Applicability Analysis of Grid Security Mechanisms on Cloud Networking

Khan, Rasib Hassan
Department of Computer Science and Engineering
School of Science and Technology, Aalto University, Finland
rkhan@cc.hut.fi

Abstract

Grid computing has been around for quite a while. It facilitates utilization of distributed resources and has been extremely popular in its implementation. Grids have evolved enough to secure their operational architecture. On the other hand, Cloud computing offers more recent alternative in distributed virtualization of resources, providing an on-demand architecture for service charges. However, Cloud computing is still struggling with different approaches to secure its operations. This paper discusses the security mechanisms in Grid and Cloud computing, and based on the current implementations in Grid security, proposes a simple architecture for secured access control and policy enforcement system for Cloud networks.

1 Introduction

Grid technology has been evolving over the last decade. The problem Grids aim to solve is coordinated resource sharing and distributed computation, which is accomplished using a dynamic multi-institutional Virtual Organisation (VO). In Grids, a VO is referred to as an institution with resource sharing capabilities, who functions together with other VOs towards a common goal. In general, Grid architectures use standard and open general-purpose protocols. The physical resources are accessible through a middleware, which is shared by clusters of computing infrastructure. Therefore, when a user interacts with the Grid through the middleware, the information and the computational workload is virtualized by distributing them on a dynamic set of distributed resources on the Grid.

The existing security mechanisms in Grid computing concern the distributed nature of both the environment and the resources for computing. The security in Grids is primarily related to authentication and authorization of users with Single Sign-On, delegation of identity, integrity, confidentiality, and auditing.

Clouds provide a cyber-infrastructure which implies a service oriented model. Users are able to access the Cloud services from a much simpler service front-end, with greater flexibility and simplicity than Grids. Clouds provide a middleware for the users to access the services, which are located on third-party computing and storage facilities. Unlike Grids, Clouds provide virtualization of services at three different levels: infrastructure, platform, and software. Users can purchase services on any level, and use the services with a simple on-demand fashion or a Pay-Per-Use (PPU) model.

The security challenges in Cloud computing are similar to those in Grids. However, while security of the Cloud is guaranteed by the service provider, the security of the applications running on top of the services remain the responsibility of the users. The security issues in Clouds are related to access control, identity management, network security, storage protection, intrusion detection, and application and code management.

In this paper, we have discussed the operational architecture of Grid security and the security mechanisms available today. Further, we discuss the security issues in Clouds, and suggest an architecture for a secured access control and policy enforcement system in Cloud networks.

2 Grid Computing and Security

2.1 Grid Architecture Overview

A Grid is a collection of heterogeneous computers and resources. It can be defined as an architecture coordinating non-centralized resources, and is not subject to centralized administration. Grids spread over multiple administrative domains, and includes standard middleware APIs which provide users with access to resources. In grids, an administrative domain, or a VO is the collection of resources controlled by a single authority [11, 7]. The different administrative domains or the VOs should implement standardized interfaces, which collectively deliver standardized qualities of service. The architecture defines systems and applications which are responsible for integrating and managing the resources. The load on a Grid may vary and subsequently, a specific domain is able distribute computation to other VOs with variable quality of service [17, 8].

Grids are most commonly implemented with dynamic VOs [9]. The VOs comprise user groups from different domains that have associated privileges to access resources and services. Thus, as shown in figure 1, the VO has a common overlay of policies from different domains, which allows coordinated resource sharing[17]. It is this, the cross-domain functionality for coordinated resource sharing across multiple domains in Grids, that poses the primary challenge for security in Grids.
2.2 Security in Grids

The platforms in Grids are considered to be heterogeneous and dynamic. Security in Grids is not directed towards inter-domain trust, but rather aims to set up trust relationships based on VO acting as the bridge. The main issues addressed in Grid security are:

- Single Sign-On to enable users to log in only once and obtain access to multiple Grid domains and subsequently, simplify the task of accounting and auditing for the Grid providers.
- Delegation of access rights to other programs on the Grid to access other domains on the users’ behalf.
- Privacy and integrity for the access of resources, which should prevent unauthorized access to the domains, and prevent the data from being modified.
- Resource reservation and authorization for both local and global resources to implement the user specific policies.

