GRID AND CLOUD COMPUTING
Unit 5

UNIT V SECURITY

Trust models for Grid security environment – Authentication and Authorization methods – Grid security infrastructure – Cloud Infrastructure security: network, host and application level – aspects of data security, provider data and its security, Identity and access management architecture, IAM practices in the cloud, SaaS, PaaS, IaaS availability in the cloud, Key privacy issues in the cloud.

Definition of Trust

- Trust is the firm belief in the competence of an entity to behave as expected such that this firm belief is a dynamic value associated with the entity and is subject to the entity's behavior and applies only within a specific context at a given time

Trust

- Trust value is a continuous and dynamic value in the range of [0,1]
- 1 means very trustworthy
- 0 means very untrustworthy
- It is built on past experience
- It is context based (under different context may have different trust value)

Reputation

- When making trust-based decisions, entities can rely on others for information regarding to a specific entity.
- The information regarding to a specific entity x is defined as the reputation of entity x.

Definition of Reputation

- The reputation of an entity is an expectation of its behavior based on other entities' observations or information about the entity's past behavior within a specific context at a given time.

Evaluating Trust and Reputation

- Trusts decays with time
- Entities may form alliances and they may trust their allies and business partners more than others
- Trust value is based on the combination of direct trust and reputation

Trust models for Grid security environment

- Many potential security issues may occur in a grid environment if qualified security mechanisms are not in place. These issues include
  1. network sniffers,
  2. out-of-control access,
  3. faulty operation,
  4. malicious operation,
  5. integration of local security mechanisms,
  6. delegation,
  7. dynamic resources and services,
  8. attack provenance, and so on.

Security Demand (SD) and Trust Index (TI)

- On the one hand, a user job demands the resource site to provide security assurance by issuing a security demand (SD).
- On the other hand, the site needs to reveal its trustworthiness, called its trust index (TI).
- These two parameters must satisfy a security assurance condition: TI $\geq$ SD during the j ob mapping process.
- When determining its security demand, users usually care about some typical attributes. These attributes and their values are dynamically changing and depend heavily on the trust model, security policy, accumulated reputation, self-defense capability, attack history, and site vulnerability.
- Three challenges are outlined below to establish the trust among grid sites

The first challenge is integration with existing systems and technologies.

- The resources sites in a grid are usually heterogeneous and autonomous.
- It is unrealistic to expect that a single type of security can be compatible with and adopted by every hosting environment.
- At the same time, existing security infrastructure on the sites cannot be replaced overnight. Thus, to be successful, grid security architecture needs to step up to the challenge of integrating with existing security architecture and models across platforms and hosting environments.

The second challenge is interoperability with different “hosting environments.”

- Services are often invoked across multiple domains, and need to be able to interact with one another.
- The interoperation is demanded at the protocol, policy, and identity levels. For all these levels, interoperation must be protected securely.

The third challenge is to construct trust relationships among interacting hosting environments.

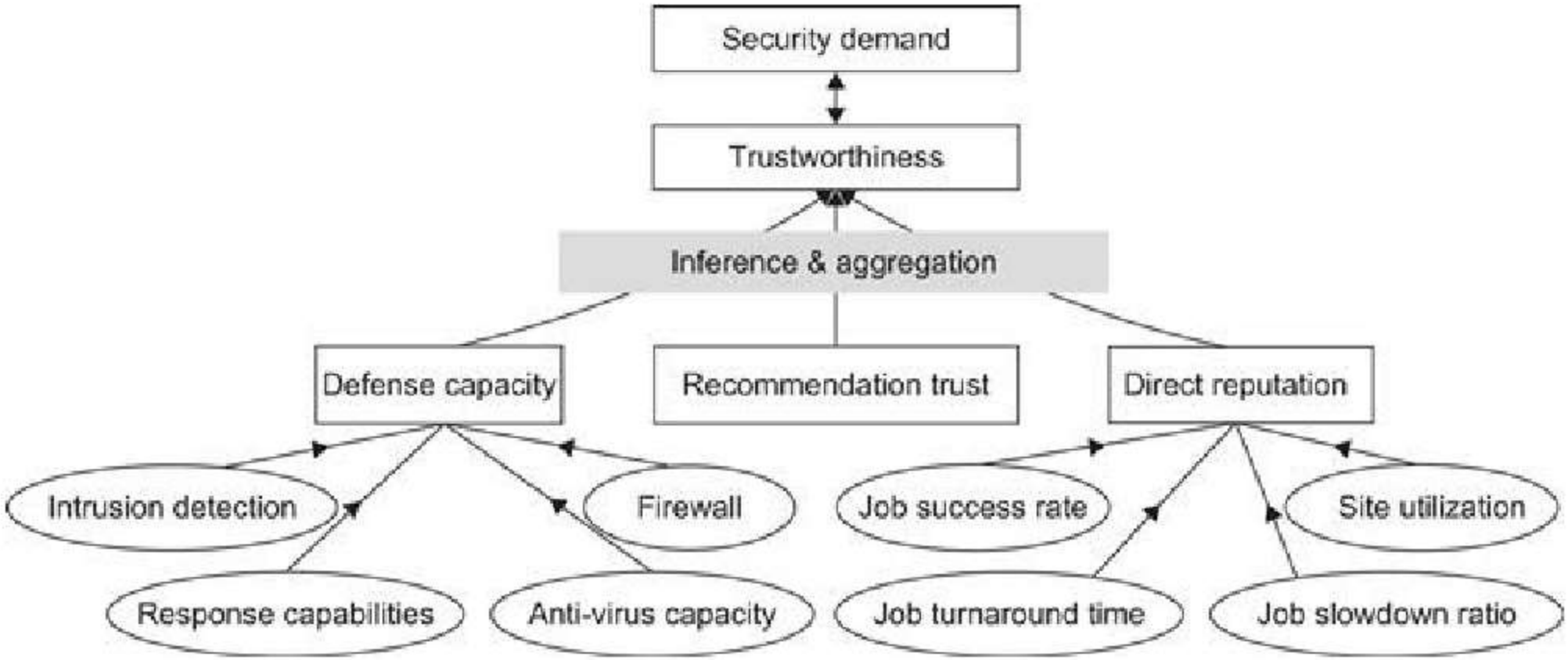
- Grid service requests can be handled by combining resources on multiple security domains.
- Trust relationships are required by these domains during the end-to-end traversals.
- A service needs to be open to friendly and interested entities so that they can submit requests and access securely.

