28 JANUARY THURSDAY

WK 05 • 028-338

Cyber Security

JANUARY 2016

S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Information Security Threats

In Information security, threats can be many like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage & information extortion.

Threat can be anything that can take advantage of a vulnerability to breach security & negativity alter, erase, harm object or objects of interest.

Software attacks means attack by Viruses, Worms, Trojan Horses etc.

Many users believe that malware, virus, worms, bots are all same things.

But they are not same, only similarity is that they all are malicious software that behave differently.

A threat is something that may or may not happen, but it has the potential to cause serious damage.

Threats can lead to attacks on computer systems, networks & more.

2016

Security refers to providing a protection system to computer system resources such as CPU, memory, disk, software programs & most importantly data/ information stored in the computer system.

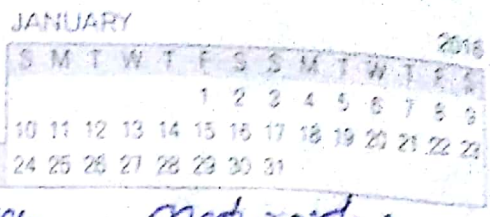
If a computer program is run by an unauthorized user, then he/she may cause severe damage to computer or data stored into it.
So a computer system must be protected against unauthorized access, malicious access to system memory, viruses, worms, etc.

Some of security threats are:

1. Privilege Escalation: Software programs often have bugs that can be exploited. These bugs can be used to gain access to certain resources with higher privileges that can bypass security controls.

2. Virus:- The term virus has been used as a catchall phrase for many threats. Essentially, a virus is a computer program that like a medical virus, has the ability to replicate & infect other computers.

2016



Viruses are transmitted over networks or via USB drives & other portable media.

3. Worm :- A worm is a specific type of virus. Unlike a typical virus, it's goal isn't to alter system files, but to replicate so many times that it consumes hard disk space or memory. Worm victims will notice their computer running slower or crashing.

4. Trojan :- Trojan horses, commonly referred to as Trojan, are programs. They masquerade (masked/related) as normal, safe applications, but their mission is to allow a hacker remote access to your computer. In turn, the infected computer can be used as part of a denial of service attack and data theft can occur

A particularly nasty Trojan is a keystroke logger that can be used to capture passwords, credit card numbers and other sensitive information.

5 Spyware :- Spyware usually invades computers through software downloads.

31 SUNDAY

2016

Shareware & freeware downloads, in addition to peer-to-peer file sharing are typical infection points.

Like Trojans, spyware can pilfer system sensitive information, but are often used as advertising tools as well. The intent is to gather a user's info by monitoring Internet activity & transmitting that to an attacker.

6. Spam :- Some view spam is more of an annoyance than a threat. Still, legislation like the CAN-SPAM Act, has been enacted to help combat the problem, so that view may not hold weight with many others.
Spam is unsolicited junk mail. It comes in the form of an advertisement, and in addition to being a time waster, has the ability to consume precious n/w bandwidth.

7. Adware : Similar to spyware, adware observes a user's internet browsing habit. But the purpose is to be able to better target the display of web advertisements.

8. Rootkits :- Rootkits are some of the most difficult to detect. They are activated when your system boots up- before antivirus software is started. Rootkits allow the installation of files and accounts, or the purposes of intercepting (stop) sensitive information.

9. Botnets :- Botnets are created with a Trojan & reside on IRC networks. The bot can launch an IRC client, and join chat room in order to spam and launch denial (disallowance) of service attacks.

10. Logic bomb :- You may have also heared the term "slag code" to refer to logic bombs. They are bits of code added to software that will set off a specific function.
Logic bombs are similar to viruses in that they can perform malicious actions like deleting files and corrupting data.

04 FEBRUARY
THURSDAY
WK 06 • 035-331

Cyber offence & cyber crime

FEBRUARY 2016
S M T W T F S S M T W T F S
1 2 3 4 5 6 7 8 9 10 11 12 13
14 15 16 17 18 19 20 21 22 23 24 25 26 27
28 29

Cybercrime, or computer-oriented crime is the crime that involves a computer and a network.

