Gmail Annanth Prabhu <annanthprabhu@gmail.com>

CS Questions

Ananth Prabhu <educatorananth@gmail.com> Sun, Apr 10, 2022 at 12:45 PM
Reply-To: educatorananth@gmail.com
To: Annanth Prabhu <annanthprabhu@gmail.com>

1. “Is there a difference between cybersecurity and information security?”

The activity can be defined as the defending of computers, servers, mobile devices, electronic systems, networks and data from malicious attacks which range from business organisations to personal devices. The attacks are divided into different categories such as network security, application security, information security, operational security, and disaster recovery along with business continuity. Network security and application security focuses on securing computer networks, along with software and device free from threats and vulnerabilities, respectively. Disaster recovery is associated with the reaction of an organisation in case a loss of data takes place and tries to restore its operational capabilities in order to continue the functioning of the organisation.

The main goal of cyber security is

Confidentiality: Confidentiality is used to provide privacy to prevent unauthorized access to data. It ensures that the data is only accessible to those who are authorized to use it and restricts access to others. It restricts vital information to be exposed to the wrong hands. A good example of Confidentiality is Data encryption which is used to keep information private.

Integrity: The Integrity principle is used to assure that the data is genuine, correct, and safe from unwanted threat actors or unintentional user alteration. It also specifies that the source of information must be genuine. If any changes are made, precautions should be taken to protect sensitive data from corruption or loss and recover from such an incident quickly.

Availability: The Availability principle ensures that the information is constantly available and accessible to those who have access to it. It also ensures that any types of system failures or cyber-attacks do not obstruct these accesses.

Information security in a simplified manner can be described as the prevention of unauthorised access or alteration during the time of storing data or transferring it from one machine to another. The information can be biometrics, social media profile, data on mobile phones etc. due to which, the research for information security covers various sectors such as cryptocurrency and online forensics.

2. Is there any law in India for Information Security?

In the absence of specific legislation for data protection in India, the Information Technology Act 2000 (the IT Act) and a collection of other statutes stand in for this purpose.

The Information Technology Act (2000) and the Information Technology (Amendment) Act 2008
The Information Technology Act (2000) (the IT Act)5 contains provisions for the protection of electronic data. The IT Act penalises 'cyber contraventions' (Section 43(a)–(h)), which attract civil prosecution, and 'cyber offences' (Sections 63–74), which attract criminal action.

In addition to the legislation described above, data protection may also sometimes occur through the enforcement of property rights based on the Copyright Act (1957). Further, other legislation such as the Code of Criminal Procedure (1973), the Indian Telegraph Act 1885, the Companies Act (1956), the Competition Act (2002) and, in cases of unfair trade practices, the Consumer Protection Act (1986), would also be relevant. Finally, citizens may also make use of the common law right to privacy, at least in theory – there is no significant, recent jurisprudence on this.

Additionally, the Personal Data Protection Bill 2019 is expected to pass into law within the next year, becoming India's first and most comprehensive cross-sectoral data protection legislation.

3. What is Cyber Crime? Give some examples of Cyber Crime.

Cyber Crime is just like regular crime but happens on the Internet. Following are some examples of Cyber Crime:

Identity Theft
Online Predators
Hacking of sensitive information from the Internet

BEC ("Business Email Compromise")
Ransomware
Stealing intellectual property

4. Difference between IDS and IPS

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) both are components of the network infrastructure. IPS vs IDS both are the database containing known cyber Attack Signatures that compares network packets to cyber threats, with a matching flag. The main difference is that IDS is a system for tracking, while IPS is a system for regulation. Whereas the IPS prevents the packet from being transmitted depending on the packet content, IDS does not change the network packet in any way, much like firewalls block the traffic by IP address.

IPS – This tool will take action and does not require the administrators' decision to prevent any data packet to identified as a threat by the IPS tool. In addition, IPS systematically evaluated and applied for all packets reaching the network automatically. And also, IPS have two types which are Statistical Anomaly Detection, Signature-Based detection.

Statistical Anomaly Detection: They randomly use samples of network traffic and compare them. They are linked by ports, bandwidth, protocols, and tools.
Signature –Based Detection: Every type of attack uses significant patterns recognizable. The signature can be an attacker-facing signature where packets can be tracked by finding a match in your stored exploit attack file.

IDS – IDS is described as a tool to detect packet intrusion and classify which packets may or may not be threatened. It should only be noticed not to obstruct. It is a hybrid hardware/software protection platform that tackles external and internal threats and tracks in real-time network activity. IDS also have two types which are as follows.

Host-Based Intrusion Detection System: This is a host-based sensor, which involves the use of software as agents on workstations. HIDS has tracked such agents. The agents track and log files of a specific operating system when the agents are installed.
If the activity has been changed unusually and the job starts as soon as the activity monitoring is installed. They can monitor attacks based on changes in internal system activities.

Network-Based Intrusion Detection System: It is a network-based sensor (Ethernet or WIFI) located in segment points or boundaries and tracked device and system transfer data packets
These use real-time surveillance so that attackers can no longer hide, modify or erase evidence of an attack. These are extremely useful for forensic analysis.

5. What is Cryptography in security? What are the different types of Cryptography?

Cryptography is the study of securing communications from outside observers. Encryption algorithms take the original message, or plaintext, and converts it into ciphertext, which is not understandable. The key allows the user to decrypt the message, thus ensuring on they can read the message. The strength of the randomness of an encryption is also studied, which makes it harder for anyone to guess the key or input of the algorithm. Cryptography is how we can achieve more secure and robust connections to elevate our privacy. Advancements in cryptography makes it harder to break encryptions so that encrypted files, folders, or network connections are only accessible to authorized users.

Cryptography can be broken down into three different types:

Secret Key Cryptography
Public Key Cryptography
Hash Functions
Secret Key Cryptography, or symmetric cryptography, uses a single key to encrypt data. Both encryption and decryption in symmetric cryptography use the same key, making this the easiest form of cryptography. The cryptographic algorithm utilizes the key in a cipher to encrypt the data, and when the data must be accessed again, a person entrusted with the secret key can decrypt the data. Secret Key Cryptography can be used on both in-transit and at-rest data, but is commonly only used on at-rest data, as sending the secret to the recipient of the message can lead to compromise.

Examples:

AES
DES
Caesar Cipher

Public Key Cryptography, or asymmetric cryptography, uses two keys to encrypt data. One is used for encryption, while the other key can decrypts the message. Unlike symmetric cryptography, if one key is used to encrypt, that same key cannot decrypt the message, rather the other key shall be used.

One key is kept private, and is called the “private key”, while the other is shared publicly and can be used by anyone, hence it is known as the “public key”. The mathematical relation of the keys is such that the private key cannot be derived from the public key, but the public key can be derived from the private. The private key should not be distributed and should remain with the owner only. The public key can be given to any other entity.

Examples:

ECC
Diffie-Hellman
DSS
Hash functions are irreversible, one-way functions which protect the data, at the cost of not being able to recover the original message. Hashing is a way to transform a given string into a fixed length string. A good hashing algorithm will produce unique outputs for each input given. The only way to crack a hash is by trying every input possible, until you get the exact same hash. A hash can be used for hashing data (such as passwords) and in certificates.

Some of the most famous hashing algorithms are:

MD5
SHA-1
SHA-2 family which includes SHA-224, SHA-256, SHA-384, and SHA-512
SHA-3
Whirlpool
Blake 2
Blake 3

6. What is the difference between a threat, vulnerability and risk?

Generally, people think that threat, vulnerability and risk are the same, but there are some crucial differences between them:

Threat: A threat can be any form of hazard capable of destroying or stealing data, disrupting operations, or cause harm in general. Some examples of threats are Malware, phishing, data breaches, and even unethical employees etc. Any type of threat may be harmful for the organization, so; it is essential to understand threats for developing effective mitigation and making informed cyber security decisions.

Vulnerability: Vulnerability is a possible problem or a flaw in hardware, software, personnel, or procedures that can harm the organization. Threat actors can use these vulnerabilities to achieve their objectives.

Some examples of vulnerabilities are given below:

Physical vulnerabilities: Publicly exposed networking equipment is an example of Physical vulnerability.
Software vulnerabilities:e. buffer overflow vulnerability in a browser.
Human vulnerabilities:e. an employee vulnerable to phishing assaults.
Zero-day vulnerability: It is a type of vulnerability for which a remedy is not yet available.
To cope up with vulnerabilities, we have a method called Vulnerability management. It is the process of identifying, reporting and repairing vulnerabilities.

Risk: Risk is a combination of threat and vulnerability. When we combine the probability of a threat and the consequence of vulnerability, it is called a risk. Risk is the likelihood of a threat agent successfully exploiting vulnerability.

A formula to calculate risk:

Risk = likelihood of a threat * Vulnerability Impact
To control and manage the risk, we use a method called Risk management. It is a process of identifying all potential hazards, analyzing their impact, and determining the best course of action. This is an always running procedure used to examine the new threats and vulnerabilities regularly. By using this method, we can avoid or minimize risks. We can also accept or passed them to a third party according to the response chosen.

7. What is a firewall

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.

A firewall can be hardware, software, or both.Types of firewalls

Proxy firewall
An early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality such as content caching and security by preventing direct connections from outside the network. However, this also may impact throughput capabilities and the applications they can support.

Stateful inspection firewall
Now thought of as a “traditional” firewall, a stateful inspection firewall allows or blocks traffic based on state, port, and protocol. It monitors all activity from the opening of a connection until it is closed. Filtering decisions are made based on both administrator-defined rules as well as context, which refers to using information from previous connections and packets belonging to the same connection.

Unified threat management (UTM) firewall
A UTM device typically combines, in a loosely coupled way, the functions of a stateful inspection firewall with intrusion prevention and antivirus. It may also include additional services and often cloud management. UTMs focus on simplicity and ease of use.

Next-generation firewall (NGFW)
Firewalls have evolved beyond simple packet filtering and stateful inspection. Most companies are deploying next-generation firewalls to block modern threats such as advanced malware and application-layer attacks.

According to Gartner, Inc.’s definition, a next-generation firewall must include:

Standard firewall capabilities like stateful inspection
Integrated intrusion prevention
Application awareness and control to see and block risky apps
Upgrade paths to include future information feeds
Techniques to address evolving security threats
While these capabilities are increasingly becoming the standard for most companies, NGFWs can do more.

Threat-focused NGFW
These firewalls include all the capabilities of a traditional NGFW and also provide advanced threat detection and remediation.

