Introduction to Ethical Hacking

Dayanand Ambawade
Sardar Patel Institute of Technology,Mumbai

Overview

1. Introduction to Cybersecurity
2. Defining Cyberspace
3. Defining Cybercrimes
4. Classification of Cybercrimes & Cybercriminals
5. Anatomy of Hack
6. Critical Infrastructure and Cybersecurity
7. Cybersecurity Challenges
8. Security services and security mechanisms
9. Information Warfare

Cybersecurity and Cybercrime

IT research firm Gartner predicts that by 2020, 30 percent of Global 2000 companies will have been directly compromised by independent cyber activists or cyber criminals.

[Source: Google Images]

Cybercrimes and Cybersecurity

Cyber crime damage costs to hit $6 trillion annually by 2021.

Cybersecurity spending to exceed $1 trillion from 2017 to 2021. The rising

Cyber crime will more than triple the number of unfilled cybersecurity jobs, which is predicted to reach 3.5 million by 2021.

Human attack surface to reach 6 billion people by 2022.

Global ransomware damage costs are predicted to exceed $5 billion in 2017.

https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html

Introduction to Cybersecurity

Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from cyber attacks.

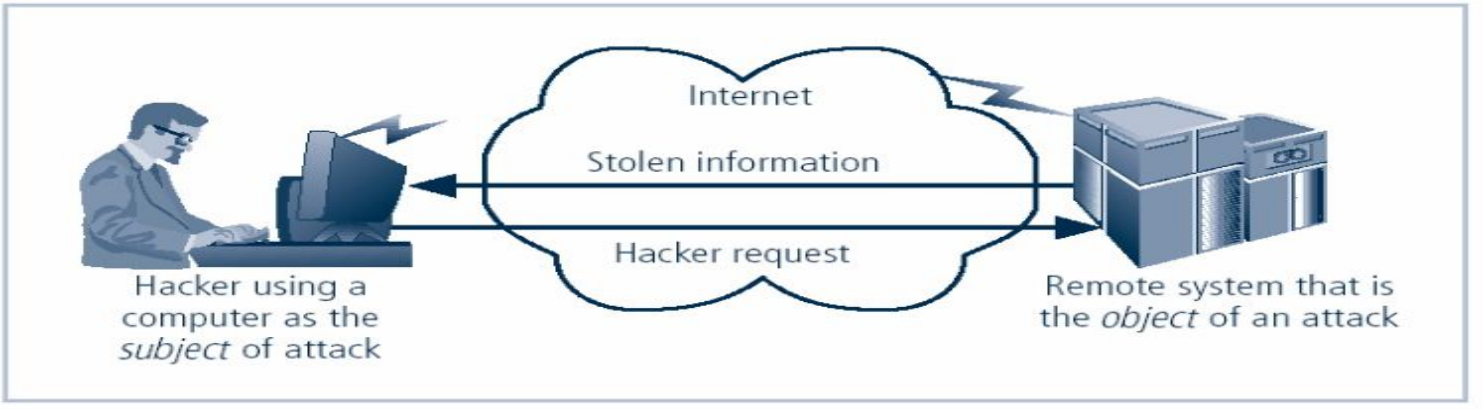
[Source: Google Images]

Defining Cyberspace

“ A global domain within the information environment consisting of the independent network of information technology infrastructures, including the Internet, telecommunication networks, computer systems, and embedded processors and controllers”

Defining Cybercrime

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes).



Defining the Cybercrime

Crime committed using a computer and the internet to steal data or information.

Illegal imports.

Malicious programs.

[Source: Google Images]

Cybercrime

The Computer as a Target

The computer as a weapon

Cybercrimes

Using the Internet to commit a crime.

- Identity Theft
- Hacking
- Viruses

Facilitation of traditional criminal activity

- Stalking
- Stealing information
- Child Pornography

Cybercrime components

Computers

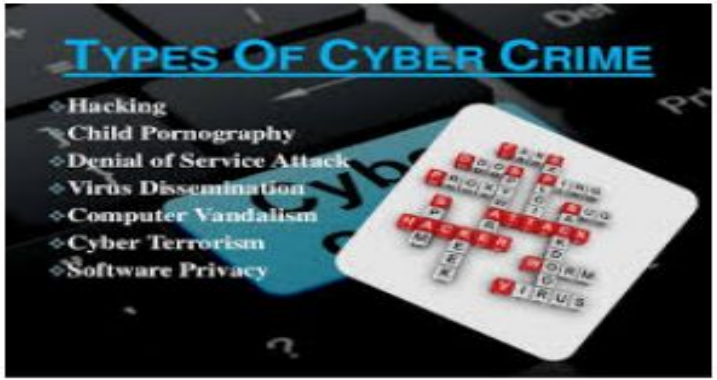
Cell Phones

PDA’s

Game Consoles

Cybercrimes

Cybercrimes



[Source: Google Images]

Classifications of Cybercrimes

It can be classified in to 4 major categories as:

- Cyber crime against Individual
- Cyber crime Against Property
- Cyber crime Against Organization
- Cyber crime Against Society

[1] Cybercrimes against Individuals

- **(i) Email spoofing :**
- A spoofed email is one in which e-mail header is forged so that mail appears to originate from one source but actually has been sent from another source
- **(ii) Spamming :**
- Spamming means sending multiple copies of unsolicited mails or mass e-mails such as chain letters.
- **(iii) Cyber Defamation :**
- This occurs when defamation takes place with the help of computers and / or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information.
- **(iv) Harassment & Cyber stalking :**
- Cyber Stalking Means following the moves of an individual's activity over internet. It can be done with the help of many protocols available such at e- mail, chat rooms, user net groups.

