**Computer Science 530 - Assignment #3 -- Fall 2013**

Virtual Memory:

For virtual memory, the processes that are running are isolated from each other to prevent access to exclusive objects or data in another process. This is called process isolation. It is a set of hardware and software technologies, which gives each process its own private virtual address space. This prevents process A from writing onto process B. DOS does not provide as much security, because any process can write into the memory of any other process. Security is easier to implement by disallowing inter-process memory access. The policy enforced differs for each process, in the case of no shared variables or data, the process data interchange occurs via channels like internet or local sockets or shared memory. If there is common data and working on the same data, then write and input access is given to multiple processes. Web browsers such as Firefox, Chrome and Safari have an inbuilt process isolation technique.

Most operating systems enforce process isolation through hardware protection mechanisms such as memory segmentation, page mapping, and differentiated user and kernel instructions. For Microsoft Windows, singularity is a new operating system that uses software mechanisms to enforce process isolation. A software isolated process (SIP) is a process whose boundaries are established by language safety rules and enforced by static type checking. SIPs provide a low cost isolation mechanism that provides failure isolation and fast inter-process communication. Windows provides for optional hardware isolation. Protection domains are hardware-enforced address spaces, which can contain one or more SIPs. Domains can either run at the kernel's privilege level or be fully isolated from the kernel and run at the normal application privilege level. With protection domains, Windows can construct Singularity configurations that are similar to micro-kernel and monolithic kernel systems. However, hardware isolation remains valuable as a defense-in-depth against potential failures in software isolation mechanisms. Singularity's ability to employ hardware isolation selectively enables careful balancing of the costs and benefits of each isolation technique.

Shortcomings would involve that it would not work for real time systems. [1]

Firewall:

A firewall is a system designed to prevent unauthorized access and misuse of client machines. Firewalls can be implemented in both hardware and software. They provide isolation by controlling the network traffic entering and leaving the network based on some pre-defined rules. The firewall has two modes of operation: default - deny policy and default - allow policy. Both these methods provide isolation by their functionality. In default-deny policy the administrator lists the allowed network services and everything else is denied. In default-allow policy the administrator list services which are not allowed and everything else is accepted. The default - deny policy is more secure when compared to default-allow policy.

Depending on the type of firewall, either a network based or a host based firewall, in case of the former- the IP address, protocol, and the port number are used to determine if the packet can pass through the network by the firewall admin. This operates in collaboration with IDS. The host based firewall can only analyze the packets leaving the system. The isolation provided is bidirectional.

Application Proxies: These are servers that receive requests from machines within a network and communicate with the outside of the network, on behalf of the internal machines. Since only a single machine is being seen, this system isolates the external network from internal network. The isolation is to protect monitor and log the data for the internal client machine. The isolation is one way -it only isolates internal network from the outside world, and is absolute. The policy can specify which type of traffic to block or cache. The policy is specified in the proxy machine by the system. A bottle neck for communication with the outside network is a shortcoming here. It also causes delay of packets to be routed from the outside to the internal client. The internal client IP and ports are also to be kept a track of by the proxy server. If the proxy server is compromised the entire system is at risk. [7]

Virtualization:

Virtual machines have been employed to provide various features like emulation, optimization, translation, isolation, or replication.

Based on levels of abstraction and the number of processes it supports, we can classify Virtual Machine based isolation into 4 categories as:

(a) ***Process Virtual Machines:*** Process Virtual Machines support individual processes or a group of processes and enforce isolation between the processes and operating system environment.

(b) ***System Virtual Machines (Hypervisor Virtual Machines):*** System virtual machines provide a full replica of the underlying platform and thus enable complete operating systems to be run within it. The virtual machine monitor (also called the hypervisor) runs at the highest privilege level and divides the platforms hardware resources amongst multiple replicated guest systems. All accesses by the guest systems to the underlying hardware resources are then mediated by the virtual machine monitor. This mediation provides the \necessary isolation between the virtual machines.

