RGPVNOTES.IN

Subject Name: **Wireless & Mobile Computing**

Subject Code: **IT-7003**

Semester: **7th**

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

Downloaded from be.rgpvnotes.in

RGPVNOTES.IN

Intruder

An intruder is something that invades your computer or network without permission. Sometimes user don't even know that an intruder has arrived. User may think he is giving permission for one thing such as accepting sharing or download, but are actually opening your computer or network to attack.Here are the most common intruders:

- Adware: ad-supported software that is automatically loaded when a web page is viewed. These are often pop-up windows or bars on the computer screen. Some adware is also spyware that collects personal information.
- Hijacking:A spyware or a virus is hidden in a software program that normally does something harmful. When the program opens, it performs an operation such as stealing personal information.
- Spam: unwanted e-mail messages that are usually mailed out to many people at once.
- Spyware: It is a software that automatically collects personal information without permission. Spyware is usually associated with download software such as music or games because it can be hidden in the download. Spyware software does not self-replicate.
- Phishing: Unethical methods to find personal information about the user likehis passwords or account information,it can be used for identify theft.
- Virus - software programs designed to interfere with computer operation. A virus replicates itself and attaches itself to programs such as e-mail. Viruses may corrupt data, slow down functions, or cause other problems. They attack software, but will not physically harm your computer components such as monitor or keyboard.
- Worm – It is like a virus, it is designed to interfere and manipulate computer operation. It also takes control of features of computer and does bad things like send email to all the people in e-mail address book. This can overload networks and slow down the Internet.

Intruders are sometimes referred to as a hacker or cracker. There are three classes of intruders:

- **Masquerader:** An individual who is not authorized to use the computer andwho penetrates a system's access controls to exploit a legitimate user's account
- **Misfeasor:** A legitimate user who accesses data, programs, or resources forwhich such access is not authorized, or who is authorized for such access butmisuses his or her privileges
- **Clandestine user:** An individual who seizes supervisory control of the systemand uses this control to evade auditing and access controls or to suppress auditcollection

Intrusion detection

Intrusion detection is a method for monitoring a network or systems for malicious activity or policy violations. Any detected activity or violation is typically reported either to an administrator or collected centrally using a security information database and a event management system.

Intrusion detection is based on the assumption that the behavior of theintruder is slightly differs from that of a legitimate user.

These are thetwo approaches to intrusion detection:

Follow us on facebook to get real-time updates from RGPV

Downloaded from be.rgpvnotes.in

RGPVNOTES.IN

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.

 Follow us on facebook to get real-time updates from RGPV

Downloaded from be.rgpvnotes.in

RGPVNOTES.IN

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

 Follow us on facebook to get real-time updates from RGPV

Downloaded from be.rgpvnotes.in

RGPVNOTES.IN

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.

RGPVNOTES.IN

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

 Follow us on facebook to get real-time updates from RGPV

Downloaded from be.rgpvnotes.in

RGPVNOTES.IN

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.

RGPVNOTES.IN

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.

 Follow us on facebook to get real-time updates from RGPV

Downloaded from be.rgpvnotes.in

RGPVNOTES.IN

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.

Follow us on facebook to get real-time updates from RGPV

Downloaded from be.rgpvnotes.in

RGPVNOTES.IN

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.

RGPVNOTES.IN

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.

Follow us on facebook to get real-time updates from RGPV

Downloaded from be.rgpvnotes.in

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.

 Follow us on facebook to get real-time updates from RGPV

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