Information Security

Dr. Rakesh Singhal

Information Security?

Information?

- **Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected.**

Information security?

- **Protecting information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities.**

Information Security

We are building our lives around our wired and wireless networks. The question is, are we ready to work together to defend them?

Internet

The Internet is a collection of inter-connected computer networks and other devices spanning across the globe which are able to communicate with each other.

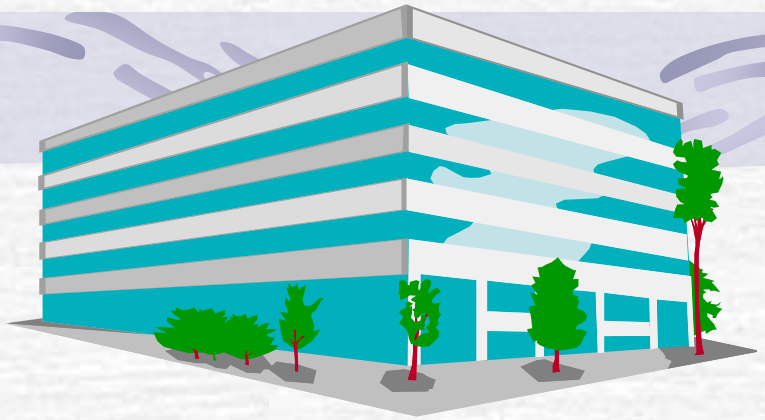
Your Greatest Strength is Your Greatest Weakness

- Everyone is using to computer/ Laptop/ PDA/ SMART Phone
- You are now connected with others through a modem or LAN
- You now have international presence
- Geographical boundaries are almost non-existing
- You have access to your partners system (and they have access to yours; and so do their other partners and so on i.e. you and your partners now collaborate through computers)
- Your entire business is through internet
- Your employees can work from home, at night, over the weekends, and on holidays or even while on the move..
- Your application server can support entire divisions
- BUT AT WHAT COST

In the ever changing technological environment today's state of the art security may be obsolete tomorrow.