8. What do you understand by Black Hat Hackers, White Hat Hackers and Grey Hat Hackers?

Black Hat Hackers: Black Hat Hackers are the most critical types of hackers. They attempt to obtain unauthorized access to a system to disrupt its operations or steal sensitive and important data. Black Hat Hackers are also known as crackers.

Black Hat Hacking is always illegal due to its malicious aim. The main purpose of Black Hat Hacking is to steal company data, violate privacy, cause system damage, block network connections, etc.

White Hat Hackers: White Hat Hackers are used to accessing the system for penetration testing and vulnerability assessments. They never intend to harm the system; rather, than strive to uncover holes in a computer or network system. White Hat Hackers are also referred to as Ethical Hackers.

Hacking done by White Hat Hackers is called Ethical hacking. It is not a crime, and it is considered one of the most difficult professions in the IT business. Many businesses hire ethical hackers to do penetration tests and vulnerability assessments.

Grey Hat Hackers: Grey Hat Hackers are a combination of Black Hat Hackers and White Hat Hackers. They use elements of both black and white hat hacking techniques. They are supposed to act without malice, but for the sake of amusement, they can exploit the security flaw in a computer system or network without the permission or knowledge of the owner.

The main goal of Grey Hat Hackers is to draw the owners' attention to the security flaw or hole in the network in the hope of receiving gratitude or a reward.

9. Difference between surface web , deep web and dark web.

Surface web: Surface web is the portion of the World Wide Web that is readily available to the general public and searchable with standard web search engines. It is the opposite of the deep web. The section of the internet that is being indexed by search engines is known as the “Surface Web” or “Visible Web”.

Deep web: Deep web is part of the World Wide Web whose contents are not indexed by standard web search engines for any reason.The content of the deep web is hidden behind HTTP forms, and includes many common uses such as web mail, online banking, and services that users must pay for, and which is protected by a paywall, such as video on demand, some online magazines and newspapers, and many more.Content of the deep web can be located

and accessed by a direct URL or IP address, and may require password or other security access past the public website page.

Dark web: The Dark Web is defined as a layer of information and pages that you can only get access to through so-called "overlay networks", which run on top of the normal internet and obscure access. You need special software to access the Dark Web because a lot of it is encrypted, and most of the dark web pages are hosted anonymously.

10. What is Brute Force Attack

What do you understand by Brute Force Attack? How can you prevent it?
Brute Force Attack is a method of finding the right credentials by repetitively trying all the permutations and combinations of possible credentials. Brute Force Attacks are automated in most cases where the tool/software automatically tries to log in with a list of possible credentials.

Following is a list of some ways to prevent Brute Force Attacks:

Password Length: The length of a password is an important aspect to make it hard to crack. You can specify to set at least a minimum length for the password. The lengthier the password, the harder it is to find.
Password Complexity: You can include different characters formats in the password to make brute force attacks harder. Using the combination of alpha-numeric keywords along with special characters and upper and lower case characters can increase the password complexity making it difficult to be cracked.
Limiting Login Attempts: You can make the password hard for brute force attacks by setting a limit on login failures. For example, you can set the limit on login failures as 5. So, when there are five consecutive login failures, the system will restrict the user from logging in for some time or send an Email or OTP to log in the next time. Because brute force is an automated process, limiting login attempts will break the brute force process.

11. What do you understand by Unicasting, Multicasting, and Broadcasting? What is the difference between them?

Unicasting, Multicasting, and Broadcasting are the three methods used to transmit data over a network.

Unicasting: Unicasting is used to send information from a single user to a single receiver. This method is used for point-to-point communications.
Multicasting: Multicasting is used to send data from one or more sources to multiple destinations.
Broadcasting: Broadcasting is also known as one-to-all. In this method, a single sender sends the data over multiple receivers. I.e. the communication is done between a single user and several receivers. The best example of broadcasting is radio or TV broadcasting, where a single sender sends signals to multiple receivers.

12. 1G Vs. 2G Vs. 3G Vs. 4G Vs. 5G

1G: Voice Only
Remember analog phones back in the day? Cell phones began with 1G technology in the 1980s. 1G is the first generation of wireless cellular technology. 1G supports voice only calls.

1G is analog technology, and the phones using it had poor battery life and voice quality, little security, and were prone to dropped calls.

The maximum speed of 1G technology is 2.4 Kbps.

2G: SMS and MMS
Cell phones received their first major upgrade when their technology went from 1G to 2G. This leap took place in Finland in 1991 on GSM networks and effectively took cell phones from analog to digital communications.

The 2G telephone technology introduced call and text encryption, along with data services such as SMS, picture messages, and MMS.

Although 2G replaced 1G and is superseded by later technology versions, it's still used around the world.

The maximum speed of 2G with General Packet Radio Service (GPRS) is 50 Kbps. The max theoretical speed is 384 Kbps with Enhanced Data Rates for GSM Evolution (EDGE). EDGE+ can get up to 1.3 Mbps.

2.5G and 2.75G: Data, Finally
Before making the major leap from 2G to 3G wireless networks, the lesser-known 2.5G and 2.75G were interim standards that bridged the gap to make data transmission — slow data transmission — possible.

2.5G introduced a new packet-switching technique that was more efficient than 2G technology. This led to 2.75G, which provided a theoretical threefold speed increase. AT&T was the first GSM network to support 2.75G with EDGE in the U.S.

2.5G and 2.75G were not defined formally as wireless standards. They served mostly as marketing tools to promote new cell phone features to the public.

3G: More Data, Video Calling, and Mobile Internet
The introduction of 3G networks in 1998 ushered in faster data-transmission speeds, so you could use your cell phone in more data-demanding ways such as for video calling and mobile internet access. The term "mobile broadband" was first applied to 3G cellular technology.

Like 2G, 3G evolved into the much faster 3.5G and 3.75G as more features were introduced to bring about 4G.

The maximum speed of 3G was around 2 Mbps for non-moving devices and 384 Kbps in moving vehicles.

4G: The Current Standard
The fourth generation of networking, which was released in 2008, is 4G. It supports mobile web access like 3G does and also gaming services, HD mobile TV, video conferencing, 3D TV, and other features that demand high speeds.

The max speed of a 4G network when the device is moving is 100 Mbps. The speed is 1 Gbps for low-mobility communication such as when the caller is stationary or walking.

Most current cell phone models support both 4G and 3G technologies.

5G: The Next Standard
5G is a wireless technology with a limited rollout that's intended to improve on 4G.

5G promises significantly faster data rates, higher connection density, much lower latency, and energy savings, among other improvements.

The anticipated theoretical speed of 5G connections is up to 20 Gbps per second.

13. What Is AI, ML and DL

AI is an umbrella discipline that covers everything related to making machines smarter. Machine Learning (ML) is commonly used along with AI but it is a subset of AI. ML refers to an AI system that can self-learn based on the algorithm. Systems that get smarter and smarter over time without human intervention is ML. Deep Learning (DL) is a machine learning (ML) applied to large data sets. Most AI work involves ML because intelligent behaviour requires considerable knowledge.

Artificial Intelligence (AI)

Humans have been obsessed with automation since the beginning of technology adoption. AI enables machines to think without any human intervention. It is a broad area of computer science. AI systems fall into three types: ANI: Artificial Narrow Intelligence, which is goal-oriented and programmed to perform a single task. AGI (Artificial General Intelligence) which allows machines to learn, understand, and act in a way that is indistinguishable from humans in a given situation. ASI (Artificial Super Intelligence) is a hypothetical AI where machines are capable of exhibiting intelligence that surpasses brightest humans.

2. Machine Learning (ML)
ML is a subset of AI that uses statistical learning algorithms to build smart systems. The ML systems can automatically learn and improve without explicitly being programmed. The recommendation systems on music and video streaming services are examples of ML. The machine learning algorithms are classified into three categories: supervised, unsupervised and reinforcement learning.

3. Deep Learning (DL)
This subset of AI is a technique that is inspired by the way a human brain filters information. It is associated with learning from examples. DL systems help a computer model to filter the input data through layers to predict and classify information. Deep Learning processes information in the same manner as the human brain. It is used in technologies such as driver-less cars. DL network architectures are classified into Convolutional Neural Networks, Recurrent
Neural Networks, and Recursive Neural Networks.

14. What is IoT

The term IoT, or Internet of Things, refers to the collective network of connected devices and the technology that facilitates communication between devices and the cloud, as well as between the devices themselves. Thanks to the advent of inexpensive computer chips and high bandwidth telecommunication, we now have billions of devices connected to the internet. This means everyday devices like toothbrushes, vacuums, cars, and machines can use sensors to collect data and respond intelligently to users.

The Internet of Things integrates everyday “things” with the internet. Computer Engineers have been adding sensors

and processors to everyday objects since the 90s. However, progress was initially slow because the chips were big and bulky. Low power computer chips called RFID tags were first used to track expensive equipment. As computing devices shrank in size, these chips also became smaller, faster, and smarter over time.
The cost of integrating computing power into small objects has now dropped considerably. For example, you can add connectivity with Alexa voice services capabilities to MCUs with less than 1MB embedded RAM, such as for light switches. A whole industry has sprung up with a focus on filling our homes, businesses, and offices with IoT devices. These smart objects can automatically transmit data to and from the Internet. All these “invisible computing devices” and the technology associated with them are collectively referred to as the Internet of Things.

How does IoT work?
A typical IoT system works through the real-time collection and exchange of data. An IoT system has three components:

Smart devices
This is a device, like a television, security camera, or exercise equipment that has been given computing capabilities. It collects data from its environment, user inputs, or usage patterns and communicates data over the internet to and from its IoT application.

IoT application
An IoT application is a collection of services and software that integrates data received from various IoT devices. It uses machine learning or artificial intelligence (AI) technology to analyze this data and make informed decisions. These decisions are communicated back to the IoT device and the IoT device then responds intelligently to inputs.

A graphical user interface
The IoT device or fleet of devices can be managed through a graphical user interface. Common examples include a mobile application or website that can be used to register and control smart devices.

What are examples of IoT devices?

Connected cars
There are many ways vehicles, such as cars, can be connected to the internet. It can be through smart dashcams, infotainment systems, or even the vehicle's connected gateway. They collect data from the accelerator, brakes, speedometer, odometer, wheels, and fuel tanks to monitor both driver performance and vehicle health. Connected cars have a range of uses:

Monitoring rental car fleets to increase fuel efficiency and reduce costs.
Helping parents track the driving behavior of their children.
Notifying friends and family automatically in case of a car crash.
Predicting and preventing vehicle maintenance needs.

