

Chapter 1

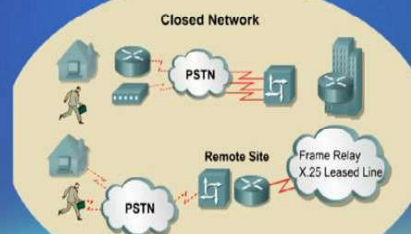
Introduction to Network Security

ITT450

Copyright 2010

1

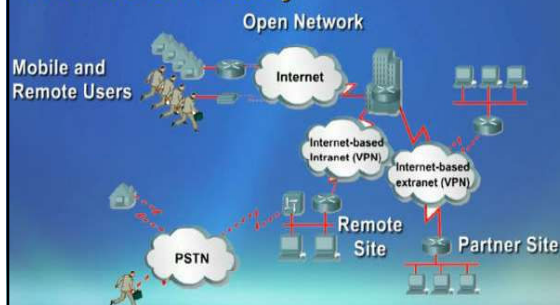
The Closed Network



Copyright 2010

2

The Network Today



Copyright 2010

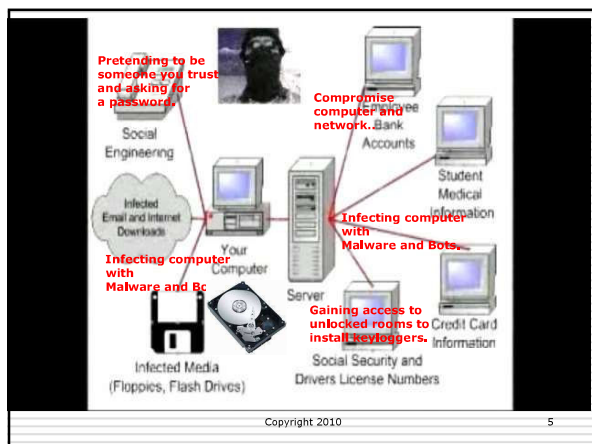
3

Unsecure behaviors:

- ✓ **Compromise computer and network.**
- ✓ **Infecting computer with Malware and Bots.**
- ✓ **Pretending to be someone you trust and asking for a password.**
- ✓ **Gaining access to unlocked rooms to install keyloggers.**

Copyright 2010

4



Copyright 2010

5



Copyright 2010

6



What is Network Security?

“**Network security** is a branch of **computer science** that addresses enforcement of ‘**secure behavior**’ on the operation of computers”.

Copyright 2010

9

What is Network Security?

.....taking physical and software preventive measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform and computing environment for all computers, users and programs.

Copyright 2010

What is Network Security?

Network Security is a PROCESS, not an end state.

Network Security is a JOURNEY, not a destination.

Copyright 2010

11

Assets

□ A network-based system has 3 assets:

- Hardware
- Software
- Data

Copyright 2010

12

3 Goals / Objectives of Security

to protect and assure:

- ✓ **confidentiality (C)**
 - ✓ **integrity (I)**
 - ✓ **availability (A)**
- of the assets.

Copyright 2010

Confidentiality

"Assets are only accessible to authorized person"

□ also called secrecy or privacy.

Copyright 2010

Integrity

"Assets can only be modified by authorized person in an authorized ways."

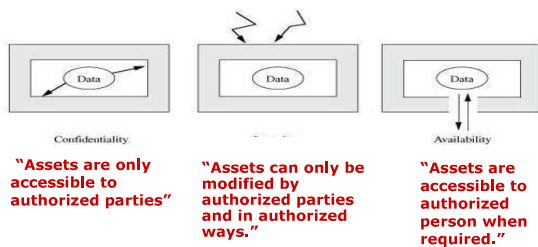
Copyright 2010

Availability

"Assets are accessible to authorized person when they required."

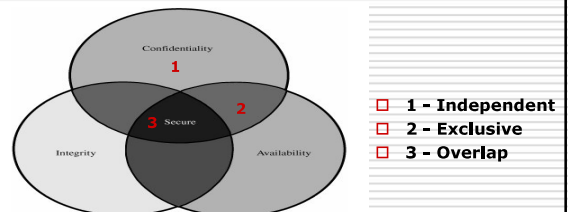
Copyright 2010

Example: How 3 goals of security secure data ?



Copyright 2010

Relationship between: C I A



Copyright 2010

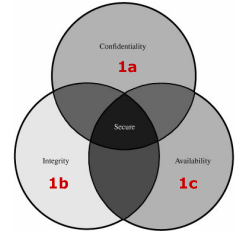
Relationship between C I A

Process of balancing all the 3 goals --> difficult.
Challenge in building a secure system --> finding the right balance among the 3 goals.

