RGPVNOTES.IN

Subject Name: **Wireless & Mobile Computing**

Subject Code: **IT-7003**

Semester: **7th**

Unit 4:

Mobile IP:A standard that allows users with mobile devices whose IP addresses are associated with one network to stay connected when moving to a network with a different IP address.

When a user leaves the network with which his device is associated (home network) and enters the domain of a foreign network, the foreign network uses the Mobile IP protocol to inform the home network of a care-of address to which all packets for the user's device should be sent.

Mobile IP is used in wireless WAN environments where users need to carry their mobile devices across multiple LANs with different IP addresses.

A common example to explain Mobile IP is, if someone moves his residence from one location to another. Person moves from Indore to Bhopal. Person drops off new mailing address to Bhopal post office. Bhopal post office notifies Indore post office of new mailing address. When Indore post office receives mail for person it knows to forward mail to person's Bhopal address

DHCP (Dynamic host configuration protocol)

The dynamic host configuration protocol) isused to simplify the installation and maintenance of networked computers.If a new computer is connected to a network, DHCP can provide it with all thenecessary information for full system integration into the network, e.g., addressesof a DNS server and the default router, the subnet mask, the domain name, and anIP address. DHCP is based on a client/server model. DHCPclients send a request to a server (DHCPDISCOVER in the example) to whichthe server responds. A client sends requests using MAC broadcasts to reach alldevices in the LAN. A DHCP relay mightbe needed to forward requests acrossinter-working units to a DHCP server. The dynamichost con figuration protocol ismainly used to simplify the installation and maintenance of networked computers. If a new computer is connected to a network, DHCP can provide it with all thenecessary information for full system integration in to the network, e.g., addressesof a DNS server an d the default router, the subnet m ask, the domain n am e, an d anIP address. Providing an IP address, makes DHCP very attractive for mobile IP as asource of care-of-addresses.

DHCP is based on a client/ server model. DHCPclients send a request to a server (DHCPDISCOVER in the example) to whichthe server responds. A client sends requests u sin g MAC broadcasts to reach alldevices in the LAN. A DHCP relay might be needed to forward requests acrossinter-working units to a DHCP server.)

Characteristics of Ad Hoc Networks

The MANET working group has defined some unique propertiesof ad hoc networks. The propertiesdoes not directly relate to performance.

In a manner, they affect performance, since theygreatly affect on the design of ad hoc routing protocols.The following characteristics of Ad-hoc networks are defined:

1. Dynamic topologies

Nodes can move arbitrarily with respectto other nodes in the network.

2. Bandwidth-constrained

Nodes in an ad hoc network are mobile. Thus, they areusing radio links that have far lower capacity than hardwiredlinks could use.

3. Energy constrained operation

Mobile nodes are likely to rely on batteries. That is whythe primary design criteria may sometimes be energyconservation.

4. Limited physical security

The radio networks are vulnerable to physicalsecurity threats compared to fixed networks. The possibilityof eavesdropping, spoofing and DoS attacks ishigher. Existing link security techniques can be applied.However, a single point failure in an ad hoc network isnot as crucial as in more centralized networks.

Performance Issues in Ad Hoc Networks

To judge the merit of a routing protocol, one needs metrics which both qualitative and quantitative to measure its suitability and performance. These metrics should be independent of any given routing protocol.

Qualitative properties of MANET routing protocols:

- Distributed operation: This is an essential property, but it should be stated nonetheless.
- Loop-freedom: It is not required for certain quantitative measures (i.e. performance criteria), but generally desirable to avoid problems such as worst-case phenomena, e.g. a small fraction of packets spinning around in the network for arbitrary time periods. Ad hoc solutions such as TTL values can bound the problem, but a more structured and well-formed approach is generally desirable as it usually leads to better overall performance.
- Demand-based operation: Instead of assuming an uniform traffic distribution within the network (and maintaining routing between all nodes at all times), let the routing algorithm adapt to the traffic pattern on a demand or need basis. If this is done intelligently, it can utilize network energy and bandwidth resources more efficiently, at the cost of increased route discovery delay.

