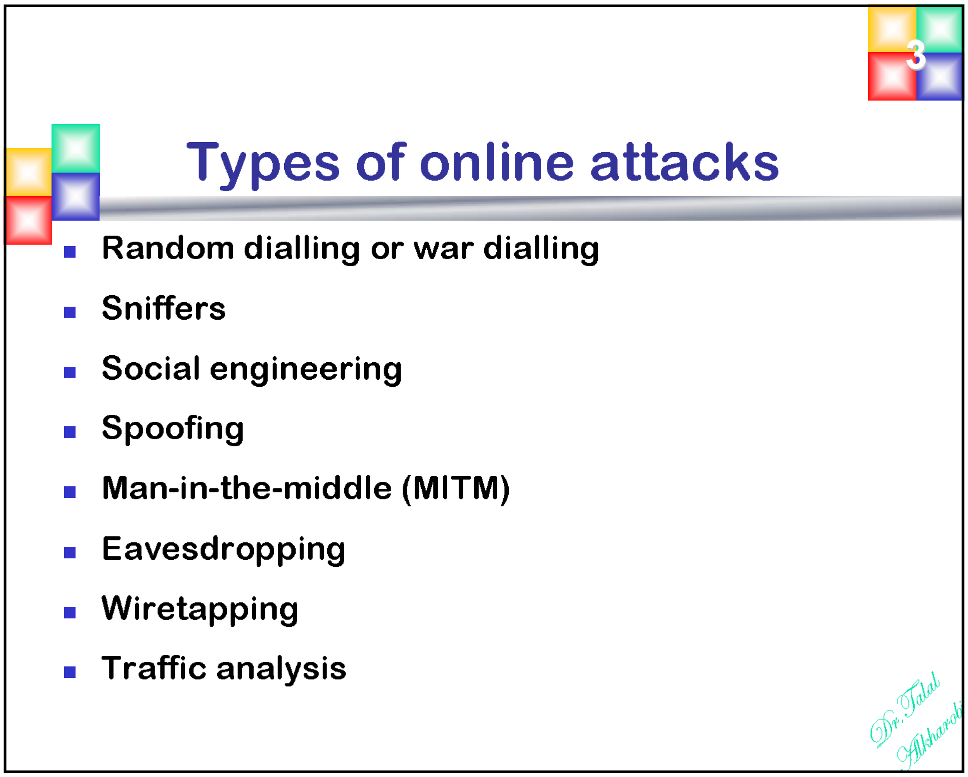
Types of attacks

Dr.Talal Alkharobi

Types of online attacks

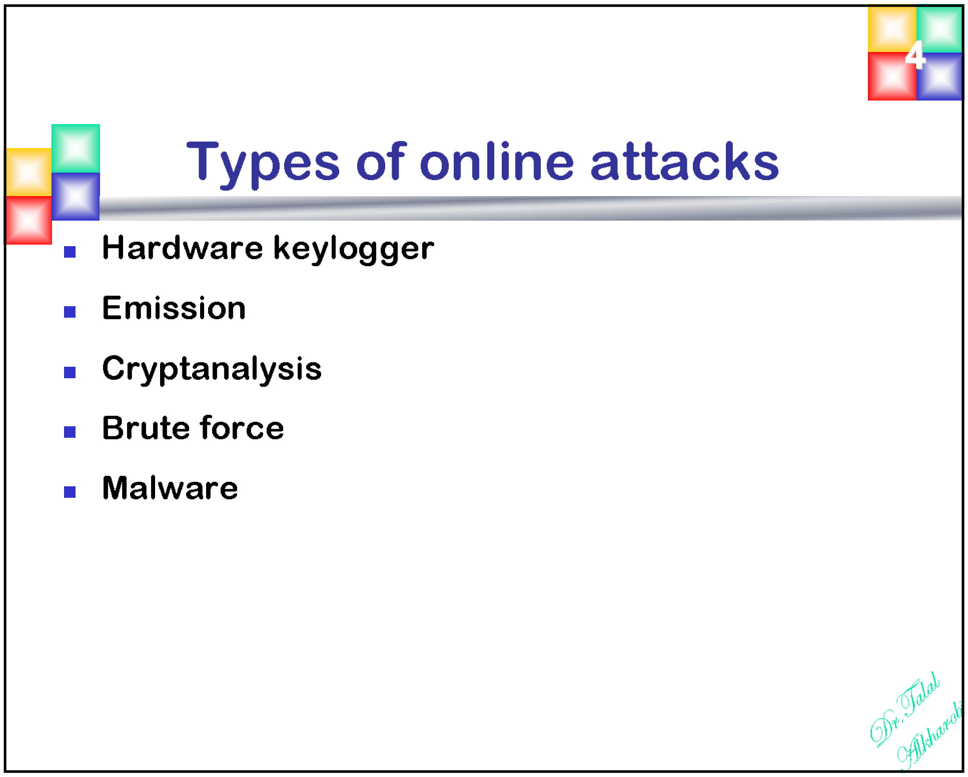
- Backdoors
- Denial of service DoS & DDoS
- Exploiting known security vulnerabilities
- Guessing passwords
- IP hijacking
- Page hijacking
- Session hijacking
- Phishing
- Pharming



3

Types of online attacks

- Random dialling or war dialling
- Sniffers
- Social engineering
- Spoofing
- Man-in-the-middle (MITM)
- Eavesdropping
- Wiretapping
- Traffic analysis



4

Types of online attacks

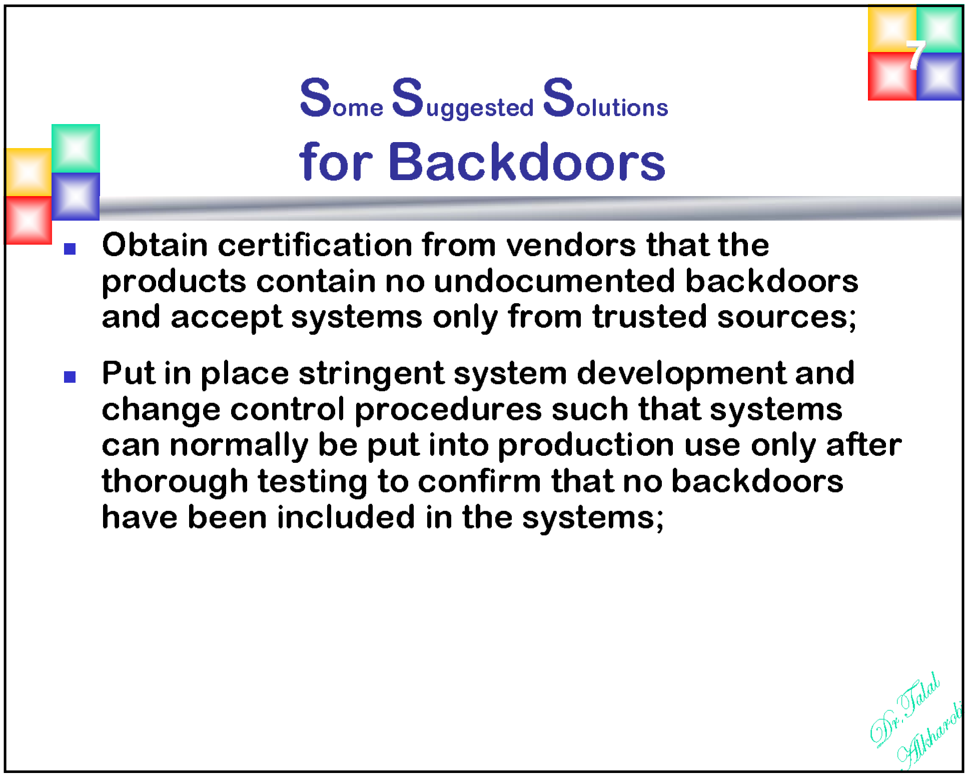
- Hardware keylogger
- Emission
- Cryptanalysis
- Brute force
- Malware

Backdoors

- Pieces of program code written into applications or operating systems to grant programmers access to programs without the need to go through the normal security controls.
- Can either recognise some special sequence of input, or is triggered by being run from a certain user ID which is then granted special access rights accordingly.
- Used by programmers to achieve faster access to facilitate debugging or monitoring of the programs that they are developing.
- Many computer manufacturers preinstall backdoors on their systems to provide technical support for customers.

