For Prof. Rajendra Singh (Rajju Bhaiya) University Students

Cyber Law & Internet Security

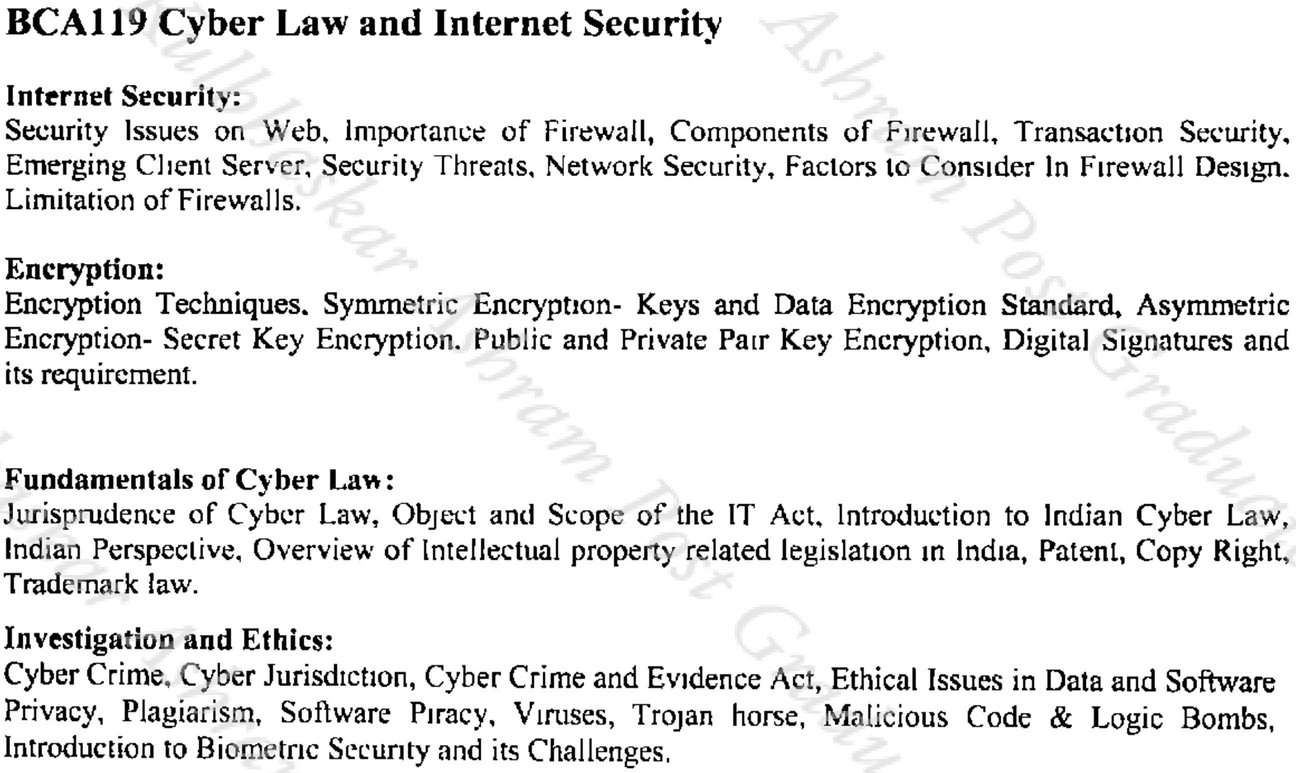
BCA– IVth Sem

Prepared By

SUSHANT SRIVASTAVA
(Assistant Professor)
Kulbhaskar Ashram Post Graduate College, Prayagraj

UNIT-I

Introduction:



BCA119 Cyber Law and Internet Security

Internet Security:
Security Issues on Web, Importance of Firewall, Components of Firewall, Transaction Security, Emerging Client Server, Security Threats, Network Security, Factors to Consider In Firewall Design, Limitation of Firewalls.

Encryption:
Encryption Techniques, Symmetric Encryption- Keys and Data Encryption Standard, Asymmetric Encryption- Secret Key Encryption, Public and Private Pair Key Encryption, Digital Signatures and its requirement.

Fundamentals of Cyber Law:
Jurisprudence of Cyber Law, Object and Scope of the IT Act, Introduction to Indian Cyber Law, Indian Perspective, Overview of Intellectual property related legislation in India, Patent, Copy Right, Trademark law.

Investigation and Ethics:
Cyber Crime, Cyber Jurisdiction, Cyber Crime and Evidence Act, Ethical Issues in Data and Software Privacy, Plagiarism, Software Piracy, Viruses, Trojan horse, Malicious Code & Logic Bombs, Introduction to Biometric Security and its Challenges.

Q 1: What do you mean by Web security?

Answer:

Web application security is a branch of information security that deals specifically with security of websites, web applications and web services. At a high level, web application security draws on the principles of application security but applies them specifically to internet and web systems.

Website security is the last thing that many companies will think while they're on their website building process. Even if a website security expert is hired in their team, they'll always focus how and when to put their websites live – leaving major vulnerabilities unattended.
You have to understand that an effective approach to website security must be proactive and defensive. This is a gentle reminder to you that website security must be taken seriously. It's good to be worried about the bad effects of it to your business and reputation.
List of the 5 website security issues and notable website creation mistakes that you should know:

- Security Issues with Websites #1: Injection Mistakes
- Security Issues with Websites #2: Cross Site Scripting (XSS)
- Security Issues with Websites #3: Not Updating Security Settings
- Security Issues with Websites #4: Exposing Sensitive Data
- Security Issues with Websites #5: A Lost Function Level Access Control

Security Issues with Websites #1: Injection Mistakes

If you want a smooth filter of untrusted input, injections flaws must be avoided at all cost. An injection flaw can let you pass unfiltered data to the SQL server, to the browser, to the LDAP server (LDAP injection), or anywhere else. These website layers can be used by a hacker to inject commands. This can result in loss of data and hacking your own website. In fact, it can also infect other websites as well.