- Proactive operation: The flip-side of demand-based operation. In certain contexts, the additional latency demand-based operation incurs may be unacceptable. If bandwidth and energy resources permit, proactive operation is desirable in these contexts.
- Security: Without some form of network-level or link-layer security, a MANET routing protocol is vulnerable to many forms of attack. It may be relatively simple to snoop network traffic, replay transmissions, manipulate packet headers, and redirect routing messages, within a wireless network without appropriate security provisions. While these concerns exist within wired infrastructures and routing protocols as well, maintaining the "physical" security of the transmission media is harder in practice with MANETs. Sufficient security protection to prohibit disruption of modification of protocol operation is desired.
- Sleep period operation: As a result of energy conservation, or some other need to be inactive, nodes of a MANET may stop transmitting and/or receiving (even receiving requires power) for arbitrary time periods. A routing protocol should be able to accommodate such sleep periods without overly adverse consequences. This property may require close coupling with the link-layer protocol through a standardized interface.
- Unidirectional link support: Bidirectional links are typically assumed in the design of routing algorithms, and many algorithms are incapable of functioning properly over unidirectional links. Nevertheless, unidirectional links can and do occur in wireless networks. Oftentimes, a sufficient number of duplex links exist so that usage of unidirectional links is of limited added value.However, in situations where a pair of unidirectional links (in opposite directions) form the only bidirectional connection between two ad hoc regions, the ability to make use of them is valuable.
- End-to-end data throughput and delay: Statistical measures of data routing performance (e.g., means, variances, distributions) are important. These are the measures of a routing policy's effectiveness i.e.., how well it does its job as measured from the external perspective of other policies that make use of routing.
- Route Acquisition Time: A particular form of external end-to-end delay measurement of particular concern with "on demand" routing algorithms which is the time required to establish route(s) when requested.
- Percentage Out-of-Order Delivery: An external measure of connectionless routing performance of particular interest to transport layer protocols such as TCP which prefer in-order delivery.
- Efficiency: If data routing effectiveness is the external measure of a policy's performance, efficiency is the internal measure of its effectiveness. To achieve a given level of data routing performance, two different policies can expend differing amounts of overhead, depending on their internal efficiency. If control and data traffic must share the same channel, and the channel's capacity is limited, then excessive control traffic often impacts data routing performance. It is useful to track several ratios that illuminate the internal efficiency of a protocol in doing its job (there may be others that the authors have not considered).
- Average number of data bits transmitted/data bit delivered: This can be thought of as a measure of the bit efficiency of delivering data within the network. Indirectly, it also gives the average hop count taken by data packets.
- Average number of control bits transmitted/data bit delivered: This measures the bit efficiency of the protocol in expending control overhead to delivery data. Note that this should include not only the bits in the routing control packets, but also the bits in the header of the data packets. In other words, anything that is not data is control overhead, and should be counted in the control portion of the algorithm.
- Average number of control and data packets transmitted/data packet delivered: Rather than measuring pure algorithmic efficiency in terms of bit count, this measure tries to capture a protocol's channel access efficiency, as the cost of channel access is high in contention-based link layers .
- In networking context, the essential parameters that should be varied include:
- Network size: Measured in the number of nodes.

- Network connectivity: The average degree of a node (i.e. the average number of neighbors of a node).
- Topological rate of change: The speed with which a network's topology is changing
- Link capacity: Effective link speed measured in bits/second, after accounting for losses due to multiple access, coding, framing, etc.
- Fraction of unidirectional links: How effectively does a protocol perform as a function of the presence of unidirectional links?
- Traffic patterns: How effective is a protocol in adapting to non-uniform or busty traffic patterns?
- Mobility: When and under what circumstances, is temporal and spatial topological correlation relevant to the performance of a routing protocol?

Routing In Mobile Host

wireless networks with infrastructure support a base station always reaches all mobile nodes, this is not always the case in an ad-hoc network. Adestination node might be out of range of a source node transmitting packets. Routing is needed to find a path between source and destination and to forward the packets appropriately. In wireless networks using an infrastructure, cellshave been defined. Within a cell, the base station can reach all mobile nodeswithout routing via a broadcast. In the case of ad-hoc networks, each node mustbe able to forward data for other nodes.

These are the basic algorithms for routing in mobile host.

- Link state: In link-state,routing each router first obtains a view of the complete topology of the network with a cost for each link and then computes the shortest path to every other router by using, for instance, Dijkstra's algorithm.
- Distance vector: In distance vector, every node only monitors the cost of its outgoing links and periodically broadcasts an estimation of the shortest distance to every other node in the network. The receiving nodes then use this information to recalculate the routing tables.
- Source routing: In source, routing each packet carries the complete path it has to follow around the network, which requires great overhead if the route has many hops. Given that the routing decision is made at the source, it is easy to avoid routing loops.

Wireless Sensor Network

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. A WSN system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes. The selection of wireless protocol depends on the application requirements. Some of the available standards include 2.4 GHz radios based on either IEEE 802.15.4 or IEEE 802.11 (Wi-Fi) standards or proprietary radios, which are usually 900 MHz.

Transport Layer

Supporting mobility only on lower layers up to the network layer is notenough to provide mobility support for applications. Most applicationsrely on a transport layer, such as TCP (transmission control protocol) or UDP (user datagram protocol) in the case of the internet. Two functions of thetransport layer in the internet.Two functions of the transport layer in the internet are check summing over user data and multiplexing/de-multiplexing of data from/to applications.

