D Y PATIL INTERNATIONAL UNIVERSITY
AKURDI PUNE

MCAICS 302

Applications of AI in cyber security

By Sarika Jadhav

D Y PATIL INTERNATIONAL UNIVERSITY
AKURDI PUNE

Unit I Fundamentals of AI and CS

1.1 Introduction: Security measures in Computing

1.1.1 Elements, attributes

1.1.2 Types of Cyber Crimes and Criminals

1.1.3 Basic Security Terminology

1.1.4 Threats and Vulnerability

1.2 Machine Learning Algorithms and usage

1.3 Impact of AI on Cybersecurity

1.4 AI Applications in Cybersecurity: Real-Life Examples

1.4.1 Security screening
1.4.2 Security & crime prevention
1.4.3 Analyze mobile endpoints
1.4.4 AI-powered threat detection
1.4.5 Detection of sophisticated cyber-attacks
1.4.6 Reducing Threat Response Time

1.5 Drawbacks and Limitations of Using AI for Cybersecurity

D Y PATIL INTERNATIONAL UNIVERSITY
AKURDI PUNE

Reason behind Cyber / Information Security

- Major issues are hacking, viruses, worms, Trojans, spoofing, sniffing, denial of services, spay, malware, mobile malware, crypto virology etc.

- Attackers take advantage of security gaps to gain access to a computer system without owner's awareness, making the computer system not working properly, changing source/destination of IP address packet to show that it originates from a legitimate source

- To protect information, techniques, methods, and advices that can be found on information security……
  such as anti-virus, anti-spyware, software, Windows and applications updates, firewalls, content filtering/parental control, smart encryption codes etc.

Cybersecurity

Two parts :

1. Cyber
2. security.

Cyber refers to the technology that includes systems, networks, programs, and data.

Security is concerned with the protection of systems, networks, applications, and information.

Cybersecurity is the **practice of protecting systems, networks, and programs from digital attacks**.

- Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

- It's also known as information technology security or electronic information security.

- A strong cybersecurity strategy has layers of protection to defend against cybercrime, including cyber attacks that attempt to access, change, or destroy data; extort money from users or the organization, or aim to disrupt normal business operations.

    - Cyber security industry is primarily focused on protecting devices and systems from attackers.

How to manage information security

- To protect information Companies, organizations or individuals should give the importance to actions, plans, policies, proved objectives, self-hacking-audit, training and awareness activities.

- To manage Information Security standards (rules, strategies and best practices) are:

  - ISO/IEC 27001 Information Security Management System
  - ISO/IEC 15408 Evaluation Criteria for IT Security
  - ISO/IEC 13335IT Security Management for technical security control
  - ISO 29100 Privacy Framework
  - ISO 80001 Risk Management for IT-networks incorporating medical devices etc.

D Y PATIL INTERNATIONAL UNIVERSITY
AKURDI PUNE

Information System and Information System Security

- **Data: Unorganized** raw facts, data are a set of values of qualitative or quantitative variables about one or more persons or objects, while a datum is a single value of a single variable.
  - Alphanumeric, image, audio, and video
- **Information:** processed, organized **data** presented in a given context and is useful to humans that they have additional value beyond the value of the facts themselves
- An *Information System* is a set of interrelated components that collect or retrieve, process, store and distribute information to support decision making and control in an organization.

Information System examples

- Most common types of information systems used in business organizations
- Electronic and mobile commerce systems : any business transaction executed electronically between parties
  - Transaction processing systems:

  Payments to employees
  - Sales to customers
  - Payments to suppliers
  - Management information systems
  - Decision support systems
  - Specialized business information systems

D Y PATIL INTERNATIONAL UNIVERSITY
AKURDI PUNE

Basics of Information System

- In the past decade, the nature of IS has undergone a great change, from Mainframe based IS to Client /Server to today's Web based information system.
- Information Systems today are distributed and component based.
- Wide spread of internet and increase in bandwidth helped development of Global Information Systems.