Connected homes
Smart home devices are mainly focused on improving the efficiency and safety of the house, as well as improving home networking. Devices like smart outlets monitor electricity usage and smart thermostats provide better temperature control. Hydroponic systems can use IoT sensors to manage the garden while IoT smoke detectors can detect tobacco smoke. Home security systems like door locks, security cameras, and water leak detectors can detect and prevent threats, and send alerts to homeowners.
Connected devices for the home can be used for:
Automatically turning off devices not being used.
Rental property management and maintenance.
Finding misplaced items like keys or wallets.
Automating daily tasks like vacuuming, making coffee, etc.

Smart cities
IoT applications have made urban planning and infrastructure maintenance more efficient. Governments are using IoT applications to tackle problems in infrastructure, health, and the environment. IoT applications can be used for:
Measuring air quality and radiation levels.
Reducing energy bills with smart lighting systems.
Detecting maintenance needs for critical infrastructures such as streets, bridges, and pipelines.
Increasing profits through efficient parking management.

Smart buildings
Buildings such as college campuses and commercial buildings use IoT applications to drive greater operational efficiencies. IoT devices can be use in smart buildings for:
Reducing energy consumption.
Lowering maintenance costs.
Utilizing work spaces more efficiently.

15. How is cloud computing different from serverless computing

Traditionally, companies used to set up their own huge data centers and deployment servers, spending tons of cost and effort only to ensure that the hardware that has to run the underlying application is up and running smoothly. Nowadays, this additional effort of setting up the infrastructure has been taken over by cloud providers who ensure the high availability and reliability of servers and other infrastructures by exposing them as a service to consumers.

Cloud computing is a phenomenon where the computer hardware services; be it computing services, database services, network services, all are available via a cloud. The cloud providers host these services on their infrastructure and provide them as a service to the technology consumers. You may already know that there are many cloud providers, and eventually cloud computing resources, right now out there in the market but a few popular names are AWS, Azure, Google Cloud, and IBM Cloud.

Cloud computing works on an on-demand model which means that you can request computing resources anywhere and at any time and these cloud providers will have them ready for you after a few initial configuration steps.

Serverless computing is an extension of cloud computing in a way that it also utilizes the idea of cloud to offer services but with a slightly different strategy and use case. In serverless computing, you do not even have to worry about the infrastructure and hardware configurations; it is all managed by the cloud provider itself.

Unlike cloud computing, which is an on-demand experience, serverless computing operates on a pay-as-you-go model. It means that the consumers are only going to be charged for the number of times their piece of code runs on a serverless service.

In terms of a concrete example, Lambda is, by far, the most popular serverless computing resource offered by Amazon Web Services (AWS) that allows you to connect your code with a lambda function and it would execute as needed.

16. What are Biometrics?

For a quick biometrics definition: Biometrics are biological measurements — or physical characteristics — that can be used to identify individuals. For example, fingerprint mapping, facial recognition, and retina scans are all forms of biometric technology, but these are just the most recognized options.

Researchers claim the shape of an ear, the way someone sits and walks, unique body odors, the veins in one’s hands, and even facial contortions are other unique identifiers. These traits further define biometrics.

Three Types of Biometrics Security
While they can have other applications, biometrics have been often used in security, and you can mostly label biometrics into three groups:

Biological biometrics
Morphological biometrics
Behavioral biometrics

Biological biometrics use traits at a genetic and molecular level. These may include features like DNA or your blood, which might be assessed through a sample of your body’s fluids.

Morphological biometrics involve the structure of your body. More physical traits like your eye-retina, eye-iris, fingerprint, finger geometry, hand geometry,shape of ear,sclerical vein in eye, or the shape of your face can be mapped for use with security scanners.

Behavioral biometrics are based on patterns unique to each person. How you walk, speak, or even type on a keyboard can be an indication of your identity if these patterns are tracked.

17. What are VR, AR, and MR?

Virtual reality (VR), augmented reality (AR) and mixed reality (MR) are emerging technologies utilizing a variety of digital (artificial) immersion and overlays on the real world that users can interact with.

Virtual Reality (VR) encompasses immersive experiences and content via a VR headset or HMD (head-mounted display). The content is 100% digital and computer-generated. The current reality is replaced with a new 3D digital environment in which the user is isolated from the real world.

Augmented reality (AR) overlays computer-generated content on top of the real world. This superimposed digital overlay can superficially interact with the environment in real-time. AR is primarily experienced via a wearable glass device or through smartphone applications.

Mixed reality (MR) combines several technologies into one wearable device. MR lenses or headsets present an

overlay of digital content that interacts with objects in the real world in real-time. The products are, in most cases, in the research and development phase, but MR is viewed through transparent wearable glasses.

Extended reality (XR) is an umbrella term that encompasses all real and virtual environments which include VR, AR, and MR.

18. What is a Block Chain?

A blockchain is a decentralized ledger of all transactions across a peer-to-peer network. Using this technology, participants can confirm transactions without a need for a central clearing authority. Potential applications can include fund transfers, settling trades, voting, and many other issues.

A blockchain is “a distributed database that maintains a continuously growing list of ordered records, called blocks.” These blocks “are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network.”

While blockchain is still largely confined to use in recording and storing transactions for cryptocurrencies such as Bitcoin, proponents of blockchain technology are developing and testing other uses for blockchain, including these:

Blockchain for payment processing and money transfers. Transactions processed over a blockchain could be settled within a matter of seconds and reduce (or eliminate) banking transfer fees.
Blockchain for monitoring of supply chains. Using blockchain, businesses could pinpoint inefficiencies within their supply chains quickly, as well as locate items in real time and see how products perform from a quality-control perspective as they travel from manufacturers to retailers.
Blockchain for digital IDs. Microsoft is experimenting with blockchain technology to help people control their digital identities, while also giving users control over who accesses that data.
Blockchain for data sharing. Blockchain could act as an intermediary to securely store and move enterprise data among industries.
Blockchain for copyright and royalties protection. Blockchain could be used to create a decentralized database that ensures artists maintain their music rights and provides transparent and real-time royalty distributions to musicians. Blockchain could also do the same for open source developers.
Blockchain for Internet of Things network management. Blockchain could become a regulator of IoT networks to “identify devices connected to a wireless network, monitor the activity of those devices, and determine how trustworthy those devices are” and to “automatically assess the trustworthiness of new devices being added to the network, such as cars and smartphones.”
Blockchain for healthcare. Blockchain could also play an important role in healthcare: “Healthcare payers and providers are using blockchain to manage clinical trials data and electronic medical records while maintaining regulatory compliance.”
What are the business benefits of blockchain?
The primary benefit of blockchain is as a database for recording transactions, but its benefits extend far beyond those of a traditional database. Most notably, it removes the possibility of tampering by a malicious actor, as well as providing these business benefits:

Time savings. Blockchain slashes transaction times from days to minutes. Transaction settlement is faster because it doesn’t require verification by a central authority.
Cost savings. Transactions need less oversight. Participants can exchange items of value directly. Blockchain eliminates duplication of effort because participants have access to a shared ledger.
Tighter security. Blockchain’s security features protect against tampering, fraud, and cybercrime.

19. What is Crypto Currency? Name them.

A cryptocurrency, broadly defined, is virtual or digital money that takes the form of tokens or “coins.” Though some cryptocurrencies have ventured into the physical world with credit cards or other projects, the large majority remain entirely intangible.

The “crypto” in cryptocurrencies refers to complicated cryptography that allows for the creation and processing of digital currencies and their transactions across decentralized systems. Alongside this important “crypto” feature is a common commitment to decentralization; cryptocurrencies are typically developed as code by teams who build in mechanisms for issuance (often, although not always, through a process called mining) and other controls.

Cryptocurrencies are almost always designed to be free from government manipulation and control—although, as they have grown more popular, this foundational aspect of the industry has come under fire. The cryptocurrencies modeled after Bitcoin are collectively called altcoins, and in some cases, shitcoins, and have often tried to present themselves as modified or improved versions of Bitcoin. Though some of these currencies may have some impressive features that Bitcoin does not, matching the level of security that Bitcoin’s networks achieve largely has yet to be seen by an altcoin.

Below, we'll examine some of the most important digital currencies other than Bitcoin. First, though, a caveat: It is impossible for a list like this to be entirely comprehensive. One reason for this is the fact that there are over 18,000 cryptocurrencies in existence as of March 2022.1

Though many of these cryptos have little to no following or trading volume, some enjoy immense popularity among dedicated communities of backers and investors.

Beyond that, the field of cryptocurrencies is always expanding, and the next great digital token may be released tomorrow. Though Bitcoin is widely seen as a pioneer in the world of cryptocurrencies, analysts adopt many approaches for evaluating tokens other than BTC. It's common, for instance, for analysts to attribute a great deal of importance to ranking coins relative to one another in terms of market capitalization. We've factored this into our consideration, but there are other reasons why a digital token may be included in the list.

Some of the popular crypto

Ethereum (ETH)
Litecoin (LTC)
Cardano (ADA)
Polkadot (DOT)
Bitcoin Cash (BCH)
Stellar (XLM)
Dogecoin (DOGE)
Binance Coin (BNB)
Solana
Terra
XRP

20. What is Quantum Computing?

Imagine you want to seat 10 fussy people at a dinner party, where there is only one optimal seating plan out of all the different possible combinations. How many different combinations would you have to explore to find the optimal?

2 people, 2 combinations
5 people, 120 combinations
10 people, 3,628,800 combinations

The answer is over 3 million and that's just 10 people around a table.

Larger versions of these kinds of problems stump our most powerful supercomputers, because:

Supercomputers don't have the working memory to hold the myriad combinations of real world problems.

Supercomputers have to analyze each combination one after another, which can take a long time.

Quantum computing is an area of computing focused on developing computer technology based on the principles of quantum theory (which explains the behavior of energy and material on the atomic and subatomic levels). Computers used today can only encode information in bits that take the value of 1 or 0—restricting their ability.

Quantum computing, on the other hand, uses quantum bits or qubits. It harnesses the unique ability of subatomic particles that allows them to exist in more than one state (i.e., a 1 and a 0 at the same time).

Superposition and entanglement are two features of quantum physics on which these supercomputers are based. This empowers quantum computers to handle operations at speeds exponentially higher than conventional computers and at much lesser energy consumption.

Quantum computers process information differently. Classical computers use transistors, which are either 1 or 0. Quantum computers use qubits, which can be 1 or 0 at the same time. The number of qubits linked together increases the quantum computing power exponentially. Meanwhile, linking together more transistors only increases power linearly.

