MODEL PAPER–I
FIRST TERM EXAMINATION
SEVENTH SEMESTER (B.TECH)
INFORMATION SECURITY [ETCS–401]

Time : 1½ hrs. **M.M. : 30**

Note: *Ques no. 1 is compulsory and attempt any two from the rest. In all attempt 3 questions.*

Q.1. (*a*) Describe Goal of Information Security.

Ans. Information security follows three overarching principles:

Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorized to have the information.

Integrity: In information security, integrity means that data cannot be modified without authorization. This is not the same thing as referential integrity in databases. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a web site, when someone is able to cast a very large number of votes in an online poll, and so on.

Availability: For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial -of- service attacks.

Q.1. (*b*) What are various mobile device attacks?

Ans. Mobile Security has become a crucial aspect of protecting sensitive data and information. Malicious attacks once focused on PC's have now shifted to mobile phones and applications. Mobile makers are aware of this fact and are investing heavily in security.

Mobile device attacks can be split into 4 main categories:

OS Attacks: Loopholes in operating systems create vulnerabilities that are open to attack. Vendors try to solve these with patches.

Mobile App Attacks: Poor coding and improper development creates loopholes and compromises security.

Communication Network Attacks: Communications such as Bluetooth and Wi-Fi connections make devices vulnerable.

Malware Attacks: There has been a constant rise in malware for mobile devices. The focus is on deleting files and creating chaos.

Q.1. (c) What are various security measures?

Ans. Measures to ensure Security

Major security measures are following:

• **Encryption**: It is a very effective and practical way to safeguard the data being transmitted over the network. Sender of the information encrypts the data using a secret code and specified receiver only can decrypt the data using the same or different secret code.

• **Digital Signature**: Digital signature ensures the authenticity of the information. A digital signature is a e-signature authentic authenticated through encryption and password.

• **Security Certificates**: Security certificate is unique digital id used to verify identity of an individual website or user.

Q.1. (d) What are the advantages and disadvantages of Electronic Payment Methods.

Ans. E-payment Advantages:

Increased Speed and Convenience: E-payment is very convenient compared to traditional payment methods such as cash or check. Since you can pay for goods or services online at any time of day or night, from any part of the world, you don't have to spend time queuing in banks or merchant offices waiting for your turn to transact. Nor do you have to wait for a check to clear the bank so you can access the funds. E-payment also eliminates the security risks that come with handling cash money.

Increased Sales: As Internet banking and shopping become widespread, the number of people making cash payments is decreasing. In a 2014 survey, Bankrate established that more than 75 percent of those surveyed carry less than $50 a day, meaning electronic alternatives are increasingly becoming the preferred payment option. As such, e-payment enables businesses to make sales to the customers who choose to pay electronically and gain a competitive advantage over those that only accept traditional methods.

Reduced Transaction Costs: While there are no additional charges for making a cash payment, trips to the store typically cost money, and checks also need postage. On the other hand, there are usually no fees — or very small ones — to swipe your card or pay online. In the long run, e-payment could save both individuals and businesses hundreds to thousands of dollars in transaction fees.

E-payment Disadvantages:

Security Concerns: Although stringent measures such as symmetric encryption are in place to make e-payment safe and secure, it is still vulnerable to hacking. Fraudsters, for instance, use *phishing* attacks to trick unsuspecting users into providing the log-in details of their e-wallets, which they capture and use to access the victims' personal and financial information. Speaking to Information Security Media Group's BankInfoSecurity.com, Scott Dueweke, a payment systems consultant, notes that inadequate authentication also ails e-payment systems. Without superior identity verification measures like biometrics and facial recognition, anyone can use your cards and e-wallets and get away without being caught.

Disputed Transactions: If someone uses your electronic money without your authorization, you would identify the unfamiliar charge and file a claim with your bank, online payment processor or credit card company. Without sufficient information about the person who performed the transaction, though, it can be difficult to win the claim and receive a refund.

Increased Business Costs: E-payment systems come with an increased need to protect sensitive financial information stored in a business's computer systems from unauthorized access. Enterprises with in-house e-payment systems must incur additional costs in procuring, installing and maintaining sophisticated payment-security technologies.

Q.2. (a) Explain different types of payment methods with the help of example.

Ans. There are three main categories of EPS.

1. Banking and Financial Payments

- Large-scale or whole payment (e.g., bank-to-bank transaction)
- Small-scale or retail payment (e.g., ATM)
- Home banking (e.g., bill payment)

2. Retail Payments

- Credit cards (VISA or Master cards)
- Private label credit/debit cards (e.g., JC Penny cards)
- Charges cards (e.g., American Express)

3. Online e-commerce Payments

(*i*) Electronic token-based payment system

- Electronic cash (e.g., DigiCash)
- Electronic cheques (e.g., NetCheque)
- Smart cards or debit cards (e.g., Mondex e-currency cards)

(*ii*) Credit card-based payment systems

- Encrypted credit cards (www form-based encryption)
- Third-party authorization number (e.g., First Virtual)

Electronic Token-based Payment System

Now a days, 'electronic token' (e-token) in the form of electronic cash/cheque has been developed. It is recognized as equivalent to cash and is backed by banks.

1. Electronic Cash: Electronic cash (e-cash) is a form of electronic payment system based on encryption. This means it is a secure payment system. Before a product is bought or services availed cash has to be obtained from a currency server. The safety of e-cash is ensured by digital signature.

2. Electronic Cheques: Electronic cheque has all the same features as a paper cheque. It functions as a message to the sender's bank to transfer funds, the message is given to the receiver, who in turn, endorses the cheque and presents it to the bank to obtain funds.

3. Smart Cards: Smart cards, containing microprocessors, are able to hold more information than cards based on the traditional magnetic strips. They help the cardholder to perform operations, especially of financial nature. Most of these methods are known as stored value cards or electronic purse system. Units of prepayment or currency value are electronically stored on an IC (integrated circuit) chip embedded in these cards.

Credit Card-based Payment Systems: When a customer buys a product or avails a service, the details of the credit card is given to the seller of goods or to the service providers involved. The credit card provider makes the payment.

The credit card transaction simply requires that the consumer has a legitimate credit card number and expiration date while placing an order. This information has

been provided through standard Internet options like e-mail/SMS. Credit cards use personal information number (PIN).

Payment using encrypted credit card details: In this type of credit card system, the credit card data is encrypted and fed into a browser or any other e-commerce devices and safely sent through the network from the buyers to the sellers. This provides safety, privacy and security as encrypted information is transferred over the public network.

Payment using third party verification: This credit card system uses a third party for security. An organization that gathers and allows payments from one client to another is known as third party. After a lapse of sometime, the transaction of one credit card for the whole accrued amount is completed.

Q.2.(b) What are various essential requirements for safe e-payments/ transactions?

Ans. Following are the essential requirements for safe e-payments/transactions:

•**Confidential** " Information should not be accessible to unauthorized person. It should not be intercepted during transmission.

• **Integrity** " Information should not be altered during its transmission over the network.

•**Availability** " Information should be available wherever and whenever requirement within time limit specified.

• **Authenticity** " There should be a mechanism to authenticate user before giving him/her access to required information.

• **Non-Repudiabiity** " It is protection against denial of order or denial of payment. Once a sender sends a message, the sender should not able to deny sending the message. Similary the receipient of message should not be able to deny receipt.

• **Encryption** " Information should be encrypted and decrypted only by authorized user.

• **Auditability** " Data should be recorded in such a way that it can be audited for integrity requirements.

Q.3. What are various classification of security threats.

Ans. In order for one to produce a secure system, it is important to classify threats. The classification of threats could be:

Physical threats

Accidental error

Unauthorized access

Malicious misuse.

Pysical Threat: Physical threat to a computer system could be as a result of loss of the whole computer system, damage of hardware, damage to the computer software, theft of the computer system, vandalism, natural disaster such as flood, fire, war, earthquakes etc. Acts of terrorism such as the attack on the world trade centre is also one of the major threats to computer which can be classified as physical threat.

Another good example of a physical threat to computer system is the flooding of the city of New Orleans (Hurricane Katrina) during which valuable information was lost and billions of computer data were destroyed.

Accidental error: This is also an important security issue which computer security experts should always put into consideration when designing security measures for a system. Accidental errors could occur at any time in a computer system but having proper

checks in place should be the major concern of the designer. Accidental error includes corruption of data caused by programming error, user or operator error.

Unauthorized access: Dada stored on the computer system has to be accessed for it to be translated into useful information. This also poses a great security threats to the computer system due to unauthorized person's having access to the system. Not only this, information can be accessed via a remote system in the process of being transmitted from one point to the other via network media which includes wired and wireless media. Considering an example of an organization in which a member of staff at a particular level of hierarchy within the establishment is only allowed access to specific area according to the policy of the organization. If this employee by other means not set in the organization policy gain access to the restricted data area on the computer, this can be termed an un authorized access.

Malicious misuse: Any form of tampering of the computer system which includes penetration, Trojan horses' viruses and any form of illegal alteration of the computer system which also includes the generation of illegal codes to alter the standard codes within the system can be termed as malicious misuse. This could also lead to a great financial loss and should be prevented in all cases.

Q.4. What are various essential Challenges of Mobile Security?

Ans. The various essential challenges of Mobile Security are:

1. Physical Security: Lookout Labs estimated that a mobile phone was lost in the USA every 3.5 seconds in 2011 – and that nearly all who found lost devices tried to access the information on the phone. Now, I hope the "access" was an attempt to determine the owner, but who knows? Even temporarily misplacing a phone can put sensitive data at risk.

2. Multiple User Logging: Mobile phones have come a long way, but they are still not versatile machines like computers. Multiple users on mobile devices still have trouble in opening unique protected accounts. Simply put, what one user does on a mobile device is hardly a private affair. Customizable 3rd party solutions are available, but it's much safer when phones are not shared.

3. Secure Data Storage: Mobile phones need good file encrypting for strong security. After all, who wants sensitive corporate data to end up in the wrong hands? Without the proper encryption, not only are personal documents up for grabs, but also passwords to bank, credit card and even business apps. Encrypting sensitive data ensures would-be thieves gain a whole lot of nothing.

4. Mobile Browsing: Perhaps one of the best features of mobile devices is the ability to browse the web on the go, but this also opens up the mobile phones to security risks. The problem is that users cannot see the whole URL or link, much less verify whether the link or URL is safe. That means that users could easily browse their way into a phishing-related attack.

For a deeper look into mobile device security, check out the iPhone forensics course offered by the InfoSec Institute.

5. Application Isolation: There are mobile applications for just about everything, from social networking to banking. Before installing any app that comes your way, be sure to read the application access request for permission agreement. This often overlooked agreement contains valuable information regarding specific permissions on how the app is to access your device.

Be mindful of what your application purports to do and what it is that it actually does. Chances are a calculator application does not need access to the internet or your personal information.

6. System Updates: People have a tendency to point fingers at mobile device vendors when it comes to security mishaps, but they aren't always to blame. Updates and patches designed to fix issues in mobile devices are not quite as cut and dry as with PCs. Mobile devices vendors often release updates and patches, but unfortunately carriers don't always stream them due to commercial or bureaucratic reasons.

7. Mobile Device Coding Issues: Sometimes developers make honest mistakes, inadvertently creating security vulnerabilities via poor coding efforts. Many times there is bad implementation of encrypted channels for data transmission or even improper password protection. Ineffective development can lead to security weaknesses whether in PCs or mobile phones.

8. Bluetooth Attacks: As easy as Bluetooth is to use, it can be just as easy for attackers to gain access to one's phone and everything stored within. It's fairly simple for a hacker to run a program to locate available Bluetooth connections and Bingo – they're in. It's important to remember to disable the Bluetooth functionality when not in use.

9. Malware on the Rise: As is the case with computers, malware is rather damaging to mobile phones. The news does not get any better either. 2014 is projected to be far worse, leaving industry leaders and mobile device users no choice but to become proactive about mobile protection. For example, take the Android malware incident in January which impacted more than 600,000 phones.

10. Serious Threats in New Features: Newly added features and updates are serious risks too. The Neat Field Communication, or NFC, technology is a prime example. NFC is designed to allow people to use their mobile phones as a wallet to purchase products. Unfortunately, all one needs to do to take over the mobile device is brush a NFC chip embedded tag over the phone.

It should not come as a surprise that security is such a problem considering the wide variety of mobile devices and smartphones available today. Every phone and mobile OS has its own unique security issues and one should always take precaution, especially as we are becoming increasingly dependent on our mobile devices.

MODEL PAPER–I
SECOND TERM EXAMINATION
SEVENTH SEMESTER (B.TECH)
INFORMATION SECURITY [ETCS–401]

Time : 1½ hrs. **M.M. : 30**

Note: *Ques no. 1 is compulsory and attempt any two from the rest. In all attempt 3 questions.*

Q.1. (a) What is physical security? What are components of physical security.

Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.

Physical security is often overlooked (and its importance underestimated) in favor of more technical and dramatic issues such as hacking, viruses, Trojans, and spyware. However, breaches of physical security can be carried out with little or no technical knowledge on the part of an attacker. Moreover, accidents and natural disasters are a part of everyday life, and in the long term, are inevitable.

There are three main components to physical security. First, obstacles can be placed in the way of potential attackers and sites can be hardened against accidents and environmental disasters. Such measures can include multiple locks, fencing, walls, fireproof safes, and water sprinklers. Second, surveillance and notification systems can be put in place, such as lighting, heat sensors, smoke detectors, intrusion detectors, alarms, and cameras. Third, methods can be implemented to apprehend attackers (preferably before any damage has been done) and to recover quickly from accidents, fires, or natural disasters.

Q.1. (b) What is Biometrics?

Ans. "Biometrics refers to the automatic identifications of a person based on his or her physiological or behavioral characteristics" .It is an authorization method that verifies or identifies a user based on what they are before authorizing access. The search for a more reliable authorization method to secure assets has lead to the revelation of biometrics and many organizations have shown interest in the technology.

Q.1. (c) What is difference between data security and data privacy?

Ans. Data security is commonly referred to as the confidentiality, availability, and integrity of data. In other words, it is all of the practices and processes that are in place to ensure data isn't being used or accessed by unauthorized individuals or parties. Data security ensures that the data is accurate and reliable and is available when those with authorized access need it. A data security plan includes facets such as collecting only the required information, keeping it safe, and destroying any information that is no longer needed. These steps will help any business meet the legal obligations of possessing sensitive data.

Data privacy is suitably defined as the appropriate use of data. When companies and merchants use data or information that is provided or entrusted to them, the data should be used according to the agreed purposes. The Federal Trade Commission enforces penalties against companies that have negated to ensure the privacy of a customer's data. In some cases, companies have sold, disclosed, or rented volumes of the consumer information that was entrusted to them to other parties without getting prior approval.

Q.1. (*d*) What is meant by cryptography?

Ans. The science of coding and decoding messages so as to keep these messages secure. Coding takes place using a key that ideally is known only by the sender and intended recipient of the message.

Q.2. What are various characteristics of biometric?

Ans: A number of biometric characteristics may be captured in the first phase of processing. However, automated capturing and automated comparison with previously stored data requires that the biometric characteristics satisfy the following characteristics:

1. Universal: Every person must possess the characteristic/attribute. The attribute must be one that is universal and seldom lost to accident or disease.

2. Invariance of properties: They should be constant over a long period of time. The attribute should not be subject to significant differences based on age either episodic or chronic disease.

3. Reducibility: The captured data should be capable of being reduced to a file which is easy to handle. G. Reliability and tamper-resistance: The attribute should be impractical to mask or manipulate. The process should ensure high reliability and reproducibility. H. Privacy The process should not violate the privacy of the person. I. Comparable It should be able to reduce the attribute to a state that makes it digitally comparable to others. The less probabilistic the matching involved, the more authoritative the identification. J. Inimitable The attribute must be irreproducible by other means. The less reproducible the attribute, the more likely it will be authoritative. Among the various biometric technologies being considered, the attributes which satisfy the above requirements are fingerprint, facial features, hand geometry, voice, iris, retina, vein patterns, palm print, DNA, keystroke dynamics, ear shape, odor, signature etc. I The properties should be suitable for capture without waiting time and must be easy to gather the attribute data passively.

4. Singularity: Each expression of the attribute must be unique to the individual. The characteristics should have sufficient unique properties to distinguish one person from any other. Height, weight, hair and eye color are all attributes that are unique assuming a particularly precise measure, but do not offer enough points of differentiation to be useful for more than categorizing.

5. Acceptance: The capturing should be possible in a way acceptable to a large percentage of the population. Excluded are particularly invasive technologies, i.e. technologies which require a part of the human body to be taken or which (apparently) impair the human body.

6. Reducibility: The captured data should be capable of being reduced to a file which is easy to handle.

7. Reliability and tamper-resistance: The attribute should be impractical to mask or manipulate. The process should ensure high reliability and reproducibility.

8. Privacy: The process should not violate the privacy of the person.

9. Comparable: It should be able to reduce the attribute to a state that makes it digitally comparable to others. The less probabilistic the matching involved, the more authoritative the identification.

10. Inimitable: The attribute must be irreproducible by other means. The less reproducible the attribute, the more likely it will be authoritative. Among the various biometric technologies being considered, the attributes which satisfy the above requirements are fingerprint, facial features, hand geometry, voice, iris, retina, vein patterns, palm print, DNA, keystroke dynamics, ear shape, odor, signature etc.

Q.3. What do you mean by VPN? Discuss security mechanism of VPN.

Ans. A virtual private network (VPN) extends a private network across a public network or internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

VPNs can provide functionality, security and/or network management benefits to the user. But they can also lead to new issues, and some VPN services, especially "free" ones, can actually violate their users' privacy by logging their usage and making it available without their consent, or make money by selling the user's bandwidth to other users.

Some VPNs allow employees to securely access a corporate intranet while located outside the office. Some can securely connect geographically separated offices of an organization, creating one cohesive network. Individual Internet users can use some VPNs to secure their wireless transactions, to circumvent geo-restrictions and censorship, and/or to connect to proxy servers for the purpose of protecting personal identity and location. But some Internet sites block access via known VPNs to prevent the circumvention of their geo-restrictions.

A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN). From a user perspective, the resources available within the private network can be accessed remotely.

VPNs cannot make online connections completely anonymous, but they can usually increase privacy and security. To prevent disclosure of private information, VPNs typically allow only authenticated remote access using tunneling and encryption techniques.

The VPN security model provides:

- Confidentiality such that even if the network traffic is sniffed at the packet level (see network sniffer and Deep packet inspection), an attacker would only see encrypted data
- Sender authentication to prevent unauthorized users from accessing the VPN
- Message integrity to detect any instances of tampering with transmitted messages

The most commonly used tunnelling protocols are IPsec, L2TP, PPTPand SSL. A packet with a private non-routable IP address can be sent inside a packet with globally unique IP address, thereby extending a private network over the Internet. VPN uses encryption to provide data confidentiality.

Q.4. What is intrusion detection system? Explain its need. Also discuss various components of IDS.

Ans. An IDS (Intrusion Detection System) is a device or application used to inspect all network traffic and alert the user or administrator when there has been unauthorized attempts or access. The two primary methods of monitoring are signature-based and anomaly-based. Depending on the device or application used, the IDS can either simply alert the user or administrator or it could be set up to block specific traffic or automatically respond in some way. The intrusion detection systems didn t have the ability to stop such attacks rather than detecting and reporting to the network personnel.

The Intrusion detection system in a similar way complements the firewall security. The firewall protects an organization from malicious attacks from the Internet and the Intrusion detection system detects if someone tries to break in through the firewall or

manages to break in the firewall security and tries to have access on any system in the trusted side and alerts the system administrator in case there is a breach in security. Moreover, Firewalls do a very good job of filtering incoming traffic from the Internet; however, there are ways to circumvent the firewall. For example, external users can connect to the Intranet by dialing in through a modem installed in the private network of the organization. This kind of access would not be seen by the firewall. Therefore, an Intrusion detection system (IDS) is a security system that monitors computer systems and network traffic and analyzes that traffic for possible hostile attacks originating from outside the organization and also for system misuse or attacks originating from inside the organization.

Components of Intrusion Detection System: An Intrusion Detection system comprises of Management console and sensors. Management console is the management and reporting console. Sensors are agents that monitor hosts or networks on a real time basis. An Intrusion Detection System has a database of attack signatures. The attack signatures are patterns of different types of previously detected attacks. If the sensors detect any malicious activity, it matches the malicious packet against the attack signature database. In case it finds a match, the sensor reports the malicious activity to the management console. The sensor can take different actions based on how they are configured. For example, the sensor can reset the TCP connection by sending a TCP FIN, modify the access control list on the gateway router or the firewall or send an email notification to the administrator for appropriate action.

MODEL PAPER–I
END TERM EXAMINATION
SEVENTH SEMESTER (B.TECH)
INFORMATION SECURITY [ETCS–401]

Time : 3 hrs. **M.M. : 75**

Note: *Ques no.1 is compulsory and attempt any two from the rest. In all attempt 3 questions.*

Q.1. (a) What is Digital media forensics?

Ans. The area of digital media forensics is not just the art of finding deleted or hidden data; it is also the understanding of the underlying technologies behind the various tools used and the ability to present scientifically valid information. Digital media forensics is a growing science that governmental agencies have long practiced, with the commercial sector not far behind. Many governmental agencies are far ahead of most companies when it comes to searching, seizing, and analyzing information systems and the proper accountability of digital evidence. With secrets and lives to lose if sensitive information were released to the wrong people, the reasons behind their expertise are understood. The ability to identify the person(s) responsible for the compromise or theft and means of transmittal is paramount for further protection and control of sensitive information. Many companies are now focusing on the problem of industrial espionage and the control of proprietary information.

