

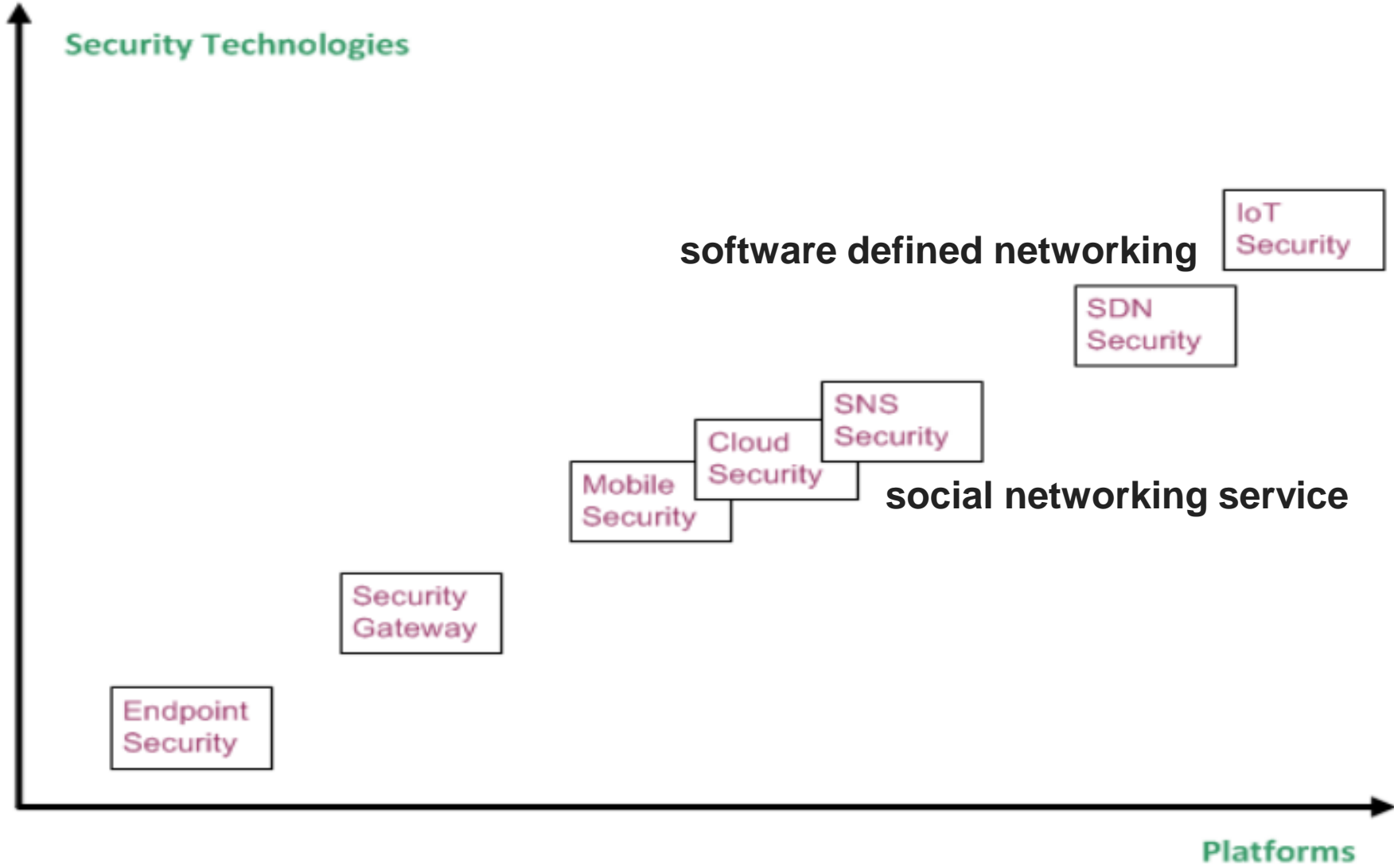
IoT Security and Privacy

IoT Security Concerns and ways to resolve them

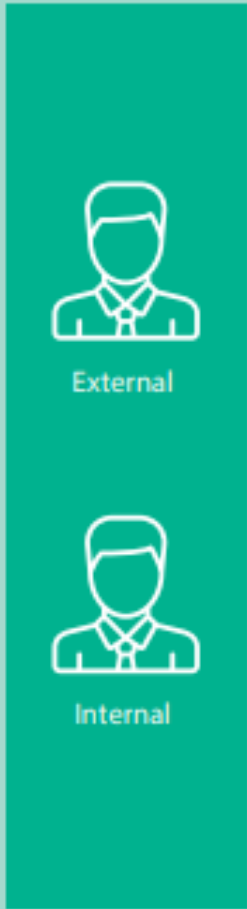
- While the benefits of IoT are **undeniable**, the security can be an issue which has to keep up with the pace of **IoT deployment**.
- As increasingly network integrated connections arise, important processes **that once were performed manually are now vulnerable to cyber threats**.
- Many IoT devices will require the **collection, analysis and transmission of potentially sensitive data**.
- It is essential that this **data is adequately protected at all times** and that the user is aware what private data is being processed.

These issues need to be addressed from a security point of view

- **Preservation of privacy** or secrecy of the data
- **Integrity** of the data for safety
- Staleness or **latency** permissible in the data share
- Level of **restriction** of access to or control of the device
- **Updating** of the software on the device
- **Ownership** of the device whether to be managed or transferred in a secure manner
- **Necessity for the data to be audited**

