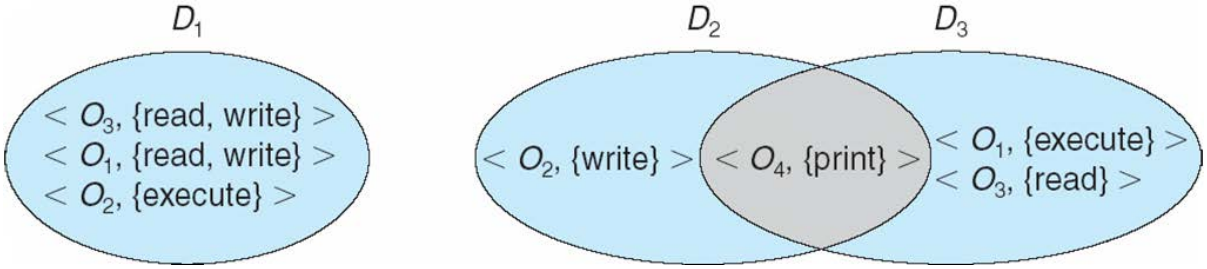
Protection and Security

Principles of Protection

Guiding principle – principle of least privilege
Programs, users and systems should be given just enough privileges to perform their tasks

Domain Structure

Access-right = <*object-name, rights-set*>
where *rights-set* is a subset of all valid operations that can be performed on the object.
Domain = set of access-rights



System consists of 2 domains:

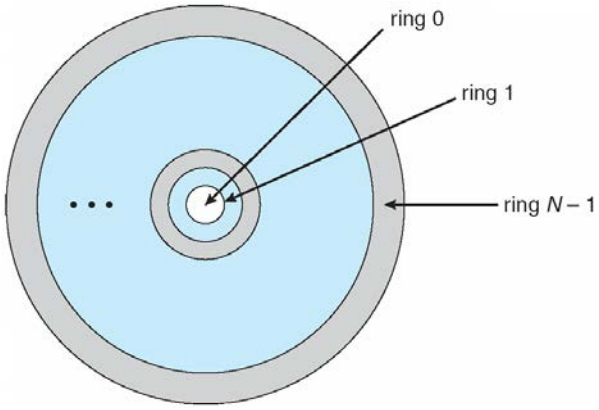
1. User
2. SupervisonUNIX

Domain = user-id

- Domain switch accomplished via file system
- Each file has associated with it a domain bit (setuid bit)
- When file is executed and setuid = on, then user-id is set to owner of the file being executed. When execution completes user-id is reset

Domain Implementation (MULTICS)

Let D_i and D_j be any two domain rings
If $j < I$ Þ D_i Í D_j



Access Matrix

View protection as a matrix (*access matrix*)
Rows represent domains
Columns represent objects
Access(i, j) is the set of operations that a process executing in Domain$_i$ can invoke on Object$_j$

domain \ object	F_1	F_2	F_3	printer
D_1	read		read	
D_2				print
D_3		read	execute	
D_4	read write		read write	

Use of Access Matrix
If a process in Domain D_i tries to do "op" on object O_j, then "op" must be in the access matrixnCan be expanded to dynamic protection
Operations to add, delete access rights
Special access rights:
□ *owner of O_i* □ *copy op from O_i to O_j* □ *control – D_i can modify D_j access rights*
□ *transfer – switch from domain D_i to D_j*
Access matrix design separates mechanism from policy
Mechanism
□ Operating system provides access-matrix + rules
□ If ensures that the matrix is only manipulated by authorized agents and that rules are strictly enforced
Policy
□ User dictates policy
□ Who can access what object and in what mode
Implementation of Access Matrix
Each column = Access-control list for one object
Defines who can perform what operation.

