UNIT 4

Cloud security fundamentals

Organizational pressure to reduce costs and optimize operations has led many enterprises to investigate cloud computing as a viable alternative to create dynamic, rapidly provisioned resources powering application and storage platforms. Despite potential savings in infrastructure costs and improved business flexibility, security is still the greatest barrier to implementing cloud initiatives for many companies. Information security professionals need to review a staggering array of security considerations when evaluating the risks of cloud computing.

Cloud security policies should be applied to both internal and third-party managed cloud environments. Whether building private or utilizing public cloud infrastructure within the enterprise, the responsibility for cloud security is shared between your organization and any cloud service providers you engage with. When conducting due diligence on cloud service providers, carefully review their published security policies and ensure that that it aligns with your own corporate policies.

The fundamental security concept employed in many cloud installations is known as the defense-in-depth strategy. This involves using layers of security technologies and business practices to protect data and infrastructure against threats in multiple ways. In the event of a security failure at one level, this approach provides a certain level of redundancy and containment to create a durable security net or grid. Security is more effective when layered at each level of the cloud stack.

When it comes to cloud security, no universal solutions are available to neutralize all threats against IT infrastructure. Corporate firewalls no longer demarcate a secure perimeter, which can often be extended well beyond the datacenter and into the cloud. It is similarly unwise to assume the security policies of third-party public and hybrid cloud service providers meet the standards and levels of compliance mandated by your internal policies. It is imperative that security requirements expected of third-parties are clearly defined and agreed upon.

Vulnerability assessment for cloud

Security vulnerabilities are prevalent across all facets of software. The vulnerabilities are increasing every year at an exponential rate. Our experience with software engineering shows it is very difficult, even impossible to build software without vulnerabilities, because of the complexity of modern software systems. So the only way to deal with vulnerabilities is find them and patch them. Discovering and patching vulnerabilities is not an easy task.

To deal with this complex vulnerability management we need standard and efficient methods and tools. The first step to deal with vulnerabilities is classifying them. Vulnerability classification is a well-studied area in computer security. Many vulnerability classifications have been proposed and devised. Most of them have chosen the taxonomy approach to classify vulnerabilities. However many of these classifications have proven to be inefficient, incomplete or erroneous. In taxonomy based classification the elements being classified are divided into groups and subgroups. Hence the taxonomy approach requires assigning vulnerabilities to one and only one sub-group. But many times vulnerability would be present in more than one sub group. This could be due to incomplete and/or incorrect definition of the vulnerability or the subgroup. It has been observed that this situation arises due to the nature of vulnerabilities themselves.

Vulnerabilities are concepts, not entities themselves. It is natural for them to overlap across different groups. Ontologies are better suited than taxonomies to model concepts. Ontology is a knowledge representation technique which is used to model real-world concepts and their relationships. It is one of the prominent techniques used to model and share a domain specific knowledge in the field of information science. Ontologies are widely used in artificial intelligence, semantic web, and library science where classification of concepts is very essential. These properties of ontologies make them perfect candidate for vulnerability classification. A rich collection of existing tools and frameworks will make creating ontology based vulnerability classification easy and efficient. The structured nature of ontologies makes it easy to reason, query and infer.

As Cloud Computing continues to expand and evolve it is influencing the way we think about computing. Every aspect of computing is now connected to cloud computing. It is a big game changer across all verticals of computing. This demands a lot of attention and research for cloud computing. The Cloud Security Alliance had mentioned that, security is one of the biggest roadblocks in adopting cloud computing. As many businesses and users are adopting and using cloud, there will be lot of software running in the cloud. Vulnerability management is still relatively new. This makes the problem even more interesting with respect to cloud computing.

Privacy and Security in cloud

Developing secure software is based on applying the secure software design principles that form the fundamental basis for software assurance. Software assurance has been given many definitions, and it is important to understand the concept. The Software Security Assurance Report2 defines software assurance as “the basis for gaining justifiable confidence that software will consistently exhibit all properties required to ensure that the software, in operation, will continue to operate dependably despite the presence of sponsored (intentional) faults. In practical terms, such software must be able to resist most attacks, tolerate as many as possible of those attacks it cannot resist, and contain the damage and recover to a normal level of operation as soon as possible after any attacks it is unable to resist or tolerate.”