Keep pace with the change

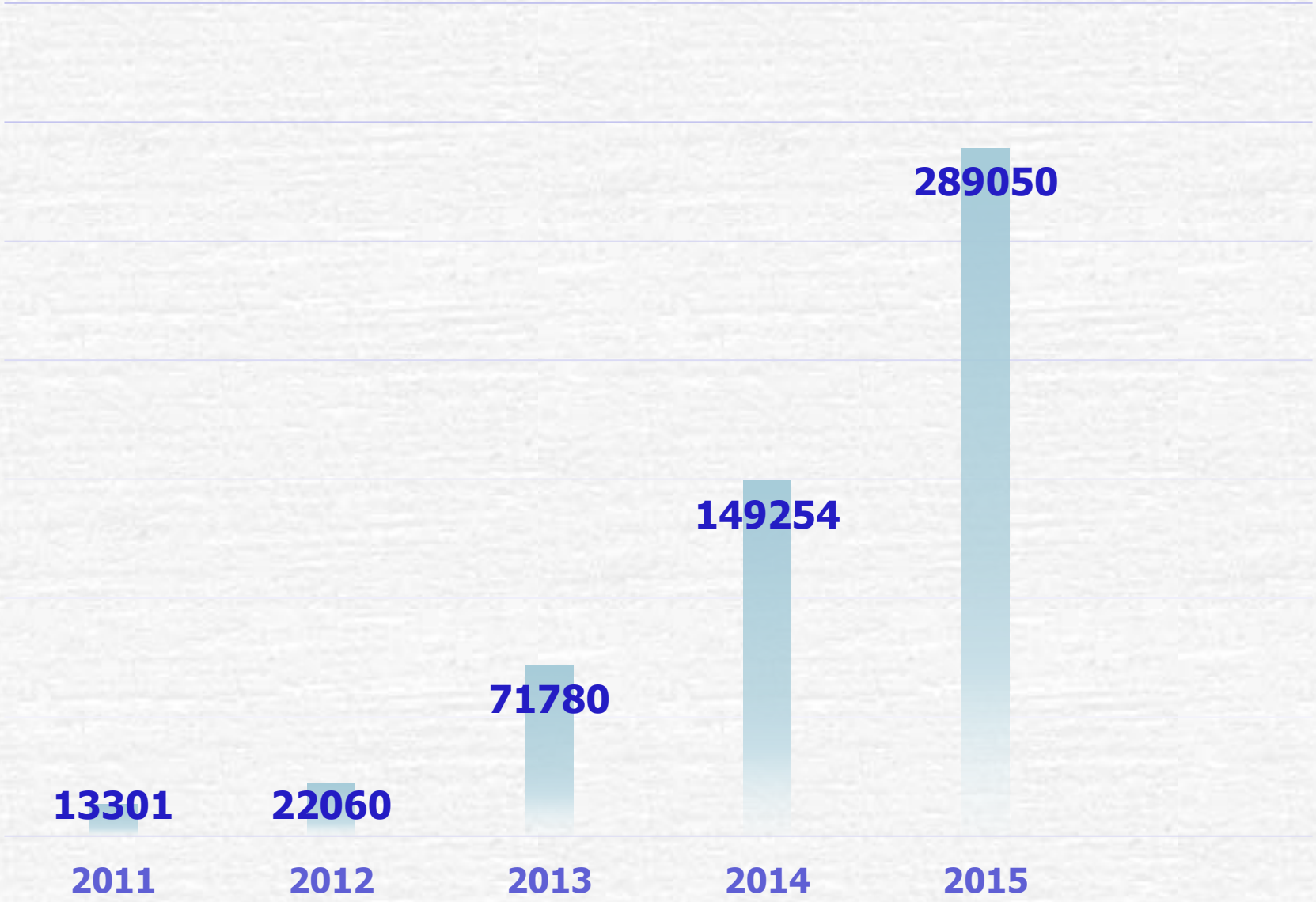
Information Security – General trends



Fortune 1,000 firms are spending less on security than they spend on coffee and soft drinks.

Forrester Research, Inc.

Reported Cyber Crime in INDIA



What is Security

- **Protecting the interests of those relying on information, systems and communications that deliver the information, resulting from failures of**
  - **Confidentiality – Is information available only to those who are authorized to access it**
  - **Integrity – Is information sufficiently right for the purpose at the time of use**
  - **Availability – Is information available wherever and whenever required by authorized persons**

Organizations are highly dependent on information systems to obtain business and deliver products/services thus, it is important that your clients/ customers/ business partners trust you…

If you do not , consequences of Security Breach

- ✓ Loss of time in recovering from problem - Minor or Major
- ✓ Corruption/ loss of integrity in data
- ✓ Decrease in Productivity
- ✓ Physical damage /theft
- ✓ Leakage of confidential information
- ✓ Significant loss of money or staff time
- ✓ Devastating loss of credibility or market opportunity
- ✓ Business no longer able to compete
- ✓ Legal Liability
- ✓ Loss of life

Many More….

This consequences could be caused due to intentional efforts of someone

Cyber Crime

- All crimes performed or resorted to by misuse of electronic media or otherwise, with the purpose of influencing the functioning of computer (Laptop/ PDA/ Mobile or any other such device), network or information system
- Thus Computer Crime is any crime where
  - Computer is a target
  - Computer is a tool of crime
  - Computer is incidental to crime

Who is Cyber Criminal ?

A 5th class student who know how to use FACEBOOK

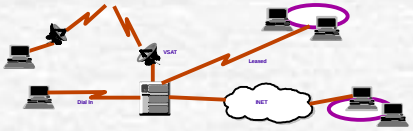
SHOKED !!!

But its truth anyone can be a cyber criminal . Child to aged anyone can be ..

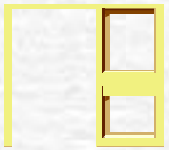
Most of them are :

1. **Disgruntled employees**
2. **Teenagers**
3. **Boyfriend/ ex Boyfriend**
4. **Girlfriend / ex Girlfriend**
5. **Professional Hacker**
6. **Divorced Husband**

Security Threats and Risks



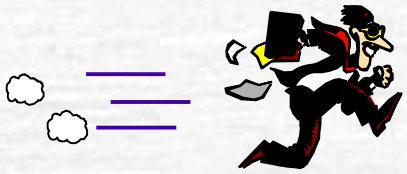
Systems / Network Failure



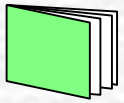
Unauthorized/ Unrestricted Access

Software Version Problems/ Piracy/ Vulnerability

Virus/ Spy ware/ spam



Theft of data, Message Alteration, Misuse,



Lack of documentation

Hacking/ Phishing/ click fraud

Denial of Service

Web Defacement

Natural Disasters

Floods

Fire

Obscene or Offensive Content

Online Fraud

Net Extortion

Virus

Malicious software that attaches itself to other software. (virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are the malicious

