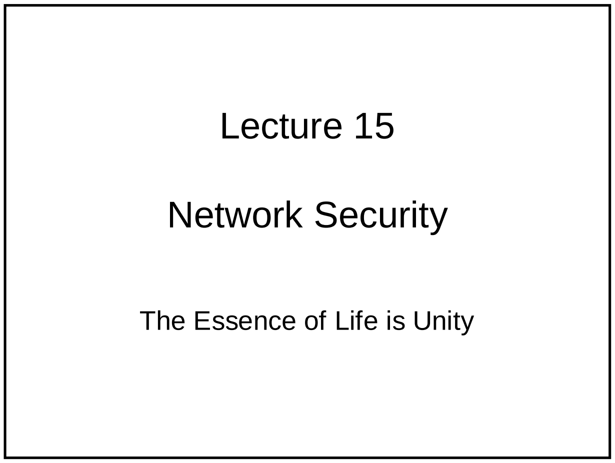
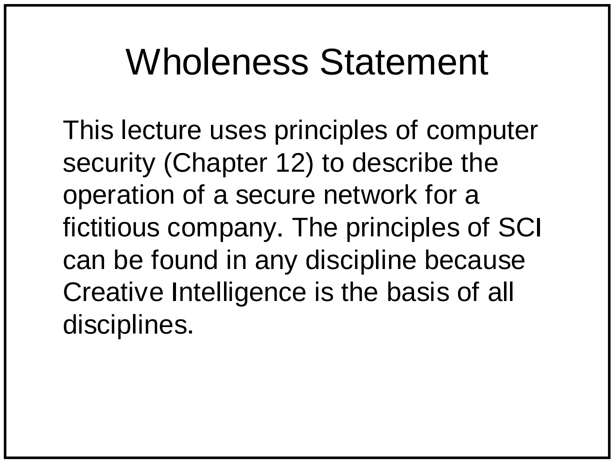


Lecture 15

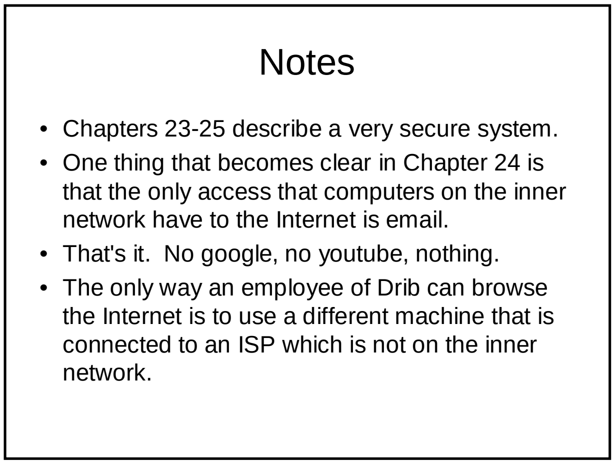
Network Security

The Essence of Life is Unity



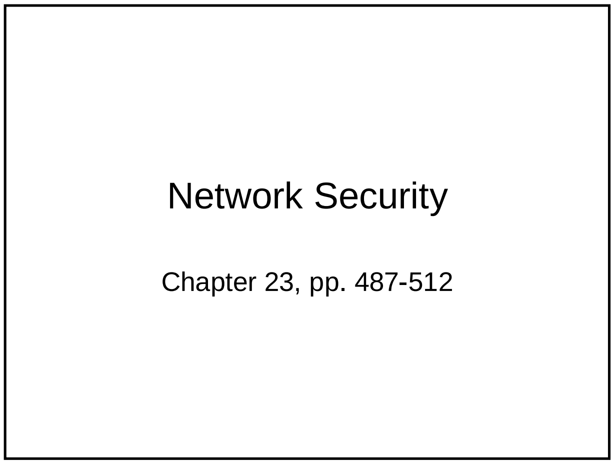
Wholeness Statement

This lecture uses principles of computer security (Chapter 12) to describe the operation of a secure network for a fictitious company. The principles of SCI can be found in any discipline because Creative Intelligence is the basis of all disciplines.