Q.1. (b) What is security metrices?

Ans. SecurityMetrics is a multinational merchant data security and compliance company headquartered in Orem, Utah. The company is a Payment Card Industry (PCI) Data Security Standard (DSS) vendor, listed as a Qualified Security Assessor (QSA), Approved Scanning Vendor (ASV), P2PE QSA, PCI Forensic Investigator (PFI) and Payment Application Qualified Security Assessor (PA-QSA) by the PCI Security Standards Council. Security Metrics has working relationships with major payment processing companies and global acquiring banks such as Global Payments Inc, Sterling Payment Technologies, and First Merit Bank to provide PCI compliance and other security solutions to their merchants. Security Metrics currently has the largest support staff in the PCI industry worldwide; fielding over 132,000 calls a month, and employs nearly 400 employees.

Q.1. (c) List four elements of an EDI system.

Ans. To make EDI happen, four elements of infrastructure must exist:

(1) format standards are required to facilitate automated processing by all users;

(2) translation software is required to translate from a user's proprietary format for internal data storage into the generic external format and back again;

(3) value-added networks are very helpful in solving the technical problems of sending information between computers; and

(4) inexpensive microcomputers are required to bring all potential users—even small ones-into the market. It has only been in the past several years that all of these ingredients have fallen into place.

Q.1. (d) What is SET? How SET makes our transaction secure?

Ans. Secure Electronic Transaction (SET) is a system for ensuring the security of financial transactions on the Internet. It was supported initially by Mastercard, Visa,

Microsoft, Netscape, and others. With SET, a user is given an electronic wallet (digital certificate) and a transaction is conducted and verified using a combination of digital certificates and digital signatures among the purchaser, a merchant, and the purchaser's bank in a way that ensures privacy and confidentiality. SET makes use of Netscape's Secure Sockets Layer (SSL), Microsoft's Secure Transaction Technology (STT), and Terisa System's Secure Hypertext Transfer Protocol (S-HTTP). SET uses some but not all aspects of a public key infrastructure (PKI).

Q.2. (a) What are the popular protocols used over the internet which ensures security of transactions made over the internet?

Ans. Security Protocols in Internet

Following are the popular protocols used over the internet which ensures security of transactions made over the internet.

Secure Socket Layer (SSL): It is the most commonly used protocol and is widely used across the industry. It meets following security requirements:

- Authentication
- Encryption
- Integrity
- Non-reputability

"https://" is to be used for HTTP urls with SSL, where as "http://" is to be used for HTTP urls without SSL.

Secure Hypertext Transfer Protocol (SHTTP): SHTTP extends the HTTP internet protocol with public key encryption, authentication and digital signature over the internet. Secure HTTP supports multiple security mechanism providing security to end users. SHTTP works by negotiating encryption scheme types used between client and server.

Secure Electronic Transaction: It is a secure protocol developed by MasterCard and Visa in collaboration. Thereoritically, it is the best security protocol. It has following components "

- **Card Holder's Digital Wallet Software**: Digital Wallet allows card holder to make secure purchases online via point and click interface.
- **Merchant Software**: This software helps merchants to communicate with potential customers and financial institutions in secure manner.
- **Payment Gateway Server Software**: Payment gateway provides automatic and standard payment process. It supports the process for merchant's certificate request.
- **Certificate Authority Software**: This software is used by financial institutions to issue digital certificates to card holders and merchants and to enable them to register their account agreements for secure electronic commerce.

Q.2. (b) Explain the difference between Cyber Cash and First Virtual Electronic Payment System.

Ans. Cyber cash has been described as Federal Express of Internet payment business, since it offers safe, efficient and inexpensive delivery of payments across Internet. Cyber cash makes available the software and services needed to exchange payments securely across the Internet with its Secure Internet Payment Service. Using a procedure that incorporates encryption and digital signatures, cyber cash gives consumers a "digital wallet", and merchants a conduit to Internet payment processing through their own banks. Customers are able to authorize payments out of their digital wallets. The payments are signed and encrypted, then sent through the merchant bank

to cyber cash, which in turn passes the transaction to the merchant's bank for processing. The digital wallet initially supported only credit cards, but now supports digital cash transfers for small dollar amounts for products and services that are too expensive to justify using a credit card.

First virtual has created a payment system, the Internet Payment System, to be used exclusively for the sale of information over the Internet, rather than for products or services. Using an automated telephone system to collect payment information about the participant, first virtual eschews cryptographic methods encryption or digital signatures preferring to rely instead on close monitoring of sales and purchases to reduce fraud.

Q.3. What are various shopping and online selling techniques? Discuss how E-Commerce online resources help to sell products on the Internet.

Ans. Various Shopping and Online Selling Techniques

1. Establish your strategy. Just like any business venture, to sell online well you need to work out what your strategy is and stick to it. This includes your ecommerce business structure – are you online only (just selling via the website) or do you also have a physical store? You'll also need to decide on the product range you're going to stock – are you a specialist in one thing or do you sell a wide range of goods tailored to your customers' requirements?

2. Think "cross-device" not "mobile". Consumers don't think of surfing the net on their mobile as being any different than surfing on their tablet, desktop or laptop. So you can't afford to either. Make sure you're providing the right customer experience across every platform (including your bricks and mortar shop if you have one).

3. Choose the right website software. There are so many different website options you can choose from it's important to pick the right one for your business. Most businesses are best off starting with a simple off the shelf option - like Shopify or WooCommerce. These are powerful systems which will do everything you need quickly and easily so you can focus on your marketing - getting people to the website to buy.

4. Take pride in customer service. The common factor of all the successful businesses I've interviewed on my podcast is that they are committed to providing their customers with a great service. And that does not just mean having nice people on the phone; it's about putting the needs of the customer in everything your business does - from the products, to the website, to the delivery.

5. Create a great delivery experience. If you get your delivery strategy right you'll increase the conversion rate of your website and encourage more repeat purchases. Your delivery strategy covers everything from the price you charge and the services you offer, through to what arrives in the parcel and how the parcel looks. It's really important to invest some money and thought in getting this right for your customers. After all, delivery is consistently the number one reason people don't buy from a website.

6. Market to get the first purchase and the repeat purchase. To be successful you want to take people from not knowing about you, to visiting your website, then enquiring, to ordering for the first time, and then get them to buy again and again. Many businesses only focus on the first order and forget all about getting the second order – which is crazy because it's easier. You'll find different marketing methods suit each of the stages of this journey, so you'll have to test and analyse and change your plans accordingly.

7. Build a trusted brand. Today's online shoppers are pretty savvy. Just as you wouldn't buy fish and chips from a run-down, dirty old van because you don't trust that

they're giving you good food, an online shopper won't buy from a website or a business that they don't trust. You need to work hard to build the trust of your customers; it's hard to gain but easy to lose. Trust needs to be built into every interaction the customer has with your business - include customer testimonials and reviews on your site, deliver on your promises and make sure all the information on the site is accurate.

8. Keep optimising. This is my personal motto. Nothing you ever do in your business will be finished; in some ways everything is permanently in test mode. So you have to have a policy of constant optimisation – find the area that is working the least well and make it better. Once that's done, find the next area you need to focus on and repeat. One month it might be the delivery strategy, the next your repeat customer strategy and the following month testing a new marketing method.

Online shopping (sometimes known as **e-tail** from "electronic retail" or **e-shopping**) is a form of electronic commerce which allows consumers to directly buy goods or services from a seller over the Internet using a web browser. Alternative names are: e-web-store, e-shop, e-store, Internet shop, web-shop, web-store, online store, online storefront and virtual store. Mobile commerce (or m-commerce) describes purchasing from an online retailer's mobile optimized online site or app.

An online shop evokes the physical analogy of buying products or services at a bricks-and-mortar retailer or shopping center; the process is called business-to-consumer (B2C) online shopping. In the case where a business buys from another business, the process is called business-to-business (B2B) online shopping. The largest of these online retailing corporations are Alibaba, Amazon.com, and eBay.

You can use the *Internet* to find sales *resource* for *help* in identifying and selecting appropriate *e-commerce* options.

Q.4. (*a*) What are the different types of VPN?

Ans. (*a*) Remote Access VPN: Also called as Virtual Private dial-up network (VPDN) is mainly used in scenarios where remote access to a network becomes essential. Remote access VPN allows data to be accessed between a company's private network and remote users through a third party service provider; Enterprise service provider. **E.g.** Sales team is usually present over the globe. Using Remote access VPN, the sales updates can be made.

(*b*) Site to Site VPN: Intranet based: This type of VPN can be used when multiple Remote locations are present and can be made to join to a single network. Machines present on these remote locations work as if they are working on a single network.

(*c*) Site to Site VPN: Extranet based: This type of VPN can be used when several different companies need to work in a shared environment. **E.g.** Distributors and service companies. This network is more manageable and reliable.

Q.4. (*b*) What are the different VPNs protocols.

Ans. Types of VPN protocols

1. PPTP VPN: This is the most common and widely used VPN protocol. They enable authorized remote users to connect to the VPN network using their existing Internet connection and then log on to the VPN using password authentication. They don't need extra hardware and the features are often available as inexpensive add-on software. PPTP stands for Point-to-Point Tunneling Protocol. The disadvantage of PPTP is that it does not provide encryption and it relies on the PPP (Point-to-Point Protocol) to implement security measures.

2. Site-to-Site VPN: Site-to-site is much the same thing as PPTP except there is no "dedicated" line in use. It allows different sites of the same organization, each with its own real network, to connect together to form a VPN. Unlike PPTP, the routing, encryption and decryption is done by the routers on both ends, which could be hardware-based or software-based.

3. L2TP VPN: L2TP or Layer to Tunneling Protocol is similar to PPTP, since it also doesn't provide encryption and it relies on PPP protocol to do this. The difference between PPTP and L2TP is that the latter provides not only data confidentiality but also data integrity. L2TP was developed by Microsoft and Cisco.

4. IPsec: Tried and trusted protocol which sets up a tunnel from the remote site into your central site. As the name suggests, it's designed for IP traffic. IPSec requires expensive, time consuming client installations and this can be considered an important disadvantage.

5. SSL: SSL or Secure Socket Layer is a VPN accessible via https over web browser. SSL creates a secure session from your PC browser to the application server you're accessing. The major advantage of SSL is that it doesn't need any software installed because it uses the web browser as the client application.

6. MPLS VPN: MPLS (Multi-Protocol Label Switching) are no good for remote access for individual users, but for site-to-site connectivity, they're the most flexible and scalable option. These systems are essentially ISP-tuned VPNs, where two or more sites are connected to form a VPN using the same ISP. An MPLS network isn't as easy to set up or add to as the others, and hence bound to be more expensive.

7. Hybrid VPN: A few companies have managed to combine features of SSL and IPSec & also other types of VPN types. Hybrid VPN servers are able to accept connections from multiple types of VPN clients. They offer higher flexibility at both clienbt and server levels and bound to be expensive.

Q.5. (*a*) What do you mean by Intrusion prevention systems? What are various types of IPS?

Ans. Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected. More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address.[4] An IPS can also correct Cyclic Redundancy Check (CRC) errors, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options.

Intrusion prevention systems can be classified into four different types

1. Network-based intrusion prevention system (NIPS): monitors the entire network for suspicious traffic by analyzing protocol activity.

2. Wireless intrusion prevention systems (WIPS): monitor a wireless network for suspicious traffic by analyzing wireless networking protocols.

3. Network behavior analysis (NBA): examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware and policy violations.

4. Host-based intrusion prevention system (HIPS): an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.

Q.5. (b) What is firewall? What are characteristics of firewall?

Ans. A firewall is software or hardware-based network security system that controls the incoming and outgoing network traffic based on applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is not assumed to be secure and trusted.

FIREWALL CHARACTERISTICS

1. All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are possible.

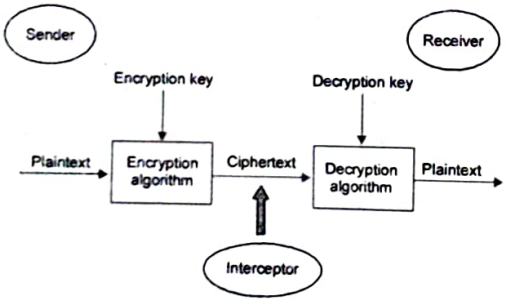
2. Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies.

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

Q.6.What do you mean by cryptosystem? What are various components of Components of a Cryptosystem?

Ans. A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a cipher system.

Let us discuss a simple model of a cryptosystem that provides confidentiality to the information being transmitted. This basic model is depicted in the illustration below:



The illustration shows a sender who wants to transfer some sensitive data to a receiver in such a way that any party intercepting or eavesdropping on the communication channel cannot extract the data.

The objective of this simple cryptosystem is that at the end of the process, only the sender and the receiver will know the plaintext.

Components of a Cryptosystem: The various components of a basic cryptosystem are as follows "

• **Plaintext:** It is the data to be protected during transmission.

• **Encryption Algorithm:** It is a mathematical process that produces a cipher text for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a cipher text.

• **Cipher text:** It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key. The cipher text is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.

• **Decryption Algorithm,** It is a mathematical process, that produces a unique plaintext for any given cipher text and decryption key. It is a cryptographic algorithm that takes a cipher text and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.

• **Encryption Key.** It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the cipher text.

• **Decryption Key.** It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the cipher text in order to compute the plaintext.

For a given cryptosystem, a collection of all possible decryption keys is called akey space.

An interceptor (an attacker) is an unauthorized entity who attempts to determine the plaintext. He can see the cipher text and may know the decryption algorithm. He, however, must never know the decryption key.

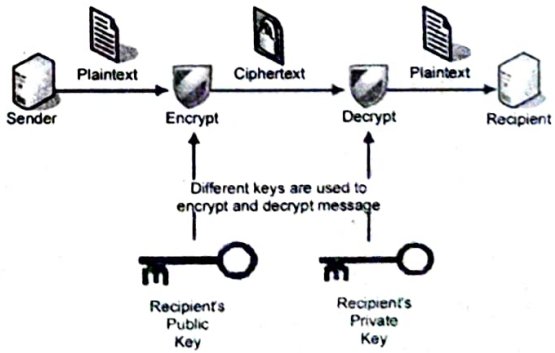
Types of Cryptosystems: Fundamentally, there are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system:

• Symmetric Key Encryption

• Asymmetric Key Encryption

Q.7. Describe public key cryptography.

Ans. Unlike symmetric key cryptography, we do not find historical use of public-key cryptography. It is a relatively new concept.



Symmetric cryptography was well suited for organizations such as governments, military, and big financial corporations were involved in the classified communication.

With the spread of more unsecure computer networks in last few decades, a genuine need was felt to use cryptography at larger scale. The symmetric key was found to be non-practical due to challenges it faced for key management. This gave rise to the public key cryptosystems.

The process of encryption and decryption is depicted in the following illustration "

The most important properties of public key encryption scheme are "

•Different keys are used for encryption and decryption. This is a property which set this scheme different than symmetric encryption scheme.

•Each receiver possesses a unique decryption key, generally referred to as his private key.

•Receiver needs to publish an encryption key, referred to as his public key.

• Some assurance of the authenticity of a public key is needed in this scheme to avoid spoofing by adversary as the receiver. Generally, this type of cryptosystem involves trusted third party which certifies that a particular public key belongs to a specific person or entity only.

• Encryption algorithm is complex enough to prohibit attacker from deducing the plaintext from the ciphertext and the encryption (public) key.

• Though private and public keys are related mathematically, it is not be feasible to calculate the private key from the public key. In fact, intelligent part of any public-key cryptosystem is in designing a relationship between two keys.

Q.8. What is firewall? Explain different types of firewall.

Ans. A firewall is software or hardware-based network security system that controls the incoming and outgoing network traffic based on applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is not assumed to be secure and trusted.

There are three main classes of firewalls: packet filters, application and circuit gateways (proxies), and stateful inspection (or smart filter) firewalls.

Proxy Servers: A proxy service is an application that redirects users' requests to the actual services based on an organization's security policy. All communication between a user and the actual server occurs through the proxy server. Thus, a proxy server acts as a communications broker between clients and the actual application servers. Because it acts as a checkpoint where requests are validated against specific applications, a proxy server is usually processing intensive and can become a bottleneck under heavy traffic conditions. Proxy servers can operate at either the application layer or the transport layer. Thus, there are two classes of proxy servers: application gateways, which operate at the application layer; and circuit-level gateways, which operate at the transport layer.

Application Gateways: An application gateway is a proxy server that provides access control at the application layer. It acts as an application-layer gateway between the protected network and the untrusted network. Because it operates at the application layer, it is able to examine traffic in detail and, therefore, is considered the most secure type of firewall. It can prevent certain applications, such as FTP, from entering the protected network. It can also log all network activities according to applications for both accounting and security audit purposes. Application gateways can also hide information. Since all requests for services in the protected network pass through the application gateway, it can provide network address translation (or IP address hiding) functionality and conceal IP addresses in the protected network from the Internet by replacing the IP address of every outbound packet (that is, packets going from the protected network to the Internet) with its own IP address. Network address translation also permits unregistered IP addresses to be freely used in the protected network because the gateway will map them to its own IP address when the users attempt to communicate with the outside world.

Circuit-Level Gateways: A circuit-level gateway is a proxy server that validates TCP and UDP sessions before allowing a connection or circuit through the firewall. It is actively involved in the connection establishment and does not allow packets to be forwarded until the necessary access control rules have been satisfied. A circuit level gateway is not as secure as an application gateway because it validates TCP and UDP sessions without full knowledge of the applications that use these transport services. Moreover, once a session has been established, any application can run across that connection. This behavior exposes the protected network to attacks from intruders. Unlike a circuit-level gateway, an application gateway can differentiate the applications that need to be blocked from those that can be allowed to pass through the gateway.

Stateful Packet Filters: Although the application gateway provides the best security among the preceding firewalls, its intensive processing requirement slows down network performance. A stateful packet filtering gateway attempts to provide tight security without compromising performance. Unlike the application gateway, it checks the data that passes through at the network layer but does not process it. The firewall maintains state information for each session, where session states include a combination of communication phase and the endpoint application state. When a stateful packet filtering gateway receives a data packet, it checks the packet against the known state of the session. If the packet deviates from the expected session state, the gateway blocks the rest of the session.

Q.9 .Write short notes on the following:

(*a*) VPN Security

(*b*) Digital Signature

Ans 9 (*a*) VPN Security: VPN uses encryption to provide data confidentiality. Once connected, the VPN makes use of the tunneling mechanism described above to encapsulate encrypted data into a secure tunnel, with openly read headers that can cross a public network. Packets passed over a public network in this way are unreadable without proper decryption keys, thus ensuring that data is not disclosed or changed in any way during transmission. VPN can also provide a data integrity check. This is typically performed using a message digest to ensure that the data has not been tampered with during transmission. By default, VPN does not provide or enforce strong user authentication. Users can enter a simple username and password to gain access to an internal private network from home or via other insecure networks. Nevertheless, VPN does support add-on authentication mechanisms, such as smart cards, tokens and RADIUS.

Ans 9 (b) A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message (authentication and non-repudiation), and that the message was not altered in transit (integrity).

Digital signatures are a standard element of most cryptographic protocol suites, and are commonly used for software distribution, financial transactions, contract

management software, and in other cases where it is important to detect forgery or tampering.

A digital signature scheme typically consists of three algorithms;

• A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.

• A *signing* algorithm that, given a message and a private key, produces a signature.

• A *signature verifying* algorithm that, given the message, public key and signature, either accepts or rejects the message's claim to authenticity.

Two main properties are required. First, the authenticity of a signature generated from a fixed message and fixed private key can be verified by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party without knowing that party's private key. A digital signature is an authentication mechanism that enables the creator of the message to attach a code that acts as a signature.

FIRST TERM EXAMINATION [SEPT. 2016]
SEVENTH SEMESTER [B.TECH]
INFORMATION SECURITY [ETCS-401]

Time : 1:30 hrs. **M.M. : 30**

Note: *Questions One is complusory. Attempt any two more questions from the rest of the Questions..*

Q.1. Attempt all parts of the following: (5)

Q.1. (a) What do you mean by Computer crime? Point out four basic sources of security threats?

Ans. Computer crime describes a very broad category of offenses. Some of them are the same as non-computer offenses, such as larceny or fraud, except that a computer or the Internet is used in the commission of the crime. Others, like hacking, are uniquely related to computers. Read on to find out what kinds of activities are considered computer crimes and how to prevent them.

A threat is the potential, of chance, for a threat source to use a vulnerability which will cause the threat to materialize. A threat source is a method by which a vulnerability is triggered or exploited. This page lists threat sources which when deliberately used are attacks or accident happening in the case of an unintentioned situation. Security threats can come from two locations:

• External users

• Internal users

An external security threat occurs when someone outside your network creates a security threat to your network. An internal security threat occurs when someone from inside your network creates a security threat to your network.

Q.1. (b) What are the security attacks related to computer crime?

Ans. There are various security attacks related to computer crime

1. Malware
2. Phising
3. SQL Injection attack
4. Denial of service
5. Session Hijacking and Man-in-the- Middle Attacks, etc.

Q.1. (c) Why Information is so important for individual or organization?