The existing security mechanisms in Grid computing have been implemented in various ways. However, standardized Grid implementations provide security as follows:

- **Security Assertion Markup Language (SAML)** is an XML-based definition for security tokens to exchange identity information between multiple security domains or VO for authentication and authorization. The Community Authorization Service (CAS) [14, 4] is an architecture for policy management and enforcement, which uses SAML to authorize assertions between VOs, and enables resource providers to delegate policy authorities to other VOs.
- **X.509 long-term Certificates** are created for each user accessing resources on the Grid. For the purpose of cross-domain delegation for authentication and authorization of resources, for each X.509 certificate, multiple short-lived X.509 Proxy certificates are created and presented by the VOs at different resource boundaries of the different domains.
- **Extensible Access Control Markup Language (XACML)** is a declarative access control policy language implemented in XML, designed to express security policies and access rights. Access to resources in a Grid, and delegation of access rights for cross-domain authentication and access control are done with XACML defined policies.

One of the most dominant middleware for Grid deployments is called the Globus Toolkit (GT) [4, 3], which uses public key technology to address some of the authentication issues in Grids. Globus security is based on the Grid Security Infrastructure (GSI) [3]. GSI specifies a format for X.509 certificates [16], and requires SSL/TLS transport layer security protocol. A credential identity is formed using an X.509 certificate with the associated private key. Further, GSI has been extended to allow a user with a valid X.509 public key certificates to delegate certain privileges to a newly created X.509 identity certificate. This mechanism allows a dynamic delegation of privileges for a brief period of time, or even to delegate access rights to dynamically created services and entities. The dynamic creation of X.509 proxy certificates therefore simplifies the management of overlay trust domains, as per the requirement of VO overlays. This implicit trust establishment of dynamically created trust domains allows for a CAS to implement a flexible policy framework for authentication, authorization, delegation and resource management in Grids [17, 16].

The Open Grid Services Architecture (OGSA) [13] introduced further opportunities and challenges in the Grid infrastructure. The emergence of Web services has required the definition Web Service Security Policy (WS-Policy) with XACML in GT version 3. GT3 also defines standard formats for secured token exchange in web services to authorize assertions in VOs, which is done with the use of SAML and Web Service Security (WS-Security) [7, 17].

Later versions of GT attempt to address the security services of OGSA by focussing security functionality and publishing the policies. The published polices include mechanism requirements, trusted roots, token formats, and other parameters. This enables dynamic discovery of credentials with specifications of secured exchange of tokens with interoperability. The different security services can be described as the following:

- **Credential processing service** to handle the validation of authentication tokens;
- **Authorization services** to evaluate policy rules for the requester against the target domain;
- **Credential conversion service** to bridge different trust mechanisms in different domains;
- **Identity mapping service** to delegate the identity from one domain to another;
- **Auditing service** to securely log the resource utilization for specific users [13, 7, 17]
The different approaches for trust and security are all defined at the point of interaction with the enforcement point, usually called the Policy Enforcement Point (PEP), or Access Control Enforcement Point (AEF). As seen in figure 2, the PEP receives an access request from the client-side component, and gathers information relevant to an authorization request. Subsequently, the PEP then sends the authorization request to the Policy Decision Point (PDP) for evaluation. The PDP receives the authorization request from the PEP and evaluates the request against authorization policies retrieved from the Policy Administration Point (PAP). Upon successful authorization and evaluation of the policy, the result is sent back to the PEP, which then acts by allowing the request to proceed to the VO.

3 Cloud Computing and Security

3.1 Cloud Architecture Overview

There are multiple ways to define the term Cloud [1]. Ian Foster et. al in [5] have defined it as,

“A large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted, virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet”.