D Y PATIL INTERNATIONAL UNIVERSITY
AKURDI PUNE

Information System Security

- Today most of the IS are connected to internet.
- Thus they are exposed to the outside world directly.
- Threats from the outside world must be addressed.
- Damage from a non-secure IS can result in catastrophic consequences for the organization.
- Thus organizations must investigate and evaluate the factors that could be a threat.

What Is Information Security???

Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of the service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

Why Information Security?

- **Web site defacement** : Defacing a website means replacing the webpage (index.html file) of a site with hackers file.

- **Theft of confidential data** : Data theft is the act of stealing virtual information with an intent to compromise someone's privacy or to obtain confidential information.

- **Financial Frauds**: Financial fraud occurs when someone takes money or other assets from you through deception or criminal activity.

- **Legal requirements**: Implement appropriate security measures to protect personal data.

Why Information Security?

- **Cross Site Scripting (XSS)** : Process of addition of malicious code to a genuine website to gather user's information with a malicious intent.
- **SPAM**: Use of electronic messaging systems to send out unrequested or unwanted messages in bulk.
- **Denial Of Service (DOS)/ DDOS**: Multiple compromised systems are used to target a single system.
- **Virus / Worms/ Trojans**:

Virus: A computer virus is a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another.

Types: Boot sector virus, Web scripting virus, Browser hijacker, Resident virus, Direct action virus, Polymorphic virus, File infector virus, Multipartite virus, Macro virus

Why Information Security?

- **Worm:** A computer worm is self-replicating malware that duplicates itself to spread to uninfected computers

Ex: Stuxnet virus

- **Trojan**: A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer.

Types: Backdoor Trojan, Distributed Denial of Service (DDoS) attack Trojan, Downloader Trojan, Fake AV Trojan, Game-thief Trojan, Infostealer Trojan, Mailfinder Trojan, Ransom Trojan, Remote Access Trojan, Rootkit Trojan, SMS Trojan, Trojan banker, Trojan IM

Why Information Security?

- **Spyware / Adware:** Adware and spyware are both forms of malware that can infect your computer without your knowledge.

- **Phishing** : **Phishing** attack is a process of creating a duplicate copy or a clone of a reputed website in the intention of stealing user's password or other sensitive information like credit card details.

- **Spoofing**: Type of scam in which criminals attempt to obtain someone's personal information by pretending to be a legitimate business, a neighbor, or some other innocent party.

- Crime …….. Etc.

Elements of Information Security

- Three basic elements of Information Security.

1. **Confidentiality:** Data is confidential when only those people who are authorized to access it can do so

2. **Integrity:** maintaining data in its correct state and preventing it from being improperly modified

3. **Availability: I**nformation must be available when needed

Elements of Information Security

4. Authenticity : Authenticity refers to the characteristic of a communication, document, or any data that ensures the quality of being genuine or corrupted. The major role of authentication is to confirm that a user is genuine, one who he / she claims to be.

5. Non-Repudiation: Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message, and that the recipient cannot deny having received the message. Individuals and organization use digital signatures to ensure non-repudiation.

Attributes of Information Security

1. **Data Confidentiality :** The system and associated processes shall be designed, implemented, operated and maintained so as to prevent unauthorized access

1. **Authenticity**: It shall be possible to verify the authenticity of inputs to and outputs from the system, its state and any associated processes. It shall also be possible to verify the authenticity of components, software and data used within the system and any associated processes.

Attributes of Information Security

3. Possession and/or Access Control:
The system and associated processes shall be designed, implemented, operated and maintained so as to prevent unauthorized control, manipulation or interference.

4. Integrity – the system and associated processes shall be designed, implemented, operated and maintained so as to prevent unauthorised changes being made to assets, processes, system state or the system itself.

5. Availability – The system and associated processes shall be consistently accessible in an appropriate and timely manner.

6. Utility – The system and associated processes shall be designed, implemented, operated and maintained so that the utility of their assets is maintained throughout their life cycle.

7. Safety – The design, implementation, operation and maintenance of the system and associated processes shall not put at risk the health and safety of individuals, the environment or any associated assets.

- Crimes
- Types of Cyber Crimes
- Criminals

Cyber crime

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device.

Cyber crime is defined as criminal activity involving the IT infrastructure, including illegal access, illegal interception, data interference, misuse of devices, ID theft and electronic fraud.

