BITS Pilani Presentation

BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

innovate achieve lead

BITS Pilani
Pilani Campus

SSZG681: Cyber Security
Lecture No: 01

Agenda

- Course description
  - Objective
  - Content
  - Text books
  - Structure & schedule
  - Lecture plan
- Understanding cyber space environment and security
  - Introduction
  - Attacks on web

Course objectives

No	Objective
CO1	To learn techniques for assessing network attacks & vulnerabilities, to learn for systematically reducing vulnerabilities and mitigating risks.
CO2	Acquire knowledge about Cybercrime tools and applications.
CO3	To provide depth knowledge in computer, information, organizational and human security to recover the important evidence for identifying various computer crimes.
CO4	To have a fundamental understanding of Digital Forensics and to learn theoretical and practical knowledge in forensic computing.

Course content

- Introduction
- The web attacks
- Operating system security
- Network attacks
- Strategic defense
- Management and incidents
- Introduction to cyber crime
- Cyber offenses
- Tools and methods used in cyber crime
- Cyber laws and ethics: The legal perspective
- Understanding computer forensics

Text books

Text books

T1	Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, Security in Computing, 5th edition Pearson Education , 2015
T2	Nina Godbole, Sunit Belapure, Cyber Security, Wiley India, New Delhi

Reference books

R1	Ethical Hacking & Network Defense, Michael T. Simpson, Cengage Learning
R2	Cryptography, Network Security and Cyber Laws – Bernard Menezes, Cengage Learning, 2010 edition
R3	Cyber security and Cyber Laws, Alfred Basta, Nadine Basta, Mary brown, Ravindrakumar, Cengage learning

Course structure & schedule

- 16 on-line lectures (2 hours each) + self study
- Assessment strategy
  - Quiz(s) – 3 Quiz(s) after 4th, 8th & 12th lectures
  - Lab assignments (TBD)
  - Mid-Semester Test (close book): Topics 1-8
  - Comprehensive Examination (open book): Full course
- Schedule

• Semester start (first lecture)	: 08-Aug-2020
• Last lecture	: 25-Nov-2020
• Mid Sem Test	: 09-11-Oct-2020
• Mid Sem Test Makeup	: 16-18-Oct-2020
• Comprehensive Exam	: 27-29-Nov-2020
• Comprehensive Exam Makeup	: 11-13-Dec-2020

Lecture plan

Lecture #	Topic Covered	Date
LO1	Understanding the cyber space environment and security	08-Aug
LO2	The attacks on web	16-Aug
LO3	Security in operating systems	29-Aug
LO4	The attacks in networks	30-Aug
L05 – L06	Strategic defence	05-Sep, 12-Sep
L07	Management & Incidents	19-Sep
L08	Risk analysis	26-Sep
L09	Introduction to cyber crime	27-Sep
L10	Cyber offenses	03-Oct
L11– L12	Tools and methods used in cyber crime	04-Oct, 24-Oct
L13	Cyber laws and ethics – The legal perspective	31-Oct
L14	Understanding computer forensics	07-Nov
L15	Network forensics	08-Nov
L16	OSI 7 layer model for computer forensics and social networking	25-Nov
Buffer	If required	

