**Types of Computer Forensics Systems**:

Study different Security System:

1) Internet Intrusion Detection,

2)Firewall

3)Storage Area

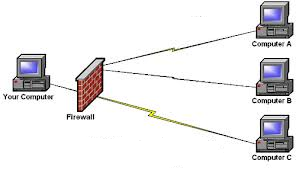
4) Network Disaster Recovery

5) Public Key Infrastructure

**1)What is a firewall?**

A firewall is a device installed between the internal network of an organization and the rest of the network. It is designed to forward some packets and filter others. For example, a firewall may filter all incoming packets destined for a specific host or a specific server such as HTTP, or it can be used to deny access to a specific host or a service in the organization.

The following image depicts a firewall installation in the network.



Firewalls are a set of tools that monitors the flow of traffic between networks. Placed at the network level and working closely with a router, it filters all network packets to determine whether or not to forward them towards their destinations.

Working architecture

A firewall is often installed away from the rest of the network so that no incoming requests get directly to the private network resource. If it is configured properly, systems on one side of the firewall are protected from systems on the other side. Firewalls generally filter traffic based on two methodologies:

* A firewall can allow any traffic except what is specified as restricted. It relies on the type of firewall used, the source, the destination addresses and the ports
* A firewall can deny any traffic that does not meet the specific criteria based on the network layer on which the firewall operates

The type of criteria used to determine whether traffic should be allowed through varies from one type to another. A firewall may be concerned with the type of traffic or with source or destination addresses and ports. A firewall may also use complex rules based on analyzing the application data to determine if the traffic should be allowed through.

Firewall pros and cons

Every security device has advantages and disadvantages and firewalls are no different. If we applied strict defensive mechanisms into our network to protect it from breach, then it might be possible that even our legitimate communication could malfunction; or if we allow entire protocol communications into our network, then it can be easily hacked by malicious users. We should maintain a balance between strictly-coupled and loosely-coupled functionalities.

Advantages

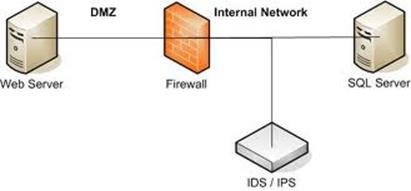
* A firewall is an intrusion detection mechanism. Firewalls are specific to an organization’s security policy. The settings of firewalls can be altered to make pertinent modification to the firewall functionality.
* Firewalls can be configured to bar incoming traffic to POP and SNMP and to enable email access.
* Firewalls can also block email services to secure against spam.
* Firewalls can be used to restrict access to specific services. For example, the firewall can grant public access to the web server but prevent access to the Telnet and the other non-public daemons.
* Firewall verifies the incoming and outgoing traffic against firewall rules. It acts as a router in moving data between networks.
* Firewalls are excellent auditors. Given plenty of disk or remote logging capabilities, they can log any and all traffic that passes through.

Disadvantage

* A firewall can’t prevent revealing sensitive information through social engineering.
* A firewall can’t protect against what has been authorized. Firewalls permit normal communications of approved applications, but if those applications themselves have flaws, a firewall will not stop the attack: to the firewall, the communication is authorized.
* Firewalls are only as effective as the rules they are configured to enforce.
* Firewalls can’t stop attacks if the traffic does not pass through them.
* Firewalls also can’t secure against tunneling attempts. Applications that are secure can be attacked with Trojan horses. Tunneling bad things over HTTP, SMTP and other protocols is quite simple and easily demonstrated.

**2)Intrusion detection system (IDS)**

Intrusion Detection (ID) is the process of monitoring for and identifying attempted unauthorized system access or manipulation. An ID system gathers and analyzes information from diverse areas within a computer or a network to identify possible security breaches which include both intrusions (attack from outside the organization) and misuse (attack from within the organization).