Cybercrime, especially involving the Internet, represents an extension of existing criminal behavior alongside some novel illegal activities.

Types of Cyber Crimes

1. Hacking
2. Salami Attack
3. Malware dissemination
4. Software Piracy
5. Forgery
6. Obscene or Offensive Content
7. Pornography
8. Cyber Sex
9. Fraud
10. Phishing
11. Spoofing
12. Spam
13. Denial of Service
14. Threatening
15. Net Extortion
16. Cyber Terrorism
17. Drug Trafficking
18. Cyber Warfare
19. Cyber Stalking
20. Cyber Defamation
21. IRC Crime

Types of Cyber Crime

1. **Hacking :** Hacking is an act committed by an intruder by accessing your computer system without your permission.

2. **Salami Attack**: A “salami slicing attack” or “salami fraud” is a technique by which cyber-criminals steal money or resources a bit at a time so that there’s no noticeable difference in overall size.

3. Malware Dissemination: Worms/Viruses are computer programs that attach themselves to or infect a system or files, and have a tendency to circulate to other computers on a network.

Types of Cyber Crime

4. Software Piracy: Software piracy is the unauthorized use and distribution of computer software.

The following constitute software piracy:

- Loading unlicensed software on your PC
- Using single-licensed software on multiple computers
- Using a key generator to avoid copy protection
- Distributing a licensed or unlicensed ("cracked") version of software over the internet and offline

Types of Cyber Crime

5. Forgery :

Forgery is a white-collar crime that generally refers to the false making or material alteration of a legal instrument with the specific intent to defraud anyone

It involves a false document, signature, or other imitation of an object of value used with the intent to deceive another.

6. Offensive Content: This cybercrime involves criminals sharing and distributing inappropriate content that can be considered highly distressing and offensive.

Types of Cyber Crime

7. **Pornography:**

Child pornography is a form of child sexual exploitation

8. Cyber sex: Cybersex crimes occur when the person either trades, distributes, purchases, downloads or interacts with others to send or receive child pornography or to solicit sex with another person

9. **Fraud**: ATM Frauds and others

Types of Cyber Crime

9. **DDoS Attacks**: Used to make an online service unavailable and take the network down by overwhelming the site with traffic from a variety of sources

10. Botnets: Botnets are networks from compromised computers that are controlled externally by remote hackers.

11. Identity Theft: Identity theft occurs when someone steals your identity and pretends to be you to access resources such as credit cards, bank accounts and other benefits in your name.

12. Cyber stalking: This kind of cybercrime involves online harassment where the user is subjected to a plethora of online messages and emails.

Types of Cyber Crime

13. Social Engineering : Social engineering involves criminals making direct contact with you usually by phone or email and gain your confidence and usually pose as a customer service agent so you'll give the necessary information needed.

14. PUPs: PUPS or Potentially Unwanted Programs are a type of malware. They uninstall necessary software in your system.

15. Phishing: This type of attack involves hackers sending malicious email attachments or URLs to users to gain access to their accounts or computer.

16. Online Scams: Criminals promises of rewards or offers of unrealistic amounts of money through ads or spam emails.

17. Exploit Kits: Kits are readymade tools criminals can buy online and use against anyone with a computer.

Types of Cyber Crime

18. **Web jacking or Hijacking**: Hacker takes control of a web site fraudulently and may change the content of the original site or even redirect the user to another fake similar looking page controlled by him.

19. **Logic bombs** : It is a malicious piece of code which is intentionally inserted into software to execute a malicious task when triggered by a specific event. Logic bombs are usually employed by disgruntled employees working in the IT sector.

20. **Data diddling**

Data Diddling is unauthorised altering of data before or during entry into a computer system, and then changing it back after processing is done.

5 Types of Cyber Criminals

The
Social Engineer

The
Spear Phisher

The Hacker

The
Rogue Employee

The
Ransom Artist

1. Hackers:

- It typically refers to an individual who uses his or her skills to achieve unauthorized access to systems or networks so as to commit crimes.

- The intent of the burglary determines the classification of those attackers as white, gray, or black hats.

