가상 이종시스템간의 보안 구조 분석

김정태

목원대학교

Analyses of Security Architecture for a Virtual Heterogeneous Machine

Jung-Tae Kim,

Mokwon University

E-mail : jtkim3050@mokwon.ac.kr

요 약

In this paper, we describe security for a virtual heterogeneous machine. Our security architecure is based on separation of services into for distinct system support for domains, where available. We have chosen to use emergong public key technology as an interim solution to provide domain seperation. Th proposed architecture has been analysed in numerically.

Ⅰ. Introduction

Since engineering and defence are witnessing the emergence of a new approach to computation. It depends not on single isolated centers of excellence for high performance computing, but upon a network of computers bound together by an overlying framework that presents to users a powerful virtual heterogeneous machine(VHM) intended to support high throughtput computing. Applications may consist of a single thread of execution, a set of sequential job, or may require a variety of computational and storage resources ranging from desktop PCs for the submission of jobs to supercomputers for computationally intensive tasks. The diversity of user population employing a VHM implies that one security solution may not be appropriate for all individuals or even for all tasks of one paticular individual.

Ⅱ. Management Sysem for Heterogeneous Networks

The intent of the Management system for Heterogeneous networks(MSHN) is to constructs a virtual heterogeneous machine designed to run as an application on a variety of operating systems and hardware platforms[1]. It will provide end-to-end support for applications in distributed and heterogeneous, shared environments. In addition to supporting computer-intensive jobs, MSHN is intended to provide a respective and flexible execution environment for real time, interactive, and I/O intensive tasks. When heterogeneous resources are simultaneously shared by several applications, each with its own unique quality of services requirement, MSHN will be able to efficiently assign resources to the applications so that they will atain their requested QoS. These early resource management system demonstrations lacked the ability to address quality of servicerequirements in a

highly distributed and dynamic heterogeneous envirnment. MSHN will address issues. It will monitor the load on a large pool of resources and will advise jobs as to the best strategy for achieving QoS objectives for a paticular run. It is anticipated that, despite the extra processing required for MSHN to provide monitoring and advisory services, the performance advantages will outweigh the slight computational tax imposed by the VHM. User involvement in the schedulaing and execution of jobs might be streamlined throught the use of a special MSHN shell that would hide MSHN processing. MSHN activity shows that the VHM depends upon communication between distributedhost: those providing MSHN core services and those executing client libries on behalf of users. We will present our approach to providing for the integrity of MSHN core components and client services within the networked environment. In addtion, we will describe how the MSHN core suports security requirements such as integrity and confidentiality for the jobs it manages.

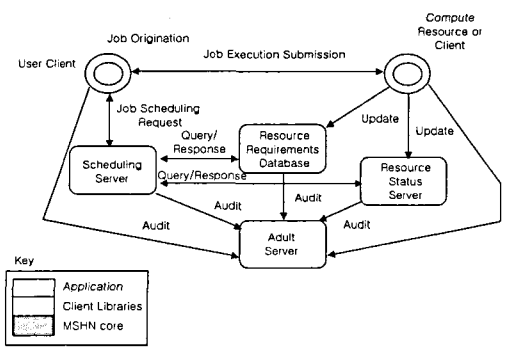

Fig 1. MSHN Architecture

Ⅲ. Security Requirements

The MSHN security mechanism are intented for environment in which users elect to use MSHN services to enhance the quality of service they receive on their job. Users request advisory schedules from MSHN services. When the schedule is returned, jobs are submitted to compute resources under user control and executed in the context of user accounts. Dynamic and summary job status information is reported to MSHN core services via client librarieswhich "wrap" the user's unaltered job. During jobexecution, the MSHN scheduler may send revised scheduling information to the client libraries. Under certain conditions, a job may be moved to a different compute conditions, a job may be moved to a different compute resource. If the job is adaptive, information relayed by the MSHN scheduler permits the job to modify its runtime characteristics in order to achieve desired quality of service goals.

Ⅳ. MSHN Security Architecture

MSHN security is based on the establishment of the following domains:[2]

1. MSHN core domain
2. Client Library Domain
3. Application Domain

Each domain will authenticate itself to other domains using certificate-based technology. The basis for believing the cetificates is the integrity provided at the certificate authorities, hence the certificate authorities are the most trusted components of our separated on a peak-task basis using appropriate keys supplied to each domain. Within MSHN, the highest integrity domain,

viz. the MSHN core, will manage the creation and allocation of session keys used by lower integritydomain. Thus the client domains are issued per-task keys when a job is scheduled and these keys are used for dynamic task management and core database update. In addition to being isolated on a pertask basis, each domain is able to distinguish communications from members at its integrity from those of entities of greater or lesser integrity.

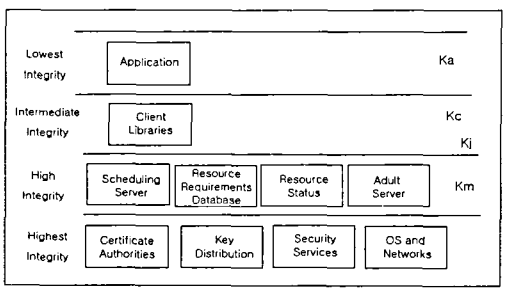

Fig 2. MSHN Security Domain Architecture

V. Mechanisms

Cryptographic mechanism will be used to isolate and protect the elements of the MSHN architecture in "lightweight" domains. Key types are symmetric, S, and public/private, P, cryptography. We inend to support update of session keys during job runs. The frequency of these updates will be defined as part of the quality of service for security. It is expected that, as the public key infrastructure matures, key distribution center(KDCs) will isssue public/private key pairs. In the interim, individual systems may be required to act as their own KDCs.

- Core keys
- Client and application keys
- User Authentication

VI. Common Data Security Architecture

The Intel Common Data Security Architecture(CDSA) has been used as the basis for a proof of concept demonstration of the MSHN core services. CDSA is intended to provide a basic security. It is a layered architecture and is intended to be modular, portable and adaptable. It has currently been implemented on Windows NT. An implementation of CDSA by RSA security is underway and will provide the components on UNIX platform using encryption software.

CDSA consosts of three primary layers:

- a set of system security services
- the Common Security Services Manager(CSSM)
- add-in security modules

The add-in security modules are organized by the CSSM so that services provider interfaces(SPIs) can be defined for each module job manager.

Services are separated into four catagories: cryptographic services: An add-in cryptographic service module can provide the following functions

- bulk encryption and decryption
- creation and verification of digital signatures
- cryptographic hash creation
- key generation
- random number generation
- encrypted storage of private keys. We note here that ultimately the protection of keys, must depend upon a system based protection mechanism.

Ⅶ. Summary

This paper describe a security architecture intended to support a virtual heterogeneous machine. A consistent set of choices must be made to construct data structures and mechanism use the underlying environment effectively. We build assurance into the system by relying on underlying mechanism rather than constructing our own. Our architecture for the MSHN VHM consists of four domains: the underlying operating system, MSHN Core Services, Client Services, and Application. Domains start with their own identification and authentication evidence provided by key distribution centers and certificate authorities. When the VHM is started, the Core Services establish their own cryptologically defined domain. Client Services submit requests to Core and are provided with session keys which estabish per-session domains that permit communication between Clients and Core Services.

References

[1] Tilmann H, "On/off phase shift keying for chaos encrypted communication using external cavity semiconductor lasers". IEEE J. of QE, v.38, n.9, sep. 2002, pp.1162-1170

[2] Shuo T, "Effects of message encoding and decoding on synchronized chaotic optical communication", IEEE J. QE, v.39,n.11, Nov, 1003, pp1468-1474