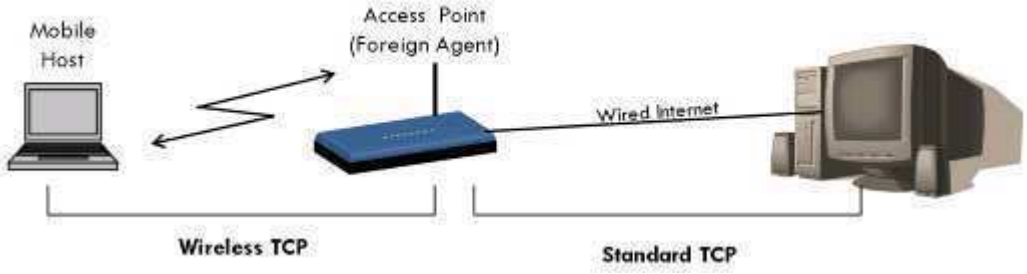

Figure 28: Indirect TCP segments a TCP connection into two parts

The above figure shows a mobile host connected via a wireless link to an access point (AP). Also access node is connected to the internet via the wired Internet.Standard TCP is used to connect to the AP from fixed computer. No computer over the internet recognizes any change to the TCP.The Access point acts as a proxy of mobile host and terminates the TCP connection.Therefore, the fixed computer now sees the AP as mobile host; on other hand, the mobile host sees AP as the fixed computer.In between the AP and the mobile host, a special TCP adapted to wireless links is used.A change is TCP is not needed as even as unchanged TCP produces the same round trip time.Such segmentation methods can be used is connection between mobile node and correspondent host when host is at the FA. Therefore, during handover, control transfers from one FA to another FA in the nearby cell.

Advantages of I-TCP:

- I-TCP does not require any changes in TCP protocol as used by the different hosts in network.
- Because of a strict partition between the two connections, transmission error on the wireless link will not propagate to the wired link. Therefore, flow will always be in a sequence.
- The delay between the FA and Mobile host is small and if optimized properly, precise time-outs can be used to carry out retransmission of lost packets.
- Different solutions can be implemented ad tested between the FA and mobile host without jeopardizing the stability of the internet.
- With two partitions, we can use a different transport layer protocol in the second half with the FA acting as a translator.

Disadvantages of I-TCP:

- The end-to-end connection for which TCP has been designed will fail if the Foreign Agent (FA) crashes.
- The foreign agent (FA) must be a trusted entity as the TCP connections end at this point.
- Increased handover may latency may be much more problematic. (During handover from old FA to new FA, some delay will occur. During this period, some extra data will come at old FA. This data also needs to be send)

Snoop-TCP

One of the main feature of I-TCP also goes on to become its major disadvantage i.e. segmentation of TCP. To overcome it but also to provide enhanced feature a new TCP was designed which worked completely transparent and also left the TCP end-to-end connection intact.The new idea for making an enhancement is to buffer the data close to the mobile host to perform fast local retransmission in case of packet loss. A good place tocarry out this enhancement is at the foreign agent (FA).

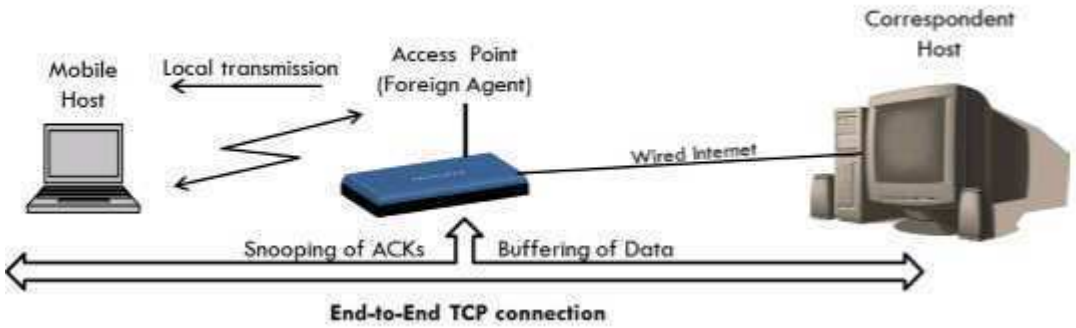

Figure 29: Snooping TCP as a transparent TCP extension

Methodfor Snoop-TCP

The foreign agent instead of terminating all packet with destination mobile host, it buffers (i.e. temporarily stores all these packets). It also 'snoops' each packet flowing in both the directions for reading acknowledgements.Buffering towards the mobile host is carried out so that a retransmission can be done in case of missing acknowledgements.The FA buffers every packet until an acknowledgement is received from the mobile host.If the foreign agent does not receive an acknowledgement within the stipulated time, the packet or the acknowledgement has been lost.In such a situation, the FA can directly retransmit the packet without waiting for the correspondent host.

Advantages of Snoop-TCP:

- The original TCP sematic i.e. end-to-end connection is preserved.
- The correspondent node need not be changed as all the new enhancements are made in the FA.
- During handover form on cell to another, there is no need to transfer the previous incoming data (as in I-TCP).
- In handover, the next foreign Agent (FA) need not use the same enhancements used here i.e. follow Snoop-TCP method.

Disadvantages of Snoop-TCP:

- If any encryption is applied at both ends, the snooping and buffering process would be a waste of time as no data can be read by FA.
- Does not fully isolate wireless link error from the fixed network (e.g. problems like congestion and interference may cause a delay in retransmission).
- The Mobile host needs to be modified to handle the NACK signals (No Acknowledgement) for reverse traffic (i.e. from MH to Sender)

Mobile TCP:

The M-TCP splits up the connection into two parts:
An unmodified TCP is used on the Standard host-Supervisory Host section
An optimized TCP is used on the Supervisory Host- Mobile Host section.
The Supervisory Host (SH) adorns the same role as the proxy (Foreign Agent) in I-TCP.The SH is responsible for exchanging data to both the Standard host and the Mobile host.