Trust Model

- Resource sharing among entities is one of the major goals of grid computing. A trust relationship must be established before the entities in the grid interoperate with one another.
- To create the proper trust relationship between grid entities, two kinds of trust models are often used.

1. One is the PKI -based model, which mainly exploits the PKI to authenticate and authorize entities.
2. The other is the reputation-based model.

A Generalized Trust Model



A Generalized Trust Model conti...

- Figure shows a general trust model.
- The three major factors which influence the trustworthiness of a resource site.
- An inference module is required to aggregate these factors. Followings are some existing inference or aggregation methods. An intra-site fuzzy inference procedure is called to assess defense capability and direct reputation.
- Defense capability is decided by the firewall, *intrusion detection system (I DS), intrusion response capability, and anti-virus capacity of the individual* resource site.
- Direct reputation is decided based on the j ob success rate, site utilization, job turnaround time, and j ob slowdown ratio measured.
- Recommended trust is also known as secondary trust and is obtained indirectly over the grid network.

Reputation-Based Trust Model

- In a reputation-based model, jobs are sent to a resource site only when the site is trustworthy to meet users' demands.
- The site trustworthiness is usually calculated from the following information: the defense capability, direct reputation, and recommendation trust. The defense capability refers to the site's ability to protect itself from danger.
- It is assessed according to such factors as intrusion detection, firewall, response capabilities, anti-virus capacity, and so on.
- Direct reputation is based on experiences of prior jobs previously submitted to the site.
- The reputation is measured by many factors such as prior j ob execution success rate, cumulative site utilization, job turnaround time, job slowdown ratio, and so on.
- A positive experience associated with a site will improve its reputation. On the contrary, a negative experience with a site will decrease its reputation.

A Fuzzy-Trust Model

- In this model, the j ob *security demand (SD) is supplied by the user programs. The trust index (TI) of a resource site is aggregated through the fuzzy-logic inference process* over all related parameters. Specifically, one can use a two-level fuzzy logic to estimate the aggregation of numerous trust parameters and security attributes into scalar quantities that are easy to use in the j ob scheduling and resource mapping process.
- The TI is normalized as a single real number with 0 representing the condition with the highest risk at a site and 1 representing the condition which is totally risk-free or fully trusted.
- The fuzzy inference is accomplished through four steps: *fuzzification, inference, aggregation, and defuzzification*.
- *The second salient feature of the trust model is that if a* site's trust index cannot match the job security demand (i.e., SD > TI), the trust model could deduce detailed security features to guide the site security upgrade as a result of tuning the fuzzy system.

Authentication and Authorization Methods

- The major authentication methods in the grid include passwords, PKI , and Kerberos. The password is the simplest method to identify users, but the most vulnerable one to use.
- The PKI is the most popular method supported by GSI . To implement PKI , we use a trusted third party, called the *certificate authority (CA). Each user applies a unique pair of* public and private keys. The *public keys are issued by the CA by issuing a certificate, after* recognizing a legitimate user.
- The *private key is exclusive for each user to use, and is* unknown to any other users. A digital certificate in IEEE X.509 format consists of the user name, user public key, CA name, and a secrete signature of the user.