Backdoors

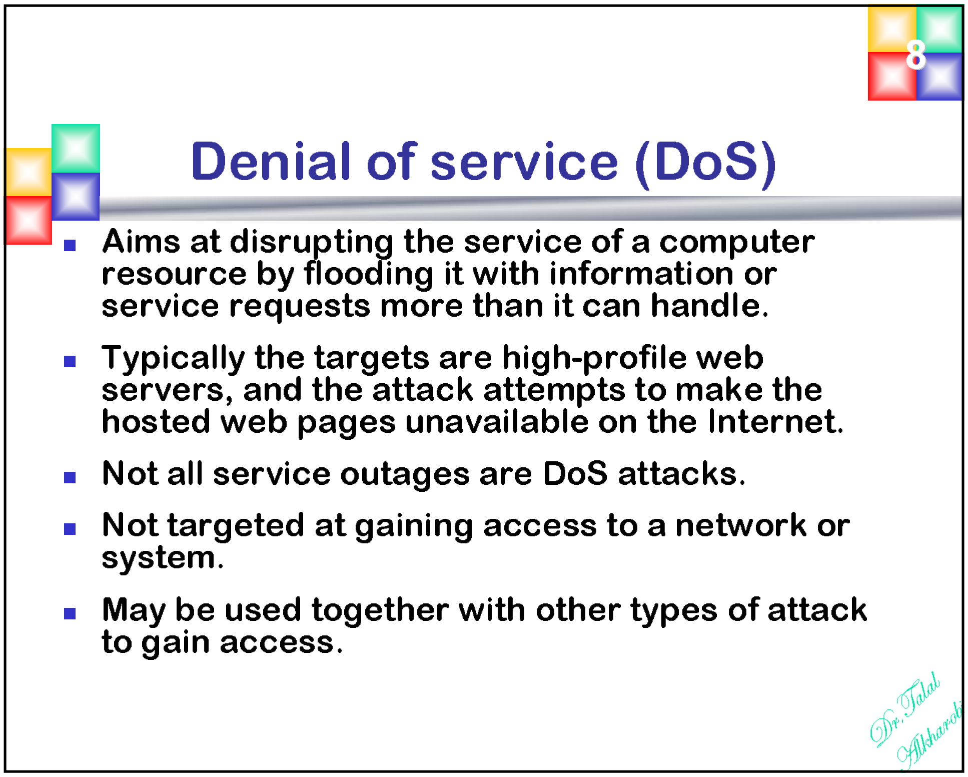
- Become a problem when the programmer forgets to remove them after debugging.
- Hackers typically use backdoors to secure remote access to a computer, while attempting to remain hidden from casual inspection.
- After gaining access, hackers create backdoors for future access
- Hackers may use of Trojan horses or computer worm to install backdoors.



7

Some Suggested Solutions for Backdoors

- Obtain certification from vendors that the products contain no undocumented backdoors and accept systems only from trusted sources;
- Put in place stringent system development and change control procedures such that systems can normally be put into production use only after thorough testing to confirm that no backdoors have been included in the systems;



8

Denial of service (DoS)

- Aims at disrupting the service of a computer resource by flooding it with information or service requests more than it can handle.
- Typically the targets are high-profile web servers, and the attack attempts to make the hosted web pages unavailable on the Internet.
- Not all service outages are DoS attacks.
- Not targeted at gaining access to a network or system.
- May be used together with other types of attack to gain access.

9

Denial of service (DoS)

- Although the direct impact of DoS attacks may be disruptions to services, rather than immediate security breaches, their occurrence may affect the working of certain security measures and hence increase the probability of security breaches

10

Denial of service (DoS) forms

- Force the **computer** to reset or consume its resources such that it can no longer provide its intended service.
- Obstruct the **communication** between the computer and the intended users.

11

Distributed Denial of service (DDoS)

- DoS attack can be initiated at one or multiple sources.
- In a distributed denial of service ("DDoS") attack, a single attacker deliberately introduces DoS attack programs into dozens or even hundreds of other systems by various techniques of online attack.
- The attacker then simultaneously initiates all those DoS attack programs to bombard the target network or system.

12

SSS-DoS

- Implement adequate network security to block unnecessary network traffic to the systems
- Arrange with internet service providers ("ISPs") to accept traffic from authorized sources only
- Prepare adequate standby system capacity
- Put in place adequate backup and recovery arrangements

13

Exploiting known security vulnerabilities

- Attackers may exploit known security flaws to gain unauthorized access to a particular system.
- Security vulnerabilities can be related to the hardware or software
- The internet provides various sources of such information.
- Alternatively, attackers may make use of automated tools to probe particular systems to identify security weaknesses.
- Vulnerabilities of web servers, firewalls or development tools used for developing applications of web servers may allow intruders to modify the content of web pages.

14

Vulnerability

- A weakness in a system allowing an attacker to violate the confidentiality, integrity, availability, access control, consistency or audit mechanisms of the system.
- Vulnerabilities may result from bugs or design flaws in the system.
- A vulnerability can exist either only in theory, or could have a known exploit.
- Vulnerabilities are of significant interest when the program containing the vulnerability operates with special privileges, performs authentication or provides easy access to user data or facilities (such as a network server or DBMS: database management system).

15

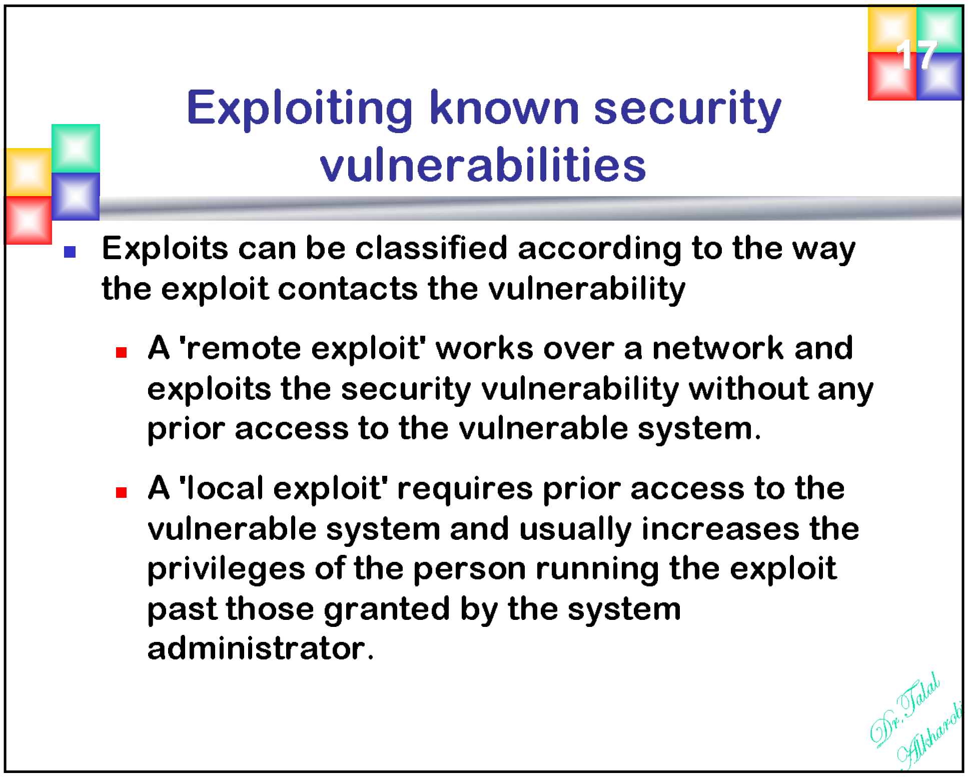
Exploit

- A piece of software, a chunk of data, or sequence of commands that take advantage of a bug, glitch or vulnerability in order to get unintended or unanticipated behavior out of computer software, hardware, or something electronic (usually computerized).
- This frequently includes such things as gaining control of a computer system or allowing privilege escalation or a denial of service attack.