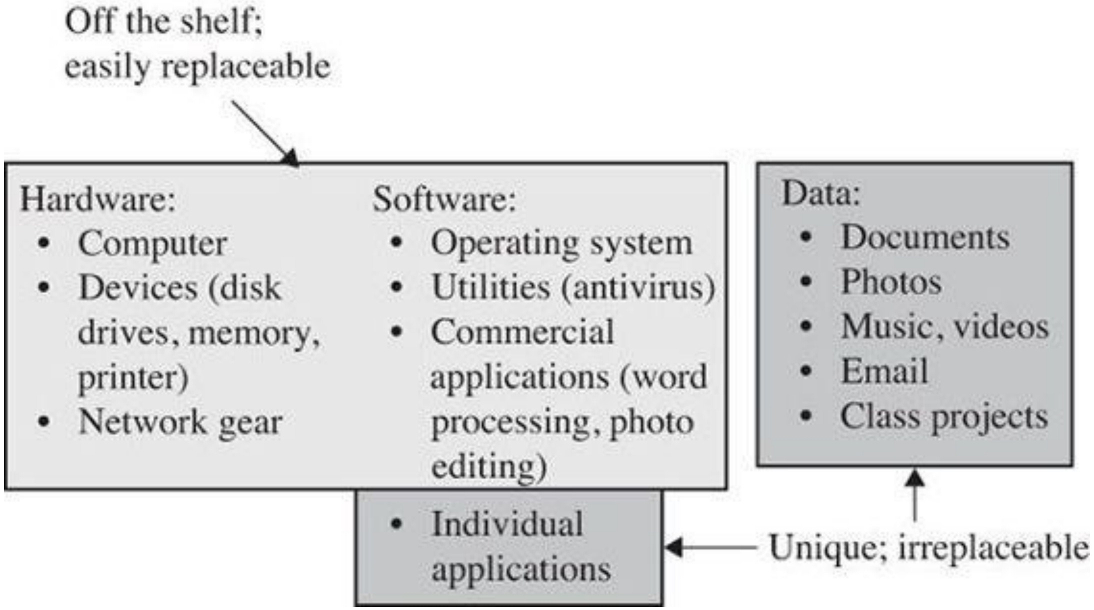
Introduction

Computer security

- Computer security is protection of items or ASSETS of a computer or computer system
- The ASSETS have a value to an individual
- Assets are of following types:
  - **Hardware:** Computers, Devices (disk drives, memory cards, printers etc), Networks
  - **Software:** Operating system, utilities, commercial applications (MS-Office, Oracle apps, SAP etc), individual applications
  - **Data:** Documents, photos, emails, projects, corporate data etc
- The computer systems (hardware, software, data) have a value and deserve security protection

Asset value

- Has an owner or user perspective
- May be monetary or non-monetary
- Is personal, time dependent & often imprecise



Off the shelf; easily replaceable

Hardware:
- Computer
- Devices (disk drives, memory, printer)
- Network gear

Software:
- Operating system
- Utilities (antivirus)
- Commercial applications (word processing, photo editing)
- Individual applications

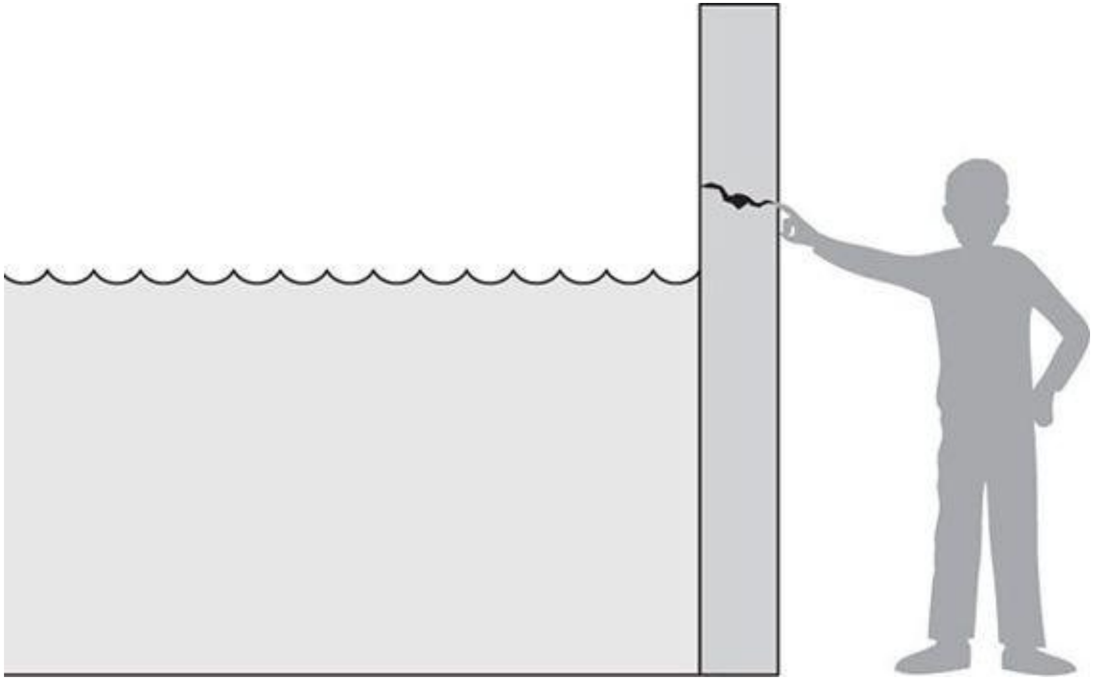
Data:
- Documents
- Photos
- Music, videos
- Email
- Class projects

Unique; irreplaceable

Vulnerability – Threat - Control paradigm

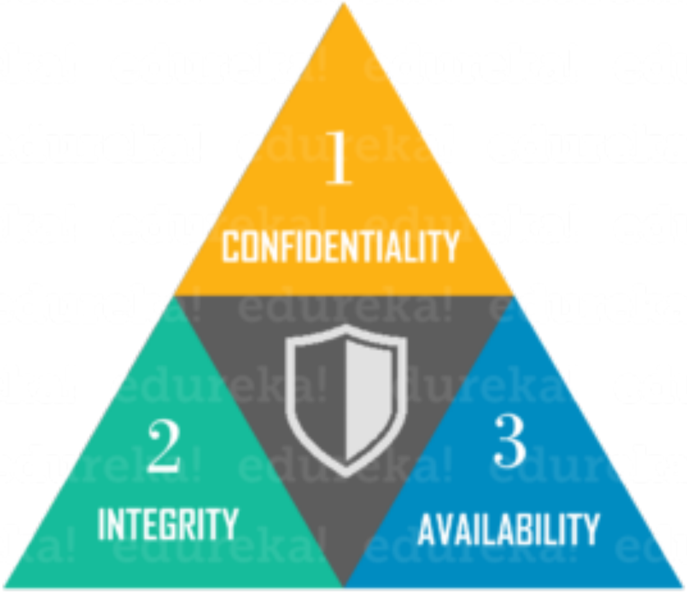
- ‘**Vulnerability**’ is a weakness in the system that might be exploited to cause loss or harm
- ‘**Threat**’ is a set of circumstances that has a potential to cause loss or harm to system
- A person who exploits the vulnerability perpetrates an ‘**Attack**’
- ‘**Control**’ is an action, device, procedure of technique that removes or reduces the vulnerability