Security Issues with Websites #2: Cross Site Scripting (XSS)

This is another form injection vulnerability that can input sanitization failure. A hacker sets up your web application JavaScript tags on input. When this input is returned to the user unsanitized, the user's browser will carry it out. It can be as simple as crafting a link and persuading a user to click it, or it can be something much more sinister. On page load the script runs and, for example, can be used to post your cookies to the hacker.

Security Issues with Websites #3: Not Updating Security Settings

Any responsible website security personnel will always make sure to personalize your security settings such as passwords and authentications. Perhaps, some people are still human to miss important things in their jobs. Some concrete scenarios are:

- They let the application run with debug enabled in production.
- They didn't change default keys and passwords.
- They left the directory listing enabled on the server, which leaks valuable information.
- They allow unnecessary services running on the machine.
- They operated an outdated software (think WordPress plugins, old PhpMyAdmin).
- They didn't fix some pop-up messages on error information.

Security Issues with Websites #4: Exposing Sensitive Data

It's a huge failure for a website security personnel – to not encrypt and not protect your sensitive data. Information (such as credit card details) and user passwords should never travel or be stored unencrypted, and passwords should always be hashed. And while it goes without saying that session IDs and sensitive data should not be traveling in the URLs. Moreover, sensitive cookies should have the secure flag on, this is very important and cannot be over-emphasized.

Security Issues with Websites #5: A Lost Function Level Access Control

An authorization failure can also disrupt your website. It means that when a function is called on the server, proper authorization was not performed. A lot of times, website developers rely on the fact that the server side generated the UI. They think that the functionality that is not supplied by the server cannot be accessed by the client. It is not as easy as they thought, as a hacker can always fake requests to the "hidden" functionality and will not be prevented by the fact that the UI doesn't make this functionality easily accessible. Nothing can stop an attacker from discovering this functionality and abusing it if authorization is missing.

It is important to always keep in mind that the 5 security issue with websites mentioned above are just a few to mention. There are a lot more website security issues that website security personnel deals with as technology develops and changes.

Q 2: What is importance and types of firewall.

Answer:

Firewall is a software or hardware device that protects your computer from being attacked over the internet by hackers, viruses, and worms. This may occur either at a large corporate network, or simply at a small home network; both have the same security issues.

Here are five types of firewalls that have played significant roles as the firewall category has evolved:

- Packet filtering firewalls. ...
- Circuit-level gateways. ...
- Stateful inspection firewalls. ...
- Application-level gateways. ...
- Next-gen firewalls.

Packet filtering firewalls

This, the original type of firewall, operates inline at junction points where devices such as routers and switches do their work.

However, this firewall doesn't route packets, but instead compares each packet received to a set of established criteria -- such as the allowed IP addresses, packet type, port number, etc. Packets that are flagged as troublesome are, generally speaking, unceremoniously dropped -- that is, they are not forwarded and, thus, cease to exist.

Circuit-level gateways

Using another relatively quick way to identify malicious content, these devices monitor the TCP handshakes across the network as they are established between the local and remote hosts to determine whether the session being initiated is legitimate -- whether the remote system is considered trusted. They don't inspect the packets themselves, however.

Stateful inspection firewalls

State-aware devices, on the other hand, not only examine each packet, but also keep track of whether or not that packet is part of an established TCP session. This offers more security than either packet filtering or circuit monitoring alone, but exacts a greater toll on network performance.

A further variant of stateful inspection is the multilayer inspection firewall, which considers the flow of transactions in process across multiple layers of the ISO Open Systems Interconnection seven-layer model.

Application-level gateways

This kind of device, technically a proxy, and sometimes referred to as a proxy firewall, combines some of the attributes of packet filtering firewalls with those of circuit-level gateways. They filter packets not only according to the service for which they are intended -- as specified by the destination port -- but also by certain other characteristics, such as the HTTP request string.

While gateways that filter at the application layer provide considerable data security, they can dramatically affect network performance.

Next-gen firewalls

This looser category is the most recent -- and least-well delineated -- of the types of firewalls. A typical next-gen product combines packet inspection with stateful inspection, but also includes some variety of deep packet inspection.

Q 3: What factor consider in firewall design.

Answer:

A firewall is a device or devices that control traffic between different areas of your network. In a more robust design you typically see two or three firewall devices, as well as many other security components to protect company resources. In a firewall design, I refer to the security solution as a firewall system, indicating that many devices are being used to protect your resources.

As you will see in this section, you should follow some practical guidelines when developing a firewall system. These can include packet and application firewalls, application gateway and ATFs, host-based firewalls, and, more than likely, hybrid firewalls, as well as many other security devices, such as VPN concentrators, IDS devices, authentication security servers, and many other components.

After briefly covering the components in a security solution, I discuss some various designs that commonly are used to protect resources. Then I discuss their advantages and disadvantages and cover management issues.

Design Guidelines

You should follow five basic guidelines when designing a firewall system:

- Develop a security policy.
- Create a simple design solution.
- Use devices as they were intended.
- Implement a layered defense to provide extra protection.
- Consider solutions to internal threats that should be included in your design.

The following subsections cover these five key design points.

Developing a Security Policy

One of the first things you do when designing a firewall system is to create a security policy. The policy should define acceptable and unacceptable behavior, should state restrictions to resources, and should adhere to the company's business plan and policies. Without a security policy, it is practically impossible to develop a security solution that will meet your company's needs.

The key to a good design is basing it on a security policy. Basically, a policy defines who is allowed to access resources, what they are allowed to do with resources, how resources should be protected (in general terms), and what actions are taken when a security issue occurs. Without a security policy, it is impossible to design a firewall system that will protect your assets. In other words, if you don't have a security policy, what should you protect? How much should you protect resources? Who is allowed to access resources? If your policy does not define these items, it is hard to design and implement a solution based on hunches. Actually, without a security policy, the firewall system that you put in place might be creating a security risk: It might not be providing adequate protection to your company's resources.