Authorization for Access Control

- The authorization is a process to exercise access control of shared resources.
- Decisions can be made either at the access point of service or at a centralized place.
- Typically, the resource is a host that provides processors and storage for services deployed on it. Based on a set predefined policies or rules, the resource may enforce access for local services.
- The central authority is a special entity which is capable of issuing and revoking polices of access rights granted to remote accesses.
- The authority can be classified into three categories:

1. Attribute authorities - issue attribute assertions
2. Policy authorities - authorization policies , and
3. Identity authorities - issue certificates

- The authorization server makes the final authorization decision.

Three Authorization Models

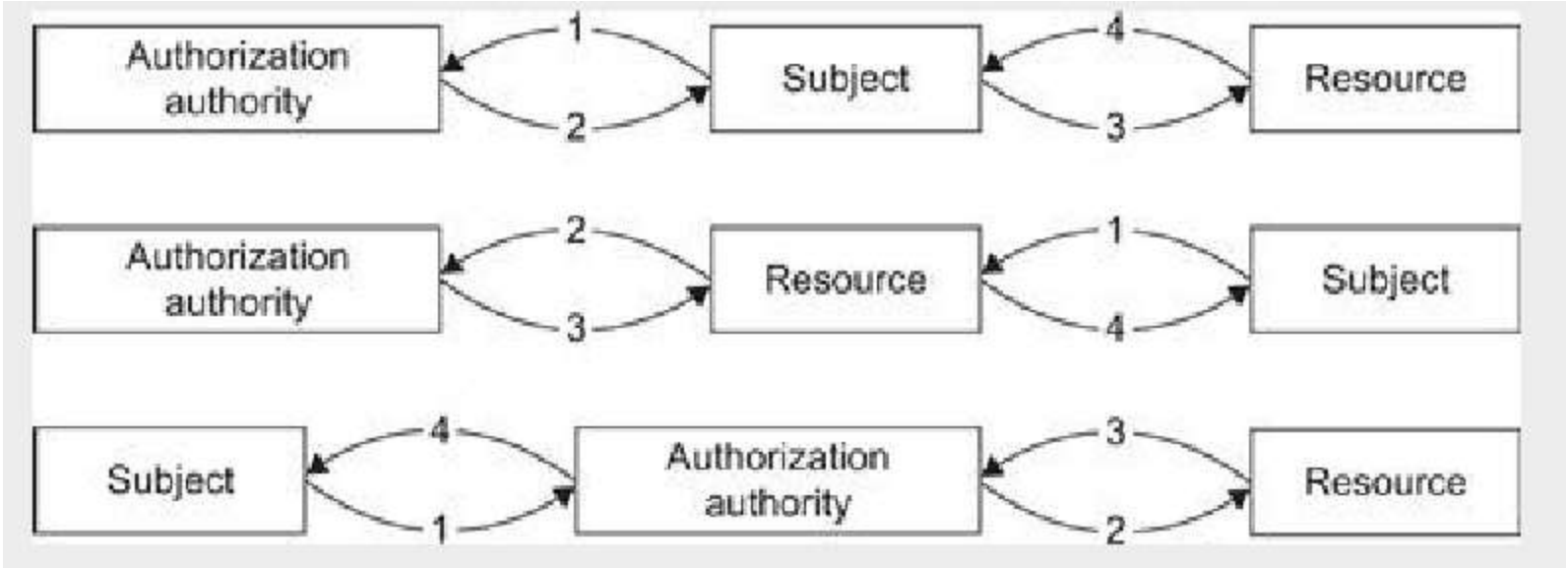


Figure shows three authorization models.

1. The subject-push model
2. The resource-pulling model
3. The authorization agent model

Three authorization model

- The *subject-push model is shown at the top diagram. The user* conducts handshake with the authority first and then with the resource site in a sequence.
- The *resource-pulling model puts the resource in the middle. The user checks the* resource first. Then the resource contacts its authority to verify the request, and the authority authorizes at step 3. Finally the resource accepts or rejects the request from the subject at step 4.
- The *authorization a gent model puts the authority in the middle. The* subject check with the authority at step 1 and the authority makes decisions on the access of the requested resources. The authorization process is complete at steps 3 and 4 in the reverse direction.

Grid Security Infrastructure (GSI)