Browser

Browser is a application and software use to open Web pages that written in specify language. Most of them are :

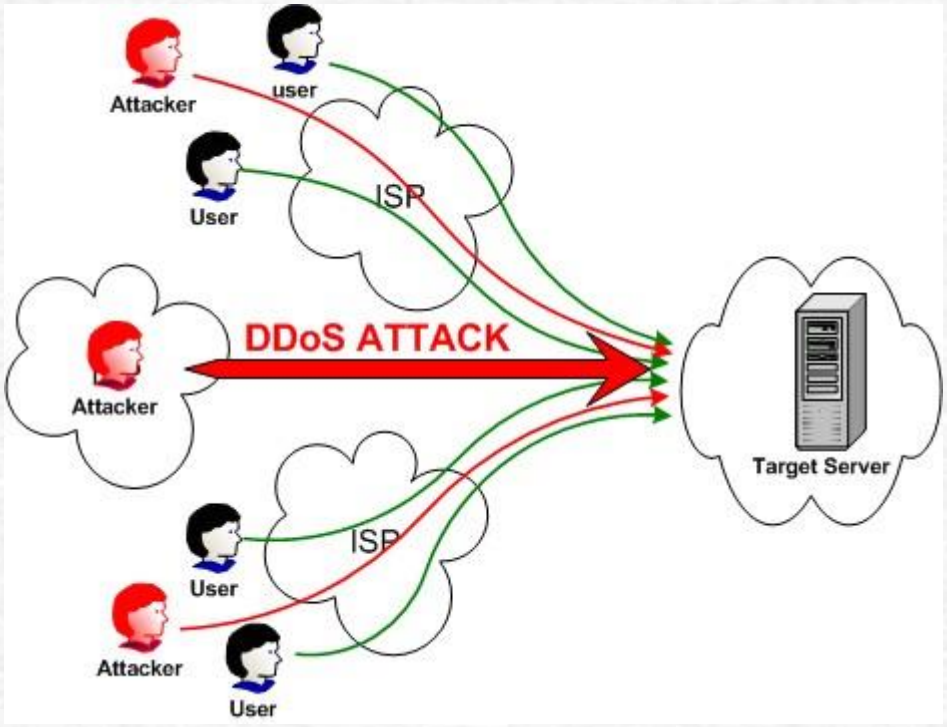
1. Internet explorer
2. Firefox
3. Opera etc..

Also browser man tasks are :
Save cookies
save history
save passwords

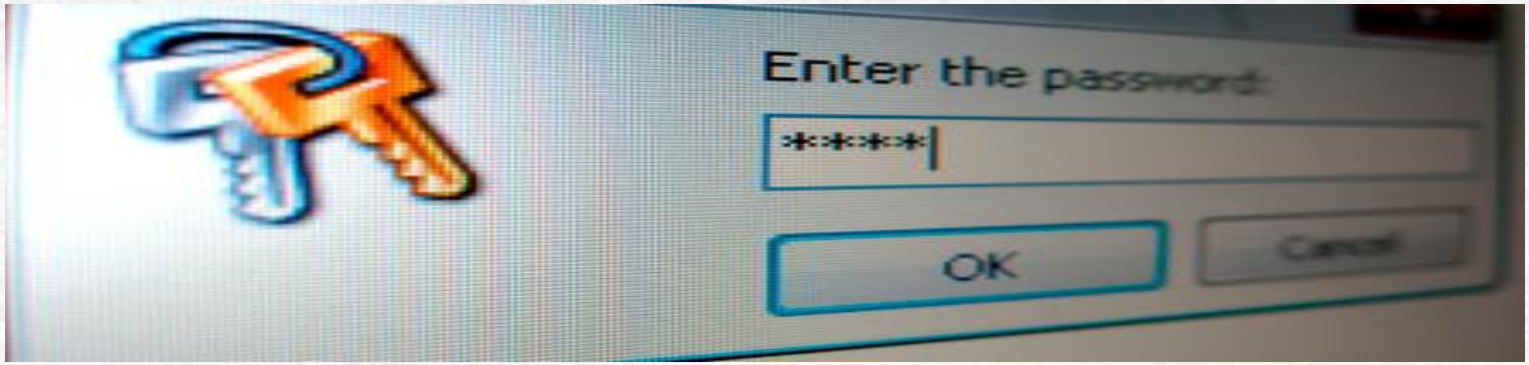
So it is need to sure that Clear all data.
(ctrl + shift +del)