Designing a security policy is beyond the scope of this book. However, it minimally should address the following items:

- The resources that require access from internal and external users
- The vulnerabilities associated with these resources
- The methods and solutions that can be used to protect these resources
- A cost-benefit analysis that compares the different methods and solutions

Designing Simple Solutions

A firewall system design should be kept simple and should follow your security policy. The simpler the design is, the easier it will be to implement it, maintain it, test and troubleshoot it, and adapt it to new changes. Many people like to call this the KISS principle: Keep it simple, stupid. The last kind of problem you want to deal with is a design or configuration error that leaves your network open to all different kinds of attacks.

CAUTION

Complex solutions are prone to design and configuration errors, and are difficult to test and troubleshoot. The simpler you can make the design, the easier it will be to manage it.

Using Devices Correctly

Network devices have functional purposes; they were built with a specific purpose in mind. For example, a Layer 2 switch is used to break up a collision or bandwidth domain, and it also uses VLANs to break up broadcast domains: It is typically not a good device to use to filter traffic because the filtering is done by creating filtering rules based on MAC addresses. The problem with this approach is that MAC addresses tend to change quite a bit: NICs fail, PCs and servers are upgraded, devices are moved to different locations in the network, and so on. Filtering is done best when logical addressing is deployed.

Using the wrong product to solve a security problem can open you to all kinds of security threats. For example, assume that you want to use an IDS to detect different kinds of network threats. You notice that your Cisco router has the capability in the Cisco IOS Firewall feature set, and you decide to enable it, feeling secure that your Cisco router will generate an alarm when an attack occurs. If you had taken time to read the security material related to Cisco routers, you would have realized that Cisco routers can detect only a few dozen different kinds of networking attacks (typically, the most common ones). Therefore, for all the other hundreds of kinds of attacks, your Cisco router will not be capable of detecting them, leaving you exposed. In this example, a better solution would have been to purchase an IDS solution that can detect hundreds of different kinds of attacks.

Q 4: What is Network Security Threats.

Answer:

The old childhood warning “Stranger danger!” has withstood the test of time even in our modern, developed world. Now that most of our daily procedures and activities are automatized and available for use on the Internet, we need to take the same level of precaution we did as children, crossing to the other side of the street whenever we saw a suspicious stranger. This precaution is needed even more after seeing some critical statistics surface, claiming that nearly one-third of the world's computers are infected with some type of malware.

The most common network security threats

1. Computer virus
2. Rogue security software
3. Trojan horse
4. Adware and spyware
5. Computer worm
6. DOS and DDOS attack
7. Phishing
8. Rootkit
9. SQL Injection attack
10. Man-in-the-middle attacks

1. Computer virus

We've all heard about them, and we all have our fears. For everyday Internet users, computer viruses are one of the most common threats to cybersecurity. Statistics show that approximately 33% of household computers are affected with some type of malware, more than half of which are viruses.

Computer viruses are pieces of software that are designed to be spread from one computer to another. They're often sent as email attachments or downloaded from specific websites with the intent to infect your computer — and other computers on your contact list — by using systems on your network. Viruses are known to send spam, disable your security settings, corrupt and steal data from your computer including personal information such as passwords, even going as far as to delete everything on your hard drive.

2. Rogue security software

Leveraging the fear of computer viruses, scammers have a found a new way to commit Internet fraud.

Rogue security software is malicious software that mislead users to believe there is a computer virus installed on their computer or that their security measures are not up to date. Then they offer to install or update users' security settings. They'll either ask you to download their program to remove the alleged viruses, or to pay for a tool. Both cases lead to actual malware being installed on your computer.

3. Trojan horse

Metaphorically, a "Trojan horse" refers to tricking someone into inviting an attacker into a securely protected area. In computing, it holds a very similar meaning — a Trojan horse, or "Trojan," is a malicious bit of attacking code or software that tricks users into running it willingly, by hiding behind a legitimate program.

They spread often by email; it may appear as an email from someone you know, and when you click on the email and its included attachment, you've immediately downloaded malware to your computer. Trojans also spread when you click on a false advertisement.

Once inside your computer, a Trojan horse can record your passwords by logging keystrokes, hijacking your webcam, and stealing any sensitive data you may have on your computer.

4. Adware and spyware

By “adware” we consider any software that is designed to track data of your browsing habits and, based on that, show you advertisements and pop-ups. Adware collects data with your consent — and is even a legitimate source of income for companies that allow users to try their software for free, but with advertisements showing while using the software. The adware clause is often hidden in related User Agreement docs, but it can be checked by carefully reading anything you accept while installing software. The presence of adware on your computer is noticeable only in those pop-ups, and sometimes it can slow down your computer’s processor and internet connection speed.

When adware is downloaded without consent, it is considered malicious.

Spyware works similarly to adware, but is installed on your computer without your knowledge. It can contain keyloggers that record personal information including email addresses, passwords, even credit card numbers, making it dangerous because of the high risk of identity theft.

5. Computer worm

Computer worms are pieces of malware programs that replicate quickly and spread from one computer to another. A worm spreads from an infected computer by sending itself to all of the computer’s contacts, then immediately to the contacts of the other computers.

6. DOS and DDOS attack

Have you ever found yourself waiting impatiently for the online release of a product, one that you’re eagerly waiting to purchase? You keep refreshing the page, waiting for that moment when the product will go live. Then, as you press F5 for the last time, the page shows an error: “Service Unavailable.” The server must be overloaded!

There are indeed cases like these where a website’s server gets overloaded with traffic and simply crashes, sometimes when a news story breaks. But more commonly, this is what happens to a website during a DoS attack, or denial-of-service, a malicious traffic overload that occurs when attackers overflood a website with traffic. When a website has too much traffic, it’s unable to serve its content to visitors.

A DoS attack is performed by one machine and its internet connection, by flooding a website with packets and making it impossible for legitimate users to access the content of flooded website. Fortunately, you can’t really overload a server with a single other server or a PC anymore. In the past years it hasn’t been that common if anything, then by flaws in the protocol.