Ans. A human rights information system is much more than just a database. To gain the maximum benefits from your company's information system, you have to exploit all its capacities. Information systems gain their importance by processing the data from company inputs to generate information that is useful for managing your operations. To increase the information system's effectiveness, you can either add more data to make the information more accurate or use the information in new ways. Part of management is gathering and distributing information, and information systems can make this process more efficient by allowing managers to communicate rapidly. How you manage your company's operations depends on the information you have. Information systems can offer more complete and more recent information, allowing you to operate your company more efficiently. He company information system can help you make better decisions by delivering all the information you need and by modeling the results of your

decisions. A decision involves choosing a course of action from several alternatives and carrying out the corresponding tasks. Your company needs records of its activities for financial and regulatory purposes as well as for finding the causes of problems and taking corrective action. The information system stores documents and revision histories, communication records and operational data.

Q.1. (*d*) Explain the meaning of Computer based IS.

Ans. Computer based information system: An **information system** is an integrated set of people, processes and mechanisms for collecting, storing, and processing data to deliver information toward a particular goal. It is common to assume that an *information system* is computerized, but by definition it is possible to have an information system in which the data is collected, stored and processed using physical artifacts and manual procedures. Similarly, the information is delivered using physical artifacts and manual procedures.

Therefore, a **computer-based information system** is an *information system* in which the data is mostly collected, stored, and processed in digital format using computerized processes. Similarly, the information is delivered in digital format via computerized mechanisms.

Q.1. (*e*) Explain the need of distributed IS in current scenario.

Ans. Need of distributed information system: Computers are essential today. We are performing different tasks using computers. In order to organize these tasks in a systematic way we need the help of Distributed Information system. **Distributed computing** is a field of computer science that studies distributed systems. A *distributed system* is a model in which components located on networked computers communicate and coordinate their actions by passing messages. The components interact with each other in order to achieve a common goal. Three significant characteristics of distributed systems are: concurrency of components, lack of a global clock, and independent failure of components. Examples of distributed systems vary from SOA-based systems to massively multiplayer online games to peer-to-peer applications.

Q.2. Write short notes on:- **(2.5)**

(*i*) LDAP Server

Ans. LDAP: LDAP is mostly used by medium-to-large organi-zations. If you belong to one that has an LDAP server, you can use it to look up contact info and the like. Otherwise, if you were just wondering about this acronym, you probably don't need it. But feel free to read on to learn the story of this bit of Internet plumbing.

LDAP is not limited to contact information, or even information about people. LDAP is used to look up encryption certificates, pointers to printers and other services on a network, and provide "single sign-on" where one password for a user is shared between many services. LDAP is appropriate for any kind of directory-like information, where fast lookups and less-frequent updates are the norm. LDAP also defines: **Permissions,** set by the administrator to allow only certain people to access the LDAP database, and optionally keep certain data private. **Schema:** a way to describe the format and attributes of data in the server.

Q.2. (*ii*) Authentication service security. **(2.5)**

Ans. Authentication Service Security: Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an **authentication** server. If the credentials match, the process is completed and the user is granted authorization for access. Authentication Service facilitates username/password validation using your on-premises Active Directory/LDAP server. Authentication Service is installed as a virtual appliance and communicates with your local directory using LDAP over SSL.

Security service is a service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers as defined by ITU-T X.800 Recommendation.

Q.2. (*iii*) Pull attack on mobile device. **(2.5)**

Ans. Pull attack on mobile devices: A mobile device attack is an exploit targeting handheld communications devices, such as smartphones and tablets. It is control of the device as a source of data by an attacker which obtained data by device itself. Mobile devices are vulnerable to new types of security attacks and vulnerable to theft not because of the get these devices itself, but because of get to sensitive data that exist within its devices. Security is an important consideration and it should be taken in all aspects of computing, especially in mobile computing because the mobile user may face many security threats that may be not exposed to the traditional computing user. These threats include lose or stolen the private and sensitive data of mobile users that stored on their devices or it could be badly used by hackers and other threats.

Q.2. (*iv*) Push attack on mobile device.

Ans. Push attack on mobile devices: It's creation a malicious code at mobile device by attacker and he may spread it to affect on other elements of the network. One aspect for the data stored within the mobile devices itself, and the second aspect of the data transmitted through the network between mobile units and mobile support stations. This division was as the result of a relationship of mobile computing with distributed computing, which is a mobile computing rely on the existence of distributed systems infrastructure with one of the most important components are wireless networks.

Q.3. Define and differentiate between:- (Any 4) **(2.5)**

(i) EFT & EDI

Ans. EFT and EDI: Electronic funds transfer (EFT) is the term used for EDI that involves the transfer of funds between financial institutions. Thus, EFTs are only one specific form of EDI, albeit the form most familiar to lay users and bank customers. While EDI has been around for decades, it wasn't until the late 1990s that this basic principle became a driving force in the rollout of electronic commerce, corporate extranets linking suppliers and customers, and related network-based technologies. Advances in EDI, combined with the rise and spread of the Internet, have led to wide use of EFTs at the same time that EDI has almost completely taken over business-to-business data transfers.

Electronic data interchange (EDI), or electronic data processing, is the electronic transmission of data between computers in a standard, structured format. EDI allows companies to process routine business transactions, such as orders and invoices, more rapidly, accurately, and efficiently than they could through conventional methods of transmission.

Q.3. (*ii*) VO & VPN

Ans. A VoIP VPN combines voice over IP and virtual private network technologies to offer a method for delivering secure voice. Because VoIP transmits digitized voice as a stream of data, the VoIP VPN solution accomplishes voice encryption quite simply, applying standard data-encryption mechanisms inherently available in the collection of protocols used to implement a VPN.

The VoIP gateway-router first converts the analog voice signal to digital form, encapsulates the digitized voice within IP packets, then encrypts the digitized voice

using IPsec, and finally routes the encrypted voice packets securely through a VPN tunnel. At the remote site, another VoIP router decodes the voice and converts the digital voice to an analog signal for delivery to the phone.

A VoIP VPN can also run within an IP in IP tunnel or using SSL-based OpenVPN. There is no encryption in former case, but traffic overhead is significantly lower in comparison with IPsec tunnel. The advantage of OpenVPN tunneling is that it can run on a dynamic IP and may provide up to 512 bits SSL encryption.

Q.3. (iii) IPv4 & IPv6

Ans. IPv4 and IPv6: The Internet Protocol version 4 (**IPv4**) is a protocol for use on packet-switched Link Layer networks (e.g. Ethernet). **IPv4**provides an addressing capability of approximately 4.3 billion addresses. The **Internet Protocol version 6** (**IPv6**) is more advanced and has better features compared to **IPv4**.

IPv4 is the most widely deployed Internet protocol used to connect devices to the Internet. IPv4 uses a 32-bit address scheme allowing for a total of 2^32 addresses (just over 4 billion addresses). With the growth of the Internet it is expected that the number of unused IPv4 addresses will eventually run out because every device — including computers, smartphones and game consoles — that connects to the Internet requires an address.

IPv6 is the successor to Internet Protocol Version 4 (IPv4). It was designed as an evolutionary upgrade to the Internet Protocol and will, in fact, coexist with the older IPv4 for some time. IPv6 is designed to allow the Internet to grow steadily, both in terms of the number of hosts connected and the total amount of data traffic transmitted.

Q.3. (iv) Attacks and Threats

Ans. Attacks and Threats: A *threat* is an event that can take advantage of vulnerability and cause a negative impact on the network. Potential *threats* to the network need to be identified, and the related vulnerabilities need to be addressed to minimize the risk of the *threat*. In computer security a *threat* is a possible danger that might exploit a vulnerability to breach *attack*, led to a new term cyberwarfare. It should be noted that nowadays the many real *attacks* exploit Psychology at least as much as technology. Modern computer systems, linked by national and global networks, face a variety of threats and attacks that can result in significant financial and information losses. These threats vary considerably, from threats to data integrity resulting from accidental, unintentional errors and omissions to threats from malicious hackers attempting to crash a system. An attack is an intentional threat and is an action performed by an entity with the intention to violate security. Examples of attacks are destruction, modification, fabrication, interruption or interception of data. An attack is a violation of data integrity and often results in disclosure of information, a violation of the confidentiality of the information, or in modification of the data. An attacker can gain access to sensitive information by attacking in several steps, where each step involves an illegal access to the system. An intentional threat can be caused by an insider or outsider, can be a spy, hacker, corporate raider, or a disgruntled employee.

Any attack on the security of a system can be a direct and indirect attack. A direct attack aims directly at the desired part of the data or resources. Several components in a system may be attacked before the intended (final) information can be accessed. In an indirect attack, information is received from or about the desired data/resource without directly attacking that resource. Indirect attacks are often troublesome in database systems where it is possible to derive confidential information by posing indirect questions to the database. Such an indirect attack is often called inference.

Q.3. (v) WWW and Internet

Ans. WWW and Internet: The World Wide Web (WWW) is one set of software services running on the Internet. The Internet itself is a global, interconnected network of computing devices. This network supports a wide variety of interactions and communications between its devices. The World Wide Web is a subset of these interactions and supports websites and URIs. The Internet is actually a huge network that is accessible to everyone & everywhere across the world. The network is composed of sub-networks comprising of a number of computers that are enabled to transmit data in packets. The internet is governed by a set of rules, laws & regulations, collectively known as the Internet Protocol (IP). The Internet & the World Wide Web (the Web), though used interchangeably, are not synonymous. Internet is the hardware part - it is a collection of computer networks connected through either copper wires, fiber-optic cables or wireless connections whereas, the World Wide Web can be termed as the software part – it is a collection of web pages connected through hyperlinks and URLs. In short, the World Wide Web is one of the services provided by the Internet.

Q.3. (vi): 1 tier and 2 tier architecture of IS

Ans. 1tier and 2 tier architecture of IS:

In 1 tier all the processing is done on only one machine,& number of clients attached to this machine. One-tier architecture involves putting all of the required components for a software application or technology on a single server or platform. This kind of architecture is often contrasted with multi-tiered architecture or the three-tier architecture that's used for some Web applications and other technologies where various presentation, business and data access layers are housed separately.

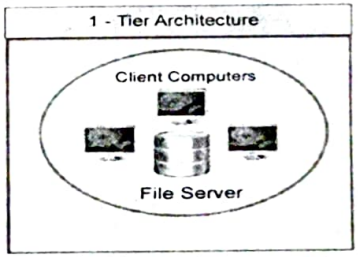


Fig 2: 1Tier Architecture of IS

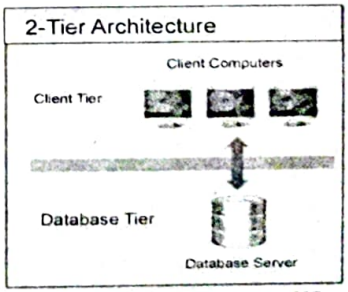


Fig: 2-Tier Architecture of IS

In 2 tier architecture Client & Database is on different system. Processing is done at client side. Application layer is at client side. The two-tier is based on Client Server architecture. The two-tier architecture is like client server application. The direct communication takes place between client and server. There is no intermediate between client and server. Because of tight coupling a 2 tiered application will run faster.

Q.4. What are the three pillars of security ? Define the following terms: (5)

(*i*) Access control **(*iii*) Denial-of-Service**

(*ii*) Non-repudation **(*iv*) Spoofing**

Ans. Pillers of security: Information security is dynamic and complex to the point that it's easy to get overwhelmed by the details and lose track of the real issues. I find it valuable to periodically relate whatever task I'm working on back to the three pillars of information security: confidentiality, integrity, and availability.

• **(*i*) Access Control:** In the fields of physical security and information security, access control (AC) is the selective restriction of access to a place or other resource. The act of accessing may mean consuming, entering, or using. Permission to access a resource is called authorization. *Access control* systems perform authorization identification, authentication, *access* approval, and accountability of entities through login credentials including passwords, personal identification numbers (PINs), biometric scans, and physical or electronic keys.

• **(*ii*) Non-repudation:** Nonrepudiation is the assurance that someone cannot deny something. Typically,nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated. Regarding digital security, the cryptological meaning and application of *non-repudiation* shifts to mean: A service that provides proof of the integrity and origin of data. An authentication that can be asserted to be genuine with high assurance.

• **(*iii*) Denial-of-Service:** In computing, a *denial-of-service* attack (DoS attack) is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. A *denial-of-service* attack is a security event that occurs when an attacker takes action that prevents legitimate users from accessing targeted computer systems, devices or other network resources.

• **(*iv*) 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, thereby gaining an illegitimate advantage. *Spoofing*, in general, is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver. *Spoofing* is most prevalent in communication mechanisms that lack a high level of security.

END TERM EXAMINATION [DEC. 2016]
SEVENTH SEMESTER [B.TECH]
INFORMATION SECURITY [ETCS-401]

Time : 3 hrs. **M.M. : 75**

Note: *Questions One is complusory. Attempt any five more questions from the rest of the Questions..*

Q.1. Attempt any 7 out of 8 parts. **(7x5=35)**

(*a*) Describe the main principles of information security.

Ans. A **principle** which is a core requirement of **information security** for the safe utilization, flow, and storage of **information** is the CIA triad. CIA stands for confidentiality, integrity, and availability and these are the three **main** objectives of **information security**.

• **Confidentiality:** This means that information is only being seen or used by people who are authorized to access it.

• **Integrity:** This means that any changes to the information by an unauthorized user are impossible (or at least detected), and changes by authorized users are tracked.

• **Availability:** This means that the information is accessible when authorized users need it.

Q.1. (*b*) Describe the various provision of Cyber Laws.

Ans. Cyber law India is an organization that is dedicated to the passing of relevant and dynamic Cyber laws in India. Considering India is one of the biggest economies impacting electronic commerce and the biggest markets to target, it is but natural to accept that India should have in place appropriate enabling legal provisions for effective and secure cyber transactions.

Cyber law is important because it touches almost all aspects of transactions and activities on and involving the internet, World Wide Web and cyberspace. Every action and reaction in cyberspace has some legal and cyber legal perspectives. Cyber law encompasses laws relating to –

- Cyber crimes
- Electronic and digital signatures
- Intellectual property
- Data protection and privacy

Q.1. (*c*) What is Cyber forensics? Is Ethical Hacking part of the Digital Hacking? Justify your answer.

Ans. Cyber **forensics** is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

Ethical hackers coming from this area of expertise also have knowledge in problem-solving strategies for security breaches, and can collect and analyze data to monitor and interpret weaknesses. Expect them to possess deep knowledge of the latest infrastructure and hardware, from routers to memory storage, with the ability to establish security policies and best practices. Some ethical hackers are doing it for the

satisfaction and challenge, and others come from robust IT backgrounds with a focus on digital security. Meanwhile, traditional hackers are usually hacking into systems illegally for fun, profit or even revenge.

Q.1. (d) What is VPN? What are the different types of VPN?

Ans. A **VPN** or **Virtual Private Network** is a method used to add security and privacy to private and public networks, like WiFi Hotspots and the Internet. **VPNs** are most often used by corporations to protect sensitive data.

Different types of VPN:

1. Remote Access VPN: Remote access VPN allows a user to connect to a private network and access its services and resources remotely. The connection between the user and the private network happens through the Internet and the connection is secure and private.

2. Site – to – Site VPN: A Site-to-Site VPN is also called as Router-to-Router VPN and is mostly used in the corporates. Companies, with offices in different geographical locations, use Site-to-site VPN to connect the network of one office location to the network at another office location.

Q. 1. (e) Describe the Security challenges in Mobile Devices?

Ans. Security challenges of mobile devices are:

- Threats.
- Consequences.
- Attack based on SMS and MMS.
- Attacks based on communication networks.
- Web browser.
- Operating system.
- Electromagnetic Waveforms.
- Juice Jacking

Q.1. (f) Explain how the digital Signatures helps to improve the information security in the real time project.

Ans. In the digital age where every single thing is changing to digital, paper signature has change to become digital signature. Digital signature is doing away with the concept of paper copy. Many businesses are therefore shifting from the acceptance of paper signatures to digital signatures. In the transition of pen on paper to digital signs laws and acts have been passed by the Govt. One such act is Electronic Signatures in Global and National Commerce Act. The act says that a signature which is signed electronically will not be denied. There are very many significances and benefits of digital signatures:

Authentication: Electronic signatures can more trustworthy and reliable in comparison to the signs on paper. Once signs get established digitally there is no way by which people can change it.

Integrity maintained: Electronic signs reduce the risk of forgery after documents are sent. It also reduced the documents getting altered after they are sent. If any minute changes are found in the sign the document gets instantly rejected.

Long distance: Businesses are taking place all over the world. Companies may have branches or clients overseas. The digital signature allows businessmen to sign contracts all over the world and send them via emails. This saves time and energy as individuals needed to fly to different parts of the world to sign their deals.

Q.1. (g) Discuss various legal challenges framework for information security.

Ans. There are various legal challenges framework for information security that are neede to improved. The existing legal framework needs to be improved in these matters:

- **Legislation** – adopting relevant laws, setting out standards and areas of Information Security, as well as functions of some institutions
- **Institutions** – responsible for tasks relating to verification and certification methods, software application, devices and systems, R&D and oversight of the IS standards implementation by state authorities
- **National CERT** – Computer Emergency Response Team

Q.1. (h) What is E-Commerce. Discuss various concepts in electronic Payment System.

Ans. E-commerce is a transaction of buying or selling online. Electronic commerce draws on technologies such as mobile commerce, electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems, and automated data collection systems. Modern electronic commerce typically uses the World Wide Web for at least one part of the transaction's life cycle although it may also use other technologies such as e-mail.

Electronic Payment is a financial exchange that takes place online between buyers and sellers. The content of this exchange is usually some form of digital financial instrument (such as encrypted credit card numbers, electronic cheques or digital cash) that is backed by a bank or an intermediary, or by a legal tender. The various factors that have lead the financial institutions to make use of electronic payments are:

(i) . Decreasing technology cost:

The technology used in the networks is decreasing day by day, which is evident from the fact that computers are now dirt-cheap and Internet is becoming free almost everywhere in the world.

(ii) . Reduced operational and processing cost:

Due to reduced technology cost the processing cost of various commerce activities becomes very less. A very simple reason to prove this is the fact that in electronic transactions we save both paper and time.

Q. 2. Compare and Contrast between different Cipher Techniques used in information Security like Caesar Cipher ,Vigenere Cipher, Rail fence Cipher, Hill Climbing Cipher, Play Fair Cipher etc. (10)

Ans. Difference between different cipher techniques

Caesar cipher : The **Caesar cipher**, also known as a shift **cipher**, is one of the simplest forms of encryption. It is a substitution **cipher** where each letter in the original message (called the plaintext) is replaced with a letter corresponding to a certain number of letters up or down in the alphabet.

Vigenère cipher: The **Vigenère cipher** is a method of encrypting alphabetic text by using a series of interwoven Caesar **ciphers** based on the letters of a keyword. It is a form of polyalphabetic substitution. Though the cipher is easy to understand and implement, for three centuries it resisted all attempts to break it; this earned it the description **le chiffre indéchiffrable** (French for 'the indecipherable cipher'). Many people have tried to implement encryption schemes that are essentially Vigenère ciphers.

Rail fence cipher : The **rail fence cipher** (also called a zigzag cipher) is a form of transposition cipher. It derives its name from the way in which it is encoded. In the rail fence cipher, the plain text is written downwards and diagonally on successive "rails" of an imaginary fence, then moving up when we reach the bottom rail. When we reach the top rail, the message is written downwards again until the whole plaintext is written out. The message is then read off in rows.

Hill cipher :In classical cryptography, the **Hill cipher** is a polygraphic substitution cipher based on linear algebra. Invented by Lester S. Hillin 1929, it was the first polygraphic cipher in which it was practical (though barely) to operate on more than three symbols at once. The following discussion assumes an elementary knowledge of matrices.

Each letter is represented by a number modulo 26. Often the simple scheme A = 0, B = 1, ..., Z = 25 is used, but this is not an essential feature of the cipher. To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible $n \times n$ matrix, against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible $n \times n$ matrices (modulo 26). The cipher can, of course, be adapted to an alphabet with any number of letters; all arithmetic just needs to be done modulo the number of letters instead of modulo 26.

Playfair cipher : The **Playfair cipher** or **Playfair square** or **Wheatstone-Playfair cipher** or **Wheatstone cipher** is a manual symmetric encryption technique and was the first literal digram substitution cipher. The scheme was invented in 1854 by Charles Wheatstone, but bears the name of Lord Playfair who promoted the use of the cipher.

The technique encrypts pairs of letters (*bigrams* or *digrams*), instead of single letters as in the simple substitution cipher and rather more complex Vigenère cipher systems then in use. The Playfair is thus significantly harder to break since the frequency analysis used for simple substitution ciphers does not work with it. The frequency analysis of bigrams is possible, but considerably more difficult. With 600 possible bigrams rather than the 26 possible monograms (single symbols, usually letters in this context), a considerably larger cipher text is required in order to be useful. It became known as the Playfair cipher after Lord Playfair, who heavily promoted its use, despite its invention by Wheatstone. The first recorded description of the Playfair cipher was in a document signed by Wheatstone on 26 March 1854.

Playfair is no longer used by military forces because of the advent of digital encryption devices. This cipher is now regarded as insecure for any purpose, because modern computers could easily break it within seconds.

Q.3. What are Biometric System. Explain their role in the information Security. Also discuss about design issues as well Criteria for the selection of biometrics taking a sample case study of any Biometric metric you have used or seen. (10)

Ans. Biometric Sytem: Biometrics refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance.

Biometric identifiers are then distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape

of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice. Some researchers have coined the term behaviometrics to describe the latter class of biometrics.