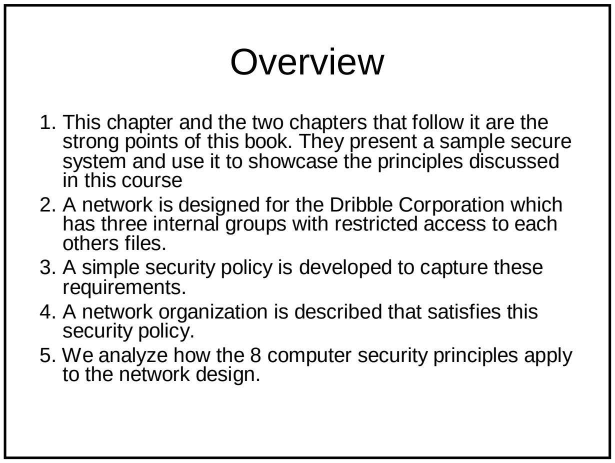
Notes

- Chapters 23-25 describe a very secure system.
- One thing that becomes clear in Chapter 24 is that the only access that computers on the inner network have to the Internet is email.
- That's it. No google, no youtube, nothing.
- The only way an employee of Drib can browse the Internet is to use a different machine that is connected to an ISP which is not on the inner network.



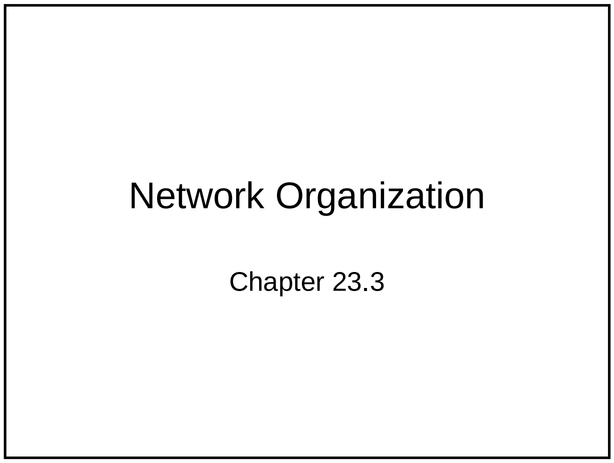
Network Security

Chapter 23, pp. 487-512



Overview

1. This chapter and the two chapters that follow it are the strong points of this book. They present a sample secure system and use it to showcase the principles discussed in this course
2. A network is designed for the Dribble Corporation which has three internal groups with restricted access to each others files.
3. A simple security policy is developed to capture these requirements.
4. A network organization is described that satisfies this security policy.
5. We analyze how the 8 computer security principles apply to the network design.



Network Organization

Chapter 23.3

Introduction

- Goal: apply concepts, principles, mechanisms discussed previously in the class to a particular situation
  - Focus here is on designing a secure network
  - We start with a description of company
  - Then define policy
  - Show how policy drives design

The Drib

- Builds and sells dribbles
- Developing network infrastructure allowing it to connect to Internet to provide mail, web presence for customers, suppliers, other partners

Specific Problems

- Hostile takeover by competitor in progress
  - Lawyers, corporate officers need access to development data
  - Developers cannot have access to some corporate data

Three Internal Organizations

- Customer Service Group (CSG)
  - Maintains customer data
  - Interface between clients, other internal organizations
- Development Group (DG)
  - Develops, modifies, maintains products
  - Relies on CSG for customer feedback
- Corporate Group (CG)
  - Handles patents, lawsuits, etc.
- The security policy describes the way that information flows between these three groups
  - **Policy**: minimize threat of data being leaked to unauthorized entities

Security Policy Goals

1. Keep sensitive information (such as company plans, new product data, etc.) confidential, on a need to know basis
2. Only employees who handle purchases can access customer data
3. Releasing sensitive data requires the consent of the company's officials and lawyers.

Data Classes

Public data (PD):
- available to all

Development data for existing products (DDEP):
- available to CG, DG only

Development data for future products (DDFP):
- available to DG only

Corporate data (CpD):
- available to CG only

Customer data (CuD):
- available to CSG only

Nature of Information Flow

- Public data
  - – Specs of current products, marketing literature
- CG, DG share info for planning purposes
  - – Problems, patent applications, budgets, etc.
- Private
  - – CSG: customer info like credit card numbers
  - – CG: corporate info protected by attorney privilege
  - – DG: plans, prototypes for new products to determine if production is feasible before proposing them to CG

Data Class Changes

- DDFP → DDEP: as products implemented
- DDEP → PD: when deemed advantageous to publicize some development details
  - – For marketing purposes, for example
- CpD → PD: as privileged info becomes public through mergers, lawsuit filings, etc.
- Note: no provision for revealing CuD directly
  - – This protects privacy of Drib's customers