The computer may have been used in the commission of a crime, or it may be the target.

Cybercrimes can be defined as the offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet & mobile phones.

Cybercrime may threaten a person or a nation's security and financial health.

Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, unwarranted mass-surveillance, sextortion & child grooming.

2016

Rahul Kundral

These are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise.

Cyber Crimes

1. Hacking :- Hacking is an act commited by an intruder by accesing your computer system without your permission. There are two types of hackers.
Hackers that display destructive conduct also known as "Crackers" and are also called as "Black Hat" Hackers. Such hackers break into systems to steal personal banking information, a coorporation's financial data. etc.

Others are reffered as "White Hat" hackers these are against the abuse of computer system.
Grey hat → a cross b/w Black & white Hackers uses various techniques to get to you via the internet.

a) SQL Injections : A technique that allows hackers to play upon the security vulnerabilities of the software that runs on a website. It can be used to attack any type of unprotected database.

2016

Rahul Kundeel

This process involves entering portions of SQL code into a web form entry field - most commonly usernames and passwords - to give hackers further access to the site backened, or to a particular user's account.

An SQL injection is usually an additional command that when inserted into the web form, tries to change the content of the database to reflect a successful login.

It can also be used to retrieve info such as credit card numbers or password from unprotected sites.

b) Theft of FTP Passwords :- This is another very common way to tamper with websites. FTP passwords hacking takes advantage of the fact that many webmasters store their website login info on their poorly protected PCs.

The thief searches the victim's system for FTP login details, and then relays them to his own remote computer and then can further logs into the website & can modifies the web pages as pleases to the one.

07 SUNDAY

c. Cross-site scripting :- Also known as XSS is very easy way of circumventing a security system. Cross-site scripting is a hard-to-find loophole in a web site, making it vulnerable to attack.

In a typical XSS attack, the hacker infects a web page with a malicious client-side script or program.

When you visit the web page, the script is automatically downloaded to your browser & executed.

2. VIRUS dissemination :- Viruses are computer programs that attach themselves to or infect a system or files, and have a tendency to circulate to other computers on a network.

They disrupt the computer operation and affect the data stored - either by modifying it or by deleting it altogether.

"Worms" unlike viruses don't need a host to cling on to. They merely replicate until they eat up all available memory in the system.

3. Logic bombs : is also known as 'slag code' is a malicious piece of code which is intentionally inserted into software to execute a malicious task when triggered by a specific event. It's not a virus, although it usually behaves in a similar manner.

4. Denial-of-Service attack :- A DoS attack is an explicit attempt by attackers to deny service to intended users of that service.
It involves flooding a computer resource with more requests than it can handle consuming its available bandwidth which results in server overloaded. This causes the resources to crash or slow down significantly so that no one can access it.

5 Phishing :- This is a technique of extracting confidential info such as credit card no. & username paswords combos by masquerading as a legitimate enterprise Phishing is typically carried out by email spoofing

6. Email bombing & spamming :- It is characterised by an abuser sending huge volumes of email to a target address resulting in victim's email account or mail servers crashing.

7. Web jacking :- Web jacking derives its name from "hijacking". Here the hacker takes the control of a website fraudently. He may change the content of the original site or even redirect the user to another fake similar looking page controlled by him.

8. Cyber - stalking :- is a new form of internet crime in our society when a person is pursued or followed online. A cyber stalker doesn't physically follow his victim; he does it virtually by following his online activity to harvest information about the stalkee & harass him & make threats using verbal intimidation. It's an invasion of one's online privacy.

9. Data - diddling :- It is an unauthorised altering of data before or during entry into a computer system,

and then changing it back after processing is done.
Using this technique, hacker can change the original information
This is one of the simplest methods of commiting a computer related crime, because even a computer amateur can do it.