Vulnerability – Threat - Control example



- **Vulnerability:** Crack in the wall
- **Threat:** Rising water level
- **Attack:** Someone pumping more water
- **Control:** Fill the gap, strengthen the wall

Security triad - CIA

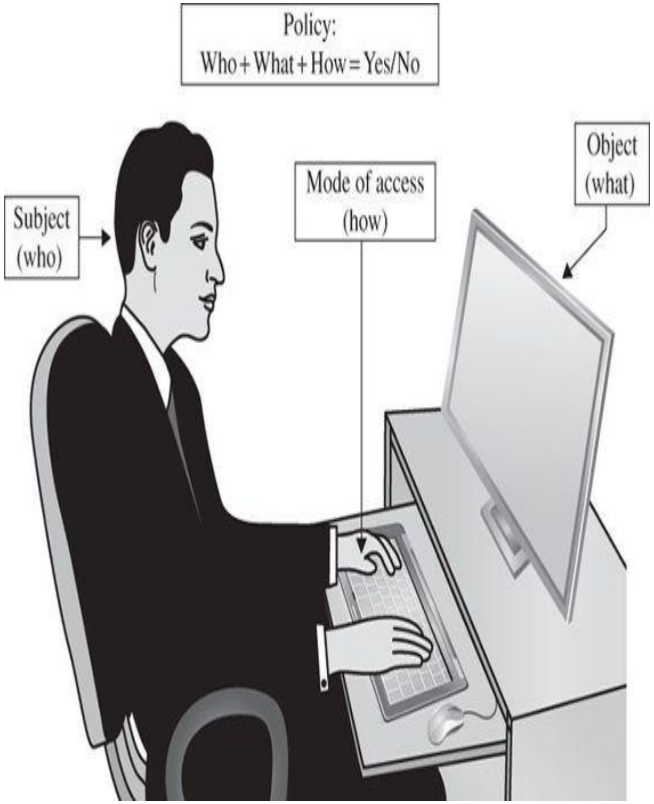


- **Confidentiality:** Ability of a system to ensure that an asset is viewed by only authorized parties
- **Integrity:** Ability of a system to ensure that an asset is modified by only authorized parties
- **Availability:** Ability of a system to ensure that an asset can be used by any authorized parties

Additional two properties:

- **Authentication:** Ability of a system to validate the identity of a sender
- **Non-repudiation or Accountability:** Ability of a system to confirm that a sender can not convincingly deny having sent something

Confidentiality



- Only authorized person, program or process can access protected data
- Failure of data confidentiality
  - An unauthorized person access a data item
  - An unauthorized program or process access a data item
  - A person authorized to access certain data accesses other data which he is not authorized to access
  - An unauthorized person accesses approximate data value
  - An unauthorized person learns the existence of data value
- Terminology:
  - **Subject:** a person, program or process. -> who
  - **Object:** data item. -> what
  - **Access mode:** kind of access (read, write, execute) -> how
  - **Policy:** authorization –> who+what+how = yes/no

Integrity

Integrity means

- Precise
- Accurate
- Unmodified
- Modified only in acceptable ways
- Modified only by authorized people
- Modified only by authorized processes
- Consistent
- Meaningful and usable