The Data and Analysis Center for Software states that software must exhibit the following three properties to be considered secure

1. **Dependability** : Software that executes predictably and operates correctly under a variety of conditions, including when under attack or running on a malicious host.
2. **Trustworthiness :** Software that contains a minimum number of vulnerabilities or no vulnerabilities or weaknesses that could sabotage the software’s dependability. It must also be resistant to malicious logic.
3. **Survivability (Resilience)** : Software that is resistant to or tolerant of attacks and has the ability to recover as quickly as possible with as little harm as possible.

Confidentiality, Integrity, and Availability

Confidentiality, integrity, and availability are sometimes known as the CIA triad of information system security, and are important pillars of cloud software assurance

Confidentiality

Confidentiality refers to the prevention of intentional or unintentional unauthorized disclosure of information. Confidentiality in cloud systems is related to the areas of intellectual property rights, covert channels, traffic analysis, encryption and inference

Integrity

The concept of cloud information integrity requires that the following three principles are met:

1. Modifications are not made to data by unauthorized personnel or processes.
2. Unauthorized modifications are not made to data by authorized personnel or processes.
3. The data is internally and externally consistent — in other words, the internal information is consistent both among all sub-entities and with the real-world, external situation.

Availability

Availability ensures the reliable and timely access to cloud data or cloud computing resources by the appropriate personnel. Availability guarantees that the systems are functioning properly when needed. In addition, this concept guarantees that the security services of the cloud system are in working order. A denial-of-service attack is an example of a threat against availability.

Cloud Security Services

Additional factors that directly affect cloud software assurance include authentication, authorization, auditing, and accountability, as summarized in the following sections.

Authentication

Authentication is the testing or reconciliation of evidence of a user's identity. It establishes the user's identity and ensures that users are who they claim to be. For example, a user presents an identity (user ID) to a computer login screen and then has to provide a password. The computer system authenticates the user by verifying that the password corresponds to the individual presenting the ID.

Authorization

Authorization refers to rights and privileges granted to an individual or process that enable access to computer resources and information assets. Once a user's identity and authentication are established, authorization levels determine the extent of system rights a user can hold.

Auditing

To maintain operational assurance, organizations use two basic methods: system audits and monitoring. These methods can be employed by the cloud customer, the cloud provider, or both, depending on asset architecture and deployment.

- A system audit is a one-time or periodic event to evaluate security.

- Monitoring refers to an ongoing activity that examines either the system or the users, such as intrusion detection.

IT auditors typically audit the following functions:

- System and transaction controls
- Systems development standards
- Backup controls
- Data library procedures
- Data center security
- Contingency plans

Accountability

Accountability is the ability to determine the actions and behaviors of a single individual within a cloud system and to identify that particular individual. Audit trails and logs support accountability and can be used to conduct postmortem studies in order to analyze historical events and the individuals or processes associated with those events. Accountability is related to the concept of non repudiation, wherein an individual cannot successfully deny the performance of an action.

Cloud computing security architecture

The security posture of a cloud system is based on its security architecture. While there is no standard definition for security architecture, the Open Security Alliance (OSA) defines security architecture as “the design artifacts that describe how the security controls (= security counter measures) are positioned, and how they relate to the overall IT Architecture. These controls serve the purpose to maintain the system’s quality attributes, among them confidentiality, integrity, availability, accountability and assurance”.

Architectural Considerations

A variety of factors affect the implementation and performance of cloud security architecture. There are general issues involving regulatory requirements, adherence to standards, security management, information classification, and security awareness. Then there are more specific architecturally related areas, including trusted hardware and software, providing for a secure execution environment, establishing secure communications, and hardware augmentation through microarchitectures.

1. Compliance

In a public cloud environment, the provider does not normally inform the clients of the storage location of their data. In fact, the distribution of processing and data storage is one of the cloud's fundamental characteristics. However, the cloud provider should cooperate to consider the client's data location requirements.

In addition, the cloud vendor should provide transparency to the client by supplying information about storage used, processing characteristics, and other relevant account information. Another compliance issue is the accessibility of a client's data by the provider's system engineers and certain other employees. This factor is a necessary part of providing and maintaining cloud services, but the act of acquiring sensitive information should be monitored, controlled, and protected by safeguards such as separation of duties.

