❖ Confidentiality Policies

The Confidentiality Policy is aimed to prevent, identify and eliminate the risks of confidential data leakage.

Goals of Confidentiality Policies

• Confidentiality Policies emphasize the protection of confidentiality.

• Confidentiality policy also called information flow policy, prevents unauthorized disclosure of information.

• Example: Privacy Act requires that certain personal data be kept confidential. E.g., income tax return info only available to IT department and legal authority with court order. It limits the distribution of documents/info.

1. Discretionary Access Control (DAC)

Discretionary access control (DAC) is a type of security access control that grants or restricts object access via an access policy determined by an object's owner group and/or subjects. DAC mechanism controls are defined by user identification with supplied credentials during authentication, such as username and password. DACs are discretionary because the owner can transfer authenticated objects or information access to other users. In other words, the owner determines object access privileges.

In DAC, each system object (file or data object) has an owner, and each initial object owner is the subject that causes its creation. Thus, an object's access policy is determined by its owner.

A typical example of DAC is Unix file mode, which defines the read, write and execute permissions in each of the three bits for each user, group and others.

✓ **DAC attributes include:**

- User may transfer object ownership to another user(s).
- User may determine the access type of other users.
- After several attempts, authorization failures restrict user access.
- Unauthorized users are blind to object characteristics, such as file size, file name and directory path.
- Object access is determined during access control list (ACL) authorization and based on user identification and/or group membership.

✓ **DAC is easy to implement and intuitive but has certain disadvantages, including:**

- Inherent vulnerabilities (Trojan horse)
- ACL maintenance or capability
- Grant and revoke permissions maintenance
- Limited negative authorization power

2. Mandatory Access Control (MAC)

Mandatory Access Control (MAC) is a set of security policies constrained according to system classification, configuration and authentication. MAC policy management and settings are established in one secure network and limited to system administrators.

MAC defines and ensures a centralized enforcement of confidential security policy parameters.

For best practices, MAC policy decisions are based on network configuration. In contrast, certain operating systems (OS) enable limited Discretionary Access Control (DAC).

✓ **MAC advantages and disadvantages depend on organizational requirements, as follows:**

- MAC provides tighter security because only a system administrator may access or alter controls.
- MAC policies reduce security errors.
- MAC enforced operating systems (OS) delineate and label incoming application data, which creates a specialized external application access control policy.

❖ Confinement Principle

- The confinement principle is the principle of preventing a server from leaking information that the user of the service considers confidential.
- The confinement principle deals with preventing a process from taking disallowed actions.

- (Confinement Problem) Consider a client/server situation: the client sends a data request to the server; the server uses the data, performs some function, and sends the results (data) back to the client.
- In this case the confinement principle deals with preventing a servers from leaking information that the user of that service considers confidential
- In confinement principle, access control affects the function of the server in two ways:
  a. **Goal of service provider:** The server must ensure that the resources it accesses on behalf of the client include only those resources that the client is authorized to access.
  b. **Goal of the service user:** The server must ensure that it does not reveal the client's data to any other entity which is not authorized to see the client's data.
- A covert channel is a path of communication that was not designed to be used for communication.
- The rule of transitive confinement states that if a confined process invokes a second process, the second process must be as confined as the caller. Confinement is a mechanism for enforcing the principle of least privilege. A properly confined process cannot transmit data to a second process unless the transmission is needed to complete their task.

→ **Isolation**

Systems isolate processes in two ways. In the first, the process is presented with an environment that appears to be a computer running only that process or those processes to be isolated. In the second, an environment is provided in which process actions are analyzed to determine if they leak information. The first type of environment prevents the process from accessing the underlying computer system and any processes or resources that are not part of that environment. The second type of environment does not emulate a computer. It merely alters the interface between the existing computer and the process(es).

a. **Virtual Machines:** The first type of environment is called a virtual machine. A virtual machine is a program that simulates the hardware of a computer system.
b. **Sandboxes:** A sandbox is an environment in which the actions of a process are restricted according to a security policy. It provides a safe environment for programs tovexecute in.

❖ Detour used in UNIX user ids and process ids.

- Detour is defined as few words about Unix user IDs and IDs associated with Unix processes.
- Every user in Unix like operating system is identified by different integer number, this unique number is called as UserID.
- There are three types of UID defined for a process, which can be dynamically changed as per the privilege of task.
- The three different types of UIDs defined are:
  a. **Real UserID :** It is account of owner of this process. It defines which files that this process has access to.
  b. **Effective UserID :** It is normally same as real UserID, but sometimes it is changed to enable a non-privileged user to access files that can only be accessed by root.
  c. **Saved UserID:** It is used when a process is running with elevated privileges (generally root) needs to do some under-privileged work, this can be achieved by temporarily switching to non-privileged account.
- A subject is a program (application) executing on behalf of some principal(s). A principal may at any time be idle, or have one or more subjects executing on its behalf.
- An object is anything on which a subject can perform operations (mediated by rights) usually objects are passive, for example :
  a. File
  b. Directory (or folder)
  c. Memory segment.
- Each user account has a unique UID. The UID O means the super user (System admin). A user account belongs to multiple groups. Subject are processes, associated with uid/gid pairs.
- There should be a one-to-many mapping from users to principals. A user may have many principals, but each principal is associated with a unique user. This ensures accountability of a user action.