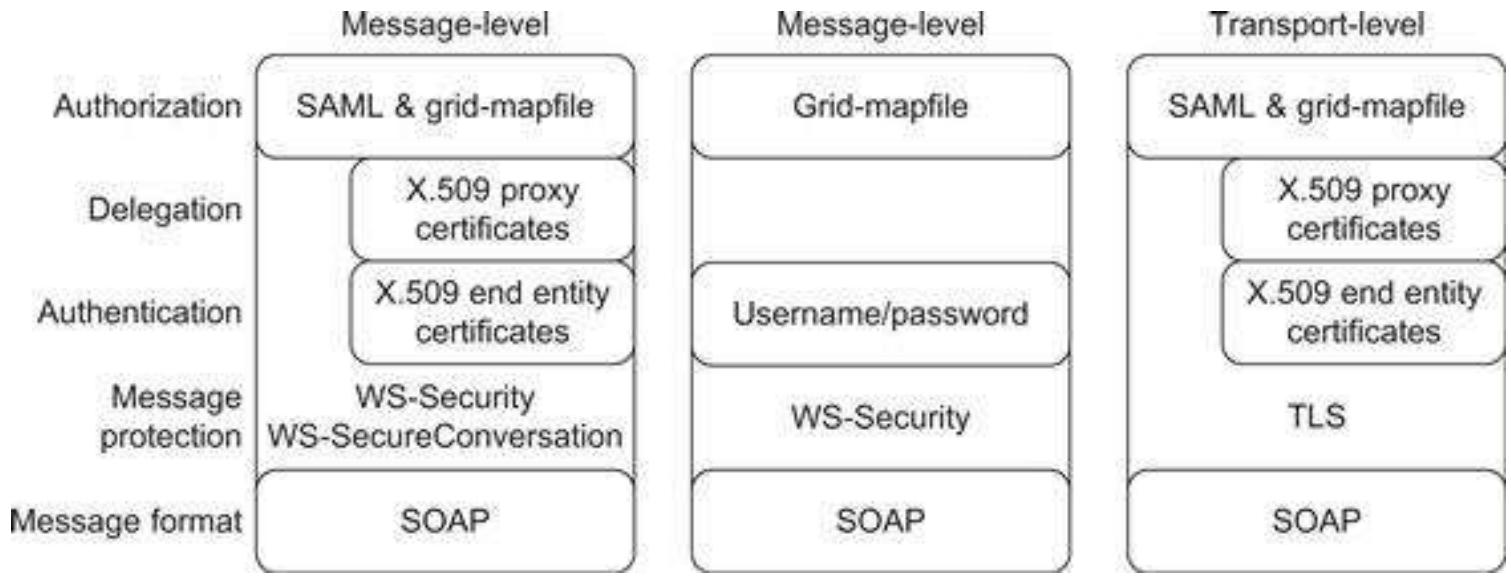
- The grid is increasingly deployed as a common approach to constructing dynamic, inter domain, distributed computing and data collaborations, still there is "lack of security/trust between different services".
- It is still an important challenge of the grid.
- The grid requires a security infrastructure with the following properties:
  1. easy to use;
  2. conforms with the virtual organization (VO's) security needs while working well with site policies of each resource provider site; and
  3. provides appropriate authentication and encryption of all interactions.

Grid Security Infrastructure (GSI) conti..

- The GSI is an important step toward satisfying these requirements.
- GSI is well-known security solution in the grid environment,
- GSI is a portion of the Globus Toolkit and provides fundamental security services needed to support grids, including supporting for message protection, authentication and delegation, and authorization.
- GSI enables secure authentication and communication over an open network, and permits mutual authentication across and among distributed sites with single sign-on capability.
- No centrally managed security system is required, and the grid maintains the integrity of its members' local policies.
- GSI supports both message-level security, which supports the WS-Security standard and the WS-Secure Conversation specification to provide message protection for SOAP messages, and transport-level security, which means authentication via *transport-level security* (TLS)with support for X.509 proxy certificates.

GSI Functional Layers

- GT4 provides distinct WS and pre-WS authentication and authorization capabilities.
- Both build on the same base, namely the X.509 standard and entity certificates and proxy certificates, which are used to identify persistent entities such as users and servers and to support the temporary delegation of privileges to other entities, respectively. As shown in Figure.
- GSI may be thought of as being composed of four distinct functions: message protection, authentication, delegation, and authorization.



GSI Functional Layers conti..

- TLS (transport-level security) or WS-Security and WS-Secure Conversation (message level) are used as message protection mechanisms in combination with SOAP.
- X.509 End Entity Certificates or Username and Password are used as authentication credentials. X.509 Proxy Certificates and WS-Trust are used for delegation.
- An Authorization Framework allows for a variety of authorization schemes, including a "grid-mapfile" ACL, an ACL defined by a service, a custom authorization handler, and access to an authorization service via the SAML protocol.
- In addition, associated security tools provide for the storage of X.509 credentials, the mapping between GSI and other authentication mechanisms and maintenance of information used for authorization.

GSI Functional Layers conti...

