वायरलैस तथा मोबाइल कम्प्यूटिंग (Wireles and Mobile Computing):

Wireless का अर्थ है किसी computing device (जैसे कि PDA) तथा data source (जैसे कि database server) के बीच बिना physical connection के information को transfer करना। सभी wireless युक्तियाँ mobile नहीं होती।

Mobile का अर्थ है कि किसी computing कार्य को एक स्थान पर स्थिर रहकर ना करना। Mobile device PDA, Smartphone, Laptop इत्यादि हो सकते है और mobile computing के लिए network से connect होना आवश्यक नहीं है।

अत: wireless communication बिना landline को use किये गए data communication को कहा जाता है जबकि mobile (या untethered) computing का अर्थ यह है कि computing device base या center network से लगातार connect नहीं है।

Wireless communication is simply data connection without the use of landlines. Mobile computing means that the computing device is not continuously connected to base or network.

Wireless तथा mobile computing हेतु विभिन्न प्रकार की technology use की जाती है जैसे कि GSM, CDMA, WLL, 3G या Edge, SMS, e-mail, video conferencing etc.

. नैटवर्क सिक्योरिटी (Network Security):

Networking आपके को कई प्रकार की possibilities (अवसर) एवं सुविधाएँ प्रदान करती है। किन्तु इसमें कई प्रकार के risk भी जुड़े है। अत: संवेदनशील कार्य हेतु यह आवश्यक होता है कि केवल अधिकृत user तथा program ही database को access कर सके। अत: network security के अन्तर्गत कई प्रकार की mechanism implement की जाती है जैसे कि authorization, authantication, smart card, biometric, firewall इत्यादि।

Network security के अन्तर्गत विभिन्न प्रकार की समस्याएं उत्पन्न होती है—

1. Physical Security Holes—इसके अन्तर्गत वह समस्याऐ आती है जिसमें कोई व्यक्ति अनधिकृत रूप से computer में access प्राप्त कर लेता है और size के साथ छेड़छाड़ (tampering) करता है। Hackers इस प्रकार की tampering करने के लिए password को guess कर लेते है।

2. Software Security Holes—सही तरीके से नहीं लिखे गए programs (body written programs) या किसी को फायदा पहुँचाने के लिए लिखे गए programs (privileged software) के कारण ये समस्याऐं उत्पन्न होती है।

3. Inconsistent Usage Holes—जब system administrator hardware तथा software के combination को use करता है जिससे system में insecurity उत्पन्न हो जाती है।

Cookies, Hackers and Crackers—Cookies एक विशेष प्रकार की messages होती है जो web server, web browser को transfer करता है तथा web server इनके द्वारा किसी website पर user की गतिविधियों को trap कर सकता है।

Cookie message web server द्वारा web browser को दी जाती है browser इस message को एक text message में save कर लेता है, जब भी browser server से किसी page की request करता है तो ये message server को भेज दी जाती है।

Cookies are messages that a web server transmits to the web browser so thatthe web server can keep track of user activity on a specific website.

Hacker वह computer enthusiast होते है जो computer को सिखने का शौक रखते है जो programmers इन programs का इस्तेमाल नकारात्मक कार्य मे करते हैं crackers कहलाते हैं।

Protection Methods

1. **Authorization**—इसके अन्तर्गत यह देखा जाता है कि user को किसी web service को use करने की अनुमति प्राप्त है कि नहीं। इसके लिए user को एक login ID दी जाती है।
2. **Authentication**—Authentication का अर्थ password protection से है जब तक user valid password नहीं डालेगा तब तक उसे network में entry नहीं मिलेगी।
3. **Biometric methods** अर्थात् finger prints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, DNA इत्यादि।
4. **Firewall** अर्थात् system को protect करना।

Firewall—सामान्य शब्दों में एक ऐसी दीवार जो आग को फैलने से बचाती है। Firewall कहलाती है। Computer की भाषा में firewall एक ऐसा network होता है जो किसी network या system को unauthorised access से सुरक्षा प्रदान करता है। Firewall को hardware, software या दोनों से बनाया जा सकता है। Firewall का use करके internet users की पहुँच को private networks जैसे कि intranet से रोका जा सकता है intranet में प्रवेश करने वाली या बाहर जाने वाली सभी messages को firewall से pass करना होता है। Firewall प्रत्येक message की जाँच करता है तथा जो message सुरक्षा सम्बन्धी शर्तों को पूरा नहीं करती है उनको pass होने से रोक देता है। Firewall को बनाने के लिए विभिन्न तकनीकों का use किया जाता है—