A DDoS attack, or distributed denial-of-service attack, is similar to DoS, but is more forceful. It’s harder to overcome a DDoS attack. It’s launched from several computers, and the number of computers involved can range from just a couple of them to thousands or even more.

Since it’s likely that not all of those machines belong to the attacker, they are compromised and added to the attacker’s network by malware. These computers can be distributed around the entire globe, and that network of compromised computers is called botnet.

Since the attack comes from so many different IP addresses simultaneously, a DDoS attack is much more difficult for the victim to locate and defend against.

7. Phishing

Phishing is a method of a social engineering with the goal of obtaining sensitive data such as passwords, usernames, credit card numbers.

The attacks often come in the form of instant messages or phishing emails designed to appear legitimate. The recipient of the email is then tricked into opening a malicious link, which leads to the installation of malware on the recipient’s computer. It can also obtain personal information by sending an email that appears to be sent from a bank, asking to verify your identity by giving away your private information.

Uncovering phishing domains can be done easily with SecurityTrails.

8. Rootkit

Rootkit is a collection of software tools that enables remote control and administration-level access over a computer or computer networks. Once remote access is obtained, the rootkit can perform a number of malicious actions; they come equipped with keyloggers, password stealers and antivirus disablers.

Rootkits are installed by hiding in legitimate software: when you give permission to that software to make changes to your OS, the rootkit installs itself in your computer and waits for the hacker to activate it. Other ways of rootkit distribution include phishing emails, malicious links, files, and downloading software from suspicious websites.

9. SQL Injection attack

We know today that many servers storing data for websites use SQL. As technology has progressed, network security threats have advanced, leading us to the threat of SQL injection attacks.

SQL injection attacks are designed to target data-driven applications by exploiting security vulnerabilities in the application's software. They use malicious code to obtain private data, change and even destroy that data, and can go as far as to void transactions on websites. It has quickly become one of the most dangerous privacy issues for data confidentiality. You can read more on the history of SQL injection attacks to better understand the threat it poses to cybersecurity.

10. Man-in-the-middle attacks

Man-in-the-middle attacks are cybersecurity attacks that allow the attacker to eavesdrop on communication between two targets. It can listen to a communication which should, in normal settings, be private.

As an example, a man-in-the-middle attack happens when the attacker wants to intercept a communication between person A and person B. Person A sends their public key to person B, but the attacker intercepts it and sends a forged message to person B, representing themselves as A, but instead it has the attackers public key. B believes that the message comes from person A and encrypts the message with the attackers public key, sends it back to A, but attacker again intercepts this message, opens the message with private key, possibly alters it, and re-encrypts it using the public key that was firstly provided by person A. Again, when the message is transferred back to person A, they believe it comes from person B, and this way, we have an attacker in the middle that eavesdrops the communication between two targets.

UNIT-II

Q 1: What is Encription. Explain encryption methods?

Answer:

Encryption is a technique for transforming information on a computer in such a way that it becomes unreadable. So, even if someone is able to gain access to a computer with personal data on it, they likely won't be able to do anything with the data unless they have complicated, expensive software or the original data key.

The basic function of encryption is essentially to translate normal text into ciphertext. Encryption can help ensure that data doesn't get read by the wrong people, but can also ensure that data isn't altered in transit, and verify the identity of the sender.

3 different encryption methods

There are three different basic encryption methods, each with their own advantages (list courtesy of Wisegeek):

- **Hashing**
  Hashing creates a unique, fixed-length signature for a message or data set. Each "hash" is unique to a specific message, so minor changes to that message would be easy to track. Once data is encrypted using hashing, it cannot be reversed or deciphered. Hashing, then, though not technically an encryption method as such, is still useful for proving data hasn't been tampered with.
- **Symmetric methods**
  Symmetric encryption is also known as private-key cryptography, and is called so because the key used to encrypt and decrypt the message must remain secure, because anyone with access to it can decrypt the data. Using this method, a sender encrypts the data with one key, sends the data (the ciphertext) and then the receiver uses the key to decrypt the data.
- **Asymmetric methods**
  Asymmetric encryption, or public-key cryptography, is different than the previous method because it uses two keys for encryption or decryption (it has the potential to be more secure as such). With this method, a public key is freely available to everyone and is used to encrypt messages, and a different, private key is used by the recipient to decrypt messages.

Any of these methods would likely prove sufficient for proper data security, and a quick Google search will reveal the multitude of software available for data encryption. Data encryption is a necessity (both for legal reasons and otherwise) when transmitting information like PHI, so no matter what method you choose, make sure you're doing everything you can to protect data.

Q 2: Which Types of Encryption are Most Secure?

Answer:

Encryption can protect your consumer information, emails and other sensitive data as well as secure network connections. Today, there are many options to choose from, and finding one that is both secure and fits your needs is a must. Here are four encryption methods and what you should know about each one.

AES

The Advanced Encryption Standard, AES, is a symmetric encryption algorithm and one of the most secure. The United States Government use it to protect classified information, and many software and hardware products use it as well. This method uses a block cipher, which encrypts data one fixed-size block at a time, unlike other types of encryption, such as stream ciphers, which encrypt data bit by bit.

AES is comprised of AES-128, AES-192 and AES-256. The key bit you choose encrypts and decrypts blocks in 128 bits, 192 bits and so on. There are different rounds for each bit key. A round is the process of turning plaintext into cipher text. For 128-bit, there are 10 rounds; 192-bit has 12 rounds; and 256-bit has 14 rounds.

Since AES is a symmetric key encryption, you must share the key with other individuals for them to access the encrypted data. Furthermore, if you don’t have a secure way to share that key and unauthorized individuals gain access to it, they can decrypt everything encrypted with that specific key.

3DES

Triple Data Encryption Standard, or 3DES, is a current standard, and it is a block cipher. It’s similar to the older method of encryption, Data Encryption Standard, which uses 56-bit keys. However, 3DES is a symmetric-key encryption that uses three individual 56-bit keys. It encrypts data three times, meaning your 56-bit key becomes a 168-bit key.