16

Exploiting known security vulnerabilities

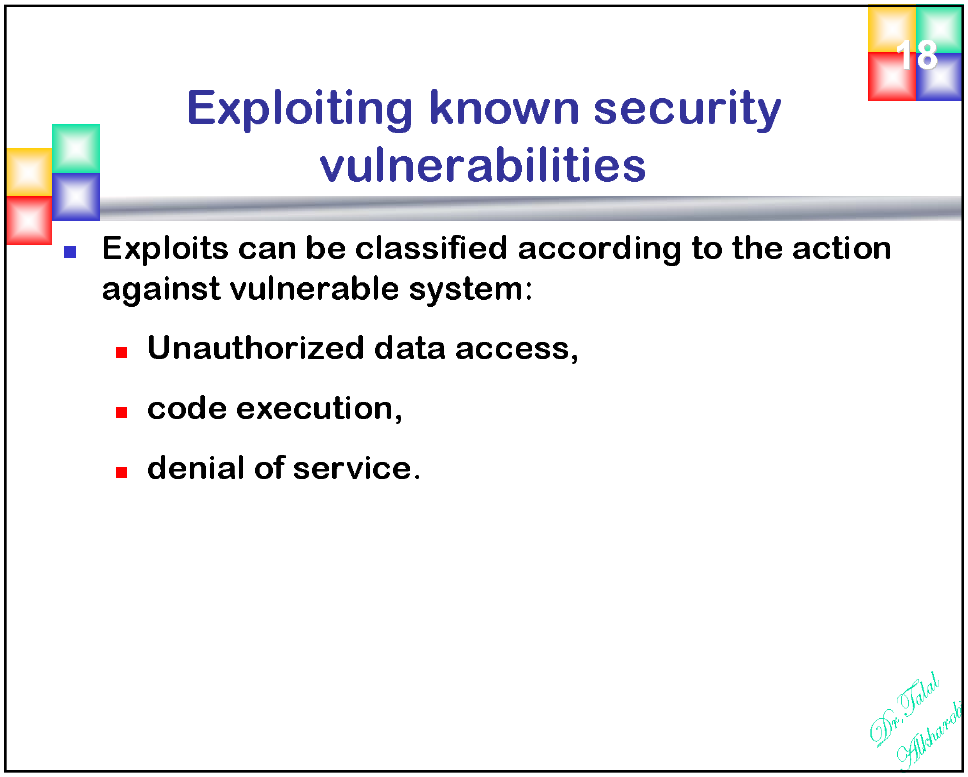
- Exploits can be categorized by what mechanism they use to take advantage of vulnerabilities. Common types of exploits are:
  - buffer overflow
  - heap overflow
  - integer overflow
  - return-to-libc attack
  - format string attack
  - race condition
  - code injection
  - SQL injection
  - cross-site scripting
  - cross-site request forgery



17

Exploiting known security vulnerabilities

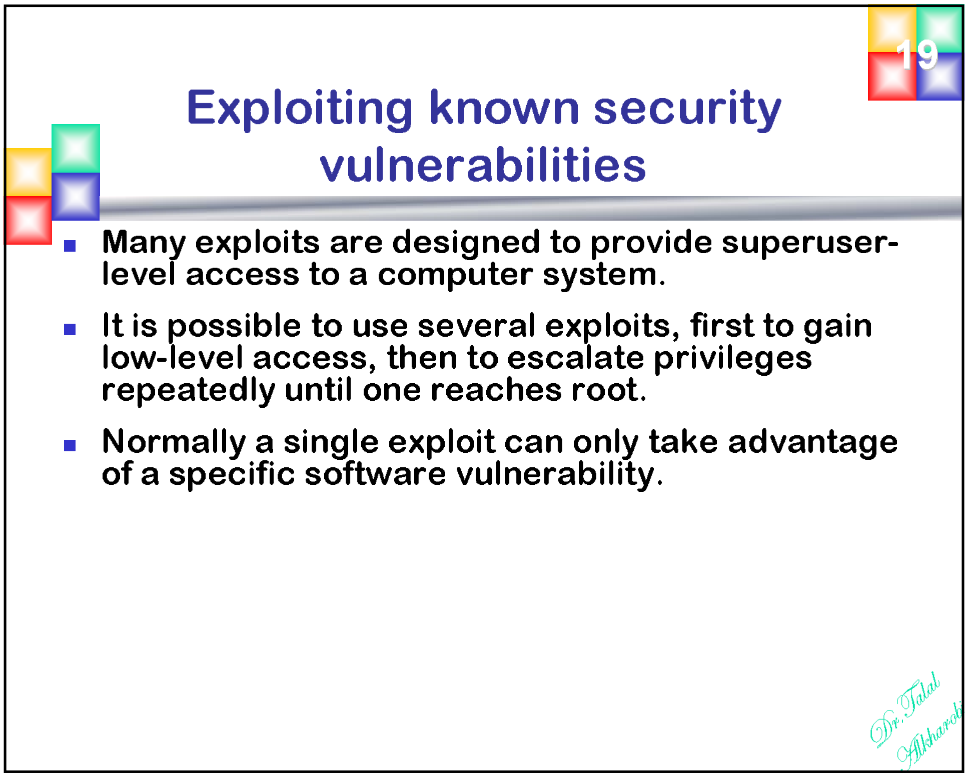
- Exploits can be classified according to the way the exploit contacts the vulnerability
  - A 'remote exploit' works over a network and exploits the security vulnerability without any prior access to the vulnerable system.
  - A 'local exploit' requires prior access to the vulnerable system and usually increases the privileges of the person running the exploit past those granted by the system administrator.



18

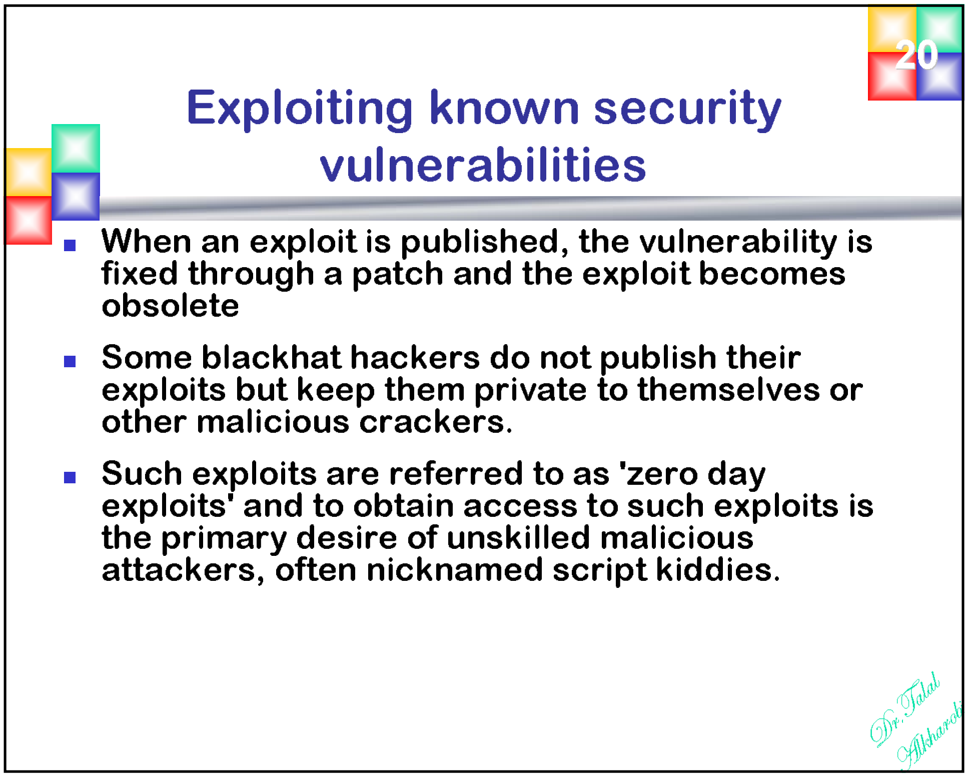
Exploiting known security vulnerabilities

- Exploits can be classified according to the action against vulnerable system:
  - Unauthorized data access,
  - code execution,
  - denial of service.