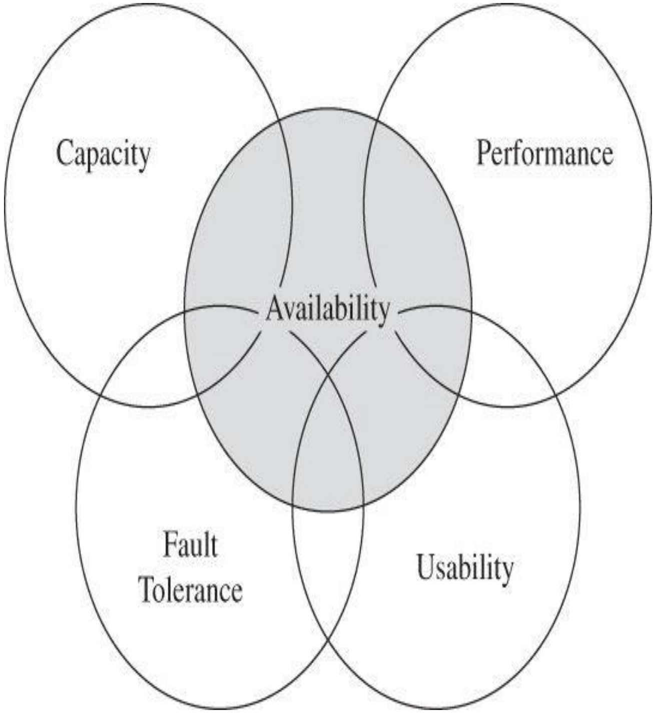
Integrity requires

- Actions are authorized,
- Resources are separated & protected
- Errors are detected & corrected

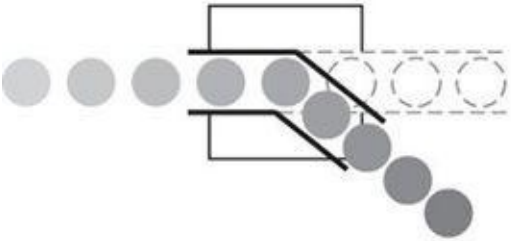
Integrity enforcement: Who or what can access which resources in what ways

Availability

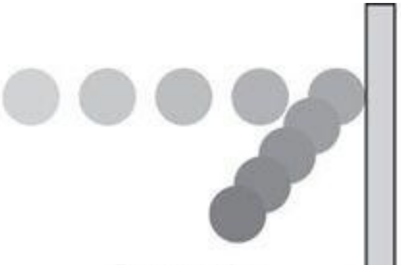
- An object or service is available if:
  - it is present in usable form
  - It has enough capacity to meet the service needs
  - It is making clear progress i.e. it has bounded waiting time
  - It is completed in an acceptable period of time
- Applies to both services and data
  - Timely response to requests
  - resources are allocated fairly so that some requests don't get preferred treatment
  - concurrency is controlled
  - Services or systems are fault tolerant
  - Services or systems are easily usable



