Table of Contents

Chapter 1 – Security Overview

Learning Objectives

What this chapter is about?

- This chapter will give an overview on Security overview

What you should be able to do

- Understand what Security is?
- IT Management challenge
- Operating System Security
- Authentication
- System threats
- Data center security
- Cloud computing security
- Security frame work

How you will check your progress

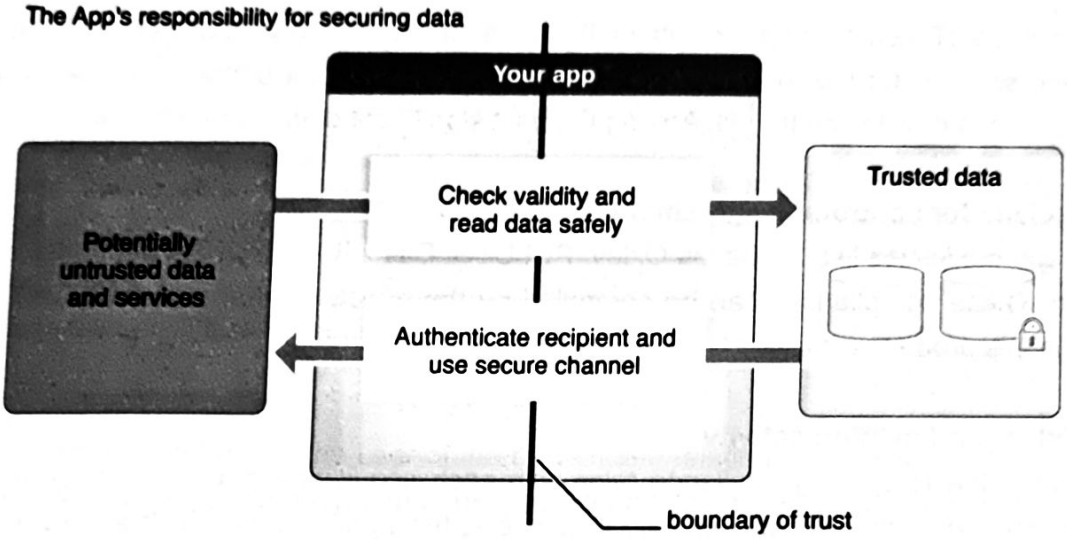
Accountability:

- Checkpoint questions

ecurity Overview

the cloud-enabled, highly networked domain of modern computing, security is one of the most important spects of appropriate software industry.

e most important thing to realize about security is that it cannot be determined. It cannot be locked at the d of the development process. Security must be designed consciously into the application or service m the beginning, and make it a sensible part of the entire process from design through implementation, sting, and release.



the application layer, security is

the application layer, security means being conscious of how the code uses data and confirming that it ovides security so securely and reliably. For example, it is the users' responsibility to:

- **Save users' private data safe from intruders.** Store the data in a protected method, and confirm that the software gathers only the data that it needs.
- **Untrusted files and data should be handled with care.** The software must properly validate the data if it accesses the data from the internet or read files that have been sent through internet. If the software is unable to validate the data properly, then it may accidentally provide a path for the attackers to access the personal information that may be available on the user's computer or other device.
- **Safeguard the data that travels.** If the software transfers the personal data over the internet, it must be transferred in a secure manner to prevent the unauthorized access to the data while in transfer.

- **Authenticate the data wherever necessary.** If the software offers access to or works with encrypted data, it should authenticate those signatures to confirm that the data has not been damaged.

The IT security management challenge

There are large number of pressures faced by the security managers today. They should maintain a secure environment to safeguard the company's assets and industry reputation, and also all should be done at a lower cost.

This stress to raise IT competence occurs in the face of growing demands for more and improved applications and services for the wide user population. The demands for better proficiencies and services spring from numerous developing trends. Among the best significant of these trends are:

Improved requisite for controlling agreement

Current rules and guidelines like Sarbanes-Oxley, PCI DSS, Basel II, and HIPAA put heavy burden on the security group. These compliances can be controlled by the effective internal security which can create huge strains on this group

Improved mixture and gaining activity

The complexity of the IT security challenge raise with each acquisition of the company as the company develops through acquirement or fusion. The new users, the applications and the mixture of the legacy systems must be combined with an current IT infrastructure. As a result, the complexity of the new infrastructure can grow considerably

Progressively growing user populations

Handling cumulative numbers of users, their profiles, and their access rights to secured applications puts a pressure on funds and rises the requirement for an operative way of refining the overall efficacy and competence of IT and other associated organizations (such as the Help Desk).

Evolving skills modify the IT security setting

Of the many new expertise and service representations that have appeared in recent times, virtualization and cloud computing seems to have the major potential effect on IT security administrations. The momentum to these skills is based, to a large extent, on the operational proficiency and cost savings benefits that they can potentially offer. Therefore, IT security managers are challenged to integrate these new models into their approach to gain these profits, while at the same time not losing any security abilities that their existing infrastructure delivers.

These aspects are motivating IT security organizations to implement solutions that can reorganize the management of their security processes.

Operating System - Security

Security refers to providing a shield to computer system resources such as CPU, memory, disk, software programs and most essentially data/information stored in the computer system. If a computer program is executed by unauthorized user then the user may source severe damage to computer or information available in it. So a computer system must be secured against unauthorized access, mischievous access to system memory, viruses, worms etc.

Security can be provided by

- Authentication
- One Time passwords
- Program Threats
- System Threats
- Computer Security Classifications

Authentication

Authentication refers to recognizing the user of the system and relating the executing programs with those users. It is the duty of the Operating System to generate a protection system which guarantees that a user who is executing a specific program is authentic. Operating Systems normally recognizes/authenticates users using following three ways:

- **Username / Password** – To access the resources of the system, a username and password should be provided by the user that has been registered with the Operating system.
- **User card/key** - punch cards are used by the user in card slot, keys generated by the key generator can be provided for logging in into the system.
- **User attribute - fingerprint/ eye retina pattern/ signature** – users can provide their attribute through the particular input device connected to operating system for logging in into the system.

One Time passwords

One time passwords offers additional security along with usual validation. In One-Time Password system, a distinctive keyword is required every time user attempts to login into the system. After a one-time password is used then it cannot be used again. One time password is implemented in various ways.

- **Random numbers** – Cards printed with the numbers along with the respective alphabets are provided to the users. System queries for the numbers respective to some alphabets in a random manner
- **Secret key** - A hardware device is provided to the user that generates a secret id bound to the user id. The user can provide the secret id to the system every time before logging in.
- **Network password** – One time password is sent to the user by some commercial applications on the user's registered email or mobile that can be used before logging in.

Program Threats

The designated task will be done by the kernel and the operating system's processes as instructed. If the processes invoked by the user program do malicious tasks then it is called as Program Threats. The most common example of program threat is a program available on a system that can store and transfer the user credentials over the network to a hacker. A list of few well known program threats as follows

- **Trojan Horse** – These program steals user login credentials and save them to transfer to mischievous user who can further login to computer and can use the system resources.
- **Trap Door** - If a program which is intended to work as required, have a security hole in its program and carry out dishonest action without awareness of user then it is known to have a trap door.
- **Logic Bomb** - Logic bomb is a condition while a code misbehaves simply when some circumstances met else it executes as honest code. It is tougher to identify this kind of a program.
- **Virus** - Virus is a program that can duplicate itself on computer system. They are very dangerous and can change/remove user information, crash systems. A virus is normally a small code embedded in a program. As user executes the program, the virus gets embedded in other records/ programs and can make system inoperative for user.

System Threats

System threats are mismanagement of system services and network connections to put user in trouble. System threats launches program threats on a comprehensive network known as program attack. System threats generate such an atmosphere that operating system resources/ user information are misused. A list of few well known system threats as follows.

- **Worm** -Worm is a method which can upset down a system routine by using system resources to dangerous levels. A Worm procedure produces it's numerous copies where each copy uses system resources, avoids all other processes to get essential resources. Worms' processes can even shut down an entire network.

- **Port Scanning** - Port scanning is a method by which a hacker can identify system vulnerabilities to attempt an attack on the system.
- **Denial of Service** - Denial of service attacks usually avoids user to make genuine usage of the system. For instance suppose the denial of service changes browser's content settings, the internet cannot be used by the user.

Computer Security Classifications

In computer systems, based on U.S. Department of Defense Trusted Computer System's Evaluation criteria, security is classified into four types. They are A, B, C and D. These specifications are widely used to determine and design the security of systems and of security solutions. Each classifications is briefly described as follows

S.N.	Classification Type	Description
1	Type A	• Top Level. Recognized verification methods and design specifications are used. A high degree of assurance is granted for process security. • Protection system is provided mandatorily. Properties of the class C2 system are incurred. Each object is attached with the sensitivity label.
2	Type B	• **B1** – The security label is maintained for each object in the system. Decisions to access control are made using the label. • **B2** – The sensitivity labels are extended to each of the system resource like auditing of events, storage objects and supports covert channels. • **B3** – creation of lists or user groups for access-control is permitted to revoke access or grant access to a given named object. Audit capabilities are used to offer safety and user accountability. It is of two types.
3	Type C	• **C1** - Integrates controls so that users can safeguard their reserved data and prevent other users from accidentally accessing / removing their data. UNIX versions are mostly CI class.

- C2 - Enhances an individual-level access control to the abilities of a Cl level system

4 Type D Bottom level. Least protection. MS-DOS, Window 3.1 fall in this category.

Application Security

The organization suffers from badly coded applications. A considerable quantity of private consumer data resides within the application layer as more and more companies develop applications to reorganize internal progressions and expand the customer skill. However, without making security an essential part of the Software Development Life Cycle (SDLC), the threat related with insecure applications far be greater than these advantages in productivity and customer fulfillment.

Trustwave's full set of application security clarifications carried by a professional team of application experts guarantees that the application is verified and studied thoroughly. The application security group uses manual procedures to check and review applications according to needs of the user. The outcome is precise guidance that can considerably progress the security of the applications. Traditional application testing with programmed tools offers common results that do little to fight the rapidly changing landscape of security adventures.

Application Penetration Testing

An application penetration test pretends an attack against an application to conclude the efficiency of its security controls. Accomplished by Trustwave's application security experts, the manual testing process analyses the application much more carefully than predetermined assessment tools that can yield generic reactions and excessive false positives. By systematically testing an application from a range of authenticated- and unauthenticated user perceptions, the Trustwave application penetration testing service highlights threats posed by exploitable vulnerabilities. Trustwave application penetration tests assess an application's vulnerability to all recognized application exploits comprising but not limited to:

- Arbitrary Code Execution
- Authentication Bypass
- Input Validation
- Input Tampering
- Cross-Site Scripting
- URL Manipulation
- SQL Injection

- Hidden Variable Manipulation
- Buffer Overflows
- Cookie Modification

The purpose of Trustwave's application penetration testing methodology is to determine current, exploitable vulnerabilities within an application that can lead to the compromise of critical data. Clients obtain the significances in a complete deliverable comprising both considered and strategic approvals. The simulated attack helps clients in pinpointing faults and justifying the threat of data compromise.

Trustwave can accomplish systematic penetration tests of any application including but not limited to:

- Web-Based Applications—Web application interfaces are suitable, but a growth in threat accompanies this comfort of use. Trustwave's application penetration testing service comprises of a complete test of the complete Web application and its associate environment.
- Thin-Client Applications—Thin-client applications are installed on the client machine but are mainly used to carry data from a central server, where the bulk of processing and data controls are held. Using Trustwave's experts to conduct testing of thin-client applications offers clients with a complete test of the thin-client environment.
- Thick-Client Applications—Thick-client applications run nearly exclusively on the client machine, and server associations are used only for storage or communication. Restricted or no dependence on a server does not eradicate the threat of data compromise.

Application Code Review

Custom applications need convention security. In the Trustwave application code review, our application security specialists manually examine all appropriate application source code to determine deficits in security controls and recognize development faults that interrupt best practices or may lead to vulnerabilities.

A Trustwave application code assessment observes all features of an application's security at the source-code level. In addition, the assessment comprises an valuation of the tools and viable applications used to generate and run the front- and back-end services.

Trustwave's study will assess the application for vulnerabilities including:

- Improper Buffer Checking
- Dynamic Content Creation Issues
- Unintended Operations
- Secure Code Signing
- Input Validation
- Improper Cryptography

- SQL Injection
- Unexpected Failure Conditions
- Command Redirection
- Insecure Automatic Data Inclusion

The code assessment concludes in a comprehensive report that facts precise areas of application code that require repair in order to sustain a secure system. Trustwave's manual evaluation confirms that the developers collect actionable, prescriptive data exact to the application rather than common data delivered by automated tools.

Specifically, Trustwave will deliver a report for each revised application that will describe:

- Particular application and its version verified
- Modules of evaluation done on the application
- Valuation of the efficiency of existing controls in terms of design and working value
- Testing records
- Application threats recognized
- Application security threat justification references based on assessments
- Complete risk-level assessment of the application
- Discussion of the assessment activities done to attain at the overall rating

Secure Developer Training

Trustwave offers a tailored preparation class to an organization's designers based upon industry finest practices and the outcomes of the actual assessments done. This service, Secure Developer Training, has been established to be more operative in justifying upcoming coding errors as developers are accomplished on instances taken from their personal applications.

Trustwave can offer one to three days of client-site preparation designed to fit the client's application development setting. Preferably, the training session follows an application program assessment or application penetration test arrangement so that particular illustrations from those engagements can be incorporated within the training session. This approach the client's staff absorbs from real-world and business-relevant coding problems and can place their understanding to practice instantly.

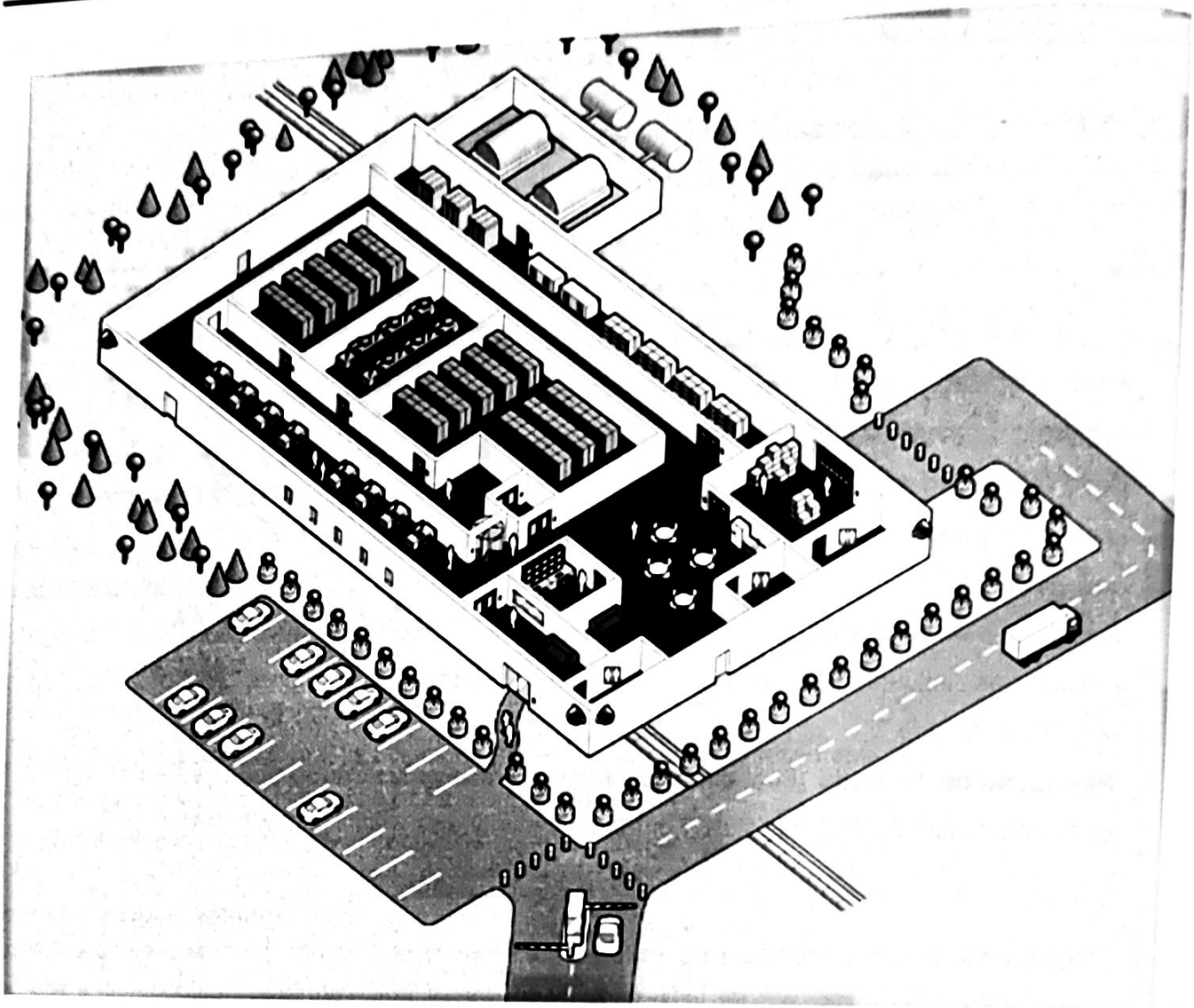
Data Center Security

There are abundant of complex documents that can lead companies through the procedure of planning a secure data center—from the gold-standard provisions used by the federal government to form sensitive amenities like delegations, to setup principles distributed by industry groups like the Telecommunications Industry Association, to security necessities from the likes of the National Fire Protection Association. The

CSO's high-level goals should make sure that protection for the new data center is constructed into the strategies, instead of being an expensive or incompetent postscript.

An imaginary data center is intended to withstand all from corporate intelligence performers to terrorists to natural tragedies is described below. Certainly the additional protections can be costly. Nevertheless they are just a portion of the cost of construction a secure capacity that also can retain humming through tragedies.

1. **Shape on the right spot.** Be certain the construction is specific distance from headquarters (20 miles is typical) and minimum 100 feet from the main road. Neighbors should not be available: aerodromes, chemical services, power plants
2. **Have redundant services.** Data centers require two sources for services, such as power, water, vocal sound and information. Identify electricity sources back to two distinct substations and water back to two different main lines. Lines should be concealed and should be available into different areas of the building, with water distinct from other services. Use the data center's predicted power practice as influence for receiving the electric company to house the building's special requirements.
3. **Pay attention to walls.** Foot-thick concrete is a economical and operative barrier against the components and explosive utilities. For further security, use walls lined with Kevlar.



4. **Avoid windows.** Consider warehouse, not workplace structure. If there are windows, restrict them to the break room or executive area, and use bomb-resistant sealed glass.
5. **Use landscaping for security.** Trees, stones and channel can block the building from cars passing near, vague security devices (like fences), and also aid to park vehicles from getting too close.
6. **Retain a 100-foot defense zone all over the place.** If landscaping does not defend the building from vehicles, replace crash-proof barriers in its place. Bollard planters are not as much obvious and smarter than other devices.
7. **Use coverable crash blocks at vehicle entrance points.** Control entree to the parking lot and stocking dock with a supervised guard station that controls the coverable bollards. Use a elevated gate and a green light as visual signals that the bollards are down and the driver can go forward. In

conditions when additional safety is required, have the fences left up by default, and dropped only when someone has authorization to pass through.

8. **Proposal for bomb discovery.** For data centers that are specifically delicate or possibly targets, have guards use mirrors to search under vehicles for explosives, or offer handy bomb-sniffing devices. A raised threat can be responded by increasing the amount of vehicles that are checked possibly by inspecting employee vehicles as well as visitors and delivery trucks.
9. **Restrict entry points.** Control admission to the building by forming one main entrance, plus a rear one for the stocking dock. This saves costs too.
10. **Create fire doors exit only.** For exits needed by fire codes, mount doors that don't have handles externally. When any of these entries is opened, a loud alarm should sound and generate a reaction from the security command center.
11. **Use cameras abundantly.** Observation cameras should be mounted about the boundary of the building, at all entrances and exits, and at each access point all over the building. An arrangement of low-light cameras, standard fixed cameras, pan-tilt-zoom cameras and motion-detection devices is perfect. Footage should be digitally documented and stored offsite.
12. **Defend the building's equipment.** Retain the machine-driven area of the building, which stocks conservational systems and uninterruptible power supplies, strictly off limits. If generators are outdoor, use concrete walls to protect the area. For both areas, be certain that all contractors and repair crews are escorted by an employee at all times.
13. **Design for protected air management.** Make assured the heating, ventilating and air-conditioning systems can be fixed to recirculate air rather than bringing in air from the external area. This could help safeguard people and equipment if there were particular kind of genetic or organic attack or hefty smoke dispersal from a nearby fire. For additional security, set devices in place to observe the air for organic, genetic or radiological pollutant.
14. **Confirm nothing can hide in the walls and ceilings.** In protected areas of the data center, make certain interior walls track from the slab ceiling all the way to subflooring where cabling is normally accommodated. Also assure drop-down ceilings could not provide concealed access points.
15. **Practice two-factor authentication.** Biometric identification is suitable standard for admission to mild areas of data centers, with fingerprint scanners or hand geometry generally considered less intense than retinal scanning. In other areas, it is possibly to get away with less-expensive access cards.
16. **Strengthen the core with safety layers.** Anyone arriving the most protected part of the data center will have been authenticated at least thrice, including:

1. At the outer door. There must be a way for the visitors to call the front desk.
2. At the inner door. Parts guest area from common employee area.
3. At the admission to the "data" portion of the data center. Normally, this is the level that has the firmest "positive control," meaning taking credit is not allowed. For implementation, there are two options:

    a) A floor-to-ceiling entrance. If someone attempts to sneak in behind an authenticated user, the door gradually rotates in the opposite direction. (In case of a fire, the walls of the entrance level to permit rapid outlet.)

    b) A "mantrap." Offers alternate admission for tools and for persons with disabilities. This comprises of two distinct doors with an airlock in between. Only one door can be unlocked at a time, and validation is required for both doors.

4. At the door to an separate computer processing area. This is for the area where real servers, mainframes or further acute IT equipment is placed. Offer admission only on an as-needed basis, and part these rooms as much as possible in order to control and observe access.

17. **Monitor the exits too.** Watch entrance and exit—not only for the primary facility but for more delicate areas of the facility as well. It will help to keep track of who was where when. It also aids with building clearance if there's a fire.
18. **Do not allow food in the computer rooms.** Provide a communal area where people can have food without spilling food on computer equipment.
19. **Set up guest time-out area.** Make certain to include bathrooms for usage by visitors and distribution people who do not have admission to the protected parts of the building.

Security – Cloud Computing

Data security is the primary anxiety for IT professionals when it comes to cloud computing. The open cloud may not be prepared to address the security and confidentiality needs of data-sensitive organizations. As public cloud services propose server illustrations for many clients on the same hardware, the user may have very little control over where the data exists.

If a user points to machine to say that the machine has only that user's data, then there is security for the data in the cloud. Dedicated hardware is the foremost stage in cloud computing services in order to pass the most severe security strategies.

Private cloud hosting permits for the control that numerous data-sensitive organizations necessitate over their information. When it comes to security, this leads many IT professionals to implement private cloud hosting over the public cloud.

When security is concerned, knowing where the user data exists is very essential. Firewalls and interference discovery and avoidance can preserve most intruders out, and data encryption retains the data safer.

It is important to back up the data frequently when it comes to cloud computing. One of the most unnoticed features of cloud computing and one of the coolest way to rise the control of the data is to make certain that whatever happens, there is a secure backup of that data. This is more about securing the business than the actual data. There have been a number of large companies that have missed its customer's data, by not devising a backup, leaving them with nothing.

In addition to backup, the user should make certain that the data center proceeds security completely. By knowing the server and data center the data is being kept at, the user can inquire them for all related security actions that are in place. The user can see if they are SSAE 16 or SAS 70 examined, and if they have clients that are HIPAA compliant or PCI compliant. Accomplished services can also enhance a great deal of advantage and proficiency to make the applications, data, and business more strong. Services like managed firewalls, antivirus, and interference discovery are presented by respectable data center or cloud providers, and permit for improved security dealings for managed servers.

It is very essential to acquire references from other clients. When in doubt, cloud provider can be asked for client references that need strict security measures. Healthcare, insurance, Financial, or government organizations are a decent start. If other organizations that have comparable security objectives are using the provider, the user could be a good fit as well. The user should be sure to interact with these references openly when possible to understand what these companies are utilizing the cloud services for, and the stages they have reserved to protect their data.

However, the solitary method to make definite that something is secure is to examine it. It is not rare for extremely data-sensitive organizations to hire a expert ethical-hacker to check their security requirements. Vulnerability scanning and valuations are just as significant inside the cloud as they are external to the cloud. Probabilities are that if a user can discover a way to acquire unauthorized access to the user's data, someone else can as well.

Accomplishing adequate security promises in the cloud is possible but it is not definite. Just like any other IT assignment, the user has to do the homework. The private cloud hosting model can definitely offer a safer outline than the public clouds.

Important Cloud Security Issues When Moving Data to the Cloud

The profits of cloud implementation are abundant, comprising better productivity, reduced charges and better approachability and flexibility. As with other major business conclusions, an organization must assess the profits and be organized to address any risks and experiments cloud implementation brings. Transferring applications to the cloud and getting into the benefits means first assessing particular **cloud security issues.**

When organizations move applications from on-premise to cloud-based, challenges arise from data storage, industry agreement necessities, discretion, and third party requirements regarding the usage of delicate information. Corporate rules or the guidelines of the leading authorities influence the way complex data is managed with where it is positioned, what categories of data can be collected and stored and who has right to use it. These issues can define the grade to which organizations can appreciate the significance of cloud computing. Cloud security issues fall mainly into three areas:

Data Residency - Many companies experience legislation by their nation of origin or the local nation that the corporate entity is functioning in, necessitating certain categories of data to be retained within distinct geographic borders. There are precise guidelines that must be followed, focused around data access, management and control.

Data Privacy - Commercial data frequently required to be secured and protected more severely than non-sensitive information. The enterprise is in charge for any breaches to information and must be able confirm strict cloud security in order to safeguard sensitive information.

Industry & Regulation Agreement - Administrations often have rights to and are responsible for data that is extremely controlled and constrained. Many industry-specific principles such as GLBS, ITAR and PCI DSS, necessitate an enterprise to follow well-defined principles to protect reserved and business data and to fulfill with applicable laws.

Solutions for Cloud Security Concerns

New clarifications have developed for refining cloud security and shielding delicate data and vital applications. One result is the cloud encryption gateway. The gateway can assist as a proxy "entry" to a cloud application, interchanging sensitive data with encrypted or tokenized values for communication and storage in the cloud. Since the sensitive data remains under corporate control at all times, organizations can assertively make the transfer to the cloud without the related confidentiality, safety and regulatory concerns of retaining sensitive data with external cloud service providers.

Security Framework

What is an IT security framework?

An information security framework is a series of documented processes that are used to define policies and procedures around the implementation and ongoing management of information security controls in an enterprise environment. These frameworks are basically a "blueprint" for building an information security program to cope up with risk and minimize vulnerabilities. Data security pros can use these structures to describe and select the tasks necessary to construct security into an organization.

Frameworks are regularly tailored to solve particular data security complications, just like constructing proposals are tailored to meet their requisite specifications and usage. There are frameworks that were established for particular industries as well as different monitoring compliance objectives. They also come in fluctuating degrees of complication and scale. However, there is a huge amount of overlap in overall security models as each one progresses.

A business-driven methodology to security is not like a technology-centric methodology in that the commercial objectives initiate the necessities in securing the enterprise. Organizations regularly take a bottoms-up method to security as security solution vendors normally encourage this approach to their clients. To end recognized security holes, enterprises extend and strengthen their defenses by repeatedly constructing on top of or adding to their current security investments. This technology-centric method often produces an exceptionally complex and fragmented security infrastructure.

Instead of trying to defend against every possible threat, organizations should recognize and prioritize the security threat administration activities that create the greatest sense for their organization. By understanding the level of threat acceptance inside an organization, the IT teams can certainly extra focus on qualifying threats that the organization can't afford to abandon. Exaggerating certain threats leads to unused possessions and efforts, while undervaluing others can have terrible penalties.

The IBM Security Framework is intended to provide assistance to organizations to take a business driven approach the security. The IBM Security Framework sets business security concerns into 5 domains of concentration. The Security Governance, Risk Management, and Compliance component characterizes business concerns related to handling IT security. These "5+1" domains are taken together by a collective methodology to policy management, reporting and event handling.

The IBM Security Framework classifies business-driven security into a number of domains. The subsequent step is to break these down into more detail to work towards an architectural framework that can assist to outline and device the organization's goals. This architectural structure is called the IBM Security Blueprint.

The IBM Security Blueprint practices a product-agnostic and solution-agnostic approach to classify and describe security proficiencies and services that are necessary to respond the business security necessities. In the blueprint, IBM purposes to recognize **architectural principles** and a common terminology that are usable across all domains. The IBM Security Blueprint **follows IT security management from a risk management point of interpretation** and highlights appropriate IT standards.

The blueprint has been produced based on studying many customer oriented scenarios concentrating on how to construct IT solutions based on the IBM Security Framework. The purpose of the blueprint is that it can be used as a road map to help in planning and installing security solutions in the organization.

Architecture Principles

1. **Support open standards and embrace transparency**

- Support all chief platforms, run-time settings, and languages.
- Support major industry standards
- Publish interfaces and algorithms. Avoid "security by obscurity."
- Document trust and threat models.
- Support Common Principles and similar proper security validation programs.

2. **Provide security by default**

- Ship security policies "out of the box" with security enabled.
- Create reliability in the description and administration of IT configuration.
- Create a constant set of security roles in security solutions.

3. **Design for accountability**

- Record and inspect all security-relevant actions.
- Deliver accessible audit structure.
- Offer audit infrastructure that guarantees audit data is unchallengeable and dishonest.

4. **Design for regulatory reporting**

- Confirm traceability between guidelines, principles and business strategies to the security policies used to apply them.
- Support flexible reporting to house the necessities and limitations set by government principles and industry criteria.

5. **Design for privacy**

- Decrease the use of individually recognizable data whenever possible and use complication, misidentification, and accumulation when possible.
- When individually recognizable data is used, focus its use and the corresponding defenses to all stakeholders.
- Support the values of notification, choice, and contact when using individually recognizable data.

6. **Design for extensibility**

- Propose IT systems to support the split-up of management of security controls from control application to enable incorporation with alternate management systems.
- Propose systems to maintain adding and lengthening their capabilities.

7. **Design for sharing**

- Plan security management systems to incorporate several IT security domains and work with security controls using their individually set security strategies and identity simulations.
- Construction descriptions must explicitly record the expectations and restrictions made in terms of period of control.

8. **Design for consumability**

- Security services must be operable by programmers who develop and incorporate applications with security services.
- Security services must be controllable by a multiple IT security management systems.
- Security services must facilitate IT operations staff to control the contact to the security services and review their usage.

9. **Provide multiple levels of protection**

- Implement "least privilege" as a fundamental principle.
- Plan IT systems as resources that protect themselves as a first layer of defense.
- Propose security services to provide multiple layers of enforcement and detection.
- Support separation and zoning to contain interferences.

10. **Design for separate of security duties.**

- Plan security services to separate the roles of enforcement, management, and audit.

11. Design for context awareness

- Security-critical resources must be attentive to their security framework and their environment including physical location, logical co-location.

12. Use security models to create consistency.

- Implement common models and consistent formats for identity and trust, data, policy, application structure, security information and events, and cryptographic keys.
- Confirm that models are consistently interpreted across the stack (e.g., network identities are linked to application-level identities) and across units (e.g., policies and trust are negotiated and understood within a federation).
- Validate that models are consistently validated against reality.

13. Consistency in approaches, mechanisms and software components

- Decrease the number of types of security services that provide the same type of control in the IT environment.

System Management Components

The Foundational Security Management components accomplish the common Security Services and Infrastructure using a closed-loop, risk management process. This risk management method explains a way to describe all features of security controls required to address a business risk including:

- Describing the outcomes that indicate that the business risk has been mitigated.
- Transforming the business risk into one of more IT security policies.
- Outlining the security control processes needed to implement the IT security policies.
- Describing the performance indicators that need to be measured in order to determine that the control processes are functioning correctly and within desired performance goals.
- Determining the regulatory reporting requirements that must be addressed for the control.
- Defining the security and event information that needs to be collected and the compliance and performance reports that need to be produced.
- Determining a maturity model for the security controls in order to match business risk appetite to an appropriate level of IT security investment.

Business-Driven Security

Command and Control Management

This module offers the command center for security management as well as the operational security for non-IT properties; it warrants defense, reaction, steadiness, and regaining. The Command and Control Module represents the principal point of reporting and situational attentiveness in order to respond to security threats and modify IT security policy as well as to address modifications in business security policy.

Command and control management covers topics such as confirming that physical and operational security is preserved for places, properties, individuals, environment and services, providing investigation and observing of places, boundaries and regions, applying entry controls, providing for locating, tracking, and identification of persons and properties, and providing a principal point for steadiness and recovery operations.

Security Policy Management

This module provides all services and sources to author, determine, assess, alter, distribute, and evaluate IT security policies.

Risk and Compliance Assessment

This module permits the IT organization to gather, evaluate, and report security data and security measures in order to recognize, calculate, evaluate, and report on IT related risks that can contribute to the organization's operational risk.

This module includes risk aggregation and reporting, IT security risk procedures, business controls administration, resiliency and stability management, compliance reporting, and legal detection services.

Identity, Access, and Entitlement Management

This module offers services related to roles and identities, access privileges, and powers. The appropriate use of these services can confirm that access to resources has been agreed to the right individualities, at the right time, and for the right purpose. These services can also address that usage of resources is monitored and audited for unauthorized or intolerable use.

Data and Information Security Management

This module offers services that safeguard unstructured and structured information from unauthorized access and data loss, according to the business value of information. It also affords usage and access monitoring and audit services to follow the access to data.

Software, System, and Service Assurance

This module addresses how software, systems, and services are intended, established, verified, functioned, and sustained throughout the software life cycle to produce certainly secure software. This component covers planned design, threat modeling, software risk valuation, strategy assessments for security, source code assessments and investigation, active application analysis, source code control and access observing, code/package validation and confirmation, quality assurance analysis, and supplier and third-party code confirmation.

IT Service Management

This module delivers the procedure automation and work flow establishment for security administration. Specifically, Change & Release Management procedures play a substantial role in security management.

Threat and Vulnerability Management

This module facilitates to recognize vulnerabilities in installed systems and obtain reports of vulnerabilities from external sources, determine the appropriate reaction, and do proactive variations to deployed systems to retain the security of the deployed system.

Physical Asset Management

This module offers awareness of the place and status of physical properties as well as awareness of physical security control and organizes the security information for physical systems with the IT security controls.

Summary

You should be able to

- Understand what is security is
- Understand what is authentication and password
- Understand System threats
- Understand Program threats
- Understand Cloud computing

Chapter 2 – Understanding Security Risks

Learning Objectives

What this chapter is about?

- This chapter will give an overview on Understanding Security Risks

What you should be able to do?