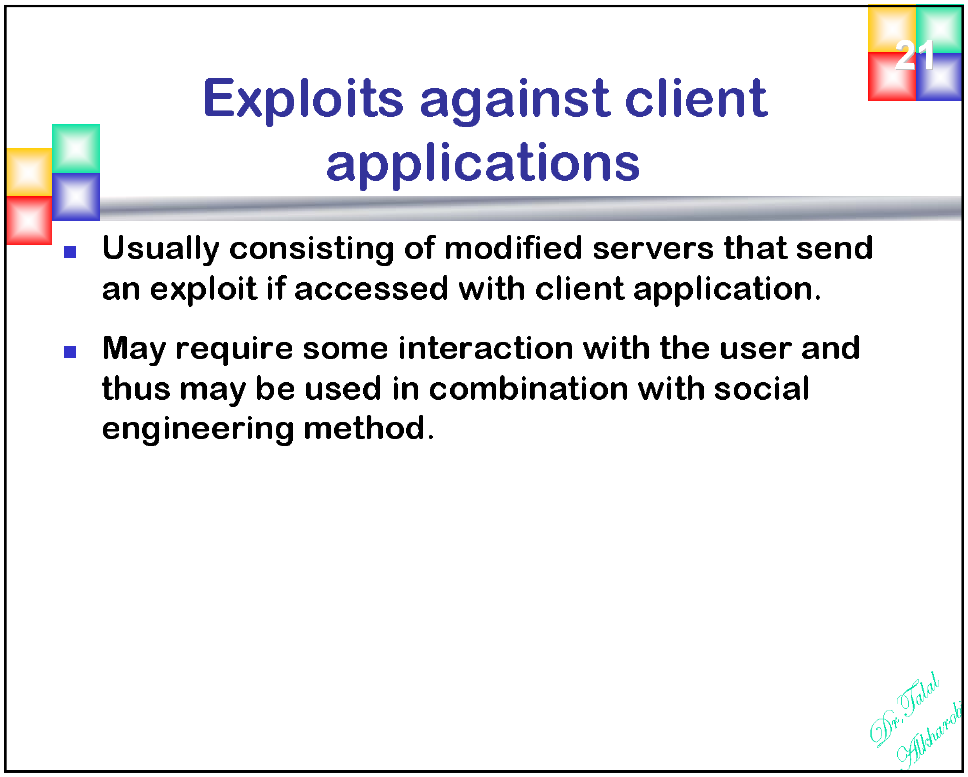
Exploiting known security vulnerabilities

- Many exploits are designed to provide superuser-level access to a computer system.
- It is possible to use several exploits, first to gain low-level access, then to escalate privileges repeatedly until one reaches root.
- Normally a single exploit can only take advantage of a specific software vulnerability.



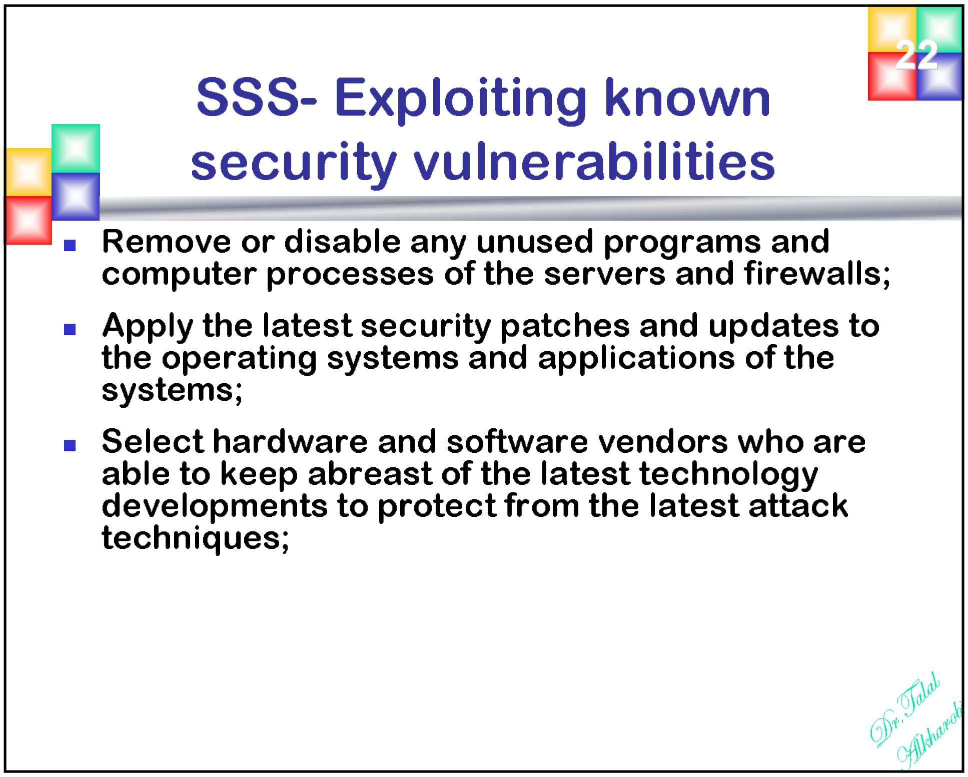
Exploiting known security vulnerabilities

- When an exploit is published, the vulnerability is fixed through a patch and the exploit becomes obsolete
- Some blackhat hackers do not publish their exploits but keep them private to themselves or other malicious crackers.
- Such exploits are referred to as 'zero day exploits' and to obtain access to such exploits is the primary desire of unskilled malicious attackers, often nicknamed script kiddies.



Exploits against client applications

- Usually consisting of modified servers that send an exploit if accessed with client application.
- May require some interaction with the user and thus may be used in combination with social engineering method.



SSS- Exploiting known security vulnerabilities

- Remove or disable any unused programs and computer processes of the servers and firewalls;
- Apply the latest security patches and updates to the operating systems and applications of the systems;
- Select hardware and software vendors who are able to keep abreast of the latest technology developments to protect from the latest attack techniques;

23

Guessing passwords

- A technique using software to test all possible combinations to gain entry into a system or network.
- Some attacks speed up this process by trying commonly used combinations first (e.g., words in dictionaries).

24

SSS-Guessing password

- Enforce password policies (e.g., mandating minimum length of passwords, or periodic changes in passwords);
- Enforce stringent access controls (e.g. disable user IDs after multiple unsuccessful logon attempts);
- Meticulously change all default passwords on critical network components;
- Provide adequate guidance to customers on security precautions (particularly on setting passwords).

25

IP hijacking

- IP hijacking (sometimes referred to as "BGP hijacking") is the illegitimate taking over of groups of IP addresses by corrupting Internet routing tables.
- The internet enables communication between one IP address and another by passing data from one server to another, closer to the destination, again and again until it is safely delivered.
- To do this, each server must be regularly supplied with up-to-date routing tables.
- At the global level, individual IP addresses are grouped together into autonomous systems (AS) and the routing tables between them are maintained using the Border Gateway Protocol (BGP).

26

Autonomous System (AS)

- A group of networks that operate under a single external routing policy.
- Each AS has its own unique AS identifier number.
- BGP is the standard routing protocol used to exchange information about IP routing between autonomous systems.
- Each AS uses BGP to advertise (i.e., broadcast) IP networks that it can deliver traffic to.
- For example if the network 192.168.1.0/24 is inside AS 123, then that AS will advertise to other providers that it can deliver any traffic destined for 192.168.1.0/24 (obviously this is not a real externally routed network).

IP hijacking

- IP hijacking can occur on purpose or by accident if an AS advertises a network that it is not actually authorized to use.
- If AS X advertises a network that really resides in AS Y then it is possible for traffic to be diverted.
- Typically ISPs will filter BGP traffic so that BGP advertisements from their downstream networks contain only valid IP space.
- IP hijacking is sometimes used by malicious users to obtain IP addresses for use with spamming or a DDoS attack.

Page hijacking

- A form of spamming the index of a search engine (spamdexing).
- It is achieved by creating a rogue copy of a popular website which shows contents similar to the original to a web crawler, but redirects web surfers to unrelated or malicious websites.
- Spammers can use this technique to achieve high rankings in result pages for certain key words.
- Page hijacking is a form of cloaking, made possible because some web crawlers detect duplicates while indexing web pages.
  - If two pages have the same content, only one URL will be displayed.
  - A spammer will try to ensure that the rogue website is the one shown on the result pages.

29

Session hijacking

- Exploitation of a valid computer session to gain unauthorized access to information or services in a computer system.
- In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server.
- It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer

30

Session hijacking

- There are three main methods used to hijack a session:
  - Sniffing to obtain illicit session keys.
  - Taking advantage of Cross-site scripting vulnerabilities
  - Steal the session key by, for example, obtaining the file or memory contents of the appropriate part of either the user or the server's computer.

31

SSS-Session Hijacking

- Use of a long random number or string as the session key. This reduces the risk that an attacker could simply guess a valid session key through trial and error.
- Encryption of the data passed between the parties; in particular the session key. This technique is widely relied-upon by web-based banks and other e-commerce services, because it completely prevents sniffing-style attacks.
- Some services make secondary checks against the identity of the user. For example, a web server could check with each request that the IP address of the user matched the one last used during that session. This does not prevent attacks by somebody who shares the same IP address, however, and could be frustrating for users who's IP address is liable to change during a browsing session.

32

SSS-Session Hijacking

- Some services will change the value of the cookie with each and every request. This dramatically reduces the window in which an attacker can operate and makes it easy to identify whether an attack has taken place, but can cause some problems (for example, preventing the back button from working properly wile browsing).
- Use of SecurID card, or other token based secondary authentication is useless as protection against hijacking, as the attacker can simply wait until after the user authenticates, then hijack the session.