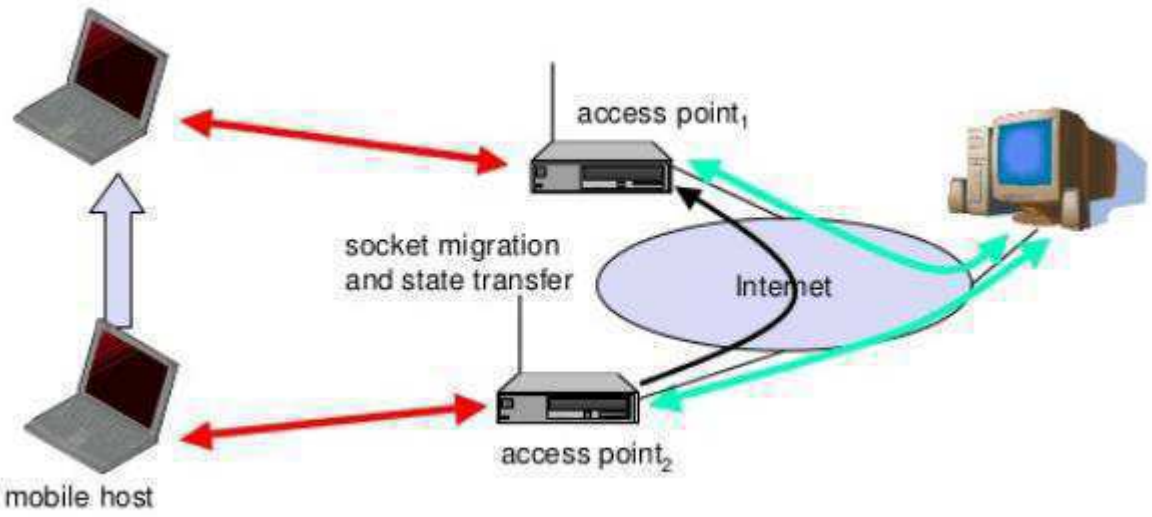

Figure 30: Working of Mobile TCP

Here in this approach, we assume that the error bit rate is less as compared to other wireless links.So if any packet is lost, the retransmission has to occur from the original sender and not by the SH. (This also maintains the end-to-end TCP semantic). The SH monitors the ACKs (ACK means acknowledgement) being sent by the MH. If for a long period ACKs have not been received, then the SH assumes that the MH has been disconnected (maybe due to failure or moved out of range, etc...).If so the SH chokes the sender by setting its window size to 0.Because of this the sender goes into persistent mode i.e. the sender's state will not change no matter how long the receiver is disconnected.

This means that the sender will not try to retransmit the data.Now when the SH detects a connectivity established again with the MH (the old SH or new SH if handover), the window of the sender is restored to original value.

Advantages:

- Maintains the TCP end-to-end semantics. (No failed packet retransmission is done by the SH.All job handled by original sender)
- Does not require the change in the sender's TCP.
- If MH disconnected, it doesn't waste time in useless transmissions and shrinks the window size to 0.
- No need to send old buffer data to new SH in case of handover (as in I-TCP).

Disadvantages:

- M-TCP assumes low bit error which is not always true. So, any packet loss due to bit-errorsoccurring, then its propagated to the sender.
- Modifications are required for the MH protocol software.

Transmission/time-out freezing

In some cases mobile hosts can be disconnected for a longer time therefore no packet exchange possible, e.g., in a tunnel, disconnection due to overloaded cells or mux with higher priority traffic TCP disconnects after time-out completely called freezing.

TCP freezing

MAC layer is often able to detect interruption in advance and MAC can inform TCP layer of upcoming loss of connection then TCP stops sending, but does now not assume a congested link after that MAC layer signals again if reconnected

Advantage

This scheme is independent of data

Disadvantage

TCP on mobile host has to be changed, this mechanism dependson MAC layer

Selective retransmission

TCP acknowledgements are often cumulative. ACK n acknowledges correct and in-sequence receipt of packetsup to n and if single packets are missing quite often a whole packet sequencebeginning at the gap has to be retransmitted (go-back-n) thus wasting bandwidth

Selective retransmission gives a solution

The RFC2018 allows for acknowledgements of single packets, not onlyacknowledgements of in-sequence packet streams without gapsand now sender can now retransmit only the missing packets

Advantage

It provides much higher efficiency

Disadvantage

It is very complex

Transaction oriented TCP

TCP has the following phases

For connection setup, data transmission, connection release theTCP uses 3-way-handshake therefore needs 3 packets for setup and release,respectively thus, even short messages need a minimum of 7 packets, it results in overhead.