Superposition
In superposition, quantum particles are a combination of all possible states. They fluctuate until they're observed and measured. One way to picture the difference between binary position and superposition is to imagine a coin. Classical bits are measured by "flipping the coin" and getting heads or tails. However, if you were able to look at a coin and see both heads and tails at the same time, as well as every state in between, the coin would be in superposition.

Quantum interference
Quantum interference is the intrinsic behavior of a qubit, due to superposition, to influence the probability of it collapsing one way or another. Quantum computers are designed and built to reduce interference as much as

possible and ensure the most accurate results.

How does quantum computing work?
A quantum computer has three primary parts:

An area that houses the qubits
A method for transferring signals to the qubits
A classical computer to run a program and send instructions
For some methods of qubit storage, the unit that houses the qubits is kept at a temperature just above absolute zero to maximize their coherence and reduce interference. Other types of qubit housing use a vacuum chamber to help minimize vibrations and stabilize the qubits.

Signals can be sent to the qubits using a variety of methods, including microwaves, laser, and voltage.

Entanglement
Entanglement is the ability of quantum particles to correlate their measurement results with each other. When qubits are entangled, they form a single system and influence each other. We can use the measurements from one qubit to draw conclusions about the others. By adding and entangling more qubits in a system, quantum computers can calculate exponentially more information and solve more complicated problems.

21. What is robotics

A robot is the product of the robotics field, where programmable machines are built that can assist humans or mimic human actions. Robots were originally built to handle monotonous tasks (like building cars on an assembly line), but have since expanded well beyond their initial uses to perform tasks like fighting fires, cleaning homes and assisting with incredibly intricate surgeries. Each robot has a differing level of autonomy, ranging from human-controlled bots that carry out tasks that a human has full control over to fully-autonomous bots that perform tasks without any external influences.

While the overall world of robotics is expanding, a robot has some consistent characteristics:

Robots all consist of some sort of mechanical construction. The mechanical aspect of a robot helps it complete tasks in the environment for which it's designed. For example, the Mars 2020 Rover's wheels are individually motorized and made of titanium tubing that help it firmly grip the harsh terrain of the red planet.
Robots need electrical components that control and power the machinery. Essentially, an electric current (a battery, for example) is needed to power a large majority of robots.
Robots contain at least some level of computer programming. Without a set of code telling it what to do, a robot would just be another piece of simple machinery. Inserting a program into a robot gives it the ability to know when and how to carry out a task.
We're really bound to see the promise of the robotics industry sooner, rather than later, as artificial intelligence and software also continue to progress. In the near future, thanks to advances in these technologies, robots will continue getting smarter, more flexible and more energy efficient. They'll also continue to be a main focal point in smart factories, where they'll take on more difficult challenges and help to secure global supply chains.

Though relatively young, the robotics industry is filled with an admirable promise of progress that science fiction could once only dream about. From the deepest depths of our oceans to thousands of miles in outer space, robots will be found performing tasks that humans couldn't dream of achieving alone.

Types of Robots
Mechanical bots come in all shapes and sizes to efficiently carry out the task for which they are designed. All robots vary in design, functionality and degree of autonomy. From the 0.2 millimeter-long "RoboBee" to the 200 meter-long robotic shipping vessel "Vindskip," robots are emerging to carry out tasks that humans simply can't. Generally, there are five types of robots:

1) Pre-Programmed Robots
Pre-programmed robots operate in a controlled environment where they do simple, monotonous tasks. An example of a pre-programmed robot would be a mechanical arm on an automotive assembly line. The arm serves one function — to weld a door on, to insert a certain part into the engine, etc. — and its job is to perform that task longer, faster and more efficiently than a human.

2) Humanoid Robots
Humanoid robots are robots that look like and/or mimic human behavior. These robots usually perform human-like activities (like running, jumping and carrying objects), and are sometimes designed to look like us, even having human faces and expressions. Two of the most prominent examples of humanoid robots are Hanson Robotics' Sophia (in the video above) and Boston Dynamics' Atlas.

3) Autonomous Robots
Autonomous robots operate independently of human operators. These robots are usually designed to carry out tasks in open environments that do not require human supervision. They are quite unique because they use sensors to perceive the world around them, and then employ decision-making structures (usually a computer) to take the optimal next step based on their data and mission. An example of an autonomous robot would be the Roomba vacuum cleaner, which uses sensors to roam freely throughout a home.

4) Teleoperated Robots
Teleoperated robots are semi-autonomous bots that use a wireless network to enable human control from a safe distance. These robots usually work in extreme geographical conditions, weather, circumstances, etc. Examples of teleoperated robots are the human-controlled submarines used to fix underwater pipe leaks during the BP oil spill or drones used to detect landmines on a battlefield.

5) Augmenting Robots
Augmenting robots either enhance current human capabilities or replace the capabilities a human may have lost. The field of robotics for human augmentation is a field where science fiction could become reality very soon, with bots that have the ability to redefine the definition of humanity by making humans faster and stronger. Some examples of current augmenting robots are robotic prosthetic limbs or exoskeletons used to lift hefty weights.

22. What are Drones and what are the laws associated with it.

Originally developed for the military and aerospace industries, drones have found their way into the mainstream because of the enhanced levels of safety and efficiency they bring. These robotic UAVs operate without a pilot on board and with different levels of autonomy. A drone’s autonomy level can range from remotely piloted (a human controls its movements) to advanced autonomy, which means that it relies on a system of sensors and LIDAR detectors to calculate its movement.

Different drones are capable of traveling varying heights and distances. Very close-range drones usually have the ability to travel up to three miles and are mostly used by hobbyists. Close-range UAVs have a range of around 30 miles. Short-range drones travel up to 90 miles and are used primarily for espionage and intelligence gathering. Mid-range UAVs have a 400-mile distance range and could be used for intelligence gathering, scientific studies and meteorological research. The longest-range drones are called “endurance” UAVs and have the ability to go beyond the 400-mile range and up to 3,000 feet in the air.

Because drones can be controlled remotely and can be flown at varying distances and heights, they make perfect candidates to take on some of the toughest jobs in the world. They can be found assisting in a search for survivors after a hurricane, giving law enforcement and military an eye-in-the-sky during terrorist situations and advancing scientific research in some of the most extreme climates on the planet. Drones have even made their way into our homes and serve as entertainment for hobbyists and a vital tool for photographers.

Drone Powered Inspections Monitoring Bridge Safety
Safir Project Aims to Harmonize Rules for Drone Use in Europe
Drones Spot Protected Bird Species in Tall Grass

FOR EMPLOYERS
JOBS
TECH COMPANIES
REMOTE
TECH TOPICS
SALARIES
LEARN
FIND MY TECH HUB
Drones.
What Is A Drone? What Are Uses For Drones?
10 Examples of Rescue Robots
By land, sea or air, life-saving rescue robots go where human first responders can't or shouldn't. Here's how.rescue robot examples
READ ARTICLE
drone companies
24 Drone Companies Taking Flight Across Industries
SEE MORE STORIES
Drone Technology
The term “drone” usually refers to any unpiloted aircraft. Sometimes referred to as “Unmanned Aerial Vehicles" (UAVs), these crafts can carry out an impressive range of tasks, ranging from military operations to package delivery. Drones can be as large as an aircraft or as small as the palm of your hand.

OVERVIEW TYPES USES
OVERVIEW
drone pillar page what is a drone
DRONES ARE BEING IMPLEMENTED IN A VARIETY OF INDUSTRIES TO CARRY OUT DANGEROUS TASKS OR MAKE MONOTONOUS TASKS MORE EFFICIENT.
What is a Drone?
Outer space. Hurricane disaster zones. Antarctica. Your front door. One of these destinations is a little less extreme than the others, but that's the point for drones. Drones, sometimes referred to as "Unmanned Aerial Vehicles" (UAVs) are meant to carry out tasks that range from the mundane to the ultra-dangerous. These robot-like vehicles can be found assisting the rescue of avalanche victims in the Swiss Alps, at your front doorstep dropping off your groceries and almost everywhere in between.

Originally developed for the military and aerospace industries, drones have found their way into the mainstream because of the enhanced levels of safety and efficiency they bring. These robotic UAVs operate without a pilot on board and with different levels of autonomy. A drone's autonomy level can range from remotely piloted (a human controls its movements) to advanced autonomy, which means that it relies on a system of sensors and LIDAR detectors to calculate its movement.

Different drones are capable of traveling varying heights and distances. Very close-range drones usually have the ability to travel up to three miles and are mostly used by hobbyists. Close-range UAVs have a range of around 30 miles. Short-range drones travel up to 90 miles and are used primarily for espionage and intelligence gathering. Mid-range UAVs have a 400-mile distance range and could be used for intelligence gathering, scientific studies and meteorological research. The longest-range drones are called "endurance" UAVs and have the ability to go beyond the 400-mile range and up to 3,000 feet in the air.

Because drones can be controlled remotely and can be flown at varying distances and heights, they make perfect candidates to take on some of the toughest jobs in the world. They can be found assisting in a search for survivors after a hurricane, giving law enforcement and military an eye-in-the-sky during terrorist situations and advancing scientific research in some of the most extreme climates on the planet. Drones have even made their way into our homes and serve as entertainment for hobbyists and a vital tool for photographers.

Drone Powered Inspections Monitoring Bridge Safety
Safir Project Aims to Harmonize Rules for Drone Use in Europe
Drones Spot Protected Bird Species in Tall Grass

Vector illustration of three drones in flight carrying brown boxed packages. Cityscape and mountain ranges in the background with a blue sky and three clouds overhead.

How do drones work?

Unmanned Aerial Vehicles
Drones are commonly referred to as Unmanned Aerial Vehicles (UAV)whereas the entire system that allows a drone to function is a UAS (Unmanned Aerial System.) The UAV is the heart of the UAS and possesses fixed wings or either a single or multi-rotary build for flight. Lighter-than-air UAVs, such as blimps and balloons, and small "Flapping Wing" UAVs also exist.

Ground Control Station (GCS)
Ground Control Stations are the central control unit that allows a UAV to fly and a UAS to operate. These stations can be as large as a desk with multiple views to as small as a handheld controller or even an app. The GCS can be user controlled or operated via satellites and is capable of controlling flight, controlling payload sensors, providing status readouts, mission planning and tethering the data link system.

Payloads
Drones, UAVs specifically, come in a variety of sizes and are capable of carrying payloads of equally variable sized payloads. From life saving medication to packages and more, drones provide an efficient method of delivery but must be built to handle the job at hand. Many drones are capable of rapid flight across oceans while others may be restricted to just a few thousand feet. Some drones may be capable of carrying hundreds of pounds while others can only manage under ten. It is crucial for operators to choose the right drone to help them complete the job at hand.