Dos Attack

Act by the criminal, who floods the bandwidth of the victim's network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide

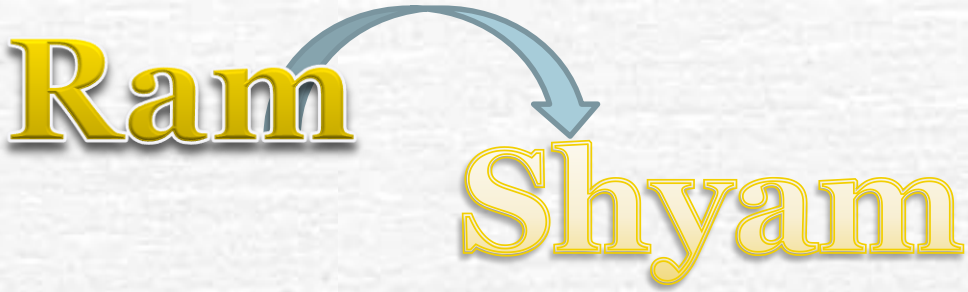


Hacking



Hacking is a unauthorized access of computer or network

Data Diddling



Tampering OR Alteration of data without permission of owner comes under DATA DIDDLING

Net Extortion

Intimidation and extortion scams use demands for money or property through undue exercise of authority, including threats of physical harm, criminal prosecution, or public exposure.

Like :

Copying the company's confidential data in order to extort said company for huge amount

Web Defacement

Is it next world war ? Would call !!! CYBER WAR !!!

Online Fraud

Any type of fraud like :
Nigerian scam, online betting on games, Chain systems, Fake Consultancy to gather money, Abuse services Etc. comes under subject of Online Fraud.

Software Piracy

Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.

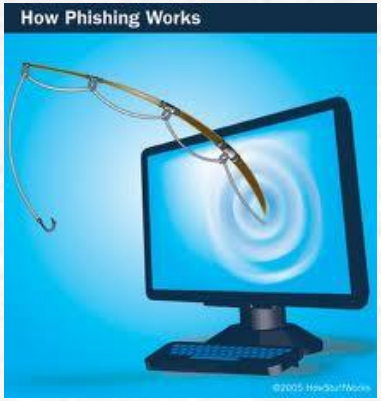
Spoofing

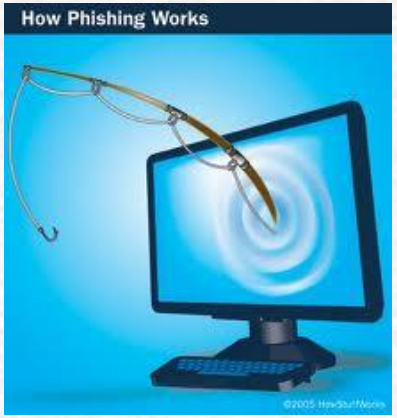
Using someone's Identity without his/her permission in technically called as SPOOFING.

Like :

1. **Call spoof -Making calls to any number using any number.**
2. **SMS spoof -SMS to any number using any number.**
3. **Email spoof - Sending Email from any email address.**

Phishing





The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has.

TECHNOLOGIES AND TOOLS FOR SECURITY

Whose Responsibility is to secure?

- ✓ It is YOUR responsibility to protect Personal Information from …
  - ✓ Theft
  - ✓ Loss
  - ✓ unauthorized Access
  - ✓ unauthorized Copying
  - ✓ unauthorized Use

  - ✓ This applies to both Paper & Computer documents

PASSWORD

A password like a key of digital lock. And a secret word or string of characters that is used for user authentication to prove identity,

Good passwords :
1. lower and upper case Character
2. Numeric digits
3. special character
4. minimum 8 digit
Ex: pAss@123

Bad password :
1. Your mobile number
2. date of birth etc..