Transaction oriented TCP

The RFC1644, T-TCP, describes a TCP version to avoid this overheadIn T-TCP the connection setup, data transfer and connection release can becombined therefore it requires only 2 or 3 packets are needed

Advantage

It is highly efficient

Disadvantage

- It requires changed TCP
- In T-TCP mobility not longer transparent

The following shows the comparison of different approaches for a “mobile” TCP

Approach	Mechanism	Advantages	Disadvantages
Indirect TCP	splits TCP connection into two connections	isolation of wireless link, simple	loss of TCP semantics, higher latency at handover
Snooping TCP	“snoops” data and acknowledgements, local retransmission	transparent for end-to-end connection, MAC integration possible	problematic with encryption, bad isolation of wireless link
M-TCP	splits TCP connection, chokes sender via window size	Maintains end-to-end semantics, handles long term and frequent disconnections	Bad isolation of wireless link, processing overhead due to bandwidth management
Fast retransmit/ fast recovery	avoids slow-start after roaming	simple and efficient	mixed layers, not transparent
Transmission/ time-out freezing	freezes TCP state at disconnect, resumes after reconnection	independent of content or encryption, works for longer interrupts	changes in TCP required, MAC dependant
Selective retransmission	retransmit only lost data	very efficient	slightly more complex receiver software, more buffer needed
Transaction oriented TCP	combine connection setup/release and data transmission	Efficient for certain applications	changes in TCP required, not transparent

Table 7: comparison of different approaches for a “mobile” TCP

Introduction to WAP

WAP stands for Wireless Application Protocol and it is a worldwide standard for providing Internet communications and advanced telephony services on digital mobile phones, pagers, personal digital assistants, and other wireless terminals

- Wireless: Lacking or not requiring a wire or wires pertaining to radio transmission.
- Application: A computer program or piece of computer software that is designed to do a specific task.
- Protocol: A set of technical rules about how information should be transmitted and received using computers.

WAP is the set of rules governing the transmission and reception of data by computer applications on or via wireless devices like mobile phones. WAP allows wireless devices to view specifically designed pages from the Internet using only plain text and very simple black-and-white pictures.

WAP is a standardized technology for cross-platform, distributed computing very similar to the Internet's combination of Hypertext Markup Language (HTML) and Hypertext Transfer Protocol (HTTP), except that it is optimized for:

- low-display capability
- low-memory
- low-bandwidth devices, such as personal digital assistants (PDAs), wireless phones, and pagers.\

WAP specifies architecture based on layers that follows the OSI model fairly closely. The WAP model, or stack as it is commonly known, is illustrated below

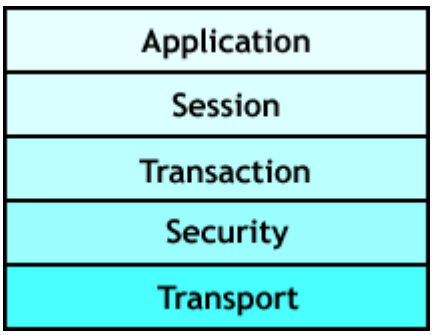

Figure 31: WAP layered architecture

Application Layer

WAP's application layer is the Wireless Application Environment (WAE). WAE directly supports WAP application development with Wireless Markup Language (WML) instead of HTML and WMLScript instead of JavaScript. WAE also includes the Wireless Telephony Application Interface (WTAI, or WTA for short) that provides a programming interface to telephones for initiating calls, sending text messages, and other networking capability.

Session Layer

WAP's session layer is the Wireless Session Protocol (WSP). WSP is the equivalent to HTTP for WAP browsers. WAP involves browsers and servers just like the Web, but HTTP was not a practical choice for WAP because of its relative inefficiency on the wire. WSP conserves precious bandwidth on wireless links; in particular, WSP works with relatively compact binary data where HTTP works mainly with text data.

Transaction, Security, and Transport Layers

There are three protocols in WAP:

- Wireless Transaction Protocol (WTP)
- Wireless Transaction Layer Security (WTLS)
- Wireless Datagram Protocol (WDP)

WTP provides transaction-level services for both reliable and unreliable transports. It prevents duplicate copies of packets from being received by a destination, and it supports retransmission, if necessary, in

cases where packets are dropped. In this respect, WTP is analogous to TCP. However, WTP also differs from TCP. WTP is essentially a pared-down TCP that squeezes some extra performance from the network.

WTLS provides authentication and encryption functionality analogous to Secure Sockets Layer (SSL) in Web networking. Like SSL, WTLS is optional and used only when the content server requires it.

WDP implements an abstraction layer to lower-level network protocols; it performs functions similar to UDP. WDP is the bottom layer of the WAP stack, but it does not implement physical or data link capability. To build a complete network service, the WAP stack must be implemented on some low-level legacy interface not technically part of the model. These interfaces, called bearer services or bearers, can be IP-based or non-IP based.

Statistical anomaly detection: Involves the collection of data relating to thebehavior of legitimate users over a period. Then statistical testsare applied to observed behavior to determine with a high level of confidencewhether that behavior is not legitimate user behavior.

- Threshold detection: This approach involves defining thresholds, independent of user, for the frequency of occurrence of various events.
- Profile based: A profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts.

Rule-based detection: Involves an attempt to define a set of rules that can beused to decide that a given behavior is that of an intruder.

- Anomaly detection: Rules are developed to detect deviation from previous usage patterns.
- Penetration identification: An expert system approach that searches for suspicious behavior.

In practical practice, a systemmay use a combination of both approaches to be effective against a wide rangeof attacks.