Unfortunately, since it encrypts data three times, this method is much slower than others. Also, because 3DES uses shorter block lengths, it is easier to decrypt and leak data. However, many financial institutions and businesses in numerous other industries use this encryption method to keep information secure. As more robust encryption methods emerge, this one is being slowly phased out.

Twofish

Twofish is a symmetric block cipher based on an earlier block cipher – Blowfish. Twofish has a block size of 128-bits to 256 bits, and it works well on smaller CPUs and hardware. Similar to AES, it implements rounds of encryption to turn plaintext into cipher text. However, the number of rounds doesn’t vary as with AES; no matter the key size, there are always 16 rounds.

In addition, this method provides plenty of flexibility. You can choose for the key setup to be slow but the encryption process to be quick or vice versa. Furthermore, this form of encryption is unpatented and license free, so you can use it without restrictions.

RSA

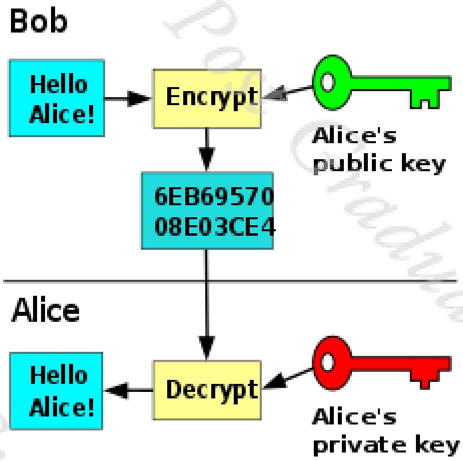
This asymmetric algorithm is named after Ron Rivest, Adi Shamir and Len Adelman. It uses public-key cryptography to share data over an insecure network. There are two keys: one public and one private. The public key is just as the name suggests: public. Anyone can access it. However, the private key must be confidential. When using RSA cryptography, you need both keys to encrypt and decrypt a message. You use one key to encrypt your data and the other to decrypt it.

According to Search Security, RSA is secure because it factors large integers that are the product of two large prime numbers. Additionally, the key size is large, which increases the security. Most RSA keys are 1024-bits and 2048-bits long. However, the longer key size does mean it's slower than other encryption methods.

While there are many additional encryption methods available, knowing about and using the most secure ones ensures your confidential data stays secure and away from unwanted eyes.

Q 3: What is Asymmetric cryptography?

Answer:



Asymmetric **cryptography**, also known as **public key cryptography**, uses **public and private keys** to **encrypt** and decrypt data. ... One **key** in the pair can be shared with everyone; it is called the **public key**. The other **key** in the pair is kept secret; it is called the **private key**.

Public-key cryptography, or asymmetric cryptography, is a cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner. The generation of such keys depends on cryptographicalgorithms based on mathematical problems to produce one-way functions. Effective security only requires keeping the private key private; the public key can be openly distributed without compromising security.

In such a system, any person can encrypt a message using the receiver's public key, but that encrypted message can only be decrypted with the receiver's private key.

Robust authentication is also possible. A sender can combine a message with a private key to create a short digital signature on the message. Anyone with the corresponding public key can combine a message, a putative digital signature on it, and the known public key to verify whether the signature was valid, i.e. made by the owner of the corresponding private key.

Public key algorithms are fundamental security ingredients in modern cryptosystems, applications and protocols assuring the confidentiality, authenticity and non-repudiability of electronic communications and data storage. They underpin various Internet standards, such as Transport Layer Security (TLS), S/MIME, PGP, and GPG. Some public key algorithms provide key distribution and secrecy (e.g., Diffie–Hellman key exchange), some provide digital signatures (e.g., Digital Signature Algorithm), and some provide both (e.g., RSA).

Q 4: What is digital Signature and its requirnment.

Answer:

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. The digital equivalent of a handwritten signature or stamped seal, a digital signature offers far more inherent security, and it is intended to solve the problem of tampering and impersonation in digital communications.

Digital signatures can provide the added assurances of evidence of origin, identity and status of an electronic document, transaction or message and can acknowledge informed consent by the signer.

In many countries, including the United States, digital signatures are considered legally binding in the same way as traditional document signatures. The United States Government Publishing Office publishes electronic versions of the budget, public and private laws, and congressional bills with digital signatures.

How digital signatures work

Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm, such as RSA, one can generate two keys that are mathematically linked: one private and one public.

Digital signatures work because public key cryptography depends on two mutually authenticating cryptographic keys. The individual who is creating the digital signature uses their own private key to encrypt signature-related data; the only way to decrypt that data is with the signer's public key. This is how digital signatures are authenticated.

Digital signature technology requires all the parties to trust that the individual creating the signature has been able to keep their own private key secret. If someone else has access to the signer's private key, that party could create fraudulent digital signatures in the name of the private key holder.

How to create a digital signature

To create a digital signature, signing software -- such as an email program -- creates a one-way hash of the electronic data to be signed. The private key is then used to encrypt the hash. The encrypted hash -- along with other information, such as the hashing algorithm -- is the digital signature.

The reason for encrypting the hash instead of the entire message or document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter. This saves time as hashing is much faster than signing.

The value of a hash is unique to the hashed data. Any change in the data, even a change in a single character, will result in a different value. This attribute enables others to validate the integrity of the data by using the signer's public key to decrypt the hash.

If the decrypted hash matches a second computed hash of the same data, it proves that the data hasn't changed since it was signed. If the two hashes don't match, the data has either been tampered with in some way -- integrity -- or the signature was created with a private key that doesn't correspond to the public key presented by the signer -- authentication.

A digital signature can be used with any kind of message -- whether it is encrypted or not -- simply so the receiver can be sure of the sender's identity and that the message arrived intact. Digital signatures make it difficult for the signer to deny having signed something -- assuming their private key has not been compromised -- as the digital signature is unique to both the document and the signer and it binds them together. This property is called nonrepudiation.

