित बफ़र
Internet	असुरक्षित सार्वजनिक नेटवर्क
Intranet	संगठन का सुरक्षित निजी नेटवर्क
VLAN	फिजिकल नेटवर्क पर लॉजिकल सेगमेंटेशन
Security Implications	गलत डिजाइन से सुरक्षा जोखिम बढ़ते हैं
Tunneling	सुरक्षित डेटा ट्रांसमिशन की तकनीक

IP Security (IPSec) – संपूर्ण समाधान हिंदी में

1. परिचय (Overview)

IPSec (Internet Protocol Security) एक नेटवर्क प्रोटोकॉल है जो IP नेटवर्क में डेटा को सुरक्षित बनाने के लिए उपयोग किया जाता है। इसका उद्देश्य है:

- डेटा की गोपनीयता (Confidentiality)
- डेटा की अखंडता (Integrity)
- डेटा की प्रमाणीकरण (Authentication)

IPSec का मुख्य कार्य है IP पैकेट्स को एन्क्रिप्ट करना और यह सुनिश्चित करना कि कोई अनधिकृत व्यक्ति उन्हें पढ़ न सके या उनमें बदलाव न कर सके।

2. आर्किटेक्चर (Architecture of IPSec)

IPSec दो मुख्य भागों में काम करता है:

A. Security Protocols (सुरक्षा प्रोटोकॉल):

1. **AH (Authentication Header)**
    - डेटा की अखंडता और प्रमाणीकरण सुनिश्चित करता है
    - लेकिन एन्क्रिप्शन नहीं करता
2. **ESP (Encapsulating Security Payload)**
    - डेटा को एन्क्रिप्ट करता है
    - प्रमाणीकरण और गोपनीयता दोनों प्रदान करता है

B. Security Associations (SA):

- SA दो नेटवर्क डिवाइसों के बीच एक सिक्योर कनेक्शन स्थापित करता है
- यह तय करता है कि कौन-सा प्रोटोकॉल (AH या ESP), कौन-सा एल्गोरिद्म और कौन-सी कुंजी उपयोग होगी

3. IPsec Modes (मोड्स)

1. **Transport Mode (ट्रांसपोर्ट मोड):**
    - केवल IP पैकेट के **डेटा** को सुरक्षित करता है
    - IP हेडर अपरिवर्तित रहता है
    - उपयोग: एंड-टू-एंड कनेक्शन के लिए
2. **Tunnel Mode (टनल मोड):**
    - पूरा IP पैकेट (डेटा + हेडर) को सुरक्षित करता है
    - एक नया IP हेडर जोड़ा जाता है
    - उपयोग: VPN, गेटवे-टू-गेटवे कनेक्शन

4. IPsec Configuration (कॉन्फ़िगरेशन)

IPSec को निम्नलिखित चरणों के माध्यम से कॉन्फ़िगर किया जाता है:

1. **Policy Setup:**
    - यह तय किया जाता है कि कौन-से ट्रैफ़िक पर IPSec लागू होगा
2. **Key Management:**
    - कुंजियों का आदान-प्रदान किया जाता है
    - आमतौर पर IKE (Internet Key Exchange) प्रोटोकॉल का उपयोग होता है
3. **Security Association (SA):**
    - दोनों पक्षों में SA का निर्माण होता है
4. **Authentication Method:**
    - Pre-shared key या Digital Certificate से प्रमाणीकरण होता है

5. IPsec Security (सुरक्षा विशेषताएँ)

IPSec निम्न सुरक्षा सेवाएं प्रदान करता है:

सेवा	विवरण
Confidentiality	डेटा को एन्क्रिप्ट कर भेजता है, जिससे कोई और नहीं पढ़ सकता
Integrity	डेटा में छेड़छाड़ को रोकता है
Authentication	स्रोत की पहचान को सत्यापित करता है
Anti-Replay Protection	पहले से भेजे गए पैकेट्स को दोबारा इस्तेमाल करने से रोकता है
Access Control	केवल अधिकृत यूज़र्स को नेटवर्क में आने देता है

संक्षिप्त रूप में (Summary Table):