An intrusion detection system (IDS) is yet another tool in the network administrator’s computer security arsenal. It inspects all the inbound and outbound network activity. The IDS identifies any suspicious pattern that may indicate an attack on the system and acts as a security check on all transactions that take place in and out of the system.

Types of IDS

For the purpose of dealing with IT, there are four main types of IDS.

Network intrusion detection system (NIDS)

A NIDS is an independent platform that identifies intrusions by examining network traffic and monitors multiple hosts. Network intrusion detection systems gain access to network traffic by connecting to a network hub, a network switch configured for port mirroring or a network tap. In a NIDS, sensors are placed at choke points in the network to monitor, often in the demilitarized zone (DMZ) or at network borders. Sensors capture all network traffic and analyze the content of individual packets for malicious traffic. An example of a NIDS is Snort.

Host-based intrusion detection system (HIDS)

A HIDS consists of an agent on a host that identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability databases, access control lists and so on) and other host activities and state. In a HIDS, sensors usually consist of a software agent. Some application-based IDS are also part of this category. An example of a HIDS is OSSEC.

Intrusion detection systems can also be system-specific using custom tools and honeypots

A **honeypot** is a computer or computer system intended to mimic likely targets of cyberattacks. It **can** be used to detect attacks or deflect them from a legitimate target. It **can** also be used to gain information about how cybercriminals operate.

. In the case of physical building security, IDS is defined as an alarm system designed to detect unauthorized entry.

Perimeter intrusion detection system (PIDS)

Detects and pinpoints the location of intrusion attempts on perimeter fences of critical infrastructures. Using either electronics or more advanced fiber optic cable technology fitted to the perimeter fence, the PIDS detects disturbances on the fence. If an intrusion is detected and deemed by the system as an intrusion attempt, an alarm is triggered.

VM-based intrusion detection system (VMIDS)

A VMIDS detects intrusions using virtual machine monitoring. By using this, we can deploy the intrusion detection system with virtual machine monitoring. It is the most recent type and it’s still under development. There’s no need for a separate intrusion detection system since by using this, we can monitor the overall activities.

**Comparison with firewall**

Though they both relate to network security, an intrusion detection system (IDS) differs from a firewall in that a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm.

An IDS also watches for attacks that originate from within a system. This is traditionally achieved by examining network communications, identifying heuristics and patterns (often known as signatures) of common computer attacks and taking action to alert operators. A system that terminates connections is called an intrusion prevention system and is another form of an application layer firewall.

Anomaly detection model

All intrusion detection systems use one of two detection techniques:

Statistical anomaly-based IDS

A statistical anomaly-based IDS establishes a performance baseline using normal network traffic evaluations. It will then sample current network traffic activity to this baseline in order to detect whether or not it is within baseline parameters. If the sampled traffic is outside baseline parameters, an alarm will be triggered.

Signature-based IDS

Network traffic is examined for preconfigured and predetermined attack patterns known as signatures. Many attacks today have distinct signatures. In good security practice, a collection of these signatures must be constantly updated to mitigate emerging threats.

Indication of intrusions

System intrusions

* System failure in identifying valid user
* Active access to unused logins
* Login during non-working hours
* New user account created automatically
* Modification in system software or configuration files
* System logs are deleted
* System performance decreased drastically
* Unusual display of graphics, pop-ups
* System crashes suddenly and reboots without user interventions

File intrusions

* Identifications of unknown files and program on your system
* File permission modifications
* Unexplained modifications in file size
* Identifications of strange file presence into system directories
* Missing files

Network intrusions

* Identifications of repeated attempts to log in from remote locations
* Sudden increase in bandwidth consumptions
* Repeated probes of the existing services
* Arbitrary log data in log files