Digital signatures are not to be confused with digital certificates. A digital certificate, an electronic document that contains the digital signature of the issuing certificate authority, binds together a public key with an identity and can be used to verify that a public key belongs to a particular person or entity.

Most modern email programs support the use of digital signatures and digital certificates, making it easy to sign any outgoing emails and validate digitally signed incoming messages. Digital signatures are also used extensively to provide proof of authenticity, data integrity and nonrepudiation of communications and transactions conducted over the internet.

Digital signature vs. electronic signature

While *digital signature* is a technical term, defining the result of a cryptographic process that can be used to authenticate a sequence of data, the term electronic signature -- or *e-signature* -- is a legal term that is defined legislatively.

UNIT-III, IV

Q 1: What is Jurisprudence of Cyber Law.

Answer:

Jurisprudence studies the concepts of law and the effect of social norms and regulations on the development of law.
Jurisprudence refers to two different things.

1. The philosophy of law, or legal theory
2. Case Law

Legal theory does not study the characteristics of law in a particular country but studies law in general i.e. those attributes common to all legal systems.

Case law is the law that is established through the decisions of the courts and other fficials. Case law assumes even greater significance when the wordings of a particular law are ambiguous. The interpretation of the Courts helps clarify the real objectives and meaning of such laws.

What is Cyber Law?

Cyber Law is the law governing cyber space. Cyber space is a very wide term and includes computers, networks, software, data storage devices (such as hard disks, USB disks etc), the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc.

Law encompasses the rules of conduct:

1) that have been **approved** by the government, and
2) which are in **force** over a certain territory, and
3) which must be **obeyed** by all persons on that territory.

Violation of these rules could lead to government action such as imprisonment or fine or an order to pay compensation.

Cyber law encompasses laws relating to:

1. Cyber Crimes
2. Electronic and Digital Signatures
3. Intellectual Property
4. Data Protection and Privacy

Cyber crimes are unlawful acts where the computer is used either as a tool or a target or both. The enormous growth in electronic commerce (e-commerce) and online share trading has led to a phenomenal spurt in incidents of cyber crime.

Electronic signatures are used to authenticate electronic records. Digital signatures are one type of electronic signature. Digital signatures satisfy three major legal requirements – signer authentication, message authentication and message integrity. The technology and efficiency of digital signatures makes them more trustworthy than hand written signatures.

Intellectual property is refers to creations of the human mind e.g. a story, a song, a painting, a design etc. The facets of **intellectual property** that relate to cyber space are covered by cyber law. These include:

1) **copyright law** in relation to computer software, computer source code, websites, cell phone content etc,
2) software and source code **licences**
3) **trademark law** with relation to domain names, meta tags, mirroring, framing, linking etc
4) **semiconductor law** which relates to the protection of semiconductor integrated circuits design and layouts,
5) **patent law** in relation to computer hardware and software.

Data protection and privacy laws aim to achieve a fair balance between the privacy rights of the individual and the interests of data controllers such as banks, hospitals, email service providers etc. These laws seek to address the challenges to privacy caused by collecting, storing and transmitting data using new technologies.

Q 2: What is Need for Cyber Law.
Answer:

There are various reasons why it is extremely difficult for conventional law to cope with cyberspace. Some of these are discussed below.

1) Cyberspace is an **intangible** dimension that is impossible to govern and regulate using conventional law.
2) Cyberspace has complete **disrespect for jurisdictional boundaries**.
3) Cyberspace handles **gigantic traffic volumes every second**. Billions of emails are crisscrossing the globe even as we read this, millions of websites are being accessed every minute and billions of dollars are electronically transferred around the world by banks every day.
4) Cyberspace is absolutely **open to participation by all**.
5) Cyberspace offers **enormous potential for anonymity** to its members.
6) exchanged between cyber-citizens.
7) Cyberspace offers never-seen-before **economic efficiency**. Billions of dollars worth of software can be traded over the Internet without the need for any government licenses, shipping and handling charges and without paying any customs duty.
8) Electronic information has become the main object of cyber crime. It is characterized by **extreme mobility**, which exceeds by far the mobility of

persons, goods or other services. International computer networks can transfer huge amounts of data around the globe in a matter of seconds.

9) A software source code worth crores of rupees or a movie can be **pirated across the globe** within hours of their release.

10) **Theft of** corporeal **information** (e.g. books, papers, CD ROMs, floppy disks) is easily covered by traditional penal provisions. However, the problem begins when electronic records are copied quickly.

Q 3: Jurisprudence of Indian Cyber Law..
Q 3: Object and Scope of IT Act.
Answer:

The primary source of cyber law in India is the **Information Technology Act**, 2000 (IT Act) which came into force on 17 October 2000.

The primary purpose of the Act is to provide **legal recognition to electronic commerce** and to facilitate filing of **electronic records with the Government**.

The IT Act also penalizes various **cyber crimes** and provides strict punishments (imprisonment terms upto 10 years and compensation up to Rs 1 crore).

An **Executive Order** dated 12 September 2002 contained instructions relating provisions of the Act with regard to protected systems and application for the issue of a Digital Signature Certificate.

Minor errors in the Act were rectified by the **Information Technology (Removal of Difficulties) Order**, 2002 which was passed on 19 September 2002.

The IT Act was amended by the **Negotiable Instruments (Amendments and Miscellaneous Provisions) Act**, 2002. This introduced the concept of electronic cheques and truncated cheques.

Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004 has provided the necessary legal framework for filing of documents with the Government as well as issue of licenses by the Government.

It also provides for payment and receipt of fees in relation to the Government bodies.

On the same day, the **Information Technology (Certifying Authorities) Rules**, 2000 also came into force.

These rules were amended in 2003, 2004 and 2006.

Q 4: Write Short notes on.