Actions for users

- Awareness! Awareness! Awareness!
  - Have your own policy
  - Install and enable :
    - Personal firewall
    - Anti-spyware
    - Anti-phishing controls
- Keep up-to-date patches and fixes on the operating system and application software
- Enable/Install anti phishing toolbars such as “Phishing Filter”, “Web Forgery” etc..
- Use latest Internet Browsers having capability to detect phishing/malicious sites.
- Exercise caution while opening unsolicited emails and do not click on a link embedded within
- Only open email attachments from trusted parties
- Practice limited account privilege.
- Report suspicious emails/system activities to CERT-In Incident Response Help Desk - Phone: 1800 11 4949, FAX: 1800 11 6969, e-mail: incident@cert-in.org.in http://www.cert-in.org.in

E-Mail Policy

- Users should update their profile and contact number, so that unauthorized activity can be reported to users on the updated number.
- Never auto save password in the browsers.
- Always use secure password (strong password) and change it frequently.
- Never share your personal information or password with anyone.
- Never exchange advertisements, solicitations, chain letters and other un official, e-mail from your mail id.
- Always use https instead of http
- Your password must be strong
- Don’t use easy answer for security question
- Don’t click any link from unwanted mails
- Never use or attempt to use account of others without their permission.
- Always take backup of your important files.
- Be cautious while using “reply to all” or “distribution list” on mail.

Computer security

To secure Your Computer ensure following :

- **Use Genuine windows – Updates/ Patches**
- **Use updated and registered antivirus.**
- **Backup your important data always in external drive.**
- **Always scan first your pen drive before using it**
- **Ensure your wireless router is protected with password**
- **Make your system password protected .**

Access Control

Only Authorized persons are able to access the system

- **Password**
- **Virtual Keyboard**
- **OTP/ Token** - physical device that is designed to prove the identity of a single user
- **Smart Card** - contains a chip formatted with access permission and other data.
- **Biometric authentication**
  - Finger Print/ facial expression/ retina/ voice recognition/ hand geometry

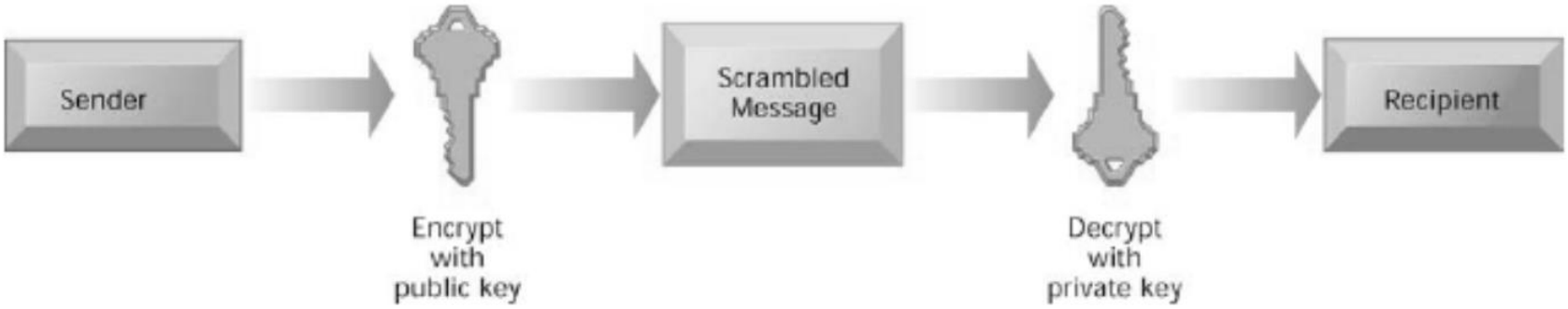
Software Tools

- **Antivirus Software**
- **Firewalls –** Tries to stop outsiders to get into the network
- **Intrusion Detection Systems -** track the hacker attempts
- **Network Security Tools**

Encryption and Digital Signature

- Most people are reluctant to buy and sell on the Internet because they're afraid of theft, fraud, and interception of transactions
- **Digital signature** software can create a method of verifying that the message, document, or file has not been altered between the time it left the sender and you received it

FIGURE 8-7 PUBLIC KEY ENCRYPTION



Security Policy

- Principle document that determines security goals and how they will be achieved
  - **Acceptable user policy (AUP):** outlines acceptable and unacceptable uses of hardware and telecommunications equipment
  - **Authorization policy:** determines what access users may have to information resources
  - **Authorization management systems:** manages access to each part of the information system.

User Awareness Program

- User training
- Importance of information Security
- Dos and Don’ts

Ensuring Business Continuity

- **Backup**
- **Fault-tolerant computer systems -** promise continuous availability and eliminate recovery time altogether.

- **High-availability computer systems** - help firms recover quickly from a crash
  - **load balancing**
  - **redundant servers**
  - **mirroring**
  - **storage area networks**
  - **disaster recovery plan**
  - **recovery-oriented computing**

Risk Assessment

determine weak links in their information system

- Computers
- Users
- Network
- Internet Access.
- Data Bank

Final Message

"Failure is not when you fall down, but when you fail to get up"