More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information

Role: Many different aspects of human physiology, chemistry or behavior can be used for biometric authentication. The selection of a particular biometric for use in a specific application involves a weighting of several factors. Universality means that every person using a system should possess the trait.

- Uniqueness means the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another.
- Permanence relates to the manner in which a trait varies over time. More specifically, a trait with 'good' permanence will be reasonably invariant over time with respect to the specific matching algorithm.
- Measurability (collectability) relates to the ease of acquisition or measurement of the trait. In addition, acquired data should be in a form that permits subsequent processing and extraction of the relevant feature sets.
- Performance relates to the accuracy, speed, and robustness of technology used (see performance section for more details).
- Acceptability relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed.
- Circumvention relates to the ease with which a trait might be imitated using an artifact or substitute.

Proper biometric use is very application dependent. Certain biometrics will be better than others based on the required levels of convenience and security.[9] No single biometric will meet all the requirements of every possible application

Design issues: Biometric data contains information acquired from individuals, which can be used to identify them. This raises issues of privacy and data protection. If the biometric data is recorded in a central database, privacy concerns may be higher than for systems where an individual's data is stored only on a card retained by the individual. Note however, some biometric applications require a central database for their basic functionality e.g. to check for multiple enrolment attempts.

Enrollees may be concerned that their biometric data could be used for other purposes than it was originally acquired; for example, face image data might be used for surveillance purposes and fingerprint data checked against forensic databases. These concerns are at the heart of many objections to the use of biometrics.

It is therefore necessary to understand privacy issues in regard to biometric data and biometric systems and to apply to protective safeguards in the deployment of these systems.

Biometric Case Study:

States Beat Benefit Fraud

Many states are investigating and piloting biometric systems to identify benefit recipients in order to reduce fraud and increase efficiency. One state's high-tech benefit system checks for evidence of wrongdoing and creates identification cards as clients enroll. Applicants place their index fingers on an optical reader which scans the prints to create images for the database. At the same time, the applicant's photo is taken with a digital camera. Next, the client signs his or her name on a tablet that captures the signature electronically. All these files are transmitted to a host computer, where, in minutes, search engines verify that the person has not enrolled in the system under another identity. After a client is accepted into the system, an identification card is created on the spot. A two-dimensional symbol on the card encodes the fingerprint file. The card also carries the client's photo and signature, and a magnetic stripe for future use. Clients present their cards and have their fingerprint scanned for verification when they collect benefits. In this state, 41 percent of General Assistance and 31 percent of AFDC recipients failed to re-enroll in those programs when the new identification cards were issued. This is attributed to the deterrence factor the new system provides. Those who attempt multiple enrollments will be caught; suspected fraud cases are now under investigation.

Q.4. Differentiate between Public and Private Key Cryptography. Tasking an example of any algorithm of your choice,(example : DES and RSA etc) explain which of the two is more secure and why? (10)

Ans. Difference between public and private key cryptography:

For symmetric **encryption**, the same **key** is used to encrypt the message and to decrypt it. For **public-key encryption**, instead the recipient generates two **keys** together, a **public encryption key** and a **private** decryption **key**. The message is encrypted with the **public key**, and can only be decrypted with the **private key**. A published key that can be used to send a secure message to a receiver. A secret key that can be used to decrypt messages encrypted with the corresponding public or private key.

Examples of RSA:

We will see two aspects of the RSA cryptosystem, firstly generation of key pair and secondly encryption-decryption algorithms.

Generation of RSA Key Pair

Each person or a party who desires to participate in communication using encryption needs to generate a pair of keys, namely public key and private key. The process followed in the generation of keys is described below—

- **Generate the RSA modulus (n)**

→ Select two large primes, p and q.

→ Calculate n=p*q. For strong unbreakable encryption, let n be a large number, typically a minimum of 512 bits.

- **Find Derived Number (e)**

→ Number e must be greater than 1 and less than (p – 1)(q – 1).

→ There must be no common factor for e and (p – 1)(q – 1) except for 1. In other words two numbers e and (p – 1)(q – 1) are co prime.

- **Form the public key**

→ The pair of numbers (n, e) form the RSA public key and is made public.

→ Interestingly, though n is part of the public key, difficulty in factorizing a large prime number ensures that attacker cannot find in finite time the two primes (p & q) used to obtain n. This is strength of RSA.

- **Generate the private key**

→ Private Key d is calculated from p, q, and e. For given n and e, there is unique number d.

→ Number d is the inverse of e modulo (p –1)(q – 1). This means that d is the number less than (p – 1)(q – 1) such that when multiplied by e, it is equal to 1 modulo (p – 1) (q – 1).

→ This relationship is written mathematically as follows –

ed = 1 mod (p – 1)(q – 1)

The Extended Euclidean Algorithm takes p, q, and e as input and gives d as output.

Example:

An example of generating RSA Key pair is given below. (For ease of understanding, the primes p & q taken here are small values. Practically, these values are very high).

- Let two primes be p = 7 and q = 13. Thus, modulus n = pq = 7 x 13 = 91.
- Select e = 5, which is a valid choice since there is no number that is common factor of 5 and (p – 1)(q – 1) = 6 × 12 = 72, except for 1.
- The pair of numbers (n, e) = (91, 5) forms the public key and can be made available to anyone whom we wish to be able to send us encrypted messages.
- Input p = 7, q = 13, and e = 5 to the Extended Euclidean Algorithm. The output will be d = 29.
- Check that the d calculated is correct by computing

de = 29 × 5 = 145 = 1 mod 72

- Hence, public key is (91, 5) and private keys is (91, 29).

Encryption and Decryption

Once the key pair has been generated, the process of encryption and decryption are relatively straight forward and computationally easy.

Interestingly, RSA does not directly operate on strings of bits as in case of symmetric key encryption. It operates on numbers modulo n. Hence, it is necessary to represent the plain text as a series of numbers less than n.

RSA Encryption:

- Suppose the sender wish to send some text message to someone whose public key is (n, e).
- The sender then represents the plain text as a series of numbers less than n.
- To encrypt the first plain text P, which is a number modulo n. The encryption process is simple mathematical step as–

$$C = P^e \bmod n$$

- In other words, the ciphertext C is equal to the plaintext P multiplied by itself e times and then reduced modulo n. This means that C is also a number less than n.
- Returning to our Key Generation example with plaintext P = 10, we get cipher text C

$$C = 10^5 \bmod 91$$

RSA Decryption

- The decryption process for RSA is also very straightforward. Suppose that the receiver of public-key pair (n, e) has received a cipher text C.
- Receiver raises C to the power of his private key d. The result modulo n will be the plaintext P.

$$\text{Plaintext} = C^d \bmod n$$

• Returning again to our numerical example, the cipher text C = 82 would get decrypted to number 10 using private key 29–

$$\text{Plaintext} = 82^{29} \mod 91 = 10$$

Q 5. What is IDS(Intrusion Detection System)? Explain the need for intrusion monitoring and detection. Explain any three network attacks you have studied. (10)

Ans. Intrusin Detection System: An **Intrusion Detection System** (IDS) is a network security technology originally built for detecting vulnerability exploits against a target application or computer. Intrusion Prevention Systems (IPS) extended IDS solutions by adding the ability to block threats in addition to detecting them and has become the dominant deployment option for IDS/IPS technologies. This article will elaborate on the configuration and functions that define the IDS deployment.

An IDS needs only to detect threats and as such is placed out-of-band on the network infrastructure, meaning that it is not in the true real-time communication path between the sender and receiver of information. Rather, IDS solutions will often take advantage of a TAP or SPAN port to analyze a copy of the inline traffic stream (and thus ensuring that IDS does not impact inline network performance).

IDS was originally developed this way because at the time the depth of analysis required for intrusion detection could not be performed at a speed that could keep pace with components on the direct communications path of the network infrastructure.

Why do I need IDS: In today's fast-changing IT world, even the best available security is insufficient for the latest vulnerabilities in various products, and against malware/attacks created to target those vulnerabilities. While cyber-security cannot be 100 per cent fool-proof, we can still try to achieve the maximum security possible. This article describes intrusion detection systems (IDS), usually found in a hardware-based offering, that detect attackers and the unauthorised access to a computer network. Network administrators and architects, as well as senior members of the IT management team, may find the information given here, useful.

In a typical network scenario, a firewall is usually capable of keeping the bad guys out. While anti-virus (AV) software detects and stops most viruses, password protection systems take care of access-control, etc. Thus, most people in IT management naturally wonder, "Why do I need an IDS?"

The reasons are in how an IDS works. A firewall controls network traffic at the TCP/IP port level, by blocking access to unwanted ports. However, it keeps open those ports used by applications — for example, port 80 for HTTP traffic. Thus, all attacks over HTTP will not be stopped by the firewall. Similarly, AV systems are great at detecting viruses, but time has proven that they fail to protect the system from malware like adware or spyware. Passwords certainly provide the basic building blocks in security systems, but are prone to attack attempts; they could be stolen manually or electronically, or even be easily guessed, in the worst-case scenario.

Thus, having basic security only gives you the misleading feeling of being secure, rather than actual security. Modern attackers are experts who exploit software vulnerabilities by using technical tools, and devise methods to break into a network to achieve their goals. To handle smart attack attempts, an even smarter security mechanism is needed, which will proactively and intelligently keep an eagle's eye on the network, and monitor and report incidents swiftly. IDSs or IPSs (Intrusion Protection Services) are solutions that encompass these requirements.

Common Types of Network Attacks:

Eavesdropping: In general, the majority of network communications occur in an unsecured or "cleartext" format, which allows an attacker who has gained access to data paths in your network to "listen in" or interpret (read) the traffic. When an attacker is eavesdropping on your communications, it is referred to as sniffing or snooping. The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise. Without strong encryption services that are based on cryptography, your data can be read by others as it traverses the network.

Data Modification: After an attacker has read your data, the next logical step is to alter it. An attacker can modify the data in the packet without the knowledge of the sender or receiver. Even if you do not require confidentiality for all communications, you do not want any of your messages to be modified in transit. For example, if you are exchanging purchase requisitions, you do not want the items, amounts, or billing information to be modified.

Identity Spoofing (IP Address Spoofing): Most networks and operating systems use the IP address of a computer to identify a valid entity. In certain cases, it is possible for an IP address to be falsely assumed— identity spoofing. An attacker might also use special programs to construct IP packets that appear to originate from valid addresses inside the corporate intranet.

Password-Based Attacks: A common denominator of most operating system and network security plans is password-based access control. This means your access rights to a computer and network resources are determined by who you are, that is, your user name and your password.

Older applications do not always protect identity information as it is passed through the network for validation. This might allow an eavesdropper to gain access to the network by posing as a valid user.

When an attacker finds a valid user account, the attacker has the same rights as the real user. Therefore, if the user has administrator-level rights, the attacker also can create accounts for subsequent access at a later time.

Denial-of-Service Attack: Unlike a password-based attack, the denial-of-service attack prevents normal use of your computer or network by valid users.

After gaining access to your network, the attacker can do any of the following:

• Randomize the attention of your internal Information Systems staff so that they do not see the intrusion immediately, which allows the attacker to make more attacks during the diversion.

• Send invalid data to applications or network services, which causes abnormal termination or behavior of the applications or services.

• Flood a computer or the entire network with traffic until a shutdown occurs because of the overload.

• Block traffic, which results in a loss of access to network resources by authorized users.

Compromised-Key Attack: A key is a secret code or number necessary to interpret secured information. Although obtaining a key is a difficult and resource-intensive process for an attacker, it is possible. After an attacker obtains a key, that key is referred to as a compromised key.

An attacker uses the compromised key to gain access to a secured communication without the sender or receiver being aware of the attack. With the compromised key, the attacker can decrypt or modify data, and try to use the compromised key to compute additional keys, which might allow the attacker access to other secured communications.

Sniffer Attack: A *sniffer* is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. Even encapsulated

(tunneled) packets can be broken open and read unless they are encrypted *and* the attacker does not have access to the key.

Application-Layer Attack: An application-layer attack targets application servers by deliberately causing a fault in a server's operating system or applications. This results in the attacker gaining the ability to bypass normal access controls. The attacker takes advantage of this situation, gaining control of your application, system, or network, and can do any of the following:

- Read, add, delete, or modify your data or operating system.
- Introduce a virus program that uses your computers and software applications to copy viruses throughout your network.
- Introduce a sniffer program to analyze your network and gain information that can eventually be used to crash or to corrupt your systems and network.
- Abnormally terminate your data applications or operating systems.
- Disable other security controls to enable future attacks.

Q. 6. Explain the differences between various networking devices like : Hubs, Switches, Routers, Bridges and Gateways etc, explain their role, functionality and on which layer of the OSI Model do they operate. (10)

Ans. Difference between different networking devices:

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do no amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

2. Hub – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

3. Bridge – A bridge operates at data link layer. A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

4. Switch – A switch is a multi port bridge with a buffer and a design that can boost its efficiency(large number of ports imply less traffic) and performance. Switch is data link layer device. Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.

5. Routers – A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.

6. Gateway – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

FIRST TERM EXAMINATION [SEPT. 2017]
SEVENTH SEMESTER [B.TECH.]
INFORMATION SECURITY [ETCS–401]

Time : 1½ hrs. **M.M. : 30**

Note: *Attempt any three questions including Q.1 is compulsory.*

Q.1. Attempts all parts of the following:

Q.1. (a) What do you mean by cyber crime? Point out four basic sources of security threats? (2)

Ans. Cybercrime: Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitive or malicious purposes.

Common types of cybercrime include online bank information theft, identity theft, online predatory crimes and unauthorized computer access. More serious crimes like cyberterrorism are also of significant concern.

Cybercrime encompasses a wide range of activities, but these can generally be broken into two categories:

- Crimes that target computer networks or devices. These types of crimes include viruses and denial-of-service (DoS) attacks.
- Crimes that use computer networks to advance other criminal activities. These types of crimes include cyberstalking, phishing and fraud or identity theft.

For basic sources of security threats:

1. Spoofing

- **Spoofing** - Done at the data link and network layers, this is an attack where an attacker will try to get one computer to pretend it is another computer to fool another system or part of the network into allowing privileges of the spoofed computer. Sequence number spoofing may be used for this type of attack.
- Masquerade - Done at the network layer, this is an attack where an attacker will try to access a computer pretending to have an authorized user identity such as a network administrator.

2. Scanning

- Sequential Scanning - Attempting to log onto a system by sequentially trying different combinations of passwords and user IDs.
- Dictionary Scanning - Attempting to log onto a system by sequentially trying passwords for users that may be dictionary words such as "password"

3. Snooping or Sniffing

- Digital Snooping - Monitoring a private or public network for passwords or data. This attack is at the network layer.
- Shoulder Snooping - This is a physical attack where someone trys to watch for typed passwords or see information on a computer monitor that they should not have access to.

4. Scavenging

o **Dumpster Diving** - Trying to get information from the trash with the hope that it will allow the attacker to get access or priviledged information

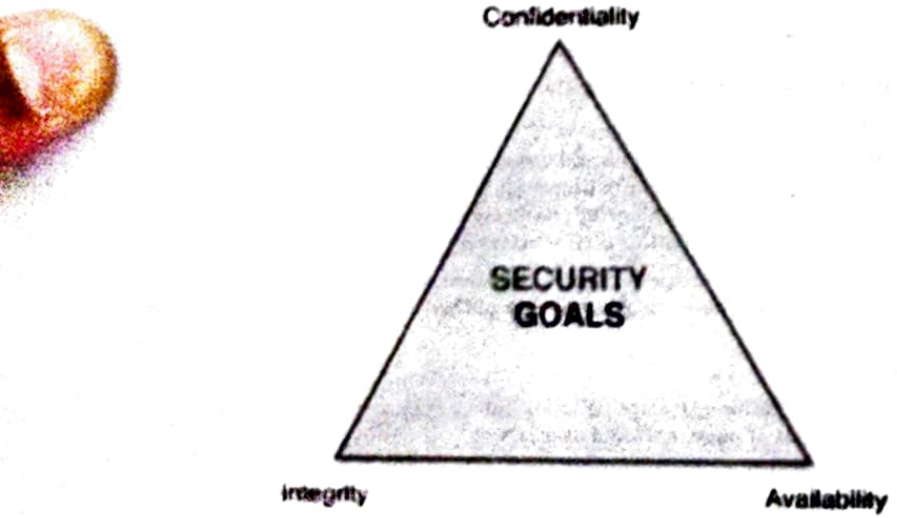
o **Browsing** - Scanning of large amounts of unprotected data to get information for greater access. This is usually automated and an indication of its activity would be an authorized user on line at unusual times

Q.1.(b) Why confidentiality is an important principle of security describe the ways of achieving it? (2)

Ans. All information security measures try to address at least one of three goals:

- Protect the confidentiality of data
- Preserve the integrity of data
- Promote the availability of data for authorized use

Confidentiality refers to protecting information from being accessed by unauthorized parties. Imagine your bank records. You should be able to access them, of course, and employees at the bank who are helping you with a transaction should be able to access them, but no one else should. A failure to maintain confidentiality means that someone who shouldn't have access has managed to get it, through intentional behavior or by accident. Such a failure of confidentiality, commonly known as a *breach*, typically cannot be remedied.



A very key component of protecting information confidentiality would be encryption. Encryption ensures that only the right people (people who knows the key) can read the information. A very prominent example will be SSL/TLS, a security protocol for communications over the internet that has been used in conjunction with a large number of internet protocols to ensure security.

Q.1.(c) Differentiate between active and passive attacks. Name some active and passive attacks. (2)

Ans.

Basic for Comparison	Active attack	Passive attack
Basic	Active attack tries to change the system resources or affect their operation.	Passive attack tries to read or make use of information from the system but does not influence system resources
Modification in the information	Occurs	Does not take place
Harm to the system	Always causes damage to the system	Do not cause any harm
Threat to	Integrity and availability	Confidentiality
Attack awareness	The entity (victim) gets informed about the attack.	The entity is unaware of the attack
Task performed by the attacker	The transmission is captured by physically controlling the portion of a link.	Just need to observe the transmission

Active attack: Some active attacks are spoofing attack, Wormhole attack, Modification, Denial of services, Sinkhole, and Sybil attack.

Passive attack: The names of some passive attacks are traffic analysis, Eavesdropping, and Monitoring.

Q.1.(d) Explain the meaning of computer based IS. (2)

Ans. Refer Q.1.(d) First term september-2016 [page no. – 2-2016]

Q.1.(e) Explain the need of distributed IS in current scenario. (2)

Ans. Refer Q.1.(e) First term september-2016 [page no. – 2-2016]

Q.2. Write short notes on:

(i) Message Integrity: (2.5)

Ans. Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality). These measures include file permissions and user access controls. Version control may be used to prevent erroneous changes or accidental deletion by authorized users becoming a problem. In addition, some means must be in place to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse (EMP) or server crash. Some data might include checksums, even cryptographic checksums, for verification of integrity. Backups or redundancies must be available to restore the affected data to its correct state.

The basic premise is a sender wishes to send a message to a receiver, and wishes for the integrity of their message to be guaranteed. The sender will calculate a hash on the message, and include the digest with the message.

On the other side, the receiver will independently calculate the hash on just the message, and compare the resulting digest with the digest which was sent with the message. If they are the same, then the message must have been the same as when it was originally sent.

Q.2.(ii) Denial of Service **(2.5)**

Ans. Denial-of-Service: In computing, a denial-of-service attack (DoS attack) is a cyber-attack where the perpetrator seeks to make a machine or network resource unvailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. A *denial-of service* attack is a security event that occurs when an attack takes action that prevents legitimate users from accessing targeted computer systems, devices or other network resources.

Q.2.(iii) Passive Attack **(2.5)**

Ans. 1. Passive Attack: It attempts to learn or make use of information from the system but does not affect system resources.

2. Active Attack: It attempts to alter system resources or affect their operation.

3. Passive Attacks:

1. Passive attacks are in the nature of eavesdropping on, or monitoring of transmissions.

2. The goal of the opponent is to obtain information that is being transmitted.

3. There are 2 types of passive attacks they are

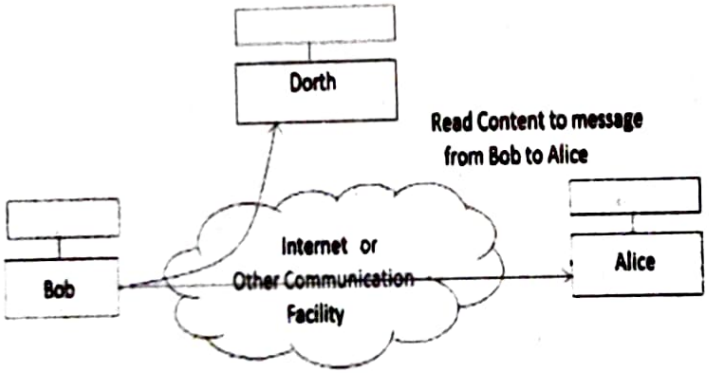


Fig. Release of Message Contents

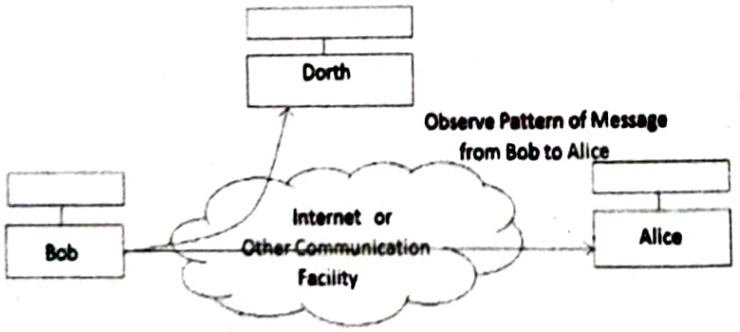


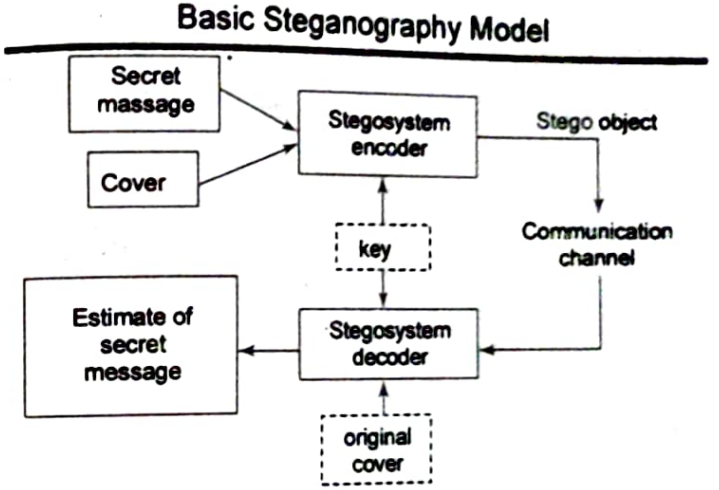
Fig. Traffic analysis

Q.2.(iv) Steganography **(2.5)**

Ans. Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity.