1. **Patent**
2. **Copy Right**
3. **Trademark**
4. **Plagiarism**
5. **Software Piracy**
6. **Viruses**
7. **Trojan Horse**
8. **Malicious Code**
9. **Logic Bombs**
10. **Biometric Security and its Challenges**

Answer:

Patent

A **patent** is a form of intellectual property. A patent gives its owner the right to exclude others from making, using, selling, and importing an invention for a limited period of time, usually twenty years. The patent rights are granted in exchange for an enabling public disclosure of the invention. In most countries patent rights fall under civil law and the patent holder needs to sue someone infringing the patent in order to enforce his or her rights. In some industries patents are an essential form of competitive advantage; in others they are irrelevant.

The procedure for granting patents, requirements placed on the patentee, and the extent of the exclusive rights vary widely between countries according to national laws and international agreements. Typically, however, a granted patent application must include one or more claims that define the invention. A patent may include many claims, each of which defines a specific property right. These claims must meet relevant patentability requirements, such as novelty, usefulness, and non-obviousness.

Under the World Trade Organization's (WTO) TRIPS Agreement, patents should be available in WTO member states for any invention, in all fields of technology, provided they are new, involve an inventive step, and are capable of industrial application.[4]Nevertheless, there are variations on what is patentable subject matter from country to country, also among WTO member states. TRIPS also provide that the term of protection available should be a minimum of twenty years.

Copyright

Copyright is a legal right, existing in many countries, that grants the creator of an original work exclusive rights to determine whether, and under what conditions, this original work may be used by others. This is usually only for a limited time. Copyright is one of two types of intellectual property rights, the other is industrial property rights.

Copyright is applicable to certain forms of creative work. Some, but not all jurisdictions require "fixing" copyrighted works in a tangible form. It is often shared among multiple authors, each of whom holds a set of rights to use or license the work, and who are commonly referred to as rights holders. These rights frequently include reproduction, control over derivative works, distribution, public performance, and moral rights such as attribution.

Copyrights can be granted by public law and are in that case considered "territorial rights". This means that copyrights granted by the law of a certain state, do not extend beyond the territory of that specific jurisdiction.

Typically, the public law duration of a copyright expires 50 to 100 years after the creator dies, depending on the jurisdiction.

Copyright licenses can also be granted by those deputized by the original claimant, and private companies may request this as a condition of doing business with them. Services of internet platform providers like YouTube, Facebook, GitHub, Hotmail, DropBox, Instagram, WhatsApp or Twitter only can be used when users grant the platform provider beforehand the right to co-use all uploaded content, including all material exchanged per email, chat or cloud-storage. These copyrights only apply for the firm that operates such a platform, no matter in what jurisdiction the platform-services are being offered. Private companies in general do not recognize exceptions or give users more rights than the right to use the platform according certain

Trademark

Trademark law is the set of **laws** and **legal** regulations that are set up to protect **trademarks**. A **trademark** is a **legal** protection given to any word, name, symbol, or design that is used in commerce to identify the product of one manufacturer from another.

Indian trademark law statutorily protects trademarks as per the Trademark Act, 1999 and also under the common law remedy of passing off. Statutory protection of trademark is administered by the Controller General of Patents, Designs and Trade Marks, a government agency which reports to the Department of Industrial Policy and Promotion (DIPP), under the Ministry of Commerce and Industry.

The law of trademark deals with the mechanism of registration, protection of trademark and prevention of fraudulent trademark.[2] The law also provides for the rights acquired by registration of trademark, modes of transfer and assignment of the rights, nature of infringements, penalties for such infringement and remedies available to the owner in case of such infringement.

Plagiarism

Plagiarism is the "wrongful appropriation" and "stealing and publication" of another author's "language, thoughts, ideas, or expressions" and the representation of them as one's own original work. **Plagiarism** is not in itself a crime, but can constitute copyright infringement.

The Common Types of Plagiarism

- Direct Plagiarism. Direct plagiarism is the word-for-word transcription of a section of someone else's work, without attribution and without quotation marks. ...
- Self Plagiarism. ...
- Mosaic Plagiarism. ...
- Accidental Plagiarism.

Is plagiarism punishable by law?

- Most cases of **plagiarism** are considered misdemeanors, **punishable** by fines of anywhere between $100 and $50,000 — and up to one year in jail. **Plagiarism** can also be considered a felony under certain state and federal **laws**.Jun 23, 2010

Is plagiarism a legal issue?

- Although **plagiarism** is not a criminal or civil offense, **plagiarism** is illegal if it infringes an author's intellectual property rights, including copyright or trademark. For example, the owner of a copyright can sue a plagiarizer in federal court for copyright violation.

Software Piracy

Software Piracy Law and Legal Definition. **Software piracy** is the unauthorized copying/distribution of **software**. Most retail programs are licensed for use at just one **computer** site or for use by only one user at any time. Purchasing **software**means that you are actually purchasing a license to use the **software**.

Copyright infringement (colloquially referred to as **piracy**) is the use of works protected by copyright law without permission, infringing certain exclusive rights granted to the copyright holder, such as the right to reproduce, distribute, display or perform the protected work, or to make derivative works. The copyright holder is typically the work's creator, or a publisher or other business to whom copyright has been assigned. Copyright holders routinely invoke legal and technological measures to prevent and penalize copyright infringement.

Copyright infringement disputes are usually resolved through direct negotiation, a notice and take down process, or litigation in civil court. Egregious or large-scale commercial infringement, especially when it involves counterfeiting, is sometimes prosecuted via the criminal justice system. Shifting public expectations, advances in digital technology, and the increasing reach of the Internet have led to such widespread, anonymous infringement that copyright-dependent industries now focus less on pursuing individuals who seek and share copyright-protected content online, and more on expanding copyright law to recognize and penalize, as indirect infringers, the service providers and software distributors who are said to facilitate and encourage individual acts of infringement by others.