विषय	विवरण
IPSec	IP स्तर पर सुरक्षा प्रदान करने वाला प्रोटोकॉल
प्रोटोकॉल	AH और ESP
मोड	ट्रांसपोर्ट और टनल मोड
कॉन्फ़िगरेशन	पॉलिसी सेटअप, कुंजी प्रबंधन, प्रमाणीकरण
सुरक्षा विशेषताएँ	गोपनीयता, प्रमाणीकरण, अखंडता, एंटी-रीप्ले

Virtual Private Network (VPN) – पूर्ण विवरण हिंदी में

1. परिचय (Introduction)

VPN (Virtual Private Network) एक ऐसी तकनीक है जो सार्वजनिक नेटवर्क (जैसे इंटरनेट) के ऊपर एक **निजी, सुरक्षित नेटवर्क कनेक्शन** प्रदान करती है।

उद्देश्य:

- इंटरनेट के माध्यम से **सुरक्षित संचार** करना
- डेटा को **एन्क्रिप्ट** करके भेजना
- दूरस्थ (Remote) यूज़र्स को निजी नेटवर्क से **जोड़ना**

2. VPN कैसे काम करता है?

VPN एक **"टनल" (Tunnel)** बनाता है जिसमें आपका सारा नेटवर्क ट्रैफिक एन्क्रिप्ट होकर सुरक्षित रूप से गंतव्य तक पहुंचता है।

कार्य प्रणाली:

1. यूज़र VPN सॉफ्टवेयर से कनेक्ट करता है।
2. VPN सर्वर एक सुरक्षित "टनल" बनाता है।
3. सारा डेटा इस टनल से एन्क्रिप्ट होकर गुजरता है।
4. डेटा को डिक्रिप्ट कर गंतव्य तक पहुंचाया जाता है।

3. VPN के प्रकार (Types of VPN)

प्रकार	विवरण
Remote Access VPN	यूज़र्स को घर या अन्य स्थानों से ऑफिस नेटवर्क से जोड़ता है
Site-to-Site VPN	दो या अधिक ऑफिस लोकेशन के नेटवर्क को जोड़ता है
Client-to-Site VPN	उपयोगकर्ता को एक विशेष सर्वर से कनेक्ट करता है
SSL VPN	ब्राउज़र के ज़रिए सुरक्षित कनेक्शन (https) प्रदान करता है

4. VPN टनलिंग प्रोटोकॉल (VPN Tunneling Protocols)

प्रोटोकॉल	कार्य
PPTP (Point-to-Point Tunneling Protocol)	पुराना और तेज़, लेकिन कम सुरक्षित
L2TP/IPSec	सुरक्षा बढ़ाने के लिए दो प्रोटोकॉल का मिश्रण
OpenVPN	सबसे सुरक्षित, ओपन-सोर्स
IKEv2/IPSec	तेज और मोबाइल डिवाइस के लिए उपयुक्त

प्रोटोकॉल	कार्य
SSL/TLS	ब्राउज़र आधारित सुरक्षित कनेक्शन

5. VPN की सुरक्षा विशेषताएं (Security Features)

- **डेटा एन्क्रिप्शन:** ट्रैफिक को छिपा देता है ताकि कोई बीच में पढ़ न सके
- **ट्रैफिक टनलिंग:** इंटरनेट पर एक निजी रास्ते से डेटा भेजना
- **IP Masking:** असली IP छुपाकर दूसरा IP दिखाना
- **Authentication:** केवल अधिकृत यूज़र ही कनेक्ट हो सकता है

6. VPN के लाभ (Advantages of VPN)

सार्वजनिक Wi-Fi पर सुरक्षा
लोकेशन छुपाना
प्रतिबंधित वेबसाइट्स तक पहुंच
ऑफिस नेटवर्क को दूर से एक्सेस करना
डेटा चोरी और साइबर अटैक से बचाव

7. VPN की सीमाएँ (Limitations of VPN)

सीमाएँ	विवरण
गति कम हो सकती है	एन्क्रिप्शन के कारण इंटरनेट स्पीड धीमी हो सकती है
कॉन्फ़िगरेशन जटिल हो सकता है	सही तरीके से सेटअप न होने पर सुरक्षा कमजोर हो सकती है
कुछ वेबसाइट VPN ब्लॉक करती हैं	जैसे Netflix या बैंकिंग साइट्स