Data Links
Data Links act as the transmission center that allow the drone to communicate with the ground operator while in flight. Typically utilizing radio frequency technology to communicate, the data link provides the operator with crucial data like remaining flight time, distance from the operator, distance from target, airspeed altitude and more. UAV control at 2.4 GHz for control and 5 GHz for video will provide the operator with approximately four miles of usability, while

frequencies of 900 MHz for flight control and 1.3 GHz for video control can provide more than 20 miles of usability — adding to the list of reasons why pilots must use the right UAS for the task they mean to achieve.

How do drones fly?

VTOL drones
Many drones, typically multi-rotor drones, are considered Vertical Take-off and Landing (VTOL) drones due to their ability to take off, fly, hover and land in a vertical position.

GNSS
Found in numerous types of drones, dual Global Navigation Satellite Systems (GNSS) like GPS and GLONASS drones are able to operate in both non-satellite and satellite modes, providing enhanced connectivity during operation

GNSS allows Return to Home safety technology to function on a drone and can be activated through the ground station's remote controller. This allows pilots to be informed as to whether there are enough drone GNSS satellites available for the drone to be flown independently, the current location of the drone compared to the pilot and the "home point" for the drone to return to. In addition to being controllable through the controller, Return to Home can also be automatically activated once the battery is low or when loss of contact between the drone and the controller occurs.

Types of Drones

Single Rotor Helicopters
Single rotor helicopters look exactly like tiny helicopters and can be gas or electric-powered. The single blade and ability to run on gas help its stability and fly for longer distances. These UAVs are usually used to transport heavier objects, including LIDAR systems, that can be used to survey land, research storms and map erosion caused by global warming.

Multi-Rotor Drones
Multi-rotor drones are usually some of the smallest and lightest drones on the market. They have limited distance, speed and height, but make the perfect flying vehicle for enthusiasts and aerial photographers. These drones can usually spend 20-30 minutes in the air carrying a lightweight payload, such as a camera.

Fixed Wing Drones
Fixed-wing drones look like normal airplanes, where the wings provide the lift instead of rotors- making them very efficient. These drones usually use fuel instead of electricity, allowing them to glide in the air for more than 16 hours. Since these drones are usually much larger, and because of their design, they need to take off and land on runways just as airplanes do. Fixed-wing UAVs are used by the military to carry out strikes, by scientists to carry large amounts of equipment and even by nonprofits to deliver food and other goods to areas that are hard to reach.

Drone laws in India

The government has now announced the Drone (Amendment) Rules, 2022 which says that remote pilot certificate (earlier it was called licence) will not be required for flying small to medium size drones of up to 2kg for non-commercial purposes.The government has categorised drones into five categories:

Nano: Less than or equal to 250 grams. (No permits required)
Micro: Greater than 250 grams and less than or equal to 2 kg. (No permits required for non-commercial usage only)
Small: Greater than 2 kg and less than or equal to 25 kg.
Medium: Greater than 25 kg and less than or equal to 150 kg.
Large: Greater than 150 kg.

Drone (Amendment) Rules, 2022 dated 11 Feb 2022

What are the penalties for non-compliance with the laws and regulations governing drones?

In the case of violation of the CAR, the following penalties may be imposed: an operator's unique identification number (UIN) or unmanned aircraft operator permit (UOAP) issued by the DGCA may be suspended or cancelled.

Breach of compliance to any of the requirements of the CAR and falsification of records or documents may attract penal action, including imposition of penalties as per the Indian Penal Code 1860 (IPC), which includes but is not limited to:

section 287: negligent conduct with respect to machinery (carrying a maximum sentence of imprisonment that may extend to six months or a fine that may extend up to 1,000 Indian rupees, or both);
section 336: act endangering life or personal safety of others (carrying a maximum sentence of imprisonment that may extend to three months or a fine that may extend to 250 rupees, or both);
section 337: causing hurt by an act endangering the life or personal safety of others (carrying a maximum sentence of

imprisonment that may extend to six months or a fine that may extend to 500 rupees, or both);
section 338: causing grievous hurt by an act endangering the life or personal safety of others (carrying a maximum sentence of imprisonment that may extend to two years or a fine that may extend to 1,000 rupees, or both); or
any other relevant section of the IPC.
Penalties for contravention or failure to comply with any rules or directions issued under Rule 133A of the Aircraft Rules 1939 (the rule under which CARs are issued), are punishable to the extent of imprisonment for a term not exceeding six months or a fine not exceeding 200,000 rupees or both.

23. Throw some light on the recent Digital Intermediary and social media ethics code

(i) Providing users, the privacy policy, rules and regulations, and terms and conditions for using its services. The policy must provide that the user is prohibited from hosting, displaying, uploading, modifying, publishing, transmitting, storing, updating, or sharing any information that is contrary to societal norms, immoral, defamatory to the general public or misleads the general public.

(ii) Upon a court or government order, blocking access to illegal information within 36 hours.

(iii) The intermediary shall not publish any information that is against the interests, unity, integrity, and sovereignty of the state.
(iv) Within 24 hours of receiving a complaint, the intermediary shall take all appropriate steps to disable access to material that is non-consensual and sexual in nature.

(v) Identification of the First Originator of Information.

(vi) After a user's registration has been canceled or withdrawn, the information gathered for registration should be stored180 days.

(vii) A grievance Officer to oversee victim complaints must be appointed and his information should be published on the intermediary's website or application.

(viii) Mandatorily publishing a Monthly Compliance Report containing details of complaints received and action taken thereon.

(ix) As per the rules the intermediaries must appoint Chief Compliance Officer, a Nodal Contact Person, and a Resident Grievance Officer.

(x) Additionally, for social media intermediaries there is an additional proviso for 'Voluntary User Verification.

(xi) Significant Social Media Intermediary "shall endeavor to deploy" technology-based measures such as automated tools or other frameworks for proactively identifying any information that depicts any act or stimulation, whether explicit or implied with regards to rape, child sexual abuse or conduct and information identical to the content that has been removed/disabled.

Code of Ethics: The Code of Ethics under the Rules apply to publishers of digital media including such as news and current affairs content providers and OTT platforms. The 2021 Rules stipulate that news publishers in the digital media must adhere to Norms of Journalistic Conduct and the Cable Television Networks Regulation Act, 1995. For the OTT platforms, the necessary requirements are demarcating content into age-appropriate categories [Universal, U/A 7+, U/A 13+, U/A 16+, and Adult], introducing an age verification system for access to adult content and content accessibility to disabled people. A publisher of news and current affairs material, as well as a publisher of online curated content, are required to notify the Ministry of its entity's details, as well as provide information and the required documentation to facilitate communication and coordination.

Grievance Redressal System: Under Rule 10 a grievance redressal mechanism has been established. It has three levels:

(i) Level 1-Self-regulation by the Publisher: This level entails the grievance redressal mechanism established by the Publisher. Rule 11 provides that an applicable entity must appoint a Grievance Redressal Officer who must resolve the grievance received by it within 15 days. The said officer would also serve as a point of contact for complaints related to the Code of Ethics.

(ii) Level 2- Self Regulatory Mechanism: Rule 12 establishes one or more self-regulatory bodies consisting of publishers. Thus, this stage is self-regulation by the aforementioned bodies. These bodies must be registered with the Ministry of Information and Broadcasting. This body will monitor the publisher's compliance with the Code of Ethics, resolve complaints that have not been settled by the publisher within 15 days, and hear appeals lodged by complainants against the publisher's decision.

(iii) Level 3 -Oversight Mechanism: There is the formation of Oversight Mechanism, which ensures adherence to the Code of Ethics by the publishers. This mechanism initiates an Inter-Departmental Committee for hearing grievances. The Authorized Officer will lead the committee, which will hear and investigate complaints or grievances received from Level I/ Level II or the ones made to MIB.

Blocking of Information: In an emergency, authorized officers may investigate digital media material and the Secretary, MIB, may issue an interim order blocking the use of such content. The final order for blocking will be passed only after the Inter-Departmental Committee gives the approval.

24. What is Cyber Warfare?

Cyber warfare is usually defined as a cyber attack or series of attacks that target a country. It has the potential to wreak havoc on government and civilian infrastructure and disrupt critical systems, resulting in damage to the state and even loss of life.

Espionage
Refers to monitoring other countries to steal secrets. In cyber warfare, this can involve using botnets or spear phishing attacks to compromise sensitive computer systems before exfiltrating sensitive information.

Sabotage
Government organizations must determine sensitive information and the risks if it is compromised. Hostile governments or terrorists may steal information, destroy it, or leverage insider threats such as dissatisfied or careless employees, or government employees with affiliation to the attacking country.

Denial-of-service (DoS) Attacks
DoS attacks prevent legitimate users from accessing a website by flooding it with fake requests and forcing the website to handle these requests. This type of attack can be used to disrupt critical operations and systems and block access to sensitive websites by civilians, military and security personnel, or research bodies.

Electrical Power Grid
Attacking the power grid allows attackers to disable critical systems, disrupt infrastructure, and potentially result in bodily harm. Attacks on the power grid can also disrupt communications and render services such as text messages and communications unusable.

Propaganda Attacks
Attempts to control the minds and thoughts of people living in or fighting for a target country. Propaganda can be used to expose embarrassing truths, spread lies to make people lose trust in their country, or side with their enemies.

Economic Disruption
Most modern economic systems operate using computers. Attackers can target computer networks of economic establishments such as stock markets, payment systems, and banks to steal money or block people from accessing the funds they need.

Surprise Attacks
These are the cyber equivalent of attacks like Pearl Harbor and 9/11. The point is to carry out a massive attack that the enemy isn’t expecting, enabling the attacker to weaken their defenses. This can be done to prepare the ground for a physical attack in the context of hybrid warfare.

Examples of Cyber Warfare Operations
Here are several well-publicized examples of cyber warfare in recent times.

Stuxnet Virus
Stuxnet was a worm that attacked the Iranian nuclear program. It is among the most sophisticated cyber attacks in history. The malware spread via infected Universal Serial Bus devices and targeted data acquisition and supervisory control systems. According to most reports, the attack seriously damaged Iran’s ability to manufacture nuclear weapons.

Sony Pictures Hack
An attack on Sony Pictures followed the release of the film “The Interview”, which presented a negative portrayal of Kim Jong Un. The attack is attributed to North Korean government hackers. The FBI found similarities to previous malware attacks by North Koreans, including code, encryption algorithms, and data deletion mechanisms.