Estimates of the actual economic impact of copyright infringement vary widely and depend on many factors. Nevertheless, copyright holders, industry representatives, and legislators have long characterized copyright infringement as piracy or theft – language which some U.S. courts now regard as pejorative or otherwise contentious.[1][2][3]

Viruses

A **computer virus** is a type of malicious software that, when executed, replicates itself by modifying other computer programs and inserting its own code. When this replication succeeds, the affected areas are then said to be "infected" with a computer virus.

Virus writers use social engineering deceptions and exploit detailed knowledge of security vulnerabilities to initially infect systems and to spread the virus. The vast majority of viruses target systems running Microsoft Windows, employing a variety of mechanisms to infect new hosts, and often using complex anti-detection/stealth strategies to evade antivirus software. Motives for creating viruses can include seeking profit (e.g., with ransomware), desire to send a political message, personal amusement, to demonstrate that a vulnerability exists in software, for sabotage and denial of service, or simply because they wish to explore cybersecurity issues, artificial life and evolutionary algorithms.

Computer viruses currently cause billions of dollars' worth of economic damage each year, due to causing system failure, wasting computer resources, corrupting data, increasing maintenance costs, etc. In response, free, open-source antivirus tools have been developed, and an industry of antivirus software has cropped up, selling or freely distributing virus protection to users of various operating systems. As of 2005, even though no currently existing antivirus software was able to uncover all computer viruses (especially new ones), computer security researchers are actively searching for new ways to enable antivirus solutions to more effectively detect emerging viruses, before they have already become widely distributed.

The term "virus" is also commonly, but erroneously, used to refer to other types of malware. "Malware" encompasses computer viruses along with many other forms of malicious software, such as computer "worms", ransomware, spyware, adware, trojan horses, keyloggers, rootkits, bootkits, malicious Browser Helper Object (BHOs), and other malicious software. The majority of active malware threats are actually trojan horse programs or computer worms rather than computer viruses. The term computer virus, coined by Fred Cohen in 1985, is a misnomer. Viruses often perform some type of harmful activity on infected host computers, such as acquisition of hard disk space or central processing unit(CPU) time, accessing private information (e.g., credit card numbers), corrupting data, displaying political or humorous messages on the user's screen, spamming their e-mail contacts, logging their keystrokes, or even rendering the computer useless. However, not all viruses carry a destructive "payload" and attempt to hide themselves—the defining characteristic of viruses is that they are self-replicating computer programs which modify other software without user consent.

Trojan Horse

One of the most insidious types of **Trojan horse** is a program that claims to rid your computer of **viruses**but instead introduces **viruses** onto your computer. The term comes from the a Greek story of the **Trojan**War, in which the Greeks give a giant wooden **horse** to their foes, the Trojans, ostensibly as a peace offering.

In computing, a **Trojan horse**, or **Trojan**, is any malicious computer program which misleads users of its true intent. The term is derived from the Ancient Greek story of the deceptive wooden horse that led to the fall of the city of Troy.

Trojans are generally spread by some form of social engineering, for example where a user is duped into executing an e-mail attachment disguised to appear not suspicious, (e.g., a routine form to be filled in), or by clicking on some fake advertisement on social media or anywhere else. Although their payload can be anything, many modern forms act as a backdoor, contacting a controller which can then have unauthorized access to the affected computer. Trojans may allow an attacker to access users' personal information such as banking information, passwords, or personal identity. It can infect other devices connected to the network. Ransomware attacks are often carried out using a Trojan.

Unlike computer viruses and worms, Trojans generally do not attempt to inject themselves into other files or otherwise propagate themselves.

Malicious Code

What are Virus & Malicious Code

Malicious code refers to a broad category of programs that can cause damage or undesirable effects to computers or networks. Potential damage can include modifying, destroying or stealing data, gaining or allowing unauthorised access to a system, bringing up unwanted screens, and executing functions that a user never intended.

Examples of malicious code include computer viruses, worms, trojan horses, logic bombs, spyware, adware and backdoor programs. Because they pose a serious threat to software and information processing facilities, users and administrators must take precautions to detect and prevent malicious code outbreaks.

Computer **viruses** are still the most common form of malicious code. A virus is a program that infects a computer by attaching itself to another program, and propagating itself when that program is executed. Another frequently encountered malicious code is the worm, which is a computer program that can make copies of itself, spreading through connected systems and consuming resources on affected computers or causing other damage.

Some malicious codes, including most viruses, are fragments of programs that cannot exist alone and need to attach themselves to host programs. Other types of malicious code are able to spread and replicate by themselves (such as worms) and are able to propagate from computer to computer across a network.

It should be noted that some malicious programs are able to exhibit the behaviors of more than one type of malicious code. For example, certain programs may be a virus and a trojan horse at the same time.

Logic Bombs

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 met.

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 met. For example, a programmer may hide a piece of code that starts deleting files (such as a salary database trigger), should they ever be terminated from the company.

Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their host systems on specific dates, such as Friday the 13th or April Fools' Day. Trojans that activate on certain dates are often called "time bombs".

To be considered a logic bomb, the payload should be unwanted and unknown to the user of the software. As an example, trial programs with code that disables certain functionality after a set time are not normally regarded as logic bombs.

Biometric Security and its Challenges

Definition - What does *Biometric Security* mean?

Biometric security is a security mechanism 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 strongest and most foolproof physical security technique used for identity verification.

What is biometric security?

The basic premise of biometric authentication (the term is derived from the Greek word “bio” meaning life and “metric” meaning to measure) is that every person is unique and each individual can be identified by his or her intrinsic or behaviour traits. Biometric technology is able to recognize a person on the basis of the unique features of their face, fingerprint, signature, DNA or iris pattern and then impart a secure and convenient method for authentication purposes.

Biometrics is therefore the measurement and statistical analysis of a person’s physical and behavioural characteristics. For example, voice recognition systems work by measuring the characteristics of a person’s speech as air is expelled through their lungs, across the larynx and out through their nose and mouth.

The speech verification software will compare these characteristics with data already stored on the server and if the two voiceprints are sufficiently similar, the biometric security system will then declare it a match.