- Overview of Security risks
- Cloud computing overview
- Benefits of Cloud computing
- Virtualization and its types Overview
- Vulnerability Overview
- How will you check your progress?

How will you check your progress?

Accountability:

- Checkpoint questions

Understanding Security Risks

Information is at menace – and the corporate data have to be protected adequately.

The corporate information can cover intellectual stuff that forms the base of the competitive benefit an organization has. It obviously comprises data such as PII (personally identifiable information) that must be secured due to legal necessities. It contains the systems and information essential to cope up with the production environment or the remotely controllable systems of clients.

There are number of security solutions existing on the market. Each of them asserts to address severe security risks. Certainly, many of them actually can, in fact, assist to progress data security. But just selecting one of these solutions is not enough.

First of all, before making a security investment, a thorough understanding of the security risks is required. Who are the prospective attackers? Which are the prospective attack targets? How possible are attacks?

And what will be the influence of effective attacks?

Understanding security risks

It is all about recognizing security risks. Risk management is a firm discipline in many companies. Conversely, many companies only emphasis on what they state as business threats, comprising planned, effective and reputational risks.

The companies ignore the point that data security risks are business risks. They can significantly destruct the status of organizations, for example when client data is leaked. They can initiate immense operational difficulties, such as production interruption, compliance drawbacks, and the charge of getting systems active and running again. Information security risks can even turn out to be tactical risks, such as the prospective for enormous damage to brand status.

Data security done properly needs that organizations ensure a security risk valuation. It also necessitates the organizational infrastructure for IT risk administration to be firmly incorporated with enterprise risk administration. There should to be obviously defined organizational roles, liabilities and duties for IT risk administration.

Identifying the biggest risks

As part of a security risk valuation, the most severe risks require to be recognized. Severity is based on the possibility and the effect. Based on such organized investigation, an action strategy for data security can be established. Within an organized risk investigation, some risks will indicate that just cannot be avoided. In that instance it is essential to have a contingency proposal that minimizes the effect.

For further risks, it is about discovering the exact balance between investments for risk reduction and the result of these investments. In fact, this is very much the similar as a judgment about insurance agreements. Security risk evaluations support businesses make well-versed judgments about where to spend on risk reduction and where to experience the risk.

The next part of such a method is about understanding how several elements of information security transmit to and incorporate with each other. First of all, security risk evaluations have done right to assist in attaining an understanding of whether a specific technology can help lessen risks at all.

For instance, if the most severe risks are for information stored in the cloud and utilized from mobile customers directly via the internet, an investment in next-generation firewalls will not assist in justifying the risks, because the data will not be permitted over the firewalls.

Understanding the strength a technology has for risk reduction thus is a compulsory step in an organized investigation of the information security package. This transfers us to the second feature organizations have to study: Point solutions are not good!

A layered security approach :

Security investments should have a higher image in mind always.

Performing a organized security risk evaluation supports in structuring such a representation of security design that is associated to the current risks. Based on that, a collection of organizational and technical activities can be defined in which the designated technologies work together to shape a layered security structure.

The worst thing that can be done is spending in point solutions in "panic mode". Such point solutions are seldom good investments. Commonly, they are concentrated on indications, not sources.

A general indication is that systems or networks are at the focus. Though, it is the information itself that requires security. Information streams and it needs to be secured at rest, in motion and in consumption. So starting with information-centric results is the most capable method, in contrast to system security and network security that can offer added value – or just fail. Defending data and the access to that data – which makes IAM (identity and access management) a fundamental component of security approaches – is the key to popular risk reduction.

Merging a well-thought out method to the complete design for information security – the big picture – with a organized method to security risk evaluations aids organizations in enhancing their IT security expenditure.

Cloud computing - Working definition

Cloud computing is an on-demand package for IT facility, frequently based on virtualization and distributed computing skills. Cloud computing architectures have:

- Extremely distracted resources
- Adjacent direct scalability and flexibility
- Near instantaneous provisioning
- Shared resources (database, hardware, memory, etc)
- 'Service on demand', usually with a 'pay as you go' billing system
- Programmatic administration (e.g., through WS API).

There are three categories of cloud computing:

- **Software as a service (SaaS):** is software presented by intermediary source, accessible on demand, commonly through remote configuration using the Internet. For instance, online worksheet tools, word processing, web content distribution services (Google Docs, Sales force CRM, etc.) and CRM services.
- **Platform as a service (PaaS):** lets consumers to create fresh applications using APIs installed and configurable from the remote location. The platforms accessible include deployment platforms, configuration management, and development tools. Examples are Force, Google App engine and Microsoft Azure.

- **Infrastructure as service (IaaS):** offers virtual machines and other distracted hardware and operating systems which may be organized through a service API. Examples include Amazon S3 and EC2, Rackspace Cloud, Windows Live SkyDrive and Terre mark Enterprise Cloud.

Clouds may also be divided into:

- **Public:** obtainable publicly – can be subscribed by any organization
- **Private:** services made according to cloud computing ideologies, but available only within a private network
- **Partner or Community:** services offered by a provider to a restricted and well-defined quantity of parties.

Top security benefits

Security and the benefits of scale: All types of security methods are inexpensive when applied on a larger scale. Hence the similar extent of investment in security purchases better defense. This comprises all types of protective measures such as patch management, filtering, hypervisors and hardening of virtual machine instances, etc. Other profits of scale contains: edge networks (content delivered or processed closer to its destination), multiple locations, to incidents, threat management, and timeliness of response.

Security as a market differentiator: security is a significant concern for many cloud clients; many of them will make purchasing selections on the basis of the reputation for privacy, reliability and flexibility and the security services provided by, a provider. This is a resilient driver for cloud providers to progress security practices.

More timely, effective and efficient updates and defaults: default virtual machine images and software components used by clients can be pre-toughened and reorganized with the most recent patches and security settings according to fine-tuned procedures; IaaS cloud service APIs also permit snapshots of virtual infrastructure to be created frequently and related with a reference point. Updates can be rolled out many times more quickly across a similar platform than in customary client-based systems that trust on the patching model.

Rapid, smart scaling of resources: the capability of the cloud provider to dynamically change resources for traffic shaping, filtering, encryption, authentication, etc, to protective measures (e.g., against DDoS attacks) has recognizable benefits for flexibility.

Benefits of resource concentration: Although the attention of resources certainly has drawbacks for security, it has the noticeable improvement of inexpensive physical parameterization and physical access control (per unit resource) and the informal and low-cost application of several security-related processes

Top security risks

Loss of governance: in cloud infrastructures, the customer certainly yields control to the Cloud Provider (CP) on an extent of issues that may upset security. At the same time, SLAs may not propose a commitment to offer such services on behalf of the cloud provider, thus leaving a hole in security defenses.

This also takes account of compliance threats, because investment in attaining certification (e.g., industry standard or monitoring necessities) may be put at risk by relocation to the cloud:

- If the CP cannot offer proof of their own compliance with the appropriate necessities
- If the CP does not authorize audit by the cloud client (CC).

In certain cases, it also means that using a public cloud infrastructure denotes that certain types of compliance cannot be accomplished (e.g., PCI DSS).

Lock-in: there is quiet few on proposal in the method of procedures, tools or typical data formats or services interfaces that might assure data, application and service transferability. This can create difficulty for the client to transfer from one provider to another or transfer data and services back to an internal IT setting. This presents a dependency on a specific CP for service facility, specifically if data compactness, as the most essential feature, is not enabled.

Isolation failure: multi-rental and shared resources are describing features of cloud computing. This risk classification includes the failure of tools separating storage, memory, routing and character between different tenants (e.g., so-called guest-hopping attacks). Yet it must be considered that attacks on resource isolation mechanisms (e.g.,. against hypervisors) are still less frequent and much more tough for an hacker to put in practice related to attacks on traditional OSs.

Management interface compromise: client management interfaces of a public cloud provider are reachable over the Internet and facilitate access to more sets of resources (than traditional hosting providers) and hence pretend an increased risk, particularly when shared with remote contact and web browser vulnerabilities.

Data protection: cloud computing poses a number of data security risks for cloud customers and providers. In several cases, it may be tough for the cloud customer (in its role as data controller) to

effectually check the data management practices of the cloud provider and thus to be definite that the data is controlled in a legal way. This difficulty is intensified in cases of numerous transfers of data, e.g., among united clouds. On the other hand, some cloud providers do offer information on their data handling practices. Some also provide certification summaries on their data handling and data security events and the data controls they have with them, e.g., SAS70 certification.

Insecure or incomplete data deletion: when an application to remove a cloud resource is given, as with utmost operating systems, this might not result in real deletion of the data. Sufficient or timely data deletion may also be difficult (or undesirable from a customer perspective), either because additional copies of data are stored but are not accessible, or as the disk to be demolished also stores data from other customers. In the case of several contracts and the recycle of hardware resources, this characterizes a complex risk to the client than with dedicated hardware.

Malicious insider: while generally less probably, the destruction which may be initiated by malicious insiders is often far better. Cloud designs demands certain roles which are exceptionally high-risk. Examples include CP system administrators and accomplished security service providers.

Customers' security expectations: the view of Security levels by Customers might distinguish from the genuine security (and availability) provided by the CP or the real inducement of the CP to decrease expenses further by sacrificing on certain security features.

Availability Chain: Belief on Internet Connectivity at Customer's side produces a Single point of disaster in several cases.

The risks registered above do not monitor a particular order of criticality; they are just ten of the utmost significant cloud computing specific risks recognized during the valuation. In terms of criticality, damage of authority is still considered the top risk related with moving to the Cloud.

The risks with Cloud computing should be related to the risks of remaining with traditional results, such as desktop-based models. To ease this, the 2009 Cloud Risk Evaluation covers estimates of comparative risks as compared with a typical traditional setting. These were also reexamined during the first review round, and in several cases explanations were added.

It is often possible, and in some cases desirable, for the cloud customer to handover risk to the cloud provider. Still not entire risks can be transferred: If a risk carries the failure to a business, severe damage to status or legal inferences, it is tough or impossible for one party to pay for this damage. Eventually, responsibility can be outsourced but the accountability can't be outsourced.

Security benefits of cloud computing

It is only just necessary to repeat one another time about the commercial, technical, architectural and environmental benefits of cloud computing. However, in the direct understanding of the members of our expert group, as well as according to latest news from the 'real world', an investigation of the security risks of cloud computing must be well-adjusted by an analysis of its explicit security benefits. Cloud computing has significant prospective to improve security and flexibility. What tracks is an explanation of the key ways in which it can donate.

Security and the benefits of scale

Basically, all kinds of security methods are inexpensive when executed on a larger scale. This includes all kinds of defensive measures such as filtering, patch management, hardening of virtual machine instances and hypervisors, human resources and their management and vetting, hardware and software redundancy, strong authentication, efficient role-based access control and federated identity management solutions by default, which also improves the network effects of collaboration among various partners involved in defense. Other benefits of scale include:

- **Multiple locations:** most cloud providers have the commercial resources to duplicate content by default in several locations. This enhances redundancy and makes the content independent from disaster and offers a disaster recovery level out-of-the-box.
- **Edge networks:** processing, storage, and delivery nearer to the network edge mean service consistency and value is improved overall and local network difficulties are less likely to have total side-effects.
- **Enhanced suitability of response to incidents:** well-track larger-scale systems, for instance due to initial discovery of new malware utilizations, can advance more operative and effective incident response skills.
- **Threat administration:** cloud providers can also afford to lease experts in allocating with particular security threats, while smaller organizations can only afford a small amount of generalists.

Risks

Risk should constantly be understood in regard to general business prospect and desire for risk – occasionally risk is compensated by chance.

- Cloud facilities are not only about convenient storage, reachable by various devices, but comprise important welfares such as additional convenient communication and prompt multi-point

collaboration. Hence, a relative study necessities to compare not only the risks of storing data in different places (on buildings vs. the cloud) but as well the risks once on premises-data kept on premises – for example, a database - is sent to other persons for their assistances by mail, against the security concerns of a database stored in the cloud and exposed to partnership between those persons. Thus, the risks of using cloud work out should be related to the risks of remaining with traditional results, such as desktop-based models.

- The level of threat will be in many cases very significantly with the category of cloud design being considered.
- It is likely for the cloud client to handover risk to the cloud provider and the risks should be measured besides the cost value received from the services. Yet *not entire risks can be moved*: if a risk leads to the commercial failure, severe loss to reputation or lawful effects, it is tough or impossible for any other party to pay for this loss.

Cloud services can be a massive money saver for industries and looks to be the forthcoming track of IT for many industries. Here are five things the user needs to be aware of before he moves the data to a cloud service.

Most of the concerns will apply to all three types of cloud services: Infrastructure as a Service, Platform as a service, and Software as a service.

Right to inspect your cloud provider - Many default deals will not offer the permission to audit the cloud services properly or in several cases at all. The user must make sure that he preserves the same auditing privileges as he would anticipate having in his own data center. The user should be sure to examine how the cloud providers control confidentiality in a multi-tenant environment where all have the equal right to audit policy. The user needs to make sure that the services are properly segmented from others so they cannot audit the user as well. He should be aware that there are no private or public principles for reviewing cloud services. The user need a trusted third party who will do this auditing for the user and allows the user to compare the security of similar cloud provider services. Until this happens the user need to fight independently to get the auditing rights he desire in our contracts.

Data Privacy Concerns - In almost all cases if the user has an IaaS or PaaS service then he should be encrypting his data at rest. Be sure the Key server is not also kept in the cloud service as this would reverse the purpose. Have the key server be at the user's corporate site or some other site not related to the cloud provider.

Cloud providers are focused to law enforcement calls, data seizure and surveillance activities that the user wouldn't normally be subjected to his own Datacenter. Harm of 4th amendment rights for US companies are also at issue. By moving data to a cloud service the user may be decreasing his protection from search of his data by law enforcement and civil complainants. A warrant with a gag order means that's that the user's cloud provider must provide his data without notifying the user they did so. Capability to protest a warrant is also negotiated because the warrant is delivered to the provider. There is no legal commitment for the cloud provider to notify their customers that data was provided because of a court instruction, etc.

Digital Forensics - Cloud services do not provide themselves well to the systematic collection of digital forensics. If the user do have a security breach, digital forensics become serious to finding out how wide the breach was. Several local and state governments now ensure "breach notification" laws on the records. In addition the healthcare hi-tech law and PCI require users to inform clients of a breach. The announcement methods occasionally vary depending on the extent of the breach. The user should be sure that the contract provides the necessary forensics skills the user will need. Chain of charge is also an issue. The user should be sure that the provider will not hamper your ability to prosecute criminals. The provider should be asked about handling of log and other important data.

Penetration Testing - Penetration testing is generally forbidden in the default agreements of cloud providers. Though, this is a requisite of PCI and best security policies. This is a trick difficult for cloud providers. On the one side they need to offer their customers with this ability but on the other side offering this to them could cause loss to their systems and other clients service if used inaccurately. Several large cloud providers, like Google and Amazon, are letting customers probe their personal equipment and services. This is a worthy step forward, but it still lacks the capacity to probe the cloud providers' setup. The user should ask for this ability on his contract.

Natural disasters and end of contract issues – the user should be sure to ask his cloud provider how they deal with the following:

- Normal Disaster clean up
- Elimination of data at agreement end. Can the user authenticate it's damage?

Cloud providers are receiving well at securely removing of the user's data at the end of the contract but the user need to ask his contract to be sure it meets his needs. Ideally, they should either actually destroy hard-drives or do a permitted Department of Defense removal procedure.

An often-unnoticed concern is how cloud providers deal with the security of the data during and after a natural tragedy. For instance, if a storm hits their datacenter and splits it separately what are their measures for protecting the data safe? In several cases the physical admission controls will be rendered

unworkable by the storm and poorest case servers could be thrown throughout the site. They must show the user a complete strategy for safeguarding the site and the data during the cleanup work.

Virtualization

Overview

The method in which one physical resource is divided into multiple virtual resources is known as as virtualization. By this a particular physical resource can be used for several purpose and achieve required actions. The benefits of Virtualization are:

- Decreases hardware cost - single server acts as multiple server
- Workload is enhanced - by dynamically sharing the resources.
- IT approachability and flexibility - It gives a single consolidated access to all the available resources.

Virtualization or system virtualization is generating many virtual systems with particular physical system. These virtual systems use virtual resources with independent operating system.

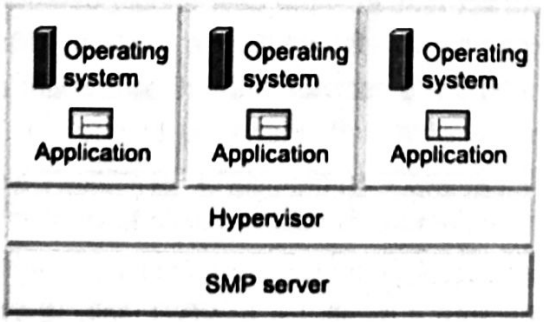
Hypervisor

A technique that permits many Operating systems to run on a single hardware at the same time, where the hardware is virtualized. This is also known as virtual machine manager.

Hypervisor types:

There are basically two type of hypervisor, type 1 and type 2 .

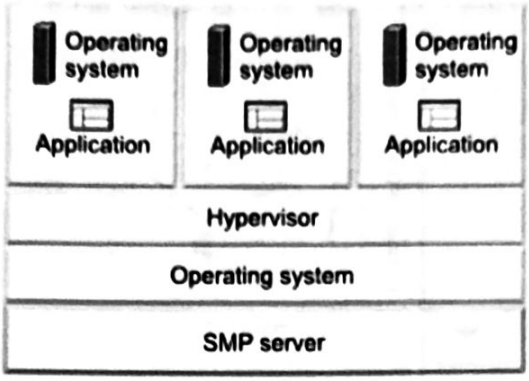
Type 1 hypervisor runs directly on the physical hardware, without out intermediate operating system. This is also called as "bare metal hypervisors".



In this case hypervisor itself is the operating system managing the hardware. This layer is more effective in comparison with the type 2 hypervisor as there is no OS system. That makes the physical resource server the need of the individual virtual machines. This hypervisor is only built to host other operating system.

Most of the enterprise operating system are type 1 operating system.

Type 2 hypervisor runs over the operating system using virtual PC or virtual box. In this case there are two layers the operating system and the hypervisor between each virtual machine.



This is more of an application which is installed over an operating system.

Hypervisor features:

Most organizations run their servers in virtual environments in their data centres. This helps them to carry their workload with high availability and better performance.

Operating system and workload can be consolidated into one server, reducing the cost of operations and hardware.

Multiple operating systems can be run on a single hardware at the same time, each running applications as per requirements.

Dynamically assigning of resources is possible from virtual resource to the physical resource through methods like dispatching and paging.

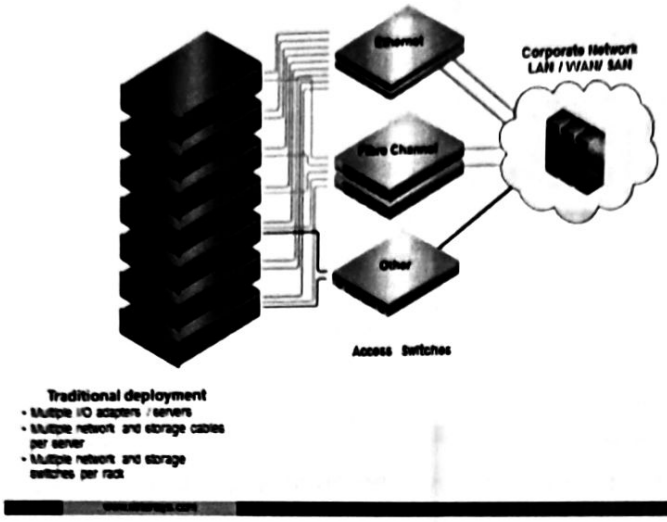
Workload is managed with ease in a single server to improve the performance, system use and price.

I/O Virtualization

Virtualizing the I/O from the server to peripherals is called I/O virtualization. Generally the devices are connected within the server using interfaces or adapter. In this method all the adapters are moved into a switching box. These adapters can be shared across different physical servers. Adapters take up lot of space in the server, once its been moved out, server space will be reduced and many servers can be accommodated in a single rack.

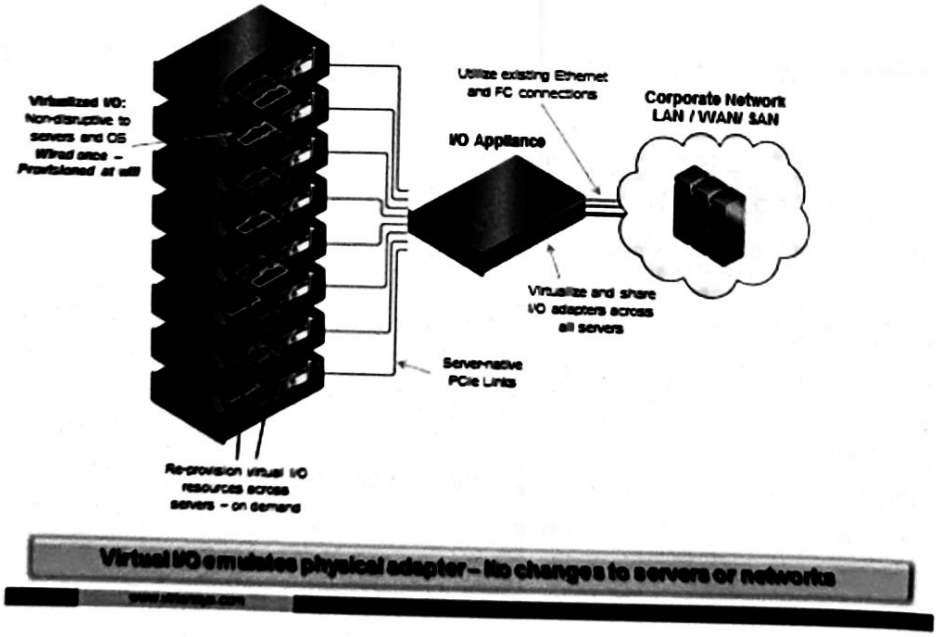
In Traditional model a single server will be having 1-4+ Ethernet cards, and these servers will be connected to SAN using fiber channels for redundancy, which requires HBA's, FC cables.

Traditional Deployment



Using I/O virtualization the SAN and network connections are consolidated on to a single High Speed cables.

Virtensys: I/O Virtualization – In action



Virtual Machines

Virtual machine is a software which emulates a physical computing environment, over which operating system and programs can be installed.

The VM are generally created within the virtualization layer like hypervisor, which runs over the operating system. The operating systems which are running in the virtual environment are not aware of the virtual platform.

Virtual machine is classified into two types:

- System Virtual machine
- Process Virtual machine

System Virtual Machine

This is also called as hardware virtualization. Where the existing architecture is emulated to suite the purpose of running the program where the real hardware is not available.

Virtual machine was mainly focused on making multiple operating systems run in a single computer allowing time-sharing over a single operating system. IBM's CP/CMS was the first system to allow full virtualization.

Process virtual machine

This is also called as application virtual machine or MRE (Managed Runtime Environment). It provides environment which is platform independent, irrespective of the hardware and the operating system.

Partitioning

This concept was originally implemented by IBM to physically divide the server into several smaller servers with dedicated resources. This gave the ability to dedicate a physical computer to a virtual machine.

Server Deployment

Server Deployment is a technology for network based installation of the operating system. The operating system deployment is necessary in the following scenarios

- In provisioning the desktops for new employees
- In redeploying the operating system of corrupt systems in order to save time and for troubleshooting
- Periodically to redeploy the operating system according to the company policies

The features of the operating system are

- **Manual Deployment:** Manual Deployment is a process in which the boot sequence of all the system needs to be manually changed to PXE (Preboot eXecution Environment) for all the new hardware which is received to install the operating system. The operating system is deployed using the image that is created. The deployment configurations is set in the deployment templates or configured manually while deploying the image.

- **Event-Driven Deployment:** Event-Driven deployment is suitable in cases where the operating system needs to be deployed to multiple systems simultaneously by controlling the bandwidth during the deployment process. The OS image is multicast to all the target computers. The time-out period can also be set by the administrators after which the deployment begins irrespective of whether the predefined number is reached or not.

- **Scheduled Deployment:** Scheduled Deployment is where the OS is deployed to multiple systems for which the MAC address is known. The deployment is scheduled by specifying the list of MAC address. The computers are powered on by the administrator using the Wake On LAN functionality and the image is deployed at the scheduled time.

- **Custom Deployment:** In the Custom Deployment process, the administrator creates a set of deployment template meeting the organization needs and assigns a name to each template and the user initiates the deployment. The custom deployment mode is set for the bootable media or the PXE package containing the set of templates. Users boot the computers from the bootable media or PXE to re-deploy their computers. The users select the template by the name from the boot menu and the deployment process starts immediately.

- **Standalone Deployment:** Standalone Deployment is a process of deployment on computers that are not a part of the network. This is performed locally using the bootable standalone utility.

Virtual Server Deployment

The system requirements for deploying the virtual server depend on the number and the type of guest operating systems, the applications to be installed on the virtual machines and the workload. Each virtual machine runs as a single processor computer irrespective of the number of processors in the physical computer. NTFS file system must be used on the host operating system as the virtual server security architecture depends on the file system security features provided by the NTFS file system. Additional disk space is required by the guest operating systems for the virtual machine paging file, dynamically expanding virtual hard disks and to save the contents of the virtual machines.

Any x86 based applications can run on a virtual machine, however the suitability of the application depends on the anticipated workload and the use of the application. The virtual server can support a maximum of 64 virtual machines, but the actual limit depends on the system resources, the quantity of memory given to each virtual machine and the total available memory on the physical computer. Virtual server supports up to 3.6 GHz of memory per virtual machine.

Deploying the virtual server consists of the following steps

- Installing IIS: The World Wide Web service component of the IIS must be installed to manage the virtual server
- Installing Virtual Server: A single physical computer can be used for both the Virtual Server service and the Administration website components or multiple computers can be used for both the services
- Adding a virtual machine: A virtual machine is added for each of the guest operating system
- Adding guest operating system: Guest operating system is added to the virtual machine which is created and performing the post setup activities on the virtual machines like running Sysprep

What is a Tenant?

The notion of a tenant in the context of cloud computing is not as simple as it might first appear. Take amazon Web Services (aWS), for example. AWS is a cloud service provider with contributions that span backup and storage, application hosting, e-commerce, and media hosting. Companies like urban Spoon, autodesk, and Second life are renters of aWS, in that they utilize aWS storage and calculate resources to power their customer contributions. Each firm also has clients who store data like personal preferences, credit cards, and data as tenant users of these businesses. In the case of Second life, for instance, if the tenants do online businesses and services of their own, they, also, will have renters and so on. In the concluding investigation, a cloud service tenant is distributing a resource among a community. And comparable to a building tenant, the tenant's space needs to be parted and isolated from other tenants to accomplish a certain grade of security and privacy.

Defining Multi-Tenancy

The knowledge of multi-tenancy, or many tenants dividing resources, is ultimate to cloud computing. Service providers are capable to build network setups and data designs that are computationally very effective, extremely scalable, and effortlessly incremented to help the customers that share them. Multi-tenancy extends the layers at which services are delivered. In IaaS, tenants share setup resources like calculate servers' hardware, and data storage devices. With SaaS, tenants are sourcing the similar application (e.g., Salesforce.com), which means that information of multiple tenants is probably stored in the same database and may even use the same tables. When security is concerned, the threats with multi-tenancy must be experienced at all layers.

Securing the Multi-Tenant Environment

Hypervisor-Based Segmentation

Virtualization is quite regularly the platform that strengthens IaaS contributions. Software, such as Citrix XenServer, VMware vSphere, and Microsoft Hyper-V, offers the means of changing a single portion of hardware into a physical host for many VMs. These virtual machines are the file servers, application servers, Web servers, and databases that include the usual physical network, and facilitate the traffic that makes commerce and communication through the Internet promising. They are also the servers presented to customers of IaaS for keeping their data or administrating their web-based businesses.

At its core, the virtualization platform includes a very specified and enhanced OS called the hypervisor, which in part aids to map traffic from VMs to the core VM host hardware so that it can create its way through the data center and available to the Internet and vice versa. The mainstream of security problems in the virtualized infrastructure relate to the co-placement of machines maintained by different customers. This provides machines in a privileged position qualified to one another. And this can raise the risk for many kinds of breaches such as illegal connection monitoring, unmonitored application login efforts, malware propagation, and various "man in the middle" attacks.

VM segmentation and segregation is also a comprehensive need for VMs including instruction and compliance focused data like employee information, customer details, etc. Most monitoring directives such as Health Insurance portability and accountability act (HIpaa), payment Card Industry data Security Standard (pCI dSS), Gramm Leach Bliley Act (glBa) and Sarbanes-oxley act (SoX) need that access be restricted to a business' requirement to know, and that control strategies be set in place to implement restricting of unnecessary access. Since the hypervisor seizes all traffic among VMs and VM hosts, it is the usual place to bring segmentation for the resources of IaaS tenants where VMs could be in the same VM host or VM host cluster.

APIs like VMware VMsafe have allowed an environment of security solutions that implant inside the hypervisor for the purpose of presenting appropriate segregation, isolation, and security of tenant resources—thus permitting safe multi-tenancy. The security solution executes as a service inside the hypervisor and captures traffic or packets. In fact, those products associating VM Introspection will also have a prodigious agreement of information about the VM's state, containing installed applications and services. Based on the vendor of the security software, the key may offer virtual network visibility to traffic, VM compliance assessment, and VM inventories, as well as malware suppression and application-based access control.

Database-Based Segmentation

Contrasting IaaS where many tenants utilize the shared resources, SaaS tenants utilize a shared database. Customers of Salesforce.com or SmugMug, for example, pay to utilize an application that controls their clients and photos respectively. However the worth is in the application interfaces that make it cool to accomplish complex responsibilities and huge data sets, the information itself is kept in a database as rows in tables that the occupants of SmugMug databases and Salesforce.com utilize.

The customer Id differentiates one row from the next row. In this extent, security issues run extraordinary that misconfigured application program or a fault in an access control list might place tenant data at possibility of theft and exploitation. For restricting access to database information, there are relatively a few utilities and technologies existing. These are typically applied in a system for validation and approval of the access demand so that certain rows or fields alone are adjustable based on security procedures that confirm that access is warranted.

Encryption of information in the database is also usual to guard it at rest, so that if it is always negotiated or taken it would be tough to decipher the basic data. Segmentation is required at all layers. The categories of multi-tenancy security used mostly rely on the cloud-based service and in what way it has been applied. Many of cloud service providers will facilitate security at all layers mostly as they will ensure all types of multi-tenancy in their settings. IaaS handlers have to realize whether their VMs are being accommodated in the same host together with those of other clients and what, if any, requirements the cloud service provider has prepared to segregate them.

In the case where the responsibility is on the tenant to design the segmentation, caution must be reserved to use proficient guidance in describing and preserving access control policies that facilitate necessary access but limit risk. SaaS tenants need to confirm that how their data stored will be protected from the hackers and how the access to their data is authenticated, authorized and distinguished so that the right people alone are managing their data.

The Part of VM Introspection in relation to the Internet and network security tools, virtualization platforms and cloud computing designs are precisely new and still developing. It is essential to be alert of improvements that may enhance security for multi-tenant settings but may not be generally recognized or implicit. It is often the situation that the principles and reference designs the users depend on for proper application delay technological progression. VM Introspection is an idea that has been for certain period in academic circles and is clarified mostly as a hypervisor-based service that inspects the internal condition of a running VM.

Technologies have just been commercialized that power VM Introspection in order to offer extraordinary stages of segmentation and isolation intended for guest VMs or cloud service tenants. VM Introspection

affords rich feature about the applications and services that are set up on the VM, as well as its structure. It is likely then to build security policies on the base of VM Introspection constraints. An instance of such a rule might be:

Do not permit a fresh virtual machine to be added in a VM group or cluster except it has a particular OS structure and hot fix installed. VM Introspection proceeds security for multi-tenancy to a new level where configuration faults are automatically not permitted. This becomes specifically significant in settings where the responsibility for constructing security and VM isolation falls on tenants, who may or may not have knowledge in this area. Automation as an Enabler While safety for multi-tenant settings may be the principal distress for implementation, security automation will be the actual facilitator for wide usage of cloud-based services. Most will approve that the tools to protect IaaS and SaaS designs are largely existing and confirmed. The actual task is that the tenants aren't aware on which kind of planning they are using and what is their part and charge for guarding their data.

Cloud service providers may device the technologies, but may not completely control how they are managed and designed, as in the situation where tenants themselves have sub-tenants. The key to safeguarding multi-tenancy is for any person who is a tenant to query the cloud provider about current securities and duties for describing and preserving policies that confirm separation from other cloud tenants. Similarly key is to query the extent of the process is automated. Cloud computing settings, specifically those built on virtualization, are exceptionally vibrant. Change is constant, and this makes the possibility of resource and security misconfiguration extraordinary. With existing technologies that automate VM protection (at least for IaaS), there is no purpose to experience the advanced threat, particularly given the extent of current and projected cloud service and provider options.

Cloud computing security concerns mark it challenging to verbalize a well-founded valuation of the definite security effect for two crucial reasons. First, elementary terminology - comprising *threat*, risk, and *vulnerability* - are repeatedly used interchangeably, without concern to their respective explanations. Second, not each concern raised is explicit to cloud computing.

To accomplish a well-founded considerate of the "delta" that cloud computing enhances with respect to security concerns, the user must investigate how cloud computing effects established security problems. A important feature at this point is security *vulnerabilities*: cloud computing creates certain well-agreed vulnerabilities more important as well as adds new ones to the combination. However, the user must first found what "vulnerability" actually is.

Vulnerability: An Overview

Vulnerability is a noticeable feature of risk. ISO 27005 outlines risk as "the prospective that a given risk will abuse vulnerabilities of an asset or group of assets and thereby create damage to the organization,"

determining it in terms of both the possibility of an event and its consequence. The Open Group's risk taxonomy offers a beneficial summary of risk factors.