User Classes

- Outsiders (O): members of public
  - – Access to public data
  - – Can also order, download drivers, send email to company
- Developers (D): access to DDEP, DDFP
  - – Cannot alter development data for existing products
- Corporate executives (C): access to CD
  - – Can read DDEP, DDFP, CuD but not alter them
  - – Sometimes can make sensitive data public
- Employees (E): access to CuD only

Reclassification of Data

- Who must agree for each reclassification?
  - – C, D must agree for DDFP → DDEP
    - Member of D says new product is ready, member of C approves the reclassification
  - – C, E must agree for DDEP → PD
    - Member of E makes request, member of C approves
  - – C can do CpD → PD
    - *Two* members of C must agree to this
- Separation of privilege
  - – At least two different people must agree to the reclassification
  - – When appropriate, the two must come from different user classes

Access Control Matrix for Policy

	O	**D**	**C**	**E**
PD	*r*	*r*	*r*	*r*
DDEP		*r*	*r*	
DDFP		*r*, *w*	*r*	
CpD			*r*, *w*	
CuD	*w*		*r*	*r*, *w*

r is read right, *w* is write right

Main Point

1. An Access Control Matrix is used to describe the accesses that each class of user has to each class of data in a comprehensive manner. When the pure nature of CI comes to our awareness, application of CI to individual life is comprehensive.

Type of Policy

- Mandatory policy
  - – Members of O, D, C, E cannot change permissions to allow members of another user class to access data
- Discretionary component
  - – Within each class, individuals may have control over access to files they own

Consistency

- Need to be sure that everyone has the privileges needed to get their job done (which principle?)
- Need to do some consistency checks to be sure the ACL matches the policy goals

Security Policy Goals

1. Keep sensitive information (such as company plans, new product data, etc.) confidential, on a need to know basis
2. Only employees who handle purchases can access customer data
3. Releasing sensitive data requires the consent of the company's officials and lawyers.

Consistency Check: Goal 1

- Goal 1: keep sensitive info confidential
  - – Developers (D)
    - Need to read DDEP, DDFP, and to alter DDFP
    - No need to access CpD, CuD as don't deal with customers or decide which products to market
  - – Corporate executives (C)
    - Need to read, alter CpD, and read DDEP
- This matches access permissions

Consistency Check: Goal 2

- Goal 2: only employees who handle purchases can access customer data, and only they and customer can alter it
  - – Outsiders
    - Need to alter CuD, do not need to read it
  - – Customer support
    - Need to read, alter CuD
- This matches access permissions

Consistency Check: Goal 3

- Goal 3: releasing sensitive info requires corporate approval
  - – Corporate executives
    - Must approve any reclassification
    - No-one can write to PD, *except* through reclassification
- This matches reclassification constraints

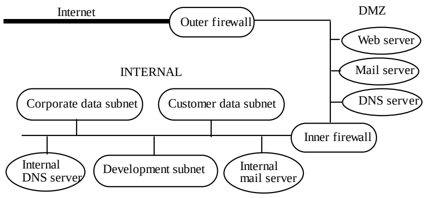
Availability

- Drib world-wide multinational corp
  - Does business on all continents
- Imperative anyone be able to contact Drib at any time
  - Requirement: Drib's systems be available 99% of the time
    - 1% allowed for planned maintenance, unexpected downtime

Network Design

Network Organization

- Partition network into several subnets
  - Guards between them prevent leaks



Firewalls

- Firewall: Host that mediates access to a network
  - Allows, disallows accesses based on configuration and type of access
- Filtering Firewall: controls access based on attributes of packets and packet headers
  - Such as destination address, port numbers, options, etc.
  - Also called a *packet filtering firewall*
  - Does not control access based on content
  - Examples: routers, other infrastructure systems

Two Ways to View a Firewall

- Access control mechanism
  - Determines which traffic goes into and out of a network
- Audit mechanism
  - Analyzes packets that enter
  - Takes action based upon the analysis
    - Leads to traffic shaping, intrusion response, etc.