Phishing

- Phishers attempt to fraudulently acquire sensitive information, like username, passwords, bank accounts and credit card details, by masquerading as a trustworthy person or business through emails or phishing websites.
- Phishing is typically carried out using email or an instant message, although phone contact has been used as well.
- Attempts to deal with the growing number of reported phishing incidents include legislation, user training, and technical measures.

Pharming

- Pharming is a hacker's attack aiming to redirect a website's traffic to another (bogus) website.
- Pharming can be conducted either by changing the hosts file on a victim’s computer or by exploitation of a vulnerability in DNS server software.
- Pharming is used with phishing to steal identity information.
- Pharming has become of major concern to businesses hosting ecommerce and online banking websites.
- Antivirus software and spyware removal software cannot protect against pharming. Sophisticated measures known as anti-pharming are required to protect against this serious threat

35

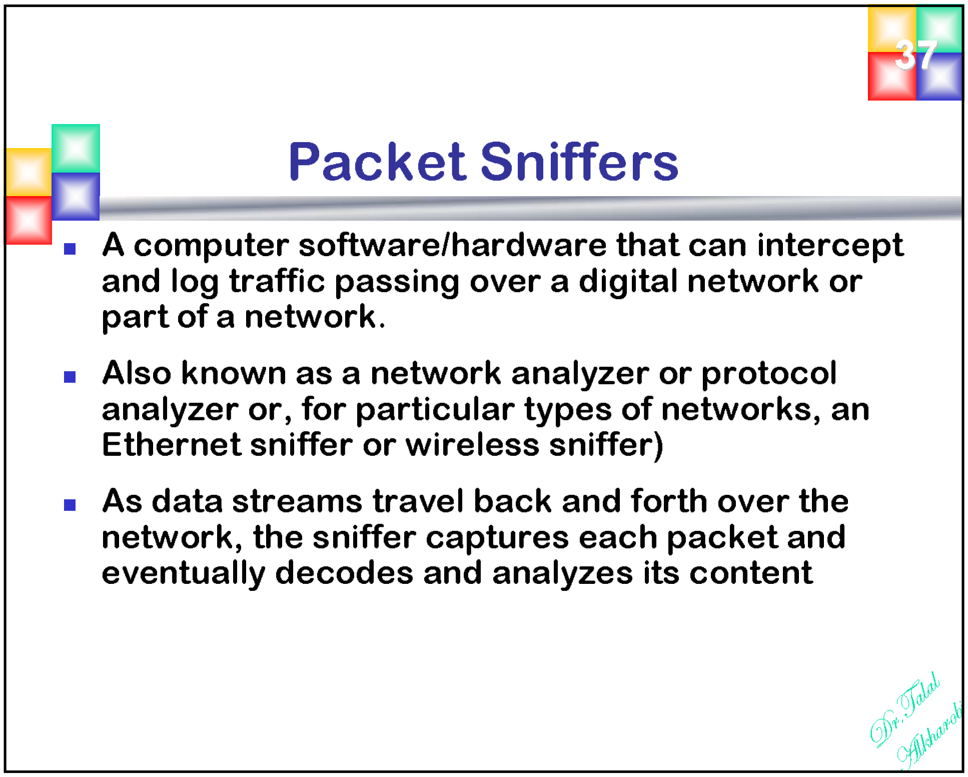
Random (war) dialling

- A technique where an attacker sequentially or randomly dials every number on a known telephone exchange with the objective of detecting modems that bypass network firewalls and other security measures so that the attacker can gain access to the networks through the modems.

36

SSS - Random (war) dialling

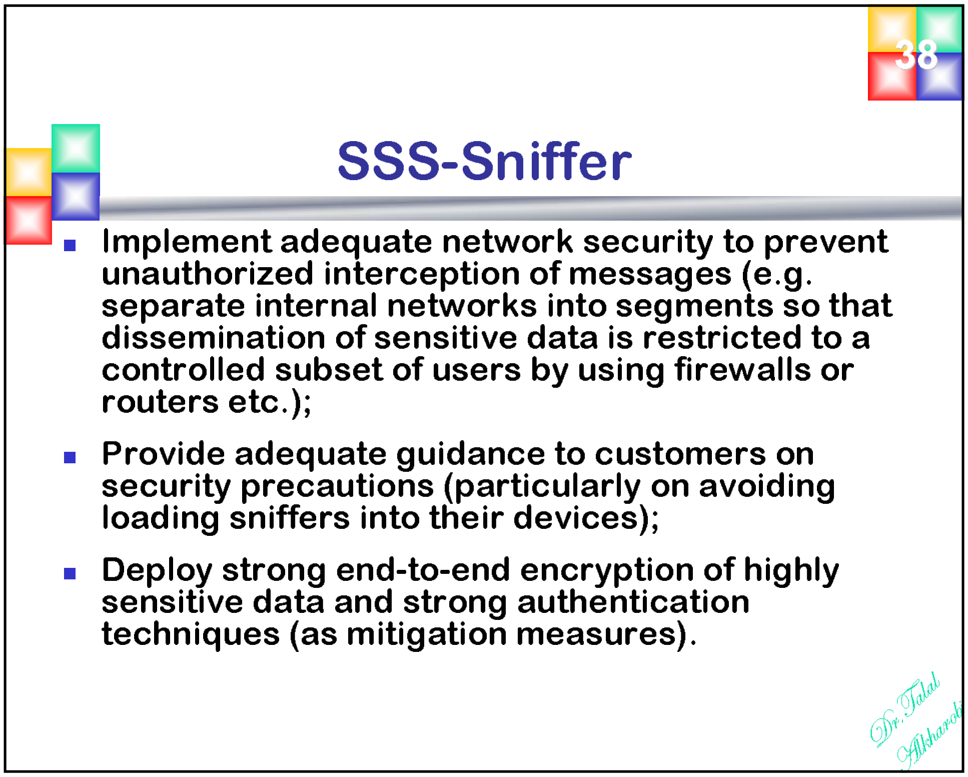
- Ensure that all modems have been authorized and controlled, e.g. periodically “war dial” all the numbers on the institution’s telephone exchange to detect unauthorized modems
- Centralise all modems in physically secure locations and separate the network segment connected to the modems from other important segments of the internal network so that even if attackers can gain unauthorized access to the internal networks through the modems, they would not be able to access other critical network segments;
- Configure the modems or other similar devices in a “dial-back” mode such that remote network connections through these modems can be initiated only from the modems to pre-approved remote parties but not the other way round



37

Packet Sniffers

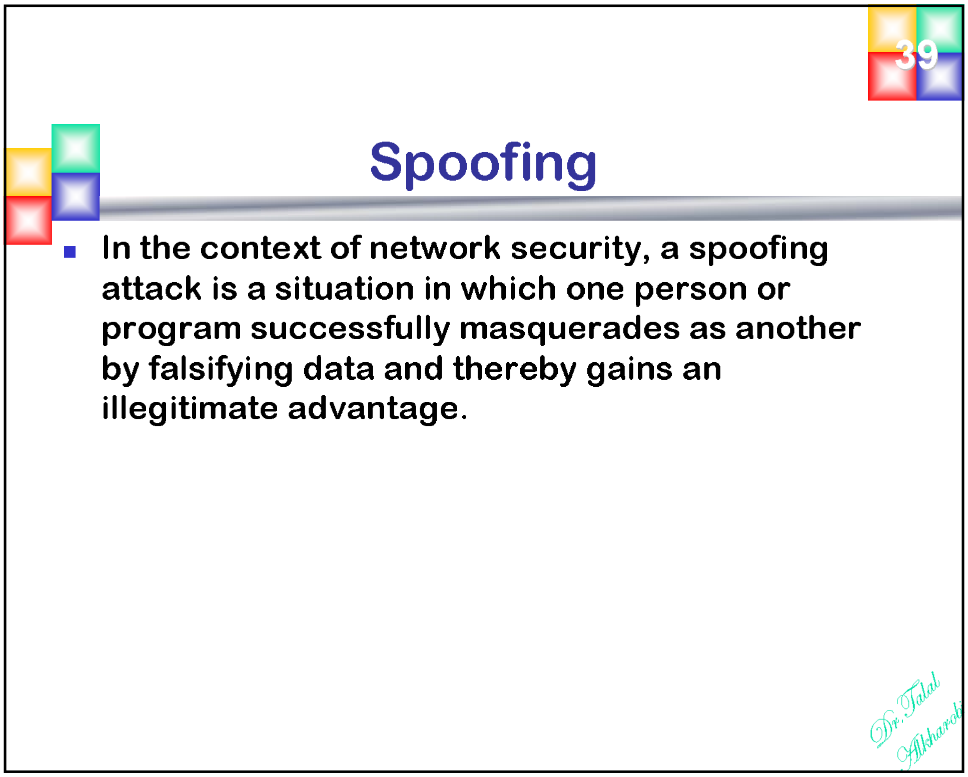
- A computer software/hardware that can intercept and log traffic passing over a digital network or part of a network.
- Also known as a network analyzer or protocol analyzer or, for particular types of networks, an Ethernet sniffer or wireless sniffer)
- As data streams travel back and forth over the network, the sniffer captures each packet and eventually decodes and analyzes its content