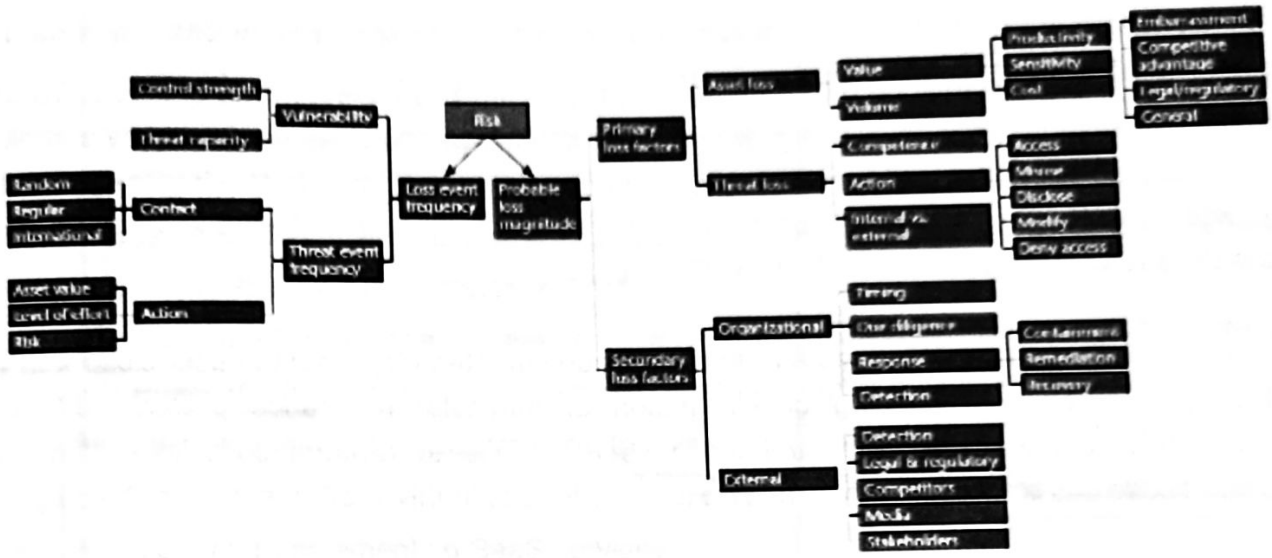


Figure 1. Features contributing to risk according to the Open Group's risk taxonomy. Risk related to the product of loss event frequency (left) and likely loss magnitude (right). Vulnerabilities affect the loss event frequency.

The Open Group's taxonomy uses the same two top-level risk factors as ISO 27005: the likelihood of a harmful event (here, *loss event frequency*) and its consequence (here, *probable loss magnitude*). The probable loss magnitude's sub factors (on the right in Figure 1) influence a harmful event's ultimate cost. The loss event frequency sub factors (on the left) are a bit more complicated. A loss event happens when a threat agent (such as a hacker) effectively abuses vulnerability. The regularity with which this occurs is influenced by on two factors:

- The regularity through which threat agents attempt to exploit vulnerability. This frequency is defined by both the agents' enthusiasm (What can they achieve with an attack? How much power does it take? What is the possibility for the attackers?) And how much access ("contact") the agents have to the outbreak targets.
- The dissimilarity between the threat agents' attack capabilities and the system's power to fight the attack.

This second factor conveys us toward a valuable definition of vulnerability.

Defining Vulnerability

Based on the Open Group's risk taxonomy,

"Vulnerability is the possibility that an asset will be incapable to fight the activities of a threat agent. Vulnerability occurs when there is a change between the power being applied by the threat agent, and an object's capability to resist that force."

So, vulnerability must constantly be defined in terms of resistance to a certain kind of attack. To deliver a real-world example, a car's failure to safeguard its driver against wound when hit directly by a truck driving 60 mph is a vulnerability; the resistance of the car's crumple zone is merely too fragile matched to the truck's power. Besides the "attack" of a motorcyclist, or even a small car driving at an extra moderate speed, the car's resistance power is perfectly sufficient.

Computer vulnerability can be described as - that is, security-related bugs that the user close with vendor-provided patches - as a weakening or elimination of particular resistance power. Buffer-overflow vulnerability, for instance, deteriorates the system's resistance to random code execution. Whether attackers can abuse this vulnerability depends on their skills.

Vulnerabilities and Cloud Risk

Now observe how cloud computing effects the risk factors in Figure 1, beginning with the right-hand side of the risk factor tree.

From a cloud client view, the right-hand side dealing with feasible magnitude of forthcoming loss isn't altered at all by cloud computing: the consequences and crucial cost of a privacy breach, is accurately the same irrespective of whether the data breach happened inside a cloud or a conventional IT setup. For a cloud service provider, things look slightly different: as cloud computing systems were formerly detached on the same infrastructure, a loss event could involve a considerably bigger effect. But this statement is easily grasped and integrated into a risk valuation: no theoretical work for adapting effect analysis to cloud computing seems essential.

So, Figure 1's left-hand side must be searched for changes - the loss event frequency. Cloud computing could modify the possibility of a damaging event's occurrence. Cloud computing sources important alterations in the vulnerability feature. Obviously, shifting to a cloud infrastructure might modify the attackers' access level and urge, as well as the work and risk - a point that must be measured as forthcoming work. But, for assisting a cloud-specific risk evaluation, it appears most cost-effective to start by investigating the appropriate nature of cloud-specific vulnerabilities.

Cloud Computing

Basically, cloud computing gathers recognized technologies (such as virtualization) in resourceful ways to offer IT services "from the conveyor belt" using economies of scale. Now look closer at what the essential technologies are and which features of their use in cloud computing is important.

Core Cloud Computing Technologies

Cloud computing builds comprehensively on skills available through some core technologies:

- ***Web applications and services.*** Software as a service (SaaS) and platform as a service (PaaS) are unimaginable without Web application and Web services technologies: SaaS offerings are normally implemented as Web applications, while PaaS offerings offer development and runtime environments for Web applications and services. For infrastructure as a service (IaaS) offerings, administrators normally device associated services and APIs, such as the administrative access for clients, using Web application/service technologies.
- ***Virtualization IaaS offerings.*** These tools have virtualization techniques at their very heart; because PaaS and SaaS services are typically made on top of a associate IaaS infrastructure, the significance of virtualization also prolongs to these service models. In the future, virtualization is expected to progress from virtualized servers to computational resources that can be used extra enthusiastically for implementing SaaS services.
- ***Cryptography.*** Many cloud computing security requirements are resolvable merely by means of cryptographic techniques.

As cloud computing advances the list of core technologies is possible to increase.

Essential Characteristics

In its account of necessary cloud features, the US National Institute of Standards and Technology (NIST) captures fine what it means to offer IT services from the conveyor belt using economies of scale:

- ***On-demand self-service.*** Users can order and manage services without human interaction with the service provider, using, for example, a Web portal and management interface. Provisioning and de-provisioning of services and associated resources occur automatically at the provider.
- ***Global network access.*** The Cloud services can be retrieved through the network (commonly the Internet), with the help of standard mechanisms and protocols.
- ***Resource pooling.*** Computing resources used to offer the cloud service are understood using a homogeneous setup that's shared among all service users.
- ***Rapid elasticity.*** Resources can be adjusted up and down quickly and elastically.
- ***Measured service.*** Resource/service usage is continuously metered, associating optimization of resource usage, usage journalized to the customer, and pay-as-you-go business models.

NIST's characterization context for cloud computing with its list of vital features has by now progressed into the de facto standard for describing cloud computing.

Cloud-Specific Vulnerabilities

According to the intellectual view of cloud computing offered before, now move to a definition of what organizes a cloud-specific vulnerability. A vulnerability is cloud specific if it

- is essential to or predominant in a core cloud computing technology,
- has its main reason in one of NIST's important cloud features,
- is affected when cloud improvements make tried-and-tested security controls demanding or difficult to implement, or
- is predominant in recognized state-of-the-art cloud contributions.

Core-Technology Vulnerabilities

Cloud computing's core technologies - virtualization, Web applications and services, and cryptography - have vulnerabilities that are either fundamental to the technology or predominant in the technology's state-of-the-art applications. Three instances of such vulnerabilities are session riding and hijacking, insecure or obsolete cryptography, and virtual machine escape.

First, the probability that an attacker might successfully escape from a virtualized setting lies in virtualization's very common. Hence, consider this vulnerability as fundamental to virtualization and extremely appropriate to cloud computing.

Second, Web application technologies must solve the problem that, by plan, the HTTP protocol is a stateless protocol, while Web applications need some idea of session status. Several techniques use session handling and - as any security professional experienced in Web application security will confirm - many session handling implementations are weak to session riding and session hijacking. Whether session riding/hijacking vulnerabilities are essential to Web application technologies or are "only" predominant in many current executions is questionable; in any case, such vulnerabilities are surely appropriate for cloud computing.

Finally, cryptanalysis progress can extract any cryptographic appliance or algorithm doubtful as novel approaches of breaking them are revealed. It's even more common to discover important errors in cryptographic algorithm implementations, which can make strong encryption into weak encryption (or sometimes no encryption at all). Since comprehensive agreement of cloud computing is impossible without the usage of cryptography to shield data privacy and reliability in the cloud, doubtful or outdated cryptography vulnerabilities are extremely important for cloud computing.

Essential Cloud Characteristic Vulnerabilities

NIST defines five necessary cloud characteristics: on-demand self-service, ubiquitous network access, resource pooling, rapid elasticity, and measured service.

Following are samples of vulnerabilities with core reasons in one or more of these characteristics:

- ***Illegitimate access to management interface.*** The cloud characteristic on-demand self-service needs a controlling interface that's reachable to cloud service users. Illegal access to the management edge is therefore a explicitly suitable vulnerability for cloud systems: the possibility that unauthorized access could occur is much higher than for traditional systems where the management functionality is accessible only to a few administrators.
- ***Internet protocol vulnerabilities.*** The cloud characteristic universal network access means that cloud services are accessed through network with standard protocols. In most cases, this network is the Internet, which must not be considered as trusted. Internet protocol vulnerabilities - such as vulnerabilities that permit man-in-the-middle attacks - are thus appropriate for cloud computing.
- ***Data recovery vulnerability.*** The cloud characteristics of pooling and elasticity demand that resources assigned to one user will be reassigned to a different user in the future. For memory or storage resources, it might therefore be likely to recover data stored by a previous user.
- ***Metering and billing avoidance.*** The cloud characteristic of measured service means that any cloud service has a metering skill at a conceptual level appropriate to the service type (such as active user accounts, storage, and processing). Metering data is used to enhance service delivery as well as billing. Applicable vulnerabilities comprises of metering and billing data manipulation and billing avoidance.

Thus, NIST's well-founded definition of cloud computing can be influenced in reasoning about cloud computing issues.

Defects in Known Security Controls

Vulnerabilities in standard security controls must be measured cloud specific if cloud discoveries directly cause the problems in applying the controls. Such vulnerabilities are also called as *control challenges*.

Here, three examples of such control challenges can be treated. First, virtualized networks deal inadequate network-based controls. Specified the nature of cloud services, the managerial access to IaaS network setup and the capacity to modify network setup are typically restricted; therefore, typical controls such as IP-based network zoning can't be applied. Similarly, standard techniques like network-based vulnerability

scanning are typically prohibited by IaaS providers because, for instance, friendly probes can't be distinguished from attacker action. Finally, skills such as virtualization mean that network traffic happens on equally real and virtual networks, such as while two virtual machine environments (VMEs) held on the same server communicates. Such problems organize a control challenge because tried and tested network-level security controls might not work in a given cloud environment.

The second task is in reduced key management techniques. As well-known in a latest study in European Network and Information Security Agency, cloud computing setups need administration and storage of many different types of keys. Since fixed hardware structure is does not required by virtual machines and cloud-based content is frequently distribute across the world, it's tougher to implement standard controls to keys on cloud setups - such as hardware security module (HSM) storage.

To end with, security metrics aren't altered to cloud structures. Now, there are no consistent cloud-specific security metrics that cloud customers can use to observe the security position of their cloud resources. Till such standard security metrics are developed and executed, controls for security assessment, inspection, and liability are more problematic and expensive, and might even be difficult to employ.

Prevalent Vulnerabilities in State-of-the-Art Cloud Offerings

Though cloud computing is reasonably new, there are already numerous cloud offerings on the market. Hence, the users can balance the three cloud-specific vulnerability pointers offered before with an onward, realistic indicator: if vulnerability is predominant in state-of-the-art cloud offerings, it must be considered as cloud-specific. Examples of such vulnerabilities comprise weak authentication schemes and injection vulnerabilities.

Injection vulnerabilities are abused by manipulating service or application inputs to understand and execute parts of them besides the programmer's intentions. Instances of injection vulnerabilities comprise

- SQL injection, in which the input comprises SQL code that's mistakenly executed in the database back end;
- command injection, in which the input holds commands that are mistakenly executed through the OS; and
- Cross-site scripting, in which the input encloses JavaScript code that's incorrectly executed by a victim's browser.

In addition, numerous broadly used authentication mechanisms are fragile. For example, usernames and passwords for authentication are fragile due to

- anxious user performance (choosing weak passwords, reusing passwords, and so on), and

- Characteristic restrictions of one-factor authentication mechanisms.

Also, the authentication mechanisms' implementation might have flaws and allow, for instance, credential interference and repetition. The major Web applications in existing state-of-the-art cloud services use usernames and passwords as authentication mechanism.

Architectural Components and Vulnerabilities

Cloud service simulations are generally divided into SaaS, PaaS, and IaaS, and every model effects the vulnerabilities unveiled by a given cloud setup. Its support to add more configuration to the service model loads: Figure 2 shows a cloud reference architecture that creates the most significant security-relevant cloud components obvious and affords an abstract overview of cloud computing for security issue analysis.

Internal Security Breaches

Moving to the cloud has clear benefits for any organization, but hiring the business's delicate data in the hands of third party providers also increases and complicates the risk scenario with which the user must struggle. Cyber convicts are currently aiming at any enterprise where they can catch data to resell interrupt or abuse.

1. Understand what the user can't afford to lose

Data breaches, according to the Cloud Security Alliance, are the highest cloud computing security risk for 2013 and further, and for decent purpose: delicate data can be of huge value. To figure out how abundant a concern this is to the enterprise, consider what sensitive data stored in the cloud. Some of the most targeted categories of information are:

- Personally Identifiable Information (PII), like full names, birth dates, telephone numbers, addresses, drivers' license and national identification numbers, some IP addresses, and online logins and passwords—whatever a hacker can use to figure out or take someone's identity.
- Sensitive financial data, like bank account and PIN numbers, credit card numbers, and whatsoever an illegitimate can use to contact accounts and funds.
- Confidential corporate information, comprising anything a competitor's usage to achieve a competitive advantage. Consider the corporate financials, internal communications, HR resources, R&D documentation, strategic plans, and, in various fields as well.

The essential consideration here is: What does the company have that others might want?

Working hand-in-hand with this concern is another: What does the company have that it can't afford to lose? Data privacy guidelines often claim public breach warnings in the occasion of a mischievous data

breach or unintentional data loss. If your cloud computing security policy is unsuccessful in protecting the data, the enterprise could face serious consequences in terms of business and status lost as a consequence of the notification.

For that purpose, it's necessary to lock down any sensitive data the user hold. In addition to comprehensive DLP measures, Cipher Cloud's resilient encryption and key management is planned to defend against breaches. In many jurisdictions, the release of accurately encrypted data to which the enterprise holds the key is not deliberated a breach and does not need public announcement.

2. Understand what can protect you if you do lose your data

Safe harbor laws create key management specifically critical. Beneath several jurisdictions' safe harbor laws, a breach is not taken as a true breach—and does not need public warning—if the enterprise still maintains control of the encryption keys.

And breaches do occur, in numerous cases for reasons exterior of enterprises' direct control. Even when the data is secure in the cloud, all it takes is one insider who has contact to the encryption keys—and shouldn't—to outcome in an undesirable disclosure. The bigger the number of CSP insiders with accesses to the data, the bigger the risk to the cloud computing security. When the enterprise preserves special control of the encryption keys, the users eliminate that concern.

Even the systems the enterprise and their CSPs may have in place to avoid accidental removal of the data can pose threats to the enterprise's data confidentiality. Redundancy, Backups, and other failover strategies may safeguard against data loss due to removal or system failures, but generate extra chances for the robbery of the data considered vital. And what happens to the data if the user chooses to terminate the services with a particular CSP? The user can never be certain that the data has been digitally demolished. Again, an encryption code that runs for limited, organized, enterprise-special encryption key access is key for defending the data, no matter where it located or how many replicas of it exist.

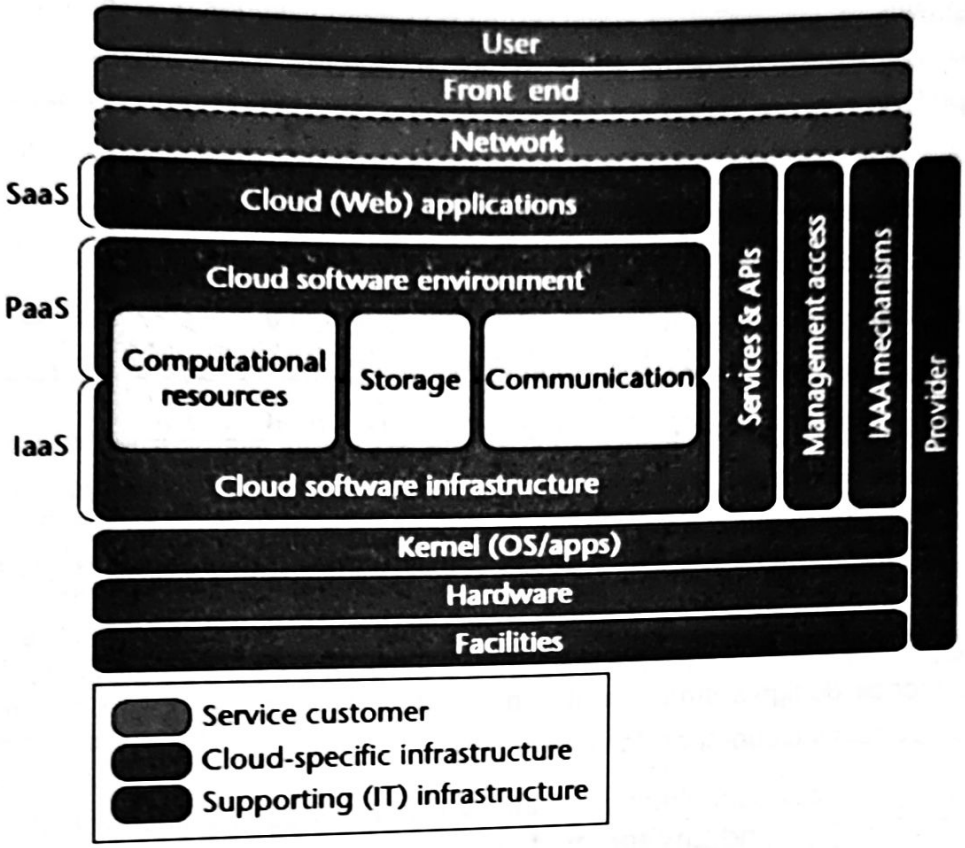


Figure 2. The cloud reference architecture. cloud-specific vulnerabilities may be mapped to modules of this reference design, which gives an outline of which vulnerabilities might be significant for a given cloud service.

The reference design is based on work done at the University of California, Los Angeles, and IBM. It succeeds to the layered method in that layers can include one or more service modules. Here, "service" is used in the broad sense of providing a little that might be both material (such as power, shelter, and hardware) and immaterial (such as a runtime environment). For two layers, the cloud software setting and the cloud software infrastructure, the model creates the layers' three main service constituents - storage, computation, and communication - obvious. Top layer services also can be applied on layers further down the stack, in effect avoiding midway layers. For example, a cloud Web application can be applied and worked in the traditional way - that is, running on top of a standard OS without using dedicated cloud software setup and environment constituents. Layering and compositionality suggest that the changeover from providing some facility or function in-house to sourcing the service or function can take place among any of the model's layers.

In addition to the original model, it has been recognized supporting utilities significant to services in several layers and added them to the model as vertical durations over several horizontal layers.

Our cloud reference design has three chief parts:

- ***Supporting (IT) structure.*** These are facilities and services public to any IT service, cloud or other-wise. It includes them in the design because it needs to deliver the entire picture; a full dealing of IT security must account for a cloud service's non-cloud-specific components.
- ***Cloud-specific infrastructure.*** These components are the heart of a cloud service; cloud-specific vulnerabilities and equivalent controls are typically mapped to these constituents.
- ***Cloud service consumer.*** Again, the cloud service customer include in the reference architecture because it's relevant to an all-encompassing security treatment.

Also, it has been made obvious the network that splits the cloud service customer from the cloud infrastructure; the fact that contact the cloud resources is carried out through a (commonly untrusted) network is one of cloud computing's main features.

Using the cloud reference design's structure, it can now run through the design's components and give samples of each component's cloud-specific vulnerabilities.

Cloud Software Infrastructure and Environment

The *cloud software infrastructure* layer offers an abstraction level for basic IT resources that are accessible as services to higher layers: computational resources (usually VMEs), storage, and (network) communication. These services can be used separately, as is usually the case with storage services, but they are often bundled such that servers are conveyed with certain network connectivity and contact to storage. This bundle, with or without storage, is usually denoted as IaaS.

The *cloud software environment* layer delivers services at the application platform level:

- a development and runtime setting for services and applications developed in one or more supported languages;
- storage services (a database edge rather than file share); and
- Communication setup, such as Microsoft's Azure service bus.

Vulnerabilities in both the infrastructure and environment layers are generally particular to one of the three resource types delivered by these two layers. However, cross-tenant contact vulnerabilities are related for all three resource types. The virtual machine escape vulnerability is a prime sample. It has been used to show a vulnerability that's inherent to the core virtualization technology, but it can also be understood as having its root cause in the crucial characteristic of resource pooling: whenever resources are assembled, unauthorized contact across resources becomes a problem. Later, for PaaS, where the technology to

distinct different tenants isn't essentially based on virtualization, cross-tenant access vulnerabilities play a vital role as well. Likewise, cloud storage is liable to to cross-tenant storage access, and cloud communication - in the method of virtual networking - is liable to to cross-tenant network access.

Computational Resources

An extremely significant set of computational resource vulnerabilities concerns how to handle the virtual machine images: the only possible way of providing closely matching server images - thus offering on-demand service for virtual servers - is by replicating template images.

Vulnerable virtual machine template images affect OS or application vulnerabilities to extend over many systems. An attacker might be capable to examine patch level, configuration, and code in detail using administrative privileges by leasing a virtual server as a service customer and thereby attaining cognizance helpful in attacking other customers' images. An associated problem is that an image can be taken from an unreliable source, a new phenomenon carried on specifically by the developing marketplace of virtual images for IaaS services. In this situation, an image might, for instance, have been manipulated so as to deliver back-door access for an attacker.

Data leakage by virtual machine duplication is a vulnerability that's also rooted in the use of cloning for providing on-demand service. Cloning leads to data leakage difficulties regarding machine secrets: some elements of an OS - such as cryptographic salt values and host keys - are expected to be private to a single host. Cloning can disturb this privacy statement. Again, the emerging market for virtual machine images, as in Amazon EC2, points to an associated problem: users can offer template images for other users by turning a running image into a template. Depending on how the image was used previously before producing a template from it, it might hold data that the user doesn't desire to make public.

There is also control challenges including those linked to cryptography routine. Cryptographic vulnerabilities due to delicate random number generation might occur if the abstraction layer between the hardware and OS kernel presented by virtualization is difficult for generating random numbers within a VME. Such generation needs an entropy source on the hardware level. Virtualization might have defective mechanisms for tapping that entropy source, or having some VMEs on the same host might drain the available entropy, resulting in weak random number generation. As noted earlier, this abstraction layer also complicates the use of advanced security controls, like hardware security modules, probably resulting in poor key management procedures.

Storage

Along with data recovery vulnerability due to resource pooling and elasticity, there's a associated control challenge in media purification, which is often tough or difficult to implement in a cloud context. For exam-

ple, data destruction policies relevant at the end of a life cycle that need physical disk destruction can't be supported if a disk is still being used by another tenant.

Because cryptography is often used to overcome storage-related vulnerabilities, this core technology's vulnerabilities - anxious or obsolete cryptography and poor key management - play a special role for cloud storage.

Communication

The most noticeable specimen of a cloud communications service is the networking delivered for VMEs in an IaaS environment. Because of resource pooling, some customers are possible to share certain network infrastructure components: vulnerabilities of common network infrastructure components, such as vulnerabilities in a DHCP, DNS server, and IP protocol vulnerabilities, might support network-based cross-tenant attacks in an IaaS infrastructure.

Virtualized networking also provides a control challenge: once more, in cloud services, the administrative access to IaaS network infrastructure and the probability for tailoring network infrastructure are typically restricted. Also, using technologies such as virtualization points to a position where network traffic happens not only on "real" networks but also inside virtualized networks (like for communication among two VMEs accommodated on the same server); most implementations of virtual networking deal limited possibilities for incorporating network-based security. On the whole, this organizes a control challenge of inadequate network-based controls because tried-and-tested network-level security controls might not work in a given cloud environment.

Cloud Web Applications

A Web application will use browser technology as the front end for user interaction. With the improved up-take of browser-based computing technologies such as Java, JavaScript, Silverlight, and Flash, a Web cloud application divides into two parts:

- an application component operated someplace in the cloud, and
- a browser component executing within the user's browser.

In the future, developers will progressively use technologies like Google Gears to allow offline usage of a Web application's browser module for use cases that don't need continuous access to distant data. It has been already designated two classic vulnerabilities for Web application technologies: injection vulnerabilities and session riding and hijacking vulnerabilities.

Extra Web-application-specific vulnerabilities concern the browser's front-end module. Among them are

client-side data manipulation vulnerabilities, in which users round up Web applications by manipulating data directed from their application module to the server's application module. In other words, the input expected by the server component isn't the "expected" input received by the client-side component, but changed or completely user-generated input. Furthermore, Web applications also depend on browser mechanisms for separating third-party content implanted in the application (like advertisements, mash up components, and so on). Browser isolation vulnerabilities could therefore permit third-party content to operate the Web application.

Services and APIs

It might appear clear that all layers of the cloud infrastructure propose services, but for observing cloud infrastructure security, it's valuable to clearly consider about all of the infrastructure's service and application programming interfaces. Most services are probably Web services, which share considerably vulnerability with Web applications. Certainly, the Web application layer might be recognized entirely by one or more Web services such that the application URL would only provide the user a browser component. Thus the API functions and supporting services share abundant vulnerability with the Web applications layer.

Management Access

NIST's description of cloud computing states that one of cloud services' vital features is that they can be promptly provisioned and released with least management strength or service provider communication. Consequently, a common component of each cloud service is a management interface - which points directly to the vulnerability regarding unauthorized access to the management interface. Additionally, because management contact is often recognized using a Web application or service, it regularly shares the vulnerabilities of the Web application layer and services/API component.

Identity, Authentication, Authorization, and Auditing Mechanisms

All cloud services (and each cloud service's administration interface) need mechanisms for authentication, identity management, authorization, and auditing (IAAA). To a certain point, portions of these mechanisms might be factored out as a stand-alone IAAA service to be used by other services. Two IAAA components that must be part of each service application are performance of sufficient authorization checks (which, obviously, use authentication and/or authorization data received from an IAAA service) and cloud infrastructure auditing.

Most vulnerability related with the IAAA module must be considered as cloud-specific because they are predominant in state-of-the-art cloud offerings. Earlier, the example of weak user authentication mechanisms were given; other samples comprise of

- ***Denial of service by account lockout.*** One often-used security control - especially for authentication with username and password - is to lock out accounts that have received some unsuccessful authentication efforts in quick succession. Attackers can use such efforts to introduce DoS attacks against a user.
- ***Weak credential-reset mechanisms.*** When cloud computing providers cope up the user credentials themselves rather than using united authentication, they must offer a mechanism for changing credentials in the situation of forgotten or lost credentials. Earlier, password-recovery mechanisms have recognized mainly weak.
- ***Insufficient or faulty authorization checks.*** High-tech Web application and service cloud offerings are regularly vulnerable to inadequate or defective authorization checks that can create unauthorized data or actions available to users. Missing authorization checks, for instance, are the source of URL-guessing attacks. In such attacks, users alter URLs to exhibit information of other user accounts.
- ***Coarse authorization control.*** Cloud services' management interfaces are mainly prone to providing authorization control models that are too rough. Thus, standard security actions, such as duty separation, can't be executed because it's difficult to provide users with only those rights they strictly need to carry out their work.
- ***Insufficient logging and monitoring possibilities***. Currently, no standards or mechanisms occur to provide cloud customers logging and monitoring services within cloud resources. This result in a serious problem: log files record all tenant events and can't easily be trimmed for a particular tenant. Also, the provider's security monitoring is frequently disturbed by insufficient monitoring capabilities. Until usable logging and monitoring standards and facilities are developed and implemented, it's difficult - if not impossible - to implement security controls that require logging and monitoring.

Among these IAAA vulnerabilities, in the experience of cloud service providers, now, authentication issues are the main vulnerability that places user data in cloud services at risk.

Provider

Vulnerabilities that are appropriate for all cloud computing mechanisms normally concern the provider - or rather users' inability to control cloud setup as they do their private infrastructure. Among the control challenges are inadequate security audit possibilities, and the point that certification schemes and security metrics aren't implemented to cloud computing. Additionally, standard security controls concerning certification, audit, and constant security monitoring can't be employed effectively.

Cloud computing is in continuous development; as the field develops, added cloud-specific vulnerabilities indeed will emerge, whereas others will come to be less of an issue. Using an accurate definition of what organizes vulnerability from the Open Group's risk taxonomy and the four indicators of cloud-specific vulnerabilities are identified here deals a precision and clarity level frequently lacking in current discourse about cloud computing security.

Control challenges normally highlight situations wherein otherwise successful security controls are ineffective in a cloud setting. Therefore, these challenges are of special attention for further cloud computing security research. Certainly, many recent efforts - such as the development of certification schemes and security metrics, and the move headed for full-featured virtualized network mechanisms - directly address control challenges by facilitating the use of such tried-and-tested controls for cloud computing.

Cloud storage can be a smart means of outsourcing the day-to-day administration of data, but eventually the charge and responsibility for that data falls on the company that possesses the data, not the hosting provider. With this in mind, it is significant to understand some of the sources of data corruption, how much concern a cloud service provider holds, some simple best practices for using cloud storage safely, and some approaches and values for monitoring the integrity of data irrespective of whether that data resides locally or in the cloud.

Data Corruption

Integrity monitoring is crucial in cloud storage for the same causes that data reliability is critical for any data center. Data corruption can occur at any level of storage and with every type of media. Bit rot (the weakening or damage of bits of information on storage media), deduplication metadata corruption, controller failures, and tape failures are all samples of different media types triggering corruption. Metadata corruption can be the consequence of any of the vulnerabilities, for example bit rot, but are also liable to software glitches external of hardware error rates. Regrettably, a side effect of deduplication is that a corrupted file, block, or byte disturbs every related piece of data tied to that metadata. The fact is that data corruption can occur anywhere inside a storage environment. Data can become corrupted just by migrating it to an alternate platform, i.e., transferring the data to the cloud. Cloud storage systems are the data centers, with hardware and software, and are exposed to data corruption. Many companies undergo from prolonged downtime, but 0.07 percent of their clients actually lost data.

At any time data is lost, specifically valuable data, there is a tendency to scramble to allot fault. Regularly in the IT world, this can effect in lost company revenue, lost jobs, and, in severe circumstances, business end. Intrinsically, it is serious to understand how much legal concern the cloud service provider, for each service level agreement (SLA), has and to confirm that every likely step has been taken to avoid data loss. As with several legal documents, SLAs are often written to the profit of the provider, not to the consumer.

Many cloud service providers' compromise varying tiers of security, but as with any storage provider they do not accept responsibility for the reliability of your data.

There are some best practices that will permit a company to take advantage of the flexibility and convenience of the cloud, without placing its data at risk. The idea of data protection is to distribute the risk so that the possibility of data loss is decreased. Even when storing data in the cloud, it makes logic to preserve a primary copy and a backup copy of the data onsite so that access to the data is not dependent upon network performance or connectivity. By observing these basic best practices and knowing the details of the cloud provider's SLA, the building blocks are in place to apply a technique for proactively observing the integrity of data irrespective of the storage platform or location.

One method for validating the integrity of a set of data is based on hash values. A hash value is derived by reducing a set of data into a single unique value by method of a pre-defined algorithm. Since the hash value is resultant of the original data itself, if the two hash values are not equal, it is an pointer that at least one of the two copies has been either changed or corrupted.

Make sure that the cloud provider offers the ability to check the hash value of the data and equate it to the hash value of a second copy of data, irrespective of where that copy is stored. Using this level of data monitoring manually would be beyond clumsy. Luckily, other approaches are available, including programmatic checks. The other members of the Active Archive Alliance and Spectra Logic provide tools that will spontaneously observe the integrity of the data among their systems.

While an active archive is one technique of monitoring data integrity, there remains a serious requisite for a broadly adopted cloud standard protocol that supports integrity monitoring and interoperability. Since not all data centers have similar equipment, nor are they essentially similar to the cloud hosting setup, interoperability between different storage devices are essential. The Cloud Data Management Interface (CDMI) standard was put forward in 2010 by the Storage Networking Industry Association (SNIA). A CDMI-compliant system can demand another CDMI compliant system for the hash value of an object, thus validating that the two copies of data are still alike. By observing the integrity of the primary copy of data with a backup copy, a company can now confirm that the copy of data stored in the cloud has not been tainted. How often these data sets necessity to be monitored can be determined by the value of the data. Industry standards, like CDMI, not only certify interoperability between compliant heterogeneous systems, but also deliver a convenient mechanism for data integrity monitoring.

It's tough to dispute that the cloud industry has taken a few punches in the media freshly, specifically with large vendors like Iron Mountain stopping their basic cloud storage services However, the moral of this section isn't that the cloud is a risky storage platform, but rather that when examining and applying cloud strategies, there are more features to consider than simply cost per gigabyte stored. Cloud storage

provides several benefits to companies of any size when appropriately implemented. The cloud doesn't remove the requirement for intelligent data management approaches. Irrespective of the data storage, it is completely essential to make sure it will be reachable and restorable when required. This declaration is at the very near of data integrity monitoring and verification.

User account and Server Hijacking

1. Data Breaches

Data breaches are one of the top threats to cloud computing. All the computer systems attached to the Internet can be used by virtually any person. This brings cloud computing service providers to the risk of expert hackers with malicious targets. In 2012 the number of stated cases of server breaches was above 200 and they resulted in the damage of about 9 million data records. More and more breaches are predictable as the amount of national underground hacking communities stays to develop.

2. Data Loss

One more serious risk stems from cloud computing service providers' potential failure to avoid data loss. In our updated world, most people recognize that loss of data is unavoidable at one point or another. Though, this risk is multiplied by the absolute quantity of data handled by cloud computing service providers. There is accumulative amount of delicate data conveyed to cloud computing firms and this data could get misplaced in any number of ways, including through accidental corruption or deletion.

3. Account Hijacking

Another potentially serious risk at cloud computing companies is hijacking of accounts. It is commonly possible for authorized company employees to remotely contact cloud data via remote computers or mobile devices.

4. Insecure application programming interfaces (APIs)

Insecure application programming interfaces (APIs) are one more threat to cloud computing. These interfaces provide methods for programs to connect with each other and their safety is not always absolutely guaranteed. The ambiguities in security might allow people with malicious intentions access to delicate data passing through the communication channel.

5. Denial of Service

Though it doesn't seriously disturb reliability of the data stored in cloud computing servers, denial of service can momentarily deny access of data to legitimate users.

6. Data Handling

Distribution of technology and resources between different organizations always attitudes a risk to the data being handled. Occasionally servers at cloud computing organizations are organized to work with data from few clients. Once data from a customer with different necessities is added to the system, there are several things that may go erroneous.