[2] Cybercrime Against Property:

(i) Credit Card Fraud :

(ii) Intellectual Property crimes : These include

Software piracy: illegal copying of programs, distribution of copies of software.

Copyright infringement:

Trademarks violations:

Theft of computer source code:

(iii) Internet time theft :

the usage of the Internet hours by an unauthorized person which is actually paid by another person.

[3] Against Organisation

(i) Unauthorized Accessing of Computer:

Accessing the computer/network without permission from the owner.

it can be of 2 forms:

a) Changing/deleting data:

Unauthorized changing of data.

b) Computer voyeur:

The criminal reads or copies confidential or proprietary information,

but the data is neither deleted nor changed.

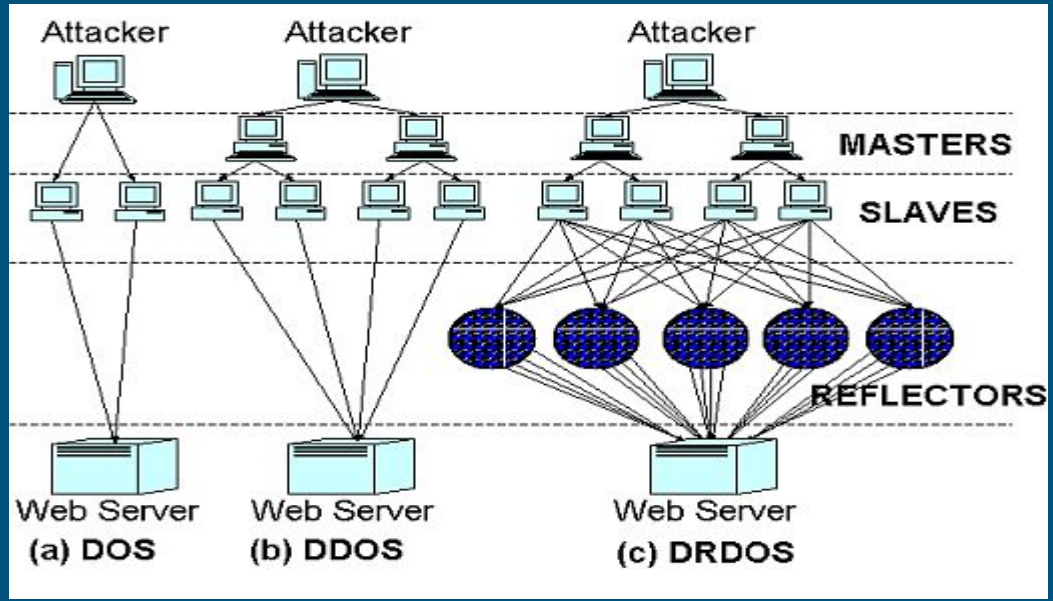
Against Organization

- **(ii) Denial Of Service :**
- When Internet server is flooded with continuous bogus requests so as to denying legitimate users to use the server or to crash the server.
- **(iii) Computer contamination / Virus attack :**
- A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of it.
- Viruses can be file infecting or affecting boot sector of the computer.
- Worms, unlike viruses do not need the host to attach themselves to.
- **(iv) Email Bombing :**
- Sending large numbers of mails to the individual or company or mail servers thereby ultimately resulting into crashing.
- This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

DoS/DDoS

Denial of Service

Distributed Denial of Service



Against Organization

(v) Salami Attack :

When negligible amounts are removed & accumulated in to something larger. These attacks are used for the commission of financial crimes.

(vi) Logic Bomb :

Its an event dependent programme , as soon as the designated event occurs, it crashes the computer, release a virus or any other harmful possibilities.

(vii) Trojan Horse :

an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

(viii) Data diddling :

This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

[4] Against Society

(i) Forgery :

currency notes, revenue stamps, mark sheets etc can be forged using computers and high quality scanners and printers.

(ii) Cyber Terrorism :

Use of computer resources to intimidate or coerce others.

(iii) Web Jacking :

Hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money.

Who are the victims of Cybercrimes

Individual

Society

Organization

Government

Who are the Cybercriminals

- White Hat Hacker
- Black Hat Hacker
- Gray Hat Hacker

Anatomy of Attack

- Internet Footprinting or Web Reconnaissance
- Scanning and Sniffing
- Probing
- Enumeration
- Privilege Escalation
- Maintaining Access
- Pillage
- Expanding the Influence

Cyberkill chain stages


EXPLOITATION
Exploitation / Installation
Workstation compromised;
Threat actor persists malware
Threat actor gathers credentials