In situations where information is stored in a foreign jurisdiction, the ability of local law enforcement agencies to access a client's sensitive data is a concern. For example, this scenario might occur when a government entity conducts a computer forensics investigation of a cloud provider under suspicion of illegal activity.

2. Security Management

Security architecture involves effective security management to realize the benefits of cloud computation. Proper cloud security management and administration should identify management issues in critical areas such as access control, vulnerability analysis, change control, incident response, fault tolerance, and disaster recovery and business continuity planning. These areas are enhanced and supported by the proper application and verification of cloud security controls.

3. Controls

The objective of cloud security controls is to reduce vulnerabilities to a tolerable level and minimize the effects of an attack. To achieve this, an organization must determine what impact an attack might have, and the likelihood of loss. Examples of loss are compromise of sensitive information, financial embezzlement, loss of reputation, and physical destruction of resources.

There are many kinds of controls, but they are generally categorized into one of the following four types

1. **Deterrent controls** : Reduce the likelihood of a deliberate attack.
2. **Preventative controls** : Protect vulnerabilities and make an attack unsuccessful or reduce its impact. Preventative controls inhibit attempts to violate security policy.
3. **Corrective controls** : Reduce the effect of an attack.
4. **Detective controls** : Discover attacks and trigger preventative or corrective controls. Detective controls warn of violations or attempted violations of security policy and include such controls as intrusion detection systems, organizational policies, video cameras, and motion detectors.

4. Information Classification

There are several good reasons to classify information. Not all data has the same value to an organization. For example, some data is more valuable to upper management, because it aids them in making strategic long-range or short-range business direction decisions. Some data, such as trade secrets, formulas, and new product information, is so valuable that its loss could create a significant problem for the enterprise in the marketplace either by creating public embarrassment or by causing a lack of credibility.

In addition to the reasons, employing information classification has several clear benefits to an organization engaged in cloud computing. Some of these benefits are as follows:

- It demonstrates an organization's commitment to security protections.
- It helps identify which information is the most sensitive or vital to an organization.
- It supports the tenets of confidentiality, integrity, and availability as it pertains to data.
- It helps identify which protections apply to which information.
- It might be required for regulatory, compliance, or legal reasons.

The following classification terms are typical of those used in the private sector and are applicable to cloud data:

Public data : Information that is similar to unclassified information, all of a company's information that does not fit into any of the next categories can be considered public. While its unauthorized disclosure may be against policy, it is not expected to impact seriously or adversely the organization, its employees, and/or its customers.

Sensitive data : Information that requires a higher level of classification than normal data. This information is protected from a loss of confidentiality as well as from a loss of integrity due to an unauthorized alteration. This classification applies to information that requires special precautions to ensure its integrity by protecting it from unauthorized modification or deletion. It is information that requires a higher-than-normal assurance of accuracy and completeness.

Private data : This classification applies to personal information that is intended for use within the organization. Its unauthorized disclosure could seriously and adversely impact the organization and/or its employees. For example, salary levels and medical information are considered private.

Confidential data : This classification applies to the most sensitive business information that is intended strictly for use within the organization. Its unauthorized disclosure could seriously and adversely impact the organization, its stockholders, its business partners, and/or its customers.

Trusted Cloud Computing

Trusted cloud computing can be viewed as a computer security architecture that is designed to protect cloud systems from malicious intrusions and attacks, and ensure that computing resources will act in a specific, predictable manner as intended. A trusted cloud computing system will protect data in use by hypervisors and applications, protect against unauthorized access to information, provide for strong authentication, apply encryption to protect sensitive data that resides on stolen or lost devices, and support compliance through hardware and software mechanisms.

Trusted Computing Characteristics

In a cloud computational system, multiple processes might be running concurrently. Each process has the capability to access certain memory locations and to execute a subset of the computer's instruction set. The execution and memory space assigned to each process is called a protection domain. This domain can be extended to virtual memory, which increases the apparent size of real memory by using disk storage. The purpose of establishing a protection domain is to protect programs from all unauthorized modification or execution interference. A trusted computing base (TCB) is the total combination of protection mechanisms within a computer system, which includes the hardware, software, and firmware that are trusted to enforce a security policy. Because the TCB components are responsible for enforcing the security policy of a computing system, these components must be protected from malicious and untrusted processes. The TCB must also provide for memory protection and ensure that the processes from one domain do not access memory locations of another domain.