How to Secure Your Cloud

1. Password security

Passwords are important components when it comes to security in a cloud set up. Unfortunately, many people are still irresponsible with the passwords, which can cause destruction in a cloud installation. Passwords for a main server should only be recognized by those who need this information, and they should be changed regularly. Furthermore, those who contact cloud servers from desktops should be trained how to generate strong passwords and the significance of keeping them secret. The cloud depends on trust, and one broken password can interrupt this trust.

2. Consider going beyond passwords

The next technique is to practice a two-level authentication. There are many different technologies to implement this and each deal some unique advantage. It should be noted, though, that these authentication methods may cause hindrance; before determining to use one of these choices, test it comprehensively to confirm that users will be able to understand it.

3. Encryption

Some security holes are inevitable and that any server can be damaged. Though this point is arguable, it can never be totally known that a specific server is safe. One of the best ways to avoid those who access a server inappropriately from stealing data is to confirm that it is encrypted. Encryption will restrict the damage that can be done from a incident, and it can provide users confidence that their data will be safe.

4. Log everything

For end users, cloud set up make getting work done and retrieving information simpler. On the servers, yet, there are certain difficulties that are inevitable. Additionally, the cloud model is still comparatively young, and even specialists only have a few years of experience. So, it can be easy to become confused when attempting to investigate problems. Strong, reliable logging can aid confirm that difficulties are determined as quickly as possible and help avoid the problem from happening again.

5. Do not forget the firewall

New approaches of securing networks have become common in recent years, but an active firewall is still the greatest frontline key to avoiding unauthorized contact. Remote access is essential when running a effective cloud operation and administrators will need to be able to use servers even if they are away from the office. By taking additional steps to confirm that the firewall is only permitting as much access as essential, it may be probable to keep away malicious attackers.

There is little suspicion that the cloud is the method the future for computing, but the cloud must be able to achieve the trust of the public. Those who are responsible of local installations can do their portion by warranting that their cloud implementations are safe as possible. Following the recent security news can also assist to give cloud operators ideas for enlightening their security.

Chapter 3
Addressing security risks in cloud

Chapter 3 – Addressing security risks in cloud

Learning Objectives

What this chapter is about?

- Security Risks in Cloud Computing
- Measures taken to control the security breach
- AAA-Authentication, Authorization and Auditing

What you should be able to do?

- Understand the possible security threats in cloud infrastructure
- Steps taken to control the security breaches, data losses etc.
- Understand the role of AAA in cloud infrastructure.

How will you check your progress?

Accountability:

- Checkpoint questions

Introduction

Security and privacy concerns are more similar to those of non-cloud services, but the concern is more as there is more of external control over the organizational assets. The control is more with the cloud provider than the organizations direct control.

It is necessary for the organization to check is the cloud service provider's security and privacy policies are in best interest of the organization. This is achieved by the Service Level Agreement (SLA) which will have appropriate provisions for security and privacy. The consumer should also maintain their own system to manage the security and privacy.

Cloud computing comes with a lot of attractive features; it also has equal number of security risks which must be addressed.

Loss of governance: While deploying in public cloud, consumer hands over most of the control to the cloud provider affecting security. In this situation the SLA from the cloud provider may not offer a commitment, which leads to a gap in the security defences.

Responsibility ambiguity: As the service spans across both providers & consumer organization, the security responsibility will also be across both the organizations, if there is a failure in allocating the responsibility clearly it might leave vital part of the defence unguarded. Responsibility across the organizations might depend varying on the model being used (e.g. iass over SaaS).

Isolation Failure: In public cloud computing shared resources and multi-tenancy defines the character of the cloud. This cloud lead to failure of memory, storage, routing and even disrupt between different tenants.

Vendor lock-in: If portability of applications and data to other providers is not supported then it leads to a risk of data and service unavailability.

Compliance and legal risks: It's a risk if the cloud provider is unable to provide evidence of their compliance or do not permit the cloud consumer to audit. The cloud consumer should always ensure that the appropriate certifications are in place, also defining the security responsibilities between the consumer and the cloud provider.

Handling of security incidents: Consumers always relay on the cloud provider with regards to detection, reporting and subsequent management of security breaches.

Management interface vulnerability: Management interface of public cloud are usually accessed via internet, which pose a risk with regards to remote access and web browser vulnerability.

Data Protection: This is a biggest challenge for the consumer and the cloud provider. Data protection risk can cause a concern of exposure of sensitive data or even to an extended of loss or unavailability of data.

Malicious Behavior of insiders: With the possible access given to the insiders working in the organization can cause damages by malicious actions. This kind of activity might occur either on the providers or consumers organization.

Business failure of the provider: These failures lead to unavailability of data and essential applications to the consumers business.

Service unavailability: There are various factors which could cause a communication between the service provider and consumers, such as equipment or software failure in the data centre.

Insecure or incomplete data deletion: When a cloud resource is terminated, the data may not be wiped out completely. This is because the disk might have other customer's data in it or copies of unavailable data in the disk.

Cloud Security Guidance:

The security in the cloud should be better than or equal to the traditional IT environment, ensuring there is no failure leading to potential loss of business.

The cloud consumer should have a understanding on some of the steps needed to evaluate and manage the cloud security. These are some of the steps discussed in details.

1. Effective governance, risk and compliance process.
2. Audit business and operational processes.
3. Manage roles, people and identities.
4. Ensuring Data and Information protection.
5. Enforcing Privacy Policies
6. Assessing security for cloud applications

7. Securing cloud networks and connections
8. Evaluate security controls on physical infrastructure and facilities
9. Manage security terms in the cloud SLA
10. Understanding the security requirements of the exit process.

Effective governance, risk and compliance process:
Organizations establish security and compliance policies and procedures to protect their intellectual property especially in IT space. Based on risk analyses the policies and procedures are developed. The polices, security plan and surrounding quality improvement process represent the risk management, compliance model and enterprise security governance.

The consumer on cloud service has to ensure that the hosted application and data are secure in accordance with the compliance and security policy between the provider and the consumer, along with the SLA.

In IaaS the service provider would provide resources like machines, disk and network. The consumer has to manage the operating system, running application etc., which gives more control to the consumer in terms of securing the data and application. In SaaS model infrastructure, data and application is handled by the provider, giving very less control to the consumer.

It is important to understand the laws or regulations applied to the service and the relevant obligations & duties imposed, before migrating to a cloud services. This is gives a brief idea about the legal issues and risk which could possibly impact the services.

Audit business and operational processes:
Auditing the compliance of IT systems is very important for the companies to see if it ad hears to the policies as per the industry standards.

Before considering the cloud provider, it's essential to have an access to audit information of the cloud provider by a independent auditor. As per the terms the cloud provider should offer access to log, event and report information's relevant to consumer specific data or applications.

The security methods are considered based on three significant areas which would be of particular interest to auditors and cloud consumers.

1. Understanding the internal control environment, risks involved controls and other governance issues in a cloud environment.

2. Access to the corporate work flow, audit trial and authorization
3. Assurance of the facilities for management and control of cloud services.

Manage People, Roles and Identities

Consumers should ensure that the cloud provider has process and functionality to govern the access to the consumer's data and applications. This ensures access to their cloud environment is controlled and managed.

Organizations have thousands of employees and users accessing the cloud applications and services, with different roles and entitlements. Cloud consumer should be allowed to manage the roles and associated levels of authorizations for their users in accordance with their security policies. These roles and authorization rights are applied on a per service, resource or application basis.

The cloud provider should have a secure system for provisioning and managing the users and services. The identity management functionality should support resource access and consumer application and work flows. All the user interaction and access of the cloud provider's management platform should be monitored and logged to provide auditing of consumer data and applications.

Ensure Proper Protection of data and information

Data a core IT security concern for any organization. Cloud computing has distributed nature of infrastructure and shared responsibilities, which makes it to secure the data at rest and also to data in motion.

The main concern of data in cloud is various forms of risk: risk of tampering, risk of theft or unauthorized disclosure of data or unauthorized modification of data, risk ok loss or unavailability of data. In case of cloud computing "data assets" will include application programs or machine images, which can also have the same risk.

Responsibility of handling particular security control also depends on the type of cloud service. In IaaS, customer is more responsible, for SaaS the responsibility is on the cloud provider.

Enforce Privacy Policies:

Privacy is often involving laws and regulations, with regards to acquisition, storage and use of PII (personally identifiable information) which is gaining importance across the globe. Privacy implies the accessibility and use of PII, tagging the data appropriately, storing it securely and permitting access to only appropriate authorized users. When a data is stored in a cloud it should have an appropriate control in place. ISO 27018 standards addresses the control required for the PII.

When a data is transferred to a cloud environment, securing the data and protecting it become the responsibility of the consumer. when an organization relies on a third party to host or process a data, it is mandatory to entry into a legal written agreement that clearly defines the roles, expectations of the parties and their responsibilities with regards to the data at stake.

The cloud contract and Service level agreement (SLA) should address the privacy issues which are critical. If not addressed then the consumer should consider alternate provider or not have sensitive data into the cloud.

It is enterprises responsibility to define polices which addresses the privacy concerns and creates the awareness of the data protection within the organization. They should also ensure that the cloud provider also adhere to their privacy policy.

Assess the security provisions of cloud applications:

Organization has to protect the business critical applications or data from internal and external threats all throughout the life cycle. Security policies and process should be clearly defined such that it should enable the business rather than additional risk.

Application security has become a greater challenge for cloud provider and consumers. Organization should apply the same policies and process for application security as they do for physical and infrastructure security.

A better understanding on the application security policy based on different cloud deployment would help us protect the application from various breaches.

Deployment Type	Application security policy consideration
Infrastructure as service (IaaS)	The consumer has all the responsibilities with regards to software deployment to managing the entire stack and all aspects of security. • Application security policy should the same as the policy enforce internal by the consumer. • The focus should be on the physical environment, network, auditing, authorization and authentication as outlined in the document. • Patch management is the responsibility of the consumer. • Data encryption standards should be enforced.
Platform as service	• Consumer has the responsibility of application deployment and securing it . • Provider has to secure the operating system, middleware and infrastructure. • Knowledge on format and location of data may or may not be known to the consumer.
Software as Service	• Application security is the responsibility of the provider as per the terms in the contract and SLA. • Consumer should have a better understanding on patch schedule, release cycle and controls of malware. • Parameters of the application are the only thing consumer can modify, Which is independent of application security.

Ensuring Cloud networks and connections are secure:

Network traffic should be constantly monitored by the cloud provider like any other internet-connection organization, to have a check of legitimate network traffic and drop malicious network.

Consumers should evaluate the external network controls of a cloud provider based on the highlighted areas such as:

Traffic screening:

- There are certain traffics which are never legitimate, e.g., traffic to a known malware port. The provider should ensure to block the same.
- Firewall device or software is used for screening traffic, some of the consideration are:
- The block list should be checked by the customer to ensure that a thoughtful network protection plan is enforced.
- Many devices nowadays are IPv6 capable, which can possible allow attacker an easy way around IPv4 firewall.

Intrusion detection/prevention:

- There is traffic which looks legitimate, but when we inspect it deeply it may carry malicious payload like viruses, spam or known attacks. These kinds of activities have to be notified or blocked.
- Instruction detection and / prevention system looks at both network traffic patterns and also the contents of the messages, unlike the firewall. Now day's firewalls include IDS/IPS

Logging and notification:

- For assurance purposes and troubleshooting, it's important that consumers have some visibility into the network health.
- Incident reporting and incident handling procedures must be clear and the consumer should look for visibility into the handling process. Note that if any PII is stored in the cloud computing environment, there may be legal requirements associated with any incident.
- Some network logging information is of a sensitive nature and may reveal information about other clients, so a cloud provider may not allow direct access to this information.

In cloud computing it has many internal network infrastructures such as access switch and routers to connect virtual cloud.

The primary categories of internal network attacks are :

1. Confidentiality breaches (disclosure of confidential data)
2. Integrity breaches (unauthorized modification of data)
3. Availability breaches (denial of service, either intentional or unintentional)

Consumers must evaluate the cloud service provider's internal network controls with respect to their requirements and any existing security policies the consumer may have

Evaluate security controls on physical infrastructure and facilities:
In cloud computing, the infrastructure and facilities will be owned and controlled by the cloud service provider and it is the responsibility of the cloud consumer to get assurance from the provider that appropriate security controls are in place.

Assurance is provided based on audit and assessment reports, demonstrating compliance to such security standards as ISO 27002.

A brief description on the security controls has to be applied to the physical infrastructure and facilities of a cloud that includes:

- Physical Infrastructure and facilities should be held in secure areas.
- Protection against external and environmental threats.
- Control of personnel working in secure areas.
- Equipment security controls.
- Supporting utilities such as electricity supply, gas supply, and water supply should have controls in place.
- Control security of cabling.
- Proper equipment maintenance.
- Control of removal of assets.
- Secure disposal or re-use of equipment.
- Human resources security.
- Backup, Redundancy and Continuity Plans.

Physical security requires a centralized management system that allows for correlation of inputs from various sources, including property, customers, employees, the general public, and local and regional weather.

Manage security terms in the cloud SLA

Security responsibility of both service consumer and service provider should be made clear. Security responsibilities should be specified and should also include the reporting aspects.

In cloud SLA it is documented that if there is any occurrence of breach it has to be notified to the customer. The provider should include specific information in the notification, data breach should be stopped as quickly as possible, restore secure access to the service at the earliest, apply best practice in investigating the circumstances and causes of the breach, and enforce long-term infrastructure changes to correct the root causes of the breach to ensure that it does not recur.

The performance and effectiveness are measured based on certain metrics and standards should be understood before subscribing to a cloud service and also should be specified in the SLA.

A data compliance report is required, which would reflect the strength or weakness of controls, services, and mechanisms supported by the provider in all security domains.

Understand the security requirements of the exit process

Once the consumer has completed the termination process, "reversibility" or "the right to be forgotten" is achieved - i.e. none of the consumer's data should remain with the provider. The provider must ensure that copies of the data are wiped clean from the provider's environment, wherever they may have been stored. Note that other data held by the provider may need "cleansing" of information relating to the consumer (e.g. logs and audit trails), although some jurisdictions may require retention of records of this type for specified periods by law.

Clearly, there is the opposite problem during the exit process itself - the consumer must be able to ensure a smooth transition, without loss or breach of data. Thus the exit process must allow the consumer to retrieve their data in a suitably secure form, backups must be retained for agreed periods before being eliminated and associated event logs and reporting data must also be retained until the exit process is complete.

Cloud Security Assessment

Security Step	Assessment Questions
1. Ensure effective governance, risk and compliance processes exist	• Does the consumer have governance and compliance processes in place? • Does the provider have appropriate governance and notification processes for their services?

2. Audit and ensure proper reporting of operational and business processes	• Is audit information available for the provider services? • Does the provider have mechanisms in place to provide reporting for both normal or exception behavior? • Is it clear that the provider's management have adequate security
3. Manage people, roles and identities	• Do the provider services offer access control? • Is single sign-on possible with the provider's services? • Can the provider give reports for monitoring user access? • Is it possible to integrate consumer identity management with the
4. Ensure proper protection of data and information	• Is there a data asset catalog for all data which will be used or stored in the cloud? • Has the handling of data been considered, in particular unstructured data such as images? • Has appropriate confidentiality, integrity and availability been applied to data used or stored in the cloud environment?

5. Enforce privacy policies	• Is PII going to be stored/processed by the cloud services? • Do the provider's services have appropriate controls in place for PII? • Are responsibilities for handling PII stated in the SLA?
6. Assess the security provisions for cloud applications	• Is it clear whether responsibility for applications running on cloud infrastructure lies with the consumer or with the provider? • Where the responsibility lies with the consumer, does the consumer have governance and policies in place that ensure the appropriate security provisions are applied to each application? • Where the responsibility lies with the provider, does the SLA make the provider's responsibilities clear and require specific security provisions to be applied to each application and all data?

7. Ensure cloud networks and connections are secure	• Is network traffic screened? • Does the provider's network have intrusion detection & prevention in place? • Does the network provide the consumer with logging and notification? • Is there separation of network traffic in a shared multi -t environment? • Is consumer network access separated from provider network access?
8. Evaluate security controls on physical infrastructure and facilities	• Can the cloud service provider demonstrate appropriate security controls applied to their physical infrastructure and facilities? • Does the service provider have facilities in place to ensure continuity of service in the face of environmental threats or equipment failures? • Does the cloud service provider have necessary security controls on their human resources?

9. Manage security terms in the cloud SLA	• Does the cloud SLA specify security responsibilities of the provider and of the consumer? • Does the SLA require that all security terms must also pass down to any peer cloud service providers used by the provider? • Does the SLA have metrics for measuring performance and effectiveness of security management? • Does the SLA explicitly document procedures for notification and handing of security incidents?
10. Understand the security requirements of the exit process	• Is there a documented exit process as part of the contract/SLA? • Is it clear that all consumer data is deleted from the provider's

Importance of AAA

Network Authentication, Authorization, and Accounting are a technology which has be in use even before internet started.

AAA, enables mobility and dynamic security. Without AAA the network should be statically configured with well-defined connectivity options, without moving the systems. In the world of mobile devices and various network access methods, creating a greater demand on AAA.

AAA plays a major role in today's way of accessing the network. Wireless hotspots, partitioned network and remote access require AAA for security, enforcing segmentation and authorizing remote users.

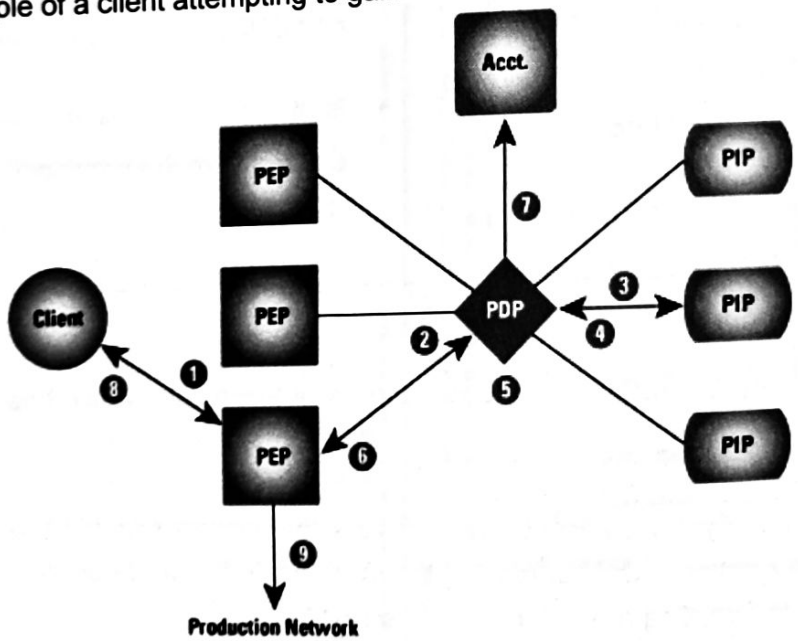
Understanding the roles of a AAA system

Core Components of AAA

- *Client:* Devices which access the network authenticating it or acts like a proxy.
- *Policy Enforcement Point (Authenticator):* it's also called as authenticator or dial-in server, gatewa
  firewall VPN concentrator, wireless access point or and security gateway. PEP enforces the clien
  access terms.
- *Policy Information Point:* it's a repository which contains information based on which acces
  decisions are made. This could be database such as LDAP, one time password token server o
  any other system which holds device or user access request.
- *Policy Decision Point (AAA Server):* This is the brain of AAA decision. The access request
  collected form the client through PEP. To make any access decisions it also queries PIPs fo
  information's. PDP is the final decision maker in the network access.
- *Accounting and Reporting System:* Tracking the network usage with accounting is one of the bes
  features of AAA. This can give you a clear picture of who got on the network, what permission wa
  granted and from where.

Example AAA Flow

Figure shows an example of a client attempting to gain access to the network.



A Client Connects to a AAA-Protected Network

1. A client is trying to connect to the network, before establishing the connection its requested for identity information, which is sent to the PEP.

2. The collected information from PEP is sent to PDP. In some cases the information is directly relay to the PDP.
3. The PDP queries any configured PIPs for information about the client and validates the client credential.
4. The success or failure message from the credential step is returned by the PIP and also sends additional information to the PDP for evaluation.
5. The PDP learns about the client through PEP, PIP or client by itself. PDP makes authorization decisions based on the information.
6. The authentication results and authorization specific to the client is sent from the PDP to the PEP. This would trigger specific PEP actions to be applied to the client.
7. The transaction results are sent to the accounting system by the PDP.
8. Once the PEP learns about the authorization profile from PDP a "authentication successful' message is sent.
9. Now the client is granted access through the production network through PEP.

Elements of Authentication

There are various elements which are being evaluated before the PDP reaches its access decision. On a broader perspective these elements are broken down into three categories: Principal, Credential & Contextual information.

Principal: It is a combination of user, device or service, which requests for authorization. When concerned with user, PIP provides various attributes like job title, e-mail address role and so on. For example, in an office they might be interested in knowing employee schedule when servicing the employee authentication request. When managing a device the PIP informs the PDP about the managed asset and its basic usage parameters. Authentication of user and the device are carried out sequentially, authenticating the device first and then the user. Lastly the service is authenticated.

Credential: This is the proof of identity the user or device submits. There are four main types of credential: shared key (password), digital certificate, one-time password (OTP) and biometric credential. Shared key is the most widely used form of credentials. These shared keys are further sub divided based on the protocol the system uses to verify the password, such as Challenge Handshake Authentication protocol (CHAP), Password authentication protocol (PAP) and Microsoft CHAP extensions (MS-CHAP). PAP authentication is not recommended in security sensitive environment as it is a plain text authentication.

CHAP is more secured in comparison with PAP as it sends the password using hash of the password. MS-CHAP Microsoft extension of CHAP, tuned for Microsoft environment. MS-CHAPv2 is common in Microsoft

environment. CHAP is more vulnerable to dictionary attacks, because passwords can be guessed and hash values can be computed.

This is one of the most widely used credential type, which is generated using the user's personal token. These tokens are randomly generated which is synchronized with the token server to act as PIP. This can be sent as clear password as its time based (30 seconds) once used it cannot be reused.

Digital certificate is the type of credential which is either stored locally or on removable device. This certificate can be freely distributed, as it can only be validated with the combination of private key from the rightful owner. Certificates are most often used to authenticate a physical entity rather than an individual. Biometric credential the least widely used credential type. Finger print, iris & facial scanners are the forms of biometric authentication.

Contextual: Contextual information is associated with the AAA request, which is used by the PDP for authentication decision. This contains information's such as network and physical location of the request, the time of the day, the type of access provided by the PEP and other elements such as network load, security threat level and so on.

Authorization Approaches

AAA network authorization options include Layer 2 segmentation, Layer 3 filtering, and Layer 7 entitlements. In this section we also discuss on the challenges encountered when sending or provisioning the authorizations from the PDP to the PEP.

- **Null Authorization (Authentication Only):** This is strangely the most common authorization in AAA, no authorization at all. The client is given full access, immediately after the authentication event occurs. This is the original goal of remote-access AAA: which performs the authentication of the client as if it were connected to the organization network. In today's network authentication is increasing to provide access to the client with network rights. \
- **Layer 2 Segmentation:** This is the common form of authorization enforcement for wireless access points and Ethernet switches, because it splits the network into multiple logical segments. This is achieved by deploying virtual LANs which separates client from two different VLANs.
- VLANs can restrict access to specific resources based on ACL on layer 3 devices. In a access point the given SSID (Service Set Identifier) can be linked to a VLAN on the wired side of the access point. WAN transport is associated with MPLS(multiprotocol label switching). so commonly client is linked with VALN and VLAn with an MPLS.

- **Layer 3 Filtering:** This authorizes access to the layer 3 devices (Ethernet switch, router, security gateway etc...) based on the ACL configuration. These ACLs enforce authorizations to a range of different hosts or services on that hosts. In network infrastructure where security gateway applies ACLs to specific client, this filtering technique is commonly used.
- **Layer 7 Entitlements:** This facilitates the security gateways to go beyond Layer 3 and 4 filtering the applications apart for just authorizing hosts on the network and the segments. There is no standard to make this interaction work transparently as this is a new technology.

Provisioning challenges: The users session rights and constrains are communicated to the PEP so that PEP can enforce this permission, that's called as provisioning. One of the challenges provisioning access rights has is communicating the decision of PDP in the format PEP understands. This is why most PEP comes with lightweight PDP. This solves the problem but creates a management problem when coordinating with network AAA across enterprises. In enterprise network the AAA polices are applied individually on each type of PEP on the network. PDP decisions are most commonly communicated with one of the AAA protocol, RADIUS.

VSAs(Vendor Specific Attributes) in RADIUS enables the PDP to speak the language of the PEP more specifically. There is upcoming option where the RADIUS is extended to send standard IP ACLs using RADIUS attributes.

Provisioning through the SNMP (Simple Network Management Protocol) is one another option using which the layer 2 port to VLANs is assigned or enabled/disabled. in deployment the SNMP typically used is SNMPv2c, which uses UDP(connection less), this makes it prone to packet losses. These makes SNMP a poor choice for secured tasked.

SSH (Secure Shell) or HTTPS is another provisioning method. The enforcement technique is managed through a standard administrative interface.

Accounting Techniques

This is the critical step in the AAA process. Auditing of network access is made mandatory by the Regulatory controls. Accounting, the last stage maintains the record of clients accessed the network, the access granted to them and when did they disconnect. Internet Service Providers (ISP) use accounting widely for auditing network access to bill their ISP customers.

Correlation helps system which are user-aware more intelligent in the security decision. For example Intrusion Detection System (IDS) understands the behavior of a IP address, when correlating this with the user who is assigned that IP address- the relevance of the IDS data increases dramatically.

Accounting system as the centralized nature of audit and decentralized nature of access, which is out-of-band with the client's communication. This makes it better for the administrators to find when the client was connected and granted access. This out-of-band makes them also a poor resource in terms of understanding what the client actually did.

Chapter 4
Identity Management

Chapter 4 – Identity Management

Learning Objectives

What this chapter is about?

- What is Identity Management?
- Benefits and Aspects of Identity Management
- What is detention of breaches and forensics?

What you should be able to do?

- Understand the aspects of Identity Management
- Securing the Cloud environment
- Prevent breaches

How will you check your progress?

Accountability:

- Checkpoint questions

Identity management

Identity management in an enterprise is a combination of processes and technology to manage and secure way of accessing to the information and resources of an organization while also protecting user profiles, including customer profiles. It includes the entire process of deciding who should have access to resources, and to what resources; providing, changing and terminating such access when appropriate; managing the process and monitoring it for compliance with internal and external policies. This usually applies to situations Where the person has to identify who he/she claims to be by means of a verified identity, such as a passport or identity card at border control, login credentials for e-banking, biometric identification for account access at an ATM machine, and so on.

Identity management has two principal components: management "of" the management and identity "by" the identity Management of the identity is the process of issuing and using digital identities and credentials (such as usernames and passwords) for authentication. Management by the identity combines the proven identity of the user with their authorization, in order to grant access to resources.

Life cycle is an Identity of an entity has its own. For example, the company network would be created, maintained, synchronized and deleted across multiple systems or platforms for an employee's login account for accessing. The employee's login credentials, with access rights, that would be granted by a process called user provisioning. This account would be maintained and updated whenever new privileges are assigned to this employee, perhaps due to internal transfer, promotion, demotion, and so on. The employee's data or passwords would be synchronized among different IT systems and platforms. Finally, his/her login credentials can be deleted across all systems due to, say termination of employment or retirement. This removal of access rights is a process called user de-provisioning.

There are three common identity management models:

Isolated identity management

This model requires that each user possess an identifier for access to each isolated service. This system is used a lot in online services and resources, because it is relatively simple for service providers to manage, but it is rapidly becoming unmanageable for users. The exponential growth in online services has led to users being overloaded with identifiers and credentials (different logins and passwords) that they need to remember and manage. For this reason, new identity management models are being proposed and implemented.

Federated identity management

Federated identity management simplifies the account problem management. A set of agreements and standards are defined among a group of service providers who recognize user identifiers from one another. A customer of one particular service provider could access all services provided by another service

provider in the group with only a single identifier. For such standardized methods of information exchange within the group to work, implementation of a common technology standard such as OASIS (Organization for the Advancement of Structured Information Standards) SAML (Security Assertion Markup Language)3, the open source initiative, Shibboleth4, and so on is required.

Centralized identity management

This model, the same identifier and credential are used by each service provider. This could for example be implemented by having a PKI, where a Certificate Authority (CA) issues certificates to users. Each user can then use the same certificate to access different services, and all providers authenticate the client through the same certificate before granting access to their services. Another example could be the Single sign-on (SSO) model, which requires a user to login once and be authenticated automatically by all other service providers. The Kerberos Authentication Server and Microsoft .Net Passport are examples of SSO implementation. A drawback of this approach is that should one of the trusted identity providers fail (e.g. under a DoS attack), the normal services of all service providers may be affected.

Authentication and Authorization

Authentication techniques make use of one or more of the following factors:

1. something you know (e.g. password),
2. something you have (e.g. a smart card),
3. something you are (e.g. fingerprint)

If two of these factors are needed for successful authentication, it is termed a "two-factor authentication". Two-factor authentication is generally believed to be more secure, and therefore many high-risk systems such as Internet banking are now implementing schemes like this.

Authorization is a process that determines whether an entity is allowed access to a given asset or resource. Common access control models are5:

1. Discretionary Access Control (DAC): in this mechanism, users own the objects under their control, and the granting and revoking of access control privileges are left to the discretion of individual users.
2. Mandatory Access Control (MAC): it is a means of restricting access to objects based on the sensitivity of the information contained in the objects, along with formal authorization of subjects to access information of such sensitivity.
3. Role-based access control (RBAC): it is an authorization mechanism in which access decisions are based on the roles that individual users have as part of an organization.

When assigning access rights to an entity, the principles of least privilege and separation of duties are strongly recommended. The principle of least privilege recommends that the least amount of privileges necessary to perform one's task should be granted to an entity. The principle of segregation of duties suggests that critical functions are divided into steps among different individuals to prevent a single individual from subverting a critical process.

Challenges of Identity Management

Identity Theft

The Internet now covers the whole world and a large part of the economy. One major challenge to e-Commerce on the Internet is that of authentication. On the Internet, we do not have a sure way of knowing who and what we are really connecting to.

Many information systems employ a username and password for authentication purposes. Early Internet banking applications have been using this authentication mechanism. Increasing identity theft incidents such as phishing have prompted institutions to use more advanced authentication mechanisms to identify their customers. The Hong Kong Monetary Authority has also recommended using stronger customer authentication in e-Banking applications7. The Internet banking systems of certain banks in Hong Kong now require two-factor authentication for login. Bank customers need a one-time password generated from a security token given to them by the bank, in addition to their standard username / password information

Identity Management Adoption and Benefits

Advances in identity management technology help enhance overall identity protection. Instead of simply relying on traditional password-based technology, two-factor authentication using biometric technology has grown as the price of biometric hardware and software has dropped. Some common characteristics that can be used for biometric identification include: fingerprints, hand geometry, retina scans, iris scans, face recognition and voice analysis. While biometric authentication has its advantages, it also has limitations and drawbacks. Biometric identification systems might not be 100% reliable. Sometimes, a legitimate user finds they need to try more than once before he / she can be authenticated. As a pre-requisite to using a biometric identification system, a customer might need to „register" his / her biometric features in the system, and this raises concerns about personal privacy.

Identity management in the public domain also requires stronger authentication. The Hong Kong Government has been issuing smart ID cards since 23 June 2003, and this provides a means for Hong Kong residents to access to a variety of government electronic services in a safe and secure manner8. Another example would be the US initiative for an electronic passport, which could provide automatic identity verification and greater border protection and security9. Biometric information such as face recognition, fingerprints or iris scans would be stored in the electronic passport.

Benefits of Identity Management

Apart from improvements in security, a well-implemented identity management system brings at least two business benefits to an organization: cost reduction and improved service levels. With an enterprise-wide identity management system in place, an organization does not need to dedicate human resources to handling user ID related issues for each individual application. As a result, fewer people are needed for ID administration activities, which could in turn reduce IT operation costs. In addition, fewer calls to the help desk regarding user ID problems would contribute to more cost savings. A common user complaint in the enterprise environment is the slow response when dealing with user ID resets, or other ID management functions. With the help of an automatic identity management system, response times for requests relating to user IDs would be improved, resulting in an improvement to IT service levels and better user ID management activities.

Conclusion

Passwords are still the most common authentication method. To reduce the possibility of passwords being compromised using brute-force attacks, consecutive unsuccessful log-in trials should be controlled. This can be accomplished by disabling an account after a limited number of unsuccessful log-ins. Alternatively, a mechanism of increasing the time delay between each consecutive login attempt could be considered as a way of preventing password guessing activities. In a SSO, user essentially only needs to remember one credential, so an attacker who can compromise that credential could break in to all the systems authorized by that user. Therefore, extra security measures are required in order to protect key credentials when implementing any SSO. A strong password policy and frequent password changes should be enforced to deter password attacks. Additional authentication methods, such as biometrics or two-factor authentication, could also be considered to strengthen the authentication process. Functions requiring another level of authorization should be implemented using re-authentication. In addition, idle logged-on sessions should be timed-out after a set period to prevent attackers from stealing idle session information. Individual accountability should also be established to hold each employee responsible for his or her actions. Within information systems, accountability can be accomplished by identifying and authenticating users of the system with a user identity (user-ID). This user-ID should uniquely identify a single individual, such that subsequent tracing of the user's activities on the system is possible should an incident occur or if a violation of the IT security policy is detected. Shared or group user-IDs should be prohibited unless it is unavoidable due to specific business needs.

Evolution of IAM — moving beyond compliance

In the past, IAM was focused on establishing capabilities to support access management and access-related compliance needs. The solutions were often focused on provisioning technology and were poorly adopted; they also resulted in high costs and realized limited value. Organizations often struggled to meet compliance demands during this period, and the solutions were deployed to manage very few applications

and systems. Centralized, standardized, automated identity management services designed to reduce risk, cost, improve operational efficiency continued to be elusive.

Many organizations now understand, or meet, their compliance requirements. While compliance is still a key driver in IAM initiatives, IAM is evolving into a risk-based program with capabilities focused on entitlement management and enforcement of logical access controls. Organizations are starting to achieve benefits from their IAM costs but are still challenged with managing time-intensive processes such as manual approval, provisioning and access review. Identity administration functions continue to be delivered in organizational silos resulting in users with excessive access, inefficient processes and higher cost of provisioning and de-provisioning.

As IAM continues to evolve, organizations will look to broader, enterprise-based solutions that are adaptable to new usage trends such as mobile and cloud computing. IAM capabilities will continue to leverage technologies to realize higher benefits versus the costs incurred. User demand will continue to drive the discipline to transform from a compliance-based program into a true business enabler (e.g., IAM is a key component for rolling out B2E and B2C applications that will drive operational efficiencies and improve the user experience) while helping to reduce risks created by emerging technologies and threats. To help reach the goal of an enabler that reduces risks, this IAM-focused paper explains life cycle phases, relevant IT trends, a capability maturity model, key considerations for transformation, tools and how to get started.