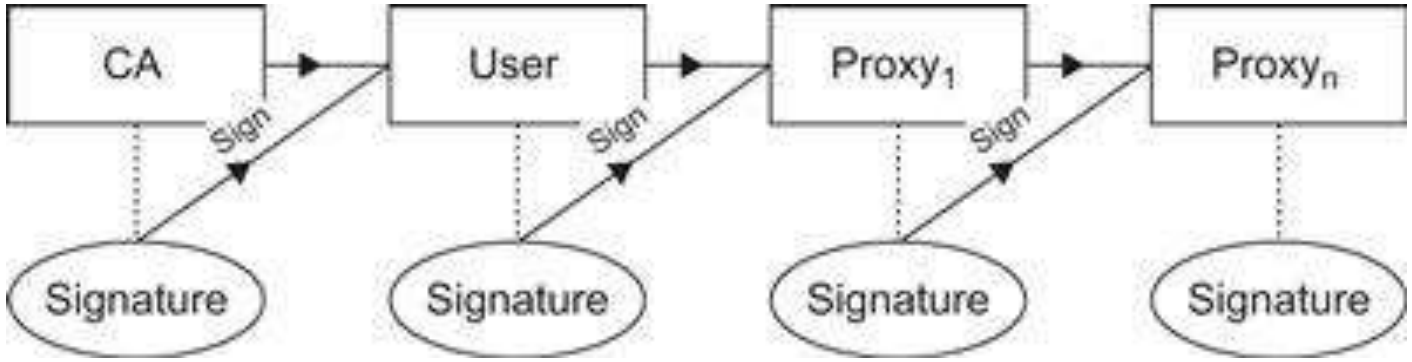
- The web services portions of GT4 use SOAP as their message protocol for communication.
- Message protection can be provided either by

1. transport-level security, which transports SOAP messages over TLS, or by
2. message-level security, which is signing and/or encrypting Portions of the SOAP message using the WS-Security standard.

GSI Functional Layers conti ...

- The X.509 certificates used by GSI are conformant to the relevant standards and conventions.
- Grid deployments around the world have established their own CAs based on third-party software to issue the X.509 certificate for use with GSI and the Globus Toolkit.
- GSI also supports delegation and single sign-on through the use of standard .X.509 proxy certificate. Proxy certificate allow bearers of X.509 to delegate their privileges temporarily to another entity.
- For the purposes of authentication and authorization, GSI treats certificate and proxy certificate equivalently. Authentication with X.509 credentials can be accomplished either via TLS, in the case of transport-level security, or via signature as specified by WS-Security, in the case of message-level security.

Authentication and Delegation



- To reduce or even avoid the number of times the user must enter his passphrase when several grids are used or have agents (local or remote) requesting services on behalf of a user, GSI provides a delegation capability and a delegation service that provides an interface to allow clients to delegate (and renew) X.509 proxy certificates to a service.
- The interface to this service is based on the WS-Trust specification. A proxy consists of a new certificate and a private key. The key pair that is used for the proxy, that is, the public key embedded in the certificate and the private key, may either be regenerated for each proxy or be obtained by other means.
- The new certificate contains the owner's identity, modified slightly to indicate that it is a proxy. The new certificate is signed by the owner, rather than a CA

Trust Delegation

- GSI has traditionally supported authentication and delegation through the use of X.509 certificate and public keys. As a new feature in GT4, GSI also supports authentication through plain usernames and passwords as a deployment option.
- As a central concept in GSI authentication, a certificate includes four primary pieces of information:
- (1) a subject name, which identifies the person or object that the certificate represents;
- (2) the public key belonging to the subject;
- (3) the identity of a CA that has signed the certificate to certify that the public key and the identity both belong to the subject; and
- (4) the digital signature of the named CA. X.509 provides each entity with a unique identifier (i.e., a distinguished name) and a method to assert that identifier to another party through the use of an asymmetric key pair bound to the identifier by the certificate.

Risks and Security Concerns With Cloud Computing

- Many of the cloud computing associated risks are not new and can be found in the computing environments. There are many companies and organizations that outsource significant parts of their business due to the globalization.
- It means not only using the services and technology of the cloud provider, but many questions dealing with the way the provider runs his security policy.
- After performing an analysis the top threats to cloud computing can be summarized as follows

1. Abuse and Unallowed Use of Cloud Computing;
2. Insecure Application Programming Interfaces;
3. Malicious Insiders;
4. Shared Technology Vulnerabilities;
5. Data Loss and Leakage
6. Account, Service and Traffic Hijacking;
7. Unknown Risk Profile.

Cloud Security Principles

- Public cloud computing requires a security model that coordinates scalability and multi-tenancy with the requirement for trust. As enterprises move their computing environments with their identities, information and infrastructure to the cloud, they must be willing to give up some level of control.
- In order to do so they must be able to trust cloud systems and providers, as well as to verify cloud processes and events.
- Important building blocks of trust and verification relationships include access control, data security, compliance and event management - all security elements well understood by IT departments today, implemented with existing products and technologies, and extendable into the cloud. The cloud security principles comprise three categories:

  1. identity,
  2. information and
  3. infrastructure.

Identity security

- End-to-end identity management, third-party authentication services and identity must become a key element of cloud security. Identity security keeps the integrity and confidentiality of data and applications while making access readily available to appropriate users. Support for these identity management capabilities for both users and infrastructure components will be a major requirement for cloud computing and identity will have to be managed in ways that build trust. It will require:
- *Stronger authentication:* Cloud computing must move beyond authentication of username and password, which means adopting methods and technologies that are IT standard IT such as strong authentication, coordination within and between enterprises, and risk-based authentication, measuring behavior history, current context and other factors to assess the risk level of a user request.
- *Stronger authorization:* Authorization can be stronger within an enterprise or a private cloud, but in order to handle sensitive data and compliance requirements, public clouds will need stronger authorization capabilities that can be constant throughout the lifecycle of the cloud infrastructure and the data.