**3)Storage Area**

Since most law enforcement agents are not computer security experts, it can be difficult for them to ensure that the integrity of the evidence is maintained. Digital forensic procedures must also be reliable enough to withstand courtroom scrutiny. Law enforcement agents compute hash values of image files to verify their integrity, but problems arise when the integrity of an image is lost. In such cases, the original storage media must be re-imaged .However, the media may not always be available or it may be damaged or destroyed. **The sheer volume of evidence involved in many cases requires examiners and investigators, who may be at different geographic locations, to cooperate in digital forensic investigations. What is needed is an efficient methodology for storing, moving and examining data across geographic boundaries. The ideal implementation is a centralized repository where evidence is stored and maintained, but which allows the evidence to be securely accessed from remote locations.** Furthermore, the system must be technologically transparent and it should

**DAS: DIRECT-ATTACHED STORAGE**

      Direct-attached storage (DAS) is digital storage directly attached to the computer accessing it, as opposed to storage accessed over a computer network. Examples of DAS include hard drives, optical disc drives, and storage on external drives.

|  |
| --- |
| http://www.storitback.de/service/das1.gif |
| Direct-Attach Storage connectivity example |

In Above Screen it shows that Storage device is directly attached to Server it means in realunit   
Example: If you attach a External USB drive to your Server/Desktop it is best example for DAS.  
  
Same as above example, we can attach SCSI(**Small Computer System Interface** )is a set of standards for physically connecting and transferring data between computers and peripheral devices. ) and SAS Storage Devices (The **SAS** (Serial Attached SCSI) interface standard is the latest evolution of the SCSI standard. **SAS** is a serial interface for transferring data point-to-point between hardware devices. As such, a **SAS storage** interface offers advantages over its SCSI predecessor which is a parallel interface )such as HDD and RAID(Redundant Array of Inexpensive Disks) Controllers.RAID Array a computer. LUNs can be re-assigned, unassigned or even increased in size dynamically according to network needs RAID disk arrays speed up data transfer and provide data integrity in the event of an accidental loss of digital evidence

**Disadvantages**

* An initial investment in a server with built in storage can meet the needs of a small organization for a period of time. But as data is added and the need for storage capacity increases, the server has to be taken out of service to add additional drives.
* DAS expansion generally requires the expertise of an IT professional, which means either staffing someone or taking on the expense of a consultant.
* A key disadvantage of DAS storage is its limited scalability.
* A Host Bus Adapter can only support a limited number of drives. For environments with stringent up time requirements, or for environments with rapidly increasing storage requirements, DAS may not be the right choice.

**Advantages**

* One advantage of DAS storage is its low initial cost.

**SAN: STORAGE AREA NETWORK**

              SAN (storage area network) is a high-speed network of storage devices that also connects those storage devices with servers. It provides block-level storage that can be accessed by the applications running on any networked servers. SAN storage devices can include tape libraries(a **tape library**, sometimes called a **tape** silo, **tape** robot or **tape** jukebox, is a storage device that contains one or more **tape** drives, a number of slots to hold **tape** cartridges, a barcode reader to identify **tape** cartridges and an automated method for loading **tapes** ) and disk-based devices, like RAID hardware.  
  
 Block level access means, server can able to create its own file system on SAN disk with mapped to server.

|  |
| --- |
| http://www.cloudinfinit.com/sites/default/files/u3/SAN_0.jpg |
| Storage Area Network Connectivity Example |

**Advantages**

* SAN Architecture facilitates scalability - Any number of storage devices can be added to store hundreds of terabytes.
* SAN reduces down time - We can upgrade our SAN, replace defective drives, backup our data without taking any servers offline. A well-configured SAN with redundant servers can bring zero downtime.

Sharing SAN is possible - As SAN is not directly attached with any particular server or network, a SAN can be shared by all

* SAN provides long distance connectivity - With Fibre channel capable of running upto 10 kilometers, we can keep our data in a remote, physically secure location.  Fibre channel switching also makes it very easy to establish private connections with other SANs for mirroring, backup, or maintenance.

* SAN is truly versatile - A SAN can be single entity, a master grouping of several SANs and can include SANs in remote locations.

**Disadvantages**

* SANs are very expensive as Fibre channel technology.