Clouds have allowed service providers to achieve diversity, distribution, and optimization in the utilization of resources. The term utility computing has been interchangeably used in the architecture of Clouds. Abstraction of the infrastructure and the point of interaction for the clients in Clouds has been defined as a Service-Oriented Architecture (SOA). A difference of Clouds and Grids in terms of scale and service can be seen in figure 3. Unlike Grids, Clouds are built on a service-based structure and resource virtualization.

The SOA in Clouds is usually defined in three distinct layers as shown in figure 4. Architecture of Clouds range from computational resources to any application layer service. The layers of Cloud computing services in SOA can be described as;

- **Infrastructure as a Service** (IaaS) provides virtual CPUs, disks, memory according to the user demands. Virtualization allows the IaaS providers to split, assign and dynamically resize the resources with flexibility to build ad-hoc systems as demanded by clients. However, the providers are only responsible for the operation of the data center, while the responsibility of the applications remain the responsibility of the clients.

- **Platform as a Service** (PaaS) acts as an abstraction between the physical resource and the service. Users demand a software component on the platform and the PaaS provider supply the software platform where systems run on, and also the application programming interfaces (APIs). Applications can then be deployed on the platform, together with other services like Cloud storage facilities, without the concern of resource availability and scaling up with an increasing utilization of the applications.

- **Software as a Service** (SaaS) provide end users with integrated services from the SaaS providers, comprising hardware, development platforms, and applications from the Cloud. SaaS are combined packages, and are deployed centrally at the data center of the SaaS provider which provides remote access to the users. The user simply avails the service over a web interface and have minimum visibility as compared to IaaS and PaaS.
3.2 Security Concerns in Clouds

Security in Cloud computing has been a challenge since the beginning. However, as Cloud services are provided by a single provider, the infrastructure is considered homogeneous. Users access the Cloud services over the Internet, and thus, the risks of web applications and remote access over the public network is the primary concern. In fact, Clouds have to face similar threats to those in traditional web applications and data centres.

With the present architecture of Cloud service networks, there are many options to exploit Clouds. As discussed in [10], some of the possible attacks are summarized as follows:

- **XML signature element wrapping:** A common use of XML signatures is authorization and authentication in Simple Object Access Protocol (SOAP) messages in web services. However, if the message is eavesdropped, the original body could be shifted to insert a new element, while the XML signature tag still remains in the SOAP message. Therefore, the modified SOAP message remains a valid request with an authentic signature from the owner, but carrying a request from the attacker. [12].

- **Phishing and browser based authentication attacks:** Cross-site scripting and phishing are significant problems associated with browser-based authentication mechanisms. Because browsers rely on third parties to provide authentication tokens (SAML tokens) to access Cloud services, the browser based authentication mechanism is always a window for attacks on Clouds.

- **Malware injection in clouds:** A simple attack on the Cloud system would be to inject a malicious application onto the platform. This also includes implementation of false service instances and tricking the Cloud network to redirect user requests to the malicious platform.

- **Spoofing meta-data:** One of the traditional attacks on web services is the spoofing and modification of metadata descriptions, where the Web Service Description Language (WSDL) call from a user is modified to perform some other action.

- **Direct and indirect denial of service:** An attacker floods the Cloud resources, thus consuming the computation power of the provider and the legitimate users would face Denial of Service (DoS). Subsequently, resources from other service instances would also be affected, thus, causing an indirect DoS on all other services residing on the same server.

3.3 Security Enhancement for Clouds

With the current business model of Cloud services, Cloud service providers take the responsibility of the services they provide (IaaS, Paas, SaaS). However, the security of the applications running on the services, primarily on the IaaS and PaaS platform, remains the responsibility of the clients. Security solutions are mostly implemented at the application level. Regardless, the risks and security implications on Clouds are targeted towards the following issues:

- **Firewalls and Network Security:** The firewalls and rules for the different user groups are targeted for filtering unauthorized access to services residing at the data center. Cloud service providers usually deploy virtual firewalls, which are stateful packet filters, running as applications in the Cloud environment. To further secure remote network access, clients can connect to the Cloud services over Virtual Private Networks (VPN), which gives them an isolated network layer [2].