IAM 1.0 — the past

- Project-based deployment
- Compliance-driven approach
- Provisioning focused
- Individual employee identity management
- High cost vs. benefits realized
- Limited compliance value
- Limited view of enterprise access
- Poor application adoption

IAM 2.0 — the present

- Program-based deployment
- Risk-driven approach
- Entitlement management focused
- All user identity management (e.g., employees, contractors, system accounts)

- High compliance value
- High compliance cost
- Moderate benefits realized vs. cost
- Central view of access
- Increased application adoption

IAM 3.0 — the future

- Enterprise-based deployment
- Capability-driven approach
- Business enablement driven
- High benefits realized vs. cost
- High business value beyond compliance
- Central view of access by technology
- Strong technology adoption

Identity access Management life cycle phases

The management of identity and access permissions can be viewed as multiple stages. The IAM life cycle diagram illustrates the stages that users proceed through when joining a business workforce and obtaining access to the tools and assets necessary to do their job. The IAM life cycle also includes stages to ensure that employees maintain appropriate access as they move within the organization with access being revoked or changed when they separate or change roles. An IAM program requires a well-defined strategy and governance model to guide all the life cycle phases.

User access request and approve

Definition objective:

- Gaining access to the applications, systems and data required to be productive.

Common challenges:

- Processes differ by location, business unit and resource.
- Approvers have insufficient context of user access needs — do users really need access to private or confidential data.
- Users find it difficult to request required access.

Reconcile

Definition objective:

- Enforcing that access within the system, matching approved access levels.

Common challenges:

- Actual rights on systems exceed access levels that were originally approved/provisioned.
- There is no single authoritative identity repository for employees/non-employees.

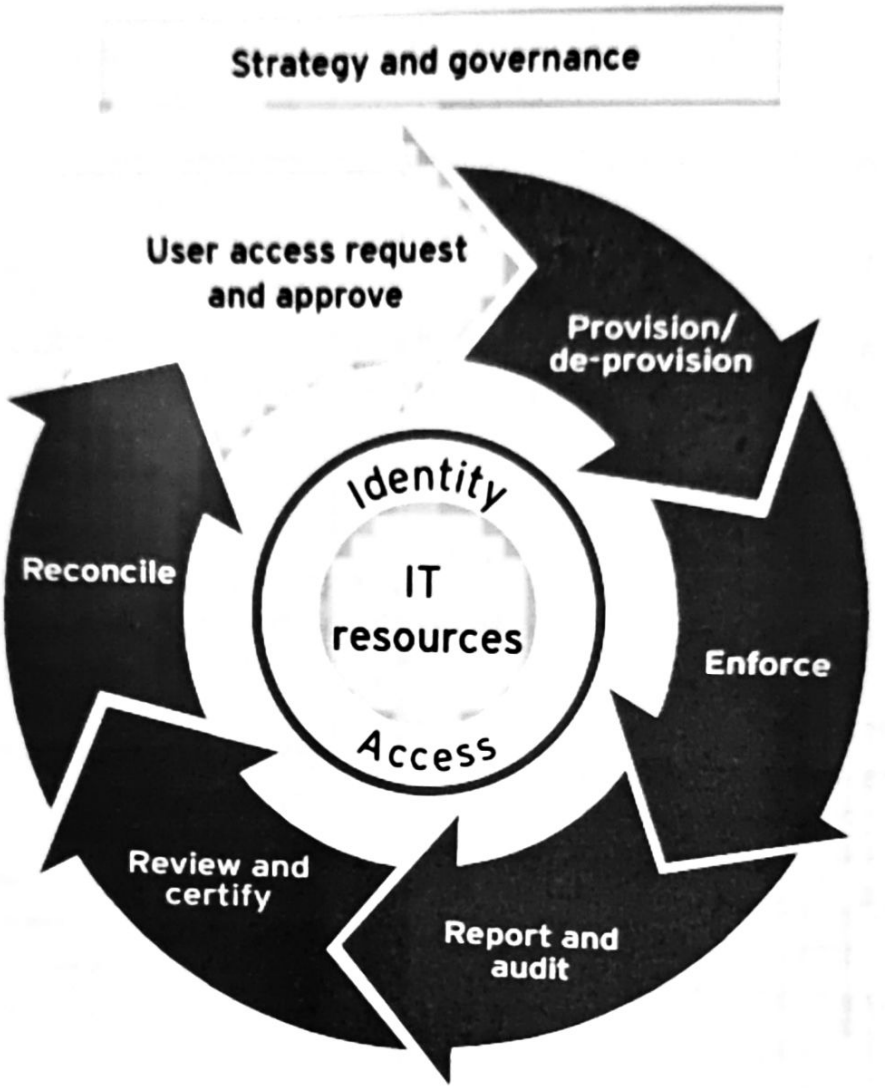
Review and certify

Definition objective:

- Reviewing user access periodically to realign it with job function or role

Common challenges:

- Processes are manual and differ by location, business unit and resource.
- Reviewers must complete multiple, redundant and granular access reviews.
- Reviewers have insufficient context of user access needs



Provision/De-provision

Definition objective:

- Granting users appropriate entitlements and access in a timely manner
- Revoking access in a timely manner when no longer required due to termination or transfer.

Common challenges

- Time lines to grant/remove access are excessive.
- Inefficient and error-prone manual provisioning processes are used.
- Access profile cloning occurs inappropriately.
- Ad hoc job role to access profile mappings exist.

- Inappropriate access may not be de-provisioned.

Enforce

Definition objective:

- Enforcing user access to applications and systems using authentication and authorization.
- Enforcing compliance with access management policies and requirements.

Common challenges:

- Applications do not support central access management solutions (directories, web single sign-on)
- Access management policies do not exist
- Role/rule-based access is used inconsistently
- Segregation of duties (toxic combinations) is not enforced

Report and audit

Definition objective:

- Defining business-relevant key performance indicators (KPIs) and metrics.
- Auditing user access.

Common challenges

- KPIs/metrics do not exist or do not align with business-driven success criteria (e.g., reduce risk by removing terminated user access on the day of termination).
- Audits are labor intensive

IAM and IT trends

IAM is a key element in enabling the use of these technologies and achieving business objectives, further emphasizing the need for IAM to grow beyond a mere compliance solution into a valued business tool.

Mobile computing

As today's workforce becomes more mobile, many organizations are adopting a bring your own device (BYOD) approach to provide remote access to email, sensitive or privacy-related data, and business applications. Consumer demand for mobile computing is also driving organizations to develop mobile applications to be used by customers to access their products. IAM is a strong enabler of mobile computing

(both for business to employee and business to consumer) and serves as a foundational component in mobile computing security.
Here are a few ways IAM can help an organization implement a more secure mobile computing program:

- Security safeguards normally in place for external connections to a network may be disabled or implemented at a reduced level because the business may not have control over management of these devices (especially in a BYOD model). As a result, it is critical that authentication mechanisms are implemented to confirm that the user of the device is authorized to access sensitive resources.
- Mobile devices allow company personnel to access critical applications (including privacy-related data) any time and from anywhere. If a device is lost or stolen, the detection of compromised devices should not be left solely to user reporting. Device and user authentication attempts can help to detect a compromised device and reduce potential incidents of fraud.
- Access controls should be designed with usability in mind; without this, users may circumvent overly restrictive and inconvenient controls, resulting in potential data loss incidents. A common example is someone forwarding personally identifiable or confidential information unencrypted to a personal email account in order to access it outside of the office. The proliferation of mobile devices (e.g., smart phones, tablets) and a strong consumer demand has driven organizations to adopt a BYOD model. This new reality has blurred the boundaries between home and office by providing constant access to email, sensitive data and even business applications enabling financial transactions.

To allow these devices to access the organizations' resources quickly and efficiently, mobile devices are set up to rely on identification mechanisms that verify and/or validate the user; security safeguards normally in place for external connections to a network may be disabled or implemented at a reduced level due to these mechanisms. As a result, it is critical that even stronger authentication mechanisms are implemented to confirm the user of the device is genuine and to safely allow users access to business critical applications anytime, anywhere.

Consumer demand for mobile computing is also driving organizations to develop mobile applications that customers can use to access their products. Mobile applications may allow consumers to access or transmit sensitive information (e.g., bank account information during an online transaction, private personal information submitted through a health insurance application). However, poor controls over authentication to the application, access to the data stored on the device by the application and external connections initiated by the application could increase the likelihood of a data compromise. IAM should be incorporated Into application design, pre-implementation testing and periodic vulnerability scans/tests performed after implementation.

Cloud computing

The emergence of, and demand for, cloud computing services has complicated the IAM landscape as control over access to sensitive data is difficult to maintain in such an environment. This reality has forced many organizations to operate IAM capabilities internally and to invest in integration with similar capabilities provided by their cloud service provider. The adoption of cloud computing platforms have resulted in reduced reliance on network access controls and increased reliance on logical access controls offered by IAM services.

Several distinct scenarios have emerged with the evolution of cloud computing and IAM — there is a need to securely access applications hosted on the cloud, and there is a need to manage identities in cloud-based applications, including protecting personally identifiable information (PII). Federation, role-based access (RBAC) and cloud application identity management solutions have emerged to address these requirements.

The concept of identity as a service (IDaaS) is also an emerging solution to this challenge and has made it possible to accelerate the realization of benefits from IAM deployments. IDaaS aims to support federated authentication, authorization and provisioning. As an alternative to on-premise IAM solutions, IDaaS allows organizations to avoid the expense of extending their own IAM capabilities to their cloud service provider but to still support secure interaction with a cloud computing environment. When using IDaaS, instead of a traditional onpremise IAM system, these capabilities are provided by a third party- hosted service provider.

However, unless cloud computing services form an organization's sole IT infrastructure, the need for IAM capabilities to manage access to internally hosted applications will persist. The truth of this hybrid operating model is that IDaaS will need IAM agents or appliances to operate within an organization's remaining IT infrastructure to completely outsource the function. Securing these agents and their interfaces represents a new source of risk for most organizations.

Regardless of the operating model used, cloud computing creates new IAM risks that must be managed. Management of virtual servers within the cloud requires elevated rights that when compromised, may give attackers the ability to gain control of the most valuable targets in the cloud. Such rights also give attackers the ability to create sophisticated data intercept capabilities that may be difficult for cloud providers to detect in a timely manner. The risk of undetected data loss, tampering and resultant fraud can be magnified by the use of cloud computing unless equally sophisticated controls are in place. As a result, the implementation of controls over cloud computing services should account for traditional and emerging risks that are unique to the cloud.

Data loss prevention

Given recent public incidents related to data loss, data protection is top of mind for many organizations. The first line of defense in protecting data is identity and access management. Data loss prevention (DLP) is a complementary information security discipline that can be enhanced when leveraged with IAM capabilities.

IAM tools can provide identity context to DLP tools to provide better monitoring capabilities. Properly controlling access to data will reduce the likelihood of a data loss incident — fewer users with access to data results in less opportunity for data to be inadvertently or intentionally compromised by an internal or external user. In addition, DLP and IAM tools can be integrated to provide more comprehensive monitoring capabilities.

A leading practice is to use an IAM tool to provide identity information to a DLP tool that continuously monitors sensitive transactions (e.g., financial statements, internal memos) to establish an identity correlation to the events monitored. The

DLP tool is then set up to monitor for data loss events related to these complex, sensitive data elements. Any events detected are also correlated against data access levels and historical access behaviors recorded by the IAM tool to detect potential fraud. These solutions could be leveraged to address insider risk and emerging threat vectors, e.g., advanced persistent threats. By utilizing identity analytics using identity (human resource) entitlement and user activity data, we can deploy more effective privileged-user monitoring solutions for forensic analysis.

Properly implemented IAM can enable an organization to handle the fast pace of emerging IT trends — as highlighted here with mobile computing, cloud computing and DLP — but to determine where an IAM program stands, we need a frame of reference or a model.

Social media

Companies look to leverage social media to interact with their customers and increase brand awareness, however there are some serious IAM risks tied to these technologies. Legal, compliance, regulatory, operational and public relations issues are at the top of the list of potential social media risks that can

Ultimately cause loss of customers and erosion of market share and revenue. For example, on most of the popular sites (Twitter, Facebook and LinkedIn), users are able to create company profiles and communicate on behalf of the organization through social media channels. This can create marketplace confusion because of multiple messages and different audiences, policies and practices. There have been other instances where a company's reputation has been damaged when their public-facing social media accounts had been compromised and used to distribute fake updates that spread quickly.

You should provide IAM requirements to suppliers of the social media tools and services that you use to protect your accounts from being compromised; typical requirements include adding a second factor of authentication, receiving notifications of failed login attempts and receiving notifications of attempts to authenticate from geographic regions known to be the source for frequent attacks designed to gain control of social media accounts.

In addition to protecting company-owned social media accounts, it is also important to educate employees on the importance of using discretion with social media. Revealing too much information publicly on social media can enable attackers to get information to help them with social engineering or abusing self service password resets. Employees can also reveal confidential information about what IAM controls are in place if they are not careful about what they post.

Properly implemented IAM can help an organization to handle the fast pace of emerging IT trends — as highlighted here with mobile computing, cloud computing, DLP and social media — but to determine where an IAM program stands, we need a frame of reference or a model.

IAM and cyber crime

Cyber-crime, particularly the extent of economic and reputational damage that it can cause and the role that some nation states play in sponsoring corporate espionage, is a contentious issue. Regardless of the position that a company takes on the extent or viability of such threats, a strong IAM program helps to mitigate the effectiveness of some of a cyber-criminal's tools: privilege escalation, reconnaissance, remote access, social engineering and data exfiltration.

The following techniques can help to counter these attack vectors:

- Privileged user review
- Password management
- Identity-enabled networking
- Authentication and access control
- Integration with data loss prevention (DLP) tools

Case study — IAM in practice

Bank

Original state
Toxic access combinations existed, user provisioning processes did not address all relevant applications, and manual review processes proved ineffective and inefficient.

Challenges
Due to the number of business units impacted by the remediation efforts, there was a lack of consensus on the approach in addition to the risks of an ineffective access management environment.

Maturity-level transformation
Repeatable to managed IAM

IAM solution
Short-term solution

Data analysis techniques were used to quickly identify segregation of duties conflicts across 800,000 entitlements (effort prioritized by application criticality).
Longer-term solution

The company implemented a standardized process for the provisioning and de-provisioning of user entitlements at the operating system, database and application levels.

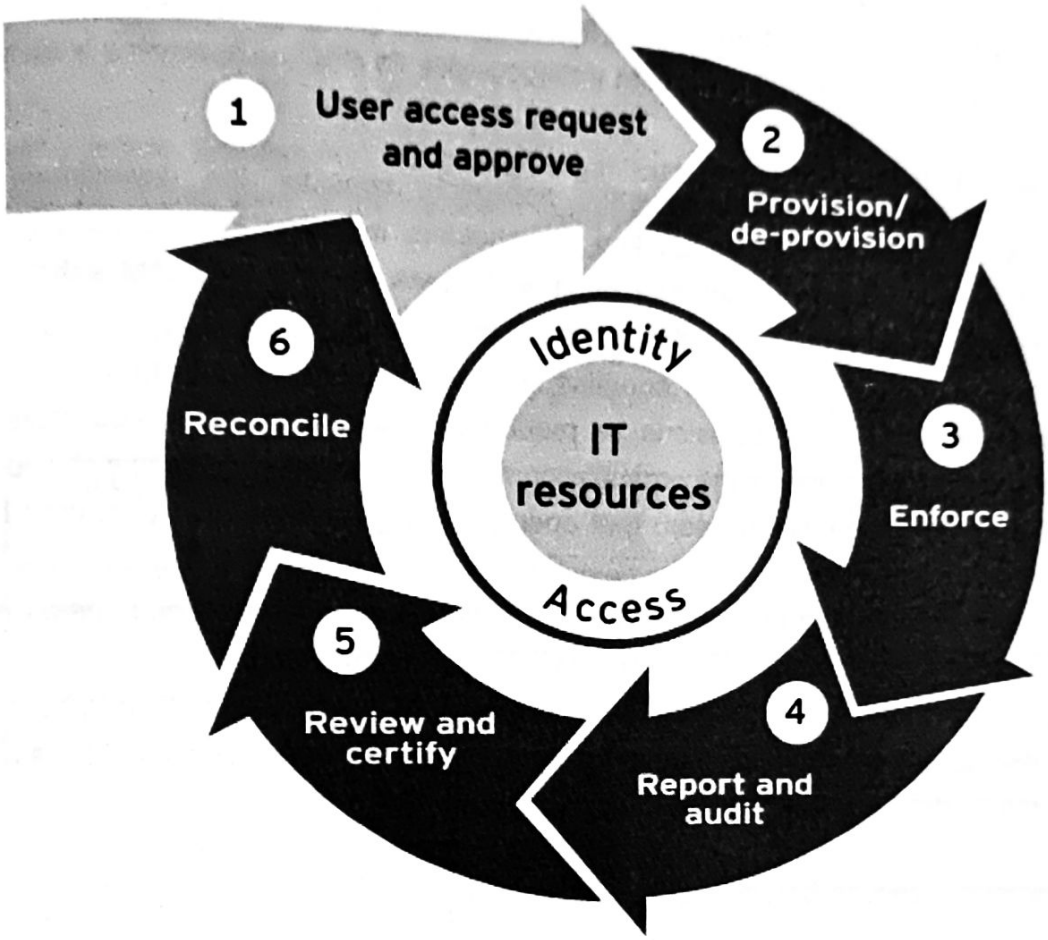
Benefits
The company developed segregation of duties remediation plans based on risk to address more than 6,000 accounts. Balance between short- and long-term solutions allowed the company to prioritize resources and funding.

Transforming IAM

To keep pace with IT trends and changing business needs, and to leverage the insights from the capability maturity model, the IAM function needs to be transformed.

IAM can be a highly manual process and still be effective in meeting an organization's goals, however in these instances the cost of labor is high and will likely outweigh the cost of technology. On the other side of the spectrum, a highly automated IAM program will have a very low cost of labor but a very high cost to implement and maintain. The key is finding the balance between the cost of labor and the cost of

implementation and maintenance while still meeting the organization's overall business, security and IAM goals.



Life cycle phase

1. User access request and approve
2. Provision/ de-provision
3. Enforce
4. Report and audit
5. Review and certify
6. Reconcile
7. Strategy and governance

Key considerations when transforming IAM

Having considered coming IT trends and evaluated your capability, you decide the time is right to transform your IAM program. The success of an IAM transformation depends on the interaction of people, processes and technology.

People

- Using a risk-based and business-centric approach, consider the downstream impact on organization structure as well as on key stakeholders including IT customers (business and operations), human resources, internal audit and users, so that any IAM enhancements can progress smoothly and with minimal disruption to the business.
- Avoid confusion and contention over priorities by appointing one executive level "program owner" who is empowered to make decisions as required, supported by committed stakeholders and executive sponsors from across the organization. IAM enhancement programs should also have a dedicated program management team that operates using an integrated plan vetted by auditors and compliance managers.
- Be proactive in establishing ongoing support by designating an experienced operational manager as the "service owner" after the enhancements have been completed.
- Place experienced staff on the program execution team as it takes a long time to become skilled in IAM methodologies, control implementation, process reengineering, stakeholder alignment, and program and change management.

Process

- Integrate process improvements into awareness campaigns designed to educate users in order to increase adoption rates.
- Document access control processes and perform periodic testing to validate that processes are being followed.
- Inform key stakeholders early (and often) that business processes will have to change to accommodate the improvement of IAM capabilities. Temper that message with the fact that IAM can simplify processes by eliminating manual, error-prone access management procedures, including access requests, approvals and reviews.

Technology

- The leading IAM products have similar capabilities and can generally meet most IAM requirements; however, these products are likely to need configuration and even customization to meet IAM requirements that are unique to your organization.

- A key activity often included in transformation programs is to redefine access profiles in terms of roles so that they can be more easily understood (using business-friendly definitions that avoid technical jargon). Activities intended to produce such role definitions will often require the use of a sophisticated, configurable role mining technology that will suggest potential access profiles.
- The definition of a business-friendly name and description for these access profiles will require a substantial amount of analysis by subject matter resources that understand your business.

When integrating people, process and technology, organizations can be inundated by technology options. The next section addresses some of the important features.

IAM tools

As they evolve their IAM programs, organizations seeking to achieve higher levels of IAM maturity commonly will use commercially available products with the features listed in this table.

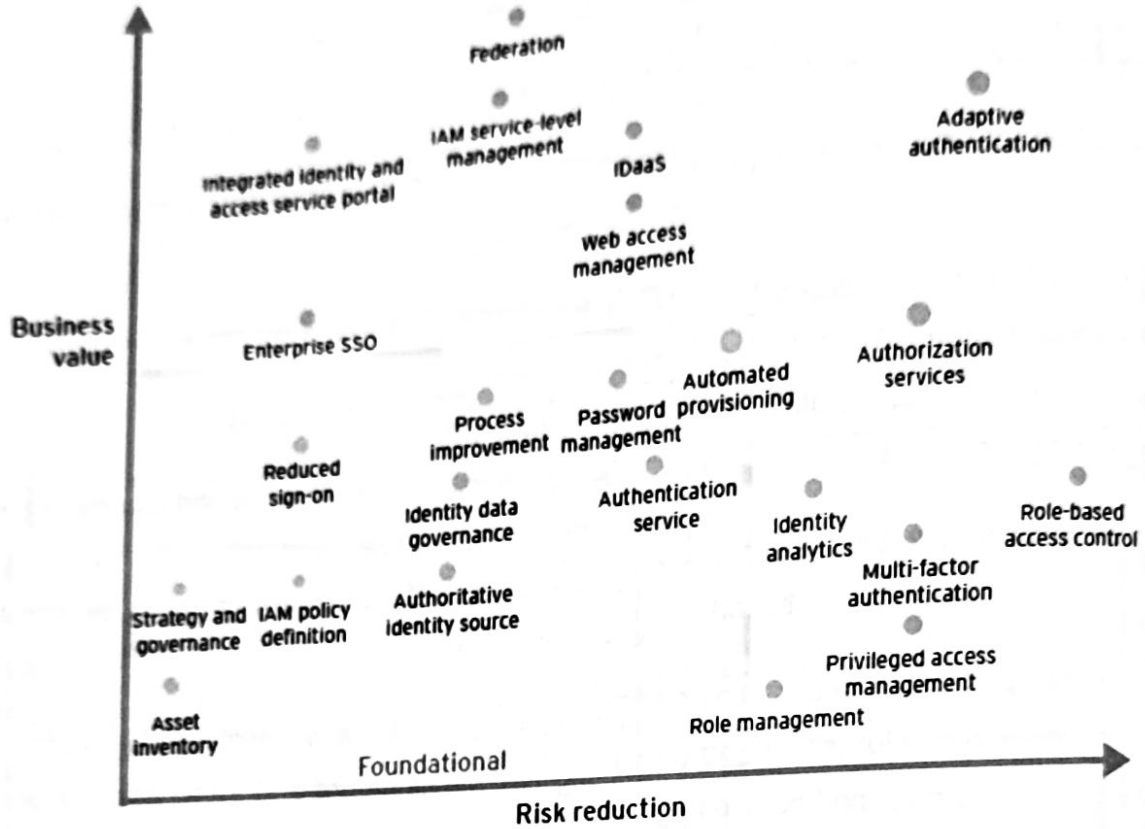
Life Cycle Phase	Technology Feature
User access request and approve	• Web-based self-service access requests • Approval processes capable of supporting risk-based approval paths, approver notifications, delegation, segregation of duties rules, and escalations for failure to approve within service-level agreements (SLAs) • Preapproved, automated access requests for "Day 1" access • Role-based access profiles to drive complex access provisioning downstream
Provision/ de-provision	• Authoritative identity source integration to detect hire, transfer and termination triggers • Configurable approval, provisioning and de-provisioning workflow, including automated escalation • Automated provisioning and de-provisioning of access to target systems using standard protocols or native

	application program interfaces (APIs) • Role-based access profile support • Policy-driven access control for web applications
Enforce	• Centralized directory services used for authentication and authorization • Web services-based authentication and authorization capabilities, including SAML (Security Assertion Mark-up Language) and XACML (eXtensible Access Control Mark-up Language) • Federated authentication and authorization services, which may be web-based
Report and audit	• Identity analytics capable of identifying high-risk user access and behavior profiles, rule- and exception-based access analysis and reporting, and continuous access monitoring and reporting. • Generation of IAM service management metric reports.
Review and certify	Configurable processes that support periodic, on-demand and user life cycle event-triggered access reviews — also referred to as attestations or certifications • The capability to tag access with risk ratings to support more frequent periodic access reviews for higher risk access • De-provisioning event generation to trigger revocation

	of access, which has been deemed inappropriate during access reviews
Reconcile	• Role- and rule-variance monitoring and reporting • High-risk user analysis (i.e., outlier analysis, behavior profiling) • Rules- and exception-based access analysis • Role and rule variance monitoring
Strategy and governance	• Role management, including role and rule mining, role definition reviews, role ownership dispositioning in response to user life cycle events, such as transfers and terminations • Governance, risk and compliance monitoring, including risk management and tracking, risk reporting dashboards, risk remediation plan tracking, data content and system configuration monitoring • IAM service management dashboards supporting KPIs and metric reports generated via reporting and auditing technology

Getting started

When determining how to transform your IAM program, the diagram below illustrates the common IAM areas classified by business value and risk reduction.



Key IAM capabilities

During the development of an IAM transformation plan, you should confirm that the following recommended capabilities are included:

- Job role or application access matrices using rule mining tools: this serves as the logical access foundation needed to embrace cloud-based and mobile applications in addition to ensuring appropriateness of access a key regulatory requirement, especially for data privacy.
- Automated workflow-based access request and approval processes, using job role or application access matrices and segregation of duties checking: this helps increase the consistency and efficiency of your IAM procedures and reduce the risk of inappropriate access.
- Entitlement warehouse solution: this accelerates the ability to address security and access management needs across a high volume of applications, host and database platforms within large organizations: it results in streamlined provisioning/ access attestation and provides a centralized view of access privileges across systems.
- Access proxy solutions, central authentication (application, host and database layers): this improves the end user experience and addresses key requirements around user de-provisioning.

- Risk-based authentication solutions: this addresses exposures related to compromise of basic authentication techniques, enables secure access for sensitive transactions (e.g., access to PII) and fulfills key regulatory requirements around multifactor authentication.
- Identity analytics and behavioral analysis services to integrate with DLP and security information and event management: this helps to enable behavior-based profiling, identifies access outliers for risk-based verification and effective reduction of insider risk. Context-aware identity and access intelligence solutions are being used to identify anomalous activities/exception-based access, perform account analysis, and execute oversight and monitoring functions, helping to protect data governed by privacy regulations.
- Data and access management process governance program, which includes HR, application owners, information security and IAM stakeholders: this helps to confirm that the appropriate people (i.e., departments, roles) are supporting and sponsoring the IAM program — vital to the success of process and technology changes.
- Federation solutions: this improves end user experience and management of identities for cloud-based applications.
- Consider emerging solutions that combine logical and physical security: these solutions will address business risks related to critical infrastructure protection.
- Design solution with future scalability requirements in mind: these access transformation initiatives are impacted by negative end user experience including performance delays; therefore, it is imperative to deploy solutions after considering future adoption and scalability requirements.

Conclusion

Effective identity and access management processes are integral to driving business value -reducing risk, sustaining compliance, improving the end user experience and responding to the changing IT landscape.

Your organization should first assess your existing IAM capabilities using the capability maturity model and then develop a risk-based action plan.

Here are some guidelines for success:

- Develop a strategy that is aligned to the needs of the business and considers people, processes and technology issues
- Don't think of IAM as an IT-only initiative, especially when it addresses business usage and regulatory requirements
- Be strategic, not tactical, when planning and designing a solution
- Because IAM is pervasive, be prepared for objections and concerns during any transformation process

- Avoid the "Big Bang" approach; use a risk-based, phased implementation approach to ease the integration and adoption of IAM changes
- Don't rush to buy and implement a tool without first considering the necessary business and process transformation requirements — tools do not guarantee enhancements in maturity
- Creating an inventory of applications, systems and definition of business friendly
- access roles (profiles) are critical activities to ensure success of an IAM program and will take longer than expected
- Don't expect 100% assignment of access through roles; start with enterprise-level roles first, then move to business-unit-level roles and allow for exceptions

Detention

Be it securing the Cloud or Performing Forensics in the Cloud We Are Experts

As cloud computing more frequently becomes the default mechanism for storing data, organizations and firms need to be cognizant of how best to secure their information. Moreover, Companies need to secure their data, to prevent harmful disclosure, and when a breach occurs, retain world class experts with substantial Cloud Computing expertise.

Law & Forensics team has an extensive background in forensics, with substantial expertise in Cloud Computing. Our team not only knows how to best manage information in the cloud, but how to manage a breach managing the daunting task of the needs of the business, legal, and technology stakeholders. We have assisted many companies bounce back after an enterprise data breach, in the Cloud or in the data center.

Law & Forensics teams have performed dozen of forensic investigations and security assessment of Cloud Computing platforms. Our services include:

- Informational sessions with specific departments within an organization or with all employees about proper protocol when storing information in a cloud.
- Advice on the structure of cloud contract accounting for potential forensic and security related issues.
- Comprehensive evaluation of available data-storage clouds, assessment of current cloud storage utilization and strategy for future use.
- Deliver critical guidance on how to respond and manage a data-breach from the legal and technical perspectives often collaborating with outside counsel, third-party technical consultants, and government agencies to quickly resolve the immediate problems and devise a long term remediation strategy.
- Create protocol for data stored in cloud server in case of e-discovery demands in litigation.

The adjectives commonly associated with clouds: vast, nebulous, and unruly, can also be used to describe the network "clouds" in cloud computing. When storing information, be it the files you use every day or confidential company e-mails and instant messages, these cloud-like qualities are troubling at best, and the root cause of a data leak at worst.

All of Law & Forensics' work reflects the highest ethical standards, no matter the scope of the task at hand. Our team frequently attends conferences, and participates in working groups and development committees to update and enhance standards and protocols. We consistently find new ways to serve our clients, and justice, better.

At Law and Forensics, we believe that at the bottom of every complex technology issue is a simple, cost-effective solution waiting to be *discovered*.

The benefits of cloud computing is well known: distributed and lean processing, resource and cost sharing, and faster integration of technology. On the other hand, some of the concerns regarding cloud computing includes digital forensics, information security, data jurisdiction, privacy and national law. For many, the benefits of migrating to the cloud outweigh these concerns, therefore the digital forensic community has started to focus on how to adapt current procedures towards cloud computing. This article focuses on the concerns or issues that a cloud computing environment presents to the digital forensic community and businesses.

When data is stored in a cloud computing environment, it is sectioned into single data structures, which in turn are divided into elements. This makes the process of identifying and acquiring data very difficult. Data that lacks preservation and integrity will prove difficult for digital forensic investigators who need to ensure data is comprehensive, inclusive and verifiable for use in criminal or corporate investigations – assuming the investigators are able to acquire the data in the first place.

The benefits that have made cloud computing so popular are reasons for concern for digital forensic investigators. First, the cloud is scalable, which means at one point or another, data from several businesses can occupy the same sectors within the storage media. This creates a dilemma during e-discovery, where the investigator could unknowingly acquire residual data from company X when company Y is being investigated.

The accessibility of data in terms of physical location and personnel access is something all organizations need to consider. If the data is stored in a country that does not recognize data privacy and security laws, or does not enforce existing laws, investigators could have a difficult time accessing the data to conduct their investigations. Also, not all data is stored in one location; a company could unknowingly be using cloud servers on several different continents. Even if the data is accessible, the jurisdiction of the data

could be in question. Investigators have to ask if they are even allowed to acquire and investigate data that is stored in a different country. Next, the location of the data, coupled with a lack of logging or use of anonymous authentication, could make it very difficult to establish and maintain an accurate chain of custody. This lack of integrity in the data will result in a failed investigation. Therefore, organizations have to be mindful of the contracts they sign with cloud providers, or chances are the physical location of their data will not be in the United States.

The digital forensic community is currently working toward creating new approaches for the extraction of digital evidence from cloud providers that will be admissible in court proceedings or corporate dispositions. This is not an easy task, and will take a considerable amount of time in order to obtain suitable results. Traditional computer forensics is not a feasible option; therefore researchers are looking at live forensics as a means of examining a cloud environment. The concerns of locating and identifying the data are proving to be quite challenging, and will take time to perfect. These challenges are in addition to the jurisdictional and chain of custody concerns. Researchers are beginning to analyze ways to show ownership of manipulated data, which will help with integrity issues. However, the jurisdictional concerns will be for the legal and governance communities to address.

As with any new technology, the benefits come with concerns, and cloud computing is no different. The cloud has allowed organizations to do more with less, but has created a challenging situation for the digital forensic world. Therefore, organizations need to be very diligent when entering into contracts with cloud service providers. They need to take the necessary steps to ensure they have access to their data should they encounter an event that needs digital forensics.

Field Acquisition & Analysis

Media Clone's Computer Forensic Field Acquisition & Analysis platform SuperImager™ Rugged 12in Unit is a very useful tool for field investigators. It is compact, rugged and easy to carry and achieves amazing data acquisition speeds and powerful computation. Assembled in the USA, it is equipped with four SAS/SATA ports and four USB3.0 ports which can be used in various combinations of storage devices and interfaces. The USB3.0 ports allow attaching a 12TB portable storage.

Users can chose to run multiple parallel operations, Capture (DD, E01/Ex01), Hash (SHA-1, SHA-2), and Drive Erase (DOD and Secure Erase). The application is designed to work with 12in LCD and touch screen, and it is a user friendly. Also includes support for saving forensic images to a network folder, acquiring data from an iSCSI drive and network. Data previewing can be done in-place.

The SI unit is a full blown PC with high end hardware, using the latest i5 4th generation technology; it allows users to run applications like: cell phone acquisition, full Encase or FTK analysis software, Triage software and many more.

Solid State Drives

SSD Architecture and Function Controllers, NAND non-volatile memory, and Program Erase Cycles (P/E) were discussed in Part 2. Pages, Blocks, Planes, Dies, TSOPs, Wear-Leveling (WL), and Garbage Collection (GC) were discussed in Part 3. Write Amplification (WA), Over-Provisioning (OP), and Bad Block Management (BBM) were discussed in Part 4.

Brief Discussion of Cylinders, Heads, and Sectors

Early traditional hard drives were supported by a PC's BIOS using Cylinder, Head, and Sector (CHS) addressing. Data was written using movable recording heads which were controlled via drive control commands. Once stored, the data could then easily be read by moving the heads over a particular cylinder. However, to read or write from a specific sector, that sector had to be specified in terms of its CHS. The combined limitations of the BIOS Int 13h routines and the IDE/ATA standard restricted the capacity of early hard drives to 504 MB (*1024 Cylinders * 63 Sectors per Track * 16 Heads * 512 Bytes per Sector = 528 Million Bytes or 504 MBs*). To circumvent the 504 MB size limit, Extended CHS addressing

was implemented. Although this added a translation step that changed the way the hard drive geometry appeared to the BIOS, CHS addressing was still used. Unfortunately this introduced another size limiting factor for hard drives, namely the 8 GB barrier [*1024 Cylinders * 63 Sectors per Track * 256 Heads * 512 Bytes per Sector = 8 GBs*).