The word steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected" and graphein meaning "writing".

" Steganography means hiding one piece of data within another".



Q.3. Define and differentiate between: **(10)**

(i) EFT & EDI **(ii) VO & VPN**

(iii) Ipv4 & Ipv6 **(iv) Attacks and Threats**

(v) WWW and Internet

Ans. Refer Q.3. First term september-2016 [page no. – 2016-3]

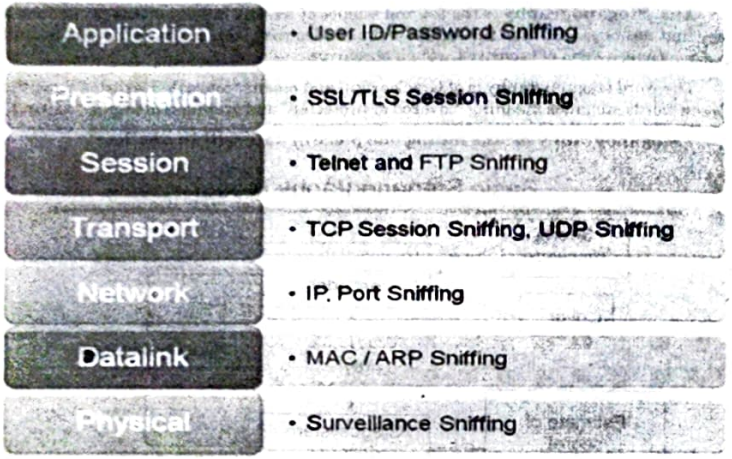
Q.4. What are the three pillars of security? Define the following terms: **(10)**

Ans. Refer Q.4. First term september-2016 [page no. – 6-2016]

(i) Sniffing:

Sniffing involves capturing, decoding, inspecting and interpreting the information inside a network packet on a TCP/IP network. The purpose is to steal information, usually user IDs, passwords, network details, credit card numbers, etc. Sniffing is generally referred to as a "passive" type of attack, wherein the attackers can be silent/ invisible on the network. This makes it difficult to detect, and hence it is a dangerous type of attack.

By its very nature, the TCP/IP protocol is only meant for ensuring that a packet is constructed, mounted on an Ethernet packet frame, and reliably delivered from the sender to the receiver across networks.



Network sniffing uses sniffer software, either open source or commercial. Broadly, there are three ways to sniff a network

It is important to remember that sniffing can range from Layer 1 through Layer 7. Talking about physical connectivity, a person (who may be an employee of the firm) who is already hooked up to the internal LAN can run tools to directly capture network traffic

Q.4.(ii) Phishing

Ans. Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft.

An organization succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust. Depending on scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering.

Phishing Attack Examples

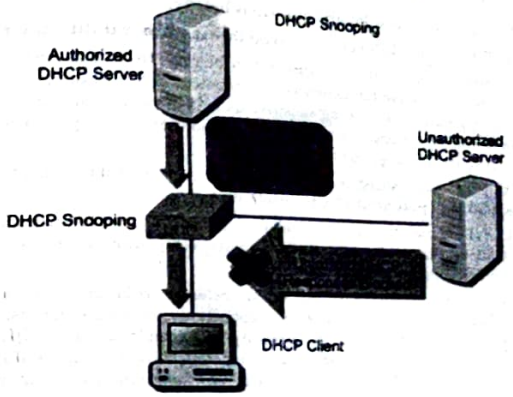
The following illustrates a common phishing scam attempt:

1. A spoofed email ostensibly from myuniversity.edu is mass-distributed to as many faculty members as possible.

2. The email claims that the user's password is about to expire. Instructions are given to go to myuniversity.edu/renewal to renew their password within 24 hours.

Q.4.(iii) Snooping

Ans. Snooping - This is when someone looks through your files in the hopes of finding something interesting whether it is electronic or on paper. In the case of physical snooping people might inspect your dumpster, recycling bins, or even your file cabinets; they can look under your keyboard for post-It-notes, or look for scraps of paper tracked to your bulletin board. Computer snooping on the other hand, involves someone searching through your electronic files trying to find something interesting.



Q.4. (iv) Spoofing

Ans. Refer Q.4. First term september-2016 [page no. – 6-2016]

END TERM EXAMINATION [DEC. 2017]
SEVENTH SEMESTER [B.TECH.]
INFORMATION SECURITY [ETCS–401]

Time : 3 hrs. **M.M. : 75**

Note: *Attempt any five question is including Q.1 which is com pulsory.*

Q.1. Attempts all the following questions briefly:

Q.1. (a) What is the difference between threat, vulnerability and risk. (3)

Ans. Threats: Cyber threats, or simply, threats refer to circumstances or events with the **potential to cause harm** by way of their outcome. A few examples of common threats include an attacker stealing sensitive data from your applications, political activists DDoSing your website, an **administrator** accidentally wiping a production system, and a storm flooding your ISP's data center.

Cyber threats are actualized by *threat actors*. Threat actors usually refer to **persons or entities who may potentially initiate a threat**.

Examples of common threat actors include financially motivated criminals (cyber criminals), politically motivated activists (hacktivists), competitors, careless employees, disgruntled employees, and nation state attackers.

Vulnerabilities: Vulnerabilities, simply refer to weaknesses in a system. Vulnerabilities make threats possible and potentially even more dangerous. A system could be exploited through a single vulnerability, for example, a single SQL injection vulnerability could provide an attacker with full-control over sensitive data, or, an attacker could *chain* several exploits together, exploiting more than one vulnerability in order to exploit a system.

examples of Vulnerabilities include:

- Lack of proper building access control
- Cross-site Scripting (XSS)
- SQL Injection
- Cleartext transmission of sensitive data
- Failure to check authorization to sensitive resources

Risks: Risks are usually confused with threats, however, there is anuanced difference between the two — a risk refers to combination of a threat's **probability** and a threat's **loss/impact** (usually in monetary terms, however, it should be noted that quantifying a breach is extremely difficult). Essentially, this translates to the following.

risk = threat probability x potential loss

Therefore, a risk is a scenario that should be avoided, combined with the likely losses to result from that scenario. The following is a hypothetical example of how a risk can be constructed.

- **SQL injection** is a *vulnerability*;
- **Sensitive data theft** is (one of) the cyber threats SQL injection enables;
- **Financially motivated attackers** are (one of) the *threat actors*;
- The *impact* of sensitive data getting stolen will bear a **significant financial cost** (financial and reputational loss) to the business;.

Q.1.(b) Describe the major security challenges in laptop and mobile devices. (4)

Ans. Refer Q.1.(E). End Term Paper Dec-2016 (page no. – 8-2016).

Q.1.(c) What are the various ethical issue framework in information security?

Ans. Information system Ethics (3)

Ethics refers to rules of right and wrong that people use to make choices to guide their behaviors. Ethics in MIS seek to protect and safeguard individuals and society by using information systems responsibly. Most professions usually have defined a code of ethics or code of conduct guidelines that all professionals affiliated with the profession must adhere to.

The medical and legal fields, however, the information technology field in general, and the information security field in particular, do not have a binding code of ethics. Instead, professional associations—such as the Association for Computing Machinery (ACM) and the Information Systems Security Association—and certification agencies—such as the International Information Systems Security Certification Consortium, Inc., or (ISC)2 —work to establish the profession's ethical codes of conduct.

Ethical Decision Evaluation

1. A student found a loophole in the university computer's security system that allowed him access to other students' records. He told the system administrator about the loophole, but continued to access others' records until the problem was corrected two weeks later. The student's action in searching for the loophole was: The student's action in continuing to access others' records for two weeks was: The system administrator's failure to correct the problem sooner was:

2. A computer user called a mail-order software company to order a particular accounting system. When he received his order, he found that the store had accidentally sent him a very expensive word-processing program as well as the accounting package that he had ordered. The invoice listed only the accounting package. The user decided to keep the word-processing package. The user's decision to keep the word-processing package was:

3. A programmer at a bank realized that he had accidentally overdrawn his checking account. He made a small adjustment in the bank's accounting system so that his account would not have the additional service charge assessed. As soon as he deposited funds that made his balance positive again, he corrected the bank's accounting system.

Q.1.(d) What is VPN and major security concerns in VPN? (4)

Ans. A VPN or **Virtual Private Network** is a method used to add security and privacy to private and public networks, like WiFi Hotspots and the Internet. **VPNs** are most often used by corporations to protect sensitive data.

Security concerns in VPN:

Hacking Attack: These can include VPN hijacking or man-in-the-middle attacks.

VPN hijacking is the unauthorised take-over of an established VPN connection from a remote client, and impersonating that client on the connecting network.

User Authentication: By default VPN does not provide / enforce strong user authentication. A VPN connection should only be established by an authenticated user. If the authentication is not strong enough to restrict unauthorised access, an unauthorised party could access the connected network and its resources.

Client Side Risks: The VPN client machines of, say, home users may be connected to the Internet via a standard broadband connection while at the same time holding a VPN connection to a private network, using split tunnelling. This may pose a risk to the private network being connected to.

Incorrect network Access Rights: Some client and/or connecting networks may have been granted more access rights than is actually needed.

Interoperability : Interoperability is also a concern. For example, IPsec compliant software from two different vendors may not always be able to work together.

Q.1.(e) Explain the following attacks: Pharming, packet-spoofing, and zombie attack. (4)

Ans. Pharming: Pharming refers to redirecting website traffic through hacking, whereby the hacker implements tools that redirect a search to a fake website. Pharming may cause users to find themselves on an illegitimate website without realizing they have been redirected to an impostor site, which may look exactly like the real site.

Pharming occurs when hackers locate vulnerabilities in domain name server (DNS) software. Pharming can also occur by rearranging the host's file on the targeted computer. Online banking websites as well as e-commerce organizations have become popular pharming targets. Pharming and phishing threats have been used simultaneously and these can cause the most potential for online identity theft.

Routers have been surfacing as being just as vulnerable to pharming as hosts files. Unfortunately, router pharming is much more difficult to detect. Harmful DNS information can land on routers in two ways:

1. Existing administrator settings can be incorrectly configured
2. Entire rewrites of embedded software (also known as firmware) can occur

Routers give administrators the option to choose a trusted DNS as opposed to a suggested one.

Packet spoofing:

- Packet spoofing or IP spoofing is the creation of Internet Protocol (IP) packets having a source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system.
- A spoofing attack is when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts, steal data, spread malware, or bypass access controls.
- The attacker creates a IP packet and sends to the server which is known as SYN request. The difference in the IP packet and normal packet is that the attacker puts the own source address as another computers IP address in the newly created IP packet. The server responds back with a SYN ACK response which travels to the forged IP address. The attacker somehow gets this SYN ACK response sent by the server and acknowledges it so as to complete a connection with the server.
- The most common methods include IP address spoofing attacks, ARP spoofing attacks, and DNS server spoofing attacks.

Zombie Attack: A zombie computer virus is a computer that's been infected by a computer virus or compromised by a hacker. It can be controlled under remote direction to perform criminal tasks, as well as infect other computers with viruses. A zombie computer can appear to be performing normally, making it hard for you to know that your computer has been compromised.

Types of attacks perpetrated by a zombie network include denial of service attacks, adware, spyware, spam and click fraud.

The following steps, or a variation, are used to create zombie networks:

- A zombie network operator uses a bot to infect thousands of computers with worms or viruses that carry a deadly payload.
- The bot inside an infected computer logs on to an online server - usually IRC but sometimes Web.
- The zombie network operator leases zombie network services to a customer.

Q.1.(f) What is media forensics? How ethical hacking different from craking? (4)

Ans. Cyber **forensics** is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

Ethical hacking: Ethical hacking is also done by hackers but they are done legally. Ethical hackers are used to check the software security. They try to find out the mistakes done by a software developer mainly in security section of networking, websites and software. Ethical hackers check and test is there any ways to break in the software developed. They are used to develop the security system. Ethical hackers are popularly called as White hats. They are the persons who protect us from black hats.

Example: 1 . If we lost our door key we call locksmith to open the door. Locksmith is ethical hacker.

2. Technically, if we lost our Gmail password we request to Gmail technicians who access our passwords through ethical hacking. They help us to recover our password.

Ethical hacking is a certified course. Anyone can study ethical hacking. This is legal activity accepted by every organization. Leaning ethical hacking is not so easy because every time a security system is improved by white hats they are destroyed by blackhats.

Cracking: From the name you can understand that it is cracking or breaking software. Cracking is editing the existing source code. Crackers usually remove or adding irrelevant information as per their wish. They don't have much knowledge like hackers. They are not expert programmers. They edit the stuff done by programmers. It is done for protection purpose. Some codes have been edited by the program developer in order to keep protected.

Example: Consider a main source code is

Ky=12345

They may edit as

Key = ----- (Source Code removed)

Or

Key = 83639 (Irrelevant source code)

One can access the software only if the code is known. So this remains protected. Cracking is done only to software or hardware components. It is not applicable to networking. Cracking is done both legally and illegally. If it is done by authorized person it is legal if not it is illegal.

Example: 1. In some games you may play only 3 levels out of 50 levels it is due to the game source code is cracked. This technique is used in demo games.

2. You may find some software remains active for only few days after that you cannot use that software because after that it automatically cracks. This technique is used in trial software.

Q.1.(g) Justify with a real time example how authentication can be achived in banking sector. **(3)**

Ans. Authentication

• Authentication is used by a server when the server needs to know exactly who is accessing their information or site.

• Authentication is used by a client when the client needs to know that the server is system it claims to be.

• In authentication, the user or computer has to prove its identity to the server or client.

• Usually, authentication by a server entails the use of a user name and password. Other ways to authenticate can be through cards, retina scans, voice recognition, and fingerprints.

Our innovative authentication (including face recognition), mobile app security and real-time fraud prevention solutions are designed to increase the trust level across all areas of mobile banking – user, device and application – so you can eliminate threats to your mobile banking platform.

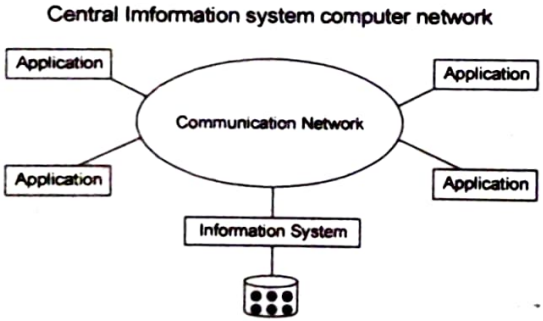
VASCO solutions also support Federal Financial Institution Examination Council (FFIEC) guidance in Mobile Financial Services (MFS) including:

Authentication and authorization. Financial institutions should use mobile payment applications that rely exclusively on two-factor or multifactor authentication.

Authentication should be used whenever you want to know exactly who is using or viewing your site. Weblogin is Boston University's primary method of authentication. Other commercial websites such as Amazon.com require people to login before buying products so they know exactly who their purchasers are.

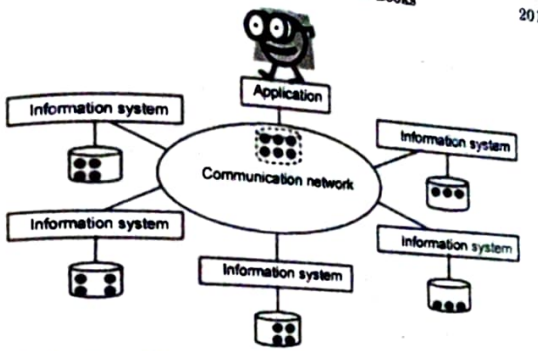
Q.2.(a) Explain Distributed information System & it's importance. **(6)**

Ans. Distributed Information Systems:



Except in the very early days, information systems had always been used in computer networks. This does not imply any fundamental problems in addition to those we have discussed up to now as long as the information system is centralized, i.e. running on one node under a single authority.

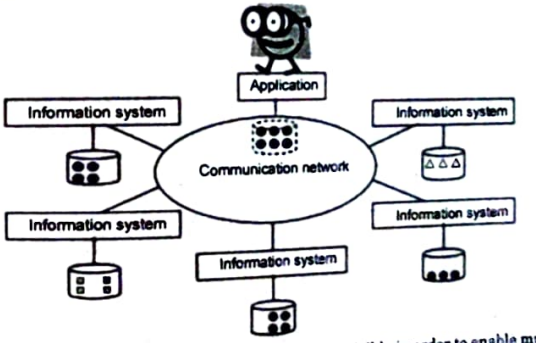
Physical Distribution: Distribution of data – support use of distributed physical resources: improve locality of access, scalability, parallelism in the execution



Nevertheless we don't want to give up the abstraction that we are still accessing a single information system that is running under a single authority.

Logical Distribution: Communication Network Information System Information System Information System Information System Information System Application

• Distribution of knowledge – enable interoperability of (pre-existing) information systems – support different interpretations of the same data for different needs and capabilities



In fact, we might want to make the distribution visible in order to enable multiple authorities to infuse their knowledge into their network, in order to make information systems that where formerly separated working together, and in order to make different interpretations of data available. Thus we are considering distribution of knowledge. In order to make use of such a logically distributed information system we need to support the application/user in order to overcome some of the problems related to logical distribution, without necessarily making the fact that the data is logically distributed completely transparent.

Importance of Distributed System :

• **Sharing Data :** There is a provision in the environment where user at one site may be able to access the data residing at other sites.

• **Autonomy** : Because of sharing data by means of data distribution each site is able to retain a degree of control over data that are stored locally.

• In distributed system there is a global database administrator responsible for the entire system. A part of global data base administrator responsibilities is delegated to local data base administrator for each site. Depending upon the design of distributed database

• Each local database administrator may have different degree of local autonomy.

• **Availability :** If one site fails in a distributed system, the remaining sites may be able to continue operating. Thus a failure of a site doesn't necessarily imply the shutdown of the System.

Q.2.(b) Explain the types of attacks and clasification of threat in detail. (6.5)

Ans. In order for one to produce a secure system, it is important to classify threats. The classification of threats could be:

(*a*) **Physical Threat:** Physical threat to a computer system could be as a result of loss of the whole computer system, damage of hardware, damage to the computer software, theft of the computer system, vandalism, natural disaster such as flood, fire, war, earthquakes etc. Acts of terrorism such as the attack on the world trade centre is also one of the major threats to computer which can be classified as physical threat.

Another good example of a physical threat to computer system is the flooding of the city of New Orleans (Hurricane Katrina) during which valuable information was lost and billions of computer data were destroyed.

(*b*) **Accidental error:** This is also an important security issue which computer security experts should always put into consideration when designing security measures for a system. Accidental errors could occur at any time in a computer system but having proper checks in place should be the major concern of the designer. Accidental error includes corruption of data caused by programming error, user or operator error.

(*c*) **Unauthorized access:** Dada stored on the computer system has to be accessed for it to be translated into useful information. This also poses a great security threats to the computer system due to unauthorized person's having access to the system. Not only this, information can be accessed via a remote system in the process of being transmitted from one point to the other via network media which includes wired and wireless media. Considering an example of an organization in which a member of staff at a particular level of hierarchy within the establishment is only allowed access to specific area according to the policy of the organization. If this employee by other means not set in the organization policy gain access to the restricted data area on the computer, this can be termed an un authorized access.

(*d*) **Malicious misuse:** Any form of tampering of the computer system which includes penetration, Trojan horses' viruses and any form of illegal alteration of the computer system which also includes the generation of illegal codes to alter the standard codes within the system can be termed as malicious misuse. This could also lead to a great financial loss and should be prevented in all cases.

Refer Q.5. End Term Paper dec-2016 [page no - 14-2016]

Q.3. How biometric system help in securing the information? What are the various criteria's biometric selection and also explain, how the design issues in biometric systems can be handled taking a case study of any biometric system you have used? (12.5)

Ans. Refer Q.3. End Term Paper dec-2016 page no - 10-2016.