10. Identity Theft & Credit Card Fraud.

11. Salami sliving attack.

12. Software privacy.

Essential Cyber Security Measures

* Use strong passwords :- Strong passwords are vital to good online security.
Make your password difficult to guess by :-

- using combination of capital & lower-case letters, numbers & symbols.
- making it b/w eight and 12 characters long.
- avoiding the we of personal data.
- changing it regularly
- never using it for multiple accounts
- using two factor authentication.

2016

* Control access :- Make sure that individuals can only access data and services for which they are authorised. For example :-

- restrict access to unauthorised users.
- limit access to data or services through application controls.
- restrict what can be copied from the system & saved to storage devices.
- limit sending & receiving of certain types of email attachment.

* Put up a firewall :- Firewalls are effectively gatekeepers b/w your computer & internet, and one of the major barriers to cyber threats such as viruses and malware. Make sure that you set up your firewall devices properly as they may not be fully effective.

* Use security software :- You should use security software, such as anti-spyware and anti-virus programs, to help detect & remove malicious code if it slips ind your network.

13 FEBRUARY
SATURDAY
WK 07 • 044-322

FEBRUARY 2019
S M T W T F S S M T W T F S
1 2 3 4 5 6 7 8 9 10 11 12 13
14 15 16 17 18 19 20 21 22 23 24 25 26 27
28 29

* Update programs and systems regularly:-

Updates contain vital security upgrades that help protect against known bugs and vulnerabilities.
Make sure that you keep your software & devices up-to-date to avoid falling prey to criminals.

* MONITOR for Intrusion :-

You can use intrusion detectors to monitor system & network activity.
If a detection system suspects a potential security breach, it can generate an alarm, such as an email alert, based upon the type of activity it has identified.

* Raise awareness :- Make sure to be awared about regular cyber security

14 SUNDAY

Biometric Security

is used to authenticate and provide access to a facility or system based on the automatic and instant verification of an individual's physical characteristics.

Because biometric security evaluates an individual's bodily elements or biological data, it is the strogest and foolproof physical security technique used for identity verification.

Biometric security include fingerprints, eye tenture, voice, hand patterns & facial recognition.

A individual's body characteristics are prestored in a biometric security system or scanner, which may be accessed by authorized personnel.

When an individual walks into a facility or tries to gain access to a system, the biometic scanner evaluates his/her physical characteristics, which are matched with the stored records.
If a match is located, the individual is granted acces.