1. Packet filter जिसमें कि network में enter करने वाले या leave करने वाले प्रत्येक packet का निरीक्षण किया जाता है तथा user द्वारा निर्धारित शर्तों द्वारा उसको स्वीकार या अस्वीकार कर दिया जाता है।
2. Application gateways जिनको कि TCP या Telnet servers के लिए use किया जाता है।
3. Circuit level gateways, जिनका कि तब use किया जाता है जब TCP या UDP connection स्थापित किये जाते हैं।
4. Proxy servers जो कि सभी messages को intercept करता है।

Cryptography—किसी code को लिखना तथा solve करना cryptography कहलाता है। Computer की भाषा में cryptography is the study of transforming in order to make it secure from unintended recipients or use अर्थात् सूचना को इस प्रकार transform कर देना तथा कोई unauthorised person उसको use न कर सके cryptography कहलाता है। Cryptography में सूचना को code कर दिया जाता है और यह process encryption कहलाता है।

Cryptography के उद्देश्य—

1. Confidentiality अर्थात् unwanted व्यक्ति उस सूचना को पढ़ या समझ न सके।

2. Integrity अर्थात् information sender तथा receiver के बीच में change न की जा सके।

3. Authentication sender तथा receiver एक दूसरे को पहचान सके।

Key Management—जिस प्रकार ताले को खोलने या बन्द करने के लिए चाबी का use किया जाता है उसी प्रकार सूचना का encryption तथा decryption करने के लिए भी keys का use किया जाता है। जो कि digital form में होती है। इन keys का पता केवल sender तथा user को रहता है। तथा इसलिए अवैध व्यक्ति इन सूचना को नहीं पढ़ सकते। इसके लिए कई प्रकार के cryptographic algorithms का विकास किया गया है। जिनको समय-समय पर test किया जाता है। Cryptographic E-management symmetric asymmetric encryption algorithm पर आधारित होती है। Symmetric algorithm एक ही private key data का encryption तथा decryption करती है। Asymmetric algorithm data public key से encrypt होता है। Private key से decrypt होता है।

Password—Password एक ऐसा secret word होता है जिससे कोई व्यक्ति किसी स्थान पर प्रवेश कर सकता है। Computer की भाषा में password एक character string होता है। जिसमें user किसी system पर अपनी पहुँच बना सकती है। सामान्यत: password 4 से 16 characters के बीच होते हैं तथा password को enter करते समय screen पर display नहीं होते हैं।

एक आसान password व्यक्ति आसानी से याद कर सकता है किन्तु attacker इसका अनुमान आसानी से लगा सकता है। मुश्किल password होने से attacker के लिए उसका अनुमान लगाना मुश्किल हो जाता है। किन्तु user उसे याद नहीं रख पाता और उसे उस password को कहीं न कहीं लिखना या store करना पड़ सकता है जिससे सुरक्षा सम्बन्धी खतरा बन सकता है।

डिजिटल सर्टिफिकेट (Digital Certificate):

Digital certificate एक electronic document होता है जिससे कोई व्यक्ति किसी public key की ownership को सिद्ध करता है। अत: यह एक प्रकार का electronic passport है जो लोगों को या computers को सुरक्षित सूचना आदान-प्रदान करने की अनुमति देता है। Digital signature से यह verify किया जा सकता है कि सूचना देने वाला व्यक्ति वास्तव में सही है। अर्थात् कोई गलत व्यक्ति तो सूचना नहीं भेज रहा है इसकी पहचान digital हस्ताक्षर से लगायी जा सकती है।

यदि कोई व्यक्ति encrypted सूचना भेजना चाहता है तो उसके लिए उसको certificate authority को apply करना पड़ता है। CA उस व्यक्ति को एक encrypted digital certificate प्रदान करता है। जिसमें आवेदक की public key होती है और पहचान सम्बन्धी कुछ अन्य सूचनाएँ भी होती हैं। CA की अपनी public key प्रचार माध्यमों द्वारा या internet पर हमेशा उपलब्ध रहती है। Encrypted message को receive करने वाला व्यक्ति CA की public key को use करके message के साथ attached digital certificate को decode कर लेता है तथा यह confirm कर लेता है कि इसको CA द्वारा ही issue किया गया है तथा sender की public key को प्राप्त करके encrypted सूचना को प्रेषित कर सकता है।