DMZ

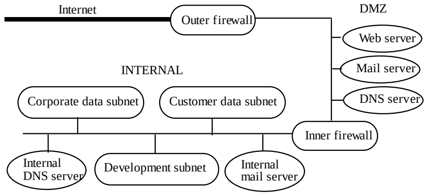
- Portion of network separating purely internal network from external network
  - Allows control of accesses to some trusted systems inside the corporate perimeter
  - If DMZ systems breached, internal systems still safe
  - Can perform different types of checks at boundary between internal and DMZ networks and between DMZ and Internet network

Proxy

- Intermediate agent or server acting on behalf of endpoint without allowing a direct connection between the two endpoints
  - So each endpoint talks to proxy, thinking it is talking to other endpoint
  - Proxy decides whether to forward messages, and whether to alter them

Network Organization

- Partition network into several subnets
  - Guards between them prevent leaks



Analysis of Drib Network

- Security policy: “public” entities on outside but may need to access corporate resources
  - Those resources provided in DMZ
- No internal system communicates directly with systems on Internet
  - Restricts flow of data to “public”
  - For data to flow out, must pass through DMZ

Implementation

- Conceals all internal addresses
  - Give each host a non-private IP address
    - Inner firewall never allows those addresses to leave internal network
- Easy as all services are proxied by outer firewall
  - Email is a bit tricky …

DMZ Mail Server

- Problem: DMZ mail server must know address in order to send mail to internal destination
  - Could simply be distinguished address that causes inner firewall to forward mail to internal mail server
- Internal mail server needs to know DMZ mail server address
  - Solved in same way as above

DMZ Mail Server (cont.)

- Performs address, content checking on *all* email
- Goal is to hide internal information from outside, but be transparent to inside
- Receives email from Internet, forwards it to internal network
- Receives email from internal network, forwards it to Internet

DMZ Web Server

- In DMZ so external customers can access it without going onto internal network
  - If data needs to be sent to internal network (such as for an order), transmission is made separately and not as part of transaction

DMZ Web Server (cont.)

- Accepts, services requests from Internet
- Never contacts servers or information sources in the internal network
- Server is www.drib.org and uses IP address of outer firewall when it must supply one

Updating DMZ Web Server

- Clone of web server kept on internal network
  - Called "WWW-clone"
- All updates done to WWW-clone
  - Periodically admins copy contents of WWW-clone to DMZ web server
- DMZ web server runs SSH server
  - Used to do updates as well as maintenance and configuration
  - Secured like that of DMZ mail server

DMZ DNS Server

- Supplies DNS information for some hosts to DMZ:
  - DMZ mail, web, log hosts
  - Internal trusted administrative host
    - Not fixed for various reasons; could be …
  - Inner firewall
  - Outer firewall
- Note: Internal server addresses not present
  - Inner firewall can get them, so DMZ hosts do not need them

DMZ Log Server

- DMZ systems all log information
  - Useful in case of problems or attempted attacks
- Problem: attacker will delete or alter logs if security is successfully compromised
  - So save logs on a different machine
- Log server saves logs to file, also to write-once media
  - Latter just in case log server is compromised
- Runs SSH server
  - Constrained in same way as SSH server on DMZ mail server is constrained

Main Point

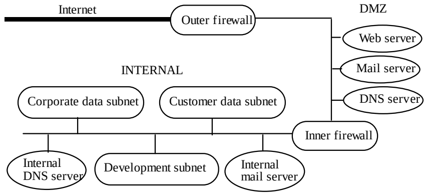
2. The DMZ is what is between the inner and outer firewalls. These two firewalls strictly control access to the DMZ both from the Internet and the internal net. The firewalls epitomize the discriminating and integrating nature of Creative Intelligence.

Summary

- Each server knows only what is needed to do its task
  - Compromise will restrict flow of information but not reveal info on internal network
- Operating systems and software:
  - All unnecessary features and servers disabled
  - Simplifies OS/servers (which principle?)
- Proxies prevent direct connection to internal servers
  - For all services from internal network to DMZ (except SSH); SSH is constrained by source (trusted administrative computer) and/or destination (DMZ server)

Network Organization

- Partition network into several subnets
  - Guards between them prevent leaks



Internal Network

- Goal: guard against unauthorized access to information
  - “read” means fetching file, “write” means depositing file
- For now, ignore email, updating of DMZ web server, internal trusted administrative host
- Internal network organized into 3 subnets, each corresponding to Drib group
  - Firewalls control access to subnets

Internal Mail Server

- Can communicate with hosts on subnets in two possible ways
  - Subnet may have mail server
    - Internal DNS need only know subnet mail server’s address
  - Subnet may allow mail to go directly to destination host
    - Internal DNS needs to know addresses of all destination hosts
- Either satisfies policy

Analysis

- DMZ servers never communicate with internal servers
  - All communications done via inner firewall
- Only client to DMZ that can come from internal network is SSH client from trusted administrative host
  - Authenticity established by public key authentication
- Only data non-administrative employees can alter are web pages
  - Even there, they do not access DMZ