❖ More on confinement techniques

1. **Chroot:** The term chroot refers to a process of creating a virtualized environment in a unix o.s, separating it from the main o.s. and directory structure. This process essentially generates a confined space to run software program. Any software program run in this environment can only access files with in its own directory tree. It cannot access file outside of that directory tree. This confined virtual environment is often called as chroot jail.
2. **JailKits:** Jailkit is a specialized tool that is developed with a focus on security. Jailkit is a set of utilities to limit user accounts to specific files using chroot() and a specific commands. It will abort in a secure way if the configuration is not secure and it will send useful log message that explain what is wrong to a system log.
3. **Free BSD Jail:** It is a popular free and open source operating system that is based on the BSD version of Unix OS. The Jail mechanism if an implementation of free BSD's PS-Level virtualization that allow & system administrators to partition a free BSD derived computer system into several independent systems called jail, all sharing the same kernel with very little overhead. It is implemented through a system call jail.

❖ System call interposition

System call interposition is a powerful method for regulating and monitoring program behavior. It gives security systems the ability to monitor all of the application's interaction with network, file system and other sensitive system resources. The discrimination between normal and abnormal behavior is based on what system calls are normally invoked by a running program. To guarantee the effectiveness and security of these security systems, system calls must be intercepted and handled safely and completely.

The major contributions are summarized as follows:

- We design a VMM-based system call interposition approach which cannot be bypassed by guest OS even if guest kernel has been comprised.
- The method of system call correlating is proposed to establish the relations among related system calls. The relations are used by VSyscall to monitor and identify process behavior based on given patterns.
- A prototype of VSyscall system is designed and implemented for two different full virtualization environments. Malware samples and benchmark applications are used to evaluate the effectiveness and performance of VSyscall. Experimental results show its effectiveness with only incurring a small runtime overhead.

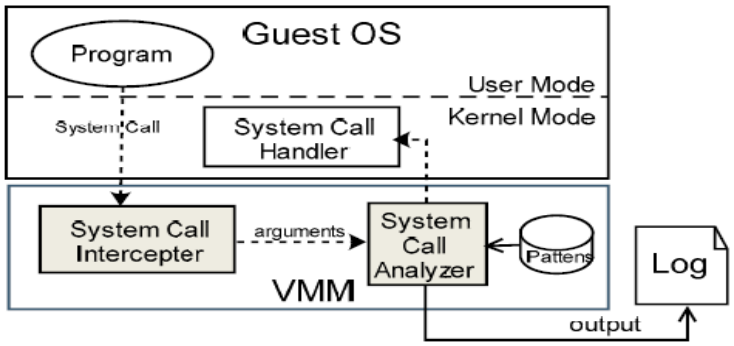

Figure 1. The VSyscall architecture

❖ Error 404 digital Hacking in India part 2 chase

- In error 404 digital hacking in India part 2 chase experts discuss about some attack related to cyber attack and the attacker can control the overall system if proper security is not provided to the system.
- Some attacks discuss in error 404 digital hacking India part 2 chase are: Israel Power Grid hit by a big hack attack is being called one of the worst cyber attacks ever.
- In 2014 a hydropower plant in upstate New York got hacked.
- France in infrastructure including its main nuclear power plant is being targeted by a new and dangerous powerful cyber worm.
- Bangladesh's best group hacked into nearly 20000 Indian websites including the Indian border security force.

- First virus that could crash Power Grid or destroy the pipeline is available online for anyone to download and Tinker with.
- India's biggest data breach, (the SBI debit card breach) when this happened Bank was initially in a state of denial but subsequently they had to own up the cyber security breach that took place in Indian history.

❖ VM based isolation

- Virtualization technology allows the sharing of the same physical resources among several users.
- This enables the consolidation of servers and a multitude of user machines into a very small set of physical servers, by replacing the physical machines with virtual machines, running on the same physical servers.
- Temporal isolation or performance isolation among virtual machine(VMs) refers to the capability of isolating the temporal behaviour (or limiting the temporal interferences) of multiple VMs among each other, despite them running on the same physical host and sharing a set of physical resources such as processors, memory, and disks.
- Which machine search software instructions of real machines provide a virtual platform for running tasks
- Virtual Machines are software abstractions of real machines. They provide a virtual platform for running tasks.
- Virtual machines have been employed to provide various features like emulation, optimization, translation, isolation, replication etc.
- A virtual machine can support individual processes or a complete system depending on the abstraction level where virtualization occurs.
- Some VMs support flexible hardware usage and software isolation, while others translate from one instruction set to another.

