Introduction to Information Security

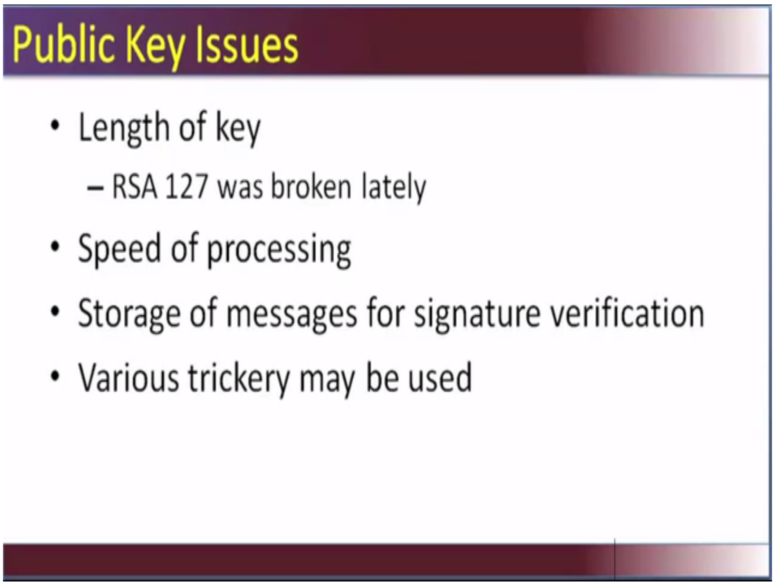
Prof. Dilip H. Ayyar

Department of Computer Science and Engineering

Indian Institute of Technology, Madras

Lecture – 42

(Refer Slide Time: 00:10)



Public Key Issues

- Length of key
  - RSA 127 was broken lately
- Speed of processing
- Storage of messages for signature verification
- Various trickery may be used

Now, what are strength of asymmetric or public key cryptography. The asymmetric nature of public key cryptography, allows it a seizable advantage or a significant advantage of symmetric algorithms. The unique private and public keys provided to each user allow them to conduct secure exchanges of information, without facilitating to devise some to secretly stop the keys.

This glaring weakness of secret key cryptography,symmetric key cryptography becomes the crucial strength of the public key encryption system, but there are weakness in public key encryption also. Keys in the public key cryptography due to their unique nature are more computationally costly than their counter part in the symmetry crypto system. Asymmetric keys must be many times longer than the keys in the secret keys cryptography in order to boast an equivalent security. Keys in symmetric cryptography are also more vulnerable to brute force attack than in the secret key cryptography.

So, there are algorithm for public key cryptography that allows attackers to crack private keys faster than a brute force method would do that. The widely used and pioneering RSA RSA stands for Rivest, Shamir and Adleman algorithm that leaves it susceptible to attack in less than brute force time. While embedding longer keys in other algorithms will usually prevent a brute force attack from succeeding in any leading length of time, this computation becomes more computationally intensive that means more resources are required.

These longer keys can still vary in effectiveness depending upon the computing power available to be attacker. Public key cryptography also has vulnerabilities to attack such as man in the middle. In this situation a malicious third party intercepts public key on its way to one of the parties involved. The third party can then get insert instead passes on his or her own public key message claiming to be from the original centre. Then the attacker can use this process at every step of the exchange in order to be or in order to successfully impersonate each member of the conversation without any other parties having knowledge of this inception.

After bit of cryptography we move on to the fundamentals of cryptography. Now, I suggest that if you are not aware of the fundamentals of cryptography. Go to google learn about oops protocols, the kind of networks. You can study in depth on the security in the networking aspects, also how routing works, what is firewall. We will go to all the fundamentals of those in this session, but I will suggest that you do deeper reading to have a strong foundation of what a network is.

So, what is a network? It is simply two or more computers connected together are linked together using some form of communication medium. The most common types are LAN and WAN. Most of you have heard about the LAN and WAN. The primary difference between the two is LAN is generally restricted to limited area or to a limited geographical area, whereas WAN cover large geographical area.