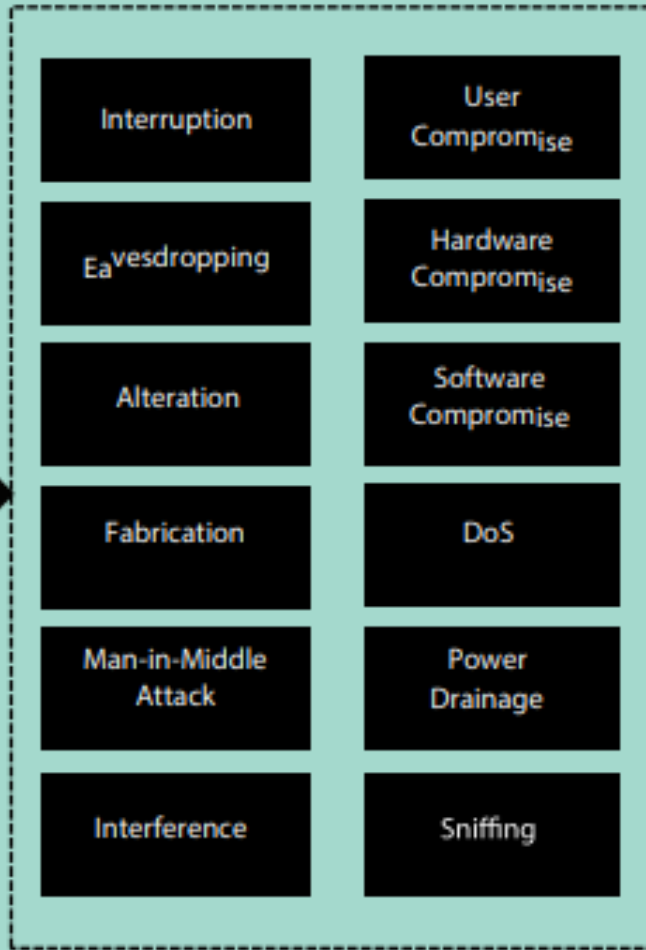


Who can do it



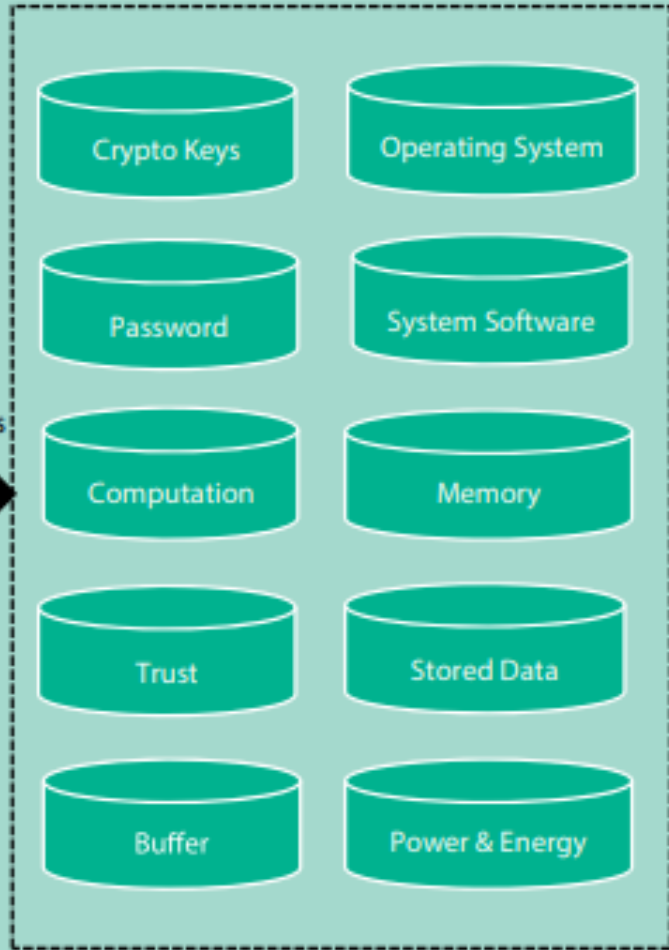
Threat Agents

How can it be done



Threats

What can be compromised



Assets

Initiates



Victimizes



Risks

- malicious actors **manipulating the flow of information** to and from network-connected devices.
- **tampering with devices** themselves, which can lead to the theft of sensitive data and loss of consumer privacy,
- **interruption** of business operations
- **the slowdown of internet functionality** through large-scale denial-of-service attacks
- potential disruptions to **critical infrastructure**.

Security Best practices

- Enable security by **unique, hard to crack user names and passwords** typically as used in **secure bank transactions**
- Changing password : from the mandatory **first change when the device** and the integrated set up is commissioned and **periodic change** in the life cycle.
- **Automatic closure** of the access beyond specific me of inactivity.
- Use **hardware** that incorporates security features to strengthen the protection and integrity of the device.
- For example, use **computer chips** that integrate security at the **module/component level**, embedded in the processor and provide encryption and anonymity. This is to enable encrypted transaction

❑ **Problems and security challenges**

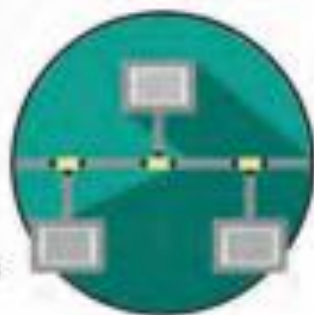
- ❑ Many small devices have limited CPU power
 - ❑ Not much processing power for security
 - ❑ Need to look for new encryption scheme with less CPU power.
 - ❑ Can not install AV software 😊
