❖ Security:

Security is defined as being free from danger, or feeling safe.

✓ **Common Goals:**

1) **Confidentiality:** Confidentiality is equivalent to privacy that avoids unauthorized access of information. It involves ensuring the data is accessible by those who are allowed to use it and blocking access to others. It prevents essential information from reaching the wrong people. Data encryption is an excellent example of ensuring confidentiality.
2) **Integrity:** Integrity refers to the trustworthiness of data or resources. Integrity includes data integrity (the content of the information) and origin integrity (the source of the data, often called authentication). This principle ensures that the data is authentic, accurate, and safeguarded from unauthorized modification by threat actors or accidental user modification. If any modifications occur, certain measures should be taken to protect the sensitive data from corruption or loss and speedily recover from such an event. In addition, it indicates to make the source of information genuine.
3) **Availability:** This principle makes the information to be available and useful for its authorized people always. It ensures that these accesses are not hindered by system malfunction or cyber-attacks.

❖ Threats:

A computer system threat is anything that leads to loss or corruption of data or physical damage to the hardware and infrastructure.

✓ **Security Threat:** Security threat is defined as a **risk** that which can potentially harm computer system.

→ **Physical damage:** It includes fire, water pollution etc.
→ **Natural Events:** It includes climate, Earthquake, volcanic activity etc.
→ **Loss of service:** It includes Electric power, air conditioning, telecom etc.
→ **Technical Failure:** It includes Problems in equipments, Software etc.
→ **Deliberate Type:** It includes Spying, illegal processing of data

✓ **Common threats:**

1. **Virus:** A computer virus is a illegal program designed to disrupt the normal functioning of computer without the permission of user.
2. **Worm:** Worm is a malicious, self- replicating software program which is affects he functions of software and hardware programs.
3. **Trojan horse:** It is hidden piece of code which is intended to leak your confidential information.
4. **Spyware:** It is a computer program that monitors user's online activities or install programs with user's consent for profit or theft of personal information.
5. **Hackers:** Hackers are programmers who put others on threats for their personal gain by breaking into computer system with purpose to steal, change or destroy information.
6. **Phishing Threat:** It is illegal activity through which phishers attempt to steal sensitive financial or personal data by means of fraudent email or instant messages.

❖ Computer Security:

Computer security refers to the protection of a computer's hardware and the data that it holds.

Computer security basically is the protection of computer systems and information from harm, theft, and unauthorized use. It is the process of preventing and detecting unauthorized use of your computer system.

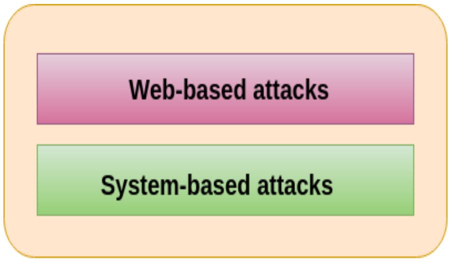
Computer security can be implemented using passwords, encryption, and firewalls, and denying physical access to a computer's location.

✓ **Types of Computer Security**

1. **Application Security:** Application security is the types of cyber security which developing application by adding security features within applications to prevent from cyber attacks. The attacks can be SQL injection, denial of service (DoS) attacks, data breaches or other cyber-attacks. There are some application security tools and techniques such as firewalls, antivirus software, encryption, and web application firewall which can help to prevent from cyber-attacks.
2. **Information security:** Information security is a type of computer security which refers to the process and methodology to protect the confidentiality, integrity and availability of computer system from unauthorized access, use, modification and destruction. Information security focuses on the CIA triad model, which ensures confidentiality, integrity, and availability of data, without affecting organization productivity.
3. **Network Security:** Network security is another type of computer security which process of preventing and protecting against unauthorized intrusion into computer networks. It is a set of rules and configurations which designed to protect the confidentiality, integrity and accessibility of computer networks system and information using both software and hardware technologies. Network Security is by securing both the software and hardware technologies.
4. **Endpoint Security:** Human error is a major weak point which is easily exploited by cyber criminals. End users are becoming the largest security risk in any organizations. However, end user has no fault of their own, and mostly due to a lack of awareness and ICT policy. They can unintentional open the virtual gates to cyber attackers.
5. **Internet Security:** Internet security is the important types of computer security which has defined as a process to create set of rules and actions to protect computer systems that are connected to the Internet. It is a branch of computer security that deals specifically with internet-based threats such as: Hacking, Computer Viruses, Denial-of-Service Attacks, Malware etc.

❖ Sample Attacks:

A cyber-attack is an exploitation of computer systems and networks.