संक्षिप्त सारांश (Quick Summary Table)

विषय	विवरण
VPN	एक सुरक्षित वर्चुअल नेटवर्क
उपयोग	सुरक्षित कनेक्शन, रिमोट एक्सेस
प्रकार	Remote Access, Site-to-Site, SSL
प्रोटोकॉल	PPTP, L2TP, OpenVPN, IKEv2
लाभ	सुरक्षा, गोपनीयता, इंटरनेट फ्रीडम
सीमाएँ	धीमी गति, कॉन्फ़िगरेशन कठिन

ईमेल सुरक्षा (Email Security) – सम्पूर्ण समाधान हिंदी में

1. ईमेल सुरक्षा का परिचय (Introduction to Email Security)

ईमेल आज के समय में संचार का सबसे प्रमुख माध्यम है, लेकिन इसके साथ ही यह **साइबर हमलों, स्पैम, फिशिंग, डेटा चोरी** जैसे खतरों का शिकार भी बन सकता है।
इसलिए **ईमेल की गोपनीयता, अखंडता और प्रमाणीकरण** को सुनिश्चित करने के लिए ईमेल सुरक्षा आवश्यक है।

2. SMTP (Simple Mail Transfer Protocol)

कार्य सिद्धांत:

- SMTP एक **एप्लिकेशन लेयर प्रोटोकॉल** है जो ईमेल भेजने के लिए उपयोग होता है।
- यह **क्लाइंट-सर्वर मॉडल** पर काम करता है।
- ईमेल भेजने वाले सर्वर से प्राप्तकर्ता के मेल सर्वर तक संदेश भेजता है।

सीमाएँ:

- SMTP **डिफॉल्ट रूप से एन्क्रिप्शन प्रदान नहीं करता**।
- प्रमाणीकरण और गोपनीयता की कमी।

➡ इसलिए इसके साथ अन्य **सुरक्षा प्रोटोकॉल** (जैसे SSL/TLS) और ईमेल सुरक्षा स्टैंडर्ड्स का उपयोग किया जाता है।

3. ईमेल सुरक्षा मानक (Email Security Standards)

3.1. PEM (Privacy Enhanced Mail)

उद्देश्य: ईमेल के लिए गोपनीयता और प्रमाणीकरण
विशेषताएं:

- मैसेज को एन्क्रिप्ट करता है (DES एल्गोरिदम)
- डिजिटल सिग्नेचर द्वारा प्रमाणीकरण
- MIME का उपयोग नहीं करता

सीमा: जटिलता और सीमित समर्थन

3.2. PGP (Pretty Good Privacy)

उद्देश्य: ईमेल की गोपनीयता, अखंडता और प्रमाणीकरण
तकनीक:

- **हाइब्रिड क्रिप्टोग्राफी:**

- डेटा को **Symmetric key (AES)** से एन्क्रिप्ट किया जाता है
- Symmetric key को **Receiver के Public Key** से एन्क्रिप्ट किया जाता है

- **डिजिटल सिग्नेचर** के लिए हैशिंग और Asymmetric key

लाभ:

- मजबूत सुरक्षा
- डिजिटल सिग्नेचर
- फाइल एन्क्रिप्शन

सीमा: कॉन्फ़िगरेशन जटिल, शुरुआती यूज़र के लिए कठिन

3.3. S/MIME (Secure/Multipurpose Internet Mail Extensions)

उद्देश्य: MIME आधारित ईमेल की सुरक्षा
प्रमुख विशेषताएं:

- **एन्क्रिप्शन और डिजिटल सिग्नेचर**
- X.509 डिजिटल सर्टिफिकेट्स का प्रयोग
- ईमेल संलग्नकों (Attachments) की सुरक्षा

लाभ:

- व्यापक रूप से समर्थित (Outlook, Thunderbird आदि)
- Enterprise में लोकप्रिय

सीमा: सर्टिफिकेट मैनेजमेंट जटिल

4. स्पैम (Spam)

क्या है स्पैम?