Mirai IoT Botnet

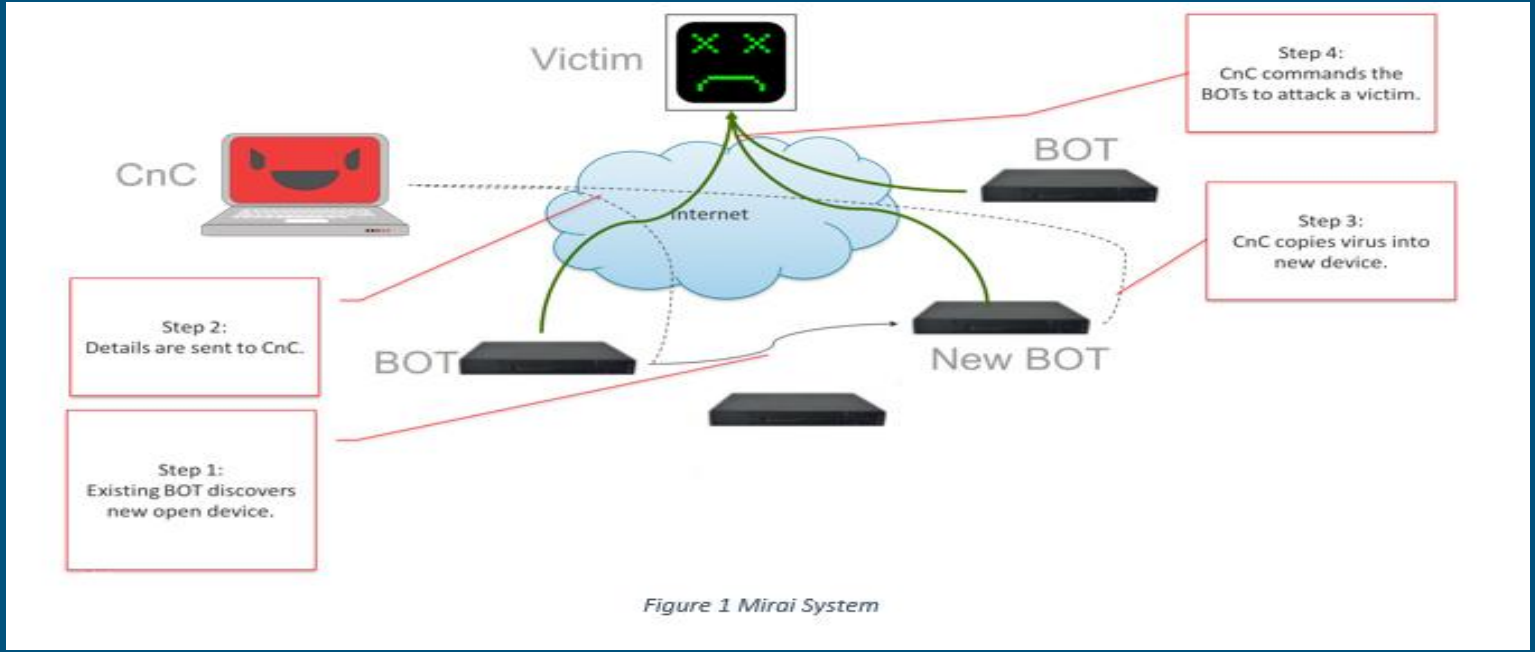


Figure 1 Mirai System

DNS

IF:

dig

host

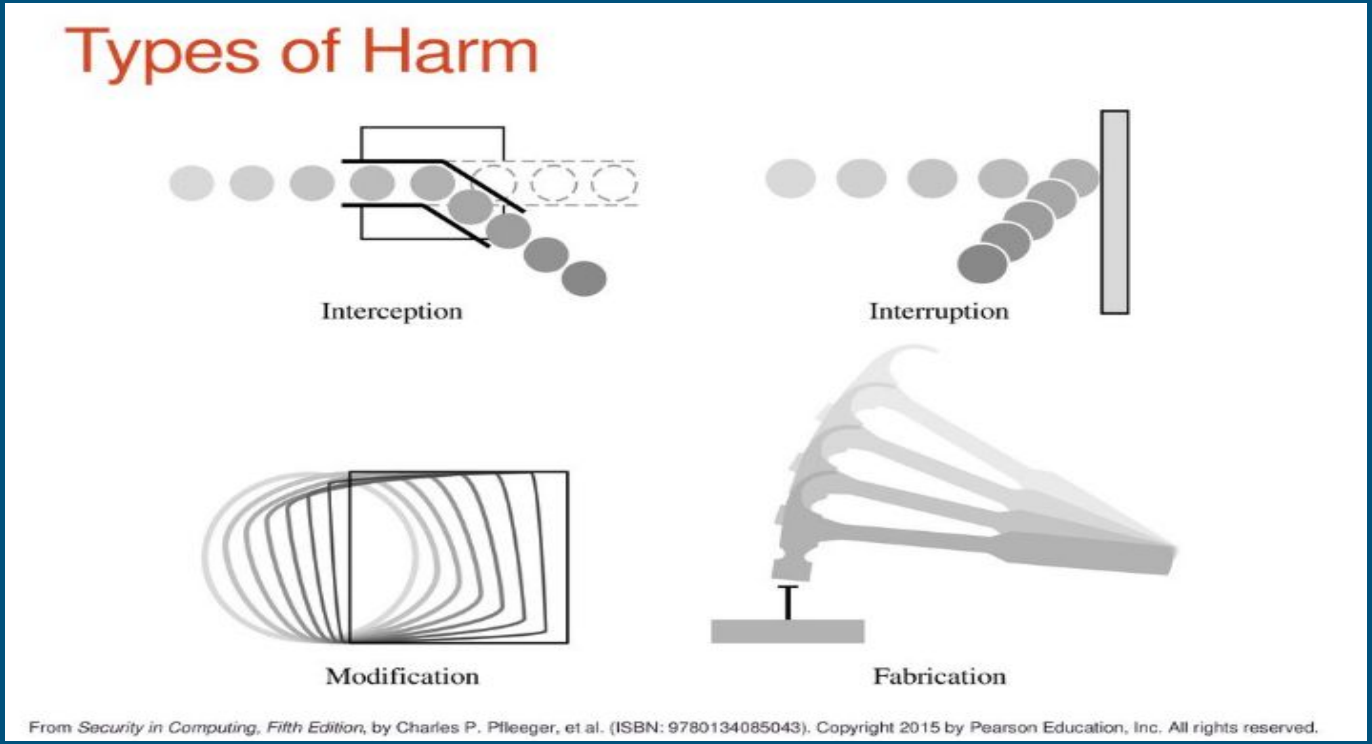
nslookup

Main Cyber Players and Their Motives

- Cyber Criminals: Seeking commercial gain from hacking banks & financial institutions as well as phishing scams and computer ransomware
- Cyber Terrorists: Mission to penetrate & attack critical assets, and national infrastructure for aims relating to political power & “branding”
- Cyber Espionage: Using stealthy IT malware to penetrate both corporate and military data servers in order to obtain plans and intelligence
- Cyber Hacktivists: Groups such as “Anonymous” with Political Agendas that hack sites & servers to virally communicate the message for specific campaigns

Tenets of Cybersecurity

Classification of Attack



Defining Critical Infrastructures (CI)

In general Critical defined as:

Infrastructure (CI) can be “those facilities, systems, or functions, whose incapacity or destruction would cause a debilitating impact on national security, governance, economy and social well-being of a nation”

" A cyber attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack of 9/11," Leon Panetta, US Secretary Of Defense, October 11th 2012

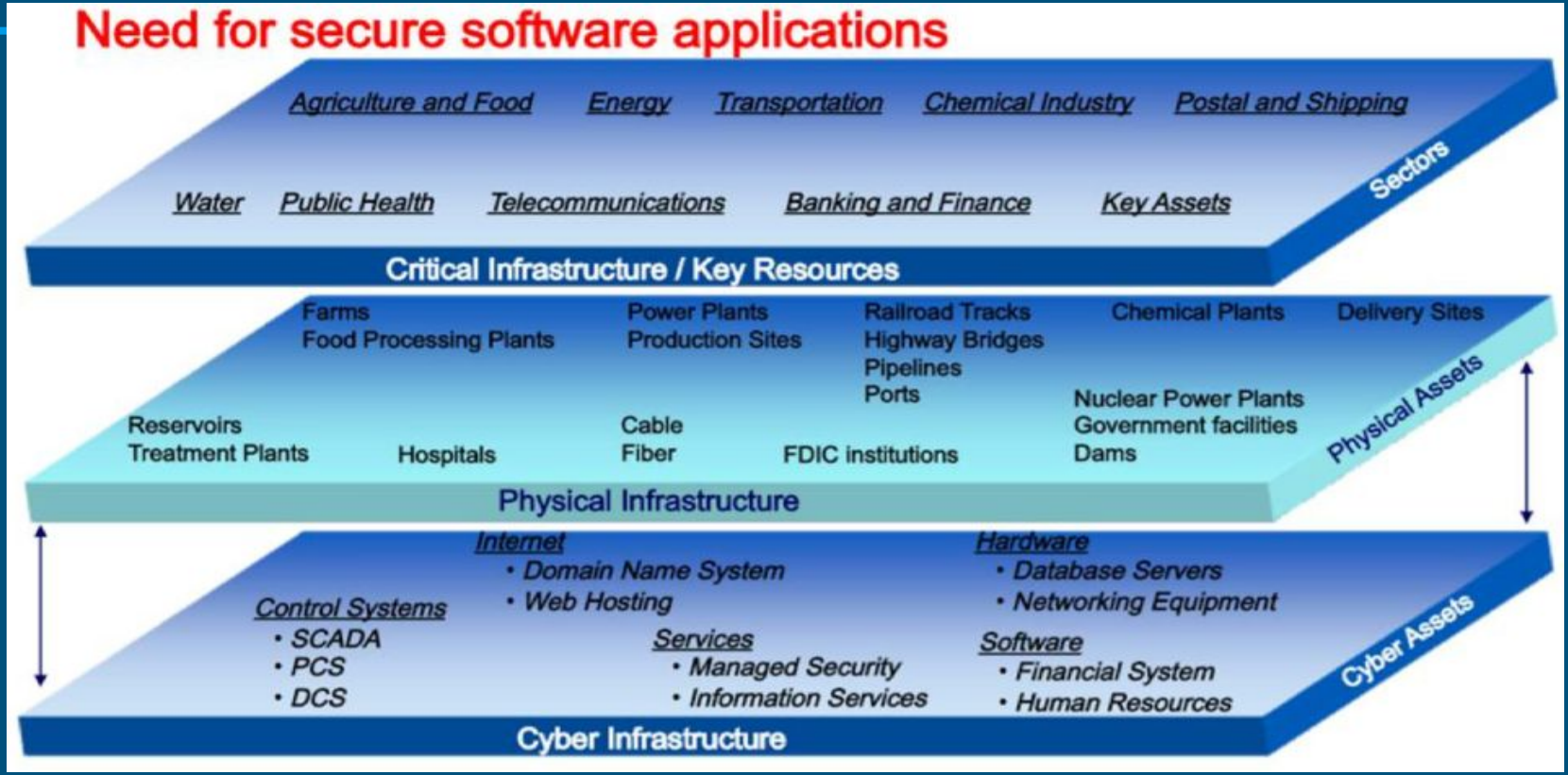
CI and Cybersecurity

Critical Infrastructure Protection

- Cyberspace is the connected Internet Ecosystem
- Trends Exposing critical infrastructure to increased risk: Interconnectedness of Sectors, Proliferation of exposure points, Concentration of Assets