Classification of Cyber attacks

1. **Web-based attacks:** These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows-
   a) **Injection attacks:** It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.
   b) Example- SQL Injection, code Injection, log Injection, XML Injection etc.
   c) **DNS Spoofing:** DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker’s computer or any other computer.
   d) **Session Hijacking:** It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.
   e) **Phishing:** Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number.

f) **Brute force:** It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number.

g) **Denial of Service:** It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server.

h) **URL Interpretation:** It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

i) **Man in the middle attacks:** It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

2. **System-based attacks:** These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-

a) **Virus**

b) **Worm**

c) **Trojan horse**

These three definition is above (in Threat Topic)

d) **Backdoors:** It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

e) **Bots**: A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

❖ The Marketplace for vulnerabilities

Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack. Vulnerabilities are weaknesses in a system that gives threats the opportunity to compromise assets. All systems have vulnerabilities. Vulnerabilities mostly happened because of Hardware, Software, Network and Procedural vulnerabilities. The aim is to significantly replace trial and error with a robust understanding of markets, markets habitually governed by social virtues.

1. Hardware Vulnerability: Hardware vulnerability is a weakness which can used to attack the system hardware through physically or remotely.

For examples: Old version of systems or devices, unprotected storage, Unencrypted devices, etc.

2. Software Vulnerability: Software vulnerability is a defect in software that could allow an attacker to gain control of a system. For examples: Lack of input validation, Unverified uploads, Unencrypted data, etc.

3. Network Vulnerability: A weakness happen in network which can be hardware or software.

For examples: Unprotected communication, Malware or malicious software (e.g.: Viruses, Keyloggers, Worms, etc), Social engineering attacks, Misconfigured firewalls etc.

4. Procedural Vulnerability: A weakness happen in an organization operational methods.

For examples: Password procedure – Password should follow the standard password policy.

Training procedure – Employees must know which actions should be taken and what to do to handle the security. Employees must never be asked for user credentials online. Make the employees know social engineering and phishing threats.

❖ Error 404 Hacking digital India part 1 chase

- In error 404 hacking digital India part 1 chase, the cyber crime and cyber attacks hack the information of users like bank detail and personal information.
- It is real time incident. In this , attacker or hacker creates an attractive video so that victim gets attracted and plays that video into system.
- When we clicked on video to play then at the time of buffering , hacker can know our current location and GPS history but also have complete access to our contacts, text messages, Facebook, Whatsapp and most importantly our bank details , including our CVV number.
- Hackers are creating a kind Trojan file , and android apk files. The apk files that will be distributed all over the internet. Those who download this file will be hacked easily.

Potential cyber attacks that is most common in error 404 hacking:

A) Web Application attacks :

- A web application is a client - server computer program which uses web browsers and web technology to allow its visitors to store and retrieve data to / from the database over the internet.
- If there is flaw in the web application, it allows the attacker to manipulate data using SQL injection attack.

B.) Network Security attacks:

- Network Security attacks are unauthorized actions against private , corporate or governmental IT assets in order to destroy them modify them or steal sensitive data.
- As more enterprises invite employees to access data from mobile devices, networks become vulnerable to data theft or total destruction of the data or network.

C). Mobile security attacks:

- Mobile security, or mobile device security, has become increasingly important in mobile computing.
- The security of personal and business information now stored on smartphones
- More and more users and businesses use smartphones to communicate, but also to plan and organize their users' work and also private life.
- Within companies, these technologies are causing profound changes in the organization of information systems and therefore they have become the source of new risks.
- Indeed, smartphones collect and compile an increasing amount of sensitive information to which access must can be controlled to protect the privacy of the user and the intellectual property of the company.

❖ Hijacking

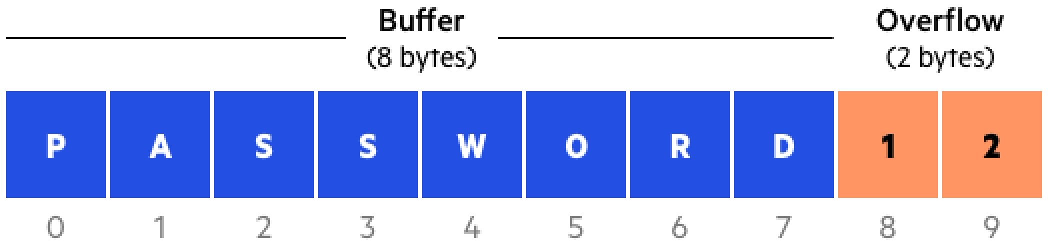
Cyber hijacking, or computer hijacking, is a type of network security attack in which the attacker takes control of computer systems, software programs and/or network communications. Ex: browser hijacking, session hijacking, domain hijacking, clipboard hijacking, domain name system (DNS) hijacking, Internet Protocol (IP) hijacking, page hijacking.