- **अनचाहे ईमेल संदेश** जो बिना अनुमति के भेजे जाते हैं।
- अक्सर **विज्ञापन, फिशिंग, मालवेयर** आदि का स्रोत होते हैं।

स्पैम से सुरक्षा उपाय:

- **स्पैम फिल्टर** का प्रयोग (जैसे Gmail filters)
- **ब्लैकलिस्ट/व्हाइटलिस्ट** बनाना
- फिशिंग लिंक और संदिग्ध अटैचमेंट से बचाव
- **DKIM, SPF, DMARC** जैसे DNS आधारित सुरक्षा तंत्र का प्रयोग

5. डिजिटल हस्ताक्षर (Digital Signature) का उपयोग

- प्रेषक की **पहचान सत्यापित** करता है

- मैसेज की **अखंडता सुनिश्चित** करता है
- **क्रिप्टोग्राफिक हैश** और **प्राइवेट की** का प्रयोग होता है

6. संक्षिप्त सारांश (Quick Summary Table)

विषय	विवरण
SMTP	ईमेल भेजने का प्रोटोकॉल, सुरक्षा सीमित
PEM	पुराना ईमेल सुरक्षा मानक, DES आधारित
PGP	हाइब्रिड एन्क्रिप्शन, डिजिटल सिग्नेचर
S/MIME	MIME आधारित ईमेल सुरक्षा, डिजिटल सर्टिफिकेट
स्पैम	अनचाहे ईमेल, स्पैम फिल्टर आवश्यक
डिजिटल सिग्नेचर	प्रमाणीकरण और अखंडता के लिए

Lecture 5

Web Security

एप्लिकेशन हार्डनिंग, पैचिंग और वेब सर्वर सुरक्षा (हिंदी में सम्पूर्ण समाधान)

1. एप्लिकेशन हार्डनिंग (Application Hardening)

परिभाषा:

एप्लिकेशन हार्डनिंग एक **सुरक्षा तकनीक** है जिसका उद्देश्य सॉफ़्टवेयर या एप्लिकेशन को **कमजोरियों (vulnerabilities)** से बचाना होता है। यह एप्लिकेशन को **हैकिंग, मैलवेयर, और साइबर हमलों** से सुरक्षित करता है।

प्रमुख उपाय:

1. **अवांछित फीचर्स बंद करना** – जैसे डिफॉल्ट अकाउंट्स, पुरानी APIs
2. **सुरक्षित कोडिंग प्रथाएं** अपनाना
3. **इनपुट वैलिडेशन** – SQL Injection, XSS से बचाव
4. **डिबगिंग और लॉगिंग बंद करना** प्रोडक्शन में
5. **एन्क्रिप्शन का प्रयोग** करना (डेटा और ट्रैफिक दोनों)
6. **फायरवॉल और IDS/IPS का समावेश**

2. एप्लिकेशन पैचेस (Application Patches)

परिभाषा:

पैचेस सॉफ्टवेयर के लिए छोटे **अपडेट्स या सुधार** होते हैं जो **बग्स, कमजोरियों और सुरक्षा दोषों** को ठीक करते हैं।

प्रकार:

- **सिक्योरिटी पैचेस:** सुरक्षा खामियों को बंद करना
- **बग फिक्सेस:** लॉजिक या कोड त्रुटियों को ठीक करना

- **फीचर अपडेट्स:** नई सुविधाएं जोड़ना

महत्व:

- डेटा लीक से सुरक्षा
- मैलवेयर, वायरस से बचाव
- एप्लिकेशन स्थिरता में सुधार

यदि पैच नहीं किया जाए:

- एप्लिकेशन हैक हो सकता है
- जीरो-डे अटैक संभव है
- गोपनीय डेटा चोरी हो सकता है

3. वेब सर्वर (Web Servers)

परिभाषा:

वेब सर्वर एक **सॉफ्टवेयर या हार्डवेयर सिस्टम** है जो **HTTP/HTTPS अनुरोधों** को संभालता है और **वेब पेज** प्रदान करता है।

लोकप्रिय वेब सर्वर:

- Apache
- NGINX
- Microsoft IIS
- LiteSpeed

वेब सर्वर की सुरक्षा के उपाय:

1. **SSL/TLS एन्क्रिप्शन** लागू करना
2. **डिफॉल्ट सेटिंग्स बदलना** (जैसे पोर्ट, इंडेक्स फाइल)
3. **डायरेक्टरी ब्राउज़िंग बंद करना**
4. **फायरवॉल और Web Application Firewall (WAF)** लगाना
5. **लॉगिंग और मॉनिटरिंग** चालू रखना
6. **रूट एक्सेस सीमित करना**