Information security

- In the traditional data center, controls on physical access, access to hardware and software and identity controls all combine to protect the data. In the cloud, that protective barrier that secures infrastructure is diffused. The data needs its own security and will require
- *Data isolation:* In multi-tenancy environment data must be held securely in order to protect it when multiple customers use shared resources. Virtualization, encryption and access control will be workhorses for enabling varying degrees of separation between corporations, communities of interest and users.
- *Stronger data security:* In existing data center environments the role-based access control at the level of user groups is acceptable in most cases since the information remains within the control of the enterprise. However, sensitive data will require security at the file, field or block level to meet the demands of assurance and compliance for information in the cloud.

Information security conti...

- *Effective data classification:* Enterprises will need to know what type of data is important and where it is located as prerequisites to making performance cost-benefit decisions, as well as ensuring focus on the most critical areas for data loss prevention procedures.
- *Information rights management:* it is often treated as a component of identity on which users have access to. The stronger data-centric security requires policies and control mechanisms on the storage and use of information to be associated directly with the information itself.
- *Governance and compliance:* A major requirement of corporate information governance and compliance is the creation of management and validation information - monitoring and auditing the security state of the information with logging capabilities. The cloud computing infrastructures must be able to verify that data is being managed per the applicable local and international regulations with appropriate controls, log collection and reporting.

Cloud Infrastructure Security

- IaaS application providers treat the applications within the customer virtual instance as a black box and therefore are completely indifferent to the operations and management of a applications of the customer. The entire pack (customer application and run time application) is run on the customers' server on provider infrastructure and is managed by customers themselves. For this reason it is important to note that the customer must take full responsibility for securing their cloud deployed applications.
- Cloud deployed applications must be designed for the internet threat model.
- They must be designed with standard security countermeasures to guard against the common web vulnerabilities.
- Customers are responsible for keeping their applications up to date - and must therefore ensure they have a patch strategy to ensure their applications are screened from malware and hackers scanning for vulnerabilities to gain unauthorized access to their data within the cloud.
- Customers should not be tempted to use custom implementations of Authentication, Authorization and Accounting as these can become weak if not properly implemented.

Cloud Infrastructure Security conti..

- The foundational infrastructure for a cloud must be inherently secure whether it is a private or public cloud or whether the service is SAAS, PAAS or IAAS.
- *Inherent component-level security:* The cloud needs to be architected to be secure, built with inherently secure components, deployed and provisioned securely with strong interfaces to other components and supported securely, with vulnerability-assessment and change-management processes that produce management information and service-level assurances that build trust.
- *Stronger interface security:* The points in the system where interaction takes place (user-to-network, server-to application) require stronger security policies and controls that ensure consistency and accountability.
- *Resource lifecycle management:* The economics of cloud computing are based on multi-tenancy and the sharing of resources. As the needs of the customers and requirements will change, a service provider must provision and decommission correspondingly those resources - bandwidth, servers, storage and security. This lifecycle process must be managed in order to build trust.
- The infrastructure security can be viewed, assessed and implemented according its building levels - the network, host and application levels

Infrastructure Security - The Network Level

- When looking at the network level of infrastructure security, it is important to distinguish between public clouds and private clouds. important to distinguish between public clouds and private clouds. With private clouds, there are no new attacks, vulnerabilities, or changes in risk specific to this topology that information security personnel need to consider.
- If public cloud services are chosen, changing security requirements will require changes to the network topology and the manner in which the existing network topology interacts with the cloud provider's network topology should be taken into account. There are four significant risk factors in this use case:

1. Ensuring the confidentiality and integrity of organization's data-in-transit to and from a public cloud provider;
2. Ensuring proper access control (authentication, authorization, and auditing) to whatever resources are used at the public cloud provider;
3. Ensuring the availability of the Internet-facing resources in a public cloud that are being used by an organization, or have been assigned to an organization by public cloud providers;
4. Replacing the established model of network zones and tiers with domains.

Infrastructure Security - The Host Level

- When reviewing host security and assessing risks, the context of cloud services delivery models (SaaS, PaaS, and IaaS) and deployment models public, private, and hybrid) should be considered.
- The host security responsibilities in SaaS and PaaS services are transferred to the provider of cloud services.
- IaaS customers are primarily responsible for securing the hosts provisioned in the cloud (virtualization software security, customer guest OS or virtual server security).