Another element associated with trusted computing is the trusted platform module (TPM). The TPM stores cryptographic keys that can be used to attest to the operating state of a computing platform and to verify that the hardware and software configuration has not been modified. However, the standard TPM cannot be used in cloud computing because it does not operate in the virtualized cloud environment. To permit a TPM version to perform in the cloud, specifi cations have been generated for a virtual TPM (VTM)4 that provides software instances of TPMs for each virtual machine operating on a trusted server.

The cloud provider must conduct quality risk assessments at regular, known intervals to meet the trust expectations of clients and auditors, and demonstrate that risk is being managed effectively. Additional factors that inspire trust include the following:

- Use of industry-accepted standards.
- Provision for interoperability and transparency.
- Robust authentication and authorization mechanisms in access control.
- Management of changing personnel and relationships in both the cloud client and provider organizations.
- Establishment of accountability with respect to security and privacy requirements in a multi-party, flexible service delivery setting.
- Use of information system security assurance techniques and metrics to establish the effectiveness of hardware and software protection mechanisms.
- Establishment of effective policies and procedures to address multiple legal jurisdictions associated with cloud international services and compliance, requirements.

Secure Execution Environment and Communications

In cloud computing, the major burden of establishing a secure execution environment is transferred from the client to the cloud provider. However, protected data transfers must be established through strong authentication mechanisms, and the client must have practices in place to address the privacy and confidentiality of information that is exchanged with the cloud. In fact, the client’s port to the cloud might provide an attack path if not properly provisioned with security measures. Therefore, the client needs assurance that computations and data exchanges are conducted in a secure environment. This assurance is affected by trust enabled by cryptographic methods. Also, research into areas such as compiler-based virtual machines promises a more secure execution environment for operating systems.

1. Secure Communications

Secure cloud communications involves the structures, transmission methods, transport formats, and security measures that provide confidentiality, integrity, availability, and authentication for transmissions over private and public communications networks. Secure cloud computing communications should ensure the following:

Confidentiality : Ensures that only those who are supposed to access data can retrieve it. Loss of confidentiality can occur through the intentional release of private company information or through a misapplication of network rights. Some of the elements of telecommunications used to ensure confidentiality are as follows:

- Network security protocols
- Network authentication services
- Data encryption services

Integrity: Ensures that data has not been changed due to an accident or malice. Integrity is the guarantee that the message sent is the message received and that the message is not intentionally or unintentionally altered. Integrity also contains the concept of non repudiation of a message source. Some of the constituents of integrity are as follows:

- Firewall services
- Communications Security Management
- Intrusion detection services

Availability : Ensures that data is accessible when and where it is needed, and that connectivity is accessible when needed, allowing authorized users to access the network or systems. Also included in that assurance is the guarantee that security services for the security practitioner are usable when they are needed. Some of the elements that are used to ensure availability are as follows:

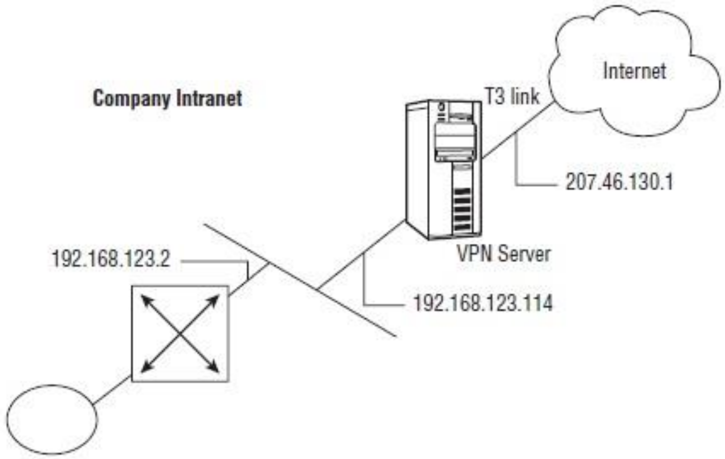
- Fault tolerance for data availability, such as backups and redundant disk systems
- Acceptable logins and operating process performances
- Reliable and interoperable security processes and network security mechanisms

2. Application Program Interface (API)

Common vulnerabilities such as weak antivirus software, unattended computing platforms, poor passwords, weak authentication mechanisms, and inadequate intrusion detection that can impact communications must be more stringently analyzed, and proper APIs must be used.