- Cyber Intrusions and Attacks have increased dramatically over the last decade, exposing sensitive personal and business information, disrupting critical operations, and imposing high costs on the economy
- Cyber Security is protecting our cyberspace (critical infrastructure) from attack, damage, misuse and economic espionage

Cyberspace and physical space are increasingly intertwined and software controlled/enabled



Cyber Security Challenges

Cyberspace has inherent vulnerabilities that cannot be removed

Innumerable entry points to internet.

Assigning attribution: Internet technology makes it relatively easy to misdirect attribution to other parties.

• Computer Network Defense techniques, tactics and practices largely protect individual systems and networks rather than critical operations (missions)

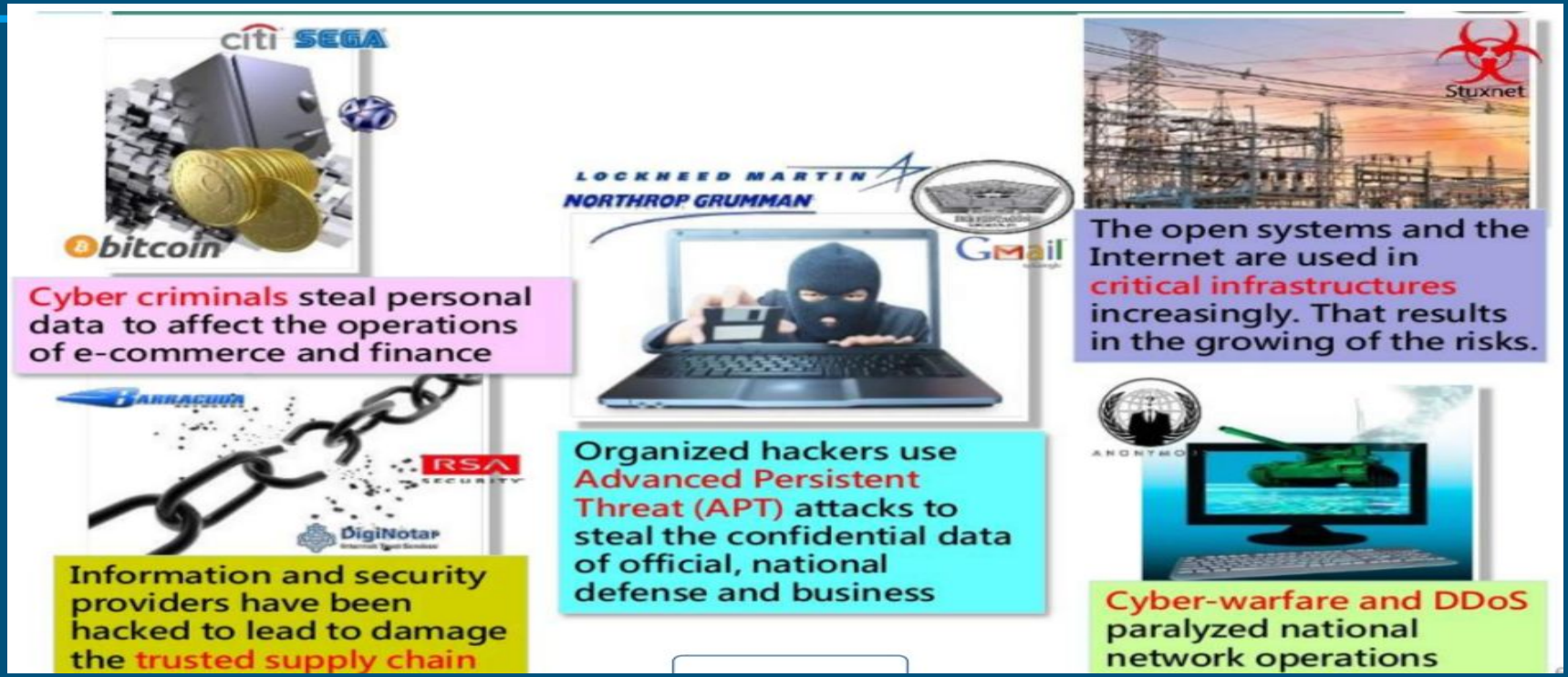
• Attack technology outpacing defense technology

• Nation states, non-state actors, and individuals are at a peer level, all capable of waging attacks

Relation

- Attack- which comprises CIA
- Attacker- person
- Assets(A)- IT infrastructure (PPI)
- Vulnerability (V)- Weakness or loop holes (inherent) Internal CVE ms08_067_netapi
- Threats (T)- potential danger (emanating from outside) External
- Exploit- defined way of breaching security
- Risk = VxAxT

Security Trends



Can be Hacking Ethical?

???

What Makes a Network Vulnerable?

Consider how a network k differs diff from f a stand-alone environment.