Q.4. What is EDI and list the benefits which EDI offers to a business organization? Explain the various components of EDI. How electronic payment system is more beneficial in comparison to traditional payment system? (12.5)

Ans. To make EDI happen, four elements of infrastructure must exist:

(1) format standards are required to facilitate automated processing by all users;

(2) translation software is required to translate from a user's proprietary format for internal data storage into the generic external format and back again;

(3) value-added networks are very helpful in solving the technical problems of sending information between computers; and

(4) inexpensive microcomputers are required to bring all potential users—even small ones-into the market. It has only been in the past several years that all of these ingredients have fallen into place.

Electronic data interchange (EDI) is the electronic transmission of structured data by agreed message standards from one computer system to another without human intervention. It is a system for exchanging business documents with external entities.

EDI refers to a family of standards and does not specify transmission methods, which are freely agreed upon by the trading partners.

The wide adoption of EDI in the business world facilitates efficiency and cost reduction. EDI is used in such diverse business-to-business relationships as:

- Interchanges between health care providers and insurers
- Travel and hotel bookings
- Education
- Supply chain management
- Administration
- Tax reporting

BENEFITS OF EDI:

- There have many benefits of electronic data interchange such as:
- **SPEED** – Data can move directly out of one computer system and into another with little to no delay.
- **ACCURACY** – Errors are reduced because data is not being re-keyed. Error rates from entering data are between .5 – 3%. On large volumes of transactions, the possibility for the introduction of errors is enormous.
- **SIMPLICITY** – EDI standards specify how data will be formatted and where it can be found.
- **SECURITY** – Much less likely to lose information transmitted through EDI than information sent via mail. EDI can be accessed only by authorized users, and then there are audit trails and archives of data. EDI data cannot be easily changed by unauthorized users. It is also not subject to viruses.

Electronic payment system is more beneficial in comparison to traditional payment system :

Electronic payment systems have a range of pros in comparison to traditional banking services:

1. **Time savings**. Money transfer between virtual accounts usually takes a few minutes, while a wire transfer or a postal one may take several days. Also, you will not waste your time waiting in lines at a bank or post office.

2. **Expenses control**. Even if someone is eager to bring his disbursements under control, it is necessary to be patient enough to write down all the petty expenses, which often takes a large part of the total amount of disbursements. The virtual account contains the history of all transactions indicating the store and the amount you spent

3. **Reduced risk of loss and theft**. You can not forget your virtual wallet somewhere and it can not be taken away by robbers

4. **Low commissions**. If you pay for internet service provider or a mobile account replenishment through the UPT (unattended payment terminal), you will encounter high fees. As for the electronic payment system: a fee of this kind of operations consists of 1% of the total amount, and this is a considerable advantage.

5. **User-friendly**. Usually every service is designed to reach the widest possible audience, so it has the intuitively understandable user interface. In addition, there is always the opportunity to submit a question to a support team, which often works 24/7.

Q.5. What is VPN? List the various protocols of VPN? Also explain in detail, the working of VPN for exchanging information between two private networks with the help of a diagram. **(12.5)**

Ans. A **virtual private network** (VPN) extends a private network across a public network or internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

VPNs can provide functionality, security and/or network management benefits to the user. But they can also lead to new issues, and some VPN services, especially "free" ones, can actually violate their users' privacy by logging their usage and making it available without their consent, or make money by selling the user's bandwidth to other users.

Some VPNs allow employees to securely access a corporate intranet while located outside the office. Some can securely connect geographically separated offices of an organization, creating one cohesive network. Individual Internet users can use some VPNs to secure their wireless transactions, to circumvent geo-restrictions and censorship, and/or to connect to proxy servers for the purpose of protecting personal identity and location. But some Internet sites block access via known VPNs to prevent the circumvention of their geo-restrictions.

A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN). From a user perspective, the resources available within the private network can be accessed remotely.

VPNs cannot make online connections completely anonymous, but they can usually increase privacy and security. To prevent disclosure of private information, VPNs typically allow only authenticated remote access using tunneling and encryption techniques.

The VPN security model provides:

• Confidentiality such that even if the network traffic is sniffed at the packet level (see network sniffer and Deep packet inspection), an attacker would only see encrypted data

• Sender authentication to prevent unauthorized users from accessing the VPN

• Message integrity to detect any instances of tampering with transmitted messages

The most commonly used tunnelling protocols are IPsec, L2TP, PPTPand SSL. A packet with a private non-routable IP address can be sent inside a packet with globally unique IP address, thereby extending a private network over the Internet. VPN uses encryption to provide data confidentiality.

Types of VPN protocols

1. PPTP VPN: This is the most common and widely used VPN protocol. They enable authorized remote users to connect to the VPN network using their existing Internet connection and then log on to the VPN using password authentication. They don't need extra hardware and the features are often available as inexpensive add-on software. PPTP stands for Point-to-Point Tunneling Protocol. The disadvantage of PPTP is that it does not provide encryption and it relies on the PPP (Point-to-Point Protocol) to implement security measures.

2. Site-to-Site VPN: Site-to-site is much the same thing as PPTP except there is no "dedicated" line in use. It allows different sites of the same organization, each with its own real network, to connect together to form a VPN. Unlike PPTP, the routing, encryption and decryption is done by the routers on both ends, which could be hardware-based or software-based.

3. L2TP VPN: L2TP or Layer to Tunneling Protocol is similar to PPTP, since it also doesn't provide encryption and it relies on PPP protocol to do this. The difference between PPTP and L2TP is that the latter provides not only data confidentiality but also data integrity. L2TP was developed by Microsoft and Cisco.

4. IPsec: Tried and trusted protocol which sets up a tunnel from the remote site into your central site. As the name suggests, it's designed for IP traffic. IPSec requires expensive, time consuming client installations and this can be considered an important disadvantage.

5. SSL: SSL or Secure Socket Layer is a VPN accessible via https over web browser. SSL creates a secure session from your PC browser to the application server you're accessing. The major advantage of SSL is that it doesn't need any software installed because it uses the web browser as the client application.

6. MPLS VPN: MPLS (Multi-Protocol Label Switching) are no good for remote access for individual users, but for site-to-site connectivity, they're the most flexible and scalable option. These systems are essentially ISP-tuned VPNs, where two or more sites are connected to form a VPN using the same ISP. An MPLS network isn't as easy to set up or add to as the others, and hence bound to be more expensive.

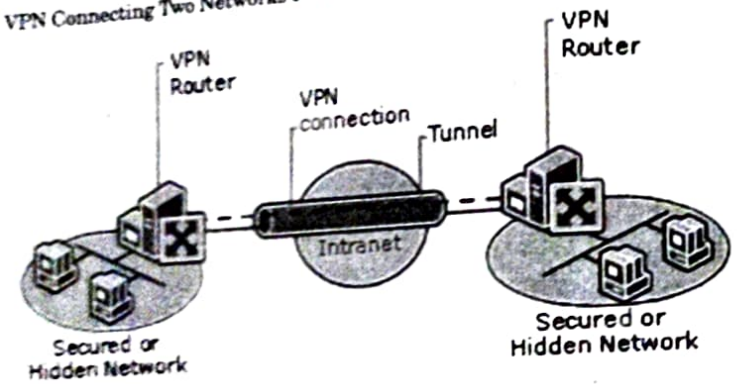
7. Hybrid VPN: A few companies have managed to combine features of SSL and IPSec & also other types of VPN types. Hybrid VPN servers are able to accept connections from multiple types of VPN clients. They offer higher flexibility at both clienbt and server levels and bound to be expensive.

Working of VPN:

VPNs help enable users working at home, on the road, or at a branch office to connect in a secure fashion to a remote corporate server using the Internet. From the user's perspective, the VPN is a point-to-point connection between the user's computer and a corporate server. The nature of the intermediate network, the Internet, is irrelevant to the user because it appears as if the data is being sent over a dedicated private link.

There are a number of ways to use VPN. The most common scenario is when a remote user accesses a private network across the Internet using a remote access VPN connection. In another scenario, a remote office connects to the corporate network using either a persistent or an on-demand site-to-site VPN connection (also known as a router-to-router VPN connection).

VPN Connecting Two Networks over an Intranet



VPN Tunneling

Tunneling is a network technology that enables the encapsulation of one type of protocol packet within the datagram of a different protocol. For example, Windows VPN connections can use Point-to-Point Tunneling Protocol (PPTP) packets to encapsulate and send private network traffic, such as TCP/IP traffic over a public network such as the Internet.

For PPTP and Layer Two Tunneling Protocol (L2TP), a tunnel is similar to a session. Both of the tunnel endpoints must agree to the tunnel and must negotiate configuration variables, such as address assignment, encryption, or compression parameters. In most cases, data transferred across the tunnel is sent using a datagram-based protocol. A tunnel management protocol is used as the mechanism to create, maintain, and terminate the tunnel.

After the tunnel is established, data can be sent. The tunnel client or server uses a tunnel data transfer protocol to prepare the data for transfer. For example, when the tunnel client sends a payload to the tunnel server, the tunnel client first appends a tunnel data transfer protocol header to the payload. The client then sends the resulting encapsulated payload across the network, which routes it to the tunnel server. The tunnel server accepts the packets, removes the tunnel data transfer protocol header, and forwards the payload to the target network. Information sent between the tunnel server and the tunnel client behaves similarly.

There are two types of tunneling:

- Voluntary tunneling
- Compulsory tunneling

Voluntary Tunneling

A user or client computer can issue a VPN request to configure and create a voluntary tunnel. In this case, the users computer is a tunnel endpoint and acts as the tunnel client.

Voluntary tunneling occurs when a client computer or routing server creates a virtual connection to the target tunnel server. To accomplish this, tunneling client software and the appropriate tunneling protocol must be installed on the client computer. For the protocols discussed in this technical reference, voluntary tunnels require an IP connection (either LAN or dial-up).

In a dial-up situation, the client must establish a dial-up connection to the network before the client can set up a tunnel. This is the most common case. The best example of this is the dial-up Internet user, who must dial an ISP and obtain an Internet connection before a tunnel over the Internet can be created.

For a LAN-attached client computer, there is already a connection to the network that can provide routing of encapsulated payloads to the chosen LAN tunnel server. This would be the case for a client that is using an always-on broadband Internet connection.

Compulsory Tunneling

In compulsory tunneling, a VPN-capable remote access server configures and creates a compulsory tunnel. With a compulsory tunnel, the user's computer is not a tunnel endpoint. Another device, the dial-up access server, between the user's computer and the tunnel server is the tunnel endpoint and acts as the tunnel client.

A number of vendors that sell dial-up access servers have implemented the ability to create a tunnel on behalf of a dial-up client. The computer or network device providing the tunnel for the client computer is variously known as a Front End Processor (FEP) for PPTP or an L2TP Access Concentrator (LAC) for L2TP. For the purposes of this reference, the term FEP is used to describe this functionality, regardless of the tunneling protocol. To carry out its function, the FEP must have the appropriate tunneling protocol installed and must be capable of establishing the tunnel when the client computer connects.

Q.6. Compare and contrast between IDS (Intrusion Detection System.) and IPS (Intrusion prevention System). What are the various intrusion detection methodologies? Also explain any three types of threats. (12.5)

Ans. Refer Q.2 (b) End Term Examination 2017.

IDS – as stated, it is a tool to detect intrusion of packets and determine which of the packets can be threat or not. It is only to detect not to block. It is a combined tool of hardware and software security system that deals with internal and external attacks and monitors network activity in real-time.

There are two types of IDS:

Host-Based Intrusion Detection System (HIDS)

- This is a Host-2based Sensor that needs software application as agents installed on workstations. HIDS are the ones who monitored these agents. The agents monitor activities and logs files of a certain operating system where the agents are installed

• Uses logs of activities and determines whether an attack actually occurred. They give more accurate detection of an attack.

• If there is any untoward change of activity and starts the job right away after installation the monitoring of activities is used . They can monitor attack based on the changes of activities of the internal system

• Sensors are installed at the host only thus it doesn't need any additional hardware

• The cost is lower

Network-Based Intrusion Detection System

• They are Network-based Sensor (Ethernet or WIFI), which are places in segment points or boundaries and monitors data packets that go through and from the system

• This system does not affect existing system and independent so it's much easier to deploy

• They can detect attacks that travels the network by the packets' content at real-time

• They use real-time monitoring so attackers can no longer hide, make changes or remove the evidence that's why evidence of an attack is retained. These are very useful in forensic study.

• The system can also detect at real-time and can have a quick response over an attack because they are deployed in the network

• Even the failed attacks can also be detected

IPS – this tool can make action and does not need administrators' decision to make actions to prevent any packet of data that the IPS tool detects as a threat. IPS are also placed to actively analyse and take actions automatically to all packets that enter the network.

They can:

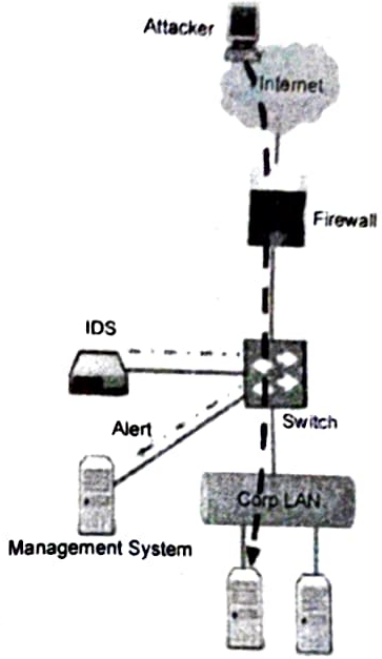
- Send an alarm
- Drop malicious packets
- Can block packets from the source address
- Reset connection
- Does not require human intervention to take an action

Two Detection Methods of IPS

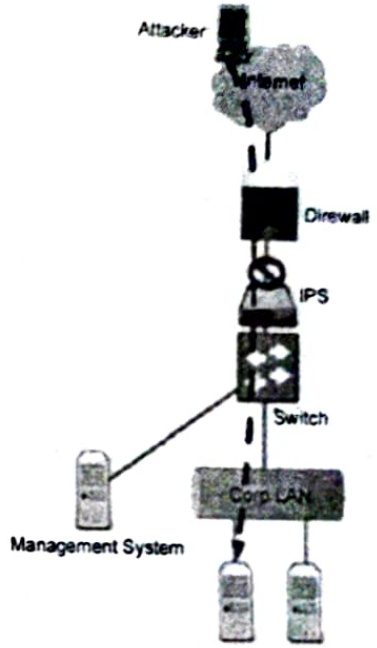
Signature –Based detection (or Misuse Detection). This method uses significant identifiable patterns each kind of attacks. The signature can be *Exploit-facing signature*where they monitor packets by finding a match from their stored file of exploit attacks. There is also *Vulnerability-facing signature* where they recognize an attack as to which part of the system is vulnerable to this kind of attack.

Statistical Anomaly Detection. They use samples of network traffic at random and compares them with each other. They use bandwidth, protocols used, ports, and devices that connect each other.

Intrusion Detection System



Intrusion Prevention System



Intrusion Detection Methodologies:

Anomaly-based intrusion detection techniques

Also called behavior-based, these solutions track activity within the specific scope (see above) looking for instances of malicious behavior — at least, as they define it, which is a difficult job, and sometimes leads to false positives. For instance, outbound URLs of Web activity might be considered, and sites involving certain domains or URL length/contents might automatically be blocked, even though it's a human being trying to go there (not malware), and that user has a business-legitimate reason.

Signature-based intrusion detection techniques

This approach, also known as knowledge-based, involves looking for specific signatures — byte combinations — that when they occur, almost invariably imply bad news. Read: malware itself, or packets sent by malware in the attempt to create or leverage a security breach. These solutions generate fewer false positives than anomaly solutions because the search criteria is so specific, but they also only cover signatures that are already in the search database (which means truly novel attacks have good odds of success).

Q.7. Distinguish between Symmetric and Asymmetric key cryptography.

Which type of crytography is more secure and why? Explain the Diffre-Hellman key Exchange algorithm for symmetric key cryptography. **(12.5)**

Ans.

Comparison Factor	Symmetric Key Cryptography	Asymmetric key Cryptography
Number of Cryptographic Keys	Symmetric encryption incorporates only one key for encryption as well as decryption.	Asymmetric Encryption consists of two cryptographic keys. These keys are regarded as Public Key and Private Key.
Complexity	Symmetric encryption is a simple technique compared to asymmetric encryption as only one key is employed to carry out both the operations.	Contribution from separate keys for encryption and decryption makes it a rather complex process.
Swiftness of Execution	Due to its simplistic nature, both the operations can be carried out pretty quickly.	Because of encryption and decryption by two separate keys and the process of comparing them make it a tad slow procedure.
Algorithms Employed	RC4 AES. DES. 3DES QUAD	RSA Diffie-Hellman ECC E1 Gamal DSA

Asymmetric Encryption is better (more secure) than Symmetric Encryption. A typical statement is something like this:

Generally asymmetric encryption schemes are more secure because they require both a public and a private key.

Certainly with symmetric encryption you have to worry about secure key exchange but as far as I can tell there's no inherent reason why one must be more secure than the other.

Especially given that the asymmetric part is often just used for the key exchange and then the actual data is encrypted with a symmetric algorithm.

Diffie-Hellman algorithm

The Diffie-Hellman algorithm is being used to establish a shared secret that can be used for secret communications while exchanging data over a public network using the elliptic curve to generate points and get the secret key using the parameters.

- For the sake of simplicity and practical implementation of the algorithm, we will consider only 4 variables one prime P and G (a primitive root of P) and two private values a and b.
- P and G are both publicly available numbers. Users (say Alice and Bob) pick private values a and b and they generate a key and exchange it publicly, the opposite person received the key and from that generates a secret key after which they have the same secret key to encrypt.

Step by step Explanation

ALICE	BOB
Public Keys available = P,G	Public Keys available = P,G
Private Key Selected = a	Private Key Selected = b
Key generated = $x = G^a \bmod P$	Key generate = $x = G^b \bmod P$
Exchange of generated keys takes piace	
key received = y	Key received = x
Generated secret key = $Ka = y^a \bmod P$	Generated secret key = $K^b = x^b \bmod P$

Algebraically it can be shown that $k_a = k_b$

Users now have a symmetric key to encryct

Example

Step 1: Alice and Bob get public numbers P = 23, G = 9

Step 2: Alice selected a private key a = 4 and
Bob selected a private key b = 3

Step 3: Alice and Bob compute public values
Alice: x =(9^4 mod 23) = (6561 mod 23) = 6
Bob: y = (9^3 mod 23) = (729 mod 23) = 16

Step 4: Alice and Bob exchange public numbers

Step 5: Alice receives public key y =16 and
Bob receives public key x = 6

Step 6: Alice and Bob compute symmetric keys
Alice: ka = y^a mod p = 65536 mod 23 = 9
Bob: kb = x^b mod p = 216 mod 23 = 9

Step 7: 9 is the shared secret.

Q.8. Write a short note on the following:

(a) Business Transaction on Web. (6)

Ans. Although most forms of online payment are relatively secure, there is always the potential for problems. Without taking the necessary precautions, your customers' payment information can be compromised and complications can ensue. Here are some options that can keep both you and your customers safe.

1. PCI Compliance: Payment Card Industry (PCI) compliant. The Payment Card Industry Security Standards Council was formed in 2006 to regulate major payment brands and help merchants keep their customers' financial data safe. It's their prerogative to maximize information security by implementing 12 security requirements.

2. Data Encryption: Another way to enhance security is to utilize encryption technology to make sure private financial information remains private. This technology confirms that the websites your business uses for transactions are part of valid organizations and have legitimate operators. It minimizes the risk of sensitive information viewed by the wrong parties. It also greatly reduces the chances of hackers cracking passwords.

3. Safe Login Screen: When customers sign in to access their accounts, it's critical the login system is as secure as possible. Otherwise, you can make it dangerously easy for hackers to infiltrate and gain access to sensitive information. In the event that a customer forgets his password, he should be required to enter a user name or email address to retrieve it. The system will then send him an email where he can temporarily log in or create a new password.

5. Security Assessment: Finally, a thorough assessment of your payment system from a company like Security Metricsshould tie up any loose ends. This company is somewhat similar to the analysis that the PCI will perform but is a bit more exhaustive in their approach. One feature they offer involves implementing ethical hacking, in which penetration test analysts inspect your network much like a hacker would. They do this manually and look for flaws that could potentially be exploited. Afterward, they will go over their findings and provide consultation to heighten security.

6. Look beyond SSL: Even though secure socket layers ensure safe and encrypted flow of information between a browser and a server, it is not the be all and end all of securing the web applications. A website may claim to be secure as they use 128 or 256 bit encryption and may even boast of a seal from an external certificate authority.

But what the online retailers fail to understand is the fact that SSL cannot protect against application layer attacks. Businesses need to deploy solutions that can provide a multi-layer protection.

Q.8.(b) Legal challenges framework for Information Security. (6.5)

Ans. There are various legal challenges framework for information security that are neede to improved. The existing legal framework needs to be improved in. these matters:

- **Legislation** - adopting relevant laws, setting out standards and areas of Information Security, as well as functions of some institutions
- **Institutions** - responsible for tasks relating to verification and certification methods, software application, devices and systems, R&D and oversight of the IS standards implementation by state authorities
- **National CERT** - Computer Emergency Response Team.

FIRST TERM EXAMINATION [SEP. 2018]
SEVENTH SEMESTER [B.TECH]
INFORMATION SECURITY [ETCS–401]

Time : 1½ hrs. **M.M. : 30**

Note: *Q. No. 1 is compulsory. Attempt any two more Questions from the rest.*

Q. 1. (a) What do you mean by Computer crime? Point out four basic sources of security threats? (2)

Ans. Refer to Q. 1. (a) First Term Sept 2016.