Logical Block Addressing, and Physical Block Addressing

Logical Block Addressing (LBA) was developed to circumvent this issue and is now the method used with conventional hard drives to translate the CHS of the drive into addresses that can be used by an enhanced system BIOS. Instead of referring to CHS, each sector is assigned a unique "section number," starting at "0" and ending at "N-1" where "N" represents the number of sectors on the disc. (As an analogy, CHS can be considered as an individual's home address which is comprised of the street number, street name, city name, and state name. LBA would be analogous to every house in every state having a unique identifying number.) LBA itself is a run time function of a system's BIOS which uses LBA for commands such as reading, writing, format tracks, and so forth. Information pertaining to the hard drive's actual true geometry is stored in the system CMOS. LBA BIOS performs a translation from the traditional MS-DOS Track, Head, and Sector to the logical block numbers used by the drive.

Although they function totally differently, from the perspective of the host OS, an SSD appears similar to a conventional hard drive with rotating discs. The Logical to Physical Sector Block Address Translation Layer manages the placement of sectors. The SSD's Controller constantly writes new data or updates previous data to the first available free block which contains the least number of writes. This is to ensure that the number of write cycles per block is minimized, thereby maximizing the drive's longevity. Blocks containing old data are marked as "not in use" by the host OS. However, the data remains in the blocks until eventually erased by the GC function. The constant movement of data between blocks and pages can result in parts of any file being stored in any physical sector. The data's location, its Physical Block Address (PBA), must be tracked. To maintain organization, the Controller uses a mapping table to remap the LBA to the PBA. The table is referred to as the Logical to Physical Block Address Translation Table, or LBA–PBA Translation Table and has to be continually updated such that it can properly identify the correct address or location of data. As long as the index is changed when the data is physically moved, the data can still be located. (This is somewhat analogous to the function of the index of a book which points to the page number or location of a specific topic.) It is important to note that the physical location of any block will inevitably not match the external Logical Block Address.

"TRIM" Command

A traditional hard drive with an NTFS file system contains a Master File Table (MFT). The MFT is essentially an index file which maps everything on the hard drive. All file, directory, and metafile data (size, date and time stamp, data location, data content, permissions, etc.) is stored in MFT entries or in space outside the MFT that is described by MFT entries. When a user deletes a file, the file's MFT entry is marked as free and available for reuse. However, the actual disk space where the file is located is not

reallocated and the data is not deleted, removed, or relocated. Essentially, all the hard drive "knows" is that this space can be reused at some future time. When additional space is needed, the OS will send new data to that location, directly overwriting the old data.

This is not the case with an SSD. An SSD uses OP to improve its longevity and overall performance. However, at some point, an SSD can eventually fill up with both valid and invalid data which can reduce its OP functionality and its performance. NAND memory pages containing old or invalid data cannot be directly overwritten. Rather, they must first be erased at the block level using the Garbage Collection function. Unlike the traditional hard drive, an SSD does need to "know" what data is old or invalid so it can be moved and eventually deleted. The TRIM command (an innovation in storage architecture) is used by the OS to identify which addresses no longer hold valid data and which are available for clearing and re-use. The SSD then takes those addresses and updates the LBA–PBA Translation Table marking the addresses as invalid. During GC, the SSD does not move that invalid data. The net effect is a reduction in the number of write cycles and an increase of the SSD's longevity. This also provides additional space for OP. The contents of the blocks are not actually erased by the TRIM command, but rather it adds them to a queue of pending blocks which are eventually cleared by the GC function.

Chapter 5
Encryption and Decryption

Chapter 5 - Encryption and Decryption

Learning Objectives

What this chapter is about?

Overview of Encryption and Decryption

What you should be able to do?

- What is cryptography and how it works
- Overview of Digital Signatures and Hash Function
- Overview of PGP Certificates and X.509
- Overview of Trust Models
- Understanding SSL and its Process

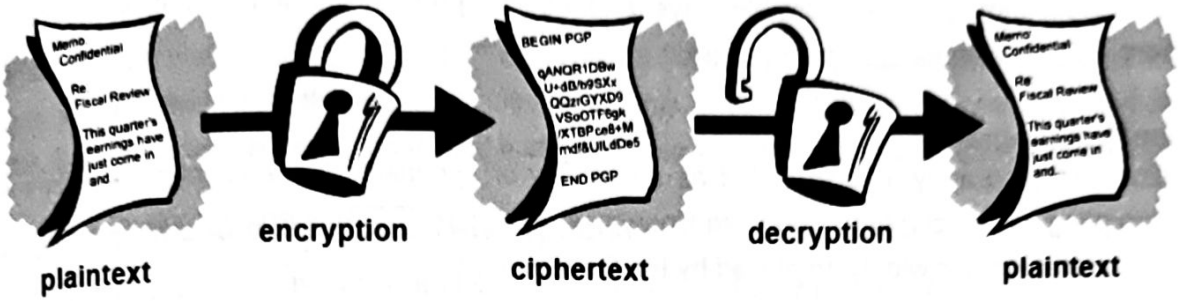
How will you check your progress?

Accountability:

- Checkpoint questions

Encryption and decryption

Data can be read and understood by without any special tools is called *plaintext* or *cleartext*. The method of disguising plaintext in such a way as to hide its substance is called *encryption*. Encrypting plaintext results in unreadable language is called *ciphertext*. You use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The method of reverting ciphertext to its original plaintext is called be *decryption*.



What is cryptography?

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive data or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

While cryptography is the method of securing data, *cryptanalysis* is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical calculations, pattern finding, patience, determination, and luck. Cryptanalysts are also called *attackers*.

Cryptology embraces both cryptography and cryptanalysis.

Strong cryptography

PGP is also about the latter sort of cryptography. Cryptography might be *strong* or *weak*, as explained. The strength of cryptography is measured in the time and resources it would require to recover the plaintext. The result of *strong cryptography* is ciphertext that is very difficult to decipher without possession of the appropriate decoding tool. How difficult? Given all of today's computing power and available time—even a millions and millions of computers doing a billion checks a second—it is not possible to decipher the result of strong cryptography before the end of the universe. One would think, then, that strong cryptography would hold up rather well against even an extremely determined cryptanalyst. Who's really to say? No one have proved that the strongest encryption obtainable today will hold up under tomorrow's computing power. However, the strong cryptography employed by PGP is the best available today. Vigilance and conservatism will protect you better, however, than claims of impenetrability.

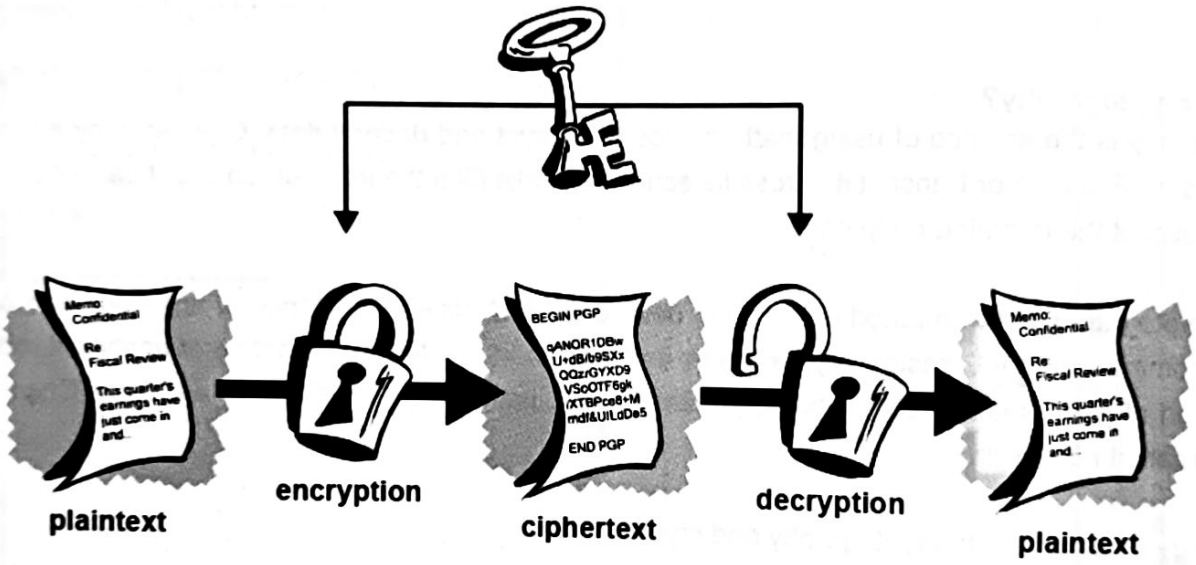
How does cryptography work?

A *cryptographic algorithm*, or *cipher*, is a mathematical functionality used in the encryption and decryption processing method. A cryptographic algorithm works in combination with a *key*—a word, number, or phrase—to encrypt the plaintext.

The same plaintext encrypts to different ciphertext with different key values. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the key secret. A cryptographic algorithm, plus all possible keys and all the protocols that make it work comprise a *cryptosystem*. PGP is a cryptosystem.

Conventional cryptography

In conventional cryptography, is also called as *secret-key* or *symmetric-key* encryption, one key is used both for encrypting and decrypting. The Data Encryption Standard (DES) is an example of a conventional cryptography system that is widely employed by the Government.



Caesar's Cipher

An simple example of conventional cryptography is a substitution cipher. A substitution cipher substitutes one piece of information for another. This is most frequently done by offsetting letters of the alphabet. Two examples are Captain Midnight's SecretDecoder Ring, which you may have owned when you were a kid, and Julius Caesar's cipher. In both cases, the algorithm is to offset the alphabet and the key is the number of characters to offset it.

For example, if we encode the word "SECRET" using Caesar's key value of 3, we offset the alphabet so that the 3rd letter down (D) begins the alphabet.

So starting with
ABCDEFGHIJKLMNOPQRSTUVWXYZ

and sliding everything up by 3, you get
DEFGHIJKLMNOPQRSTUVWXYZABC

where D=A, E=B, F=C, and so on.

Using this scheme, the plaintext, "SECRET" encrypts as "VHFUHW." To allow someone else to read the ciphertext, you tell them that the key is 3. Obviously, this is exceedingly weak cryptography by today's standards, but hey, it worked for Caesar, and it illustrates how conventional cryptography works.

Key management and conventional encryption

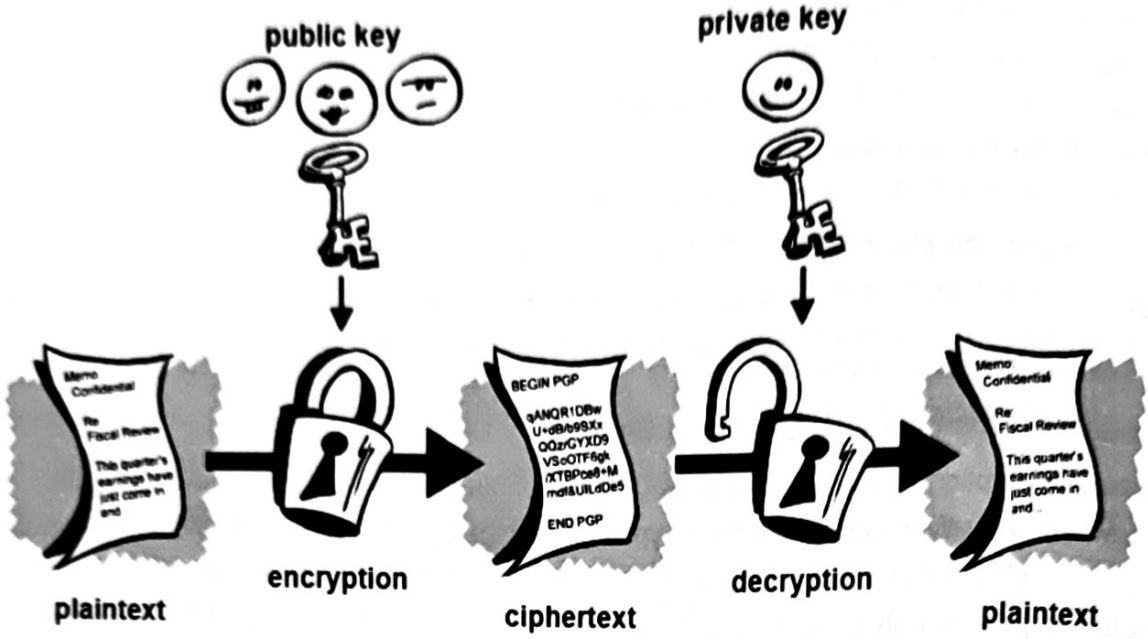
Conventional encryption has benefits. It is very fast. It is specifically useful for encrypting data that is not *going* anywhere. However, conventional encryption alone as a means for transmitting secure data can be quite expensive simply due to the difficulty of secure key distribution. Recall a character from your favorite spy movie: the person with a locked briefcase handcuffed to his or her wrist. What is in the briefcase, anyway? It's probably not the missile launch code/biotoxin formula/invasion plan itself. It's the *key* that will decrypt the secret data.

For a sender and recipient to communicate securely using conventional encryption, they should an agreement upon a key and keep it secret between themselves. If they were in different physical locations, they have to trust a courier, the Bat Phone, or some other secure communication medium to prevent the disclosure of the secret key during transmission. Anyone who overhears or intercepts the key in transit can later read, modify, and forge all information encrypted or authenticated with that key. From DES to Captain Midnight's Secret Decoder Ring, the persistent problem with conventional encryption is *key distribution*: how do you get the key to the recipient without someone
intercepting it?

Public key cryptography

The problems of key distribution are solved by *public key cryptography method* , the concept of which was introduced by Whitfield Diffie and Martin Hellman in 1975. (There are evidence that the British Secret Service invented it a few years before Diffie and Hellman, but kept it a military secret—and did nothing with it.)1 Public key cryptography is an asymmetric scheme that uses a *pair* of keys for encryption: a *public key*, which encrypts data, and a corresponding *private*, or *secret key* for decryption. You publish your public key to the world while keeping your private key secret. Anyone with a copy of your public key can then encrypt information that only you can read. Even people you have never met.

It is computationally infeasible to deduce the private key from the public key. Anyone who has a public key can encrypt information but cannot decrypt it. Only the person who has the corresponding private key can decrypt the information.

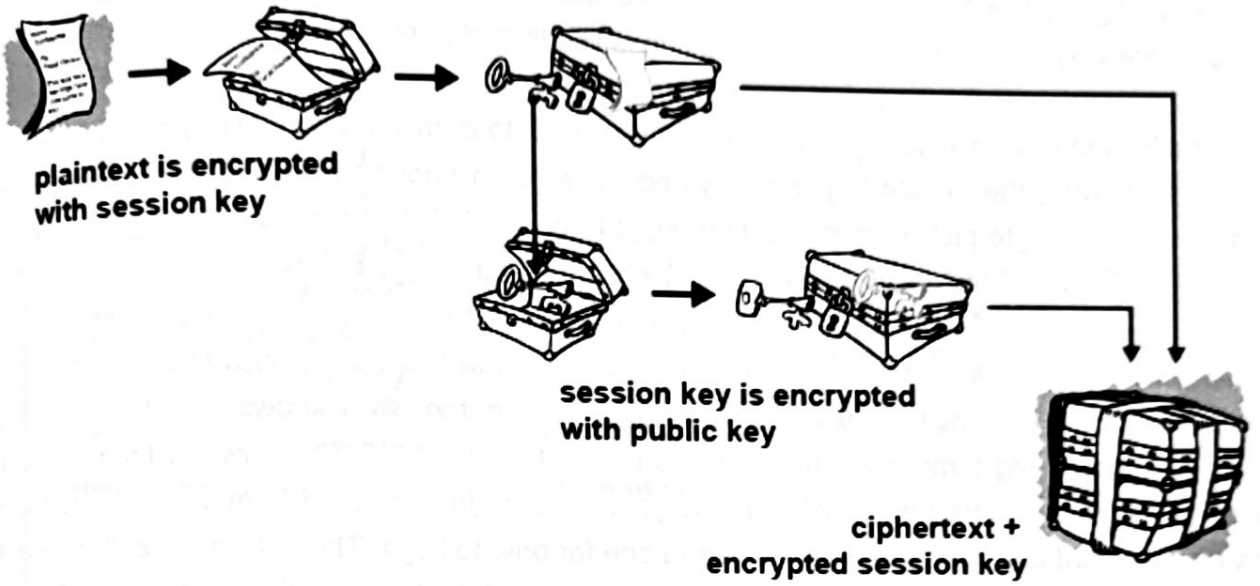


The benefit of having public key cryptography is that it allows people who have no preexisting security arrangement to exchange messages in secured manner. The need for sender and receiver to share secret keys via some secured channel is eliminated; all communications should involve only public keys, and no private key is ever transmitted or shared. Some examples of public-key cryptography systems are Elgamal (named for its inventor, Taher Elgamal), RSA (named for its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman), Diffie-Hellman (named, you guessed it, for its inventors), and DSA, the Digital Signature Algorithm (invented by David Kravitz). Because conventional cryptography was once the only available means for relaying secret information, the expense of secure channels and key distribution relegated its use only to those who could afford it, such as governments and large banks (or small children with secret decoder rings). Public key encryption is the technological revolution that provides strong cryptography to the adult masses. Remember the courier with the locked briefcase handcuffed to his wrist? Public-key encryption puts him out of business (probably to his relief).

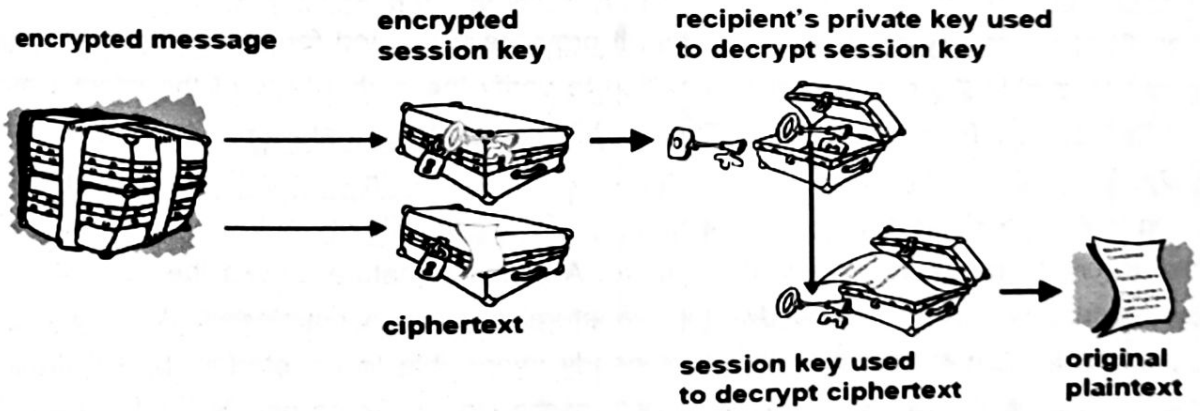
How PGP works

PGP combines some of the good features of both conventional and public key cryptography. PGP is a *hybrid cryptosystem.* When the user encrypts plaintext with PGP, PGP first compresses the plaintext. Data compression saves the bandwidth and transmitting time and disk space and, more importantly, it strengthens cryptographic security. Most cryptography techniques exploit patterns found in the plaintext to crack the cipher. Compression reduces these patterns in the plaintext, thereby greatly enhancing resistance to cryptanalysis. (Files that are too short to compress or which don't compress well aren't

compressed.) PGP then creates a *session key*, which is a one-time-only secret key. This key is a random number generated from the random movements of your mouse and the keystrokes you type. This session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is ciphertext. Once the data is encrypted, the session key is then encrypted to the recipient's public key. This public key-encrypted session key is transmitted along with the ciphertext to the recipient.



Decryption works in the reverse. The recipient's copy of PGP uses his or her private key to recover the temporary session key, which PGP then uses to decrypt the conventionally-encrypted ciphertext.



The combination of the two encryption methods combines the convenience of public key encryption with the speed of conventional encryption. Conventional encryption is about thousand times faster than public key encryption. Public key encryption in turn provides a solution to key distribution and data transmission issues. Used together, performance and key distribution are improved without any sacrifice in security.

Keys

A key is a value that works with a cryptographic algorithm to produce a specific ciphertext. Keys are basically really, really, really big numbers. Key size is measured in bits; the number representing a 1024-bit key is darn huge. In public key cryptography, the bigger the key, the more secure the ciphertext. However, public key size and conventional cryptography's secret key size are totally unrelated. A conventional 80-bit key has the equivalent strength of a 1024-bit public key. A conventional 128-bit key is equivalent to a 3000-bit public key. Again, the bigger the key, the more secure, but the algorithms used for each type of cryptography are very different and thus comparison is like that of apples to oranges.

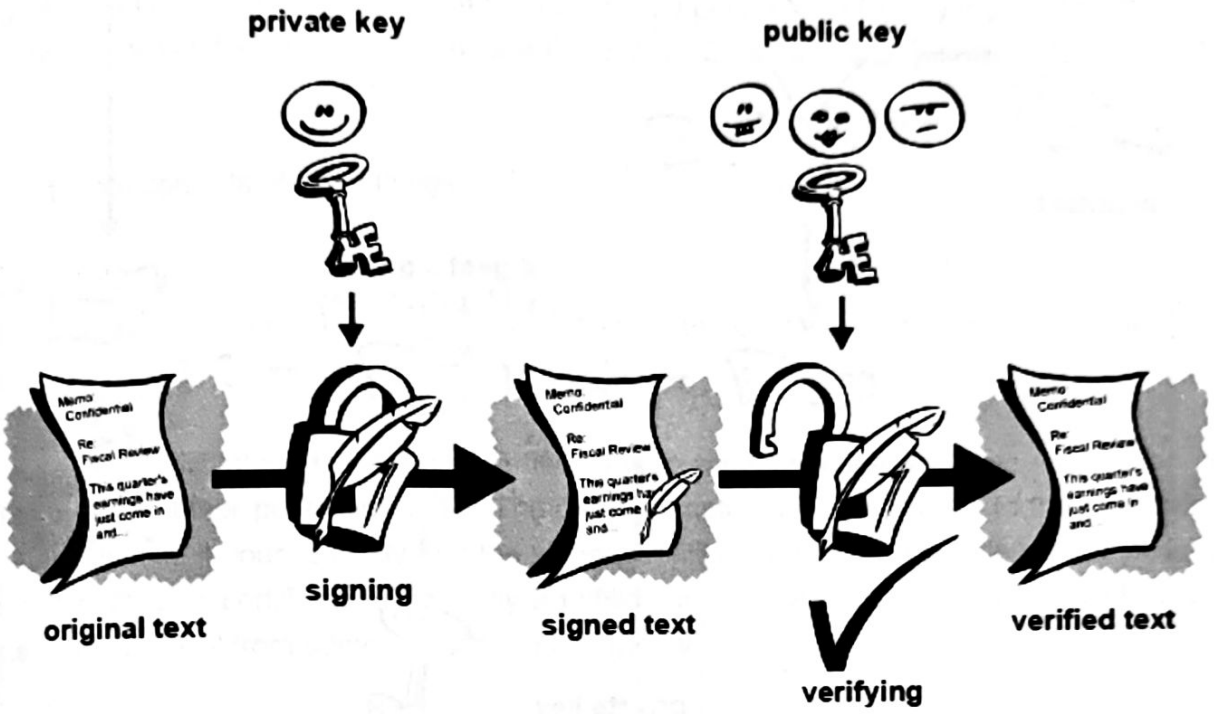
While the public and private keys are mathematically related, to derive the private key given only the public key; however, deriving the private key is always possible given enough time and computing power. This makes it very important to pick keys of the right size; large enough to be secure, but small enough to be applied fairly quickly. Additionally, you need to consider who might be trying to read your files, how determined they are, how much time they have, and what their resources might be. Larger keys will be cryptographically secure for a longer period of time. If what you want to encrypt needs to be hidden for many years, you might want to use a very large key. Of course, who knows how long it will take to determine your key using tomorrow's faster, more efficient computers? There was a time when a 56-bit symmetric key was considered extremely safe. Keys are stored in encrypted form. PGP stores the keys in two files on your hard disk; one for public keys and one for private keys. These files are called *keyrings*. As you use PGP, you will typically add the public keys of your recipients to your public key ring. Your private keys are stored on your private key ring. If you lose your private key ring, you will be unable to decrypt any information encrypted to keys on that ring.

Digital signatures

A major benefit of public key cryptography is that it provides a method for employing *digital signatures*. Digital signatures enable the recipient of information to verify the authenticity of the information's origin, and also verify that the information is intact. Thus, public key digital signature provides *authentication* and data *integrity*. A digital signature also provides *non-repudiation*, which means that it prevents the sender from claiming that he or she did not actually send the information. These features would be every bit as fundamental to cryptography as privacy, if not more. A digital signature serves the same purpose as a handwritten signature. However, a handwritten signature is easy to counterfeit. A digital signature is superior to a handwritten signature in that it is nearly impossible to counterfeit, plus it attests to the contents of the information as well as to the identity of the signer. Some people tend to use signatures more than they use encryption. For example, you may not care if anyone knows that you just deposited $500 in your account, but you do want to be darn sure it was the bank teller you were dealing with.

The basic method in which digital signatures are created Instead of encrypting information using someone

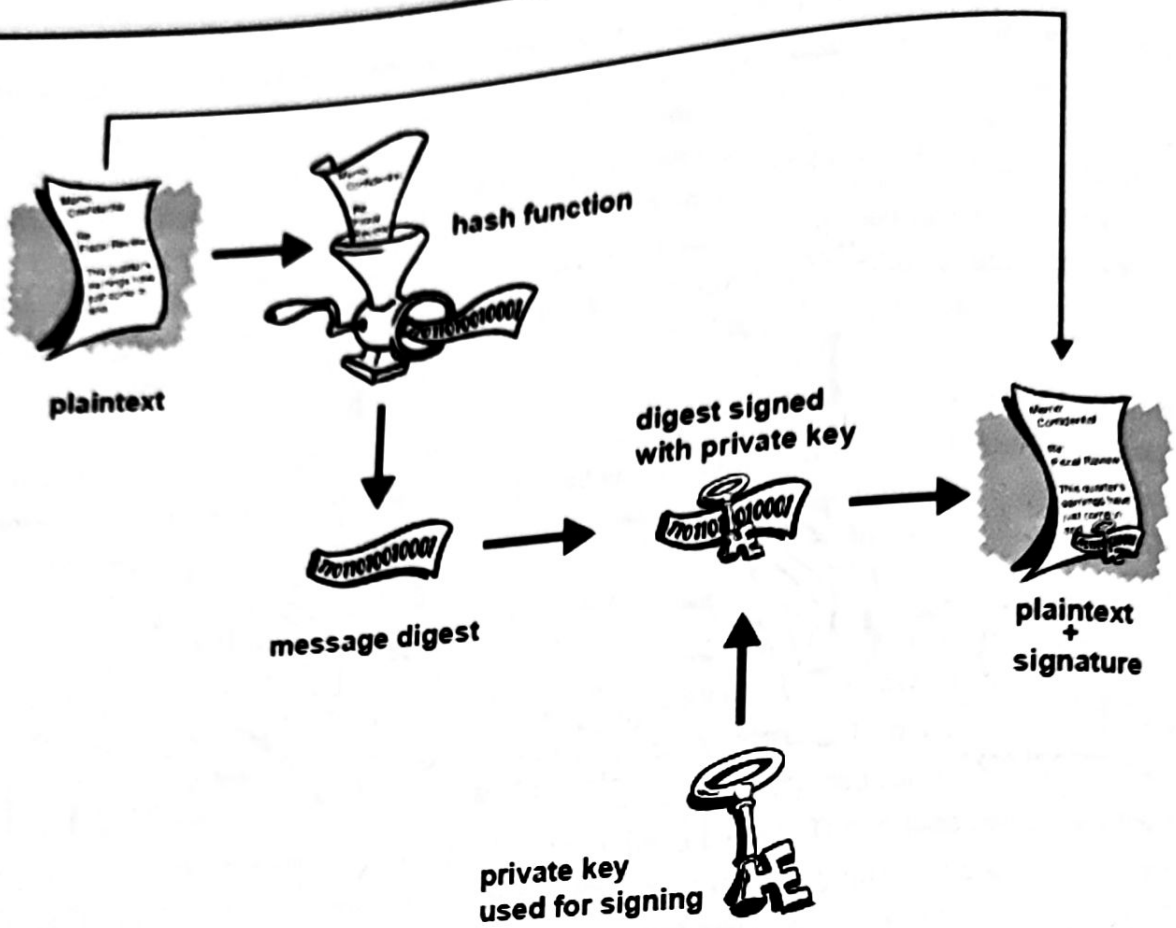
else's public key, you encrypt it with your private key. If the information can be decrypted with your public key, then it must have originated with you.



Hash functions

The system described above has some problems. It is slow, and it produces an large volume of data at least it should be double the size of the original information. An improvement on the above scheme is the addition of a one-way *hash function* in the process. A one-way hash function takes variable-length input in this case, a message of any length, even millions or billions of bits and produces a fixed-length output; say, 160-bits. The hash function makes sure that, if the information is changed or modified in any way even by just one bit or more it produce different value as output. PGP uses a cryptographically strong hash function on the plaintext when the user is signing. This generates a fixed-length data item known as a *message digest*. (Again, any change to the information results in a totally different digest.)

Then PGP uses the digest and the private key to create the "signature." PGP transmits the signature and the plaintext together. Upon receipt of the message, the recipient uses PGP to recompute the digest, thus verifying the signature. PGP can encrypt the plaintext or not; signing plaintext is useful if some of the recipients are not interested in or capable of verifying the signature. As long as a secure hash function is used, there is no way to take someone's signature from one document and attach it to another, or to alter a signed message in any way. The slightest change in a signed document will cause the digital signature verification process to fail.



Digital signatures play a major role in authenticating and *validating* other PGP users' keys.

Digital certificates

There is a problem with public key cryptography systems is that users must be constantly vigilant to ensure that they are encrypting to the correct person's key. In an network environment where it is safe to freely exchange keys via public servers, *man-in the-middle* attacks is a potential threat. In this type of attack, someone posts a phony key with the name and user ID of the user's intended recipient. Data encrypted to— and intercepted by—the real owner of this bogus key is now in the wrong hands.

In a public key environment, it is vital that you are assured that the public key to which you are encrypting data is in fact the public key of the intended recipient and not a forgery. You could simply encrypt only to those keys which have been physically handed to you. But suppose you need to exchange information with people you have never met; how can you tell that you have the correct key?

Digital certificates, or *certs*, simplify the task of establishing whether a public key truly belongs to the purported owner. A certificate is a form of credential. Examples might be your driver's license, your social security card, or your birth certificate. Each of these has some information on it identifying you and some

authorization stating that someone else has confirmed your identity. Some certificates, such as your passport, are important enough confirmation of your identity that you would not want to lose them, lest someone use them to impersonate you. A digital certificate is data that functions much like a physical certificate. A digital certificate is information included with a person's public key that helps others verify that a key is genuine or *valid*. Digital certificates are used to thwart attempts to substitute one person's key for another.

A digital certificate consists of three things:

- A public key.
- Certificate information. ("Identity" information about the user, such as name, user ID, and so on.)
- One or more digital signatures.

The purpose of the digital signature on a certificate is to state that the certificate information has been attested to by some other person or entity. The digital signature does not attest to the authenticity of the certificate as a whole; it vouches only that the signed identity information goes along with, or *is bound to*, the public key. Thus, a certificate is basically a public key with one or two forms of ID attached, plus a hearty stamp of approval from some other trusted individual.

Certificate distribution

Certificates are used when someone are necessary to exchange public keys . For small groups of people who wish to communicate in secure way, it is very easy to exchange diskettes or emails containing each own's public key manually. This is *manual public key distribution*, and it is practical only to a certain point of view. Beyond that point, it is necessary to put systems into place that can provide the necessary security, storage, and exchange mechanisms so coworkers, business partners, or strangers could communicate if need be. These can come in the form of storage-only repositories called *Certificate Servers*, or more complex systems that will provide additional key management features and are called *Public Key Infrastructures (PKIs)*.

Certificate servers

A *cert server* or a *key server*, also called as certificate server is a database that allows users will submit and retrieve digital certificates. A certificate server usually provides some administrative features that enable a company to maintain its security policies—for example, by allowing only those keys that meet certain requirements to be stored.

Public Key Infrastructures

A PKI that contains the certificate storage facilities of a certificate server, but also provides certificate management facilities (will issue, retrieve, revoke, store, and trust certificates). The main feature of a PKI is the intro of what is known as a *Certification Authority*, or *CA*, which is a human being a person, group,

department, company, or other associations that an organization has to issue authorized certificates to its system users. (ACA's role is analogous to a country's government's Passport Office.) A CA creates certificates and digitally signs them using the CA's private key. Because of its role in creating certificates, the CA is the central part of a PKI.Using the CA's public key, anyone wanting to verify a certificate's authenticity verifies the issuing CA's digital signature, and hence, the integrity of the contents of the certificate (most importantly, the public key and the identity of the certificate holder).

Certificate formats

A digital certificate is basically a collection of identifying information bound together with a public key and signed by a trusted third party to prove its authenticity. A digital certificate can be one of a number of different *formats*.

PGP recognizes two different certificate formats:

- PGP certificates
- X.509 certificates

PGP certificate format

A PGP certificate includes (but is not limited to) the following information:

- **The PGP version number**—this identifies which version of PGP was used to create the key associated with the certificate.
- **The certificate holder's public key**—the public portion of your key pair, together with the algorithm of the key: RSA, DH (Diffie-Hellman), or DSA (Digital Signature Algorithm).
- **The certificate holder's information**—this consists of "identity" information about the user, such as his or her name, user ID, photograph, and so on.
- **The digital signature of the certificate owner**—also called a *self-signature*, this is the signature using the corresponding private key of the public key associated with the certificate.
- **The certificate's validity period**—the certificate's start date/time and expiration date/time; indicates when the certificate will expire.
- **The preferred symmetric encryption algorithm for the key**—indicates the encryption algorithm to which the certificate owner prefers to have information encrypted. The supported algorithms are CAST, IDEA or Triple-DES. You might think of a PGP certificate as a public key with one or more labels tied to it On these 'labels' you'll find information identifying the owner of the key and a signature of the key's owner, which states that the key and the identification go together. (This particular signature is called a *self-signature*; every PGP certificate contains a self-signature.) One

unique aspect of the PGP certificate format is that a single certificate can contain multiple signatures. Several or many people may sign the key/identification pair to attest to their own assurance that the public key definitely belongs to the specified owner. If you look on a public certificate server, you may notice that certain certificates, such as that of PGP's creator, Phil Zimmermann, contain many signatures. Some PGP certificates consist of a public key with several labels, each of which contains a different means of identifying the key's owner (for example, the owner's name and corporate email account, the owner's nickname and home email account, a photograph of the owner—all in one certificate). The list of signatures of each of those identities may differ; signatures attest to the authenticity that one of the labels belongs to the public key, not that all the labels on the key are authentic. (Note that 'authentic' is in the eye of its beholder—signatures are opinions, and different people devote different levels of due diligence in checking authenticity before signing a key.)