38

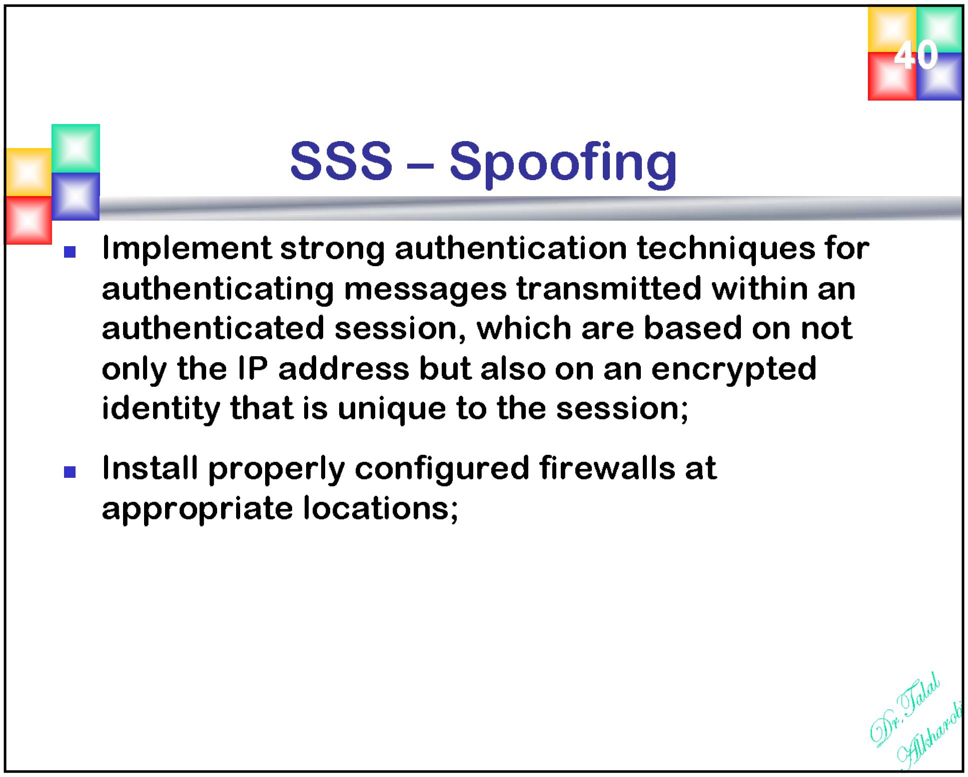
SSS-Sniffer

- Implement adequate network security to prevent unauthorized interception of messages (e.g. separate internal networks into segments so that dissemination of sensitive data is restricted to a controlled subset of users by using firewalls or routers etc.);
- Provide adequate guidance to customers on security precautions (particularly on avoiding loading sniffers into their devices);
- Deploy strong end-to-end encryption of highly sensitive data and strong authentication techniques (as mitigation measures).



Spoofing

- In the context of network security, a spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gains an illegitimate advantage.



SSS – Spoofing

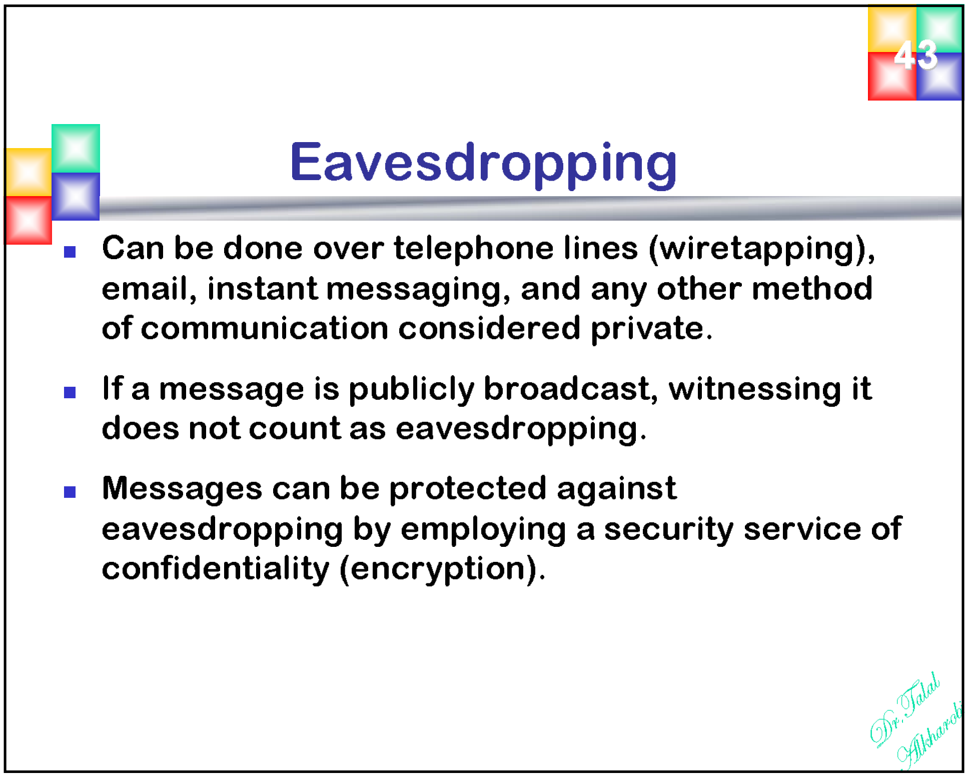
- Implement strong authentication techniques for authenticating messages transmitted within an authenticated session, which are based on not only the IP address but also on an encrypted identity that is unique to the session;
- Install properly configured firewalls at appropriate locations;

Man-in-the-middle (MITM)

- An attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised.
- The attacker must be able to observe and intercept messages going between the two victims.
- The MITM attack can work against public-key cryptography and is also particularly applicable to the original Diffie-Hellman key exchange protocol, when used without authentication.

Eavesdropping

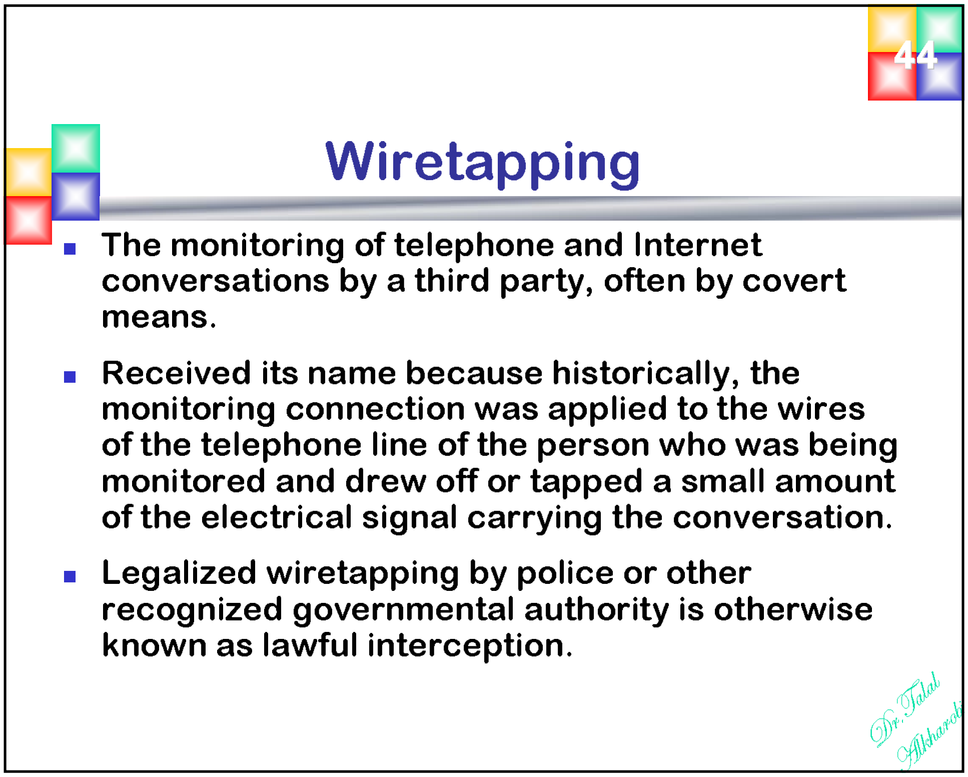
- The intercepting of conversations by unintended recipients.
- One who participates in eavesdropping (i.e. someone who secretly listens in on the conversations of others) is called an eavesdropper.
- The origin of the term comes from situations in which people would literally hide out in the eavesdrip of a house to listen in on private conversations.