Most wans are made up of several interconnected or several connected LANs. Then you have intranet and extranet intranet is a private WAN designed to use by everyone within the organization. An intranet may consist of an internal email system a file server a message board, a print server maybe one or two website portals which have information about the company, news, company news forms HR systems. And access to the Intranet website is generally restricted to the use of a firewall.

Extranet is a network that connects people within your organization to people who are outside your organization like your members, consultants, your auditors. All within a secured password protected network that can be accessed from anywhere. What are the benefits of the network of having a network? One is information sharing authorized users can use computers on the network to access and share information and data. This could include special database etc. So, you will take example of accounting package, tally is used where several peoples are several peoples in accounts department can access, update the account details share the account details.

Then hardware sharing one devices connected to a network such as a printer, scanner can be shared by many uses. So, one device which is connected to the network. So, it can be a scanner, it can be a printer it can be any other it can be a SAN, storage area network. It is connected on the network and it can be shared by different users take example of a file server file server is connected on the network people can corroborate share files with each other. Then software sharing instead of purchasing and installing software program on each computer it can be installed on the server itself.

All the users then can access program from the single location. So, it is similar to the example of it was the same as having tally installed, where all the accounts people can view it. It can be on Microsoft office suite or you can say other software which require or which is required by different users within organization. Then collaborative environment, users can work together on big projects by combining the power incapability of different diverse equipments, but then with great power comes great responsibility also.

In the words of the Stanley or who is the creator of superman, I am sorry Spiderman. The risk of network computer is that the security of a computer network is challenged everyday while equipment malfunctions. The server may stop working, printer may stop working. There can be system failures there can be hard disk failures it can be caused by natural disasters. It can be because of not connecting and equipment to an uninterrupted power supply, it can be because of computer hackers it can also be because of virus and malware attacks.

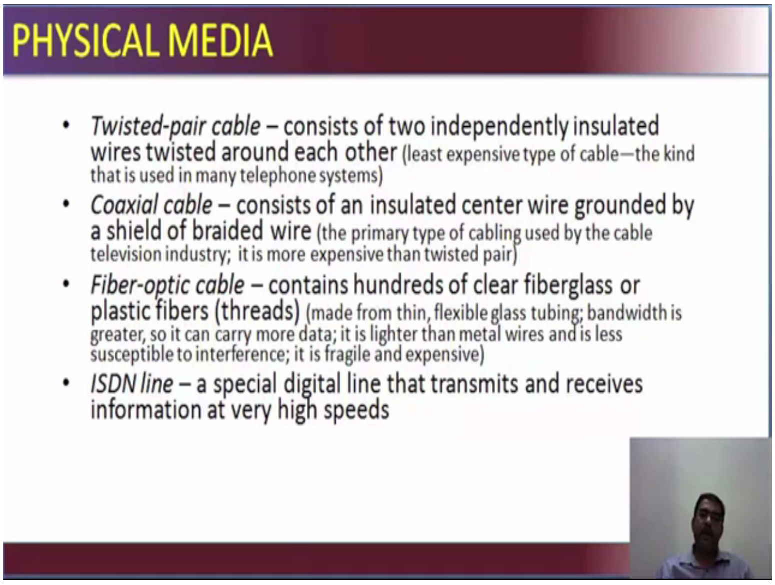
So, any of the reason can be a cause for a network down time. So, bigger your networks the more protection mechanism you have to put to safe guard from different times of times different types of failures. Then we go to communication medium. Or communication channel is to transfer data from one computer to another which require some type of a link through which the data can be transmitted. This link is known as communication channel.

Your RJ 45 cable are communication channels, your RJ11 which is a telephone cable is a communication channel. So, to send data through a channel requires some type of transmission medium. So, your media itself cable itself is a medium, the channel is within the media to transmit data to transmit voice to transmit video. And this media can be either physical or wireless. You take physical medium, there are different kind coaxial cable twisted pair, fiber optics, ISDN lines, twisted pair cable consist of two independently insulated wires, twisted around each other.