3. Virtual Private Network (VPN)

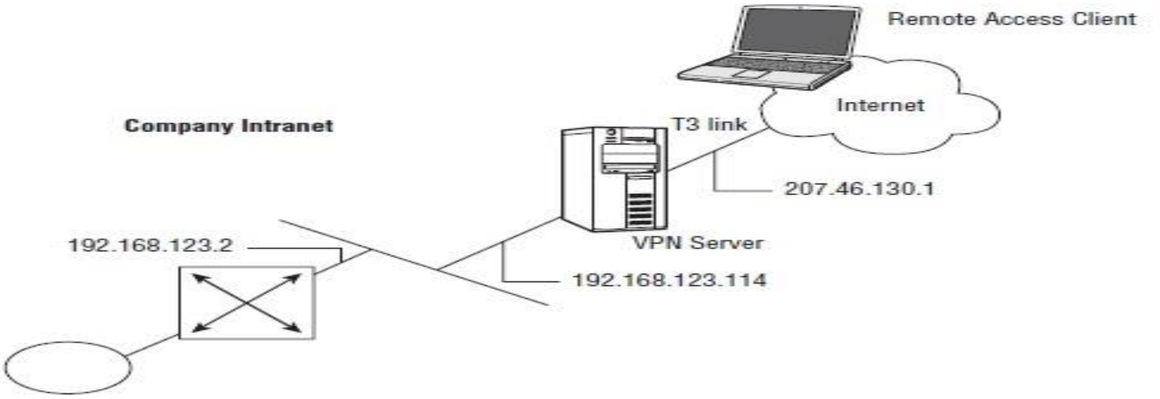
Another important method to secure cloud communications is through a virtual private network (VPN). A VPN is created by building a secure communications link between two nodes by emulating the properties of a point-to-point private link. A VPN can be used to facilitate secure remote access into the cloud, securely connect two networks together, or create a secure data tunnel within a network.



The two general types of VPNs relevant to cloud computing are remote access and network-to-network. These VPN types are described in the following sections.

3. 1 Remote Access VPNs

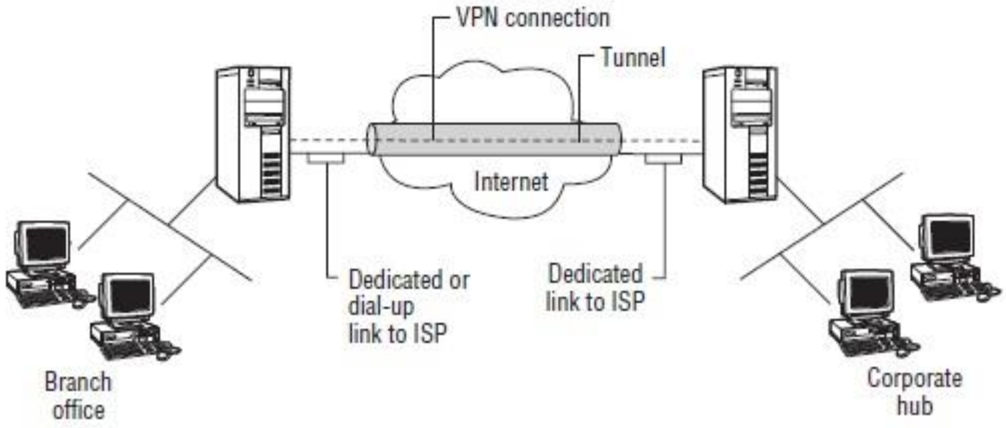
A VPN can be confi gured to provide remote access to corporate resources over the public Internet to maintain confi dentiality and integrity. This configuration enables the remote user to utilize whatever local ISP is available to access the Internet without forcing the user to make a long-distance or 800 call to a third-party access provider. Using the connection to the local ISP, the VPN software creates a virtual private network between the dial-up user and the corporate VPN server across the Internet.