Infrastructure Security - The Application Level

- Application or software security should be a critical element of a security program. Most enterprises with information security programs have yet to institute an application security program to address this realm.
- Designing and implementing applications aims at deployment on a cloud platform will require existing application security programs to reevaluate current practices and standards.
- The application security spectrum ranges from standalone single-user applications to sophisticated multiuser e-commerce applications used by many users. The level is responsible for managing .
  1. Application-level security threats;
  2. End user security;

Infrastructure Security - The Application Level conti...

3. SaaS application security;
4. PaaS application security;
5. PaaS application security;
6. Customer-deployed application security
7. IaaS application security
8. Public cloud security limitations

- It can be summarized that the issues of infrastructure security and cloud computing lie in the area of definition and provision of security specified aspects each party delivers.

Aspects of Data Security

Security for

1. Data in transit
2. Data at rest
3. Processing of data including multitenancy
4. Data Lineage
5. Data Provenance
6. Data remanance

- Solutions include encryption, identity management, sanitation

Provider Data and its Security

- What data does the provider collect – e.g., metadata, and how can this data be secured?
  1. Data security issues
  2. Access control,
- Key management for encrypting
- Confidentiality, Integrity and Availability are objectives of data security in the cloud

Identity and Access Management (IAM) in the Cloud

Trust Boundaries and IAM

- In a traditional environment, trust boundary is within the control of the organization
- This includes the governance of the networks, servers, services, and applications
- In a cloud environment, the trust boundary is dynamic and moves within the control of the service provider as well ass organizations
- Identity federation is an emerging industry best practice for dealing with dynamic and loosely coupled trust relationships in the collaboration model of an organization
- Core of the architecture is the directory service which is the repository for the identity, credentials and user attributes

Why IAM?

- Improves operational efficiency and regulatory compliance management
- IAM enables organizations to achieve access cont6rol and operational security
- Cloud use cases that need IAM
  - Organization employees accessing SaaS se4rvidce using identity federation
  - IT admin access CSP management console to provision resources and access foe users using a corporate identity
  - Developers creating accounts for partner users in PaaS
  - End uses access storage service in a cloud
  - Applications residing in a cloud serviced provider access storage from another cloud service

IAM Challenges

- Provisioning resources to users rapidly to accommodate their changing roles
- Handle turnover in an organization
- Disparate dictionaries, identities, access rights
- Need standards and protocols that address the IAM challenges

IAM Definitions

- Authentication
  - Verifying the identity of a user, system or service
- Authorization
  - Privileges that a user or system or service has after being authenticated (e.g., access control)
- Auditing
  - Exam what the user, system or service has carried out
  - Check for compliance

IAM Practice

IAMN process consists of the following:

- User management (for managing identity life cycles),
- Authentication management,
- Authorization management,
- Access management,
- Data management and provisioning,
- Monitoring and auditing
- Provisioning,
- Credential and attribute management,
- Entitlement management,
- Compliance management,
- Identity federation management,
- Centralization of authentication and authorization,

Getting Ready for the Cloud

- Organization using a cloud must plan for user account provisioning
  - How can a user be authenticated in a cloud
- Organization can use cloud based solutions from a vendor for IAM (e.g., Symplified)
  - Identity Management as a Service
- Industry standards for federated identity management
  - SAML, WS-Federation, Liberty Alliance

Relevant IAM Standards, Protocols for Cloud

- IAM Standards and Specifications for Organizations
  - SAML
  - SPML
  - XACML
  - OAuth (Open Authentication) – cloud service X accessing data in cloud service Y without disclosing credentials
- IAM Standards and Specifications for Consumers
  - OpenID
  - Information Cards
  - Open Authenticate (OATH)
  - Open Authentication API (OpenAuth)

IAM Practices in the Cloud

- Cloud Identity Administration
  - Life cycle management of user identities in the cloud
- Federated Identity (SSO)
  - Enterprise an enterprise Identity provider within an Organization perimeter
  - Cloud-based Identity provider

Cloud Authorization Management

- XACML is the preferred model for authorization
- RBAC is being explored
- Dual roles: Administrator and User
- IAM support for compliance management

Cloud Service Provider and IAM Practice

- What is the responsibility of the CSP and the responsibility of the organization/enterprise?
- Enterprise IAM requirements
  - Provisioning of cloud service accounts to users
  - Provisioning of cloud services for service to service integration'
  - SSO support for users based on federation standards
  - Support for international and regulatory policy requirements
  - User activity monitoring
- How can enterprises expand their IAM requirements to SaaS, PaaS and IaaS

Security Management in the Cloud

- Security Management Standards
- Security Management in the Cloud
- Availability Management
- Access Control
- Security Vulnerability, Patch and Configuration Management

Security Management Standards

- Security Manage3ment has to be carried out in the cloud
- Standards include ITIL (Information Technology Infrastructure Library) and ISO 27001/27002
- What are the policies, procedures, processes and work instruction for managing security

Security Management in the Cloud

- Availability Management (ITIL)
- Access Control (ISIO, ITIL)
- Vulnerability Management (ISO, IEC)
- Patch Management (ITIL)
- Configuration Management (ITIL)
- Incident Response (ISO/IEC)
- System use and Access Monitoring