. compacting of existing technology investments tends to be much difficult. Though SAN facilitates to make use of already existing legacy storage, lack of SAN-building skills has greatly require deployment of different type SANs.

* Also, there are a few SAN product vendors due to its very high price and very few mega enterprises need SAN set up.

**NAS: NETWORK ATTACHED STORAGE**

    Network-attached storage (NAS) is a type of dedicated file storage device that provides local-area network local area network (LAN) nodes with file-based shared storage through a standard Ethernet connection.

|  |
| --- |
| What is Network Attached Storage (NAS) ? |
| Network Attached Storage Example |

     NAS devices, which typically do not have a keyboard or display, are configured and managed with a Web-based utility program. Each NAS resides on the LAN as an independent network node and has its own IP address.  
**Advantages**

* NAS systems stores data as files and support NFS protocols. They can be accessed easily over the commonly used TCP/IP Ethernet based networks and support multiple users connecting to it simultaneously.
* Entry level NAS systems are quite inexpensive – they can be purchased for capacities as low as 1 or 2 TB with just two disks. This enables them to be deployed with Small and Medium Business (SMB) networks easily.
* A NAS device may support one or more RAID levels to make sure that individual disk failures do not result in loss of data.
* A NAS appliance comes with a GUI based web based management console and hence can be centrally accessed and administered from remote locations over the TCP/IP networks including Internet/ VPN / Leased Lines etc.

**Disadvantages**

* Transaction intensive databases, ERP, CRM systems and such high performance oriented data are better off when stored in SAN (Storage Area Network) than NAS as the former creates a network that has low latencies, reliable, lossless and faster.Also, for large, heterogeneous block data transfers SAN might be more appropriate.
* At the end of the day, NAS appliances are going to share the network with their computing counterparts and hence the NAS solution consumes more bandwidth from the TCP/IP network. Also, the performance of the remotely hosted NAS will depend upon the amount of bandwidth available for Wide Area Networks and again the bandwidth is shared with computing devices. So, WAN optimization needs to be performed for deploying NAS solutions remotely in limited bandwidth scenarios.

often exists only in the cloud. Backed up SaaS data is copied to another cloud from where it can be restored in an emergency.

**5)Public Key Infrastructure (PKI)**

The Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates PKI systems are today one of the most accepted and used technologies to enable successful implementation of information systems security services such as authentication and confidentiality. Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. A forensic investigation of digital evidence is commonly employed as a post-event response to a serious information security incident. In fact, there are many circumstances where an organization may benefit from an ability to gather and preserve digital evidence before an incident occurs. Digital forensic readiness enables an organization to maximize its potential to use digital evidence and minimizing the costs of an investigation. The problem that this paper addresses is that there is no Digital Forensic Readiness Framework for PKI systems, thus not enabling an implementation of Digital Forensic Readiness measures to PKI systems. This paper focuses on defining the basic postulates of a Digital Forensic Readiness Framework for PKI systems. The authors investigate a model that can be proposed to accomplish this and also certain policies, guidelines and procedures which can be followed. When proposing the framework the authors take into account requirements for preserving or improving information security and not

### PKI and Digital Certificates

Public key cryptography has become widespread as a way to protect users, networks, data, and critical business systems. Whether PKI digital certificates are used to encrypt data and ensure privacy, to digitally sign documents and messages to attest to their integrity and authenticity, or to authenticate users and systems and control access, these public key operations are integral to modern operating systems, commercial security products, and custom-built systems. E-commerce, online banking, internet gaming, smartphones, and cloud computing all rely on the use of digital certificates to represent the digital identity of users, connected devices, web services, and business applications.

Each digital certificate issued by a Certificate Authority (CA) is based on a pair of cryptographic keys that form a high strength unique credential that is tightly associated with the user or organization in question and that is used to perform secure operations such as encryption.

Public Key Infrastructure (PKI)

PKI provides assurance of public key. It provides the identification of public keys and their distribution. An anatomy of PKI comprises of the following components.