Copyright 2010

Relationship between : C I A in building secured systems

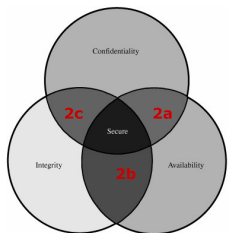
- 1a- Example of **Independent environment**: strong protection of confidentiality, can restrict integrity and availability.



Copyright 2010

Relationship between : C I A in building secured systems

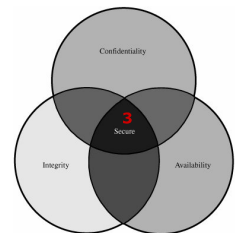
- 2a- Example of **Exclusive environment**: good protection of confidentiality and availability, can restrict integrity.



Copyright 2010

Relationship between : C I A in building a secured systems

- 3- Example of **Overlap environment**: weak protection of confidentiality, availability and integrity, can overlap all those 3 aspects.



Copyright 2010

Vulnerability

- A **vulnerability** is a **weakness** in the assets which can be exploit to cause loss or harm.

Copyright 2010

23

Hardware Vulnerabilities

- Examples :
 - Computers been drenched with water, burned, frozen.
 - Computing devices been spilled by drinks, or other kinds of food.
 - Mice have chewed cables.
 - Engineered moving parts in computer had been exposed to dust.
 - Computer been kicked, slapped, bumped & punched.
 - Machines been shot with guns, stabbed with knives, and smashed with things.
 - Computer been bombs, fires, and collisions.
 - Using external devices such as screwdrivers to **short-out circuit boards and other components.**

Copyright 2010

24

Software Vulnerabilities

- ☐ Software Deletion
 - accidentally erased, destroyed or replaced a file
- ☐ Software Modification
 - maliciously modified a program to fail or crash when certain conditions are met
 - Installed a program that overtly does one thing while covertly doing another
 - Installed a program that is dangerous such as virus, worm, trojan horse and logic bomb
- ☐ Software Theft
 - unauthorized copy of software

Copyright 2010

25

Assets and Vulnerabilities

- ☐ A network-based system has 3 assets:
 - Hardware
 - Software
 - Data
- ☐ Which one is the most important?

Copyright 2010

26

Threat

- ☐ A **threat** is a set of conditions that has potential to cause loss or harm.

Copyright 2010

Vulnerability vs Threat

- ☐ **Threat** exploits **vulnerabilities** of the assets.
- ☐ A **threat** can be block by controlling a **vulnerability**.

Copyright 2010

Vulnerability vs Threat



Which one is Threat?
Which one is Vulnerability?

Copyright 2010

Vulnerability vs Threat



Which one is Threat?
Which one is Vulnerability?

Copyright 2010

Vulnerability vs Threat



Which one is Threat?
Which one is Vulnerability?

Copyright 2010

Vulnerability vs Threat



Which one is Threat?
Which one is Vulnerability?

Copyright 2010

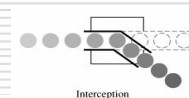
4 types of Threats

- ☐ Interception,
- ☐ Interruption,
- ☐ Modification,
- ☐ Fabrication

Copyright 2010

33

4 types of threats



Interception



Interruption



Modification



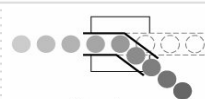
Fabrication

Copyright 2010

34

Interception

- ☐ Gaining unauthorized access to an asset.
- ☐ An **interception** (interchange) means that unauthorized party (person, program or computing system) has gained access to an asset.



Interception

Copyright 2010

35

Interruption

- ☐ Making an asset unavailable/unusable.
- ☐ An **interruption** (disruption, disturbance) means an asset of the system becomes lost, unavailable, or unusable.
- ☐ Example :
 - malicious destruction of a hardware device,
 - removal of a program or data file, or
 - malfunction (failure) of an operating system.



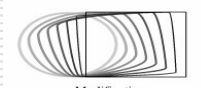
Interruption

Copyright 2010

36

Modification

- Changing the content or value of an asset.
- Modification (alteration, change) means an unauthorized party not only access, but tamper or change an asset
- Example :
 - change the content of database,
 - alter a program so that it performs wrong calculation, or
 - modify data being transmitted electronically.



Modification

Copyright 2010

37

Fabrication

- Creation of counterfeit objects on an asset.
- Fabrication (untruth, falsehood) means unauthorized party might create a counterfeit objects on a computing system.
- Example :
 - the intruder may insert false messages to a network communication system, or
 - add false records to an existing database.