This is the least expensive kind of cable, the kind that is used in many telephone systems. So, I mentioned RJ11, RJ 11 is that cable which is used to connect the telephone instrument or the different lines that comes to your building. Then coaxial cable consists of insulated center wire rounded by shield of braidedwire, this is your cable, cable that connects to a set top box or which you directly used to connect to the television, but this is a little more expensive than the twisted wire.

Then you have fiber optic cable which consist of hundreds of clear fibre glass or plastic fiber or threads which is the latest or which is the media which is used more frequently nowadays, where the data transmission are much more faster, then there is a type called UTP which is unshielded twisted pair which is used in your internet cables.

(Refer Slide Time: 10:08)



PHYSICAL MEDIA

- *Twisted-pair cable* – consists of two independently insulated wires twisted around each other (least expensive type of cable—the kind that is used in many telephone systems)
- *Coaxial cable* – consists of an insulated center wire grounded by a shield of braided wire (the primary type of cabling used by the cable television industry; it is more expensive than twisted pair)
- *Fiber-optic cable* – contains hundreds of clear fiberglass or plastic fibers (threads) (made from thin, flexible glass tubing; bandwidth is greater, so it can carry more data; it is lighter than metal wires and is less susceptible to interference; it is fragile and expensive)
- *ISDN line* – a special digital line that transmits and receives information at very high speeds

Then there is an ISDN line which is a special kind of digital line that transmits and receives information at very high speeds. So, the ISDN lines are also more expensive. There are wireless media also like your microwave system, it transmits data via high frequency radio signals through the atmosphere through the air. Then there is satellite system which receives transmitted signal, amplifies them and retransmits the signal to the appropriate location, cellular technology just the ones we use in mobile phones.

It uses an antenna which is build in built to pick up radio signals within a specific area of a cell that is why it is called a cell tower. Infrared technologies which transmits data as infrared light waves from one device to another providing wireless links in PCs and devices. Again what point you not here is the type selected is dependent by the type of the network size of the network and the cost that the company is ready to put in. How are the networks categorized? They are classified using three properties based on topologies, based on protocols used and based on the architecture, we look at all those.

Topology is nothing but the layout which refers to the way computers and peripherals are configured to from the networks. There are different types of topologies of network, the older one was the but topology then all the computers are linked by a single line of cable. The problem with this was if there is a loose connection or if one computer fails, then all the other computers also used to fail. Then there was ring topology the second one where each computers was connected to the other computer would be entire network forming a cycle.

Here also there was a problem, then came the star topology which is widely used now where multiple computers and peripheral device are linked to a central computer called host. So, it is like a server and clients then you have the hybrid topology where the combined network layout types to meet needs of the organization. What is a protocol? Protocol is simply an agreed set of rules and procedures for transmitting data between two or more devices. In simple terms rules of communication is called protocols.

What a computer can do to communicate is determined by what a protocol is, now what are the features determined by protocol how would sending device indicates that it has finished sending a message. How would a receiving device indicates that it has received a message and what is the type of error checking that have been done. Again this is are the basics of what a protocol, the definition of protocol. You can google it and find more and what an in-depth information of what a protocol is and how they communicate, what are the different types of protocol, what are the common protocol we will of course, go through the coming slides.

Most of the computer is use , but some use IBMs token ring protocol. When you use the internet the major protocol is TCP/IP transmission control protocol internet protocol an acronym for transmission control protocol internet protocol for TCP IP there are different types of protocol protocols internet protocols you have. If you see the OSI layers which is a seven layer model starts from the physical and goes up to application. Here in your internet protocol shows several of the protocol sit in the different layers of the implement protocol.

Now, some of the protocols are given, sfile transfer protocol FTP, the first one is Telnet, second one is file transfer protocol, simple network management protocol, message transfer protocol, hypertext transfer protocol. If you noticed all the things are called protocol TCP, transfer control protocol, UDP is user data card protocol, IP is internet protocol, ARP is addresses resource protocol which is used for converting IP addresses to hardware addresses ARP, RARP does the reverse.