(c) ***Hosted Virtual Machines:*** Hosted Virtual Machines are built on top of an existing operating system called the host. The virtualization layer sits above the regular operating system and makes the virtual machine look like an application process The processes running inside the Virtual machine cannot affect the operation of processes outside the virtual machine. System emulators are also loosely classified under hosted virtual machines

(d) ***Hardware Virtual Machines:*** Hardware virtual machines are virtual machines built using virtualization primitives provided by the hardware like processor or I/O. The advantage of hardware level virtualization is tremendous performance improvements over the software based approaches and guarantees better isolation between machines. The isolation provided by the hardware assisted virtualization is more secure than that provided by its software counterpart [2]

Data Encryption

Protection against the adversary is the sole use of data encryption. An encryption key is used to encrypt and the same or different key is used to decrypt the message. Isolation is achieved due the fact that the data can only be decrypted by a person with the corresponding key. Isolation is unidirectional and the algorithms used for encryption and decryption govern the security of data.

Some of the major disadvantages with data encryption which include its vulnerability towards brute force attacks, man in the middle attacks, DOS attacks, dictionary attacks etc. However, providing a harder encryption scheme and a more secure service towards the protection will exponentially increase the key size, hence reducing the speed of the process. The policy of the data encryption depends purely on the security mechanism provided. [3]

VPN’s

It is a generic concept which designates a part of a bigger network which is logically isolated from the bigger network through non-hardware means The use of cryptographically secure approaches towards building the VPN’s have ensures the isolation remains concrete. The isolation and policy provided by VPN is one way and depends on the encryption mechanism used. VPNs provide security by the use of tunneling protocols and through security procedures such as encryption. The VPN security model provides:

a) Confidentiality such that even if the network traffic is sniffed at the packet level, an attacker would only see encrypted data

b) Sender authentication to prevent unauthorized users from accessing the VPN.

c) Message integrity to detect any instances of tampering with transmitted messages [4]

IPSec(as mentioned earlier) design meets most security goals: authentication, integrity, and confidentiality. IPSec uses encryption, encapsulating an IP packet inside an IPSec packet. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination. There is also a level of security that comes along with the usage of VPN’s.

Some of the security risks that are involved with using VPN and other methods include the following:

a) When data leaves the VPN provider's server it is encrypted. It means that the VPN provider and well as other networking equipment between them and the server can see your data.

b) Many authentication methods that are used are too weak to provide adequate security.

c) VPNs are prone to man in the middle attacks and offline password cracking attacks. [5]

TPM’s

A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer, and it communicates with the remainder of the system by using a hardware bus.

Computers that incorporate a TPM can create cryptographic keys and encrypt them so that they can only be decrypted by the TPM. This process, often called wrapping or binding a key, can help protect the key from disclosure. Each TPM has a master wrapping key, called the storage root key, which is stored within the TPM itself. The private portion of a storage root key or endorsement key that is created in a TPM is never exposed to any other component, software, process, or user.

Computers that incorporate a TPM can also create a key that has not only been wrapped, but is also tied to certain platform measurements. This type of key can be unwrapped only when those platform measurements have the same values that they had when the key was created. This process is referred to as “sealing the key to the TPM.” Decrypting the key is called unsealing. The TPM can also seal and unseal data that is generated outside the TPM. With this sealed key and software (such as BitLocker Drive Encryption), data can be locked until specific hardware or software conditions are met.

With a TPM, private portions of key pairs are kept separate from the memory that is controlled by the operating system. Keys can be sealed to the TPM, and certain assurances about the state of a system (assurances that define the trustworthiness of a system) can be made before the keys are unsealed and released for use. Because the TPM uses its own internal firmware and logic circuits to process instructions, it does not rely on the operating system, and it is not exposed to vulnerabilities that might exist in the operating system or application software.

Since TPM cannot directly access a software application, there is a level of bidirectional isolation.

For a TPM to be usable by a trusted application, it must contain an endorsement key, which is an RSA key pair. The private half of the key pair is held inside the TPM, and it is never revealed or accessible outside the TPM. If the TPM does not contain an endorsement key, the application might cause the TPM to generate one automatically as part of the setup. An endorsement key can be created at various points in the TPM’s lifecycle, but it needs to be created only once for the lifetime of the TPM. The existence of an endorsement key is a requirement before TPM ownership can be taken. [6] Shortcomings include no flexibility.

Sources:

[1] <http://dl.acm.org/citation.cfm?doid=1178597.1178599>

[2] <http://www.arunviswanathan.com/survey_isolation_techniques.pdf>

[3] http://en.wikipedia.org/Encryption

[4] <http://en.wikipedia.org/wiki/Virtual_private_network>

[5] <http://en.wikipedia.org/wiki/Man_In_The_Middle>

[6] <http://technet.microsoft.com/en-us/library/jj131725.aspx>

[7] <http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=%2Frzatj%2Fappprox.htm>