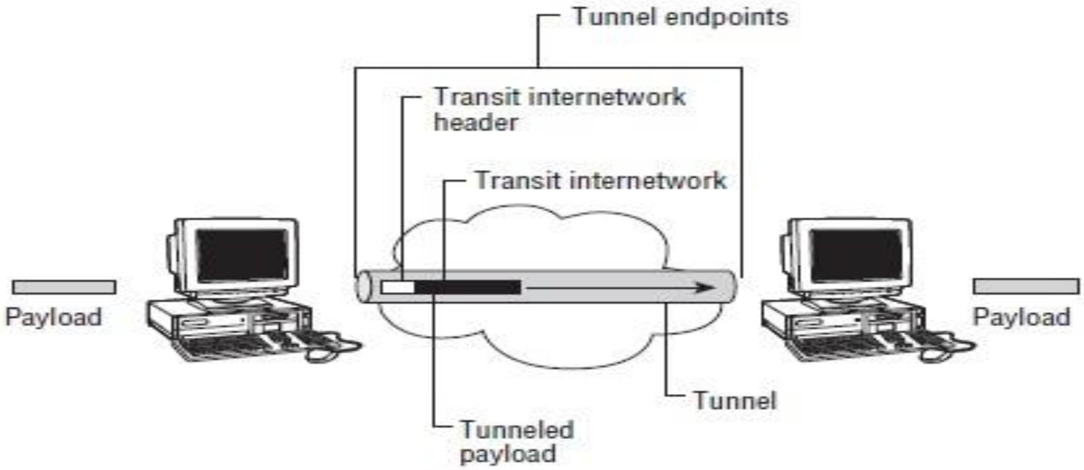
3.2 Network-to-Network VPNs

A VPN is commonly used to connect two networks, perhaps the main corporate LAN and a remote branch offi ce LAN, through the Internet. This connection can use either dedicated lines to the Internet or dial-up connections to the Internet. However, the corporate hub router that acts as a VPN server must be connected to a local ISP with a dedicated line if the VPN server needs to be available 24/7.

The VPN software uses the connection to the local ISP to create a VPN tunnel between the branch office router and the corporate hub router across the Internet. Following figure shows a remote branch office connected to the corporate main office using a VPN tunnel through the Internet.



4. VPN Tunneling



VPN Tunneling is a method of transferring data from one network to another network by encapsulating the packets in an additional header. The additional header provides routing information so that the encapsulated payload can traverse the intermediate networks. For a tunnel to be established, both the tunnel client and the tunnel server must be using the same tunneling protocol. Tunneling technology can be based on either a Layer 2 or a Layer 3 tunneling protocol. These layers correspond to the Open Systems Interconnection (OSI) Reference Model.

Micro-architectures

The design elements of the microprocessor hardware and firmware that provide for the implementation of the higher-level architecture are referred to as Microarchitecture.

A microarchitecture design might incorporate the following:

Pipelining : Increases the performance of a computer by overlapping the steps of different instructions. For example, if the instruction cycle is divided into three parts — fetch, decode, and execute instructions can be overlapped to increase the execution speed of the instructions.

Superscalar processor : A processor that enables the concurrent execution of multiple instructions in both the same pipeline stage as well as different pipeline stages.

Very-long instruction word (VLIW) processor : A processor in which a single instruction specifies more than one concurrent operation.

Multi-programming : Executes two or more programs simultaneously on a single processor (CPU) by alternating execution among the programs.

Multi-tasking : Executes two or more subprograms or tasks at the same time on a single processor (CPU) by alternating execution among the tasks.

Multi-processing : Executes two or more programs at the same time on multiple processors. In symmetric multi-processing, the processors share the same operating system, memory, and data paths, while in massively parallel multi-processing, large numbers of processors are used.

Multi-threading : Concurrent tasks that share resources and run inside a process. In a multi-processing system, threads run in parallel.

Identity Management and Access Control

Identity management and access control are fundamental functions required for secure cloud computing. The simplest form of identity management is logging on to a computer system with a user ID and password. However, true identity management, such as is required for cloud computing, requires more robust authentication, authorization, and access control.

1. Identity Management

Identification and authentication are the keystones of most access control systems.

1. **Identification** is the act of a user professing an identity to a system, usually in the form of a username or user logon ID to the system. Identification establishes user accountability for the actions on the system. User IDs should be unique and not shared among different individuals.
2. **Authentication** is verification that the user's claimed identity is valid, and it is usually implemented through a user password at logon. Authentication is based on the following three factor types:
    - Type 1 — Something you know, such as a personal identification number (PIN) or password
    - Type 2 — Something you have, such as an ATM card or smart card
    - Type 3 — Something you are (physically), such as a fingerprint or retina scan

1.1 Passwords

Because passwords can be compromised, they must be protected. In the ideal case, a password should be used only once. This "one-time password," or OTP, provides maximum security because a new password is required for each new logon.