(a) **White Hat Hackers** –
These hackers utilize their programming aptitudes for good and lawful reasons.
They may perform network penetration tests in an attempt to compromise networks to discover network vulnerabilities.
Security vulnerabilities are then reported to developers to fix them.

(b) **Gray Hat Hackers** –
These hackers carry out violations and do seemingly deceptive things however not for individual addition or to cause harm.

(c) **Black Hat Hackers** –
These hackers are unethical criminals who violate network security for personal gain.
They misuse vulnerabilities to bargain PC frameworks.

2. Organized Hackers

Cybercriminals are typically teams of skilled criminals targeted on control, power, and wealth. These criminals are extremely subtle and organized, and should even give crime as a service.

- These attackers are usually profoundly prepared and well-funded.

3. **Internet stalkers**:

- Internet stalkers are people who maliciously monitor the web activity of their victims to acquire personal data.

- This is conducted through the use of social networking platforms and malware, that are able to track an individual's PC activity with little or no detection.

4. Disgruntled Employees

Disgruntled employees become hackers with a particular motive and also commit cyber crimes.
It is simple for disgruntled employees to do more damage to their employers and organization by committing cyber crimes.

5. Social engineer:

A social engineer finds out everything they about an individual or a business.
This could be through the means of social media or finding the target's data online.

6. Spear phisher:

spear phishing is a targeted form of phishing in which fraudulent emails target specific organizations in an effort to gain access to confidential information.
Spear phishing focuses on specific individuals or employees within an organization and social media accounts such as Twitter, Facebook, and LinkedIn to specifically customize accurate and compelling emails.

Basic Security Terminology

Attack:
Availability of Data:
Brute Force Attack:
Confidentiality of Data:
Countermeasures:
Cracker:
Crash:
Defense in Depth:
DoS Attack:
Explosure:
Hacker:
Integrity of Data:

Basic Security Terminology

D Y PATIL INTERNATIONAL UNIVERSITY
AKURDI PUNE

Least Privileges:
Malicious Code:
Buffer:
Buffer overflow:
Reliability:
Risk:
Sniffer:
Social Engineering:
Treat:
Trojan Horse:
Virus:
Worms:

Non malicious Program Errors

- Intentional
  - Malicious
  - Nonmalicious
- Inadvertent
  - Validation error (incomplete / inconsistent) : permission checks
  - Domain error : controlled access to data
  - Serialization and aliasing: program flow order
  - Inadequate identification and authentication : basis for authorization
  - Boundary condition violation : failure on first and last case
  - Other exploitable logic errors

Non malicious Program Errors

- Most of the mistakes made by the programmers are unintentional and non malicious.
- Many such errors will not lead to more serious vulnerabilities but few will put many security professionals in trouble.
- We look at three such classic error types and explain why they are relevant to security and how can they be prevented.

Buffer overflows

- Its like pouring 2 liters of water into a 1 liter jug.
- **Definition**
  - A buffer is a space in memory in which data is held.
  - As memory in finite => buffer capacity is finite
    - Therefore, in programming languages the programmer must declare the buffers maximum size.

```
char sample[10];
// compiler sets 10 bytes to store this buffer.


sample[10]='B';
// out of bounds error, compiler detects this during compilation.
```

Now, what if we do

```
sample[i]='B';
```

In some programming languages, buffer sizes need not be predefined.