Domain 1 = Read, Write
Domain 2 = Read
Domain 3 = Read

Each Row = Capability List (like a key)
Fore each domain, what operations allowed on what objects.
Object 1 – Read
Object 4 – Read, Write, Execute
Object 5 – Read, Write, Delete, Copy

Access Matrix of Figure A With Domains as Objects

object / domain	F_1	F_2	F_3	laser printer	D_1	D_2	D_3	D_4
D_1	read		read			switch		
D_2				print			switch	switch
D_3		read	execute					
D_4	read write		read write		switch			

Access Matrix with *Copy* Rights

object / domain	F_1	F_2	F_3
D_1	execute		write*
D_2	execute	read*	execute
D_3	execute		

(a)

object / domain	F_1	F_2	F_3
D_1	execute		write*
D_2	execute	read*	execute
D_3	execute	read	

(b)

Access Matrix With *Owner* Rights

domain \ object	F_1	F_2	F_3
D_1	owner execute		write
D_2		read* owner	read* owner write
D_3	execute		

(a)

domain \ object	F_1	F_2	F_3
D_1	owner execute		write
D_2		owner read* write*	read* owner write
D_3		write	write

(b)

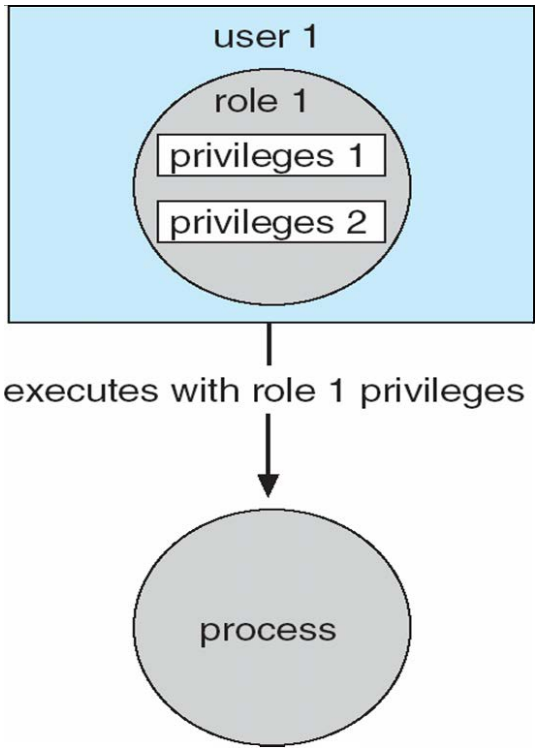
Modified Access Matrix of Figure B

domain \ object	F_1	F_2	F_3	laser printer	D_1	D_2	D_3	D_4
D_1	read		read			switch		
D_2				print			switch	switch control
D_3		read	execute					
D_4	write		write		switch			

Access Control

Protection can be applied to non-file resources
Solaris 10 provides role-based access control **(**RBAC**)** to implement least privilege
Privilege is right to execute system call or use an option within a system call

Can be assigned to processes
Users assigned roles granting access to privileges and programs
Role-based Access Control in Solaris 10



Revocation of Access Rights

Access List – Delete access rights from access list
Simple
ImmediatenCapability List – Scheme required to locate capability in the system before capability can be revoked

- Reacquisition
- Back-pointers
- Indirection
- Keys

Capability-Based Systems

- Hydra
- Fixed set of access rights known to and interpreted by the system
- Interpretation of user-defined rights performed solely by user's program; system provides access protection for use of these rightsnCambridge CAP System
- Data capability - provides standard read, write, execute of individual storage segments associated with object
- Software capability -interpretation left to the subsystem, through its protected procedures

Language-Based Protection

Specification of protection in a programming language allows the high-level description of policies for the allocation and use of resourcesnLanguage implementation can provide software for protection enforcement when automatic hardware-supported checking is unavailablenInterpret protection specifications to generate calls on whatever protection system is provided by the hardware and the operating system

Protection in Java 2

Protection is handled by the Java Virtual Machine (JVM)nA class is assigned a protection domain when it is loaded by the JVMnThe protection domain indicates what operations the class can (and cannot) performnIf a library method is invoked that performs a privileged operation, the stack is inspected to ensure the operation can be performed by the library

Stack Inspection

protection domain:	untrusted applet	URL loader	networking
socket permission:	none	*.lucent.com:80, connect	any

class:	gui:
	...
	get(url);
	open(addr);
	...
		get(URL u):
		...
		doPrivileged {
		open('proxy.lucent.com:80');
		}
		<request u from proxy>
		...
			open(Addr a):
			...
			checkPermission
			(a, connect);
			connect (a);
			...