✓ Control Hijacking

1) Buffer overflows attacks:

Buffers are memory storage regions that temporarily hold data while it is being transferred from one location to another. A **buffer overflow** (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer.

For example, a buffer for log-in credentials may be designed to expect username and password inputs of 8 bytes, so if a transaction involves an input of 10 bytes, the program may write the excess data past the buffer boundary.



Buffer overflow attack, Attackers exploit buffer overflow issues by overwriting the memory of an application. If attackers know the memory layout of a program, they can intentionally feed input that the buffer cannot store, and overwrite areas that hold executable code, replacing it with their own code. For example, an attacker can overwrite a pointer (an object that points to another area in memory) and point it to an exploit payload, to gain control over the program.

C and C++ are two languages that are highly susceptible to buffer overflow attacks, as they don't have built-in safeguards against overwriting or accessing data in their memory.

✓ **Types of Buffer Overflow Attacks**

i. **Stack-based buffer overflows** are more common, and leverage stack memory that only exists during the execution time of a function.

ii. **Heap-based attacks** are harder to carry out and involve flooding the memory space allocated for a program beyond memory used for current runtime operations.

✓ **How to Prevent Buffer Overflows**

a) **Address space randomization (ASLR)—**randomly moves around the address space locations of data regions.

b) **Data execution prevention—**flags certain areas of memory as non-executable or executable, which stops an attack from running code in a non-executable region.

c) **Structured exception handler overwrite protection (SEHOP)—**helps stop malicious code from attacking Structured Exception Handling (SEH), a built-in system for managing hardware and software exceptions. It thus prevents an attacker from being able to make use of the SEH overwrite exploitation technique. At a functional level, an SEH overwrite is achieved using a stack-based buffer overflow to overwrite an exception registration record, stored on a thread's stack.

2) Integer overflow attack: Integer overflow, also known as wraparound. An integer overflow is a type of an arithmetic overflow error when the result of an integer operation does not fit within the allocated memory space. Instead of an error in the program, it usually causes the result to be unexpected. Integer overflows have been listed as the number 8 most dangerous software error in the most recent CWE 2019 list.

For example, we have a 16-bit integer value which may store an unsigned integer ranging from 0 to 65535, or signed integer ranging from -32768 to 32767. So, during an arithmetic operation, if the results require more than the allocated space (like 65535+1), the compiler may:

- completely ignore the error caused, or
- Abort the program.

Most compilers will ignore the overflow and store unexpected output or error. This will result in various attacks such buffer overflow which is the most common attack and leads to executing malicious programs or privilege escalation.

✓ **Preventing Integer Overflow Attacks**

a) **Requirement Phase:** We need to ensure that all rules and protocols are defined strictly for all out-of-bound operations.

b) **Architecture & Design:** It is recommended to use libraries and frameworks that are used in secure coding, and best practices in order to avoid undefined or erroneous behavior while handling numbers.

c) **Implementation Phase:** As pointed out earlier, make sure to provide input validation for numbers that are entered by the user.

3) Format string vulnerabilities: A Format String attack can occur when an input string's submitted data is evaluated as a command by the application. Taking advantage of a Format String vulnerability, an attacker can execute code, read the Stack, or cause a segmentation fault in the running application – causing new behaviors that compromise the security or the stability of the system.

Safe Code

The line printf("%s", argv[1]); in the example is safe, if you compile the program and run it:

./example "Hello World %s%s%s%s%s%s"

The printf in the first line will not interpret the “%s%s%s%s%s%s” in the input string, and the output will be: “Hello World %s%s%s%s%s%s”.

Vulnerable Code

The line printf(argv[1]); in the example is vulnerable, if you compile the program and run it:

./example "Hello World %s%s%s%s%s%s"

The printf in the second line will interpret the %s%s%s%s%s%s in the input string as a reference to string pointers, so it will try to interpret every %s as a pointer to a string, starting from the location of the buffer (probably on the Stack). At some point, it will get to an invalid address, and attempting to access it will cause the program to crash.

✓ **Preventing Format String Vulnerabilities**

a) Always specify a format string as part of program, not as an input. Most format string vulnerabilities are solved by specifying “%s” as format string and not using the data string as format string

b) If possible, make the format string a constant. Extract all the variable parts as other arguments to the call. Difficult to do with some internationalization libraries.

c) If the above two practices are not possible, use defenses such as Format_Guard . Rare at design time. Perhaps a way to keep using a legacy application and keep costs down. Increase trust that a third-party application will be safe.