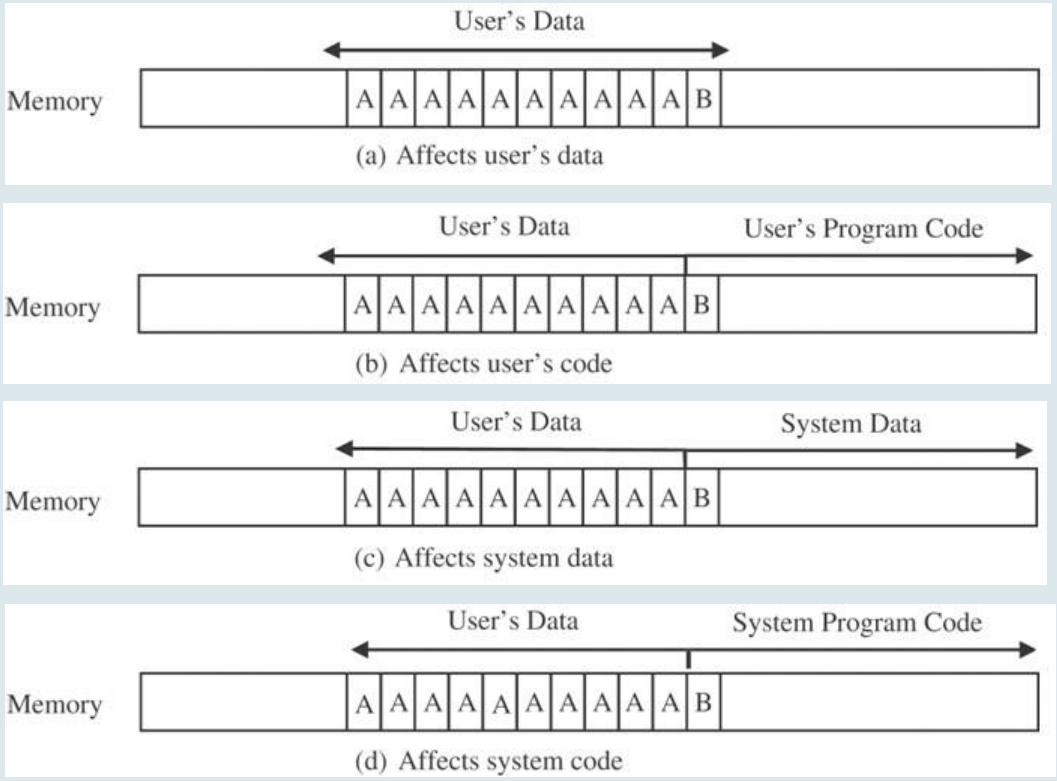
- C does *not* perform array bounds checking.
- Similar problem caused by pointers
  - No reasonable way to define limits for pointers

- Where does ‘B’ go?

- Depends on what is adjacent to ‘sample[10]’

  - Affects user’s data - overwrites user’s data
  - Affects users code - changes user’s instruction
  - Affects OS data - overwrites OS data
  - Affects OS code - changes OS instruction

Buffer overflows



- Implications of buffer overflow:
  - Attacker can insert malicious data values/instruction codes into "overflow space"
- Buffer overflow affects OS code area
  - Attacker code executed as if it were OS code
    - An attacker might need to experiment to see what happens when he inserts **B** into OS code area
  - Can raise attacker's privileges (to OS privilege level)
    - When **B** is an appropriate instruction
  - An attacker can gain full control of OS

- Buffer overflow affects a call stack area

A scenario:

- Stack: [data][data][...]

- Pgm executes a subroutine
  => return address pushed onto stack
  (so sub-routine knows where to return control to when finished)
  Stack: [ret_addr][data][data][...]

- Subroutine allocates dynamic buffer char sample[10]
  => buffer (10 empty spaces) pushed onto stack
  Stack: [.....][ret_addr][data][data][...]

- Subroutine executes: sample[i] = 'A' for i = 10
  Stack: [.....][A][data][data][...]
  Note: ret_address overwritten by **B**!
  (Assume: size of ret_address is 1 char)

- Buffer overflow affects a call stack area
  Stack: [.....][A][data][data][...]

- Subroutine finishes
  - Buffer for char sample[10] is de-allocated
    Stack: [A][data][data][...]

  - RET operation pops **B** from stack (considers it ret. addr)
    Stack: [data][data][...]

  - Pgm (which called the subroutine) jumps to **B**
    => shifts program control to where attacker wanted

Buffer overflows- security implication

- Even if the flaw came from a honest mistake, the flaw can still cause great harm. A malicious attacker can exploit these flaws.