 - ❑ Example: IP-addressable light bulbs.
- ❑ IoT also needs both encryption key management and identity management
 - ❑ It may scale into billions!

THE RISKS

how can cybercriminals attack the internet of everything?

SNIFFER ATTACKS

An attack which involves a program called a 'sniffer', which sniffs out any unencrypted information being passed through a network and then steals it.



MAN-IN-THE-MIDDLE

An attack where cybercriminals break into a network and/or a device connected to a specific network by guessing or stealing its password



DENIAL OF SERVICE

An attack where cybercriminals prevent or slow down the use of certain networks and/or devices



MAN-IN-THE-MIDDLE

An attack where a third entity steals the data being transmitted between two parties and/or device



RECOMMENDATIONS

What can you do to protect your IoT ecosystem and network?

Enable all security features on all smart devices



Always keep the firmware of smart devices updated



Close any unused ports on all devices and routers



use secure passwords



Patch vulnerabilities as soon as they are announced



Utilize encryption for network and smart devices



Read our guide: What to consider when buying a smart device



Policy options

- Two general principles should be carefully considered in the IoT policy making:
- The IoT **shall not violate human identity**, human integrity, human rights, privacy or individual or public liberties.
- Individuals shall **remain in control of their personal data generated** or processed within the IoT, except where this would conflict with the previous principle.