- Anonymity. An attacker can mount an attack from thousands of miles away
- and never come into direct contact with the system
- Many points of attack both targets and origins
- Sharing
- Complexity of system
- Unknown perimeter,
- Unknown path.

Basics of Computer Security

The basics….

Principles of Computer Security

- Principle of Easiest Penetration

  An intruder must be expected to use any available means of penetration (p. 5)

- Principle of Adequate Protection

  Computer items must be protected only until they lose their value (p. 16)

- Principle of Effectiveness

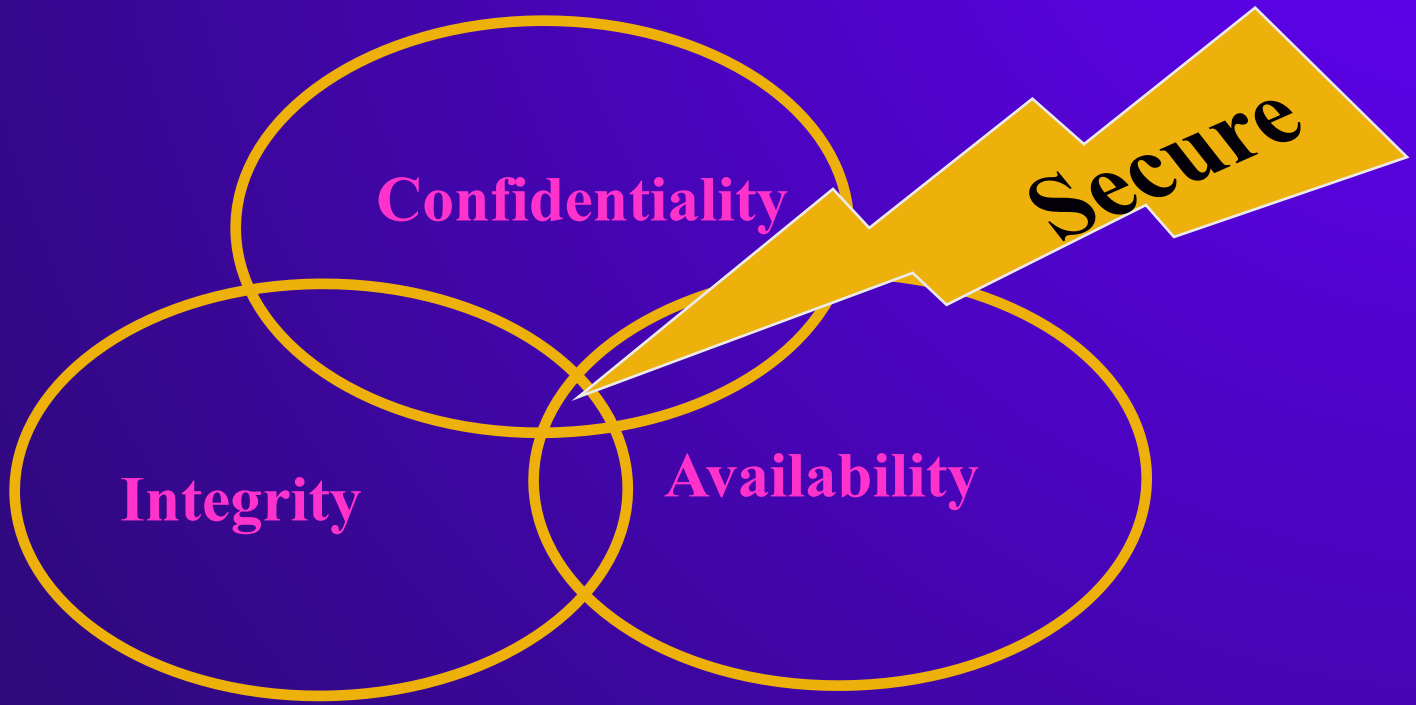
  Controls must be used—and used properly—to be effective (p. 26)

- Principle of Weakest Link

  Security can be no stronger than its weakest link (p. 27)

Source: Pfleeger & Pfleeger

Goal of Computer Security



Source: Pfleeger & Pfleeger

Threats

- Interception
- Interruption
- Modification
- Fabrication

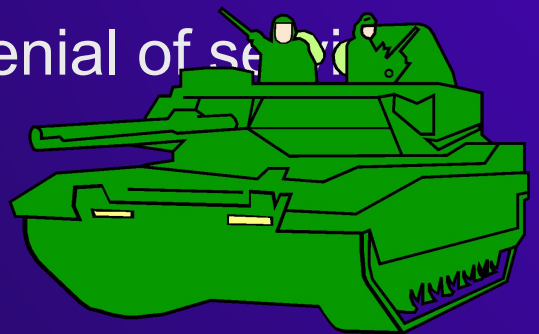
"A threat is blocked by control of a vulnerability"

Pfleeger & Pfleeger

Source: Pfleeger & Pfleeger

Top Methods of Attack

- Exploiting known OS vulnerabilities 33%
- Exploiting unknown application 27%
- Guessing passwords 17%
- Denial of se[illegible] 12%



Information Week 2001

“MOM”