- Web server attack similar to buffer overflow attack: pass a very long string to a web server
- Buffer overflows are still common
  - Used by attackers
    - to crash systems
    - to exploit systems by taking over control
  - A large number of vulnerabilities due to buffer overflows still persists in many software and systems

Web server attack example

- Parameter passing in the URL:

Consider:

http://www.somesite.com/subpage/userinput.asp?param1=(808)555-1212&param2=2009Jan17

What can be the possible attack on this URL?

Passing a very long string is a slight variation on the classic buffer overflow, but no less effective.

Incomplete mediation

- Consider the same previous example

http://www.somesite.com/subpage/userinput.asp?param1=(808)555-1212&param2=2009Jan17

What happens if we pass values like 1800Jan01 or 1800Feb30 or 2048Min32 or 1Aardvark2Many?

1. Data type error
2. Continue to execute but end up with a wrong result

What if we do all the validations properly on the client browser?

Incomplete mediation

Mediation means checking: the process of intervening to confirm an actor's authorization before it takes an intended action.

Thus verifying that an actor is authorized to perform the operation on an object.

Incomplete mediation is a security problem e.g. Data is validated and incorrect input is captured by users resulting in errors

Incomplete mediation occurs when the app accepts incorrect data from the user

Need to know that any user input falls within specified values

- Unchecked data values represent a serious potential vulnerability.
- Example: A firm named “Things” started an e-commerce site to sell its products.
- Once a person places his order the return URL is as follows:

http://www.things.com/order.asp?custID=101&part=555A&qy=20&price=10&ship=boat&shipcost=5&total=205

If you’re a malicious attacker, what will you do?

A serious concern about this flaw was the length of time it could have run undetected.

Time of check to Time of use errors

- Unintentional but with serious security consequences.
- Modern processors and OS usually change the order in which the instructions and procedures are executed.
- Adjacent instructions may not even execute in the same order.
- Time-of-check to time-of-use (TOCTTOU) flaw is performed by “bait and switch” strategy.
- Also called a synchronization or serialization flaw.
- It exploits the delay between the two times. That is, between the time the access was checked and the time the result of the check was used, a change occurred, invalidating the result of the check.
- Time-of-check to time-of-use flaw exploits the time lag between the time we check and the time we use.

Why Information Security?

- Increased rate of cyber crime issues.

- **Cyber crime** is defined as criminal activity involving the IT infrastructure, including illegal access, illegal interception, data interference, misuse of devices, ID theft and electronic fraud.

Cyber Crime Techniques

- Data Scavenging
- Shoulder Surfing
- Piggy Backing
- Man In the middle
- Social Engineering
- Buffer overruns
- SQL injections

D Y PATIL INTERNATIONAL UNIVERSITY
AKURDI PUNE

Why Information Security???

- Cookies
- Cross Site Scripting (XSS)
- SPAM
- Denial Of Service (DOS)/ DDOS
- Virus / Worms/ Trojans
- Spyware / Adware
- Phising
- Spoofing …….. Etc.

Confidentiality

- It is the principle that information will not be disclosed to unauthorized subjects.

- Examples:
- Unauthorized network data sniffing
- Listening a phone conversation.

Integrity

- It is the protection of system information or process from intentional or accidental unauthorized changes.

Availability

- It defines that information or resources are available when required.

Information Security

- In another words …….

- **……Information security means making sure to provide required information for the correct people at the correct time.**

Other Elements of Information Security

- ***Identification*** – recognition of an entity by a system.
- ***Authentication***-Process of verifying identity.
- ***Accountability*** –Tracing activities of individual on a system.
- ***Authorization***- Granting access or other permissions.
- ***Privacy***- Right of individual to control the sharing of information about him.

D Y PATIL INTERNATIONAL UNIVERSITY
AKURDI PUNE

How to achieve Information Security???

- Information Security does not mean only installing antivirus and firewalls.
- Information security tends to protect hardware, software, data, procedures, records, supplies and human resources.
- Information assets are those resources that store, transport, create, use or are information.

How to achieve Information Security???

- **Administrative Controls-** Policies, standards, procedures, guidelines, employee screening, change control, Security awareness trainings.

- **Technical Controls-** Access controls, encryption, Firewalls, IDS, IPS,HTTPS

- **Physical Controls-** controlled physical access to resources, monitoring, no USB or CDROM etc.