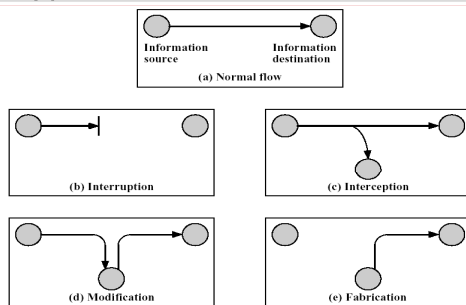


Fabrication

Copyright 2010

38

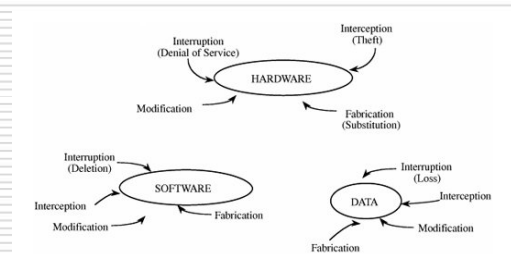
4 types of threats



Copyright 2010

39

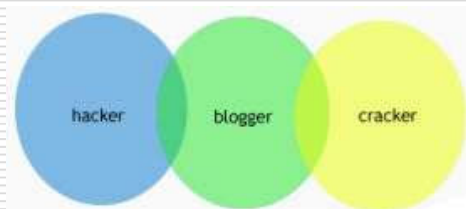
Vulnerabilities vs Threats in Computing System



Copyright 2010

40

Different terms of 'Malicious Person'



Copyright 2010

Different terms of 'Malicious Person'

Hacker

- are most often programmers
- enjoys programming and good at programming quickly
- enjoys exploring the details of programmable systems
- an expert at a particular program
- likes to explore the computers in order to know the details of the programmable system and discover how the system works.
- hacker generally does not have intention destroy data maliciously or to steal things.
- They might discover holes within systems and the reasons for such holes. Hackers constantly seek further knowledge, freely share what they have discovered, and never intentionally damage system or data.

Copyright 2010

Different terms of 'Malicious Person'

Cracker

- ❑ breaks through the system's security and proves to be far more dangerous than the hackers
- ❑ a person who breaks security on a system without permission
- ❑ A cracker is a technical person who has mastered the art of breaking systems
- ❑ the people who were able to crack the protection mechanisms
- ❑ who breaks into the system integrity of remote machines with malicious intent
- ❑ their activities is wrong on the side of law
- ❑ destroy vital data, deny legitimate users service, or cause problems for their victims
- ❑ cracker who is often termed to be a cyber burglar brings out significant harm to the network or steals the information like passwords or credit card numbers.

Copyright 2010

Hacker vs Cracker

- ❑ A **hacker** is a person intensely interested in the workings of any computer operating system. Hackers are most often programmers. They obtain advanced knowledge of operating systems and programming languages. They might discover holes within systems and the reasons for such holes. Hackers constantly seek further knowledge, freely share what they have discovered, and never intentionally damage data.
- ❑ A **cracker** is one who breaks into or otherwise violates the system integrity of remote machines with malicious intent. Having gained unauthorized access, crackers destroy vital data, deny legitimate users service, or cause problems for their targets. Crackers can easily be identified because their actions are malicious.

http://searchwindowssecurity.techtarget.com/tip/1,289483,sid45_gci998037,00.html

Copyright 2010

44

Different terms of 'Malicious Person'

Hactivism

- ❑ described as person hacking for political reasons
- ❑ hacker use his skills to forward political agenda
- ❑ example : web-page defacement of some well-selected site with a related message
- ❑ planting a virus or logic bomb at some company

Script kiddies

- ❑ use scripts and programs written by others to perform their intrusions
- ❑ assumed to be incapable of producing their own tools, and lacks proper understanding of how tools work
- ❑ no skills, no knowledge
- ❑ get tools from crackers or hackers

Copyright 2010

45

Different terms of 'Malicious Person'

White hat

- ❑ Good guys
- ❑ Hackers who 'do the right thing' such as exposing security problems to vendor

Black hat

- ❑ Bad guys
- ❑ Hacker that uses their skills to commit a crime

Grey hat

- ❑ Are somewhere between the two

Copyright 2010

46

White, Black or Grey

- ❑ "As in Westerns, where the "bad guys" wore black hats, and "good guys" wore white hats, the term "black hat" is used for designation of the attacking malefactor, but "white hat" is used for the expert in the field of computer safety, who tries to protect systems against breaking. "Black hat" tries to penetrate into system, a "white hat" finds weak spots and corrects defects. It is obvious, that people which work on two fronts (sometimes they attack systems, and sometimes protect them), are called "gray hats".

<http://www.crime-research.org/news/2003/06/Mess2803.html>

Copyright 2010

47

Black Hat

- ❑ Black hat is used to describe **hacker who breaks into a computer system or network with malicious intent.**
- ❑ Black hat hacker takes advantage of the break-in, perhaps destroying files or stealing data for some future purpose.

from: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci550815,00.html

Copyright 2010

48

White Hat

- White hat describes a hacker who identifies a security weakness in a computer system or network but, instead of taking malicious advantage of it, exposes the weakness in a way that will allow the system's owners to fix the breach before it is can be taken advantage by others.

from : http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci550815,00.html