16 FEBRUARY TUESDAY

WK 08 • 047-319

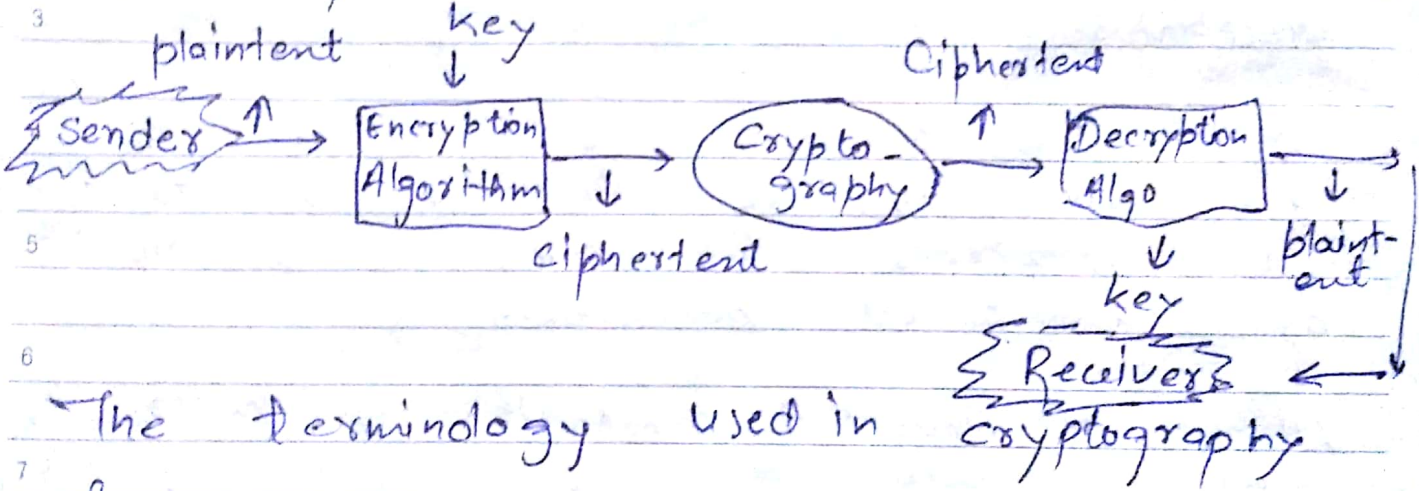
Cryptography

is a technique to provide message confidentiality.

- The term Cryptography means "secret writing".

- It is an art science of transforming messages so as to make them secure and immune to attacks.

- Cryptography involves the process of encryption and decryption. This process is depicted.



The terminology used in cryptography is given below:-

1) Plaintext :- The original message or data that is fed into the algorithm as input is called plaintext.

2016

2. Encryption algorithm : The encryption algorithm is the algorithm that performs various substitutions and transformations on the plaintext.

→ Encryption is the process of changing plaintext into cipher text. ←

3. Ciphertext : Ciphertext is the encrypted form the message. It is the scrambled message produced as output. It depends upon the plaintext and the key.

4. Decryption algorithm : The process of changing Ciphertext into plaintext is known as decryption.

Decryption algorithm is essentially the encryption algorithm run in reverse.

It takes the Ciphertext and the key and produces the original plaintext.

18 FEBRUARY
THURSDAY
WK 08 • 049-317

FEBRUARY 2016
S M T W T F S S M T W T F S
1 2 3 4 5 6 7 8 9 10 11 12 13
14 15 16 17 18 19 20 21 22 23 24 25 26 27
28 29

5. Key :- It also acts as input to to the encryption algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.

Thus a key is a number or a set of number that the algorithm uses to perform encryption and decryption.

Cryptography can be used to achieve several goals of information security, including confidentiality, integrity & authentication.

* Confidentiality :- First, cryptography protects the confidentiality of information. Even when the transmission or storage medium has been compromised, the encrypted info is practically useless to unauthorized persons without the proper ways for decryption.

* Integrity :- Cryptography can also be used to ensure the integrity of

2016

information through the use of hashing algorithms and message digest.

Authentication:- Finally, cryptography can be used for authentication services through digital signatures, digital certificates or a Public Key Infrastructure

CYBER LAW

Cyber law is the part of the overall legal system that deals with the Internet, cyberspace, and their respective legal issues.

It is also known as Internet law

Cyberlaws prevent or reduce large scale damage from cybercriminal activities by protecting information access, privacy communications, intellectual property (IP), and freedom of speech related to the use of Internet, websites, email, computers, cell phones, software & hardware such as data storage.

20 FEBRUARY SATURDAY

WK 08 • 051-315

FEBRUARY 2016

S M T W T F S S M T W T F S
1 2 3 4 5 6 7 8 9 10 11 12 13
14 15 16 17 18 19 20 21 22 23 24 25 26 27
28 29

Just like any law, a cyber law is created to help, protect people & organizations on the Internet & help maintain order. If someone breaks a cyber law or rule, it allows another person or organisation to take action against that person.

The Indian Information Technology Act ("IT Act") wass passed in 2000.

On the other hand most of the companies are still uninformed of the strict provision of the law.

The rising use of Information & Communication Technology has given go up to serious compliance concerns, which if unnoticed may attach various civil and criminal sanctions.

Cyberlaw is vital because it touches almost all aspects of transactions and behaviour on and concerning the Internet, the World Wide Web and cyberspace.

21 SUNDAY Primarily it may seem that Cyber laws is a very technical field & that it does not have any attitude to most activities in Cyberspace.

2016