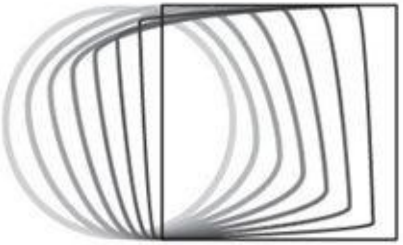
Acts of harm



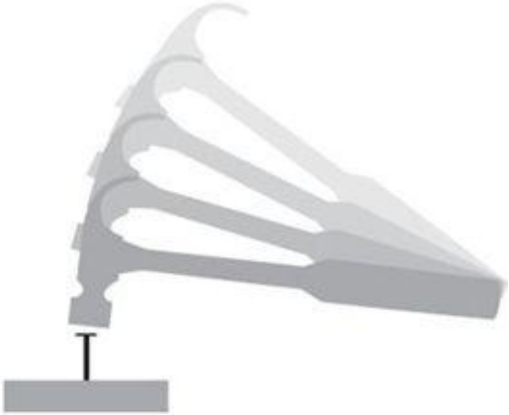
Interception



Interruption



Modification



Fabrication

Interception: Confidentiality lost

Interruption: Availability lost

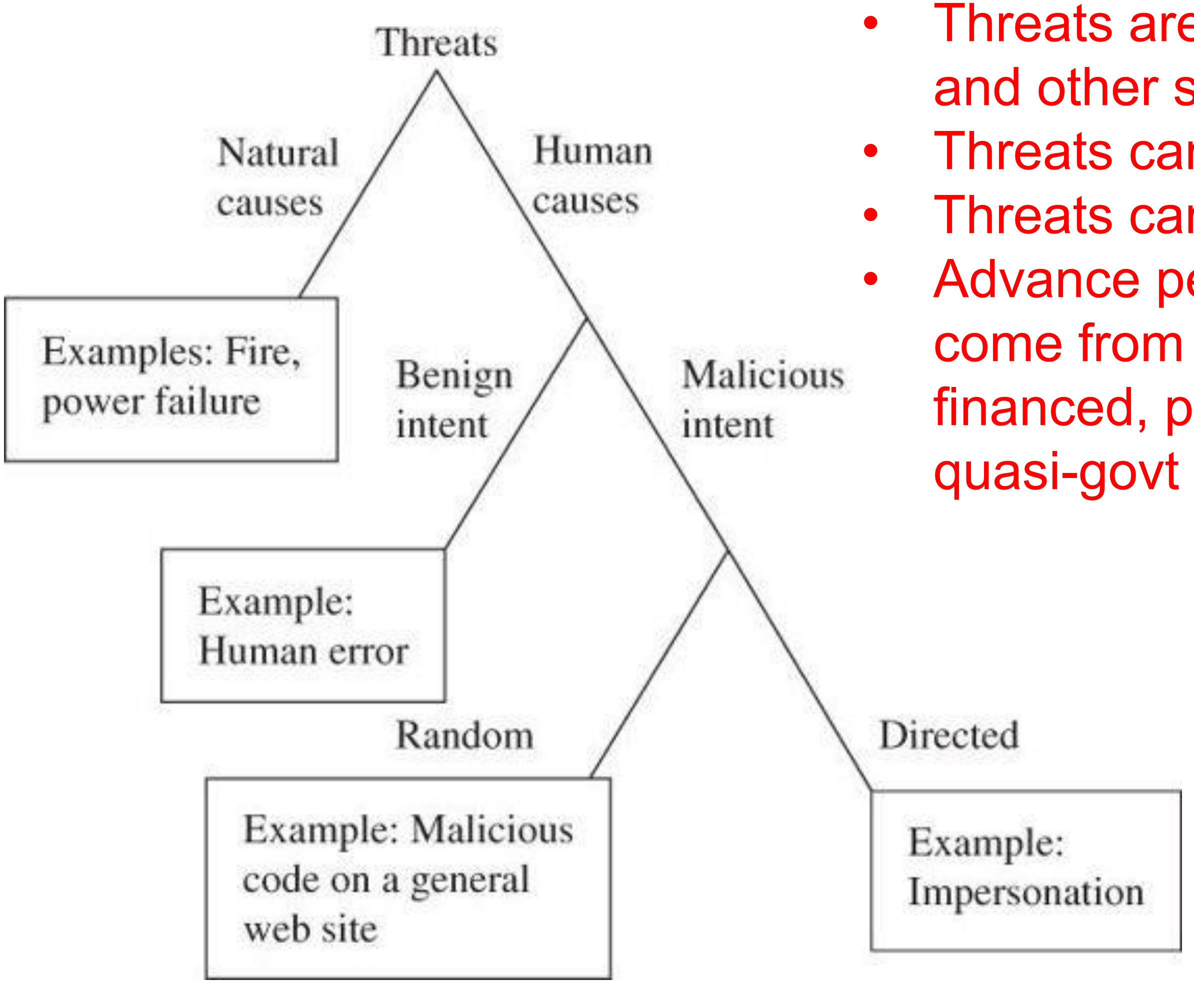
Modification: Integrity lost

Fabrication: Integrity lost

Computer security … refined

- Computer security seeks to prevent unauthorized viewing (confidentiality) or modification (integrity) of data while preserving access (availability)
- Access control is fundamental to security
- Threats are potential cause of harm
- Threats can be caused by human or non-human
- Human threats can be malicious or non-malicious
- Malicious threats can be direct or random attack

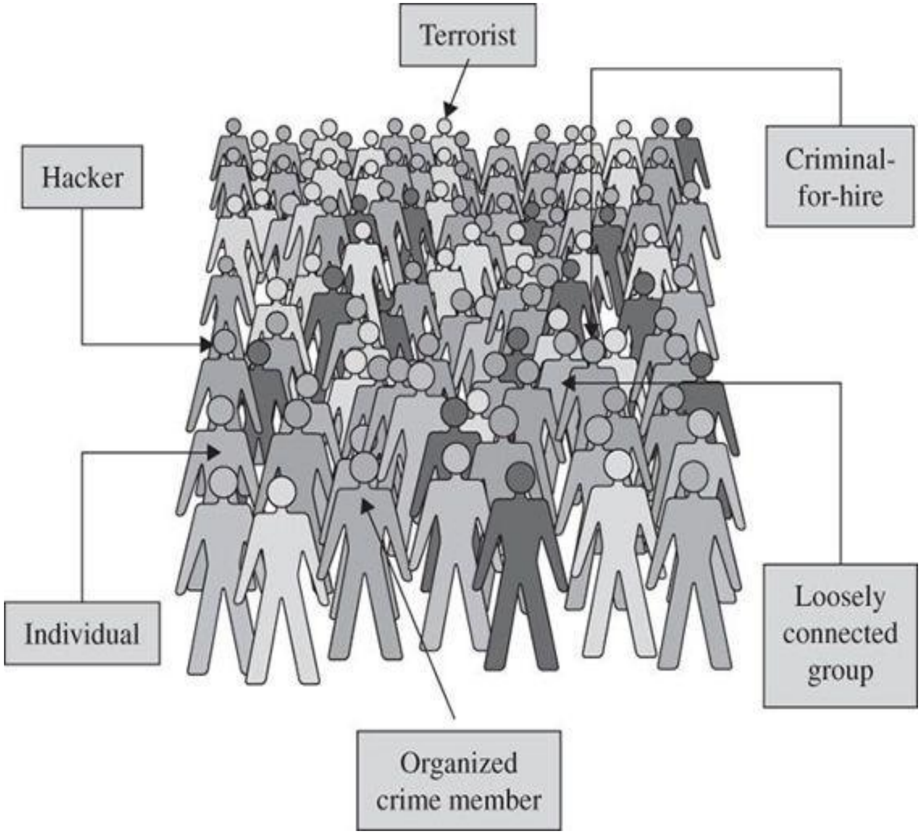
Computer security … refined



- Threats are caused both by human and other sources
- Threats can be malicious or not
- Threats can be random or targeted
- Advance persistent threat attacks come from organized, well financed, patient and often govt or quasi-govt affiliated groups