Password Management

Password Protection

The front line of defense against intruders is the password. Allthe networks require that a user provide a name or identifier (ID) and a password. The password serves to authenticate the ID of the individual loggingon to the network. The UserID provides security in the following ways:

- The UserID determines whether the user is authorized to gain access to a network. In some networks, only those who already have an ID filed on the networks are allowed to gain access.
- The ID determines the privileges accorded to the user. A few users may have supervisory or administrator status that enables them to read files and perform functions that are especially protected by the system.
- TheUserID is used in what is referred to as discretionary access control. For example, by listing the IDs of the other users, a user may grant permission to them to share files owned by that user.

Password Selection Strategies

Many users choose a password that is too short or too easy to guess. But if users are assigned passwords consisting of eight randomly selected printable characters and encrypted them by some encryption techniques, password cracking is effectively avoided.

To avoid guessable passwords while allowing the user to select a password that is memorable. Four basic techniques are recommended:

- User education: Provide guidelines to user for creating a strong password, although many users will simply ignore the guidelines or may not be good judges of what is a strong password.
- Computer-generated passwords: These passwords are quite random in nature, users will not be able to remember them therefore, it had a history of poor acceptance by users.
- Reactive password checking: In this technique system periodically runs its own password cracker to find guessable passwords and system cancels any passwords that are guessed and notifies the user.However, a user can steal a password file.
- Proactive password checking: In this scheme, the user is allowed to select his or her own password. However, at the time of selection, the system checks to see if the password is allowable and, if not, rejects it and ask for anotherpassword.

The following rules mustenforce for selecting a strong password:

- All passwords must be at least eight or more characters long.
- The passwords must include at least oneuppercase, lowercase, numeric digits, and punctuation marks.

Virus and Related Threats

Virus is a kind of malicious software written with the intention to enter a computer without the user's permission or knowledge, with an ability to copy itself, hence continuing to spread. Some viruses can cause severe harm or adversely affect program and performance of the system.

A virus can onlyspread from one computer to another when its host or file is taken to theuninfected computer, by sending it over anetwork or carrying it on a removable medium such as a floppy diskCD, or USB drive.

Types of Virus

Resident Viruses: This type of virus is a permanent which dwells in the RAM memory. From there it can overcome and interrupt all of the operations executed by the system: corrupting files and programs that are opened, closed, copied, renamed etc.

Examples include: Randex, CMJ, Meve, and MrKlunky.

Boot Virus: This type of virus affects the boot sector of a floppy or hard disk. The boot sector is a crucial part of a disk, in which information is stored together with a program that makes thecomputer boot (start) from the disk

For avoiding boot viruses ensure that floppy disks are write-protected and never to start a computer with an unknown floppy disk.

Examples of boot viruses include: Polyboot.B, AntiEXE.

Macro Virus: Macro viruses infect files that created using certain applications or programs that contain macros. These macros make it possible to automate series of operations so that they performed as a single action, thereby saving the user from having to carry them out one by one.

Examples of macro viruses: Relax, Melissa.A, Bablas, O97M/Y2K.

Polymorphic Virus: Polymorphic viruses encrypt or encode themselves (using different algorithms and encryption keys) every time they infect a computer. This makes it very difficult for anti-viruses to find them using signature searches (because they are different in each encryption) and also enables them to create a large number of copies of themselves.

Examples include: Elkern, Marburg, Satan Bug, and Tuareg.

Parasitic Viruses: Parasitic viruses modify the code of the infected files. The infected file will partially or fully functional. Parasitic viruses grouped according to the section of the file they write their code:

- Prepending: the malicious code is written to the beginning of the file
- Appending: the malicious code is written to the end of the file
- Inserting: the malicious code is inserted in the middle of the file

Inserting file viruses use different methods to write code to the middle of the file: they either move parts of the original file to the end or copy their own code to empty sections of the infected file.

Resident Viruses: This type of virus is a permanent, whichresides in the RAM memory. From there it can overcome and interrupt all of the operations executed by the system: corrupting files and programs that are opened, closed, copied, renamed etc.

Examples include: Randex, CMJ, Meve, and MrKlunky.

Logic Bomb

A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are true. For example, a programmer may hide a piece of code that starts deleting files (such as the salary database trigger), should they ever leave the company.

Malware

Malwareis software designed to infiltrate or harm a computer system without the owner's information. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

Spyware

Spyware is software that installed surreptitiously on a computer to collect or steal information about the user, their computer or browsing habits without the user's informed consent.

Worms

A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program.

Trojan Horses

The Trojan horse, it describes a class of computer threats (malware) that appears to perform a particular function but in fact performs hidden malicious functions that allow unauthorized access to the host machine, giving attackers the ability to save their files on the user's computer for further damage or even watch the user's screen and control the computer.

Different Biometrics and Authentication System

Biometric Systems:A biometric system is a technological system that uses information about a person (or other biological organism) to identify that person. Biometric systems rely on specific data about unique biological traits in order to work effectively. A biometric system will involve running data through algorithms for a particular result, usually related to a positive identification of a user or other individual.

Biometric identification works generally in four stages: enrolment, storage, acquisition and matching. Features extracted during enrolment and acquisition stages are often transformed (through a non-reversible process) into templates in an effort to facilitate the storage and matching processes. Templates contain less data than the original sample, are usually manufacturer-dependent and are therefore not generally interoperable with those of other manufacturers. Templates or full samples thus acquired may then be held in storage that is either centralized (e.g. in a database) or decentralized (e.g. on a smart card). Because of the statistical nature of the acquisition and matching stages, biometric systems are never 100% accurate. There are two kinds of possible errors: a false match, and a false non-match. These errors vary from one biometric technology to another and depend on the threshold used to determine a 'match'. The operators depending on the application set this threshold.