Q. 1.(b) What are the security attacks related to computer crime. (2)

Ans. Refer to Q. 1. (b) First Term Sept 2016.

Q. 1.(c) Why information is so important for individual or organization. (2)

Ans. Refer to Q. 1. (c) First Term Sept 2016.

Q. 1.(d) Explain the meaning of Computer based IS. (2)

Ans. Refer to Q. 1. (d) First Term Sept 2016.

Q. 1.(e) Explain the need of distributed IS in current scenario. (2)

Ans. Refer to Q. 1. (e) First Term Sept 2016.

Q. 2. Write short notes on any two

(i) LDAP Server (ii) Authentication Service Security (iii) Pull and push as attack on mobile devices (10)

Ans. Refer to Q. 2. First Term Sept 2016.

Q. 3. Define and differentiate between. (Any 4) (10)

(i) EFT and EDI

(ii) VO and VPN

(iii) IPv4 and IPv6

(iv) Attacks and Threats

(v) 1 tier and 2 tier architecture of IS.

Ans. (i) Refer to Q.3. (i) First Term Sept 2016.

(ii) Refer to Q. 3. (ii) First Term Sept 2016.

(iii) Refer to Q. 3. (iii) First Term Sept 2016.

(iv) Refer to Q. 3. (iv) First Term Sept 2016.

(v) Refer to Q. 3. (vi) First Term Sept 2016.

Q. 4. What are the three pillars of security? Define the following terms:

(i) Access control (ii) Denial-of-Service (iii) Non-repudation (iv) Spoofing. (10)

Ans. Refer to Q. 4. First Term Sept 2016.

END TERM EXAMINATION [NOV. DEC. 2018]
SEVENTH SEMESTER [B.TECH]
INFORMATION SECURITY [ETCS–401]

Time : 3 hrs. **M.M. : 76**

Note: *Attempt five questions in all including Q. No. 1 which is compulsory. Select one question from each unit.*

Q. 1. (a) Describe the main principles of information security. **(2.5)**

Ans. A principle which is a core requirement of **information security** for the safe utilization, flow, and storage of **information** is the CIA triad. CIA stands for confidentiality, integrity, and availability and these are the three **main** objectives of **information security**.

- **Confidentiality:** This means that information is only being seen or used by people who are authorized to access it.
- **Integrity:** This means that any changes to the information by an unauthorized user are impossible (or at least detected), and changes by authorized users are tracked.
- **Availability:** This means that the information is accessible when authorized users need it.

Q. 1. (b) What is SET? How SET makes our transactions secure. **(2.5)**

Ans. Secure Electronic Transaction (SET) is a system for ensuring the security of financial transactions on the Internet. It uses different encryption and hashing techniques to secure payments over internet done through credit cards. It was supported initially by Mastercard, Visa, Microsoft, Netscape, and others. With SET, a user is given an electronic wallet (digital certificate) and a transaction is conducted and verified using a combination of digital certificates and digital signatures among the purchaser, a merchant, and the purchaser's bank in a way that ensures privacy and confidentiality. SET makes use of Netscape's Secure Sockets Layer (SSL), Microsoft's Secure Transaction Technology (STT), and Terisa System's Secure Hypertext Transfer Protocol (S-HTTP). SET uses some but not all aspects of a public key infrastructure (PKI).

Q. 1. (c) Differentiate among Worms, Viruses and Trojan Horses. **(2.5)**

Ans. Worms: Worms are programs that replicate themselves from system to system without the use of a host file. Worms generally exist inside of other files, often Word or Excel documents. Usually the worm will release a document that already has the "worm" macro inside the document. The entire document will travel from computer to computer, so the entire document should be considered the worm. PrettyPark. Worm is a particularly prevalent example.

Virus: A computer virus is a small program written to alter the way a computer operates, without the permission or knowledge of the user. A virus must meet two criteria:

- It must execute itself. It will often place its own code in the path of execution of another program.
- It must replicate itself. For example, it may replace other executable files with a copy of the virus infected file. Viruses can infect desktop computers and network servers alike.

Some viruses are programmed to damage the computer by damaging programs, deleting files, or reformatting the hard disk. Others are not designed to do any damage, but simply to replicate themselves and make their presence known by presenting text, video, and audio messages.

Trojan Horses: Trojan horses are impostors—files that claim to be something desirable but, in fact, are malicious. It is a harmful piece of software that looks legitimate. After it is activated, it can achieve any number of attacks on the host, from irritating the user to damaging the host. Trojans are also known to create backdoors to give malicious users access to the system. Trojans do not reproduce by infecting other files nor do they self-replicate. Trojans must spread through user interaction such as opening an email attachment or downloading and running a file from the Internet.

Q. 1. (d) Differentiate between data security and privacy. **(2.5)**

Ans.

Security Versus Privacy

(i)	Security refers to protection against unauthorized access.	Privacy defines the ability to protect personally identifiable information.
(ii)	Security provides protection for all types of data and information including the ones that are stored electronically.	Privacy means protecting sensitive information related to individuals and organizations.
(iii)	Security can be achieved without privacy.	Privacy cannot be achieved without security.
(iv)	Security program focuses on all sorts of information assets that an organization collects.	Privacy program focuses on personal information such as names, addresses, social security numbers, log in credentials, financial accounts information, etc.
(v)	It implements security protocols to provide confidentiality, integrity and availability of information assets.	It refers to protection of privacy right with respect to processing of personal data.

Q. 1. (e) List the four elements of an EDI. **(2.5)**

Ans. Four Elements of EDI:

Standard Document Format– A standard format agree upon by both parties which do not require complicated hardware or software to access information. Both parties communicate directly through a business application.

Translator and mapper– A translator is used to convert the raw data into meaningful information according to specifications provided by a mapper. A mapper is used to create conversion specification. It compiles the specification and then gives instructions to the translator on how to convert the data.

Communication software – A communication software is used to transmit data and convert business documents into a standard format. It follows a standard communication protocol which is incorporated in the software.

Communication Network– A communication network provides a direct link between trading partners who are willing to exchange business documents through Electronic Data interchange EDI.

Q. 1. (f) What is digital media forensics? **(2.5)**

Ans. Digital media forensics is not just the art of finding deleted or hidden data; it is also the understanding of the underlying technologies behind the various tools used and the ability to present scientifically valid information.

Q. 1. (g) Enlist various criteria for selection of Biometrics. **(2.5)**

Ans. There are some important factors which should be considered before choosing a biometric modality. These include:

1. Accuracy: It is based on several criteria including error rate, false acceptance rate (FAR), identification rate, false reject rate (FRR) and additional biometric system standards.

2. Anti-spoofing capabilities: As biometric recognition systems become more widespread, more attention has been given to possible direct attacks, where potential intruders may gain access to the system by interacting with the system input device. Such attempts are commonly referred as spoofing protection is a must have capability for the right biometric modality.

3. Acceptability: User acceptance is the linchpin of biometric identification management deployment success. Certain biometric modalities may have a stigma associated with them (e.g. – fingerprint biometrics and criminality) which can negatively impact user perception in certain cultures.

4. Cost effectiveness: Depending on the underlying technology and hardware characteristics, certain modalities may be more cost effective than others. It's important to recognize that an initial investment in biometrics can and is quite often recouped in a short amount of time to achieve fast return on investment (ROI).

5. Hygiene: Contact dependent biometric hardware is an important factor to consider before making an investment. Many new deployments in industries that pay close attention to infection control prefer to use contactless biometric modalities for hygienic reasons.

Q. 1. (h) What are various types of VPNs. **(2.5)**

Ans. VPN stands for Virtual Private Network (VPN), that allows a user to connect to a private network over the Internet securely and privately. VPN creates an encrypted connection that is called VPN tunnel, and all Internet traffic and communication is passed through this secure tunnel. Virtual Private Network (VPN) is basically of 2 types:

Remote Access VPN: Remote Access VPN permits a user to connect to a private network and access all its services and resources remotely. The connection between the user and the private network occurs through the Internet and the connection is secure and private. Remote Access VPN is useful for home users and business users both.

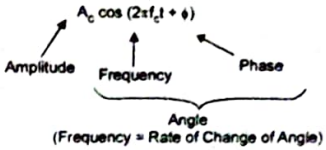
Site to Site VPN: A Site-to-Site VPN is also called as Router-to-Router VPN and is commonly used in the large companies. Site-to-site VPN create a imaginary bridge between the networks at geographically distant offices and connect them through the Internet and sustain a secure and private communication between the networks. In Site-to-site VPN one router acts as a VPN Client and another router as a VPN Server as it is based on Router-to-Router communication. When the authentication is validated between the two routers only then the communication starts.

- **Intranet based VPN:** When several offices of the same company are connected using Site-to-Site VPN type, it is called as Intranet based VPN.
- **Extranet based VPN:** When companies use Site-to-site VPN type to connect to the office of another company, it is called as Extranet based VPN.

Q. 1. (i) Discuss various modulation techniques. **(2.5)**

Ans. The two types of modulation techniques are:

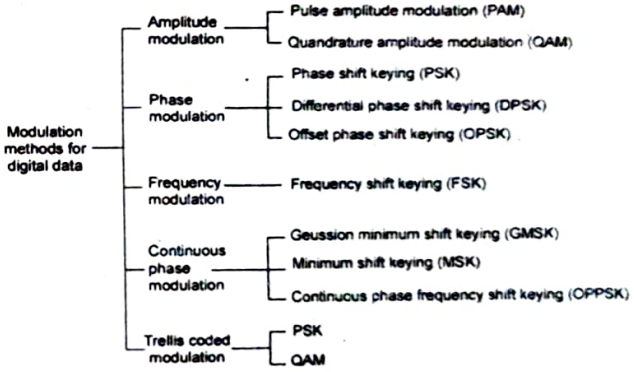
Analog Modulation: In analog modulation, analog signal (sinusoidal signal) is



The types of analog modulation are:

- Amplitude modulation (AM)
- Frequency modulation (FM)
- Phase modulation (PM)

Digital modulation techniques : The main advantages of the digital modulation over analog modulation include permissible power, available bandwidth and high noise immunity. In digital modulation, a message signal is converted from analog to digital message, and then modulated by using a carrier wave. The carrier wave is keyed or switched on and off to create pulses such that the signal is modulated.



Q. 1. (j) Discuss functionality of TCP/IP layers. **(2.5)**

Ans. TCP/IP, or the Transmission Control Protocol/Internet Protocol, is a suite of communication protocols used to interconnect network devices on the internet. TCP/IP can also be used as a communications protocol in a private network. The two main protocols in the internet protocol suite serve specific functions. TCP defines how applications can create channels of communication across a network. It also manages how a message is assembled into smaller packets before they are then transmitted over the internet and reassembled in the right order at the destination address.

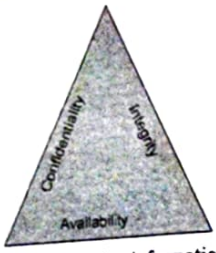
IP defines how to address and route each packet to make sure it reaches the right destination. Each gateway computer on the network checks this IP address to determine where to forward the message.

UNIT-1

Q. 2. (a) Among the fundamental challenges in information security, discuss following. **(2)**

(i) Define each of these terms: confidentiality, integrity, availablity.

Ans. Confidentiality, integrity and availability, also known as the **CIA triad**, is a model designed to guide policies for information security within an organization.



Confidentiality – ensures that sensitive information are accessed only by an authorized person and kept away from those not authorized to possess them. It is implemented using security mechanisms such as usernames, passwords, access control lists (ACLs), and encryption. It is also common for information to be categorized according to the extent of damage that could be done should it fall into unintended hands. A failure of confidentiality, commonly known as a *breach*, typically cannot be remedied. Once the secret has been revealed, there's no way to un-reveal it.

Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle . Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality). These measures include file permissions and user access controls.

Availability – ensures that information and resources are available to those who need them. It is implemented using methods such as hardware maintenance, software patching and network optimization. Processes such as redundancy, failover, RAID and high-availability clusters are used to mitigate serious consequences when hardware issues do occur. Dedicated hardware devices can be used to guard against downtime and unreachable data due to malicious actions such as distributed denial-of-service (DDoS) attacks.

Q. 2. (ii) Give a concrete example where confidentiality is more important than integrity. **(2)**

Ans. Consider a website in which a user can request information about routes between two places(maps) or news regarding a particular topic or region. Suppose this system requires the user to make a profile and saves access logs for each user and his/her request for a particular session. If these logs are compromised, then an attacker will know about the preferences of a user. That is, frequent routes that are requested or information on any topic or the contact information of the user. In this case, confidentiality becomes important.

Q. 2. (iii) Give a concrete example where integrity is more important than confidentiality. **(2)**

Ans. Consider a website in which a user can request information about routes between two places(maps) or news regarding a particular topic or region. In this case, the integrity of the data is much more important than confidentiality of data. These resources need to be available for anyone who needs to access it.

Q. 2. (iv) Give a concrete example where availability is the overriding concern. **(2)**

Ans. The CIA triad goal of availability is more important than the other goals when government-generated online press releases are involved. Press releases are generally for public consumption. For them to be effective, the information they contain should be available to the public. Thus, confidentiality is not of concern. Integrity has only second priority. In the CIA triad, to guarantee availability of information in press releases, governments ensure that their websites and systems have minimal or insignificant downtime. Backups are also used to ensure availability of public information.

Q. 2. (b) How do you classify information security risks across an organization. **(4.5)**

Ans. The classification of threats could be:

1. Physical threats: Physical threat to a computer system could be as a result of loss of the whole computer system, damage of hardware, damage to the computer software,theft of the computer system, vandalism, Natural disaster such as flood, fire, war, earthquakes etc. Acts of terrorism such as the attack on the world trade centre is also one of the major threats to computer which can be classified as physical threat.

2. Accidental error: Accidental errors could occur at any time in a computer system but having proper checks in place should be the major concern of the designer. Accidental error includes corruption of data caused by programming error, user or operator errors.

3. Unauthorized access: Data stored on the computer system has to be accessed for it to be translated into useful information. This also poses a great security threats to the computer system due to unauthorized person's having access to the system. Not only this, information can be accessed via a remote system in the process of being transmitted from one point to the other via network media which includes wired and wireless media.

4. Malicious misuse: Any form of tampering of the computer system which includes penetration, Trojan horses, viruses and any form of illegal alteration of the computer system which also includes the generation of illegal codes to alter the standard codes within the system can be termed as malicious misuse. This could also lead to a great financial loss and should be prevented in all cases

Q. 3. (a) Discuss the various type of deliberate software attacks designed to damage, destroy or deny service to target systems? **(6)**

Ans. Most common software attacks are:

1. Computer virus: 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: 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.

3. 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.

4. 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. They are not always designed to cause harm; there are worms that are made just to spread. Transmission of worms is also often done by exploiting software vulnerabilities.

5. DOS and DDOS attacks: 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. 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.

6. 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 Security Trails.

7. 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 mails, malicious links, files, and downloading software from suspicious websites.

8. 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.

9. Man in the middle attack: 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. Here are just some of the types of MITM attacks:

- DNS spoofing
- IP spoofing
- SSL hijacking
- HTTPS spoofing
- ARP spoofing
- Wi-Fi hacking

Q. 3. (b) What are the various essential challenges in mobile security. (6.5)

Ans. The various essential challenges of Mobile Security are:

1. Physical Security: Lookout Labs estimated that a mobile phone was lost in the USA every 3.5 seconds in 2011 – and that nearly all who found lost devices tried to access the information on the phone. Now, I hope the "access" was an attempt to determine the owner, but who knows? Even temporarily misplacing a phone can put sensitive data at risk.

2. Multiple User Logging: Mobile phones have come a long way, but they are still not versatile machines like computers. Multiple users on mobile devices still have trouble in opening unique protected accounts. Simply put, what one user does on a mobile device is hardly a private affair. Customizable 3rd party solutions are available, but it's much safer when phones are not shared.

3. Secure Data Storage: Mobile phones need good file encrypting for strong security. After all, who wants sensitive corporate data to end up in the wrong hands? Without the proper encryption, not only are personal documents up for grabs, but also passwords to bank, credit card and even business apps. Encrypting sensitive data ensures would-be thieves gain a whole lot of nothing.

4. Mobile Browsing: Perhaps one of the best features of mobile devices is the ability to browse the web on the go, but this also opens up the mobile phones to security risks. The problem is that users cannot see the whole URL or link, much less verify whether the link or URL is safe. That means that users could easily browse their way into a phishing-related attack.

5. Application Isolation: There are mobile applications for just about everything, from social networking to banking. Before installing any app that comes your way, be sure to read the application access request for permission agreement. This often overlooked agreement contains valuable information regarding specific permissions on how the app is to access your device.

Be mindful of what your application purports to do and what it is that it actually does. Chances are a calculator application does not need access to the internet or your personal information.

6. System Updates: People have a tendency to point fingers at mobile device vendors when it comes to security mishaps, but they aren't always to blame. Updates and patches designed to fix issues in mobile devices are not quite as cut and dry as with PCs. Mobile devices vendors often release updates and patches, but unfortunately carriers don't always stream them due to commercial or bureaucratic reasons.

7. Mobile Device Coding Issues: Sometimes developers make honest mistakes, inadvertently creating security vulnerabilities via poor coding efforts. Many times there is bad implementation of encrypted channels for data transmission or even improper

password protection. Ineffective development can lead to security weaknesses whether in PCs or mobile phones.

8. Bluetooth Attacks: As easy as Bluetooth is to use, it can be just as easy for attackers to gain access to one's phone and everything stored within. It's fairly simple for a hacker to run a program to locate available Bluetooth connections and Bingo – they're in. It's important to remember to disable the Bluetooth functionality when not in use.

9. Malware on the Rise: As is the case with computers, malware is rather damaging to mobile phones. The news does not get any better either. 2014 is projected to be far worse, leaving industry leaders and mobile device users no choice but to become proactive about mobile protection. For example, take the Android malware incident in January which impacted more than 600,000 phones.

10. Serious Threats in New Features: Newly added features and updates are serious risks too. The Neat Field Communication, or NFC, technology is a prime example. NFC is designed to allow people to use their mobile phones as a wallet to purchase products. Unfortunately, all one needs to do to take over the mobile device is brush a NFC chip embedded tag over the phone.

It should not come as a surprise that security is such a problem considering the wide variety of mobile devices and smartphones available today. Every phone and mobile OS has its own unique security issues and one should always take precaution, especially as we are becoming increasingly dependent on our mobile devices.

UNIT-II

Q. 4. (a) What is Cyber forensics? Is ethical hacking part of the digital hacking? Justify your answer. **(6)**

Ans. Cyberforensics is an electronic discovery technique used to determine and reveal technical criminal evidence. It often involves electronic data storage extraction for legal purposes. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information. Computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery Cyberforensics is also known as computer forensics. Cyberforensic techniques include:

- Cross-driven analysis that correlates data from multiple hard drives
- Live analysis, which obtains data acquisitions before a PC is shut down
- Deleted file recovery

Ethical Hacking sometimes called as Penetration Testing is an act of intruding/ penetrating into system or networks to find out threats, vulnerabilities in those systems which a malicious attacker may find and exploit causing loss of data, financial loss or other major damages. The purpose of ethical hacking is to improve the security of the network or systems by fixing the vulnerabilities found during testing. Ethical hackers may use the same methods and tools used by the malicious hackers but with the permission of the authorized person for the purpose of improving the security and defending the systems from attacks by malicious users. Ethical hackers are expected to report all the vulnerabilities and weakness found during the process to the management.

Digital hacking also known as growth hacking. **Growth hacking is a relatively new** field in marketing focused on growth. It started in relation to early-stage startups who need massive growth in a short time on small budgets, but has since then also reached bigger corporate companies. The goal of growth hacking strategies is generally to acquire

as many users or customers as possible while spending as little as possible. A growth hacking team is made up of marketers, developers, engineers and product managers that specifically focus on building and engaging the user base of a business. The typical growth hacker often focusses on finding smarter, low-cost alternatives to traditional marketing, e.g. using social media, viral marketing or targeted advertising instead of buying advertising through more traditional media such as radio, newspaper, and television.

Q. 4. (b) Explain the various types of firewalls. Also discuss the design and implementation issues of firewall. **(6.5)**

Ans. A firewall is software or hardware-based network security system that controls the incoming and outgoing network traffic based on applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is not assumed to be secure and trusted.

There are three main classes of firewalls: packet filters, application and circuit gateways (proxies), and stateful inspection (or smart filter) firewalls.

Proxy Servers: A proxy service is an application that redirects users' requests to the actual services based on an organization's security policy. All communication between a user and the actual server occurs through the proxy server. Thus, a proxy server acts as a communications broker between clients and the actual application servers. Because it acts as a checkpoint where requests are validated against specific applications, a proxy server is usually processing intensive and can become a bottleneck under heavy traffic conditions. Proxy servers can operate at either the application layer or the transport layer. Thus, there are two classes of proxy servers: application gateways, which operate at the application layer; and circuit-level gateways, which operate at the transport layer.

Application Gateways: An application gateway is a proxy server that provides access control at the application layer. It acts as an application-layer gateway between the protected network and the untrusted network. Because it operates at the application layer, it is able to examine traffic in detail and, therefore, is considered the most secure type of firewall. It can prevent certain applications, such as FTP, from entering the protected network. It can also log all network activities according to applications for both accounting and security audit purposes. Application gateways can also hide information. Since all requests for services in the protected network pass through the application gateway, it can provide network address translation (or IP address hiding) functionality and conceal IP addresses in the protected network from the Internet by replacing the IP address of every outbound packet (that is, packets going from the protected network to the Internet) with its own IP address. Network address translation also permits unregistered IP addresses to be freely used in the protected network because the gateway will map them to its own IP address when the users attempt to communicate with the outside world.