- Method

  Skill, knowledge, tools, etc. with which to pull off an attack

- Opportunity

  Time and access to accomplish an attack

- Motive

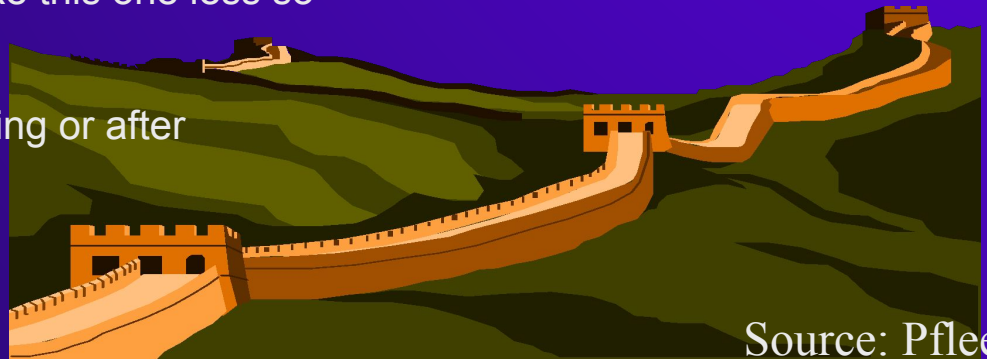
  Reason to perform an attack

Deny any of these and you prevent an attack.

Source: Pfleeger & Pfleeger

Methods of Defense

- Prevent it
  - Block attack
  - Close vulnerability
- Deter it
  - Make attack harder
- Deflect it
  - Make another target attractive
  - Make this one less so
- Detect it
  - During or after
- Recover



Source: Pfleeger & Pfleeger

Then and Now….

- Castle--Middle Ages
  - Strong gate
  - Heavy walls
  - Moat
  - Arrow slits
  - Crenellations
  - Drawbridge
  - Gatekeepers
- Cyberspace—Today
  - Encryption
  - Software controls
  - Hardware controls
  - Policies
  - Procedures
  - Physical controls

Source: Pfleeger & Pfleeger

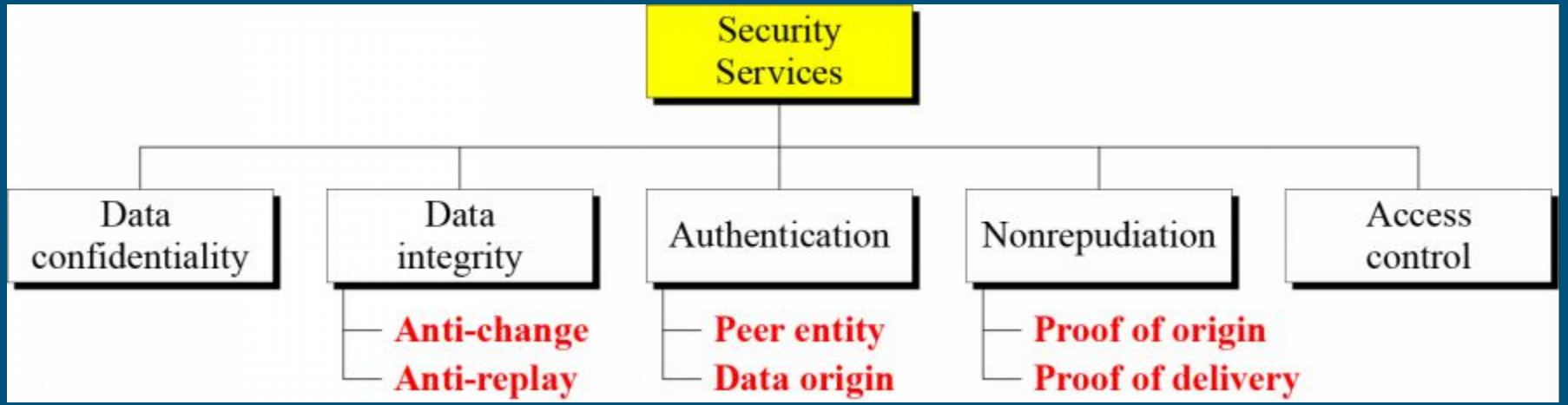
Security Effectiveness

- Awareness of problem
- Likelihood of use
- Overlapping controls
- Periodic reviews