The Security Problem:

Operating system security (OS security) is the process of ensuring OS integrity, confidentiality and availability.

OS security refers to specified steps or measures used to protect the OS from threats, viruses, worms, malware or remote hacker intrusions. OS security encompasses all preventive-control techniques, which safeguard any computer assets capable of being stolen, edited or deleted if OS security is compromised.

OS security encompasses many different techniques and methods which ensure safety from threats and attacks. OS security allows different applications and programs to perform required tasks and stop unauthorized interference.

OS security may be approached in many ways, including adherence to the following:

- Performing regular OS patch updates
- Installing updated antivirus engines and software
- Scrutinizing all incoming and outgoing network traffic through a firewall

- Creating secure accounts with required privileges only (i.e., user management)

Program Threats:

Operating system's processes and kernel do the designated task as instructed. If a user program made these process do malicious tasks then it is known as Program Threats. One of the common example of program threat is a program installed in a computer which can store and send user credentials via network to some hacker. Following is the list of some well known program threats.

- **Trojan Horse** - Such program traps user login credentials and stores them to send to malicious user who can later on login to computer and can access system resources.
- **Trap Door** - If a program which is designed to work as required, have a security hole in its code and perform illegal action without knowledge of user then it is called to have a trap door.
- **Logic Bomb** - Logic bomb is a situation when a program misbehaves only when certain conditions met otherwise it works as a genuine program. It is harder to detect.
- **Virus** - Virus as name suggest can replicate themselves on computer system .They are highly dangerous and can modify/delete user files, crash systems. A virus is generatlly a small code embedded in a program. As user accesses the program, the virus starts getting embedded in other files/ programs and can make system unusable for user.

System and Network Threats:

System threats refers to misuse of system services and network connections to put user in trouble. System threats can be used to launch program threats on a complete network called as program attack. System threats creates such an environment that operating system resources/ user files are mis-used. Following is the list of some well known system threats.

- **Worm** -Worm is a process which can choked down a system performance by using system resources to extreme levels.A Worm process generates its multiple copies where each copy uses system resources, prevents all other processes to get required resources. Worms processes can even shut down an entire network.
- **Port Scanning** - Port scanning is a mechanism or means by which a hacker can detects system vulnerabilities to make an attack on the system.
- **Denial of Service** - Denial of service attacks normally prevents user to make legitimate use of the system. For example user may not be able to use internet if denial of service attacks browser's content settings.

Cryptography as a Security Tool:

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. The term is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption).

Modern cryptography concerns itself with the following four objectives:

1) **Confidentiality** (the information cannot be understood by anyone for whom it was unintended)

2) **Integrity** (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)

3) **Non-repudiation** (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)

User Authentication:

Operating system (OS) authentication is a method for identifying an individual user with credentials supplied by the operating system of the user's computer. These credentials can be the OS password or can include digital certificates in the user's computer.

Possible benefits of using OS authentication include the following:

- You do not have to keep track of multiple user names and passwords; if the login to your computer is successful, you do not have to enter another user name and password to connect to the database.
- The database administrator (DBA) does not have to manage password changes, since that is changed on each user's computer or at the domain level.

Possible drawbacks of using OS authentication include these:

- Using operating system authentication with certain database products (those that do not use digital certificates in addition to user name and password) could be an increased security risk.
- If the password for an OS account becomes known, access is granted without the extra level of security of a different database account.
- Additional configuration in the database may be needed to support OS authentication.