Analysis

- Only data from DMZ is customer orders and email
  - Customer orders already checked for potential errors, enciphered, and transferred in such a way that it cannot be executed
  - Email thoroughly checked before it is sent to internal mail server

8 Computer Security Design Principles

Design Principles

- **Least privilege**: containment of internal addeses (also a means of confinement)
- **Complete mediation**: inner firewall mediates every access involving the DMZ and the internal networks
- **Separation of privilege**: internal network has to get through both inner and outer firewalls to get to the Internet and vice versa
- **Least common mechanism**: firewall software, mail server software, DNS software are all on separate machines

Outer Firewall Configuration

- In Bell-LaPadula terms,
  - public is unclassified, internal network is secret
  - public cannot read up (cannot access internal network)
  - internal network cannot write down (cannot access Internet).
- Public needs to be able to access the Web server and the mail server, and no other services.
- Outer firewall allows public to access Web and mail servers.
- But public uses same IP address for both, namely the IP address of the outer firewall
- Outer firewall is a proxy-based firewall, has proxies for Web, DNS, and mail servers.

Inner Firewall Configuration

- Inner firewall blocks all access to the inner network, except for those accesses that are explicitly configured (fail-safe defaults).
- Also blocks packets from entering the DMZ unless explicitly configured to do so.
- It allows
  a. inner mail server to access DMZ mail server
  b. inner DNS server to send information to DMZ DNS server
  c. system administrators can access DMZ from a trusted administrative server using SSH
- That's it. In particular, any attempt to access the Web is blocked!

DMZ

- Four servers reside in the DMZ
  - (mail, WWW, DNS, and log servers)
- DMZ Mail server (a separate machine)
- When an email message is received from Internet:
  a. Reassembles message
  b. Checks for malicious content
  c. Changes addresses of outer firewall (which is how mail server is known to outside world) to that of internal mail server and forwards the mail to the internal mail server

Email

- To send a message from the internal network to the Internet
  a. Reassembles message
  b. Checks for malicious content (and maybe for proprietary information).
  c. All internal addresses are replaced with "drib.org" (the name of the outside firewall).

Web Server

- DMZ WWW Server (a separate machine)
  - Does not contact any servers or information sources on the internal network and it contains no confidential data.
  - Accessed from the Internet using address of outer firewall

New Releases

- Developers release updates to the web site to an internal machine named WWW-Clone.
- Developers are ***NOT*** allowed access to the DMZ WWW server.
- A system administrator uses SSH to transfer from WWW-Clone to DMZ WWW server.
- DMZ WWW server invokes a simple program to validate customer data and encrypt it.
- Encrypted with the public key of the CSG (Customer Service Group).
- System administrator connects to WWW server using SSH to copy encrypted file to internal CSG network.

DMZ DNS server

- Contains entries for the following:
  a. DMZ mail, Web, and log hosts
  b. Internal trusted administrative host (how administrator connects using SSH)
  c. Outer firewall
  d. Inner firewall

- The limited information in the DNS server reflects the principle of least privilege.
- It only contains entries needed so that systems in the DMZ can talk to each other.

DMZ Log Server

- All DMZ machines have logging turned on.
- On separate machine to reduce chance that attacker can delete log files.
- Log machine writes logs to a file and to a write-once media.
- System administrator can use SSH to copy logs from DMZ log server to internal network or can go to the log server and retrieve the write-once media.

Summary

- Each of the four servers has the minimum amount of knowledge of the network that is needed to perform their function.
- OS on DMZ servers has a reduced kernel. (Economy of Mechanism)

The Internal Network

- Each subnet has its own firewall.
- Now we are worrying about internal attackers, not external attackers.
- Firewall on the developer subnet only allows read access from the corporate network.
- Firewall on the corporate subnet allows no read and write access from either developer or CSG subnets.
- Firewall on the CSG subnet only allows read access from the corporate network.
- Also allows encrypted data files to be written from DMZ (but this writing is mediated by the inner firewall).
- Each subnet may have its own mail server.
- There is an internal web server (WWW-Clone) that all subnets can access.

The Internal Network

- Trusted administrative server is physically accessible only to system administrators.
- Only data in the DMZ that non-administrators can alter is web pages but they must do that indirectly through WWW-Clone.
- The only data written from DMZ is encrypted customer data.
- This whole scheme trusts the firewall software not to have vulnerabilities.
- Separation of privilege is a backup measure in case some do.
- DMZ log server contains an intrusion detection mechanism.