Use Case 1 – Breath Alcohol Ignition Interlock Device

- Drinking and driving is one of the main causes of road accidents. It is also important to know that more than 70% of road accidents are due to drunk driving.
- **Breath Alcohol Ignition Interlock Device (BAIID)**
- employs sensors to test the breath sample and the vehicle will start only if the alcohol concentration (Breath Alcohol Concentration) is below the set point. Thus, these devices will help in controlling accidents due to drunk driving.

Security

- A **handshake protocol** is implemented at the **boot me with a unique code** stored in the SD card that allows the system to boot up with **registered** hardware only.
- **Tamper proofing:** The unit is tamper proof at the cabinet level by sensing the **tamper switch on** one of the GPIO pin. If the GPIO pin gets disconnected, the unit will stop functioning and would **not even reboot** again.
- **System level handshake** security with the service station server interface: Here each system checks the **unique ID of the car unit** before accessing the data from the system on Wi-Fi.
- **AWS data security:** The cloud data is maintained with **unique access code** and system password for both **write** operation and system level **read** operations.

Security Goals

7

- **Confidentiality**
 - The assets are accessible only by authorized parties.
- **Integrity**
 - The assets are modified only by authorized parties, and only in authorized ways.
- **Availability**
 - Assets are accessible to authorized parties.

Types of Attacks

- **Passive Attack** - A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring of transmission. The goal of the opponent is to obtain information is being transmitted. Types of passive attacks are:
 - Tapping
 - Encryption
 - Scanning
 - Traffic Analysis
- **Active Attack** - An Active attack attempts to alter system resources or effect their operations. Active attack involve some modification of the data stream or creation of false statement. Types of active attacks are:
 - Masquerade
 - Replay
 - Modification of messages
 - Denial of Service (DOS) Attacks

<https://www.geeksforgeeks.org/types-of-security-attacks-active-and-passive-attacks/>

Passive Attacks

9

Tapping

Monitoring unencrypted communications such as emails or telephone calls.

Encryption

Intercepting encrypted information flows and trying to break the encryption.

Scanning

Scanning a device connected to the internet for vulnerabilities such as open ports or a weak operating system version.

Traffic Analysis

Monitoring internet traffic to build data such as who is visiting what website.

Types of Security Breaches

10

- **Interruption**
 - Example: DOS (Denial of Service)
- **Interception**
 - Peeping eyes
- **Modification**
 - Change of existing data
- **Fabrication**
 - Addition of false or spurious data

Security Breaches - Terminology

11

- **Exposure**
 - a form of possible loss or harm
- **Vulnerability**
 - a weakness in the system
- **Attack**
- **Threats**
 - Human attacks, natural disasters, errors
- **Control** – a protective measure
- **Assets** – h/w, s/w, data

Computing System Vulnerabilities

12

- Hardware vulnerabilities
- Software vulnerabilities
- Data vulnerabilities
- Human vulnerabilities ?

Hardware Vulnerabilities

13

- A **computing system**: a collection of hardware, software, data, and people that an organization uses to do computing tasks
- Any piece of the computing system can become the **target** of a computing crime.
- The **weakest point** is the most serious vulnerability.
- The **principle of easiest penetration**

Software Vulnerabilities

14

- Destroyed (deleted) software
- Stolen (pirated) software
- Altered (but still run) software
 - Logic bomb
 - Trojan horse
 - Virus
 - Trapdoor
 - Information leaks

Logic bomb

15

- A **logic bomb** is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.
- For example, a programmer may hide a piece of code that starts deleting files (such as a salary database trigger), should they ever be terminated from the company.

Trojan horse

16

- **Trojan horse**, or **Trojan**, is any malicious computer program which is used to hack into a computer by misleading users of its true intent.
- It is a program designed to breach the security of a computer system while ostensibly performing some innocuous function.