So, there are different types of protocol used for different purposes now http is used is used for browsing the web, SNMP is used for monitoring devices, SMTP is for sending your mails messages, FTP is file transferring, Telnet is used to connect to your router firewall server different types of devices, ARP is an function where IP address is converted to a mac address. So, that a computer can understand. There are several devices used in network, hub is an electronic device with number of ports which is used in LAN to link a group of computers, repeaters they are also called amplifiers, it is a old implementation because network were limited to a certain distance because of the topology and the media used.

Then routers are the devices use to ensure that the messages are sent to their intended destination, gateways are hardware or software that allows communication between the similar networks, with this the hardware and software allows communication between two singular networks, then you have modulators and demodulators which are also called modems.

The basic purpose of the modems is to convert digital pulse to analog pulse and transmit over the wire. Now, this a simple example of how a modem works. A modem is a device that converts the digital data originating to a analog signal used by voice communication network such as the telephone industry. At one end the modems convert digital pulses to audio tones and covert the audio tones back to digital tones at the other end. So, the word modem stands for modulator demodulator.

We have seen some of the protocols, in internet protocols group, FTP stands for file transfer protocol for uploading and dowloading files, SMTP is simple mail transfer protocol used for transmitting email messages, POP which allows the recipient to retrieve the messages from a server. Wireless applications protocols enables wireless devices to access the networks using a client server architecture and 802.11 is the protocol for wireless LAN technology. So, all the basic details we are covering now you can see what is a firewall?

Firewall is a choke point, or something that controls the ingress and egress to and from the network. It is also used for monitoring it interconnects networks with different trust levels meaning I allow services of only http to network A, but I will allow the services of FTP and HTTP and SSH to network B. So, this imposes restrictions on network services. That means only authorized traffic or only we allow what is supposed to come in what is being configured to come in only will come in.

Then it also has the capability of auditing and controlling the access to the network. It can also implement alarms for abnormal behavior. So now a days you have something called a UTM device unified threat management which consist of firewall, a router, your IDs, your IPs, your antispam, email gateways all this put together into one box. So, it is itself immune from penetration and it provides perimeter defense. So, basically it provides defense at the edge of a network or the place where your network exits your internal network and goes to a external network.

When you take security consideration what are the important characteristics of the network. That is a degree of locality, media used and the protocol used. Let us see the three. Degree of locality means some networks are very local meaning it is confined to a specific physical area and where are only a small number of users and machines are there which have a common goal and interest, all have a common windows system,

all use a specific software for business and all will reside within the same office premises. So, that is a degree of locality. Now, there are other networks which are very non local example the internet backbone which consists of several servers hosted at different geographical area within the world. Many users access it many users from different areas different countries access. It they share the bandwidth. So, degree of locality determine what kind of network is this .

So, if you see you see the e-commerce site there are several millions of customers will be coming. Let us say you are subscribing for a book or subscribing a service on the network. These subscribers may be some may be form India, some may be from Russia some may be from US. So, they share the bandwidth to access this site. Share the bandwidth in the sense through different paths they come in, but the resources they are accessing is the same.

So, the degree of locality determines the type of network which are used. Here we spoke a little bit about media, so some network are wires, cables on local domain. They can be physically present. So, when we are talking about media, then it comes to wires, then it comes to cables, it comes to telephone lines with in the organizations premises it can be physically protected. It can be made tamper proof, but then the wireless technology we have seen four or five like your satellite link or other radio links, it is difficult to provide physical protection for these devices.

You may be able to protect the device itself, but not the data it is sending out or receiving in. Then the protocol types, TCP IP is the most used, but it only specifies some common intermediate levels, intermediate level. Other protocols also exists above and below the TCP. In some places other protocols also replace TCP IP and then there are a lot of supporting protocols, routing protocols, mailing protocols, directory protocols, network management protocols. Then you have security protocols which is IP set, SSH, SSL to understand TCP IP the three way handshake, how it establishes a communication from a client to a server.