Type of attackers

- Individual
- Hackers
- Terrorist
- Criminal for hire
- Loosely connected group
- Organized crime member
  - computer crime is lucrative



Security threats

- **Virus:** A computer virus is a malicious program which is loaded into the user's computer without user's knowledge. It replicates itself and infects the files and programs on the user's PC.
- **Worm:** A computer worm is a software program that can copy itself from one computer to another, without human interaction. The potential risk here is that it will use up your computer hard disk space because a worm can replicate in great volume and with great speed.
- **Phishing:** Disguising as a trustworthy person or business, phishers attempt to steal sensitive financial or personal information through fraudulent email or instant messages. Phishing in unfortunately very easy to execute. You are deluded into thinking it's the legitimate mail and you may enter your personal information.

Security threats…

- **Botnet:** A botnet is a group of computers connected to the internet, that have been compromised by a hacker using a computer virus. An individual computer is called ‘zombie computer’. The result of this threat is the victim’s computer, which is the bot will be used for malicious activities and for a larger scale attack like DDoS.
- **Rootkit:** A rootkit is a computer program designed to provide continued privileged access to a computer while actively hiding its presence. Once a rootkit has been installed, the controller of the rootkit will be able to remotely execute files and change system configurations on the host machine.
- **Key Loggers:** Keyloggers can track the real-time activity of a user on his computer. It keeps a record of all the keystrokes made by user keyboard. Keylogger is also a very powerful threat to steal people’s login credential such as username and password.
- Apart from these, there are others like **spyware, wabbits, scareware, bluesnarfing** and many more

Security approach

- Negative consequences of an actualized threat is harm
- Risk management involves choosing which threats to control and what resources to devote for protection
- The risk that remains uncovered by controls is called residual risk
- Spending on security is based on impact and likelihood of potential harm

Method – opportunity - motive

- **Method:** Skill, knowledge, tools and other things (scripts, model programs etc) to perpetrate the attack
- **Opportunity:** Time and access to execute an attack
- **Motive:** Reason for attack (money, fame, self-esteem, politics, terror etc)

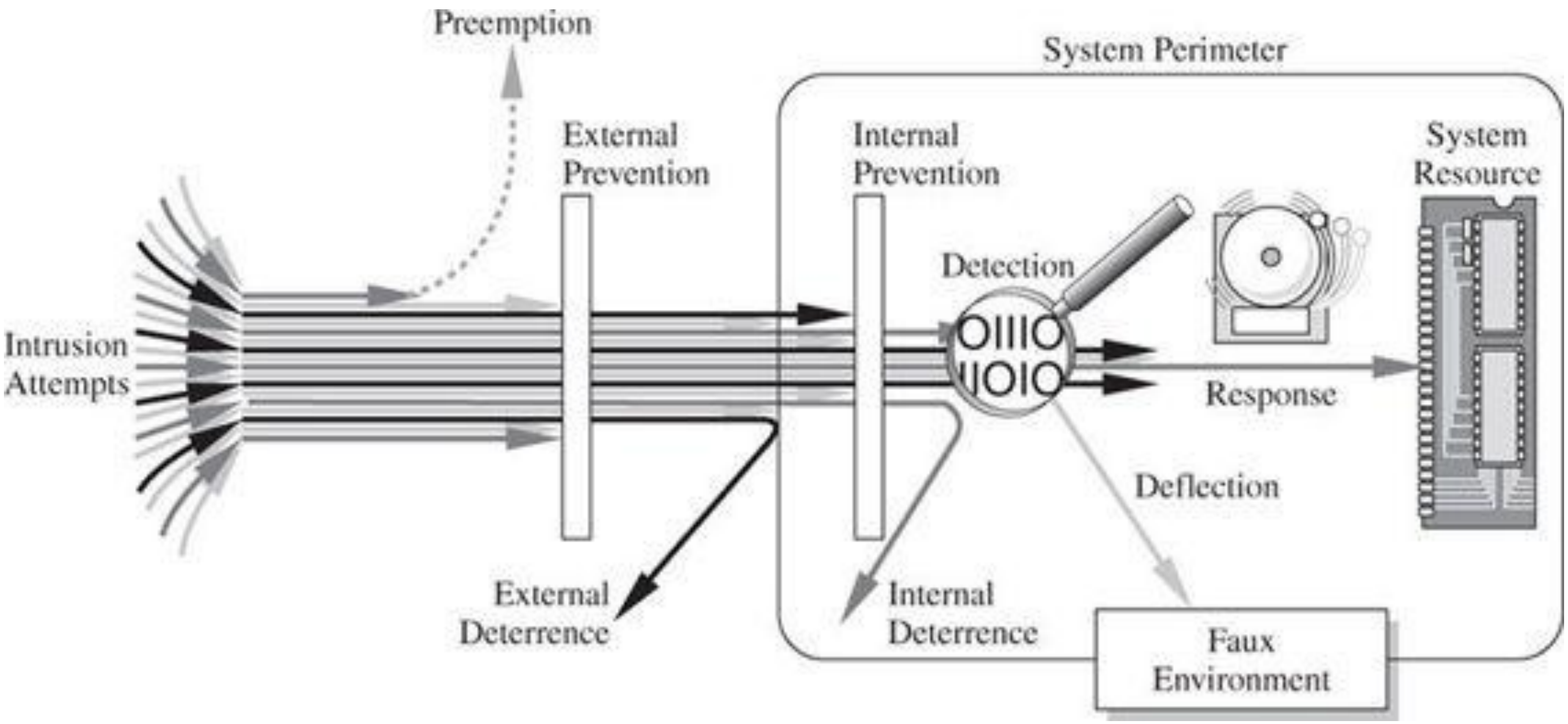
- Method, opportunity and motive are essential for an attack – deny any one of these and the attack will fail
- Vulnerabilities are weaknesses in the system that allow harm to occur