Types of Biometrics systems

A number of biometric methods have been introduced over the years, but few have gained wide acceptance.

Signature dynamics: Based on an individual's signature, but considered unforgivable because what is recorded is not the final image but how it is produced -- i.e., differences in pressure and writing speed at various points in the signature.

Typing patterns: Similar to signature dynamics but extended to the keyboard, recognizing not just a password that is typed in but the intervals between characters and the overall speeds and pattern. This is akin to the way World War II intelligence analysts could recognize a specific covert agent's radio transmissions by his "hand" -- the way he used the telegraph key.

Eye scans: This favorite of spy movies and novels presents its own problems. The hardware is expensive and specialized, and using it is slow and inconvenient and may make users uneasy.

In fact, two parts of the eye can be scanned, using different technologies: the retina and the iris.

Fingerprint recognition: Everyone knows fingerprints are unique. They are also readily accessible and require little physical space for either the reading hardware or the stored data.

Hand or palm geometry: We are used to fingerprints but seldom think of an entire hand as an individual identifier. This method relies on devices that measure the length and angles of individual fingers. Although more user-friendly than retinal scans, it is still cumbersome.

Voice recognition: This is different from speech recognition. The idea is to verify the individual speaker against a stored voice pattern, not to understand what is being said.

Facial recognition: Uses distinctive facial features, including upper outlines of eye sockets, areas around cheekbones, the sides of the mouth and the location of the nose and eyes. Most technologies avoid areas of the face near the hairline so that hairstyle changes will not affect recognition.

Authentication System

The software for identifying aperson, based on a username and password is known as Authentication System. The authentication is distinct from authorization, it is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

Authentication types

One can provide his authentication credentials to the system by several physical means. The most common—but not the most secure—are password authentication. Today's competitive business environment demands options that offer more protection when network resources include highly sensitive data. Smart cards and biometric authentication types provide this extra protection.

Password authentication: Most of us are familiar with password authentication. To log onto a computer or network, you enter a user account name and the password assigned to that account. This password is verified against a database that contains all authorized users and their passwords.

To preserve the security of the network, passwords must be "strong," that is, they should contain a combination of alpha and numeric characters and symbols, they should not be words that are found in a dictionary, and they should be relatively long (eight characters or more). Password authentication is vulnerable to a password "cracker" who uses a brute force attack (trying every possible combination until hitting upon the right one) or who uses a protocol "sniffer" to capture packets if passwords are not encrypted when they are sent over the network.

Smart card authentication: Smart cards are credit card-sized devices that hold a small computer chip, which is used to store public and private keys and other personal information used to identify a person and authenticate him or her to the system. Logging onto the network with a smart card requires that you physically insert the card into (or slide it through) a reader and then enter a Personal Identification Number (PIN) in much the same way that you use an ATM card to access an automatic teller machine.

Smart cards use cryptography-based authentication and provide stronger security than a password because in order to gain access, the user must be in physical possession of the card and must know the PIN.

Authentication Methods:

some of the most popular authentication methods are:

Kerberos

Kerberos was developed at MIT to provide secure authentication for UNIX networks. It has become an Internet standard and is supported by Microsoft's latest network operating system, Windows 2000. Kerberos uses temporary certificates called tickets, which contain the credentials that identify the user to the servers on the network. In the current version of Kerberos, v5, the data contained in the tickets is encrypted, including the user's password.

A Key Distribution Center (KDC) is a service that runs on a network server, which issues a ticket called a Ticket Granting Ticket (TGT) to the clients that authenticates to the Ticket Granting Service (TGS). The client uses this TGT to access the TGS (which can run on the same computer as the KDC). The TGS issues a service or session ticket, which is used to access a network service or resource.

The name

Kerberos derives its name from the three-headed dog of Greek mythology (spelled Cerberus in Latin) that guarded the gates to Hades. Kerberos likewise stands guard over the network to ensure that only those who are authorized can enter.

Secure Sockets Layer (SSL)

The SSL protocol is another Internet standard, often used to provide secure access to Web sites, using a combination of public key technology and secret key technology. Secret key encryption (also called symmetric encryption) is faster, but asymmetric public key encryption provides for better authentication, so SSL is designed to benefit from the advantages of both. It is supported by Microsoft, Netscape, and other major browsers, and by most Web server software, such as IIS and Apache.

SSL operates at the application layer of the DoD networking model. This means applications must be written to use it, unlike other security protocols (such as IPSec) that operate at lower layers. The Transport Layer Security (TLS) Internet standard is based on SSL.

SSL authentication is based on digital certificates that allow Web servers and clients to verify each other's identities before they establish a connection. (This is called mutual authentication.) Thus, two types of certificates are used: client certificates and server certificates.