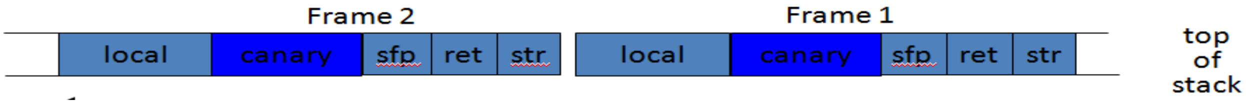
❖ Defense against Control Hijacking - Platform Defenses

Same as How to Prevent Buffer Overflows (this topic is above in this unit)

❖ Defense against Control Hijacking - Run-time Defenses

1) **StackGuard:** StackGuard is a compiler extension that enhances the executable code produced by the compiler so that it detects and thwarts buffer-overflow attacks against the stack. StackGuard basically works by inserting a small value known as a canary between the stack variables (buffers) and

the function return address. When a stack-buffer overflows into the function return address, the canary is overwritten.



✓ **Canary Types**

i. **Random canary:** A random canary is chosen at random at the time the program execution. With this method, the attacker could not learn the canary value prior to the program start by searching the executable image.

ii. **Terminator canaries:** Most buffer overflow attacks are based on certain string operations which end at string terminators. A terminator canary contains NULL(0x00), CR (0x0d), LF (0x0a), and EOF (0xff), four characters that should terminate most string operations. This prevents attacks using strcpy() and other methods that return upon copying a null character while the undesirable result is that the canary is known.

2) **Libsafe:** Libsafe is an implementation of vulnerable copy functions in C library such as strcpy().Libsafe is implemented as a shared library that is preloaded to intercept C library function calls. Programs are protected without recompilation unless they are statically linked with the C library. Libsafe protects only those C library functions whereas StackGuard and StackShield protect all functions.

3) **StackShield:** StackShield is also a GNU C compiler extension that protects the return address. When a function is called StackShield copies away the return address to a non-overflowable area, and restores the return address upon returning from a function. Even if the return address on the stack is altered, it has no effect since the original return address is remembered. As with StackGuard, programs needs to be recompiled.

4) **Control-flow integrity:** Control-flow integrity is a general term for computer security techniques that prevent a wide variety of malware attacks from redirecting the flow of execution of a program.

❖ Advanced Control Hijacking attacks

Heap spraying: Heap spraying is a technique used to aid the exploitation of vulnerabilities in computer systems. It is called "spraying the heap" because it involves writing a series of bytes at various places in the heap. The heap is a large pool of memory that is allocated for use by programs. The basic idea is similar to spray painting a wall to make it all the same color. Like a wall, the heap is "sprayed" so that its "color" (the bytes it contains) is uniformly distributed over its entire memory "surface."

✓ **Procedure For The Attack**

i. In the attack, the attacker first uses the exploits in the web browsers and other applications or languages such as Actionscript or Javascript in the Adobe Reader to put the malicious code in the memory heap at some predetermined location.

ii. The attacker further exploits the vulnerability by using the scripting support. For this, he makes the Extended Instruction Pointer (EIP) to directly point the predetermined location.

iii. The attacker thus can further run the malicious code and perform the malicious activity.

✓ **Mitigations For The Attack**

Running the web browsers with the least privileges makes it much harder for the hackers to gain the admin access, which helps in mitigating this attack. Also, update the web browsers regularly to patch up the known bugs.

❖ 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.

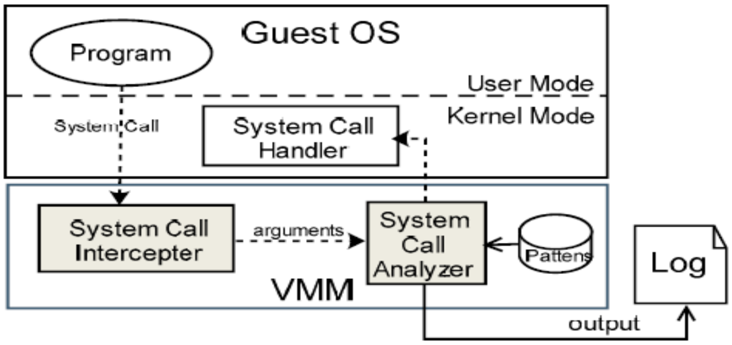


Figure 1. The VSyscall architecture

❖ 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.