Security controls

- Prevent it by blocking attack or closing the vulnerability
- Deter it by making the attack harder but not impossible
- Deflect it by making another target more attractive
- Mitigate it by making the impact of attack less severe
- Detect it as it happens or sometime after the fact
- Recover from effects

- Security professionals balance the cost and effectiveness of controls with the likelihood and severity of harm

Security controls…



Security controls…

Physical

- Walls, fence, locks
- Human guards
- Sprinklers and fire extinguishers

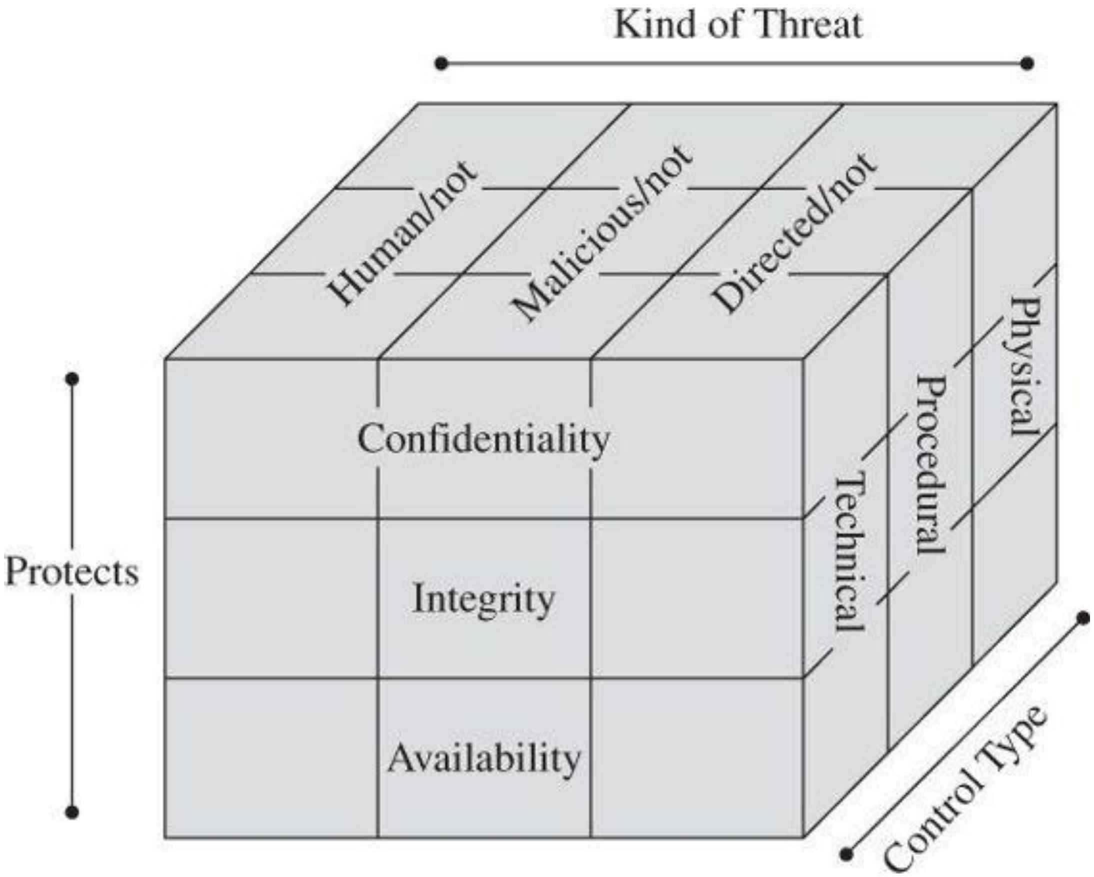
Procedural or administrative

- Advice to people on how to act
- Laws and regulations
- Policies, procedures and guidelines
- Copyright and patents
- Contracts and agreements