✓ Types of VM based isolation

a. Process virtualization machine: Process virtual machine support individual processes or a group of processes and enforce isolation between the processes and operating system environment. Process visualization machine can run processes compiled for the same instructions set architecture based ISA 44 different ideas as long as the virtual machine runtime supports the translation. Isolation policies are provided by a runtime component

b. System virtual machines: System which all machines provide a full replica of the underlined platform and thus enable complete operating system to be Run within it. The virtual machine monitor runs at the highest privilege level and divides the platform hardware resources among multiple replicated guest system.

c. Hosted virtual machines: Hostel virtual machines are built on top of an existing operating system called the host**.** The virtualization layers it's above the regular operating system and makes the virtual Machine look like and application process**.** We then install complete operating system called guest operating system within the host virtual machines. The processes running inside the virtual machine cannot affect the operation of processes outside the virtual machine

d. Hardware virtual machine: Hardware virtual machines are visual machines build using virtualization primitives provided by the hardware like processor or input output devices**.** The advantage of hardware level virtualization is tremendous performance improvements over the software based approaches and guarantees better isolation between machines.

❖ Software fault isolation

Software-based Fault Isolation (SFI) establishes a logical protection domain by inserting dynamic checks before memory and control-transfer instructions.

software fault isolation, adds instructions that perform memory access checks or other checks as the program runs, so any attempt to violate the security policy causes an error.

When protecting a computer system, it is often necessary to isolate an untrusted component into a separate protection domain and provide only controlled interaction between the domain and the rest of the system.

SFI has been successfully applied in many applications, including isolating OS kernel extensions, isolating plug-ins in browsers, and isolating native libraries in the Java Virtual Machine.

❖ Rootkit

- A rootkit is a computer program designed to provide continued privileged access to a computer while actively hiding its presence.
- Rootkit is a collection of tools that enabled administrator-level access to a computer or network.
- Root refers to the Admin account on Unix and Linux systems, and kit refers to the software components that implement the tool.
- Rootkits are generally associated with malware such as Trojans, worms, viruses that conceal their existence and actions from users and other system processes.
- A rootkit allows us to maintain command and control over a computer without the computer user/owner knowing about it.
- Once a rootkit has been installed, the controller of the rootkit has the ability to remotely execute files and change system configurations on the host machine.
- A rootkit on an infected computer can also access log files and spy on the legitimate computer owner's usage.
- Rootkits can be detected using detection methods which include:
  1. **Behavioural-based methods:** The behavioral-based approach to detecting rootkits attempts to infer the presence of a rootkit by looking for rootkit-like behavior.
  2. **Signature scanning:** Antivirus products rarely catch all viruses in public tests, even though security software vendors incorporate rootkit detection into their products. Signature-based detection methods can be effective against well-published rootkits, but less so against specially crafted, custom-root rootkits.
  3. **Memory dump analysis:** This technique is highly specialized, and may require access to non-public source code or debugging symbols. Memory dumps initiated by the operating system cannot always be used to detect a hypervisor-based rootkit, which is able to intercept and subvert the lowest-level attempts to read memory- a hardware device, such as one that implements a non-maskable interrupt, may be required to dump memory in this scenario.

❖ Intrusion Detection System (IDS)

An Intrusion Detection System is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered.

Intrusion prevention systems also monitor network packets inbound the system to check the malicious activities involved in it and at once sends the warning notifications.

✓ Classification of Intrusion Detection System:

1. Network Intrusion Detection System (NIDS): Network intrusion detection systems are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator.

2. Host Intrusion Detection System (HIDS): Host intrusion detection systems run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot.

3. Protocol-based Intrusion Detection System (PIDS): Protocol-based intrusion detection system comprises of a system or agent that would consistently resides at the front end of a server, controlling

and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol.

4. Application Protocol-based Intrusion Detection System (APIDS): Application Protocol-based Intrusion Detection System is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application specific protocols.

5. Hybrid Intrusion Detection System: Hybrid intrusion detection system is made by the combination of two or more approaches of the intrusion detection system. In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system.

- ✓ **Detection Method of IDS:**

1. Signature-based Method: Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1's or number of 0's in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures. Signature-based IDS can easily detect the attacks whose pattern already exists in system but it is quite difficult to detect the new malware attacks as their pattern is not known.

2. Anomaly-based Method: Anomaly-based IDS was introduced to detect the unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model. Machine learning based method has a better generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.