Circuit-Level Gateways: A circuit-level gateway is a proxy server that validates TCP and UDP sessions before allowing a connection or circuit through the firewall. It is actively involved in the connection establishment and does not allow packets to be forwarded until the necessary access control rules have been satisfied. A circuit level gateway is not as secure as an application gateway because it validates TCP and UDP sessions without full knowledge of the applications that use these transport services. Moreover, once a session has been established, any application can run across that connection. This behavior exposes the protected network to attacks from intruders. Unlike a circuit-level gateway, an application gateway can differentiate the applications that need to be blocked from those that can be allowed to pass through the gateway.

connection. This behavior exposes the protected network to attacks from intruders. Unlike a circuit-level gateway, an application gateway can differentiate the applications that need to be blocked from those that can be allowed to pass through the gateway.

Stateful Packet Filters: Although the application gateway provides the best security among the preceding firewalls, its intensive processing requirement slows down network performance. A stateful packet filtering gateway attempts to provide tight security without compromising performance. Unlike the application gateway, it checks the data that passes through at the network layer but does not process it. The firewall maintains state information for each session, where session states include a combination of communication phase and the endpoint application state. When a stateful packet filtering gateway receives a data packet, it checks the packet against the known state of the session. If the packet deviates from the expected session state, the gateway blocks the rest of the session.

Q. 5. (a) Suppose that you have a message consisting of 1024 bits. Design a method that will extend a key that is 64 bits long into a string of 1024 bits, so that the resulting 1024 bits can be XORed with the message, just like a one-time pad. Is the resulting cipher as secure as a one-time pad? Is it possible for any such cipher to be as secure as a one-time pad. (6)

Ans. Easy way to extend a 64 bit length is to just repeat by multiplying it by $(2^4)16$ to achieve a length of 1024 bits. And since they are the same length, they can be XORed.

No, because while they are of the same length, the one-time pad uses wholly random key of distinct 1024 bits. While, the 64 bit extension uses repeating keys.

The one-time pad seems to be the only provable secure one since you have to assume algorithms are known but specific keys are not. The one-time pad makes sure the key is wholly random and due to that, all plaintexts are equally likely.

Q. 5. (b) Explain the needs and various components of an IDs system. (6.5)

Ans. An IDS (Intrusion Detection System) is a device or application used to inspect all network traffic and alert the user or administrator when there has been unauthorized attempts or access. The two primary methods of monitoring are signature-based and anomaly-based. Depending on the device or application used, the IDS can either simply alert the user or administrator or it could be set up to block specific traffic or automatically respond in some way. The intrusion detection systems did not have the ability to stop such attacks rather than detecting and reporting to the network personnel.

The Intrusion detection system in a similar way complements the firewall security. The firewall protects an organization from malicious attacks from the Internet and the Intrusion detection system detects if someone tries to break in through the firewall or manages to break in the firewall security and tries to have access on any system in the trusted side and alerts the system administrator in case there is a breach in security. Moreover, Firewalls do a very good job of filtering incoming traffic from the Internet; however, there are ways to circumvent the firewall. For example, external users can connect to the Intranet by dialing in through a modem installed in the private network of the organization. This kind of access would not be seen by the firewall. Therefore, an Intrusion detection system (IDS) is a security system that monitors computer systems and network traffic and analyzes that traffic for possible hostile attacks originating from outside the organization and also for system misuse or attacks originating from inside the organization.

Components of Intrusion Detection System: An Intrusion Detection system comprises of Management console and sensors. Management console is the management

detect any malicious activity, it matches the malicious packet against the attack signature database. In case it finds a match, the sensor reports the malicious activity to the management console. The sensor can take different actions based on how they are configured. For example, the sensor can reset the TCP connection by sending a TCP FIN, modify the access control list on the gateway router or the firewall or send an email notification to the administrator for appropriate action.

UNIT-III

Q. 6. (a) What is IDS? Explain the need for intrusion monitoring and detection. Explain three basic network attacks. (4.5)

Ans. Refer to Q. 5. End Term Examination December 2016

Q. 6. (b) Differentiate between Router, switches, bridges, gate-way in terms of their functionality. (8)

Ans. Difference between different networking devices:

1. Bridge – A bridge operates at data link layer. A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

2. Switch – A switch is a multi port bridge with a buffer and a design that can boost its efficiency(large number of ports imply less traffic) and performance. Switch is data link layer device. Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.

3. Routers – A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.

4. Gateway – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

Q. 7. (a) What is biometric System? Explain their role in the information security. (6)

Ans. Refer to Q. 3. End Term Examination December 2016

Q. 7. (b) What is E-Commerce? Discuss various concepts in electronic payment system. (6.5)

Ans. Electronic commerce or ecommerce is a term for any type of business, or commercial transaction, that involves the transfer of information across the Internet. It covers a range of different types of businesses, from consumer based retail sites, through auction or music sites, to business exchanges trading goods and services between corporations. It is currently one of the most important aspects of the Internet to emerge. Ecommerce allows consumers to electronically exchange goods and services with no barriers of time or distance.

E-payment system is a way of making transactions or paying for goods and services through an electronic medium without the use of check or cash. It's also called an electronic payment system or online payment system.

Here's a breakdown of the main participants required for an electronic payment transaction:

- The **cardholder** is identified as the consumer who purchases a product or service online.
- The **merchant** is the person or business that sells the product or service to the cardholder.
- The **issuer** is the financial institution that provides the cardholder with the payment card. This is usually the cardholder's bank.
- The **acquirer**, or **merchant account provider**, is the financial institution that establishes an account with the merchant. The acquirer authorizes the legitimacy of the cardholder account.
- The **payments processor** handles the official transaction between the cardholder and merchant.

The **payment gateway** processes merchant payment messages and uses security protocols and encryptions to ensure transaction safety.

Electronic payment transactions are divided into two types: one-time vendor payments and recurring customer vendor payments.

- **One-time vendor payments** are commonly used on e-commerce websites. A cardholder types in the card or banking information on a checkout page and simply clicks to purchase.
- **Recurring customer vendor payments** are used when the cardholder is paying for a product or service regularly. Customers enter their information once and then opt in for a recurring billing option with a set date for the payment to go through. This is often used by car insurance agencies, phone companies, loan management companies, and other types of businesses.

E-payment methods could be classified into two areas, which are:

1. Cash Payment System

Electronic Funds Transfer (EFT): this is an electronic system used to transfer money from one bank account to another without any cash exchange by hand.

EFT comprises many other concepts of payment system include:

- Direct debit, that is a financial transaction in which the account holder instructs the bank to collect a specific amount of money from his account electronically for payment of goods or services.
- E-Check, a digital version of an old paper check. It's an electronic transfer of money from a bank account, usually checking account without the use of the paper check.
- Electronic billing: This is another form of electronic funds transfer used by companies or businesses to collect payments from customers over electronic method.

2. Credit Payment System

- Credit Card: This is another form of the e-payment system which required the use of the card issued by a financial institute to the cardholder for making payments online or through an electronic device without the use of cash.
- E-Wallet: It is a form of prepaid account that stored user's financial data like debit and credit card information to make an online transaction easier.
- Smart card: This use a plastic card embedded with the microprocessor that can be loaded with funds to make transactions and instant payment of bills. It is also known as a chip card.

UNIT-IV

Q. 8. Differentiate between public and private key cryptography. Explain the working of RSA and DES. Explain which of them is more secure and why? **(12.5)**

Ans. Refer to Q. 4. End term examination Dec 2016

Q. 9. Write short note on:

(a) Design issues in Biometrics. **(4)**

Ans. Design issues in Biometric:

→ **The Effect of Biometric on System Performance:** The signature biometrics system is extensively used in every verification area but it is not attainable for users with highly inconsistent signatures. Besides, there often exist people whose signatures are very simple and can be forged easily. It degrades the performance of the biometric system. Similarly, the facial recognition system may be confusing in distinguishing duplicate twins.

→ **Biometrics is not private-** Biometrics seems to be secure on the surface, but that doesn't necessarily make it more secure than passwords. A password is integrally a secret because only you have the authority to know it. Biometrics is innately public.

→ **Robustness of a Biometric System Environment-** The high system performances claimed by biometric manufacturers were often difficult to be realized in actual operating environments. Most of the functional tests are conducted in controlled laboratory environments where everything was supervised in ideal environmental setups, and because of that the recognition system also interacts correctly. But the same is not possible in a real-world scenario because the voice recognition system which has worked well with a quiet background might affect the accuracy of the voice verification system due to undesirable noises. Even the same is for a facial recognition system that is based on conventional cameras is also severely affected by the problem of illumination.

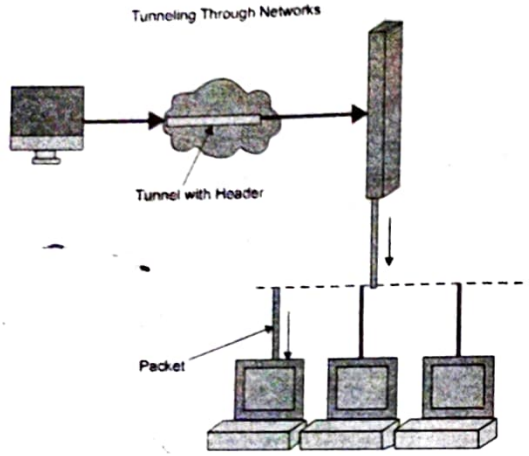
→ **The Need for 'Liveness' Detection in Capturing Devices-** As with the growing cases of signature forgery, several researchers developed signature databases for testing and reporting of skilled forgery detection.

→ **Biometrics can be hacked -** If a hacker has managed to click or arrange the picture of an individual's finger, ear or eye, they could easily gain the access of their accounts.

→ **Biometrics hacks may have greater consequences-** Biometric reveals the part of an individual's identity, if it gets stolen, then it can be used to falsify legal documents, passports, or criminal records, which can do more damage than a stolen credit card pin or number. Unlike passwords, credit cards, or other documents, you can't replace physical identifiers. If someone has managed to get the photos of your iris, you can't get another eye.

Q. 9. (b) Use of tunneling in VPN. **(4.5)**

Ans. Use of tunneling in VPN: Virtual Private Networks creates a tunnel for using a public network (such as Internet) to transfer information between client's PC and office's network. To initiate tunnel in client PC it must have VPN software to connect the ISP router (RAS). After verification of validity of user, software establishes the connection between ISP and use client machine. The data packets sent through tunnel are encapsulated by the tunneling protocol in an additional header. The additional header provides routing information so that the encapsulated payload can traverse the intermediate inter-network (Public network, i.e. Internet). When the packets arrive at destination, the VPN software strips the header off the packets (or unencapsulates the packets) and send it to its destination on the local network.



Tunneling comprises the entire process of encapsulation, transmission, and extraction of packets.

Q. 9. (c) Information security metrics. **(4)**

Ans. Information Security metrics:

- **What is its purpose?** Metrics should support a business goal. Connecting metrics to the business will help to prioritize resources more efficiently.
- **Is it controllable?** For metrics to have worth, they must demonstrate that specific goals are being met. So, metrics should measure processes and outcomes that the team controls.
- **What is the context?** Don't take the results of a security tool and call it a metric; it must have meaning. Ask questions such as, "why are we collecting it, what story does it tell?"
- **Is there an understanding of what "good" is?** Know the target value you want to achieve and the actions you want to take based on that amount.
- **Is it quantitative?** A quantitative value can be compared and demonstrate trends.
- **How trustworthy is your data?** The data used to create a metric should have a high level of accuracy, precision, reliability or
- **Is it easy to process and analyze?** The data should be collected, processed and posted to a central collection point. It should not take a long time to prepare and report your metrics. For example, if metrics are used in a weekly report, it should take two to three days to collect, process and post the received

FIRST TERM EXAMINATION [SEPT.–2019]
SEVENTH SEMESTER [B.TECH.]
INFORMATION SECURITY [ETEC–401]

Time : 1½ hrs. **M.M. : 30**

Note: *Attempt Q.No. 1 and any two more questions from remaining.*

Q. 1. What is an IP Datagram? **(2)**

Q. 1. (b) Differentiate between security and privacy. **(2)**

Ans. Refer to Q.1. (d) of End Term Examination 2018.(Pg. No. 3-2018)

Q. 1. (c) Define software forensics. **(2)**

Ans. Software forensics is the science of analyzing software source code or binary code to determine whether intellectual property infringement or theft occurred. It is the centerpiece of lawsuits, trials, and settlements when companies are in dispute over issues involving software patents, copyrights, and trade secrets. Software forensics tools can compare code to determine correlation, a measure that can be used to guide a software forensics expert.

Q. 1. (d) What is role-based access control? **(2)**

Ans. Role-based access control (RBAC), also known as role-based security, is a mechanism that restricts system access. It involves setting permissions and privileges to enable access to authorized users.This mechanism protects sensitive data and ensures employees can only access information and perform actions they need to do their jobs. For example: One role-based access control example is a set of permissions that allow users to read, edit, or delete articles in a writing application. There are two roles, a Writer and a Reader, and their respective permission levels are presented in this truth table.

Q. 1. (e) What is Data Recovery? **(2)**

Q. 2. (a) Explain the three members of the information security triad. **(5)**

Ans. Refer to Q.2 (a)(i) of End Term Examination 2018.(Pg. No. 6-2018)

Q. 2. (b) How do distributed information systems help global enterprises? **(5)**

Q. 3. (a) Describe Electronic Payment System? **(5)**

Q. 3. (b) Explain the relationship between threats, vulnerabilities, assets & risks and based on this , explain the need for risk analysis. **(5)**

Q. 4. (a) Draw the structure of IPV4 packet format and explain each of its field. **(5)**

Q. 4. (b) What is computer forensics and how does the process work? **(5)**

END TERM EXAMINATION [DEC–2019]

Time : 3 hrs. **M.M. : 75**

Note: *Attempt any five questions including Q.No. 1 which is compulsory. Select one question from each unit.*

Q. 1.Answer the following questions in brief. (Any Five)

Q. 1. (a) Differentiate between security and privacy. **(5)**

Ans. Refer to Q.1. (d) of End Term Examination 2018.(Pg. No. 3-2018)

Q. 1. (b) What is digital signature? Explain the requirement of digital signature system. **(5)**

Q. 1. (c) Write short note on EDI. **(5)**

Q. 1. (d) What are the differences between symmetric key and asymmetric key encryption. (5)

Q. 1. (e) Describe worms, viruses, and Trojan horses. (5)

Ans. Refer to Q.1 (c) of End Term Exmaination 2018.(Pg. No. 2-2018)

Q. 1. (f) What is Ethical Hacking? (5)

UNIT - I

Q. 2. (a) Explain the three members of the information security triad. (6)

Ans. Refer to Q. 2. (a) of End Term Examination 2018.(Pg. No. 6-2018)

Q. 2. (b) Describe four primary classes of threats to network security.(6.5)

OR

Q. 3. (a) How do distributed information system help global enterprises?(6.5)

Ans. A distributed information system consist of multiple autonomous computers that communicate through a computer network.and the computers interact with each other in order to achieve a common goal. A computer program that runs in a distributed system is called a distributed program.The Internet has promoted and speeded the growth of distributed information processing beyond the single enterprise, across the boundaries between enterprises. Information is shared between different enterprises and provides the foundation for trading partnerships and the automation of business collaborations.

A Business Perspective On Information Systems

Managers and business firms invest in information technology and systems because they provide real economic value to the business. Every business has an information value chain. The value of an information system to a business, as well as the decision to invest in any new information system is in large part, determined by the extent to which the system will lead to better management decisions, more efficient business processes, and higher firm profitability. Although there are other reasons why systems are built, their primary purpose is to contribute to corporate value.

Contemporary Approaches to Information Systems

Information systems are sociotechnical systems. Though they are composed of machines, devices, and "hard" physical technology, they require substantial social, oranizational, and intellectual investments to make them work properly.

Technical Approach : The Technical approach to information systems emphasizes mathematically based models to study information systems, as well as the physical technology and formal capabilities of these systems. The disciplines that contributes to the technical approach are computer science, management science, and operations research.

Behavioral Approach : An important part of the information systems field is concerned with behavioral issues that arise in the development and long-term maintenance of information systems. Issues such as strategic business integration, design, implemenation, utilization, and management cannot be explored usefully with the models used in the technical approach. Other behavioral disciplines contribute important concepts and methods.

Sociotechnical Systems : The study of MIS arose to focus on the use of computer-based information systems in business firms and government agencies. MIS combines the work of computer science, management science, and operations research with a practical orientation toward developing system solutions to real-world problems and managing information technology resources. It is also concerned with behavioral issues

surrounding the development, use, and impact of information systems, which are typically discussed in the fields of sociology, economics, and psychology.

Q. 3. (b) Describe security challenges with mobile devices. (6)

Ans. Security challenges with mobile devices:

1. ***Unsafe apps:*** Although the mobile phone vendors try to ensure app security through requiring apps to be signed to be downloaded from the official app stores, misuse of certificates means that even apps downloaded from vendor stores or enterprise sites aren't guaranteed to be free from malware. Even legitimate apps often request more permission than needed to perform their function, which can expose more data than necessary.

2. ***Unsafe operating systems:*** Large numbers of mobile devices are not kept up to date with operating system releases. Out of date operating systems mean devices are vulnerable to security threats that are patched in the later versions.

3. ***Unsafe devices:*** When users jailbreak or root devices, they work around the built-in restrictions of the device. While users feel that jailbreaking gives them freedom and more access to the device's capabilities, jailbreaking also eliminates many controls that provide security.

4. ***Unsafe connections :*** Users often rely on public Wi-Fi to stay connected when they work outside the office. These unsecured Wi-Fi networks can allow malware to be installed on devices or eavesdroppers to intercept data.

5. ***Lost devices :*** Portable devices are easily lost or stolen. When an employee loses physical control of their mobile device, they also lose control of the data on that device. If the device isn't appropriately protected with passwords and encryption, any data on that device may be exposed.

6. ***Uncontrollable users :*** No matter how well you publicize your safe mobile computing policies, there will be employees who find them too inconvenient to follow. Organizations need tools to enforce policies rather than relying on employees' good will.

7. ***Lack of monitoring :*** The large number of mobile devices used in an organization makes monitoring and managing them difficult. It isn't easy to understand the status of all mobile devices, users, and applications at a glance.

8. ***Variety of devices :*** There's no single standard for mobile devices, especially when you allow BYOD rather than supplying the devices. Because of the variety of devices and operating systems, it's difficult to apply controls consistently to ensure the safety of all of them.

UNIT - II

Q. 4. (a) What is computer forensics and how does the process work? (6.5)

Ans. Computer forensics (also known as **computer forensic science**) is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

In computer forensics, there are three types of data that we are concerned with - active, archival, and latent.

Active data is the information that can be readily seen, like data files, programs, and files used by the operating system. This is the easiest type of data to obtain.

Archival data is data that has been backed up and stored. This could consist of backup tapes, CDs, floppies, digital storage devices, or entire hard drives, to cite a few

examples.

Latent (also called ambient) data is the information one typically needs specialized tools to get at. An example would be information that has been deleted or partially overwritten.

When it comes to digital evidence, getting a certified computer forensic examiner involved early will increase the chances of recovering all deleted files, and other data which has not yet been overwritten. As a computer is used, the operating system is constantly writing data to the hard drive. From time to time, the operating system will save new data on a hard drive by overwriting data resident on the drive but no longer needed by the operating system. A deleted file, for example, will remain resident on a hard drive until the operating system overwrites all or some of the file. Thus, in order to preserve as much relevant data as possible on a computer system, you must acquire relevant computers as soon as possible. The on-going use of a computer system may destroy data that could have been extracted before being overwritten.

A skilled forensic examiner will analyze all possibly relevant data found, including in special (and typically inaccessible) areas of a disk. This includes unallocated space on a disk (currently unused, but possibly still a repository of previous data that may potentially be relevant), as well as 'slack' space in a file (the unused space at the end of a file) which is another possible site for previously created and relevant evidence.

When the analysis is completed, the forensic examiner will provide a report analysis of the computer system, as well as provide you a copy of all relevant data, parsed, formatted and arranged to be integrated into your legal theories and strategies.

Q. 4. (b) Describe Electronic Payment System in detail? (6)

OR

Q. 5. (a) What are different types of networking/internetworking devices?(6)

Q. 5. (b) Draw the structure of IPV4 packet format and explain each of its field. (6.5)

UNIT - III

Q. 6. (a) Why biometric systems are required? Explain with example. (6)

Q. 6. (b) Differentiate between cyber forensic, software forensic and media forensic. Draw the model to explain various security layers (6.5)

OR

Q. 7. (a) What are the basis, on which security metrics are designed for an organization? (6.5)

Q. 7 (b) Will fingerprint biometrics work in all types of enviornments for all types of users? (6)

UNIT - IV

Q. 8. (a) What do you mean by firewall. State the main design and implementation issues, with regard to firewalls? (6.5)

Q. 8. (b) How confidentiality of documents can be preserved, while sending them over an insecute channel? (6)

OR

Q. 9 (a) Show the various components of a remote access VPN. (6)

Q. 9. (b) What are the difference between network intrusion detection and network intrusion prevention? Why is intrusion detection required in today's computing environment? (6.5)