Microsoft NTLM (NT LAN Manager)

NTLM authentication is used by Windows NT servers to authenticate clients to an NT domain. Windows 2000 uses Kerberos authentication by default but retains support for NTLM for authentication of pre-Windows 2000 Microsoft servers and clients on the network. UNIX machines connecting to Microsoft networks via an SMB client also use NTLM to authenticate.

Native mode

NTLM uses a method called challenge/response, using the credentials that were provided when the user logged on each time that user tries to access a resource. This means the user's credentials do not get transferred across the network when resources are accessed, which increases security. The client and server must reside in the same domain or there must be a trust relationship established between their domains in order for authentication to succeed.

PAP

PAP is used for authenticating a user over a remote access control. An important characteristic of PAP is that it sends user passwords across the network to the authenticating server in plain text. This poses a significant security risk, as an unauthorized user could capture the data packets using a protocol analyzer (sniffer) and obtain the password.

The advantage of PAP is that it is compatible with many server types running different operating systems. PAP should be used only when necessary for compatibility purposes.

SPAP

SPAP is an improvement over PAP in terms of the security level, as it uses an encryption method (used by Shiva remote access servers, thus the name).

The client sends the user name along with the encrypted password, and the remote server decrypts the password. If the username and password match the information in the server's database, the remote server sends an Acknowledgment (ACK) message and allows the connection. If not, a Negative Acknowledgment (NAK) is sent, and the connection is refused.

CHAP and MS-CHAP

CHAP is another authentication protocol used for remote access security. CHAP is astandard, whichuses MD5 algorithm, which is a one-way encryption method. It performs a hash operation on the password and transmits the hash result, instead of the password itselfover the network.

CHAP specs

The hash algorithm ensures that the operation cannot be reverse engineered to obtain the original password from the hash results. CHAP is, however, vulnerable to remote server impersonation.

MS-CHAP is Microsoft's version of CHAP. MS-CHAPv2 uses two-way authentication so that the identity of the server, as well as the client, is verified. This protects against server impersonation. MS-CHAP also increases security by using separate cryptographic keys for transmitted and received data.

EAP

EAP is a means of authenticating a Point-to-Point Protocol (PPP) connection that allows the communicating computers to negotiate a specific authentication scheme (called an EAP type).

A key characteristic of EAP is its extensibility, indicated by its name. Plug-in modules can be added at both client and server sides to support new EAP types.

EAP can be used with TLS (called EAP-TLS) to provide mutual authentication via the exchange of user and machine certificates.

RADIUS

RADIUS is often used by Internet service providers (ISPs) to authenticate and authorize dial-up or VPN users. The standards for RADIUS are defined in RFCs 2138 and 2139. A RADIUS server receives user credentials and connection information from dial-up clients and authenticates them to the network.

RADIUS can also perform accounting services, and EAP messages can be passed to a RADIUS server for authentication. EAP only needs to be installed on the RADIUS server; it's not required on the client machine.

Windows 2000 Server includes a RADIUS server service called Internet Authentication Services (IAS), which implements the RADIUS standards and allows the use of PAP, CHAP, or MS-CHAP, as well as EAP.

Certificate services

Digital certificates consist of data that is used for authentication and securing of communications, especially on unsecured networks (for example, the Internet). Certificates associate a public key to a user or other entity (a computer or service) that has the corresponding private key.

Certificates are issued by certification authorities (CAs), which are trusted entities that "vouch for" the identity of the user or computer. The CA digitally signs the certificates it issues, using its private key. The certificates are only valid for specified time duration; when a certificate expires, a new one must be issued. The issuing authority can also revoke certificates.

Firewall Design Principles

Firewall is a security barrier between two networks that screens traffic coming in and out of the gate of one network to accept or reject connections and services according to a set of rules.

For a firewall to be effective the design of the firewalls should be efficient. The various principles that should be adopted while designing a firewall are as follows:

Firewall Characteristics:

i. All traffic from inside to outside and vice versa must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. The configurations used for this are screened Host Firewall (Single and Dual) and Screened Subnet Firewall.

ii. Only authorized traffic as defined by the local security policy will be allowed to pass. Various types of firewalls that can be used are Packet-Filters, Stateful Filters and Application Proxy Filters.

iii. The firewall itself is immune to penetration. This implies that use of a trusted system with a secure operating system.

Techniques for Control:

Four general techniques that firewalls use to control access and enforce security policy are as follows

i. Service Control- This determines the types of internet services that can be accessed inbound or outbound.

ii. Direction Control: This determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.

iii. User Control: Control access to a service according to which user is attempting to access it. This feature is typically applied to users inside the firewall perimeter.

iv. Behavior Control: Controls how particular services are used.

Capabilities of Firewalls: The expectations from a firewall are as follows

i. A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits vulnerability and provides protection from spoofing and routing attacks.

ii. A firewall provides a location for monitoring security-related events. Audits and alarms can be implemented on the firewall system.

iii. A firewall is a convenient platform for several internet functions that are not security related which include network address translator and a network management function.

iv. A firewall can serve as the platform for IPsec. Using the tunnel mode capability, the firewall can be used to implement virtual private networks.

RGPVNOTES.IN

We hope you find these notes useful.

You can get previous year question papers at https://qp.rgpvnotes.in .

If you have any queries or you want to submit your study notes please write us at rgpvnotes.in@gmail.com

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in