Virus

17

- A **computer virus** is a malware that, when executed, replicates by reproducing itself or infecting other programs by modifying them.
- Infecting computer programs can include as well, data files, or the boot sector of the hard drive.
- When this replication succeeds, the affected areas are then said to be "infected".

Trapdoor (Backdoor)

18

- A **backdoor** is a method, often secret, of bypassing normal authentication in a product, computer system, cryptosystem or algorithms, etc.
- Backdoors are often used for securing unauthorized remote access to a computer, or obtaining access to plaintext in cryptographic systems.

Information leaks

19

- **Information leakage** happens whenever a system that is designed to be closed to an eavesdropper reveals some information to unauthorized parties nonetheless.
- For example, when designing an encrypted instant messaging network, a network engineer without the capacity to crack encryption codes could see when messages are transmitted, even if he could not read them.

Cryptography Basics

20

- **Plain text** (Unencrypted text)
- **Encryption algorithm**
 - Algorithm: A mathematical process for doing something.
- **Secret key**
 - Key: The bits that are combined with the plain text to encrypt it. In some cases this is random numbers, in other cases it is the result of some mathematical operation.
- **Cipher text** (Encrypted text)
- **Decryption algorithm**

Legitimate Versus Fraudulent Encryption Methods



- There are many fraudulent cryptographic claims out there. You do not have to be a cryptography expert to be able to avoid many of those fraudulent claims. Here are some warning signs:
- ■ **Unbreakable:** Anyone with experience in cryptography knows that there is no such thing as an unbreakable code. There are codes that have not yet been broken. There are codes that are very hard to break. But when someone claims that their method is “completely unbreakable,” you should be suspicious.
- ■ **Certified:** There is no recognized certification process for encryption methods. Therefore, any “certification” the company has is totally worthless.

Legitimate Versus Fraudulent Encryption Methods



- ■ **Inexperienced people:** A company is marketing a new encryption method. What is the experience of the people working with it? Does the cryptographer have a background in math, encryption, or algorithms? If not, has he submitted their method to experts in peer-reviewed journals? Or, is he at least willing to disclose how their method works so that it can be fairly judged?

Legitimate Versus Fraudulent Encryption Methods



- **Digital Signatures**

- A digital signature is not used to ensure the confidentiality of a message, but rather to guarantee who sent the message. This is referred to as nonrepudiation. Essentially, it proves who the sender is.
- Digital signatures are actually rather simple, but clever. **They simply reverse the asymmetric encryption process.**
- Recall that in asymmetric encryption, the public key (which anyone can have access to) is used to encrypt a message to the recipient, and the private key (which is kept secure, and private) can decrypt it.
- **With a digital signature, the sender encrypts something with his or her private key. If the recipient is able to decrypt that with the sender's public key, then it must have been sent by the person purported to have sent the message.**

Legitimate Versus Fraudulent Encryption Methods



- **Hashing**

- A hashing is a type of cryptographic algorithm that has some specific characteristics.
- First and foremost it is one-way. That means you cannot “unhash” something.
- The second characteristic is that you get a fixed-length output no matter what input is given. This is exactly how Windows stores passwords. For example, if your password is *password*, then Windows will first hash it producing something like this:
0BD181063899C9239016320B50D3E896693A96DF
- Windows will then store that in the SAM (Security Accounts Manager) file in the Windows System directory.
- When you log on, Windows cannot unhash your password (remember it is one-way). So, what Windows does is take whatever password you type in, hash it, and then compare the result with what is in the SAM file. If they match (exactly), then you can log in.

Legitimate Versus Fraudulent Encryption Methods



- Storing Windows passwords is just one application of hashing. There are others.
- For example, in computer forensics it is common to hash a drive before you begin forensic examination.
- Then later you can always hash it again to see if anything was changed (accidentally or intentionally).
- If the second hash matches the first, then nothing has been changed.
- There are various hashing algorithms. The two most common are MD5 and SHA (it was SHA-1 but since then later versions like SHA-256 are becoming more common).