Availability Management

- SaaS availability
  - Customer responsibility: Customer must understand SLA and communication methods
  - SaaS health monitoring
- PaaS availability
  - Customer responsibility
  - ‘PaaS health monitoring
- IaaS availability
  - Customer responsibility
  - IaaS health monitoring

Access Control Management in the Cloud

- Who should have access and why
- How is a resources accessed
- How is the access monitored
- Impact of access control of SaaS, PaaS and IaaS

Security Vulnerability, Patch and Configuration (VPC) Management

- How can security vulnerability, patch and configuration management for an organization be extended to a cloud environment
- What is the impact of VPS on SaaS, PaaS and IaaS

Privacy

- Privacy and Data Life Cycle
- Key Privacy Concerns in the Cloud
- Who is Responsible for Privacy
- Privacy Risk Management and Compliance ion the Cloud
- Legal and Regulatory Requirements

Privacy and Data Life Cycle

- Privacy: Accountability of organizations to data subjects as well as the transparency to an organization's practice around personal information
- Data Life Cycle
  - Generation, Use, Transfer, Transformation, Storage, Archival, Destruction
  - Need policies

Privacy Concerns in the Cloud

- Access
- Compliance
- Storage
- Retention
- Destruction
- Audit and Monitoring
- Privacy Breaches

Who is Responsible for Privacy

- Organization that collected the information in the first place – the owner organization
- What is the role of the CSP?
- Organizations can transfer liability but not accountability
- Risk assessment and mitigation throughout the data lifecycle
- Knowledge about legal obligations

Privacy Risk Management and Compliance

- Collection Limitation Principle
- Use Limitation Principle
- Security Principle
- Retention and Destruction Principle
- Transfer Principle
- Accountab9lity Principle

Legal and Regulatory Requirements

- US Regulations
  - Federal Rules of Civil Procedure
  - US Patriot Act
  - Electronic Communications Privacy Act
  - FISMA
  - GLBA
  - HIPAA
  - HITECH Act
- International regulations
  - EU Directive
  - APEC Privacy Framework

Audit and Compliance

- Internal Policy Compliance
- Governance, Risk and Compliance (GRC)
- Control Objectives
- Regulatory/External Compliance
- Cloud Security Alliance
- Auditing for Compliance

Audit and Compliance

- Defines Strategy
- Define Requirements (provide services to clients)
- Defines Architecture (that is architect and structure services to meet requirements)
- Define Policies
- Defines process and procedures
- Ongoing operations
- Ongoing monitoring
- Continuous improvement

Governance, Risk and Compliance

- Risk assessment
- Key controls (to address the risks and compliance requirements)
- Monitoring
- Reporting
- Continuous improvement
- Risk assessment – new IT projects and systems

Control Objectives

- Security Policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information Security incident management
- Compliance
- Key Management

Regulatory/External Compliance

- Sarbanes-Oxley Act
- PCI DSS
- HIPAA
- COBIT
- What is the impact of Cloud computing on the above regulations?

Cloud Security Alliance (CSA)

- Create and apply best practices to securing the cloud
- Objectives include
  - Promote common level of understanding between consumers and providers
  - Promote independent research into best practices
  - Launch awareness and educational programs
  - Create consensus
- White Paper produced by CSA consist of 15 domains
  - Architecture, Risk management, Legal, Lifecycle management, applications security, storage, virtualization, - - - -

Auditing for Compliance

- Internal and External Audits
- Audit Framework
  - SAS 70
  - SysTrust
  - WebTrust
  - ISO 27001 certification
- Relevance to Cloud

Cloud Service Providers

1. Amazon Web Services (IaaS)
2. Google (SaaS, PaaS)
3. Microsoft Azure (SaaS, IaaS)
4. Proofpoint (SaaS, IaaS)
5. RightScale (SaaS)
6. Slaeforce.com (SaaS, PaaS)
7. Sun Open Cloud Platform
8. Workday (SaaS)

Security as a Service

- Email Filtering
- Web Content Filtering
- Vulnerability Management
- Identity Management

Impact of Cloud Computing

- Benefits
  - Low cost solution
  - Responsiveness flexibility
  - IT Expense marches Transaction volume
  - Business users are in direct control of technology decisions
  - Line between home computing applications and enterprise applications will blur
- Threats
  - Vested interest of cloud providers
  - Less control over the use of technologies
  - Perceived risk of using cloud computing
  - Portability and Lock-in to Proprietary systems for CSPs
  - Lack of integration and componentization

Directions

- Analysts predict that cloud computing will be a huge growth area
- Cloud growth will be much higher than traditional IT growth
- Will likely revolutionize IT
- Need to examine how traditional solutions for IAM, Governance, Risk Assessment etc will work for Cloud
- Technologies will be enhanced (IaaS, PaaS, SaaS)
- Security will continue o be a major concern