* Public Key Certificate, commonly referred to as ‘digital certificate’.
* Private Key tokens.
* Certification Authority.
* Registration Authority.
* Certificate Management System.

Digital Certificate

For analogy, a certificate can be considered as the ID card issued to the person. People use ID cards such as a driver's license, passport to prove their identity. A digital certificate does the same basic thing in the electronic world, but with one difference.

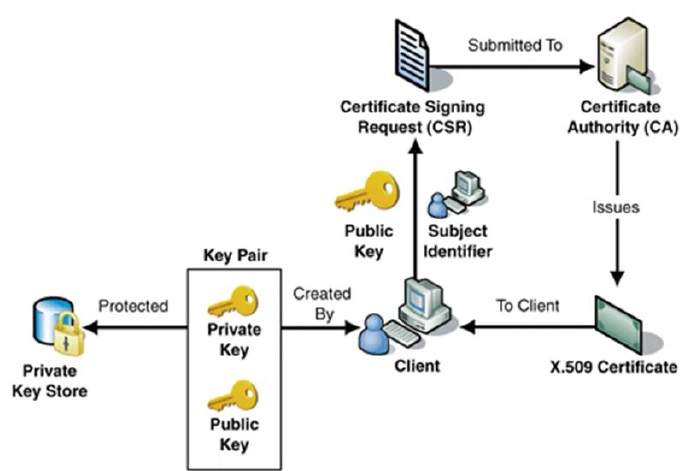
Digital Certificates are not only issued to people but they can be issued to computers, software packages or anything else that need to prove the identity in the electronic world.

* Digital certificates are based on the ITU standard X.509 which defines a standard certificate format for public key certificates and certification validation. Hence digital certificates are sometimes also referred to as X.509 certificates.

Public key pertaining to the user client is stored in digital certificates by The Certification Authority (CA) along with other relevant information such as client information, expiration date, usage, issuer etc.

* CA digitally signs this entire information and includes digital signature in the certificate.
* Anyone who needs the assurance about the public key and associated information of client, he carries out the signature validation process using CA’s public key. Successful validation assures that the public key given in the certificate belongs to the person whose details are given in the certificate.

The process of obtaining Digital Certificate by a person/entity is depicted in the following illustration.



As shown in the illustration, the CA accepts the application from a client to certify his public key. The CA, after duly verifying identity of client, issues a digital certificate to that client.

Certifying Authority (CA)

As discussed above, the CA issues certificate to a client and assist other users to verify the certificate. The CA takes responsibility for identifying correctly the identity of the client asking for a certificate to be issued, and ensures that the information contained within the certificate is correct and digitally signs it.

Key Functions of CA

The key functions of a CA are as follows −

* **Generating key pairs** − The CA may generate a key pair independently or jointly with the client.
* **Issuing digital certificates** − The CA could be thought of as the PKI equivalent of a passport agency − the CA issues a certificate after client provides the credentials to confirm his identity. The CA then signs the certificate to prevent modification of the details contained in the certificate.
* **Publishing Certificates** − The CA need to publish certificates so that users can find them. There are two ways of achieving this. One is to publish certificates in the equivalent of an electronic telephone directory. The other is to send your certificate out to those people you think might need it by one means or another.
* **Verifying Certificates** − The CA makes its public key available in environment to assist verification of his signature on clients’ digital certificate.
* **Revocation of Certificates** − At times, CA revokes the certificate issued due to some reason such as compromise of private key by user or loss of trust in the client. After revocation, CA maintains the list of all revoked certificate that is available to the environment.

Organizations deploying internal PKIs have the flexibility to Weak controls over the use of signing keys can enable the CA to be misused, even if the keys themselves are not compromised.

* Theft or misuse of keys associated with online certificate validation processes can be used to subvert revocation processes and enable malicious use of revoked digital certificates.

As new applications are brought on line, not attending to the performance aspects of signing activities associated with issuance and validation checking can result in significant business impact