Legitimate Versus Fraudulent Encryption Methods



- **Authentication**

- When one logs on to a system, the system needs to authenticate the user (and sometimes the user needs to authenticate the system!). There are many authentication protocols.
- A few of the more common are briefly described here:
- ■ **PAP:** Password Authentication Protocol is the simplest form of authentication and the least secure. Usernames and passwords are sent unencrypted, in plain text.
- ■ **SPAP:** Shiva Password Authentication Protocol is an extension to PAP that does encrypt the username and password that is sent over the Internet.
- ■ **CHAP:** Challenge Handshake Authentication Protocol calculates a hash after the user has logged in. Then it shares that hash with the client system. Periodically the server will ask the client to provide that hash (this is the challenge part). If the client cannot, then it is clear that the communications have been compromised. MS-CHAP is a Microsoft-specific extension to CHAP.

Legitimate Versus Fraudulent Encryption Methods



- ■ **Kerberos:** Kerberos is used widely, particularly with Microsoft operating systems. It was invented at MIT and derives its name from the mythical three-headed dog that was reputed to guard the gates of Hades.
- The system is a bit complex but the basic process is as follows:
- When a user logs in, the authentication server verifies the user's identity and then contacts the ticket granting server (these are often on the same machine).
- The ticket granting server sends an encrypted "ticket" to the user's machine. That ticket identifies the user as being logged in.
- Later when the user needs to access some resource on the network, the user's machine uses that ticket granting ticket to get access to the target machine.
- There is a great deal of verification for the tickets, and these tickets expire in a relatively short time.

Encryptions Used in Internet



- What sort of encryption is used on bank websites and e-commerce? In general, symmetric algorithms are faster, and require a shorter key length to be as secure as asymmetric algorithms.
- However, there is the problem of how to securely exchange keys. So most e-commerce solutions use an asymmetric algorithm to exchange symmetric keys and then use the symmetric keys to encrypt the actual data.
- When visiting websites that have an HTTPS at the beginning, rather than HTTP, the *S* denotes *secure*. That means traffic between your browser and the web server is encrypted.
- This is usually done with either SSL (Secure Sockets Layer) or TLS (Transport Layer Security). SSL, the older of the two technologies, was developed by Netscape.
- SSL and TLS are both asymmetric systems.

Encryptions Used in Internet



- **Virtual Private Networks**
- A *VPN* is a *virtual private network*. This is essentially a way to use the Internet to create a virtual connection between a remote user or site and a central location.
- The packets sent back and forth over this connection are encrypted, thus making it private.
- The VPN must emulate a direct network connection.
- There are three different protocols that are used to create VPNs:
 - ■ Point-to-Point Tunneling Protocol (PPTP)
 - ■ Layer 2 Tunneling Protocol (L2TP)
 - ■ Internet Protocol Security (IPsec)

Encryptions Used in Internet



- **PPTP**
- ***Point-to-Point Tunneling Protocol (PPTP)*** is the oldest of the three protocols used in VPNs. It was originally designed as a secure extension to Point-to-Point Protocol (PPP).
- It adds the features of encrypting packets and authenticating users to the older PPP protocol. PPTP works at the data link layer of the OSI model.
- PPTP offers two different methods of authenticating the user: Extensible Authentication Protocol (EAP) and Challenge Handshake Authentication Protocol (CHAP).
- EAP was actually designed specifically for PPTP and is not proprietary.
- CHAP is a three-way process whereby the client sends a code to the server, the server authenticates it, and then the server responds to the client. CHAP also periodically re-authenticates a remote client, even after the connection is established.
- PPTP uses Microsoft Point-to-Point Encryption (MPPE) to encrypt packets. MPPE is actually a version of DES.

Encryptions Used in Internet



- **L2TP**
- *Layer 2 Tunneling Protocol (L2TP)* was explicitly designed as an enhancement to PPTP.
- Like PPTP, it works at the data link layer of the OSI model. It has several improvements to PPTP.
- First, it offers more and varied methods for authentication—PPTP offers two, whereas L2TP offers five.
- In addition to CHAP and EAP, L2TP offers PAP, SPAP, and MS-CHAP.
- In addition to more authentication protocols available for use, L2TP offers other enhancements.
- PPTP will only work over standard IP networks, whereas L2TP will work over X.25 networks (a common protocol in phone systems) and ATM (asynchronous transfer mode, a high-speed networking technology) systems.
- L2TP also uses IPsec for its encryption.