X.509 certificate format

X.509 is another very common certificate format. All X.509 certificates .ITU-T X.509 comply with the international standard; thus (theoretically) X.509 certificates which is created for one application can be used by any other application complying with X.509. In practical, however, several companies have created their own extensions to X.509 certificates, not all of which work together. A certificate requires somebody to validate that a public key and the name of the key's owner go together. With PGP certificates, anyone can play the role of validator. With X.509 certificates, the validator is always a Certification Authority or someone designated by a CA. (Bear in mind that PGP certificates also fully support a hierarchical structure using a *CA* to validate certificates.) An X.509 certificate is a collection of a standard set of fields containing information about a user or device and their corresponding public key. The X.509 standard defines what information goes into the certificate, and describes how to encode it (the data format). All X.509 certificates have the following data:

- **The X.509 version number**—this identifies which version of the X.509 standard applies to this certificate, which affects what information, can be specified in it. The most current is version 3.
- **The certificate holder's public key**—the public key of the certificate holder, together with an algorithm identifier which specifies which cryptosystem the key belongs to and any associated key parameters.
- **The serial number of the certificate**—the entity (application or person) that created the certificate is responsible for assigning it a unique serial number to distinguish it from other certificates it issues. This information is used in numerous ways; for example when a certificate is revoked, its serial number is placed in a *Certificate Revocation List* or *CRL*.

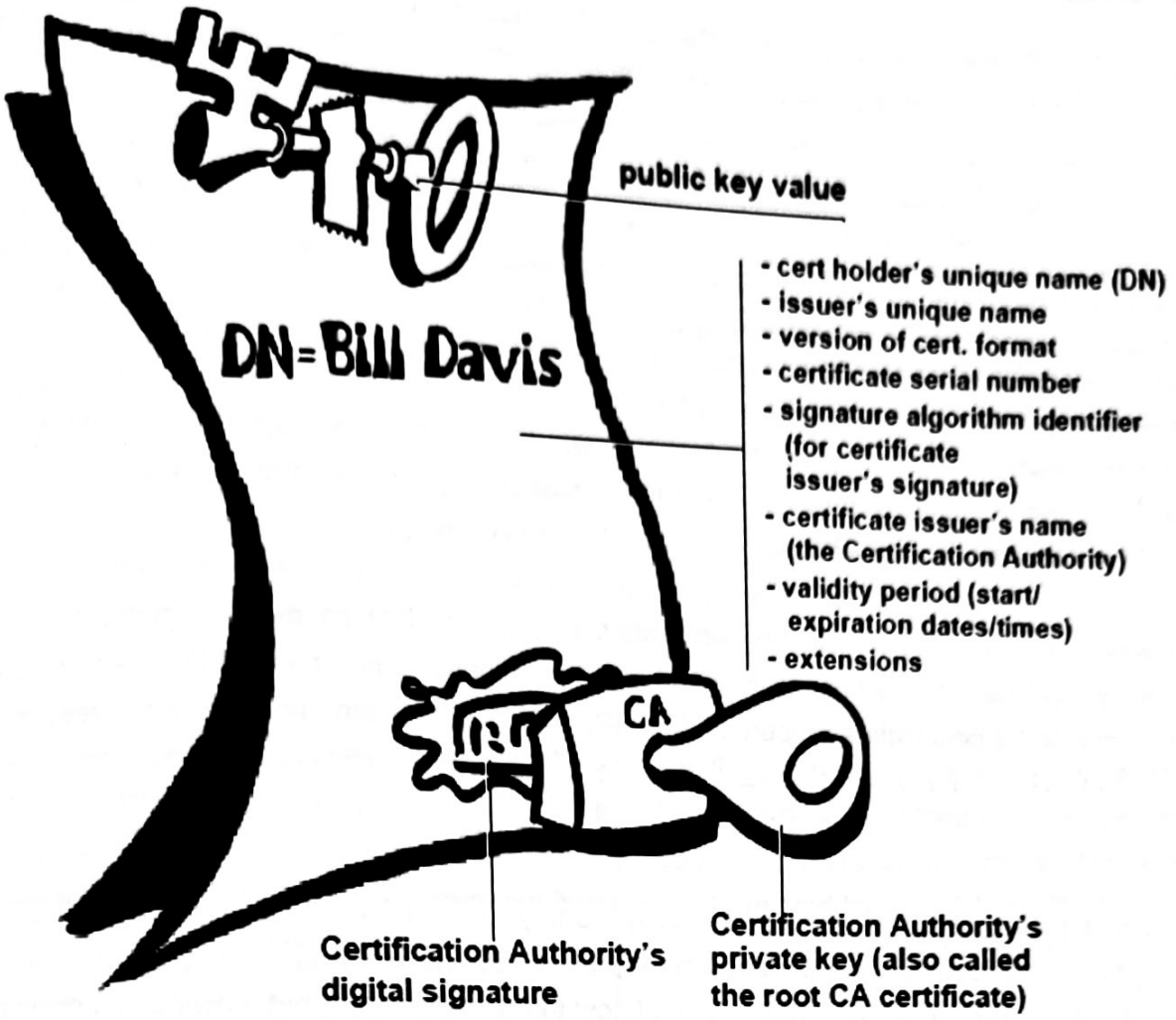
- **The certificate holder's unique identifier—** (or *DN—distinguished name*). This name is intended to be unique across the Internet. This name is intended to be unique across the Internet. A DN consists of multiple subsections and may look something like this:
  CN=Bob Allen, OU=Total Network Security Division, O=Network Associates, Inc., C=US (These refer to the subject's **C**ommon **N**ame, **O**rganizational **U**nit, **O**rganization and **C**ountry.)
- **The certificate's validity period**—the certificate's start date/time and expiration date/time; indicates when the certificate will expire.
- **The unique name of the certificate issuer**—the unique name of the entity that signed the certificate. This is normally a CA. Using the certificate implies trusting the entity that signed this certificate. (Note that in some cases, such as *root* or *top-level* CA certificates, the issuer signs its own certificate.)
- **The digital signature of the issuer**—the signature using the private key of the entity that issued the certificate.
- **The signature algorithm identifier**—identifies the algorithm used by the CA to sign the certificate.

There are many differences between an X.509 certificate and a PGP certificate, but the most salient are as follows:

- you can create your own PGP certificate; you must request and be issued an X.509 certificate from a Certification Authority
- X.509 certificates natively support only a single name for the key's owner
- X.509 certificates support only a single digital signature to attest to the key's validity

To get an X.509 certificate, you have to ask a CA to issue you a certificate. You provide your public key, proof that you possess the corresponding private key, and some specific information about yourself. You then digitally sign the information and send the whole package—the certificate *request*—to the CA. The CA then performs some due diligence in verifying that the information you provided is correct, and if so, generates the certificate and returns it.

You might think of an X.509 certificate as looking like a standard paper certificate (similar to one you might have received for completing a class in basic First Aid) with a public key taped to it. It has your name and some information about you on it, plus the signature of the person who issued it to you.



Validity and trust

Every user in a public key system is vulnerable to mistaking a phony key (certificate) for a real one. *Validity* is confidence that a public key certificate belongs to its purported owner. Validity is essential in a public key environment where you must constantly establish whether or not a particular certificate is authentic. When you've assured yourself that a certificate belonging to someone else is valid, you can sign the copy on your key ring to attest to the fact that you've checked the certificate and that it's an authentic one. If you want others to know that you gave the certificate your stamp of approval, you can export the signature to a certificate server so that others can see it.

As described in the section, "Public Key Infrastructures." some companies designate one or more Certification Authorities (CAs) to indicate certificate validity. In an organization using a PKI with X.509 certificates, it is the job of the CA to *issue* certificates to users—a process which generally entails

responding to a user's request for a certificate. In an organization using PGP certificates without a PKI, it is the job of the CA to check the authenticity of all PGP certificates and then sign the good ones. Basically, the main purpose of a CA is to bind a public key to the identification information contained in the certificate and thus assure third parties that some measure of care was taken to ensure that this binding of the identification information and key is valid. The CA is the Grand Pooh-bah of validation in an organization; someone whom everyone trusts, and in some organizations, like those using a PKI, no certificate is considered valid unless it has been signed by a trusted CA.

Checking validity

One way to establish validity is to go through some manual process. There are several ways to accomplish this. You could require your intended recipient to physically hand you a copy of his or her public key. But this is often inconvenient and inefficient.

Another way is to manually check the certificate's *fingerprint*. Just as every human's fingerprints are unique, every PGP certificate's fingerprint is unique. The fingerprint is a hash of the user's certificate and appears as one of the certificate's properties. In PGP, the fingerprint can appear as a hexadecimal number or a series of so-called *biometric words*, which are phonetically distinct and are used to make the fingerprint identification process a little easier.

You can check that a certificate is valid by calling the key's owner (so that you originate the transaction) and asking the owner to read his or her key's fingerprint to you and verifying that fingerprint against the one you believe to be the real one. This works if you know the owner's voice, but, how do you manually verify the identity of someone you don't know? Some people put the fingerprint of their key on their business cards for this very reason. Another way to establish validity of someone's certificate is to *trust* that a third individual has gone through the process of validating it. A CA, for example, is responsible for ensuring that prior to issuing to a certificate, he or she carefully checks it to be sure the public key portion really belongs to the purported owner. Anyone who trusts the CA will automatically consider any certificates signed by the CA to be valid. Another aspect of checking validity is to ensure that the certificate has not been revoked. For more information, see the section, "Certificate Revocation".

Establishing trust

You validate *certificates*. You trust *people*. More specifically, you trust people to validate other people' certificates. Typically, unless the owner hands you the certificate, you have to go by someone else's word that it is valid.

Meta and trusted introducers

In most situations, people completely trust the CA to establish certificates' validity. This means that everyone else relies upon the CA to go through the whole manual validation process for them. This is fine up to a certain number of users or number of work sites, and then it is not possible for the CA to maintain

the same level of quality validation. In that case, adding other validators to the system is necessary. A CA can also be a *meta-introducer*. A meta-introducer bestows not only validity on keys, but bestows the *ability to trust keys* upon others. Similar to the king who hands his seal to his trusted advisors so they can act on his authority, the meta-introducer enables others to act as *trusted introducers*. These trusted introducers can validate keys to the same effect as that of the meta-introducer. They cannot, however, create new trusted introducers. Meta-introducer and trusted introducer are PGP terms. In an X.509 environment, the meta-introducer is called the *root Certification Authority* (*root CA*) and trusted introducers *subordinate* Certification Authorities. The root CA uses the private key associated with a special certificate type called a *root CA certificate* to sign certificates. Any certificate signed by the root CA certificate is viewed as valid by any other certificate signed by the root. This validation process works even for certificates signed by other CAs in the system—as long as the root CA certificate signed the subordinate CA's certificate, any certificate signed by the CA is considered valid to others within the hierarchy. This process of checking back up through the system to see who signed whose certificate is called tracing a *certification path* or *certification chain*.

Trust models

In relatively closed systems, such as within a small company, it is easy to trace a certification path back to the root CA. However, users must often communicate with people outside of their corporate environment, including some whom they have never met, such as vendors, customers, clients, associates, and so on. Establishing a line of trust to those who have not been explicitly trusted by your CA is difficult. Companies follow one or another *trust model*, which dictates how users will go about establishing certificate validity.

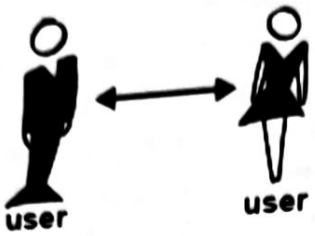
There are three different models:

- Direct Trust
- Hierarchical Trust
- A Web of Trust

Direct Trust

Direct trust is the simplest trust model. In this model, a user trusts that a key is valid because he or she knows where it came from. All cryptosystems use this form of trust in some way. For example, in web browsers, the root Certification Authority keys are directly trusted because they were shipped by the manufacturer. If there is any form of hierarchy, it extends from these directly trusted certificates.

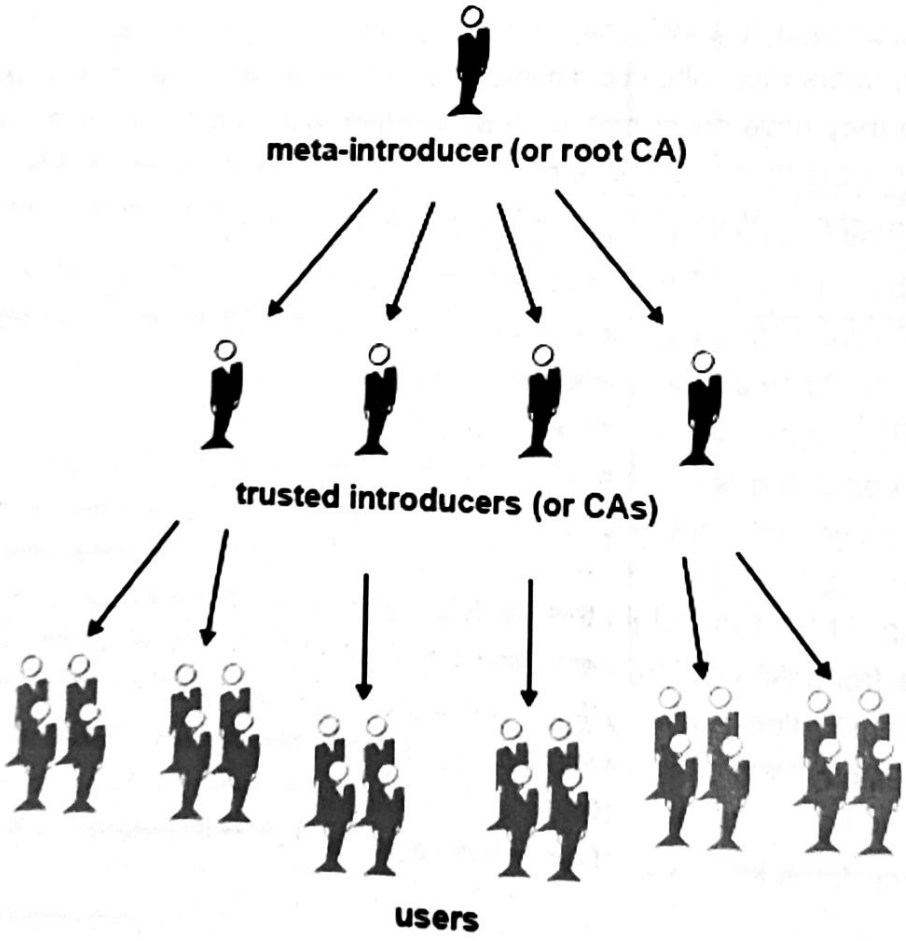
In PGP, a user who validates keys herself and never sets another certificate to be a trusted introducer is using direct trust.



Hierarchical Trust

In a hierarchical system, there are a number of "root" certificates from which trust extends. These certificates may certify certificates themselves, or they may certify certificates that certify still other certificates down some chain.

Consider it as a big trust "tree." The "leaf" certificate's validity is verified by tracing backward from its certifier, to other certifiers, until a directly trusted root certificate is found.



Web of Trust

A web of trust encompasses both of the other models, but also adds the notion that trust is in the eye of the beholder (which is the real-world view) and the idea that more information is better. It is thus a cumulative trust model. A certificate might be trusted directly, or trusted in some chain going back to a directly trusted root certificate (the meta-introducer), or by some group of introducers. Perhaps you've heard of the term *six degrees of separation*, which suggests that any person in the world can determine some link to any other person in the world using six or fewer other people as intermediaries. This is a web of introducers.

It is also the PGP view of trust. PGP uses digital signatures as its form of introduction. When any user signs another's key, he or she becomes an introducer of that key. As this process goes on, it establishes a *web of trust*. In a PGP environment, *any* user can act as a certifying authority. Any PGP user can validate another PGP user's public key certificate. However, such a certificate is only valid to another user if the relying party recognizes the validator as a trusted introducer. (That is, you trust my opinion that others' keys are valid only if you consider me to be a trusted introducer. Otherwise, my opinion on other keys' validity is moot.)

Stored on each user's public key ring are indicators of

- whether or not the user considers a particular key to be valid
- the level of trust the user places on the key that the key's owner can serve as certifier of others' keys

You indicate, on your copy of my key, whether you think my judgment counts. It's really a reputation system: certain people are reputed to give good signatures, and people trust them to attest to other keys' validity.

Levels of trust in PGP

The highest level of trust in a key, *implicit* trust, is trust in your own key pair. PGP assumes that if you own the private key, you must trust the actions of its related public key. Any keys signed by your implicitly trusted key are valid. There are three levels of trust you can assign to someone else's public key:

- Complete trust
- Marginal trust
- No trust (or *Untrusted*)

To make things confusing, there are also three levels of validity:

- Valid
- Marginally valid
- Invalid

To define another's key as a trusted introducer, you

1. Start with a valid key, one that is either
   - signed by you or
   - signed by another trusted introducer and then
2. Set the level of trust you feel the key's owner is entitled.
   For example, suppose your key ring contains Alice's key. You have validated Alice's key and you indicate this by signing it. You know that Alice is a real stickler for validating others' keys. You therefore assign her key with complete trust. This makes Alice a Certification Authority. If Alice signs another's key, it appears as Valid on your key ring. PGP requires one completely trusted signature or two marginally trusted signatures to establish a key as valid. PGP's method of considering two Marginal's equal to one Complete is similar to a merchant asking for two forms of ID. You might consider Alice fairly trustworthy and also consider Bob fairly trustworthy. Either one alone runs the risk of accidentally signing a counterfeit key, so you might not place complete trust in either one. However, the odds that both individuals signed the same phony key are probably small.

Certificate Revocation

Certificates are only useful while they are valid. It is unsafe to simply assume that a certificate is valid forever. In most organizations and in all PKIs, certificates have a restricted lifetime. This constrains the period in which a system is vulnerable should a certificate compromise occur. Certificates are thus created with a scheduled *validity period*: a start date/time and an expiration date/time. The certificate is expected to be usable for its entire validity period (its *lifetime*).When the certificate expires, it will no longer be valid, as the authenticity of its key/identification pair are no longer assured. (The certificate can still be safely used to reconfirm information that was encrypted or signed within the validity period—it should not be trusted for cryptographic tasks moving forward, however.)

There are also situations where it is necessary to invalidate a certificate prior to its expiration date, such as when an the certificate holder terminates employment with the company or suspects that the certificate's corresponding private key has been compromised. This is called *revocation*. A revoked certificate is *much*

more suspect than an expired certificate. Expired certificates are unusable, but do not carry the same threat of compromise as a revoked certificate. Anyone who has signed a certificate can revoke his or her signature on the certificate (provided he or she uses the same private key that created the signature).

Revoked signature indicates that the signer no longer believes the public key and identification information belong together, or that the certificate's public key (or corresponding private key) has been compromised. A revoked signature should carry nearly as much weight as a revoked certificate.

With X.509 certificates, a revoked signature is practically the same as a revoked certificate given that the only signature on the certificate is the one that made it valid in the first place—the signature of the CA. PGP certificates provide the added feature that you can revoke your entire certificate (not just the signatures on it) if you yourself feel that the certificate has been compromised.

Only the certificate's owner (the holder of its corresponding private key) or someone whom the certificate's owner has *designated* as a revoke can revoke a PGP certificate. (Designating a revoke is a useful practice, as it's often the loss of the passphrase for the certificate's corresponding private key that leads a PGP user to revoke his or her certificate—a task that is only possible if one has access to the private key.) Only the certificate's issuer can revoke an X.509 certificate.

Communicating that a certificate has been revoked

When a certificate is revoked, it is important to make potential users of the certificate aware that it is no longer valid. With PGP certificates, the most common way to communicate that a certificate has been revoked is to post it on a certificate server so others who may wish to communicate with you are warned not to use that public key.

In a PKI environment, communication of revoked certificates is most commonly achieved via a data structure called a *Certificate Revocation List*, or *CRL*, which is published by the CA. The CRL contains a time-stamped, validated list of all revoked, unexpired certificates in the system. Revoke certificates remain on the list only until they expire, then they are removed from the list—this keeps the list from getting too long.

The CA distributes the CRL to users at some regularly scheduled interval (and potentially off-cycle, whenever a certificate is revoked). Theoretically, this will prevent users from unwittingly using a compromised certificate. It is possible, though, that there may be a time period between CRLs in which a newly compromised certificate is used.

What is a passphrase?

Most people are familiar with restricting access to computer systems via a *password*, which is a unique string of characters that a user types in as an identification code. A *passphrase* is a longer version of a password, and in theory, a more secure one. Typically composed of multiple words, a passphrase is more secure against standard *dictionary attacks*, wherein the attacker tries all the words in the dictionary in an attempt to determine your password. The best passphrases are relatively long and complex and contain a combination of upper and lowercase letters, numeric and punctuation characters. PGP uses a passphrase to encrypt your private key on your machine. Your private key is encrypted on your disk using a hash of your passphrase as the secret key. You use the passphrase to decrypt and use your private key. A passphrase should be hard for you to forget and difficult for others to guess. It should be something already firmly embedded in your long-term memory, rather than something you make up from scratch. Why? Because **if you forget your passphrase, you are out of luck**. Your private key is totally and absolutely useless without your passphrase and nothing can be done about it. Remember the quote earlier in this chapter? PGP is cryptography that will keep major governments out of your files. Itwill certainly keep you out of your files, too. Keep that in mind when you decide to change your passphrase to the punchline of that joke you can never quite remember.

Key Splitting

They say that a secret is not a secret if it is known to more than one person. Sharing a private key pair poses such a problem. While it is not a recommended practice, sharing a private key pair is necessary at times. *Corporate Signing Keys*, for example, are private keys used by a company to sign—for example—legal documents, sensitive personnel information, or press releases to authenticate their origin. In such a case, it is worthwhile for Multiple members of the company to have access to the private key. However, this means that any single individual can act fully on behalf of the company. In such a case it is wise to *split* the key among multiple people in such a way that more than one or two people must present a piece of the key in order to reconstitute it to a usable condition. If too few pieces of the key are available, then the key is unusable. Some examples are to split a key into three pieces and require two of them tore constitute the key, or split it into two pieces and require both pieces. If a secure network connection is used during the reconstitution process, the key's shareholders need not be physically present in order to rejoin the key

Encryption

It is a critical security feature for all networks and home users. Encryption uses algorithms and mathematical schemes to scramble the data and makes it unreadable .Decrypting or decoding the data would require an associated key.

Data Encryption - Overview

Data Encryption provides the ability to encrypt data both for transmission over non-secure networks and for storage on media. The flexibility of key management schemes makes data encryption useful in a wide variety of configurations.

Encryption can be specified at following levels:

- Client level (for backup)
  - Client level encryption allows users to protect data prior to it leaving the computer. You can setup client level encryption if you need network security.
  - The data encryption keys are randomly generated per archive file.
- Client level (for backup)
  - Encryption for replication is specified on the Replication Set level, and applies to all of its Replication Pairs. For a given Replication Set, you can enable or disable encryption between the source and destination machines.
  - Replication Set level encryption encrypts data on the source computer, replicated across the network to the destination computer, and decrypted on the destination computer.
- Auxiliary Copy level (for copies)
  - Auxiliary Copy level encryption encrypts data during auxiliary copy operations enabling backup operations to run at full speed. If you are concerned that media may be misplaced, data can be encrypted before writing it to the media and keys stored in the CommServe database. In this way, recovery of the data without the CommServe is impossible - not even with Media Explorer.
  - Here, data encryption keys are generated per storage policy copy of the archive file. Thus, if there are multiple copies in a storage policy, the same archive files in each copy gets a different encryption key. Individual archive files, however, will have different encryption keys.
- Hardware level (all data)
  - Hardware Encryption allows you to encrypt media used in drives with built-in encryption capabilities, which provides considerably faster performance than data or auxiliary copy encryption. The data encryption keys are generated per chunk on the media. Each chunk will have a different encryption key.

Symmetric Encryption and Asymmetric encryption

Introduction

This article explains how symmetric and asymmetric encryption work. It also describes how to build a secure mail system using these two types of encryption.

Symmetric Encryption

Let's assume that Alice wants to talk to Bob. She wants to keep the message secret. Bob is the only one who should be able to read the message. The message is confidential, so Alice uses a key to encrypt the message. The original message is called a plaintext while the encrypted message is called a ciphertext. The ciphertext is sent to Bob, who knows the key and uses the same symmetric cipher (e.g., AES or 3DES). Thus Bob is able to decrypt the message.

Alice and Bob share the key, which is called symmetric. They are the only ones who know the key and no one else is able to read the encrypted message. This way, confidentiality is achieved.

Key Length vs. Security

The key space doubles when one bit is added to the key. Longer keys are better, but don't necessarily increase security. Because people tend to use patterns for passwords, the attacker can build a dictionary of commonly used passwords and launch a dictionary attack. This way the attacker can save time, because he doesn't have to brute force the whole key space.

Symmetric vs. Session Key

The symmetric key can be changed every time Alice communicates with Bob. Then it is called a session key (randomly generated and valid only for one session). If an attacker grabs the session key, he can decrypt only the messages from one session. If Alice and Bob always used the same key, the attacker would be able to decrypt all messages encrypted with this key.

Scalability and Secure Key Distribution

There are a few problems with symmetric ciphers. This system is not scalable. If there are 1,000 people who want to communicate with each other, everyone needs 999 different keys to establish separate and confidential communication channels. Secure key distribution is another problem. The security of the system is broken if a man-in-the-middle can grab the key while it is being transmitted from Alice to Bob.

Asymmetric Encryption

Two keys are used in asymmetric cipher (e.g., RSA)—a public and a private one. The public one is available for everyone, but the private one is known only by the owner. When the message is encrypted

with the public key, only the corresponding private key can decrypt it. Moreover, the private key can't be learned from the public one.

Asymmetric cipher solves the problem of secure key distribution. Alice takes Bob's public key and uses it to encrypt the session key. Only Bob can then decrypt the encrypted session key, because he is the only one who knows the corresponding private key. Asymmetric ciphers are quite slow when compared with the symmetric ones, which is why asymmetric ciphers are used only to securely distribute the key. Then, Alice and Bob can use symmetric cipher and the session key to make the communication confidential.

Use of an asymmetric cipher also solves the scalability problem. Everyone will need only one public key and one private key to communicate with other people.

Mail Security

Let's analyze how symmetric and asymmetric encryption can be used to build secure mail system.

Achieving Message Confidentiality

Alice is going to send a mail to Bob. She wants to keep the message secret. Bob is the only one who should be able to read the message. Confidentiality can be achieved by using symmetric encryption. The key used for symmetric encryption (the session key) needs to be securely sent to Bob. Asymmetric encryption is used for the purpose of secure key distribution.

Let's analyze this process step by step. Alice generates a session key (SESSION_KEY) and encrypts it with Bob's public key (PUB_KEY_BOB). The result is PUB_KEY_BOB (SESSION_KEY), which is denoted by PART1. Then the message (MESSAGE) is encrypted with SESSION_KEY. The result is SESSION_KEY(MESSAGE), which is denoted by PART2. Finally PART1 and PART2 are sent to Bob. Only Bob can decrypt PART1, because he is the only one who knows the corresponding private key (PRIV_KEY_BOB). Bob decrypts PART1 and gets the SESSION_KEY. Then he uses SESSION_KEY to decrypt PART2 and get the MESSAGE.

Achieving Message Confidentiality, Integrity, and Authentication of the Sender

Let's discuss a more complicated case. Alice is going to send a mail to Bob. Bob wants to verify the sender of the message and check whether its integrity is preserved. Moreover, the message should be kept secret. Bob is the only one who should be able to read the message.

Let's analyze this process step by step. Alice generates a session key (SESSION_KEY) and encrypts it with Bob's public key (PUB_KEY_BOB). The result is PUB_KEY_BOB (SESSION_KEY), which is denoted by PART1.

The message (MESSAGE) is hashed by Alice. The result is H(MESSAGE). The ideal hash function is irreversible (one can't get the message from the hash) and there are no two different messages MESSAGE1 and MESSAGE2 having the same hash. Then H(MESSAGE) is encrypted with the private key of Alice (PRIV_KEY_ALICE). The result is PRIV_KEY_ALICE(H(MESSAGE)), which is a digital signature of MESSAGE signed by Alice and is denoted by DIGITAL_SIGNATURE.

MESSAGE and DIGITAL_SIGNATURE are encrypted with SESSION_KEY. The result is SESSION_KEY(MESSAGE concatenated with DIGITAL SIGNATURE), which is denoted by PART2. Finally PART1 and PART2 are sent to Bob. Only Bob can decrypt PART1, because he is the only one who knows the corresponding private key (PRIV_KEY_BOB). Bob decrypts PART1 and gets the SESSION_KEY. Then he uses SESSION_KEY to decrypt PART2 and gets MESSAGE concatenated with DIGITAL SIGNATURE.

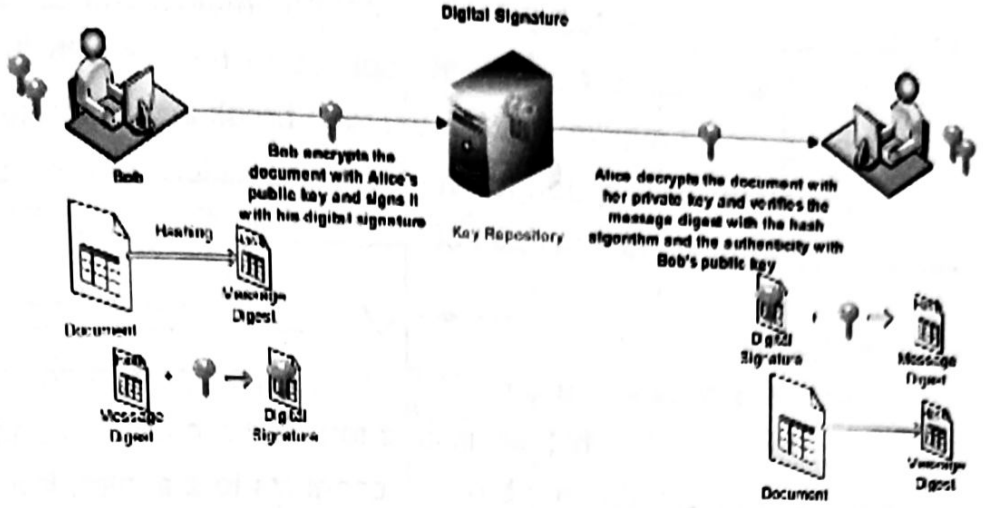
Bob uses Alice's public key (PUB_KEY_ALICE) to decrypt DIGITAL_SIGNATURE. The result of decryption is H(MESSAGE). Then Bob calculates hash of MESSAGE and compares the result with decrypted DIGITAL_SIGNATURE. When they match, Bob knows that it was Alice who sent the message and exactly what message was sent by Alice.

Conclusions

- Symmetric encryption is used to provide confidentiality of the message.
- Asymmetric encryption is used to securely distribute the session key.
- Asymmetric encryption solves the scalability problem related with symmetric encryption .

Digital signature

In order to prove that the document is sent by John to Harry, John needs to use a digital signature. Using a digital signature means applying the sender's private key to the message, or document, or to the message digest. This process is known as as signing. Only by using the sender's public key can the message be decrypted.



John will encrypt the message digest with his private key to create a digital signature. In the scenario illustrated in the image above, John will encrypt the document using Harry's public key and sign it using his digital signature. This ensures that Harry can verify that the document is sent by John, by verifying the digital signature (John's private key) using John's public key. Remember a private key and the corresponding public key are linked, albeit mathematically. Harry can also verify that the document is not altered by validating the message digest, and also can open the encrypted document using his private key. Message authentication is a procedure that facilitates to verify authenticity and integrity of the message and the source from where it is received. A certificate can also be used to uniquely identify the holder.

Secure Sockets Layer (SSL)

What Happens When a Browser Encounters SSL

1. A browser attempts to connect to a website secured with SSL.
2. The **browser** requests that the web server identify itself.
3. The **server** sends the browser a copy of its SSL Certificate.
4. The **browser** checks whether it trusts the SSL Certificate. If so, it sends a message to the server.
5. The **server** sends back a digitally signed acknowledgement to start an SSL encrypted session.
6. **Encrypted data is shared between the browser and the server and** https **appears.**

Encryption Protects Data During Transmission

Web servers and web browsers rely on the Secure Sockets Layer (SSL) protocol to help users protect their data during transfer by creating a uniquely **encrypted** channel for private communications over the public Internet. Each SSL Certificate consists of a **key pair as well as verified identification information**. When a web browser (or client) points to a secured website, the server shares the public key with the client to establish an **encryption** method and a unique session key. The client confirms that it recognizes and trusts the issuer of the SSL Certificate. This process is known as the "SSL handshake" and it begins a secure session that protects message privacy, message integrity, and **server security**

Strong **encryption**, at 128 bits, can calculate 288 times as many combinations as 40-bit **encryption**. **That's over a trillion times stronger.** At current computing speeds, a hacker with the time, tools, and motivation to attack using brute force would require a trillion years to break into a session protected by an SGC-enabled certificate. To enable strong **encryption** for the most site visitors, choose an SSL Certificate that enables 128-bit minimum **encryption** for 99.9 percent of website visitors.

Credentials Establish Identity Online

Credentials for establishing identity are common: a driver's license, a passport, a company badge. SSL Certificates are credentials for the online world, uniquely issued to a specific domain and web server and authenticated by the SSL Certificate provider. When a browser connects to a server, the server sends the identification information to the browser.

To view a websites' credentials:

- Click the closed padlock in a browser window
- Click the trust mark (such as a Norton Secured Seal)
- Look in the green address bar triggered by an Extended Validation (EV) SSL

Authentication Generates Trust in Credentials

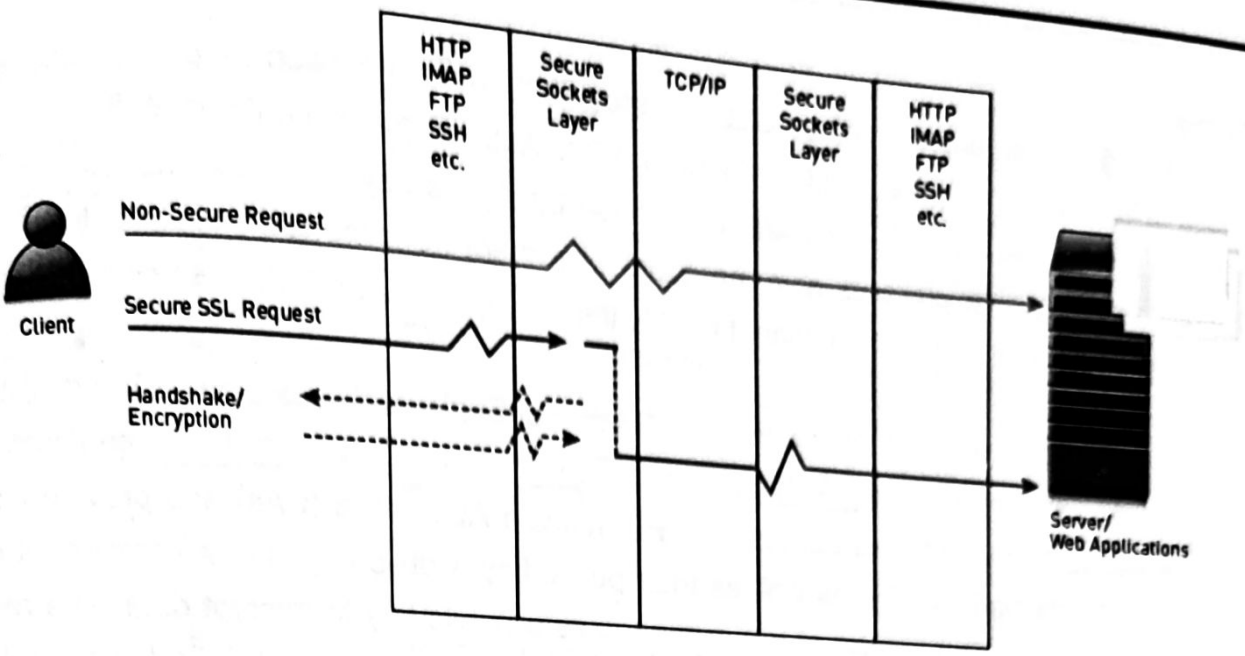
Trust of a credential depends on confidence in the credential issuer, because the issuer vouches for the credential's authenticity. **Certification Authorities** use a variety of authentication methods to verify information provided by organizations. Symantec, the leading Certification Authority, is well known and trusted by browser vendors because of our rigorous authentication methods and highly reliable infrastructure. Browsers extend that trust to SSL Certificates issued by Symantec.