Technical

- Passwords, programs or operating system access controls
- Network protocols, network traffic flow regulators
- Firewalls and intrusion detection systems
- Encryption

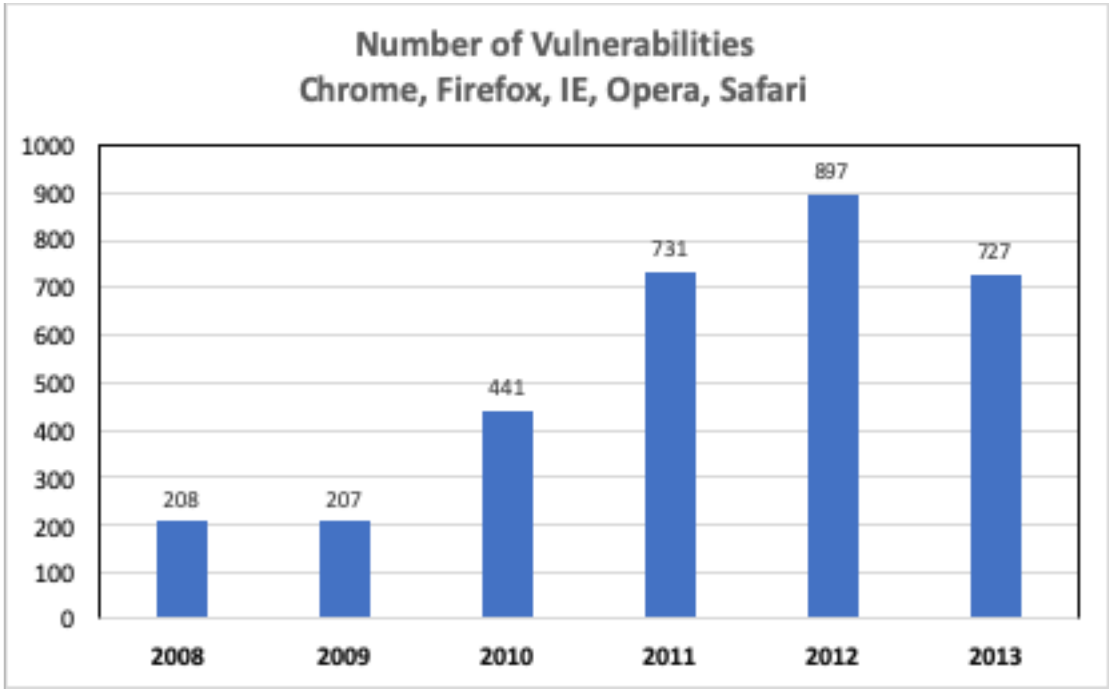
Security control dimensions



Web browser

- Browsers connects a user to more than one address shown in the address bar
- Browser software can be malicious or could be corrupted
- Browsers support add-in/extension which leave a user vulnerable to intrusions
- Browsers run with same privileges as the user and hence can access any data on user's computer
- Browser data transfer to/from user computer is invisible to user i.e. occur without user knowledge and explicit permission
- Browsers connect a user to outside network(s) but few users can monitor the actual actions, tasks and data performed / transmitted

Browser vulnerabilities



Browser attack vectors

- User operating system to impede browser’s correct and secure working
- Tackle the browser or one of it’s component/add-on/plug-in to alter browser’s working
- Intercept or modify communication to or from browser

Browser attack types

- **Man in the browser:** Trojan horse that intercepts data passing thru browser (SilentBanker)
- **Key stroke logger**: Hardware and software versions
- **Page in the middle:** user redirected to authentic looking but malicious page like fake ‘login’ page
- **Program download substitution:** A malicious program is installed using a download button
- **User in the middle:** Puts a human action between two automated processes – CAPTCHA can be defeated by using techniques pixel count, histogram analysis and color filing segment

How to avoid browser attacks?

- Strong identification and authentication
  - **Shared secret:** mother’s maiden name, 3-digit verification number on credit card etc
- One Time Password (OTP)
- Out of band communication: mail PIN separately
- Continuous communication: session id

Web attacks targeting users

- False or misleading content
- Defaced website
- Fake website
- Fake or malicious code
- Malicious web content
- Web bug
- **Clickjacking:** tricking a user into clicking by disguising what the link pertains to
- **Drive by download:** downloading and installing code other than what a user expects

Protecting web sites against attacks

- Integrity checksums
- Signed code or data
- Access control separation: separate operating system level privileges to install programs
- Manage and monitor site code
- User vigilance

Thank You