- A password that is the same for each logon is called a static password.
- A password that changes with each logon is termed a dynamic password

1.2 Tokens

Tokens, in the form of small, hand-held devices, are used to provide passwords. The following are the four basic types of tokens

- Static password tokens
- Synchronous dynamic password tokens, clock-based
- Synchronous dynamic password tokens, counter-based
- Asynchronous tokens, challenge-response

1. 3 Memory Cards

Memory cards provide nonvolatile storage of information, but they do not have any processing capability. A memory card stores encrypted passwords and other related identifying information. A telephone calling card and an ATM card are examples of memory cards.

1.4 Smart Cards

Smart cards provide even more capability than memory cards by incorporating additional processing power on the cards. These credit-card-size devices comprise microprocessor and memory and are used to store digital signatures, private keys, passwords, and other personal information.

1.5 Biometrics

Biometrics is defined as an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics. In biometrics, identification is a one-to-many search of an individual's characteristics from a database of stored images. Authentication is a one-to-one search to verify a claim to an identity made by a person. Biometrics is used for identification in physical controls and for authentication in logical controls.

There are three main performance measures in biometrics:

1. **False rejection rate (FRR) or Type I Error** : The percentage of valid subjects that are falsely rejected.
2. **False acceptance rate (FAR) or Type II Error** : The percentage of invalid subjects that are falsely accepted.
3. **Crossover error rate (CER)** : The percentage at which the FRR equals the FAR. The smaller the CER, the better the device is performing.

2. Access Control

Access control is intrinsically tied to identity management and is necessary to preserve the confidentiality, integrity, and availability of cloud data.

Three things that must be considered for the planning and implementation of access control mechanisms are threats to the system, the system's vulnerability to these threats, and the risk that the threats might materialize. These concepts are defined as follows:

1. **Threat** : An event or activity that has the potential to cause harm to the information systems or networks
2. **Vulnerability** : A weakness or lack of a safeguard that can be exploited by a threat, causing harm to the information systems or networks
3. **Risk** : The potential for harm or loss to an information system or network; the probability that a threat will materialize

2.1 Controls

Controls are implemented to mitigate risk and reduce the potential for loss. Two important control concepts are separation of duties and the principle of least privilege. Separation of duties requires an activity or process to be performed by two or more entities for successful completion. Thus, the only way that a security policy can be violated is if there is collusion among the entities.

Control measures can be administrative, logical (also called technical), and physical in their implementation.

- **Administrative controls** include policies and procedures, security awareness training, background checks, work habit checks, a review of vacation history, and increased supervision.
- **Logical or technical controls** involve the restriction of access to systems and the protection of information. Examples of these types of controls are encryption, smart cards, access control lists, and transmission protocols.
- **Physical controls** incorporate guards and building security in general, such as the locking of doors, the securing of server rooms or laptops, the protection of cables, the separation of duties, and the backing up of files.

2.2 Models for Controlling Access

Controlling access by a subject (an active entity such as an individual or process) to an object (a passive entity such as a file) involves setting up access rules. These rules can be classified into three categories or models.

- **Mandatory Access Control :** The authorization of a subject's access to an object depends upon labels, which indicate the subject's clearance, and the classification or sensitivity of the object.
- **Discretionary Access Control** : With discretionary access control, the subject has authority, within certain limitations, to specify what objects are accessible.
- **Nondiscretionary Access Control** : A central authority determines which subjects can have access to certain objects based on the organizational security policy. The access controls might be based on the individual's role in the organization (role-based) or the subject's responsibilities and duties (task-based).

Autonomic Security

Autonomic computing refers to a self-managing computing model in which computer systems reconfigure themselves in response to changing conditions and are self-healing. The promise of autonomic computing will take a number of years to fully materialize, but it offers capabilities that can improve the security of information systems and cloud computing in particular. The ability of autonomic systems to collect and interpret data and recommend or implement solutions can go a long way toward enhancing security and providing for recovery from harmful events.