Extend Protection beyond HTTPS

Symantec SSL Certificates offer more services to protect your site and grow your online business. Our combination of SSL, vulnerability assessment and daily website malware scanning helps you provide site visitors with a safer online experience and extend **server security** beyond **https** to your public-facing web pages. The Norton Secured Seal and Symantec Seal-in-Search technology help assure your customers that your site is safe from search to browse to buy

Understanding SSL

Regardless of where you access the Internet from, the connection between your Web browser and any other point can be routed through dozens of independent systems. Through snooping, spoofing, and other forms of Internet eavesdropping, unauthorized people can steal credit card numbers, PIN numbers, personal data, and other confidential information.



The Secure Sockets Layer (SSL) protocol was developed to transfer information privately and securely across the Internet. SSL is layered beneath application protocols such as HTTP, SMTP, and FTP and above the connection protocol TCP/IP. It is used by the HTTPS access method. Figure 1 illustrates the difference between a non-secure HTTP request and a secure SSL request. Transport Layer Security (TLS) is the successor of Secure Sockets Layer (SSL); they are both cryptographic protocols that provide secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, instant messaging, and other data transfers. There are slight differences between SSL and TLS, but the protocol remains substantially the same.

Who Uses SSL?

SSL is the de facto standard for encrypted and authenticated communications between clients and servers on the Internet. Virtually all online purchases and browser-based monetary transactions that occur on the Internet are secured by SSL. However, SSL is not just limited to securing e-commerce transactions; the following are a few other examples of SSL use:

- Financial institutions implement SSL to secure the transmission of PIN numbers and other confidential account information.
- Insurance companies implement SSL to secure transmission of confidential policy information.
- Organizations who have established Business-to-Business (B2B) extranets implement SSL to secure transactions between the company and its partners, suppliers, and customers.
- Private organizations implement SSL in their intranets to confidentially transfer information to and from employees.
- Email providers implement SSL to secure webmail for users.

How It Works

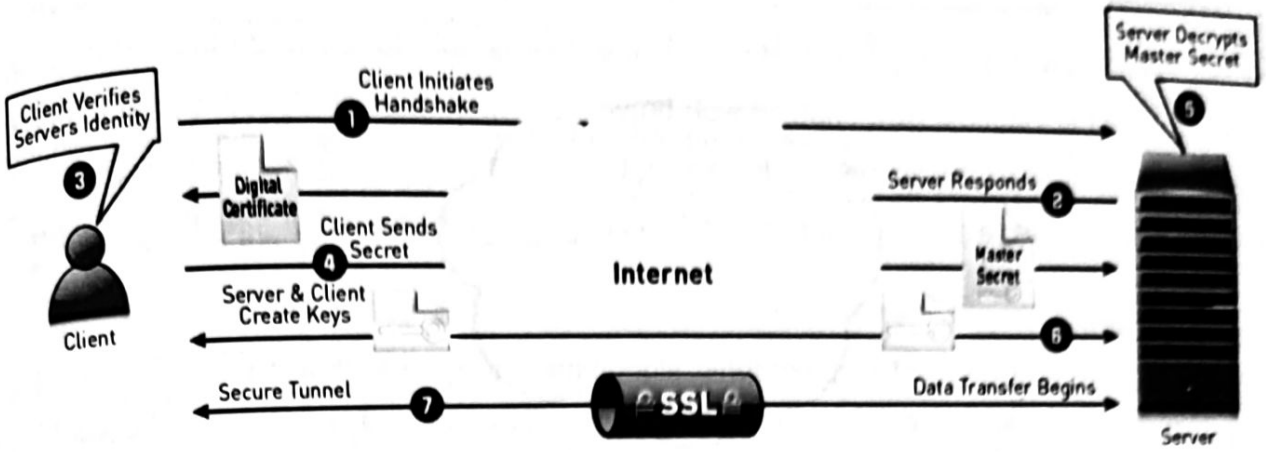
When a client and server communicate, SSL ensures that the connection is private and secure by providing authentication, encryption, and integrity checks. Authentication confirms that the server, and optionally the client, is who they say they are. Encryption through a key-exchange then creates a secure "tunnel" between the two that prevents any unauthorized system from reading the data. Integrity checks guarantee that any unauthorized system cannot modify the encrypted stream without being detected.

SSL-enabled clients (such as a Mozilla™ or Microsoft Internet Explorer™ web browser) and SSL-enabled servers (such as Apache or Microsoft IIS™) confirm each other's identities using digital certificates. Digital certificates are issued by trusted third parties called Certificate Authorities (CAs) and provide information about an individual's claimed identity, as well as their public key. Public keys are a component of public-key cryptographic systems. The sender of a message uses a public key to encrypt data. The recipient of the message can only decrypt the data with the corresponding private key. Public keys are known to everybody; private keys are secret and only known to the owner of the certificate. By validating the CA digital signature on the certificates, both parties can ensure that an imposter has not intercepted the transmission and provided a false public key for which they have the correct private key. SSL uses both public-key and symmetric key encryption. Symmetric key encryption is much faster than public-key encryption, but public-key encryption provides better authentication techniques. So SSL uses public key cryptography for authentication and for exchanging the symmetric keys that are used later for bulk data encryption.

The secure tunnel that SSL creates is an encrypted connection that ensures that all information sent between an SSL-enabled client and an SSL-enabled server remains private. SSL also provides a mechanism for detecting if someone has altered the data in transit. This is done with the help of message integrity checks. These message integrity checks ensure that the connection is reliable. If, at any point during a transmission, SSL detects that a connection is not secure, it terminates the connection and the client and server establish a new secure connection.

SSL Transactions

The SSL transaction has two phases: the SSL Handshake (the key exchange) and the SSL data transfer. These phases work together to secure an SSL transaction.



1. The handshake begins when a client connects to an SSL-enabled server, requests a secure connection, and presents a list of supported ciphers and versions.
2. From this list, the server picks the strongest cipher and hash function that it also supports and notifies the client of the decision.

Additionally, the server sends back its identification in the form of a digital certificate. The certificate usually contains the server name, the trusted certificate authority (CA), and the server's public encryption key. The server may require client authentication via a signed certificate as well (required for some on-line banking operations); however, many organizations choose not to widely deploy client-side certificates due to the overhead involved in managing a public key infrastructure (PKI).

3. The client verifies that the certificate is valid and that a Certificate Authority (CA) listed in the client's list of trusted CAs issued it. These CA certificates are typically locally configured.
4. If it determines that the certificate is valid, the client generates a master secret, encrypts it with the server's public key, and sends the result to the server. When the server receives the master secret, it decrypts it with its private key. Only the server can decrypt it using its private key.

5. The client and server then convert the master secret to a set of symmetric keys called a keyring or the session keys. These symmetric keys are common keys that the server and browser can use to encrypt and decrypt data. This is the one fact that makes the keys hidden from third parties, since only the server and the client have access to the private keys.

6. This concludes the handshake and begins the secured connection allowing the bulk data transfer, which is encrypted and decrypted with the keys until the connection closes. If any one of the above steps fails, the SSL handshake fails, and the connection is not created. Though the authentication and

encryption process may seem rather involved, it happens in less than a second. Generally, the user does not even know it is taking place. However, the user is able to tell when the secure tunnel has been established since most SSL-enabled web browsers display a small closed lock at the bottom (or top) of their screen when the connection is secure. Users can also identify secure web sites by looking at the web site address; a secure web site's address begins with **https** rather than the usual **http**.

SSL Crypto Algorithms

SSL supports a variety of different cryptographic algorithms, or ciphers, that it uses for authentication, transmission of certificates, and establishing session keys. SSL-enabled devices can be configured to support different sets of ciphers, called cipher suites. If an SSL-enabled client and an SSL-enabled server support multiple cipher suites, the client and server negotiate which cipher suites they use to provide the strongest possible security supported by both parties. A cipher suite specifies and controls the various cryptographic algorithms used during the SSL handshake and the data transfer phases. Specifically, a cipher suite provides the following:

Key exchange algorithm: The asymmetric key algorithm used to exchange the symmetric key. RSA and Diffie Hellman are common examples.

Public key algorithm: The asymmetric key algorithm used for authentication. This decides the type of certificates used. RSA and DSA are common examples.

Bulk encryption algorithm: The symmetric algorithm used for encrypting data. RC4, AES, and Triple-DES are common examples.

Message digest algorithm: The algorithm used to perform integrity checks. MD5 and SHA-1 are common examples.

For instance the cipher suite "RSA-RC4-MD5" means that RSA certificates are used for both authentication and key exchange, while RC4 is used as the bulk encryption cipher, and MD5 is used for digest computation.

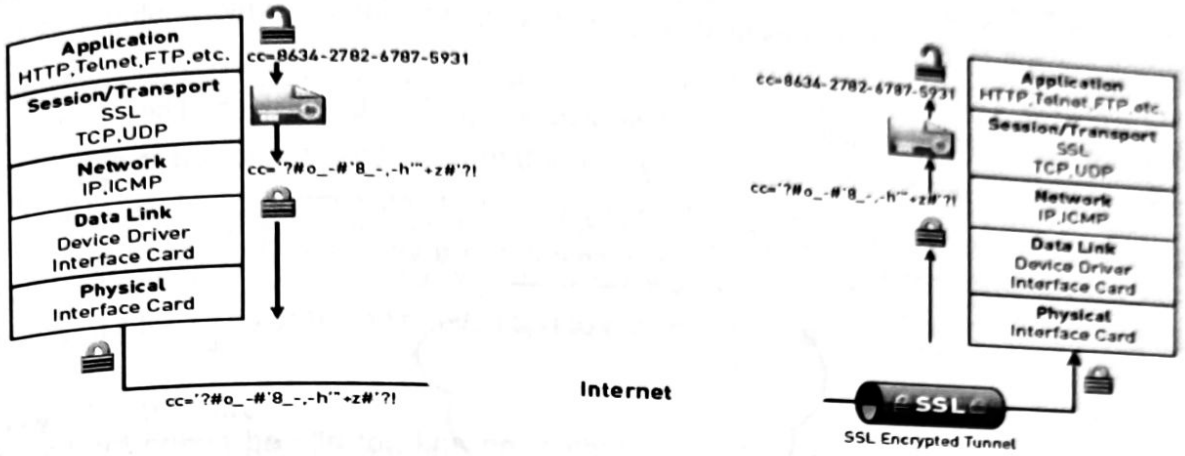
SSL and the OSI Model

The SSL protocol is a security protocol that sits on top of TCP at the transport layer. In the OSI model, application layer protocols such as HTTP or IMAP, handle user application tasks such as displaying web pages or running email servers.

Session layer protocols establish and maintain communications channels. Transport layer protocols such

as TCP and UDP; handle the flow of data between two hosts. Network layer protocols such as IP and ICMP provide hop-by-hop handling of data packets across the network.

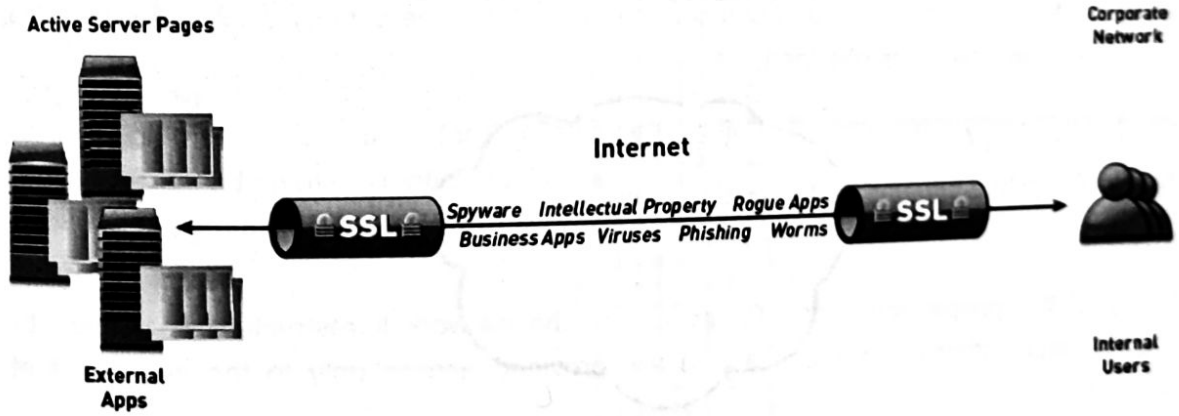
SSL operates independently and transparently of other protocols so it works with any application layer and any transport layer protocol. This allows clients and servers to establish secure SSL connections without requiring knowledge of the other party's code.



An application layer protocol hands unencrypted data to the session/transport layer, SSL encrypts the data and hands it down through the layers. When the server receives the data at the other end, it passes it up through the layers to the session layer where SSL decrypts it and hands it off to the application layer. Since the client and the server have gone through the key negotiation handshake, the symmetric key used by SSL is the same at both ends.

The Cost of Encryption

While SSL solves the problem of securely transferring private data, it introduces another problem: HTTPS traffic poses a major security risk to enterprises.



The above figure because SSL (Secure Sockets Layer) content is encrypted, it can't be intercepted by normal means.

Users can bring in various malware including viruses, access forbidden sites, and leak confidential business information over an HTTPS connection, which uses port 443. Because IT organizations have no visibility into SSL sessions, they are blind to any potential security threats sent over HTTPS. In addition to the security threat, encrypted traffic makes it difficult for IT to assess bandwidth usage and apply intelligent content control policies to ensure maximum user productivity. Additionally, key signing and certificate verification is extremely CPU-intensive. Many security-sensitive websites that have implemented SSL experience bottlenecks created by the managing and processing of SSL sessions. The end result is that SSL degrades web server performance considerably and web transactions are slowed to a crawl. Because of the performance degradation caused by SSL, many organizations cannot, because of budgetary or infrastructure limitations, implement SSL. Or they implement it in a very limited capacity by applying SSL only to sensitive data or transactions.

Secure messaging

To ensure that the document is protected from eavesdropping and not altered during the transmission, John will first encrypt the document using Harry's public key. This ensures two things: one, that the document is encrypted, and two, only Harry can open it as the document requires the private key of Harry to open it. For the accomplishment of encryption using the public key of the receiver the receiver must decrypt it with his or her private key. In this way, John could ensure that the document is encrypted and only the intended receiver (Harry) can open it. But still, John cannot ensure the Integrity (alteration of the contents) of the contents during transmission by document encryption alone.

Message digest

John performs a hash function on the document to ensure that the document is not altered during transmission. A computational value based on the contents of the document is the hash value and it can also be known as the message digest. The digest can be obtained by Harry by performing the same hash function on the decrypted message and can compare it with the one sent by John to ensure the integrity of the contents . Hence integrity is obtained.

Security Technology

Security technically falls into one of three categories.

Identity

The identity of the people requesting for access to the network infrastructure is verified through the authentication and authorization process and are provided access only to the services that they are prescribed for.

Integrity

Data integrity is maintained with the help of firewalls, routing, management control, encryption, and access control.

Active Audit

The network administrators are provided with assistance on the data on network activities such as the account of the network usage, discovery of unauthorized activities and scanning the network for security vulnerabilities.

User id's and passwords can be used as a basic security measure to authenticate remote users.

Cryptography

Concealing the confidential information to maintain the integrity of the data from unauthorized users and ensuring immediate detection of any alteration on the concealed information is the sole purpose of cryptography. It's the transformation of plain text to scrambled text and vice versa.

Public key infrastructure

Public Key Infrastructure (PKI) is a that enables integration of The various services related to cryptography are integrated into a framework enabled by Public Key Infrastructure (PKI)

The aim of PKI is to Providing authentication, integrity, confidentiality, access control,and non-repudiation.

Non-repudiation

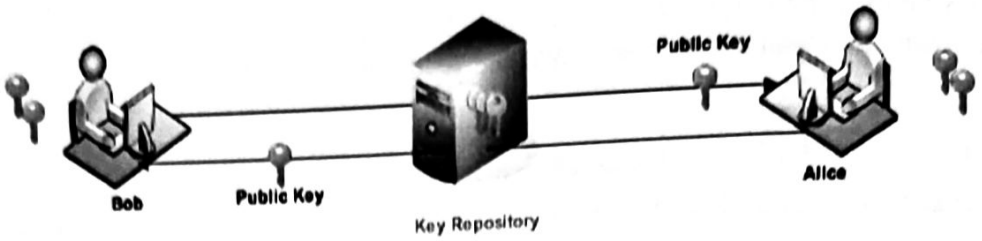
In order to ensure that the sender or the receiver don't deny that the message is sent or received by them an audit check like a time stamp is used which is an audit trial that gives the details of the time the message was sent by the sender and when it was received by the receiver .

The three primary functions of a PKI are Encryption and decryption, digital signature and key exchange .

RSS and elliptic curve The algorithms that provide the functions for encryption and decryption, digital signatures and key exchanges are RSS and Elliptic curve ,key exchanges are supported by Diffie-Hellmen algorithm , while digital signatures use Digital Signature Standard (DSS) .

Public Key Encryption

PKI is the encryption methodology used for Public key encryption . It uses asymmetric cryptography using a pair of keys and is based on mathematical functions.



Every user in a PKI will have a "pair of keys" known as a private key and a public key. The identity of a private key is never revealed and it stays with the owner whereas the public key is stored a key repository and is accessible to all.

A message can be encrypted and decrypted by using a key. Most importantly, A message encrypted by a private key can be decrypted only by a corresponding public key. Similarly, a private key is required to decrypt a message that is encrypted by a public key.

In the above example the image says, John wants to send a confidential document to Harry electronically. John has four issues to address before this electronic transmission can occur:

- Ensure that the document is encrypted and is kept confidential.
- Ensure that the document is not altered during transmission.
- Since Harry does not know John, he has to somehow prove that the document is indeed sent by him.
- Ensure that Harry receives the document and that he doesn't deny receiving it in future.

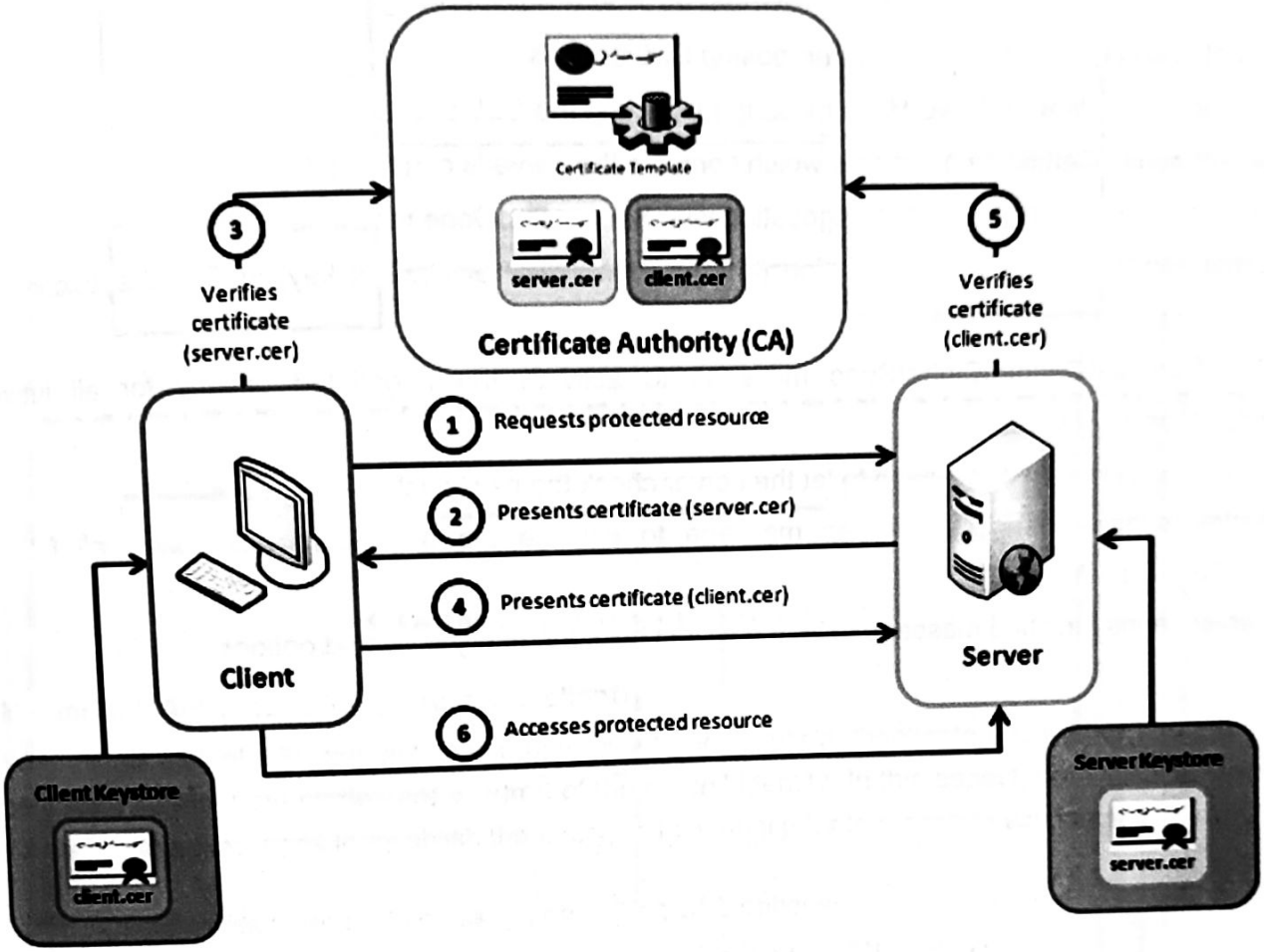
All the four requirements mentioned above can be handled by the methods of the PKI like message digests, secure messaging, digital signatures and non-repudiation services.

Introduction to Authentication

Mutual SSL authentication or certificate based mutual authentication refers to two parties authenticating each other through verifying the provided digital certificate so that both parties are assured of the others' identity. In technology terms, it refers to a client (web browser or client application) authenticating themselves to a server (website or server application) and that server also authenticating itself to the client through verifying the public key certificate/digital certificate issued by the trusted Certificate Authorities (CAs). Because authentication relies on digital certificates, certification authorities such as Verisign or Microsoft Certificate Server are an important part of the mutual authentication process. From a high-level point of view, the process of authenticating and establishing an encrypted channel using certificate-based mutual authentication involves the following steps:

1. A client requests access to a protected resource.

2. The server presents its certificate to the client.
3. The client verifies the server's certificate.
4. If successful, the client sends its certificate to the server.
5. The server verifies the client's credentials.
6. If successful, the server grants access to the protected resource requested by the client.



Mutual SSL authentication / Certificate based mutual authentication

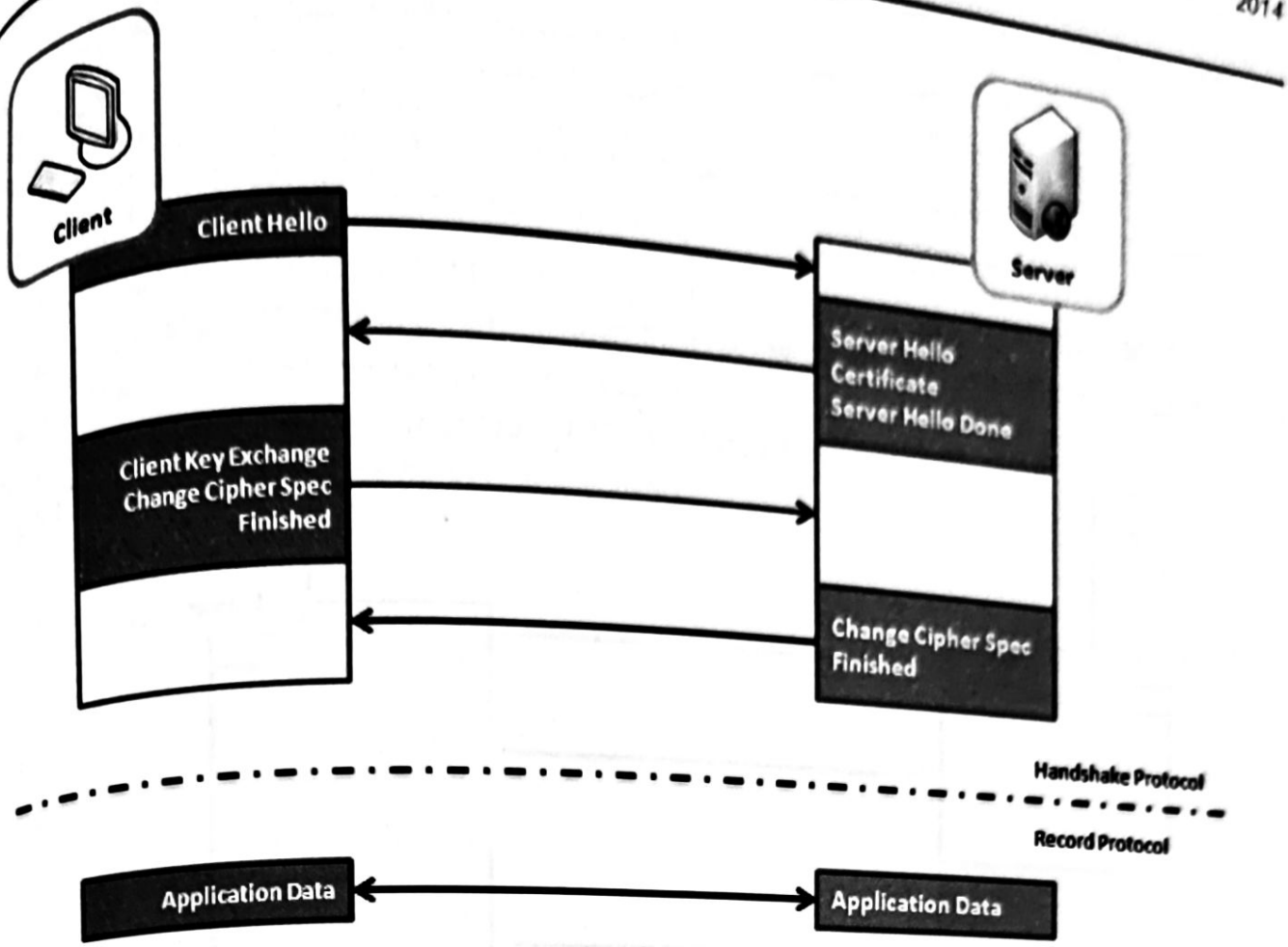
Background

Mutual SSL authentication works similar to SSL (Secure Socket Layer) authentication, with the addition of client authentication using digital signatures. Thus, SSL authentication and Mutual SSL authentication also informally known as 1-way SSL authentication and 2-way SSL authentication, respectively. As a developer, if you're interested in developing or be able to debug the mutual SSL authentication effectively, it can be very useful to understand the intricacies of the handshake messages happening under the hood.

SSL authentication (server --> client)

In SSL authentication, the client is presented with a server's certificate, the client computer might try to match the server's CA against the client's list of trusted CAs. If the issuing CA is trusted, the client will verify that the certificate is authentic and has not been tampered with. In this aspect, both client and server use **9** handshake messages to establish the encrypted channel prior to message exchanging.

1. Client sends ClientHello message proposing SSL options.
2. Server responds with ServerHello message selecting the SSL options.
3. Server sends Certificate message, which contains the server's certificate.
4. Server concludes its part of the negotiation with ServerHelloDone message.
5. Client sends session key information (encrypted with server's public key) in ClientKeyExchange message.
6. Client sends ChangeCipherSpec message to activate the negotiated options for all future messages it will send.
7. Client sends Finished message to let the server check the newly activated options.
8. Server sends ChangeCipherSpec message to activate the negotiated options for all future messages it will send.
9. Server sends Finished message to let the client check the newly activated options.



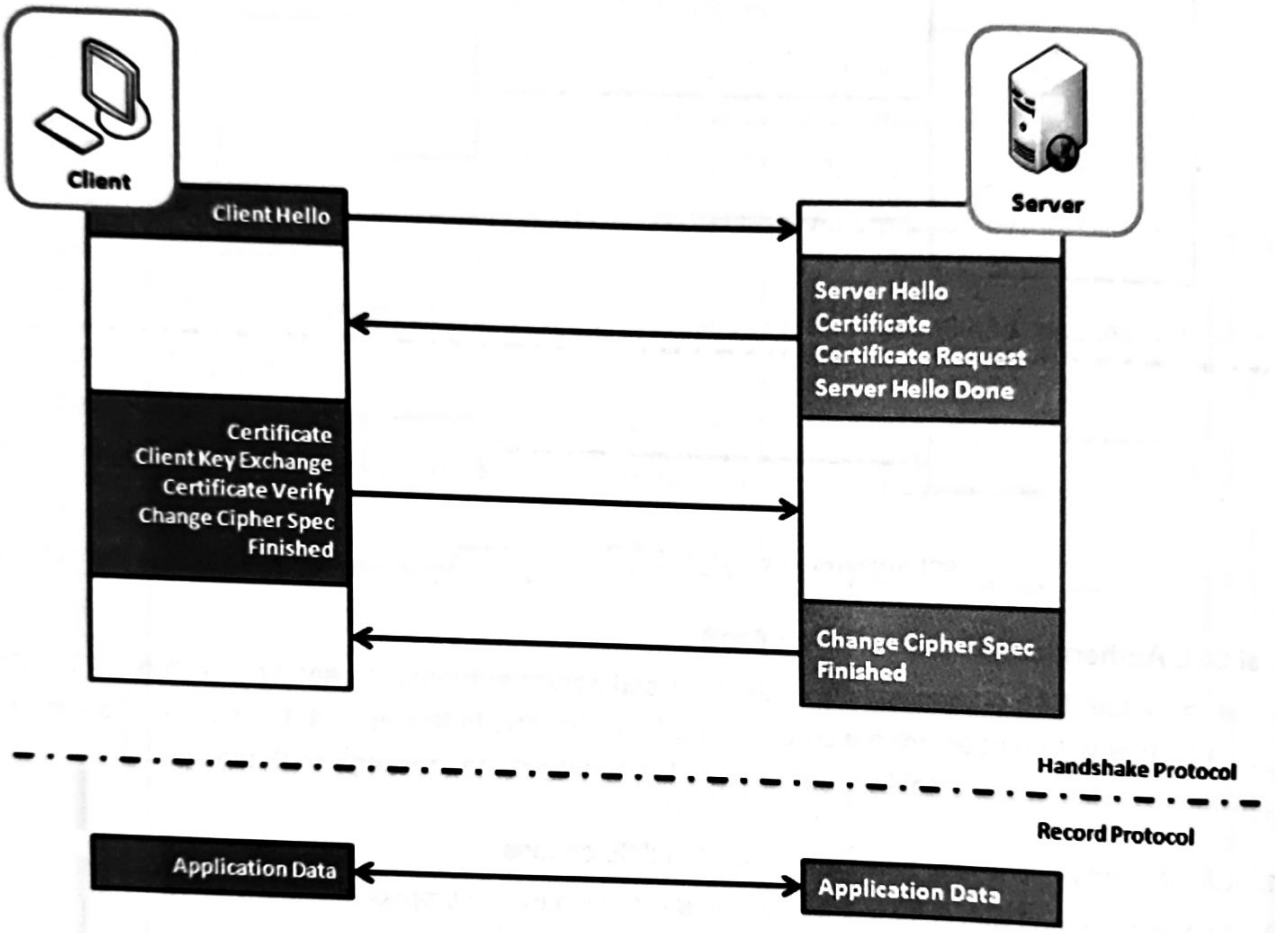
SSL authentication handshake messages

Mutual SSL Authentication (server <--> client)

Whereas in mutual SSL authentication, both client and server authenticate each other through the digital certificate so that both parties are assured of the others' identity. In this aspect, both client and server use 12 handshake messages to establish the encrypted channel prior to message exchanging.

1. Client sends ClientHello message proposing SSL options.
2. Server responds with ServerHello message selecting the SSL options.
3. Server sends Certificate message, which contains the server's certificate.
4. Server requests client's certificate in CertificateRequest message, so that the connection can be mutually authenticated.
5. Server concludes its part of the negotiation with ServerHelloDone message.
6. Client responds with Certificate message, which contains the client's certificate.
7. Client sends session key information (encrypted with server's public key) in ClientKeyExchange message.
8. Client sends a CertificateVerify message to let the server know it owns the sent certificate.

9. Client sends ChangeCipherSpec message to activate the negotiated options for all future messages it will send.
10. Client sends Finished message to let the server check the newly activated options.
11. Server sends ChangeCipherSpec message to activate the negotiated options for all future messages it will send.
12. Server sends Finished message to let the client check the newly activated options.



Mutual SSL authentication handshake messages

Capture and Analyze

To help readers better visualize what's happening under the hood, I've enhanced a code example taken from the Microsoft website so that both client and server are capable of authenticating each other using the mutual SSL authentication. The code sample is very simple, and I won't illustrate much here. Basically, what it does is the client application sends a "*Hello from the client.*" message to the server and the server application replies with a "*Hello from the server.*" message, right after the mutual SSL authentication is completed successfully.

To capture the handshake messages transacted between the client and server, I use one of the popular and open-source packet analyzer tools called WireShark. It is a powerful and easy to use packet capture and analyzer tool, which can captures messages over a hundred of protocols. To learn more about how you can make use of this tool, please visit its website.

However, due to the lack of supported Loopback Interface in Windows operating system, I've to setup the client and server application running on two different machines in order to use Wireshark to capture their handshake messages. The handshake messages captured while running the applications are shown in the screenshot below, and the IP address "***10.5.3.28***" and "***10.5.3.18***" in the *Source* or *Destination* columns represents "***The Client***" and "***The Server***", respectively.