4. Active Directory – परिचय (Active Directory – Introduction)

परिभाषा:

Active Directory (AD) माइक्रोसॉफ्ट द्वारा बनाया गया एक **डायरेक्टरी सर्विस सिस्टम** है जो नेटवर्क में **यूज़र्स, कंप्यूटर्स, ग्रुप्स और अन्य संसाधनों** को संगठित करता है।

प्रमुख कार्य:

- उपयोगकर्ता प्रमाणीकरण (Authentication)
- संसाधन प्रबंधन (Resource Access)
- Group Policies लागू करना
- SSO (Single Sign-On)

संरचना:

- **Domain:** AD का मूल घटक
- **Organizational Units (OU):** उप-समूह
- **Forest और Tree:** मल्टी-डोमेन नेटवर्क संरचना

सुरक्षा के दृष्टिकोण से लाभ:

- केंद्रीकृत यूज़र प्रबंधन
- पासवर्ड नीति नियंत्रण
- एक्सेस कंट्रोल (ACLs)
- लॉगिंग और ऑडिटिंग

संक्षिप्त सारांश तालिका:

विषय	विवरण
एप्लिकेशन हार्डनिंग	एप्लिकेशन को सुरक्षित और कठोर बनाना
एप्लिकेशन पैचेस	कमजोरियों को दूर करने वाले अपडेट्स
वेब सर्वर	HTTP अनुरोधों को संभालने वाला सिस्टम
Active Directory	नेटवर्क संसाधनों का केंद्रीकृत प्रबंधन

वेब सुरक्षा खतरों और उपायों का संपूर्ण समाधान (हिंदी में)

1. वेब सुरक्षा खतरे (Web Security Threats)

खतरा	विवरण
मैलवेयर अटैक	वायरस, वर्म्स, ट्रोजन आदि से सिस्टम को नुकसान
फिशिंग (Phishing)	नकली वेबसाइट या ईमेल से पासवर्ड चुराना
SQL Injection	इनपुट फील्ड से डेटाबेस तक अवैध एक्सेस
Cross-Site Scripting (XSS)	वेबसाइट पर दुर्भावनापूर्ण स्क्रिप्ट डालना
Man-in-the-Middle Attack	दो पक्षों के बीच डेटा चुराना या बदलना
DDoS (Distributed Denial of Service)	वेबसाइट को ठप करना

2. वेब ट्रैफिक सुरक्षा के उपाय (Web Traffic Security Approaches)

1. **HTTPS (SSL/TLS के साथ)**
2. **VPN (Virtual Private Network)**
3. **Firewall और Web Application Firewall (WAF)**
4. **Data Encryption**
5. **Intrusion Detection Systems (IDS)**
6. **Authentication और Access Control**

3. Secure Socket Layer (SSL) और Transport Layer Security (TLS)

परिभाषा:

SSL और TLS वेब ब्राउज़र और वेब सर्वर के बीच **सुरक्षित संचार** सुनिश्चित करते हैं।

कार्य:

- डेटा एन्क्रिप्शन
- सर्वर और क्लाइंट प्रमाणीकरण
- डेटा की अखंडता (Integrity)

प्रमुख लाभ:

- सुरक्षित लॉगिन और ट्रांजैक्शन
- ई-कॉमर्स सुरक्षा
- गोपनीयता बनाए रखना

नोट: **TLS** अब SSL का उन्नत संस्करण है। वर्तमान में **TLS 1.3** सबसे सुरक्षित प्रोटोकॉल है।

4. Secure Electronic Transaction (SET)

परिभाषा:

SET एक **ई-कॉमर्स ट्रांजैक्शन सुरक्षा प्रोटोकॉल** है जिसे Visa और MasterCard ने डिजाइन किया है।

उद्देश्य:

- क्रेडिट कार्ड ट्रांजैक्शन को सुरक्षित बनाना
- उपभोक्ता, व्यापारी और बैंक के बीच प्रमाणीकरण
- डेटा एन्क्रिप्शन के माध्यम से गोपनीयता बनाए रखना

तकनीकी उपयोग:

- **डिजिटल सर्टिफिकेट**

- **पब्लिक की इनक्रिप्शन**
- **डिजिटल हस्ताक्षर**

5. सॉफ्टवेयर डिवेलपमेंट में सुरक्षा (Secure Software Development)

सिक्योर कोडिंग तकनीक (Secure Code Techniques)

तकनीक	विवरण
Input Validation	यूज़र इनपुट की जाँच
Output Encoding	XSS और Injection से सुरक्षा
Error Handling	डिटेल्स लीक न हों
Authentication & Session Management	मजबूत पासवर्ड, सेशन टाइमआउट

बफर ओवरफ्लो (Buffer Overflow)

परिभाषा:
जब एक प्रोग्राम डेटा को किसी बफर की सीमा से अधिक लिखता है, तो यह **बफर ओवरफ्लो** होता है।

खतरे:

- कोड का गलत एक्सेक्यूशन
- मैलवेयर रन होने की संभावना

उपाय:

- भाषा स्तर पर सुरक्षित फ़ंक्शंस (जैसे strncpy)
- बाउंड चेकिंग
- ASLR, DEP जैसी सुरक्षा तकनीकें

कोड इंजेक्शन (Code Injection)

परिभाषा:
जब अटैकर **खतरनाक कोड** को इनपुट के माध्यम से एप्लिकेशन में इंजेक्ट करता है।

प्रकार:

- SQL Injection
- Command Injection
- HTML/JavaScript Injection

रोकथाम:

- Prepared Statements

- Input Sanitization
- सीमित अनुमति

लीस्ट प्रिविलेज (Least Privilege)

सिद्धांत:

यूज़र, एप्लिकेशन या प्रोसेस को **सिर्फ उतनी ही एक्सेस दें, जितनी आवश्यक हो।**

लाभ:

- अंदरूनी खतरे कम होते हैं
- हमलों का प्रभाव सीमित होता है

Good Practices (अच्छी प्रथाएं)

- नियमित कोड रिव्यू
- पैचेस और अपडेट्स लगाना
- लॉग मॉनिटरिंग और अलर्ट्स
- सशक्त पासवर्ड नीतियां
- मल्टी फैक्टर ऑथेंटिकेशन (MFA)

Testing for Security

टेस्ट	उद्देश्य
Static Code Analysis	बिना रन किए कोड की जांच
Dynamic Testing	रन टाइम पर कमजोरियों की पहचान
Penetration Testing	वास्तविक अटैकर की तरह टेस्ट
Vulnerability Scanning	टूल्स द्वारा जोखिमों की पहचान

Lecture 6

It Laws

सूचना सुरक्षा मानक (Information Security Standards)

1. ISO/IEC 27001:

- यह एक अंतरराष्ट्रीय मानक है जो सूचना सुरक्षा प्रबंधन प्रणाली (ISMS) को परिभाषित करता है।
- उद्देश्य: संगठन की सूचना को गोपनीय, सुरक्षित और उपलब्ध बनाए रखना।
- इसमें जोखिम मूल्यांकन, नियंत्रण उपाय और निरंतर सुधार पर बल दिया गया है।

भारत में सूचना सुरक्षा से संबंधित प्रमुख कानून

2. आईटी अधिनियम, 2000 (Information Technology Act, 2000)

उद्देश्य:

- इलेक्ट्रॉनिक लेनदेन को वैधता प्रदान करना।
- साइबर अपराधों की रोकथाम और सजा के प्रावधान करना।
- डेटा सुरक्षा और गोपनीयता सुनिश्चित करना।

मुख्य प्रावधान:

1. **धारा 43:** बिना अनुमति कंप्यूटर/नेटवर्क का उपयोग करने पर क्षतिपूर्ति देनी होगी।
2. **धारा 66:** साइबर अपराध (जैसे हैकिंग) के लिए दंड (3 साल तक की सजा/₹5 लाख जुर्माना)।
3. **धारा 66C:** इलेक्ट्रॉनिक हस्ताक्षर की चोरी।
4. **धारा 66D:** ऑनलाइन धोखाधड़ी और फिशिंग पर दंड।
5. **धारा 67:** अश्लील सामग्री को प्रकाशित या प्रसारित करने पर दंड।
6. **धारा 69:** सरकार को निगरानी, अवरोधन और डिक्रिप्शन का अधिकार।