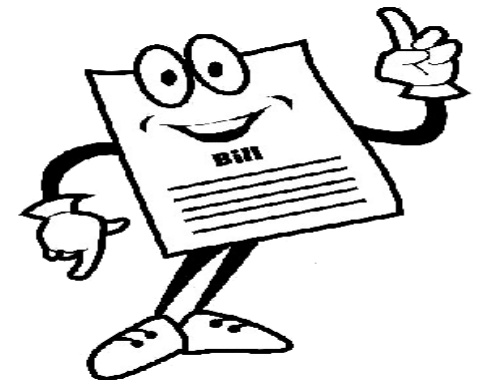
Encryptions Used in Internet



- **IPsec**
- *IPsec* is short for *Internet Protocol Security*. It is the latest of the three VPN protocols.
- One of the differences between IPsec and the other two methods is that it encrypts not only the packet data, but also the header information.
- It also has protection against unauthorized retransmission of packets. This is important because one trick that a hacker can use is to simply grab the first packet from a transmission and use it to get their own transmissions to go through.
- Essentially, the first packet (or packets) has to contain the login data. If you simply resend that packet (even if you cannot crack its encryption), you will be sending a valid logon and password that can then be followed with additional packets.
- Preventing unauthorized retransmission of packets prevents this from happening.

1.1 INTRODUCTION

- ❖ The internet in India is growing rapidly. It has given rise to new opportunities in every field we can think of be it entertainment, business, sports or education.
- ❖ There're two sides to a coin. Internet also has it's own disadvantages is Cyber crime- illegal activity committed on the internet.



E-Mail Spoofing

- E-mail spoofing is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source.
- To send spoofed e-mail, senders insert commands in headers that will alter message information.
- It is possible to send a message that appears to be from anyone, anywhere, saying whatever the sender wants it to say.
- Thus, someone could send spoofed e-mail that appears to be from you with a message that you didn't write.
- Classic examples of senders who might prefer to disguise the source of the e-mail include a sender reporting mistreatment by a spouse to a welfare agency.

E-Mail Spoofing

- Although most spoofed e-mail falls into the "nuisance" category and requires little action other than deletion, the more malicious varieties can cause serious problems and security risks.
- For example, spoofed e-mail may purport to be from someone in a position of authority, asking for sensitive data, such as passwords, credit card numbers, or other personal information -- any of which can be used for a variety of criminal purposes.
- The Bank of America, eBay, and Wells Fargo are among the companies recently spoofed in mass spam mailings.
- One type of e-mail spoofing, self-sending spam, involves messages that appear to be both to and from the recipient.

Spamming

- People who create electronic spam : **spammers**
- **Spam** is abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately
- Spamming may be
 - E-Mail Spam
 - Instant messaging spam
 - Usenet group spam
 - Web search engine spam
 - Spam in blogs, wiki spam
 - Online classified ads spam
 - Mobile phone messaging spam
 - Internet forum spam
 - Junk fax spam
 - Social networking spam

.....

Spamming

- Spamming is difficult to control
- Advertisers have no operating costs beyond the management of their mailing lists
- It is difficult to hold senders accountable for their mass mailings
- Spammers are numerous

Search engine spamming

- Alteration or creation of a document with the intent to deceive an electronic catalog or a filing system
- some web authors use “subversive techniques” to ensure that their site appears more frequently or higher number in returned search results.
- remedy: permanently exclude from the search index

Avoid the following web publishing techniques:

- Repeating keywords
- Use of keywords that do not relate to the content on the site
- Use of fast meta refresh
 - change to the new page in few seconds.
- Redirection
- IP cloaking:
 - including related links, information, and terms.
- Use of colored text on the same color background
- Tiny text usage
- Duplication of pages with different URLs
- Hidden links

Internet Time Theft

- Occurs when an unauthorized person uses the Internet hours paid for by another person
- Comes under hacking
- The person get access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means
- And uses the internet without the other person's knowledge
- This theft can be identified when Internet time is recharged often, despite infrequent usage.
- This comes under “identity theft”



Salami attack/ salami technique

- Are used for committing financial crimes.
- The alterations made are so insignificant that in a single case it would go completely unnoticed.
- Example: a bank employee inserts a program, into the bank's serve, that deduces a small amount from the account of every customer every month,
- The unauthorised debit goes unnoticed by the customers, but the employee will make a sizable amount every month.