Bronze Soldier
In 2007, Estonia relocated a statue associated with the Soviet Union, the Bronze Soldier, from the center of its capital Tallinn to a military cemetery near the city. Estonia suffered a number of significant cyber attacks in the following months. Estonian government websites, media outlets, and banks were overloaded with traffic in massive denial of service (DoS) attacks and consequently were taken offline.

Fancy Bear

CrowdStrike claims that the Russian organized cybercrime group Fancy Bear targeted Ukrainian rocket forces and artillery between 2014 and 2016. The malware was spread via an infected Android application used by the D-30 Howitzer artillery unit to manage targeting data.

Ukrainian officers made wide use of the app, which contained the X-Agent spyware. This is considered to be a highly successful attack, resulting in the destruction of over 80% of Ukraine's D-30 Howitzers.

Enemies of Qatar
Elliott Broidy, an American Republican fundraiser, sued the government of Qatar in 2018, accusing it of stealing and leaking his emails in an attempt to discredit him. The Qataris allegedly saw him as an obstacle to improving their standing in Washington.

According to the lawsuit, the brother of the Qatari Emir was alleged to have orchestrated a cyber warfare campaign, along with others in Qatari leadership. 1,200 people were targeted by the same attackers, with many of these being known "enemies of Qatar", including senior officials from Egypt, Saudi Arabia, the United Arab Emirates, and Bahrain.

How to Combat Cyber Warfare
The legal status of this new field is still unclear as there is no international law governing the use of cyber weapons. However, this does not mean that cyber warfare is not addressed by the law.

The Cooperative Cyber Defense Center of Excellence (CCDCoE) has published the Tallinn Manual, a textbook that addresses rare but serious cyber threats. This manual explains when cyber attacks violate international law and how countries may respond to such violations.

Conducting Risk Assessments with Cyber Wargames
The best way to assess a nation's readiness for cyber warfare is to conduct a real-life exercise or simulation, also known as a cyber wargame.

A wargame can test how governments and private organizations respond to a cyber warfare scenario, expose gaps in defenses, and improve cooperation between entities. Most importantly, a wargame can help defenders learn how to act quickly to protect critical infrastructure and save lives.

Cyber wargames can help cities, states, or countries improve readiness for cyber warfare by:

Testing different situations – such as detecting attacks in early stages, or mitigating risks after critical infrastructure has already been compromised.
Testing unusual scenarios – attacks are never conducted "by the book". By establishing a red team that acts as the attackers and tries to find creative ways to breach a target system, the defenders can learn how to mitigate real threats.
Division of labor and cooperation mechanisms – cyber warfare requires many individuals from different organizations and government units to collaborate. A cyber wargame can bring together those people, who may not know each other, and help them decide how to work together in the event of a crisis.
Improving policies – governments may establish cyber warfare policies, but need to test them in practice. A cyber wargame can test the effectiveness of policies and provide an opportunity for improving them.
The Importance of Layered Defense
Under the pressure of cyber warfare, governments of many countries have issued operational national security policies to protect their information infrastructure. These policies typically use a layered defense approach, which includes:

Securing the cyber ecosystem
Raising awareness for cybersecurity
Promoting open standards for combating cyber threats
Implementing a national cybersecurity assurance framework
Working with private organizations to improve their cybersecurity capabilities
Securing the Private Sector
A strategic factor in cyberwarfare is the resilience of local businesses to cyber attacks. Businesses need to tighten their security measures to reduce the benefits of an attack on a nation-state. The following is a set of measures to ensure corporate cybersecurity, which can promote national security:

Create obstacles to breaching the network
Use web application firewalls (WAF) to quickly detect, investigate, and block malicious traffic
Quickly respond to a breach and restore business operations
Facilitate cooperation between the public and private sectors
Use local hackers as a resource to help protect against foreign cyber threats
Imperva Cyber Warfare Protection
Imperva can help organizations protect themselves against cyberwarfare by implementing a comprehensive cybersecurity solution, including both application and data security.

Imperva Application Security

Imperva provides comprehensive protection for applications, APIs, and microservices:

Web Application Firewall – Prevent attacks with world-class analysis of web traffic to your applications.

Runtime Application Self-Protection (RASP) – Real-time attack detection and prevention from your application runtime environment goes wherever your applications go. Stop external attacks and injections and reduce your vulnerability backlog.

API Security – Automated API protection ensures your API endpoints are protected as they are published, shielding your applications from exploitation.

Advanced Bot Protection – Prevent business logic attacks from all access points – websites, mobile apps and APIs. Gain seamless visibility and control over bot traffic to stop online fraud through account takeover or competitive price scraping.

DDoS Protection – Block attack traffic at the edge to ensure business continuity with guaranteed uptime and no performance impact. Secure your on premises or cloud-based assets – whether you're hosted in AWS, Microsoft Azure, or Google Public Cloud.

Attack Analytics – Ensures complete visibility with machine learning and domain expertise across the application security stack to reveal patterns in the noise and detect application attacks, enabling you to isolate and prevent attack campaigns.

Client-Side Protection – Gain visibility and control over third-party JavaScript code to reduce the risk of supply chain fraud, prevent data breaches, and client-side attacks.

Imperva Data Security
Imperva protects all cloud-based data stores to ensure compliance and preserve the agility and cost benefits you get from your cloud investments

Cloud Data Security – Simplify securing your cloud databases to catch up and keep up with DevOps. Imperva's solution enables cloud-managed services users to rapidly gain visibility and control of cloud data.

Database Security – Imperva delivers analytics, protection, and response across your data assets, on-premise and in the cloud – giving you the risk visibility to prevent data breaches and avoid compliance incidents. Integrate with any database to gain instant visibility, implement universal policies, and speed time to value.

Data Risk Analysis – Automate the detection of non-compliant, risky, or malicious data access behavior across all of your databases enterprise-wide to accelerate remediation.

25. What is Critical Information System?

Modern society is built on the foundation of technological advancements. Today technology infrastructure like the internet, cloud, computers containing sensitive information, etc. is as much important as the physical infrastructure like railways, roadways, and buildings. Technology is growing fast and has a tremendous evolution rate. Seamless functioning of the physical infrastructure such as generation, transmission, and distribution of energy; air and maritime transport; banks and financial services and the water supply and storages, etc. is essential for a nation-state. Information technology has become an indispensable tool to this physical infrastructure, enabling seamless functioning. Any minor disruption at any point of the information infrastructure could create ripples affecting multiple critical infrastructure of a state. But first, what is critical information infrastructure?

Information infrastructure is the term used to describe interconnected computers and networks and the essential information flowing through them. In other words, information infrastructure includes the transmission media; telephone lines, cable television lines and satellites, and antennas, and also the routers, aggregators, repeaters, and other devices that control transmission paths. Infrastructure also includes the software used to send, receive and manage the signals that are transmitted.

The term "critical" refers to infrastructure that provides essential support for economic and social well-being, for public safety, and for the functioning of key government responsibilities. For example- telecommunication network, financial services, transportation or traffic control systems, etc. Disruption or destruction of this infrastructure could result in catastrophic and far-reaching damage. The loss, damage, unavailability, even for a short duration, can have significant consequences and cascading effects far beyond the targeted sector and physical location of the incident.

The information infrastructure that is essential for the continuity of critical infrastructure services is known as Critical Information Infrastructure (CII).

Critical information infrastructure generally refers to:

"Information and Communication Technology systems that are essential to the operations of national and international

Critical Infrastructures. Some of the examples include

i) telecommunication networks;

ii) transportation: air traffic control, railway routing and control, highway or city traffic management;

iii) financial services: credit card transactions, online payment systems or gateways, electronic stock trading; and

iv) Industrial Control Systems/SCADA (Supervisory, Control, and Data Acquisition) used to manage energy production and distribution, chemical manufacturing and refining processes"

The Information Technology Act, 2000 and the CII
In India, Section 70 of the IT (Amendment) Act, 2008 describes CII as "the computer resource, the incapacitation or destruction of which, shall have a debilitating impact on national security, economy, public health or safety."

The government amended the IT Act in 2008 to expand the scope of the existing legal framework. The broadened scope included defining CII and designating a nodal agency and its roles and responsibilities for protecting CII. The Act empowers the Central Government to designate any computer resource which directly or indirectly affects the facility of CII to be a protected system.

The scope of CII is very wide and it becomes extremely challenging to identify the computer resources supporting the functioning of CII. Moreover, tools, techniques, and frameworks for quantitative assessment of the impact of CII disruptions and degradation on national security, economy, public health, or safety are inadequate.

However, the IT Act lays down that any person who unauthorizedly accesses a protected system shall be punished with imprisonment up to 10 years, and a fine.

National Critical Information Infrastructure Protection Centre (NCIIPC)
The National Critical Information Infrastructure Protection Centre (NCIIPC) is the designated nodal agency to protect India's CII. As per NCIIPC, the sectors that were put under the auspices of the agency are:

power and energy (oil and gas, power, industrial control systems, etc.),
banking, financial services and insurance,
ICT, transportation (air, surface [rail and road] and water) and
e-governance and strategic public enterprises.
These sectors can be further subdivided into independent business or industrial functions: for example, in the case of transportation; aviation, shipping, road, and rail are the primary constituents. Similarly, the subdivision of services, such as telecommunications has landline voice services, mobile voice services, and broadband cable services.

Cybersecurity Challenges
Scale and Unlimited Boundaries: Critical infrastructure is geographically spread, across the length and breadth of the nation-state. It is impossible to set any physical boundaries, which makes it a daunting task to affix the areas of responsibility.

An Expanding Network: Critical infrastructure is growing day by day, as new facilities, industries, technologies, equipment, and processes are continuously being added to the already existing massive network.

Complexity and Interdependencies: Critical infrastructure is complex and difficult to understand in terms of its behavior under conditions of disruption, also known as cascading failures, which have unpredictable consequences. It arises out of the interdependencies between and among the sectors, as materials, products, information, etc., are passed on to the downstream sectors.

Human Element: This is most critical in CIP policymaking and its implementation. All the key decisions regarding the design, development, and operations of the systems, applications, and networks behind critical infrastructure installations are human-dependent.

Endless Vulnerabilities and Limited Knowledge: Technologies that underpin critical infrastructure sectors/industries, such as process or assembly chain automation, robotics, remote process controls, IT, database systems, industrial control system and SCADA, are built over a period of time, and probably by different vendors under varying demands of the clients. Gradually, the industrial control system networks have been integrated with IT networks, which has thrown open a wide space for the attackers to exploit the control systems for potential malfunction or disruption.