How to achieve Information Security???

- Information Security is the responsibility of everyone who can affect the security of a system.

D Y PATIL INTERNATIONAL UNIVERSITY
AKURDI PUNE

Some Good Habits

- Always use official software.
- Keep all software uptodate with patches.
- If using free software always download from original developers site.
- Do not disclose all your information on internet sites like orkut/Facebook.
- Use Internet with control.
- Use email properly.
- Take care while discarding your waste material.
- Use small gadgets carefully as information storage.
- Be careful while surfing from a cybercafe.

D Y PATIL INTERNATIONAL UNIVERSITY
AKURDI PUNE

Information System Security

- Threat
  - A threat is a possible event that can damage or harm an Information System.
- Vulnerability
  - It is the weakness within a system. It is the degree of exposure in view of threat.
- Countermeasures
  - It is a set of actions implemented to prevent threats.

Information System Security

- Network Level Threats
  - Attacker requires network access to organization systems or networks.
  - Hacking Computers, Implementing Spywares

- Information Level Threats

- Attack on the information.
  - Sending fake queries to sales department
  - Submitting false information.
  - Creating revenge web sites.

D Y PATIL INTERNATIONAL UNIVERSITY
AKURDI PUNE

Information System Security

- Major Security Threats to an IS
  - Computer Crimes / Abuse
  - Human Error
  - Failure of Hardware or Software
  - Natural Disasters
  - Political Disasters

D Y PATIL INTERNATIONAL UNIVERSITY
AKURDI PUNE

Information System Security

- Computer Crime / Abuse
- Computer Viruses
  - A code that performs malicious act.
  - Can insert itself into other programs in a system.
  - Worm is a virus that can replicate itself to other systems using network.
  - Biggest threat to personal computing.
- Trojan Horse
  - A program that performs malicious or unauthorized acts.
  - Distributed as a good program.
  - May be hidden within a good program.

Information System Security

- Denial of Service (DoS)
  - Making system unavailable to legitimate users.
- Impersonation
  - Assuming someone else's identity and enjoying his privileges.
- Salami Technique
  - Diverting small amount of money from a large number of accounts maintained by the system.
  - Small amounts go unnoticed.
- Spoofing
  - Configuring a computer to assume some other computers identity.

D Y PATIL INTERNATIONAL UNIVERSITY
AKURDI PUNE

Information System Security

- Scavenging
  - Unauthorized access to information by searching through the remains after a job is finished.
  - Dumpster diving
- Data Leakage
  - Various techniques are used to obtain stored data
  - SQL injection
  - Error Outputs
- Wiretapping
  - Tapping computer transmission lines to obtain data.
- Theft of Mobile Devices

D Y PATIL INTERNATIONAL UNIVERSITY
AKURDI PUNE

Information System Security

- Myths, rumors and hoaxes
  - Created by sending false emails to as many people as possible.
  - These may have significant impact on companies, their reputation and business.
- Web Site Attacks
  - Web site defacement
  - Adding wrong information
- Increase in cyber crime rates
  - Organized cyber criminals

D Y PATIL INTERNATIONAL UNIVERSITY
AKURDI PUNE

Information System Security

- Employee Issues
  - Disgruntle Employees
  - Availability of hacking tools
- Social Engineering Attacks
  - Sharing Passwords
  - Sharing Official Systems
  - Not following clean desk policy
- Rise in Mobile workers
  - Use mobile devices
  - Wireless access
  - Lots of organization data exposed

Classification of Threats

- Basic of the effective Security Management.
- Organization require to know the damage caused when security incident or an attack happens.
- This helps management to decide the budget for security related expenditures.
- Organizations can not secure everything.
- Organizations can not spend too much on security.

Threat & Vulnerability

- Threat
  - A threat is a possible event that can damage or harm an Information System.

- Vulnerability
  - It is the weakness within a system. It is the degree of exposure in view of threat.

Classification of Threats

- Four things to be considered while evaluating threat

- Asset
  - Something of value to the organization
- Actor / Attacker
  - Who or what may violate the security requirement
- Motive
  - Deliberate or accidental
- Access
  - How the attacker will access the asset.