Main Point

3. The WWW-Clone machine on the internal network is a clone of the DMZ web server. WWW-Clone is the developers machine. Developers do not have access to the DMZ web server. This is in keeping with Clark-Wilson's separation of function principle. Regular practice of the TM technique cultivates the mind to think like nature does.

Footnotes that Note Security Principles

- In the following, instances of a particular Chapter 12 principle have been collected together.
- There is a footnote number included in square brackets at the end of each instance.
- The footnote number corresponds to the footnotes in Chapter 23.

Principle of least privilege

1. Information classified into five classes [1]
2. Users are classified into four classes [4]
3. Containment of internal addresses [23, 34]
4. Violated because administrators have full control over the DMZ servers. But,
   a. Can only connect to DMZ machine through specific machine in internal network
   b. System administrators are trusted
   c. Administrators use SSH protocol. [39]
5. Email sanitized by removing internal network address. [43]

Principle of least privilege

6. The Web Server identifies itself as "www.drib.org" and uses the IP address of the outside firewall. [45]
7. Do not keep valuable information online; restrict who can see it. [48]
8. DMZ DNS server only has IP addresses needed by machines in the DMZ [52]
9. The use of write-once media in the log server. (Can't alter it and can only destroy it if they have access to the room containing the log server). [55]
10. DMZ servers know only about the inner firewall's address and the trusted administrative host's address. (60)

Principle of Fail-Safe defaults

1. The firewall will block all traffic except for that specifically authorized to enter.[36]
2. Only public key used to encrypt customer data is on Web Server machine, not the private key. [50]
3. Deny unknown connections rather than allowing them and then authenticating them. [51]
4. The use of write-once media in the log server. (Deny all modifications to write-once media) [56]

Principle of Economy of Mechanism

1. Design the firewall mechanisms to be as simple as possible. [33]

Principle of Complete Mediation

1. The inner firewall mediates every access involving the DMZ and the internal network.[25]

Principle of Open Design

1. Policy and rules are not secret. (But are not available to the public!) [2]

Principle of Psychological Acceptability

1. Configuration of firewalls should be so easy to do that administrators will feel comfortable doing it.

Principle of Separation of Privilege

1. Users are classified into four classes. Moving information from one class to another requires approval of more than one user. [3]
2. Going out of the inner network to the Internet requires that several criteria be met. [26]
3. Defense in depth: In order to attack a system in the DMZ by bypassing the firewall checks, the attacker must know something about the internal addresses of the DMZ.

Principle of Separation of Privilege

4. A developer who is authorized to update the company web site copies a new version to the WWW-Clone machine. A system administrator then copies from WWW-Clone to the actual web server. [46]
5. Cryptographic key is needed to read customer data. Need both conventional access to the file and the key. [49]
6. Separate log machine that writes files to disk and to a write-once medium (to delete a log entry you need to be able to access the disk and to be able to modify a write-once medium which is impossible). [53]

Principle of Least Common Mechanism

1. The firewalls are distinct computers, as are the DMZ servers, leading to a duplication rather than a sharing of network services. [27]

(See the note below)

- Note: the principle of least common mechanism was covered in detail in Chapter 16 (which we skipped). In a nutshell, consider an OS that implements multilevel security as modeled by Bell-LaPadula. Now assume that a Trojan horse is run by a user with top secret privileges. Bell-LaPadula will prevent the Trojan horse from writing to a unclassified file (no write down). However, Bell-LaPadula does not prevent the Trojan horse from renaming a file using a name that contains top secret information. A program running with unclassified privileges could read the file name (but not the contents).

- Note (cont.): Other ways of covertly smuggling out information in a way that Bell-LaPadula would not detect include hogging the CPU or moving the disk heads in a particular way. Read the first part of Chapter 16 if this sounds interesting to you. The principle of least common mechanism implies that if two processes are running on the same machine they can in principle share information covertly. But it also implies that if two processes are running on different machines that are not connected by a network, then covert sharing of information is not possible.

CONNECTING THE PARTS OF KNOWLEDGE WITH THE WHOLENESS OF KNOWLEDGE

1. The Internet is a dangerous place.

2. The DMZ is a buffer zone between the internal network and the Internet.

3. Transcendental Consciousness is a field of complete security; insecurity arises when there is duality.

4. Wholeness moving within itself: in Unity Consciousness duality is no longer the experience, rather unity and security is a living reality.