Asymmetric Angle: The threat spectrum has widened as threats originate from nation-states as well as malicious non-state actors. The present-day threats are ambiguous, uncertain, and indistinct in terms of their identity and goals.

There has been a significant increase in the number of cyber-attacks. The recent attack on Mumbai's power grid by Chinese actors is a prime example. The cyber threats, particularly categorized as cyber-crime, cyber terrorism, cyber

espionage, and cyber warfare, exploit numerous vulnerabilities in the software and hardware design, human resources, and physical systems. This concern has gained significant traction among governmental agencies, computer/network security firms, and the scientific and strategic community. There is a dire need to evolve a comprehensive security policy to address the physical, legal, cyber, and human dimensions of security. Nation-states across the globe have realized the growing challenges in preventing and containing the attacks on critical infrastructure, while ingraining resiliency in the critical infrastructure and the corresponding information infrastructure

26. **Explain the cyber security framework of india and how can it be improved.**

National Cyber Security Policy is a policy framework by Department of Electronics and Information Technology (DeitY) It aims at protecting the public and private infrastructure from cyber attacks. The policy also intends to safeguard "information, such as personal information (of web users), financial and banking information and sovereign data". This was particularly relevant in the wake of US National Security Agency (NSA) leaks that suggested the US government agencies are spying on Indian users, who have no legal or technical safeguards against it. Ministry of Communications and Information Technology (India) defines Cyberspace as a complex environment consisting of interactions between people, software services supported by worldwide distribution of information and communication technology.

To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT system and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.
To create an assurance framework for the design of security policies and promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (Product, process, technology & people).
To strengthen the Regulatory Framework for ensuring a SECURE CYBERSPACE ECOSYSTEM.
To enhance and create National and Sectoral level 24x7 mechanism for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective response and recovery actions.
-To improve visibility of integrity of ICT products and services by establishing infrastructure for testing & validation of security of such product.

To create workforce for 500,000 professionals skilled in next 5 years through capacity building skill development and training.
To provide fiscal benefit to businesses for adoption of standard security practices and processes.
To enable Protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and reducing economic losses due to cyber crime or data theft.
To enable effective prevention, investigation and prosecution of cybercrime and enhancement of law enforcement capabilities through appropriate legislative intervention.

Key Points
National Cyber Security Strategy 2020:
Aim:
To improve cyber awareness and cybersecurity through more stringent audits. Empanelled cyber auditors will look more carefully at the security features of organisations than are legally necessary now.
About:
There will be table-top cyber crisis management exercises regularly to reinforce the idea that cyber attacks can take place regularly.
It does call for an index of cyber preparedness, and attendant monitoring of performance.
A separate budget for cybersecurity is suggested, as also to synergise the role and functions of various agencies with the requisite domain knowledge.

Need:
Cyber warfare offensives:
The United States is just one of many countries that have invested significant amounts of money in developing not just defences against attack, but the ability to mount damaging cyber warfare offensives.
The countries which are believed to have the most developed cyber warfare capabilities are the United States, China, Russia, Israel and the United Kingdom.
Increased Digital usage Post-Covid:
Critical infrastructure is getting digitised in a very fast way — this includes financial services, banks, power, manufacturing, nuclear power plants, etc.
For Protecting Critical Sectors:
It is particularly significant given the increasing interconnectedness of sectors and proliferation of entry points into the internet, which could further grow with the adoption of 5G.
There were 6.97 lakh cyber security incidents reported in the first eight months of 2020, nearly equivalent to the previous four years combined, according to information reported to and tracked by Indian Computer Emergency Response Team (CERT-In).
Recent Cyber Attacks:
There has been a steep rise in the use of resources like malware by a Chinese group called Red Echo to target “a large swathe” of India’s power sector.

Red Echo used malware called ShadowPad, which involves the use of a backdoor to access servers.
Chinese hacker group known as Stone Panda had “identified gaps and vulnerabilities in the IT infrastructure and supply chain software of Bharat Biotech and the Serum Institute of India.
SolarWinds hack, impacted national critical infrastructure in the USA.
For Government:
A local, state or central government maintains a huge amount of confidential data related to country (geographical, military strategic assets etc.) and citizens.
For Individuals:
Photos, videos and other personal information shared by an individual on social networking sites can be inappropriately used by others, leading to serious and even life-threatening incidents.
For Businesses:
Companies have a lot of data and information on their systems. A cyber attack may lead to loss of competitive information (such as patents or original work), loss of employees/customers’ private data resulting into complete loss of public trust on the integrity of the organization.
Present Government Initiatives:

Cyber Surakshit Bharat Initiative.
Cyber Swachhta Kendra.
Online cybercrime reporting portal.
Indian Cyber Crime Coordination Centre (I4C).
National Critical Information Infrastructure Protection Centre (NCIIPC).
Information Technology Act, 2000.
National Cyber Policy, 2013.

Way Forward
India is the second-fastest digital adapter among 17 of the most-digital economies globally, and rapid digitisation does require forward-looking measures to boost cybersecurity.
It is important for the corporates or the respective government departments to find the gaps in their organisations and address those gaps and create a layered security system, wherein security threat intelligence sharing is happening between different layers.
There is a need for an apex body to ensure operational coordination amongst various agencies and ministries.
Cyber deterrence can be envisaged on the lines of strategic deterrence to dissuade cyberattackers. We need to acquire offensive capabilities for effective deterrence in cyberspace.

27. What is Data Analysics

Data analytics is the process of exploring and analyzing large datasets to find hidden patterns, unseen trends, discover correlations, and derive valuable insights to make business predictions. It improves the speed and efficiency of your business.

Businesses use many modern tools and technologies to perform data analytics. This is data analytics for beginners, in a nutshell.

Ways to use Data Analytics

1. Improved Decision Making: Data Analytics eliminates guesswork and manual tasks. Be it choosing the right content, planning marketing campaigns, or developing products. Organizations can use the insights they gain from data analytics to make informed decisions. Thus, leading to better outcomes and customer satisfaction.

2. Better Customer Service: Data analytics allows you to tailor customer service according to their needs. It also provides personalization and builds stronger relationships with customers. Analyzed data can reveal information about customers’ interests, concerns, and more. It helps you give better recommendations for products and services.

3. Efficient Operations: With the help of data analytics, you can streamline your processes, save money, and boost production. With an improved understanding of what your audience wants, you spend lesser time creating ads and content that aren’t in line with your audience’s interests.

4. Effective Marketing: Data analytics gives you valuable insights into how your campaigns are performing. This helps in fine-tuning them for optimal outcomes. Additionally, you can also find potential customers who are most likely to interact with a campaign and convert into leads.

1. Understand the problem: Understanding the business problems, defining the organizational goals, and planning a lucrative solution is the first step in the analytics process. E-commerce companies often encounter issues such as predicting the return of items, giving relevant product recommendations, cancellation of orders, identifying frauds, optimizing vehicle routing, etc.

2. Data Collection: Next, you need to collect transactional business data and customer-related information from the

past few years to address the problems your business is facing. The data can have information about the total units that were sold for a product, the sales, and profit that were made, and also when was the order placed. Past data plays a crucial role in shaping the future of a business.

3. Data Cleaning: Now, all the data you collect will often be disorderly, messy, and contain unwanted missing values. Such data is not suitable or relevant for performing data analysis. Hence, you need to clean the data to remove unwanted, redundant, and missing values to make it ready for analysis.

4. Data Exploration and Analysis: After you gather the right data, the next vital step is to execute exploratory data analysis. You can use data visualization and business intelligence tools, data mining techniques, and predictive modeling to analyze, visualize, and predict future outcomes from this data. Applying these methods can tell you the impact and relationship of a certain feature as compared to other variables.

Below are the results you can get from the analysis:

You can identify when a customer purchases the next product.
You can understand how long it took to deliver the product.
You get a better insight into the kind of items a customer looks for, product returns, etc.
You will be able to predict the sales and profit for the next quarter.
You can minimize order cancellation by dispatching only relevant products.
You'll be able to figure out the shortest route to deliver the product, etc.
5. Interpret the results: The final step is to interpret the results and validate if the outcomes meet your expectations. You can find out hidden patterns and future trends. This will help you gain insights that will support you with appropriate data-driven decision making.

Tools Used

1. Python: Python is an object-oriented open-source programming language. It supports a range of libraries for data manipulation, data visualization, and data modeling.

2. R: R is an open-source programming language majorly used for numerical and statistical analysis. It provides a range of libraries for data analysis and visualization.

3. Tableau: It is a simplified data visualization and analytics tool. This helps you create a variety of visualizations to present the data interactively, build reports, and dashboards to showcase insights and trends.

4. Power BI: Power BI is a business intelligence tool that has an easy 'drag and drop functionality. It supports multiple data sources with features that visually appeal to data. Power BI supports features that help you ask questions to your data and get immediate insights.

5. QlikView: QlikView offers interactive analytics with in-memory storage technology to analyze vast volumes of data and use data discoveries to support decision making. It provides social data discovery and interactive guided analytics. It can manipulate colossal data sets instantly with accuracy.

6. Apache Spark: Apache Spark is an open-source data analytics engine that processes data in real-time and carries out sophisticated analytics using SQL queries and machine learning algorithms.

7. SAS: SAS is a statistical analysis software that can help you perform analytics, visualize data, write SQL queries, perform statistical analysis, and build machine learning models to make future predictions.

28. Differences between IPv4 and IPv6

What is IP?
An IP (Internet Protocol) address is a numerical label assigned to each device connected to a computer network that uses the IP protocol for communication. An IP address acts as an identifier for a specific device on a particular network. The IP address is also called an IP number or Internet address.

IP address specifies the technical format of the addressing and packets scheme. Most networks combine IP with a TCP (Transmission Control Protocol). It also allows developing a virtual connection between a destination and a source.

Now in this IPv4 and IPv6 difference tutorial, we will learn What is IPv4 and IPv6?

What is IPv4?
IPv4 is an IP version widely used to identify devices on a network using an addressing system. It was the first version of IP deployed for production in the ARPANET in 1983. It uses a 32-bit address scheme to store 2^32 addresses which is more than 4 billion addresses. It is considered the primary Internet Protocol and carries 94% of Internet traffic.

What is IPv6?
IPv6 is the most recent version of the Internet Protocol. This new IP address version is being deployed to fulfill the need for more Internet addresses. It was aimed to resolve issues that are associated with IPv4. With 128-bit address space, it allows 340 undecillion unique address space. IPv6 is also called IPng (Internet Protocol next generation).

Internet Engineer Taskforce initiated it in early 1994. The design and development of that suite are now called IPv6.