Classification of Threats

- Types of assets
  - Hardware
  - Software
  - Information
  - Systems
  - People

Classification of Threats

- Classify Assets
- Tag Assets based on their value to the organization.
- Find various threats to important assets.
- Tag threats for an asset.
- Find the threats which have maximum risk.
- Calculate the loss due to these threats.

Classification of Threats

- Cost of a threat can be calculated considering following factors
  - Productivity
    - No. of employees affected
    - No. of hours wasted
    - Cost per hour / per employee
  - Revenue
    - Direct financial loss
    - Future business loss
  - Financial Performance
    - Credit rating and stock price
  - Other Expenses
  - Hidden Costs

Classification of Threats

- Cost of a threat can be calculated considering following factors
  - Other Expenses
    - Overtime Costs
    - Travel Expenses
    - Third Party costs
    - Equipment Rental Costs
  - Hidden Costs
    - Difficult to calculate
    - Cost of damaged reputation
    - Loss of faith by customers, bankers or vendors

Control Against Program Threats

Types of controls:

Developmental
Operating system
Administrative

Developmental Controls

Many controls can be applied during software development to ferret out and fix problems.

1. **The Nature of Software Development**
2. **Modularity**
3. **Encapsulation**
4. **Information Hiding**

Operating system

Mutual Suspicion

Confinement

Information System Security

D Y PATIL INTERNATIONAL UNIVERSITY
AKURDI PUNE

SUMMERY:

- The aim of the information system security is to protect organization assets.
- If not fully protected at least limit damage to them.
- Limit access to information to authorized users only.
- Information systems controls play a crucial role to ensure secure operations of IS.
- They safeguard the assets and the data within them.

Information System Security

- The organization needs to develop a set of security policies, procedures and technological measures.
- Information System Controls-
  - Preventive Controls
    - Prevent an error or attack
  - Detective Controls
    - Detect a security breach or incident
  - Corrective Controls
    - These control detect any error or incident and correct it.

Building Blocks of Information Security

- Basic Terms and Definitions
- Encryption
  - Modification of data for security reasons prior to their transmissions so that it is not comprehensible without the decoding method.
- Cipher
  - Cryptographic transformation that operates on characters or bits of data.
- Cryptanalysis
  - Methods to break the cipher so that encrypted message can be read.

Building Blocks of Information Security

- Electronic Signature
  - Process that operates on a message to assure message source authenticity, integrity and non-repudiation.
- Non-Repudiation
  - Methods by which the transmitted data is tagged with sender's identity as a proof so neither can deny the transmission.
- Steganography
  - Method of hiding the existence of data. The bit map images are regularly used to transmit hidden messages.

Building Blocks of Information Security

- Identification
  - It is a method by which a user claims his identity to a system.
- Authentication
  - It is the method by which a system verifies the identity of a user or another system
- Accountability
  - It is the method by which a system tracks the actions performed by a user or a process.
- Authorization
  - It is a method by which a system grants certain permissions to a user.
- Privacy
  - It is protection on individual data and information.

Building Blocks of Information Security

- The Three Pillars of Information Security
- Confidentiality
  - It is related to the access to data.
  - Any intentional or unintentional unauthorized disclosure of data will make data loose it's confidentiality.
- Integrity
  - It is nothing but the trueness or correctness of data.
  - Any unauthorized modifications to data affects integrity of that data.
- Availability
  - It means reliable and timely access to required data.

Building Blocks of Information Security

- Terms for Information Classification
- Unclassified
  - Not so important information. Can be disclosed to public.
- Sensitive but unclassified
  - Information is somewhat important but if disclosed to public will not cause any damage
- Confidential
  - Unauthorized disclosure may cause some damage.
- Secret
  - Unauthorized disclosure may cause serious damage.
- Top secret
  - Unauthorized disclosure may cause vary serious damage.

Building Blocks of Information Security

- How ever some organizations classify information as
  - Public
  - Sensitive
  - Private

- Following criteria are used to determine the classification of information
  - Value
  - Age
  - Useful Life
  - Personal Association


Thank you