नवीनतम संशोधन (Latest Amendments):

- **आईटी (मध्यवर्ती दिशा-निर्देश और डिजिटल मीडिया आचार संहिता) नियम, 2021:**
  - सोशल मीडिया प्लेटफॉर्म को अधिक जिम्मेदार बनाना।
  - फेक न्यूज़ और आपत्तिजनक कंटेंट पर रोक।
  - "पहली उत्पत्ति (First Originator)" की जानकारी देना अनिवार्य।
  -

- शिकायत निवारण अधिकारी की नियुक्ति आवश्यक।

3. कॉपीराइट अधिनियम, 1957 (Copyright Act, 1957)

उद्देश्य:

- मूल साहित्यिक, नाट्य, संगीत, कला, और सॉफ्टवेयर आदि के अधिकारों की सुरक्षा।
- किसी भी रचना की नकल या अनाधिकृत उपयोग पर दंड।

संशोधन:

- **2012 का संशोधन:** डिजिटल कॉपीराइट और ऑनलाइन प्लेटफॉर्म पर सामग्री की रक्षा पर बल।

4. पेटेंट अधिनियम, 1970 (Patent Act, 1970)

उद्देश्य:

- नए आविष्कारों और तकनीकी विकास को कानूनी सुरक्षा प्रदान करना।
- कोई भी व्यक्ति जो नया और उपयोगी आविष्कार करता है, वह पेटेंट प्राप्त कर सकता है।

प्रावधान:

- पेटेंट की वैधता 20 वर्षों तक होती है।
- केवल नवीन, आविष्कारी और औद्योगिक रूप से उपयोगी आविष्कार को ही पेटेंट प्राप्त होता है।

5. बौद्धिक संपदा अधिकार (IPR - Intellectual Property Rights)

मुख्य प्रकार:

- **कॉपीराइट (Copyright)**
- **पेटेंट (Patent)**
- **ट्रेडमार्क (Trademark)**
- **डिज़ाइन अधिकार (Design Rights)**
- **जियोग्राफिकल इंडिकेशन (GI Tag)**

महत्व:

- इन अधिकारों से आविष्कारक/कलाकार/कंपनियों को उनके कार्य का आर्थिक लाभ और कानूनी सुरक्षा मिलती है।

6. साइबर कानून (Cyber Laws in India)

प्रमुख उद्देश्य:

- इंटरनेट और डिजिटल माध्यम में होने वाले अपराधों को रोकना।
- डिजिटल लेनदेन और ऑनलाइन गतिविधियों को वैधानिक सुरक्षा देना।

साइबर अपराधों में शामिल हैं:

- हैकिंग
- साइबर स्टॉकिंग
- फिशिंग
- डाटा चोरी
- डिजिटल धोखाधड़ी

निष्कर्ष (Conclusion):

भारत में सूचना सुरक्षा को मजबूत बनाने के लिए ISO जैसे अंतरराष्ट्रीय मानकों और आईटी अधिनियम जैसे स्थानीय कानूनों की आवश्यकता है। कॉपीराइट, पेटेंट और IPR के माध्यम से सृजनात्मक कार्यों और नवाचारों की रक्षा की जाती है। समय-समय पर कानूनों में संशोधन करके सरकार साइबर अपराधों पर नियंत्रण की दिशा में कार्य कर रही है।

बौद्धिक संपदा कानून (Intellectual Property Law)

परिभाषा:
बौद्धिक संपदा (Intellectual Property - IP) का अर्थ है व्यक्ति की रचनात्मक, नवाचारपूर्ण या बौद्धिक मेहनत से उत्पन्न संपत्ति। इसे कानूनी रूप से संरक्षित किया जाता है जिससे सृजनकर्ता को उसके कार्य पर एकाधिकार (exclusive rights) मिल सके।

प्रमुख प्रकार:

1. कॉपीराइट (Copyright)
2. पेटेंट (Patent)
3. ट्रेडमार्क (Trademark)
4. डिज़ाइन
5. जियोग्राफिकल इंडिकेशन (GI)
6. सॉफ्टवेयर लाइसेंस
7. सेमीकंडक्टर चिप लेआउट डिजाइन