KEY DIFFERENCE
IPv4 is 32-Bit IP address whereas IPv6 is a 128-Bit IP address.
IPv4 is a numeric addressing method whereas IPv6 is an alphanumeric addressing method.
IPv4 binary bits are separated by a dot(.) whereas IPv6 binary bits are separated by a colon(:).
IPv4 offers 12 header fields whereas IPv6 offers 8 header fields.
IPv4 supports broadcast whereas IPv6 doesn't support broadcast.
IPv4 has checksum fields while IPv6 doesn't have checksum fields
When we compare IPv4 and IPv6, IPv4 supports VLSM (Variable Length Subnet Mask) whereas IPv6 doesn't support VLSM.
IPv4 uses ARP (Address Resolution Protocol) to map to MAC address whereas IPv6 uses NDP (Neighbour Discovery Protocol) to map to MAC address.

Features of IPv4
Following are the features of IPv4:

Connectionless Protocol
Allow creating a simple virtual communication layer over diversified devices
It requires less memory, and ease of remembering addresses
Already supported protocol by millions of devices
Offers video libraries and conferences
Features of IPv6
Here are the features of IPv6:

Hierarchical addressing and routing infrastructure
Stateful and Stateless configuration
Support for quality of service (QoS)
An ideal protocol for neighboring node interaction

IPv4 & IPv6 are both IP addresses that are binary numbers. IPv4 is a 32-bit binary number, and IPv6 is a 128-bit binary number address. IPv4 addresses are separated by periods, while IPv6 addresses are separated by colons.

Both IP addresses are used to identify machines connected to a network. In principle, they are almost similar, but they are different in how they work.

Is IPv4 or IPv6 better?
IPv4 is the fourth version of the Internet Protocol (IP), while IPv6 is the most recent version of the Internet Protocol. Therefore, IPv6 is more advanced, secure, and faster compared to IPv4.

29. **A friend of yours sends an e-card to your mail. You have to click on the attachment to get the card.** What do you do? Justify your answer

There are four risks here:

Some attachments contain viruses or other malicious programs, so just in general, it's risky to open unknown or unsolicited attachments.
Also, in some cases just clicking on a malicious link can infect a computer, so unless you are sure a link is safe, don't click on it.
Email addresses can be faked, so just because the email says it is from someone you know, you can't be certain of this without checking with the person.
Finally, some websites and links look legitimate, but they're really hoaxes designed to steal your information.

30. What is Ransomware?

Ransomware uses asymmetric encryption. This is cryptography that uses a pair of keys to encrypt and decrypt a file. The public-private pair of keys is uniquely generated by the attacker for the victim, with the private key to decrypt the files stored on the attacker's server. The attacker makes the private key available to the victim only after the ransom is paid, though as seen in recent ransomware campaigns, that is not always the case. Without access to the private key, it is nearly impossible to decrypt the files that are being held for ransom.

Many variations of ransomware exist. Often ransomware (and other malware) is distributed using email spam campaigns or through targeted attacks. Malware needs an attack vector to establish its presence on an endpoint.

After presence is established, malware stays on the system until its task is accomplished.

After a successful exploit, ransomware drops and executes a malicious binary on the infected system. This binary then searches and encrypts valuable files, such as Microsoft Word documents, images, databases, and so on. The ransomware may also exploit system and network vulnerabilities to spread to other systems and possibly across entire organizations.

Once files are encrypted, ransomware prompts the user for a ransom to be paid within 24 to 48 hours to decrypt the files, or they will be lost forever. If a data backup is unavailable or those backups were themselves encrypted, the victim is faced with paying the ransom to recover personal files.

To avoid ransomware and mitigate damage if you are attacked, follow these tips:

Back up your data. The best way to avoid the threat of being locked out of your critical files is to ensure that you always have backup copies of them, preferably in the cloud and on an external hard drive. This way, if you do get a ransomware infection, you can wipe your computer or device free and reinstall your files from backup. This protects your data and you won't be tempted to reward the malware authors by paying a ransom. Backups won't prevent ransomware, but it can mitigate the risks.

Secure your backups. Make sure your backup data is not accessible for modification or deletion from the systems where the data resides. Ransomware will look for data backups and encrypt or delete them so they cannot be recovered, so use backup systems that do not allow direct access to backup files.

Use security software and keep it up to date. Make sure all your computers and devices are protected with comprehensive security software and keep all your software up to date. Make sure you update your devices' software early and often, as patches for flaws are typically included in each update.

Practice safe surfing. Be careful where you click. Don't respond to emails and text messages from people you don't know, and only download applications from trusted sources. This is important since malware authors often use social engineering to try to get you to install dangerous files.

Only use secure networks. Avoid using public Wi-Fi networks, since many of them are not secure, and cybercriminals can snoop on your internet usage. Instead, consider installing a VPN, which provides you with a secure connection to the internet no matter where you go.

Stay informed. Keep current on the latest ransomwares threats so you know what to look out for. In the case that you do get a ransomware infection and have not backed up all your files, know that some decryption tools are made available by tech companies to help victims.

Implement a security awareness program. Provide regular security awareness training for every member of your organization so they can avoid phishing and other social engineering attacks. Conduct regular drills and tests to be sure that training is being observed.

9 steps for responding to a ransomware attack
If you suspect you've been hit with a ransomware attack, it's important to act quickly. Fortunately, there are several steps you can take to give you the best possible chance of minimizing damage and quickly returning to business as usual.

Isolate the infected device: Ransomware that affects one device is a moderate inconvenience. Ransomware that is allowed to infect all of your enterprise's devices is a major catastrophe, and could put you out of business for good. The difference between the two often comes down to reaction time. To ensure the safety of your network, share drives and other devices, it's essential that you disconnect the affected device from the network, internet and other devices as quickly as possible. The sooner you do so, the less likely it is that other devices will be infected.

Stop the spread: Because ransomware moves quickly—and the device with ransomware isn't necessarily Patient Zero— immediate isolation of the infected device won't guarantee that the ransomware doesn't exist elsewhere on your network. To effectively limit its scope, you'll need to disconnect from the network all devices that are behaving suspiciously, including those operating off-premises—if they're connected to the network, they present a risk no matter where they are. Shutting down wireless connectivity (Wi-Fi, Bluetooth, etc.) at this point is also a good idea.

Assess the damages: To determine which devices have been infected, check for recently encrypted files with strange file extension names, and look for reports of odd file names or users having trouble opening files. If you discover any devices that haven't been completely encrypted, they should be isolated and turned off to help contain the attack and prevent further damage and data loss. Your goal is to create a comprehensive list of all affected systems, including network storage devices, cloud storage, external hard drive storage (including USB thumb drives), laptops, smartphones, and any other possible vectors. At this point, it's prudent to lock shares. All of them should be restricted if possible; if not, restrict as many as you can. Doing so will halt any ongoing encryption processes and will also keep additional shares from being infected while remediation occurs. But before you do that, you'll want to take a look at

the encrypted shares. Doing so can provide a useful piece of information: If one device has a much higher number of open files than usual, you may have just found your Patient Zero. Otherwise…

Locate Patient Zero: Tracking the infection becomes considerably easier once you've identified the source. To do so, check for any alerts that may have come from your antivirus/antimalware, EDR, or any active monitoring platform. And because most ransomware enters networks through malicious email links and attachments, which require an end user action, asking people about their activities (such as opening suspicious emails) and what they've noticed can be useful as well. Finally, taking a look at the properties of the files themselves can also provide a clue—the person listed as the owner is likely the entry point. (Keep in mind, however, that there can be more than one Patient Zero!)

Identify the ransomware: Before you go any further, it's important to discover which variant of ransomware you're dealing with. One way is to visit No More Ransom, a worldwide initiative McAfee is a part of. The site has a suite of tools to help you free your data, including the Crypto Sheriff tool: Just upload one of your encrypted files and it will scan to find a match. You can also use the information included in the ransom note: If it doesn't spell out the ransomware variant directly, using a search engine to query the email address or the note itself can help. Once you've identified the ransomware and done a bit of quick research about its behavior, you should alert all unaffected employees as soon as possible so they'll know how to spot the signs that they've become infected.

Report the ransomware to authorities: As soon as the ransomware is contained, you'll want to contact law enforcement, for several reasons. First of all, ransomware is against the law—and like any other crime, it should be reported to the proper authorities. Secondly, according to the United States Federal Bureau of Investigation, "Law enforcement may be able to use legal authorities and tools that are unavailable to most organizations." Partnerships with international law enforcement can be leveraged to help find the stolen or encrypted data and bring the perpetrators to justice. Finally, the attack may have compliance implications: Under the terms of the GDPR, if you don't notify the ICO within 72 hours of a breach involving EU citizen data, your business could incur hefty fines.

Evaluate your backups: Now it's time to begin the response process. The quickest and easiest way to do so is to restore your systems from a backup. Ideally, you'll have an uninfected and complete backup created recently enough to be beneficial. If so, the next step is to employ an antivirus/antimalware solution to ensure all infected systems and devices are wiped free of ransomware—otherwise it will continue to lock your system and encrypt your files, potentially corrupting your backup. Once all traces of malware have been eliminated, you'll be able to restore your systems from this backup and—once you've confirmed that all data is restored and all apps and processes are back up and running normally—return to business as usual. Unfortunately, many organizations do not realize the importance of creating and maintaining backups until they need them and they aren't there. Because modern ransomware is increasingly sophisticated and resilient, some of those who do create backups soon find out that the ransomware has corrupted or encrypted them, too, rendering them completely useless.

Research your decryption options: If you find yourself without a viable backup, there's still a chance you can get your data back. A growing number of free decryption keys can be found at No More Ransom. If one is available for the variant of ransomware you're dealing with (and assuming you've wiped all traces of malware from your system by now), you'll be able to use the decryption key to unlock your data. Even if you're fortunate enough to find a decryptor, however, you're not done yet—you can still expect hours or days of downtime as you work on remediation.

Move on: Unfortunately, if you have no viable backups and cannot locate a decryption key, your only option may be to cut your losses and start from scratch. Rebuilding won't be a quick or inexpensive process, but once you've exhausted your other options, it's the best you can do.

--

With respectful regards,
Ananth Prabhu G
B.E, MBA, MTech, DCL, PhD, Post Doctoral Fellow
Professor- Sahyadri College of Engineering & Management
Cyber Law Trainer - Karnataka Judicial Academy
Cyber Security Trainer- Karnataka Police Academy
Director- SurePass
M: 89515-11111
F: www.facebook.com/educatorananth