Passoport की तरह ही digital certificate में पहचान सम्बन्धी सूचनाएं होती हैं और एक विश्वसनीय agency द्वारा issue किये जाने के कारण इसका verification भी किया जा सकता है। Digital certificate में certificate holder का नाम, serial no., वैधता तिथि, certificate holder की public key की copy तथा CA के digital signature इत्यादि होते हैं। जिससे certificate की reality सिद्ध हो जाती है। सामान्यत: operating system CA के root certificates की list maintain करते हैं जिससे CA द्वारा issue किये गये certificates की पुष्टि की जाए।

Digital Signature—Digital signature एक mathematical तकनीक है जो किसी digital message या document की genuinity या वैधता को सिद्ध करती है।

एक valid signature से प्राप्तकर्ता को यह तसल्ली हो जाती है कि वास्तव में वही व्यक्ति सूचना भेज रहा है जिसका होने का वह दावा कर रहा है।

अत: digital signature व्यक्ति की पहचान तो सि: करता ही है साथ ही यह भी की प्रेषक बाद में अपने message से पलट नहीं सकता तथा message को रास्ते में भी change नहीं किया जा सकता है। अत: digital signature encryption की तीन शर्तों integrity, authentication तथा non-repudiation को पूरा करता है।

Digital signatures को software वितरण के लिए वित्तीय transaction के लिए, फोरजरी रोकने के लिए, data tampering (data से छेड़छाड़) रोकने के लिए इत्यादि अनुप्रयोगों में use किया जाता है।

Digital signature के लाभ—

1. Digital signature से सूचना के स्रोत की authentication हो जाती है तथा यह सुनिश्चित हो जाता है कि सूचना वैद्य व्यक्ति के द्वारा ही भेजी गयी है। खासकर के वित्तीय लेन-देन में यह स्थिति बहुत महत्व रखती है।
2. Digital signature से सूचना की integrity बरकरार रहती है तथा यह confirm हो जाता है कि रास्ते में सूचना के साथ कोई छेड़छाड़ नहीं हुई है क्योंकि digital signature युक्त सूचना को change करने पर signature invalid हो जाते हैं।
3. Digital signature से non-repudiation का लाभ भी प्राप्त होता है तथा सूचना भेजने वाला बाद में यह इंकार नहीं कर सकता कि सूचना उसके द्वारा नहीं भेजी गयी है।

स्विचिंग तकनीक (Switching Techniques):

Switching तकनीक तीन प्रकार की होती है—

1. Circuit switching 2. Packet switching 3. Message switching

WAN networks में जहाँ दो computers एक साथ direct connected नहीं होते वहाँ दो devices के बीच data transfer path provide करने के लिए switching nodes का network use किया जाता है। एक node से दूसरे node तक data को ले जाने का process data switching कहलाता है।

Circuit switching में sending तथा receiving devices के बीच में dedicated communication path होता है तथा तीन steps का use होता है। Circuit establishment, data transfer तथा circuit termination

यह switching telephone networks में use की जाती है।

Message switching मे sender or receiver के बीच में सीधा path establish नहीं किया जाता है। Sending device message पर address डालकर उसको network को pass कर देता है तथा message कई node से होता हुआ अपनी मंजिल तक पहुँचता है।

Example—E-mail

Packet switching, message switching तथा circuit switching का संयुक्त रूप है इसमें data को blocks के रूप में node by node destination, तक भेजा जाता है। Packet switching की दो विधियाँ होती हैं। Datagram विधि में सभी packets स्वतंत्र रूप से अलग-अलग path से destination तक पहुँचते हैं जहाँ इनको reassemble किया जाता है। Virtual circuit approach में packet को भेजने से पहले ही sender तथा receiver के बीच में एक fix logical path set कर दिया जाता है।

WAN Devices—WAN में switching हेतु तथा data transfer हेतु Routing Technology का use किया जाता है। Routing के द्वारा दो computer के बीच में path search किया जाता है और data packets को इस path के द्वारा forward किया जाता है। इसके लिए कई devices जैसे कि Bridges, Router तथा gateways का use किया जाता है।

Bridges—Bridges की सहायता से दो एक समान वाले protocol वाले LANs को wide area में connect किया जाता है। Bridge address printer की तरह कार्य करती है जो एक LAN से Packet को लेकर दूसरे LAN तक पहुँचती है। Bridges OSI model के data link layer पर operate करती है। चूँकि सभी devices एक ही protocol का use करती है इसलिए bridge पर न्यूनतम processing की आवश्यकता होती है।