1. कॉपीराइट कानून (Copyright Law)

भारत में लागू:
कॉपीराइट अधिनियम, 1957

क्या संरक्षित होता है:

- साहित्यिक कृति (जैसे किताबें, लेख)
- संगीत, नाटक, कला

- फ़िल्में, फोटोग्राफ्स
- कंप्यूटर सॉफ्टवेयर

कॉपीराइट की अवधि:

- लेखक के जीवन + 60 वर्ष

अधिकार:

- प्रकाशन, वितरण, अनुवाद, प्रदर्शन, रूपांतरण आदि।

उल्लंघन (Infringement):

- बिना अनुमति किसी रचना का उपयोग करना, प्रकाशित करना या पुनरुत्पादन करना।

2012 का संशोधन:

- डिजिटल माध्यम में कॉपीराइट की सुरक्षा।
- म्यूजिक कंपोज़र/लिरिसिस्ट को रॉयल्टी का अधिकार।

2. सॉफ्टवेयर लाइसेंस (Software License)

परिभाषा:
सॉफ्टवेयर लाइसेंस एक कानूनी समझौता है, जो उपयोगकर्ता को सॉफ्टवेयर के उपयोग, वितरण और संशोधन के अधिकार देता है।

मुख्य प्रकार:

1. **प्रोपाइएटरी लाइसेंस (Proprietary License):**
    - उपयोगकर्ता केवल लाइसेंस के अनुसार सॉफ्टवेयर का उपयोग कर सकता है, सोर्स कोड बंद होता है।
    - उदाहरण: Microsoft Windows
2. **ओपन सोर्स लाइसेंस (Open Source License):**
    - उपयोगकर्ता को सोर्स कोड देखने, संशोधित करने और साझा करने की अनुमति होती है।
    - उदाहरण: Linux, Apache License
3. **फ्रीवेयर/शेयरवेयर:**
    - उपयोग मुफ्त में किया जा सकता है, लेकिन यह ओपन सोर्स नहीं होता।

भारत में कानूनी सुरक्षा:
आईटी अधिनियम, 2000 और कॉपीराइट अधिनियम, 1957 के तहत सॉफ्टवेयर को साहित्यिक कृति के रूप में संरक्षित किया जाता है।

3. सेमीकंडक्टर चिप लेआउट डिजाइन कानून (Semiconductor Law)

भारत में लागू:
"सेमीकंडक्टर इंटीग्रेटेड सर्किट लेआउट-डिज़ाइंस अधिनियम, 2000"

प्रमुख बिंदु:

- सेमीकंडक्टर चिप के लेआउट डिजाइन की संरचना को संरक्षित करता है।
- डिजाइन नवीन, मूल और वाणिज्यिक रूप से उपयोगी होनी चाहिए।
- पंजीकरण के बाद 10 वर्षों तक सुरक्षा मिलती है।

उद्देश्य:

- इलेक्ट्रॉनिक इंडस्ट्री के नवाचार को बढ़ावा देना।
- डिजाइन की नकल या अनधिकृत उपयोग को रोकना।

4. पेटेंट कानून (Patent Law)

भारत में लागू:
भारतीय पेटेंट अधिनियम, 1970 (संशोधन: 2005 में WTO के TRIPS समझौते के अनुसार)

परिभाषा:
पेटेंट एक कानूनी अधिकार है जो किसी नवीन, उपयोगी और आविष्कारी प्रक्रिया या उत्पाद के निर्माता को एक निश्चित अवधि तक विशेष अधिकार देता है।

पेटेंट योग्य आविष्कार की विशेषताएं:

1. नवीनता (Novelty)
2. आविष्कारी कदम (Inventive Step)
3. औद्योगिक उपयोगिता (Industrial Application)

पेटेंट की वैधता:

- 20 वर्ष (भारत और अंतरराष्ट्रीय स्तर पर)

जो पेटेंट नहीं हो सकते:

- प्राकृतिक सिद्धांत, गणितीय सूत्र, चिकित्सा पद्धति, पारंपरिक ज्ञान आदि।

पेटेंट उल्लंघन पर दंड:

- अनधिकृत उत्पादन, उपयोग, बिक्री पर कानूनी कार्रवाई।