Implementing Security Defenses:

Computer security is security applied to computing devices such as computers and smartphones, as well as computer networks such as private and public networks, including the whole Internet.

The field covers all the processes and mechanisms by which digital equipment, information and services are protected from unintended or unauthorized access, change or destruction, and is of growing importance due to the increasing reliance of computer systems in most societies.

It includes physical security to prevent theft of equipment and information security to protect the data on that equipment. It is sometimes referred to as "cyber security" or "IT security". Those terms generally do not refer to physical security, but a common belief among computer security experts is that a physical security breach is one

of the worst kinds of security breaches as it generally allows full access to both data and equipment.
Cybersecurity is the process of applying security measures to ensure confidentiality, integrity, and availability of data. Cybersecurity assures protection of assets, which includes data, desktops, servers, buildings, and most importantly, humans.

The goal of cybersecurity is to protect data both in transit and at rest. Countermeasures can be put in place in order to ensure security of data. Some of these measures include, but are not limited to, access control, awareness training, audit and accountability, risk assessment, penetration testing, vulnerability management, and security assessment and authorization.

Firewalling to Protect Systems and Networks:

The Internet has made large amounts of information available to the average computer user at home, in business and in education. For many people, having access to this information is no longer just an advantage, it is essential.

Yet connecting a private network to the Internet can expose critical or confidential data to malicious attack from anywhere in the world. Users who connect their computers to the Internet must be aware of these dangers, their implications and how to protect their data and their critical systems. Firewalls can protect both individual computers and corporate networks from hostile intrusion from the Internet, but must be understood to be used correctly.

We are presenting this information in a Q&A (Questions and Answers) format that we hope will be useful. Our knowledge of this subject relates to firewalls in general use, and stems from our own NAT and proxy firewall technology. We welcome feedback and comments from any readers on the usefulness or content.

We are providing the best information available to us as at date of writing and intend to update it at frequent intervals as things change and/or more information becomes available. However we intend this Q&A as a guide only and recommend that users obtain specific information to determine applicability to their specific requirements. (This is another way of saying that we can't be held liable or responsible for the content.)

Firewalls can be either hardware or software but the ideal firewall configuration will consist of both. In addition to limiting access to your computer and network, a firewall is also useful for allowing remote access to a private network through secure authentication certificates and logins.

Hardware firewalls can be purchased as a stand-alone product but are also typically found in broadband routers, and should be considered an important part of your system and network set-up. Most hardware firewalls will have a minimum of four network ports to connect other computers, but for larger networks, business networking firewall solutions are available.

Software firewalls are installed on your computer (like any software) and you can customize it; allowing you some control over its function and protection features. A software firewall will protect your computer from outside attempts to control or gain access your computer.

Computer Security Classifications:

As per the U.S. Department of Defense Trusted Computer System's Evaluation Criteria there are four security classifications in computer systems: A, B, C, and D. This is widely used specifications to determine and model the security of systems and of security solutions. Following is the brief description of each classfication.

S.N.	Classification Type	Description
1	Type A	Highest Level. Uses formal design specifications and verification techniques.Grants a high degree of assurance of process security.
2	Type B	Provides mandatory protection system. Have all the properties of a class C2 system. Attaches a sensitivity label to each object.It is of three types. **B1** - Maintains the security label of each object in the system.Label is used for making decisions to access control. **B2** - Extends the sensitivity labels to each system resource, such as storage objects, supports covert channels and auditing of events. **B3** - Allows creating lists or user groups for access-control to grant access or revoke access to a given named object.
3	Type C	Provides protection and user accountability using audit capabilities. It is of two types. **C1** - Incorporates controls so that users can protect their private information and keep other users from accidentally reading / deleting their data. UNIX versions are mostly Cl class. **C2** - Adds an individual-level

		access control to the capabilities of a Cl level system
4	Type D	Lowest level. Minimum protection. MS-DOS, Window 3.1 fall in this category.