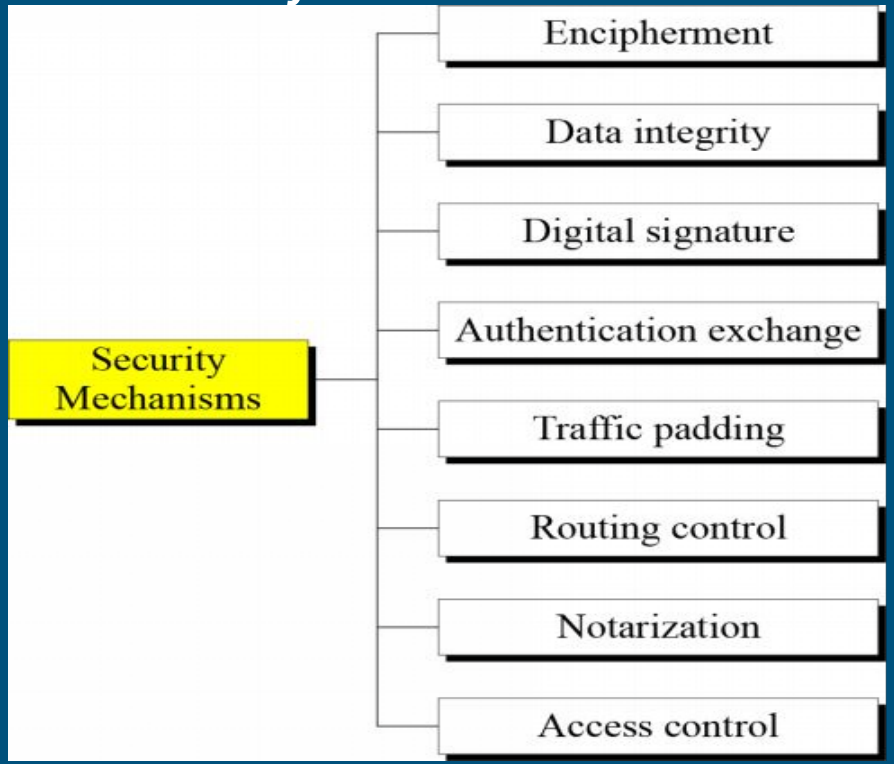
Source: Pfleeger & Pfleeger

Implementing Security

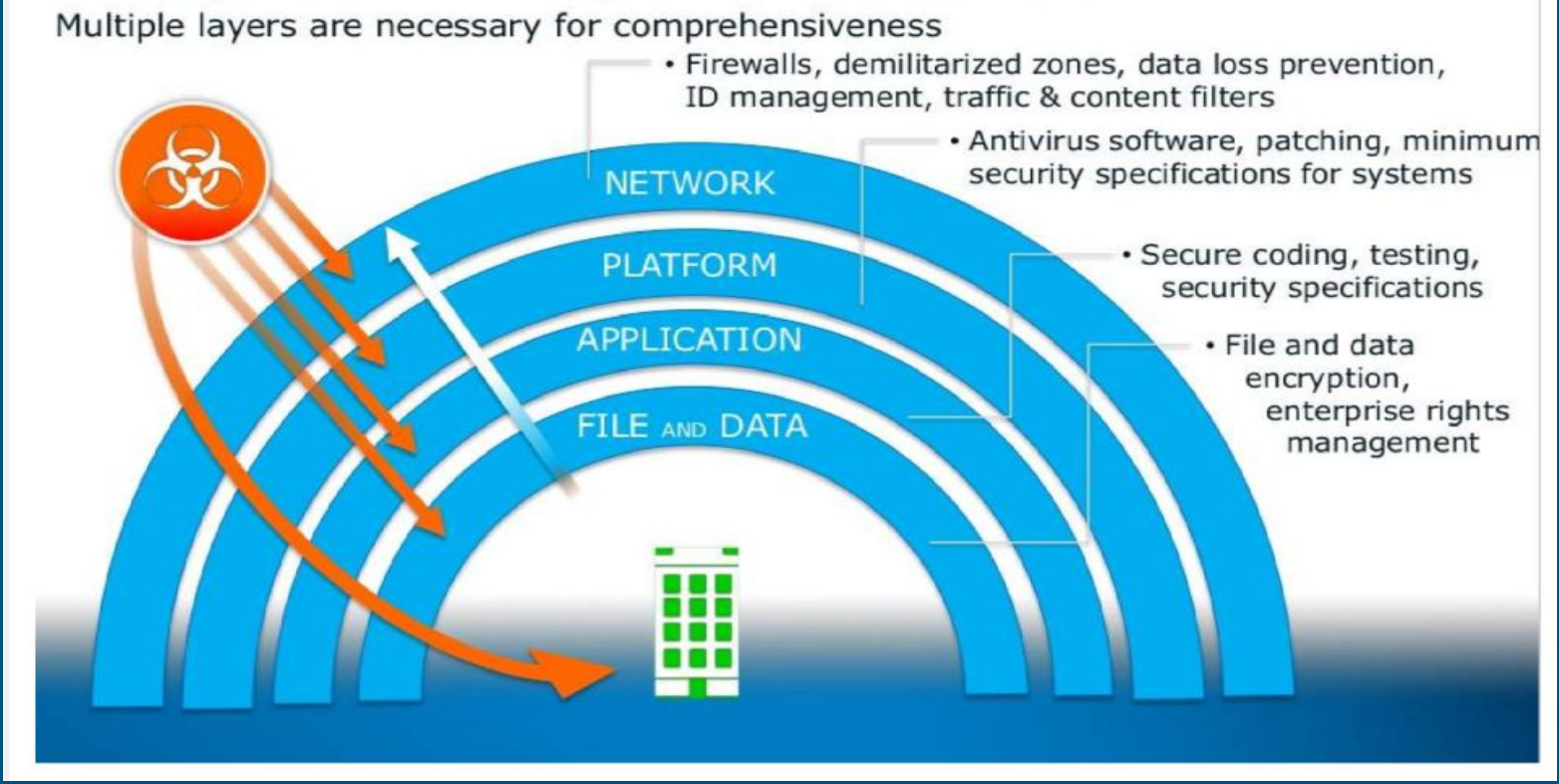
ITU-T and Five Security Services



Security Mechanisms



Layered Defense: Tactical Security Technology Integration



Relation between services and mechanisms

Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

Information Warfare

If we can defeat them sitting at home……who needs to fight with tanks and guns!!!!

References:

[1] Cryptography and Network Security by B. Forouzan

[2] Security in Computing by Pfleeger and Pfleeger

[3] Principles of Information Security by M. Whitman

[4] Management of Information Security by M. Whitman

[5] Cybersecurity by Nina Godbole and Sunit Belapure