Salami attack: real life examples

- Small “shavings” for Big gains!
- The petrol pump fraud

Data diddling



- Data diddling involves changing data input in a computer.
- In other words, information is changed from the way it should be entered by a person typing in the data.
- Usually, a virus that changes data or a programmer of the database or application has pre-programmed it to be changed.
- For example, a person entering accounting may change data to show their account, or that or a friend or family member, is paid in full. By changing or failing to enter the information, they are able to steal from the company.

- 
- To deal with this type of crime, a company must implement policies and internal controls.
 - This may include performing regular audits, using software with built-in features to combat such problems, and supervising employees.

Hacking

Every act committed toward breaking into a computer and/ or network is hacking.

Purpose

- Greed
- Power
- Publicity
- Revenge
- Adventure
- Desire to access forbidden information
- Destructive mindset

History of hacking

- *hacking* is any technical effort to manipulate the normal behavior of network connections and connected systems.
- A *hacker* is any person engaged in hacking.
- The term "hacking" historically referred to constructive, clever technical work that was not necessarily related to computer systems.
- M.I.T. engineers in the 1950s and 1960s first popularized the term and concept of hacking.
- the so-called "hacks" perpetrated by these hackers were intended to be harmless technical experiments and fun learning activities.
- Later, outside of M.I.T., others began applying the term to less honorable pursuits. for example, several hackers in the U.S. experimented with methods to modify telephones for making free long-distance calls over the phone network illegally.
- As computer networking and the Internet exploded in popularity, data networks became by far the most common target of hackers and hacking.

Hacking vs. Cracking

- Malicious attacks on computer networks are officially known as *cracking* ,
- while *hacking* truly applies only to activities having good intentions.
- Most non-technical people fail to make this distinction, however.
- Outside of academia, its extremely common to see the term "hack" misused and be applied to cracks as well.

Online frauds



- Fraud that is committed using the internet is “online fraud.” Online fraud can involve financial fraud and identity theft.
- Online fraud comes in many forms.
 - viruses that attack computers with the goal of retrieving personal information, to email schemes that lure victims into wiring money to fraudulent sources,
 - “phishing” emails that purport to be from official entities (such as banks or the Internal Revenue Service) that solicit personal information from victims to be used to commit identity theft,
 - to fraud on online auction sites (such as Ebay) where perpetrators sell fictional goods.
 - E-Mail spoofing to make the user to enter the personal information : financial fraud
 - Illegal intrusion: log-in to a computer illegally by having previously obtained actual password. Creates a new identity fooling the computer that the hacker is the genuine operator. Hacker commits innumerable number of frauds.



E-mail bombing/mail bombs

- In Internet usage, an *email bomb* is a form of net abuse consisting of sending huge volumes of *email* to an address in an attempt to overflow the mailbox or overwhelm the server where the *email* address is hosted in a denial-of-service attack.
- Construct a computer to repeatedly send E-mail to a specified person's E-mail address.
- Can overwhelm the recipient's personal account and potentially shut down the entire system.





Computer network intrusions

- An intrusion to computer network from any where in the world and steal data, plant viruses, create backdoors, insert trojan horse or change passwords and user names.
- An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.
- The practice of strong password

Password sniffing

- Password sniffers are programs that monitor and record the name and password of network users as they login, jeopardizing security at a site.
- through sniffers installed, anyone can impersonate an authorized user and login to access restricted documents.



Credit card frauds



- **Credit card fraud** is a wide-ranging term for theft and fraud committed using or involving a payment card, such as a credit card or debit card, as a fraudulent source of funds in a transaction.
- The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account.
- Credit card fraud is also an adjunct to identity theft.