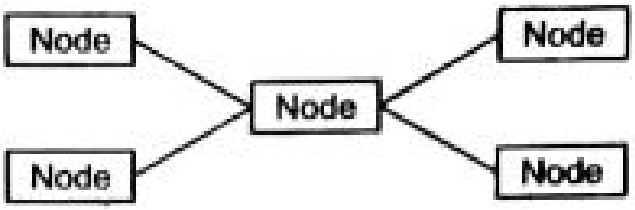
Routers—Routers दो ऐसे network को connect करते हैं जो एक समान नहीं होते है। Routers दो लम्बी दूरी के LANs या WANs के बीच connection स्थापित करते हैं। यह OSI model के network layer पर कार्य करते हैं। Routers sender से receiver के बीच best router की गणना करने में सहायक होते हैं।

Gateways—Gateways दो असमान LANs को connect करते हैं। यह OSI model के application layer पर operate करते हैं। चूँकि यह दो असमान network को connect करते हैं इसलिए data packet को forward करने से पहले यह उसको एक protocol format से दूसरे protocol format पर convert करते हैं।

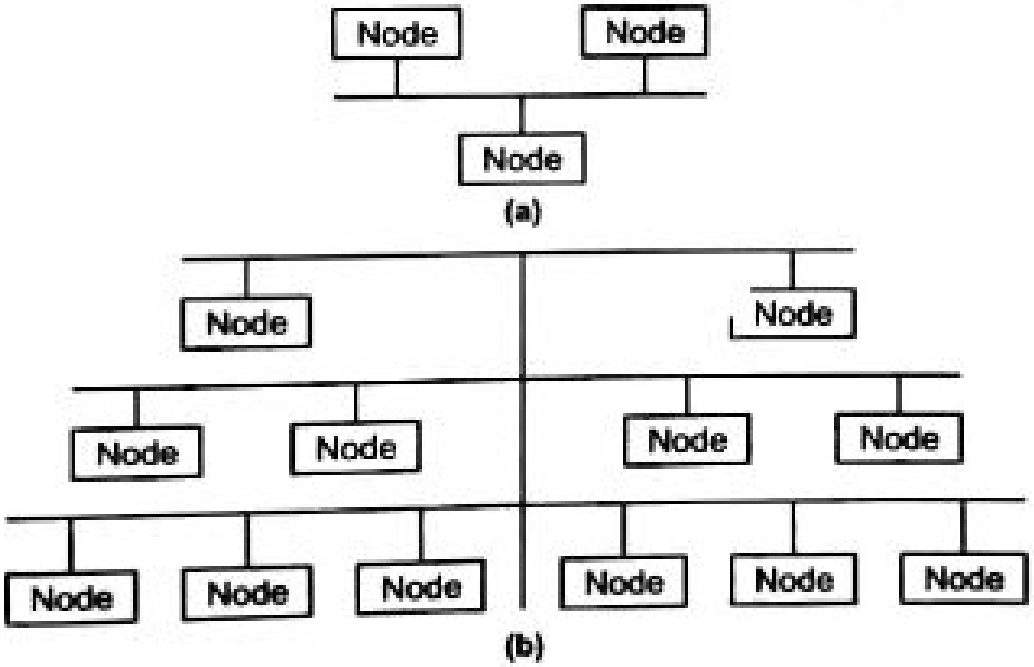
LAN (Local Area Network)—LAN एक data communication network होता है जो कई computers या workstations को connect करता है तथा इनके बीच में data तथा information exchange की सुविधा प्रदान करता है। LANs किसी एक building के अन्दर या building के समूह में स्थापित होते हैं।

Network में devices को connect करने का तरीका network topology कहलाता है। Connection के लिए provided बिन्दु nodes या link station कहलाते हैं। LAN हेतु तीन प्रकार की topologies का use किया जाता है—

1. Star Topology—इसमें कई stations को एक centre station या controller से connect किया जाता है तथा कोई भी node centre controller के माध्यम से दूसरे node को data transfer कर सकती है।



Bus Topology—इसमें सभी station एक single line से connect होते हैं जिसको bus कहते हैं। Information दोनों दिशाओं में carry हो सकती है। Bus से जुड़ा प्रत्येक station information का destination address check करता है। यदि address उस station के address से match करता है तो वह information frame को accept करके उसे process करता है अन्यथा उसे reject कर देता है। Bus topology का विस्तार tree topology कहलाता है। चूँकि bus या tree network में management या control हेतु कोई centre point नहीं होता अत: यह कार्य bus से linked stations के मध्य विभाजित होता है।



Bus network (b) Tree network

Ring Topology—Ring topology में सभी stations एक ring की shape (circular shape) में जुड़े होते हैं। प्रत्येक station information को receive करके ring में transmit करता रहता है। Information एक ही दिशा में travel करती है।