- **Trust and Identity Managements (IDM):** For a secure browser based authentication and access control, a SAML token is sent inside an X.509 certificate. The SAML token thus replaces other identification information in the certificate. Subsequently, the SAML token is bound to the public key of the certificate [15], which removes the browser dependency on third-party certificates. Further, the token is bound to a certain SSL/TLS session, which ensures that the same SSL/TLS session is used for the request response sequence. This improves the trust model for a browser based access to Cloud services [10]. To ensure user centric access control, a trusted identity management (IDM) with active directory is implemented in the Cloud, and all authentication and authorization operations are performed within the firewall [6].

- **Storage and Code Protection:** Cloud service providers should ensure secured and isolated data storage and code protection for the clients. Privacy sensitive data requires privileged access, and the security for the service must comply to defined policies as stated by the providers to the users in the user agreement. The data centre resources in the Cloud system are shared by all the clients for storing data. Therefore, data segregation and isolation is also a primary concern and there should be a virtual boundary for the data stored in the Cloud. It is significantly important in terms of auditing, privacy and integrity [5]. This is implemented by the providers using different proprietary schemes, including Lightweight Directory Access Protocol (LDAP) and SAML coupled together for access requests, and X.509 certificates [6].
3.4 A Security Architecture for Clouds

An architecture for security mechanisms and policy enforcement in Clouds can be structured similar to the architecture as in Grids. A feasible architecture for authentication, authorization and access control is proposed and illustrated in figure 5. We have considered the design from a high level perspective, and describe the processing units in generalized terms.

Initially, in step 1, the client application communicates with the Security Administration Point (SEC-AP). The client application is usually a web browser, and contacts the URL of the provider, which is redirected to the SEC-AP. This initial connection depends on users’ choice, and can be made over VPNs, SSL/TLS, or Demilitarized isolated network (DMZ). A DMZ is usually a separate network, only for the link from the client site to the Cloud provider, and therefore isolates any other network traffic.

Upon receipt of a request from the user, the SEC-AP collects the user credential, and in step 2, consults the active directory for authentication of the request. Upon successful authentication, the SEC-AP sends back a X.509 certificate to the client as a token of trust in step 3.

At this point, in step 4, the client application contacts an SSL/TLS gateway at the provider’s edge, to contact the Policy Enforcement Point (PEP), presenting the X.509 certificate with a SOAP message for the resource request. This is done each time the client wishes to contact the Cloud services over a newly created connection. In steps 5 and 6, the PEP then performs similar actions as described in figure 2 in the previous section. At first, the request is sent to the Policy Decision Point (PDP). The PDP collaborates with the Policy Administration Point (PAP) and the active directory, to evaluate the resource request, and verifies the policy definition for the specific user.

Following a successful authorization for the requested resources, the PEP then sends back a confirmation to the client in step 7.1. Along with that, in step 7.2, the PEP creates dynamic X.509 Proxy certificates and uses SAML tokens to delegate the resource requests to the cloud services on behalf of the user.

4 Conclusion

In this paper, we have discussed about the current technologies in Grid and Cloud computing clusters, with respect to their architectures and the security principles. Because Grids have evolved over a longer period of time, they have a more mature security architecture. We have shown a number of approaches and descriptions of security mechanisms considering Grids and Clouds. Subsequently, we illustrated the concerns of Cloud networks and the current technologies used to overcome the barriers. We contributed by proposing a simplified service level architecture, for implementing a secured access control and policy enforcement system for Clouds. However, Cloud technology is still evolving, and no solution can yet be stated as the best approach. Further study on the architecture, and implementations is still needed.

References