1. Autonomic Systems

Autonomic systems are based on the human autonomic nervous system, which is self-managing, monitors changes that affect the body, and maintains internal balances. Therefore, an autonomic computing system has the goal of performing self-management to maintain correct operations despite perturbations to the system. Such a system requires sensory inputs, decision-making capability, and the ability to implement remedial activities to maintain an equilibrium state of normal operation.

Examples of events that would have to be handled autonomously include the following:

- Malicious attacks
- Hardware or software faults
- Excessive CPU utilization
- Power failures
- Organizational policies
- Inadvertent operator errors
- Interaction with other systems
- Software updates

The underlying concept of autonomic systems is self-management, whereby a computational system maintains proper operation in the face of changing external and internal conditions, evaluates the necessity for upgrades, installs software, conducts regression testing, performs performance tuning of middleware, and detects and corrects problem situations in general.

2. Autonomic Protection

Autonomic self-protection involves detecting a harmful situation and taking actions that will mitigate the situation. These systems will also be designed to predict problems from analysis of sensory inputs and initiate corrective measures.

An autonomous system security response is based on network knowledge, capabilities of connected resources, information aggregation, the complexity of the situation, and the impact on affected applications.

Autonomous protection systems should, therefore, adhere to the following guidelines:

- Minimize overhead requirements.
- Be consistent with security policies.
- Optimize security-related parameters.
- Minimize impact on performance.
- Minimize potential for introducing new vulnerabilities.
- Conduct regression analysis and return to previous software versions if problems are introduced by changes.
- Ensure that reconfiguration processes are secure.

3. Autonomic Self-Healing

The process of diagnosing and repairing failures in IT systems can be difficult, time consuming, and usually requires intensive labor effort. Autonomic self healing systems can provide the capability to detect and repair software problems and identify hardware faults without manual intervention.

The autonomic process would obtain logged and monitored information and perform an analysis to diagnose the problem area. This procedure is usually conducted by an autonomic manager that controls computing resource elements with well-defined interfaces that support the diagnostic and mitigation actions. The managed elements control their internal states and have defined performance characteristics and relationships with other computational elements.

The objective of the autonomous self-healing process is to keep the elements operating according to their design specifications.

Virtualization Security Management

Although the global adoption of virtualization is a relatively recent event, threats to the virtualized infrastructure are evolving just as quickly. Historically, the development and implementation of new technology has preceded the full understanding of its inherent security risks, and virtualized systems are no different.

1. Virtual Threats

Some threats to virtualized systems are general in nature, as they are inherent threats to all computerized systems (such as denial-of-service, or DoS, attacks). Other threats and vulnerabilities, however, are unique to virtual machines. Many VM vulnerabilities stem from the fact that a vulnerability in one VM system can be exploited to attack other VM systems or the host systems, as multiple virtual machines share the same physical hardware.

2. Hypervisor Risks

The hypervisor is the part of a virtual machine that allows host resource sharing and enables VM/host isolation. Therefore, the ability of the hypervisor to provide the necessary isolation during intentional attack greatly determines how well the virtual machine can survive risk.

3. Increased Denial of Service Risk

The threat of denial-of-service (DoS) attacks against a virtualized system is as prevalent as it is against non virtualized systems; but because the virtual machines share the host's resources, such as memory, processor, disk, I/O devices, and so on, a denial-of-service attack risk against another VM, the host, or an external service is actually greatly increased.

VM Security Recommendations

The following security implementation techniques are required for most computer systems, and are still best practices for virtualized systems. These areas include physical security, patching, and remote management techniques.

- Hardening the Host Operating System
- Limiting Physical Access to the Host
- Using Encrypted Communications
- Disabling Background Tasks
- Updating and Patching
- Enabling Perimeter Defense on the VM
- Implementing File Integrity Checks
- Maintaining Backups

VM-Specific Security Techniques

A fundamental requirement for a successful virtualization security process is recognizing the dynamic nature of virtual machines. Therefore, many of the following security techniques are fairly unique to virtualized systems, and should be implemented in addition to the traditional best practice techniques just described.

- Hardening the Virtual Machine
- Harden the Hypervisor
- Root Secure the Monitor
- Implement Only One Primary Function per VM
- Firewall Any Additional VM Ports
- Harden the Host Domain
- Use Unique NICs for Sensitive VMs
- Disconnect Unused Devices