43

Eavesdropping

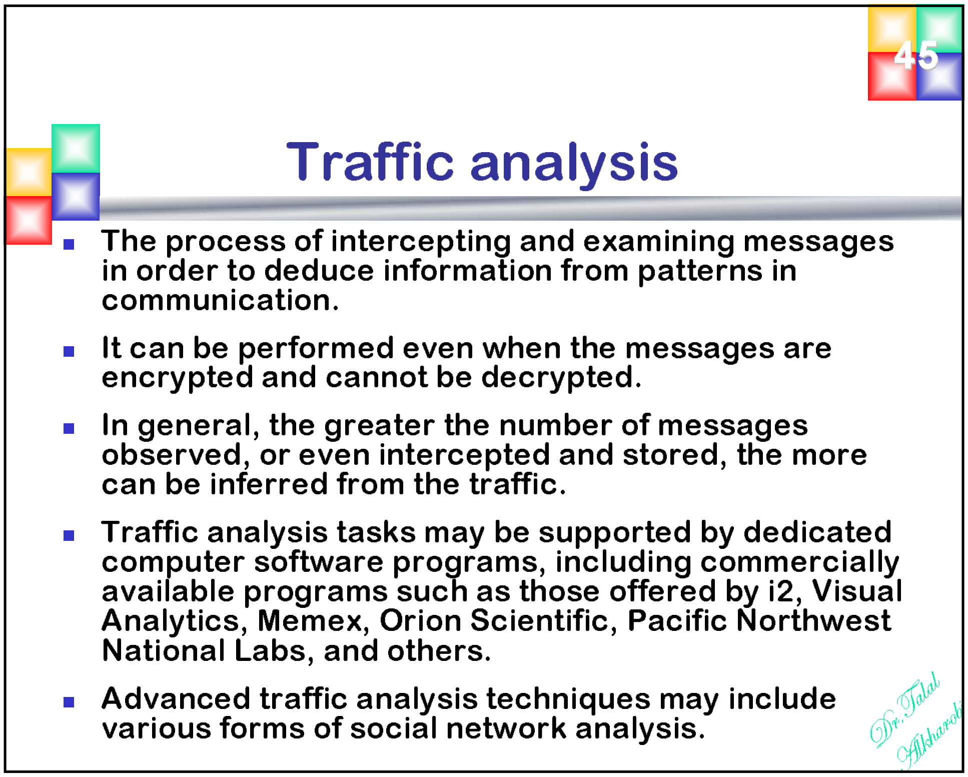
- Can be done over telephone lines (wiretapping), email, instant messaging, and any other method of communication considered private.
- If a message is publicly broadcast, witnessing it does not count as eavesdropping.
- Messages can be protected against eavesdropping by employing a security service of confidentiality (encryption).



44

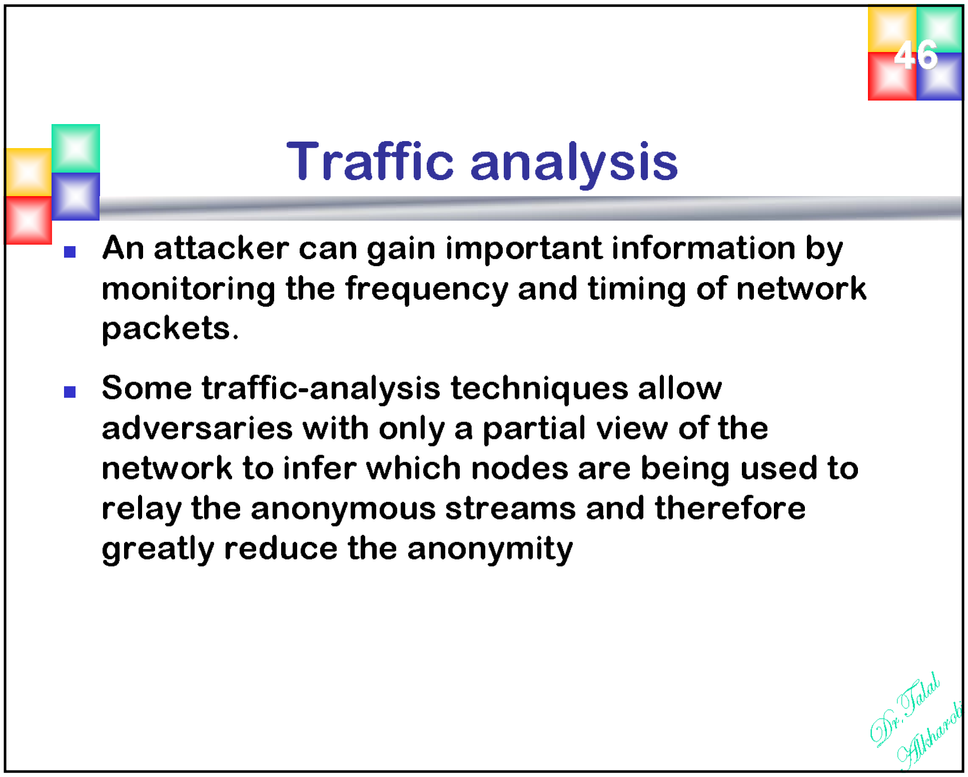
Wiretapping

- The monitoring of telephone and Internet conversations by a third party, often by covert means.
- Received its name because historically, the monitoring connection was applied to the wires of the telephone line of the person who was being monitored and drew off or tapped a small amount of the electrical signal carrying the conversation.
- Legalized wiretapping by police or other recognized governmental authority is otherwise known as lawful interception.



Traffic analysis

- The process of intercepting and examining messages in order to deduce information from patterns in communication.
- It can be performed even when the messages are encrypted and cannot be decrypted.
- In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic.
- Traffic analysis tasks may be supported by dedicated computer software programs, including commercially available programs such as those offered by i2, Visual Analytics, Memex, Orion Scientific, Pacific Northwest National Labs, and others.
- Advanced traffic analysis techniques may include various forms of social network analysis.



Traffic analysis

- An attacker can gain important information by monitoring the frequency and timing of network packets.
- Some traffic-analysis techniques allow adversaries with only a partial view of the network to infer which nodes are being used to relay the anonymous streams and therefore greatly reduce the anonymity

Traffic analysis
Attacking Remailer systems

- A remailer is a server computer which receives messages with embedded instructions on where to send them next, and which forwards them without revealing where they originally came from.
- If a message is observed going to a remailing server, and an identical length (if now anonymized) message is observed leaving that server shortly thereafter, a traffic analyst may be able (automatically) to pierce the anonymity of that sender by connecting the sender with the ultimate receiver.
- Several variations in remailer operation have been developed which can make such analysis much less informative.

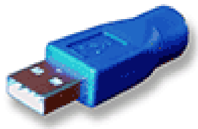
Hardware keylogger

- Plug in between the keyboard and the computer that log all keyboard activity on an internal memory.
- Designed to work with PS/2 and USB keyboards.
- Hardware keyloggers have an advantage over software keyloggers as they begin logging from the moment a computer is turned on (and are therefore able to collect a BIOS password for instance), and do not require software installation (unlike software solutions).

49

Hardware keylogger

- All hardware keyloggers have to have the following:
  - A microcontroller to interprets the datastream between the keyboard and computer, processes it, and passes it to the non-volatile memory
  - A non-volatile memory to stores the recorded data, even when power is lost



50

Hardware keylogger

- On the whole the recorded data is retrieved by typing a special password into a computer text editor.
- As the hardware keylogger is plugged in-between the keyboard and computer, it detects the password has been typed and then starts presenting the computer with "typed" data to produce a menu.
- Beyond text menu some keyloggers offers pendrive mode fast access to the stored data.

51

Emission

- Computers emit energy in various forms, mostly as unintended side effects of normal operation.
- Where these emissions take the form of radio waves, they may become noticeable when they cause interference in nearby radio receivers.
- Some of these emissions carry information about processed data.
- Under good conditions, a sophisticated and well-equipped eavesdropper can intercept and analyze such signals to steal information at a distance.

52

Emission

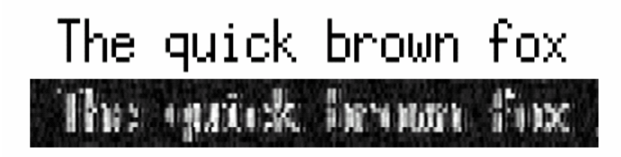
- The problem has been known since the early days of electronic computing.
- Some military organizations, concerned about these compromising emanations, started research on emission security around 1960.
- They established a set of test standards and management procedures for especially shielded equipment, known under the codename Tempest.

Eavesdropping attacks on computer displays

- Electromagnetic information leakage from computer displays was first demonstrated to the general public by van Eck in 1985.
- Nearby eavesdroppers can pick up compromising emanations from computer hardware with directional antennas and wideband receivers.
- The basic phenomenon is easily demonstrated with modified TV.
- To separate practically readable text shown on modern high-resolution displays from interfering background noise, special digital wideband signal-processing systems are needed.

Eavesdropping attacks on computer displays

- The problem is not restricted to cathode-ray tubes; some contemporary flat-panel systems are at least as vulnerable.



Cryptanalysis

- Acoustic cryptanalysis
- Adaptive chosen plaintext and chosen ciphertext attack
- Adaptive chosen-ciphertext attack
- Adaptive chosen-message attack
- Birthday attack
- Bit-flipping attack
- Boomerang attack
- Brute force attack
- Chosen-ciphertext attack
- Chosen-plaintext attack
- Ciphertext-only attack
- Custom hardware attack
- Davies' attack
- Decimalization table attack
- Dictionary attack
- Differential cryptanalysis
- Differential-linear attack
- Frequency analysis

Cryptanalysis

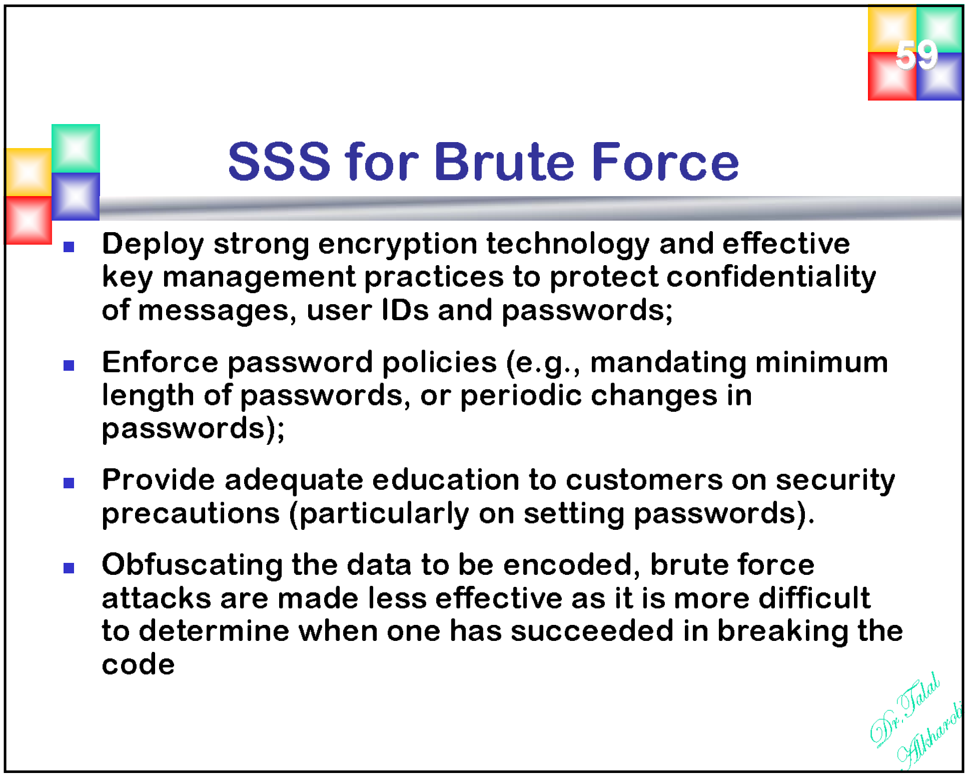
- Indifferent chosen-ciphertext attack
- Interpolation attack
- Known-plaintext attack
- Mafia Fraud Attack
- Man-in-the-middle attack
- Meet-in-the-middle attack
- Passive attack
- Preimage attack
- Random number generator attack
- Related-key attack
- Replay attack
- Side channel attack
- Slide attack
- Small subgroup confinement attack
- Stream cipher attack
- Timing attack
- Watermarking attack
- XSL attack

Brute force

- A method of defeating a cryptographic scheme by trying a large number of possibilities;
- For example, exhaustively working through all possible keys in order to decrypt a message.
- In most schemes, the theoretical possibility of a brute force attack is recognized, but it is set up in such a way that it would be computationally infeasible to carry out.
- Accordingly, one definition of "breaking" a cryptographic scheme is to find a method faster than a brute force attack.
- The selection of an appropriate key length depends on the practical feasibility of performing a brute force attack.

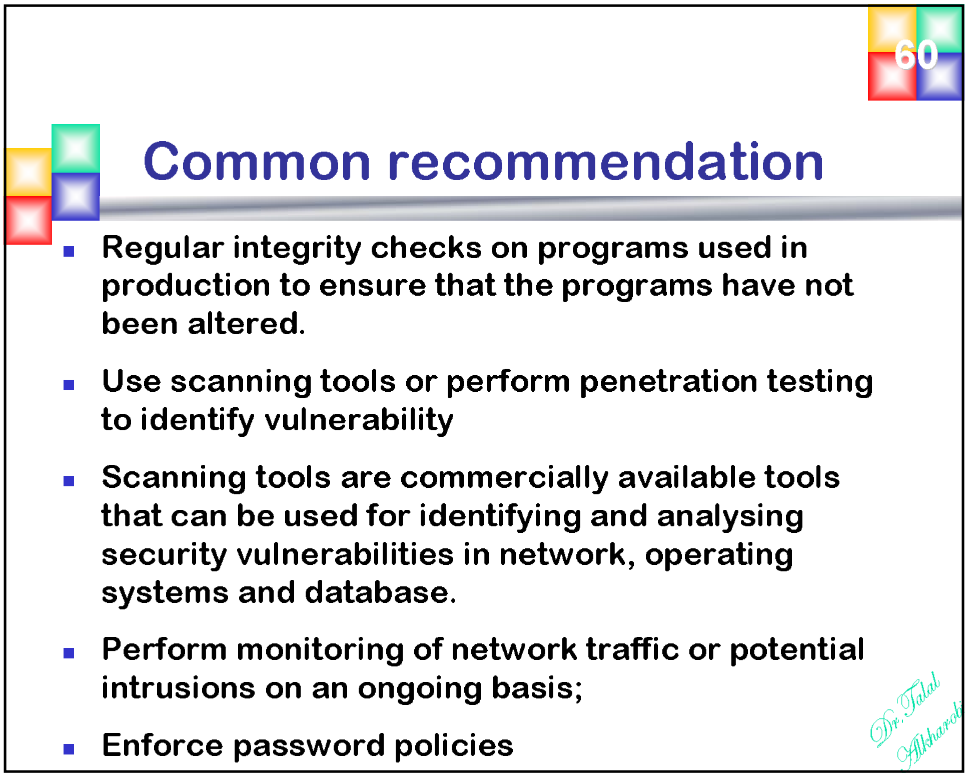
Brute force

- If an attacker captured encrypted messages and then use software to break the code and gain access to messages he may get a user IDs and passwords.
- If the attacker gains access to a user ID that has sufficient privileges, he can create a back door for future access, even if the password of the user ID is subsequently changed.



SSS for Brute Force

- Deploy strong encryption technology and effective key management practices to protect confidentiality of messages, user IDs and passwords;
- Enforce password policies (e.g., mandating minimum length of passwords, or periodic changes in passwords);
- Provide adequate education to customers on security precautions (particularly on setting passwords).
- Obfuscating the data to be encoded, brute force attacks are made less effective as it is more difficult to determine when one has succeeded in breaking the code



Common recommendation

- Regular integrity checks on programs used in production to ensure that the programs have not been altered.
- Use scanning tools or perform penetration testing to identify vulnerability
- Scanning tools are commercially available tools that can be used for identifying and analysing security vulnerabilities in network, operating systems and database.
- Perform monitoring of network traffic or potential intrusions on an ongoing basis;
- Enforce password policies