Plano de Estudos
MAC 5701 - Tópicos em Ciência da Compuação

José de Ribamar Braga Pinheiro Júnior (N.o USP: 4879050)
Orientador - Prof. Fábio Kon
IME - Instituto de Matemática e Estatística USP - Universidade de São Paulo

09 de abril de 2004

Sumário

1 Introdução

Este documento descreve o plano de estudos relativo à disciplina MAC 5701 - Tópicos em Ciência em Computação. Seu foco principal é apresentar as etapas a serem executadas durante a vigência do curso, suas motivações, objetivos e atividades realizadas. O trabalho a ser realizado cobrirá as áreas de sistemas distribuídos e segurança de dados.

2 Motivações

Com a popularização da informática no mundo, duas ocorrências contraditórias nos parecem bem claras: a definição crescente de problemas que demandam muito processamento e o aumento do parque computacional. Atualmente, computadores que se encontram comumente nos ambientes freqüentados por pessoas comuns tem a capacidade de processamento dos supercomputadores de uma década atrás. A possibilidade de permitir que estas máquinas, ociosas na maior parte do tempo, disponibilizem seus recursos computacionais para solucionar os problemas de outros usuários em uma rede de computadores, gerou a idéia da criação de uma infra-estrutura que os interconecte através de uma rede, denominada Computação em Grade (*Computacional Grid*).

As redes de computadores, em especial a internet, no entanto possuem um legado fatal: foram criadas sem a preocupação com a segurança dos dados por elas transmitidos [GS96a]. Naquela época as relações de segurança entre as partes envolvidas, que eram confiáveis e conhecidas, não obtiveram a preocupação necessária dos seus projetistas. A partir do momento que a arquitetura da internet (TCP/IP), mais recentemente , firmou-se como o padrão de fato das redes de computadores, estas herdaram o problema e técnicas adicionais tiveram que ser usadas para manter a segurança das informações [1].

Os computadores que participam das grades, também estão vulneráveis a problemas com a insegurança. Os seus sistemas operacionais podem não ser seguros o bastante, permitindo o acesso a recursos indevidos, ou códigos maliciosos podem ser executados de forma a se beneficiar de alguma falha na máquina para obter estes recursos [2]. Daí um problema grave nos sistemas de computação em grade: como garantir que as aplicações submetidas não causem prejuízos aos seus participantes. A solução seria implementar técnicas de segurança da informação para minimizar os possíveis problemas.

A segurança da informação possui quatro objetivos fundamentais: confidenciabilidade, integridade, disponibilidade e uso legítimo [For94]. A confidenciabilidade garante que as informações serão protegidas de entidades não autorizadas. A seguinte, a integridade, objetiva a consistências dos dados impedindo sua modificação de forma intencional ou não. A disponibilidade, garante que usuários legítimos terão o acesso aos recursos a que tem direito. E, finalmente, o uso legítimo determina que os recursos somente serão disponíveis a pessoas autorizadas.

[1] As técnicas utilizadas para proteger dados serão discutidas, em tempo, no relatório final da disciplina. Mais informações poderão ser obtidas em [GS96b]

[2] Técnicas bastante comuns, como o estouro de buffer *buffer overflow* [GS96a], podem ser utilizadas para obter acesso irrestrito aos recursos das máquinas

3 InteGrade

InteGrade [Kon04] é um projeto de computação em grade sendo desenvolvido pelo IME-USP (Instituto de Matemática e Estatística da Universidade de São Paulo). Implementado utilizando a tecnologia CORBA [Gro03], um padrão da industria para sistemas de objetos distribuídos, o InteGrade permite que aplicações paralelas sejam executadas em ambiente distribuído. Sua diferenciação dentre os demais sistemas de computação em grade, resume-se ao fato de ter sua arquitetura projetada de forma a diminuir os impactos ao usuário que disponibilizam seus recursos a grade. Seja por que é definido sobre uma arquitetura de objetos distribuídos padrão aberta, reutiliza a base computacional já instalada ou ainda teve como premissa de projeto da sua arquitetura, a prioridade aos processos do usuário nativo, minimizando os impactos a quem se disponibiliza a usá-la.

Atualmente o InteGrade encontra-se numa fase intermediária de desenvolvimento. O sistema já é executado em caráter experimental nos laboratórios do IME [3], permitindo que usuários cadastrados possam submeter suas aplicações. Uma grande equipe de pesquisadores e desenvolvedores continua trabalhando no projeto que inclui professores deste instituto e de outras universidades.

As definições das políticas de segurança e sua implementação foram definidas dentro do cronograma do projeto InteGrade para a presente fase. Como utiliza a infra-estrutura de comunicação da internet, o integrade recebe o legado de todas as ameaças presente naquela arquitetura. Uma ameaça é qualquer evento ou circunstância que permita comprometer a segurança de dados de um sistema [TS02]. Existem quatro tipos de ameaças que devem ser consideradas, a saber:

- **Interceptação** - refere-se ao acesso não autorizado a um determinado recurso ou serviço. Durante este processo, os dados poderiam, por exemplo, ser copiados pela escuta de um meio de comunicação de dois processos ou pelo acesso indevido a um sistema de arquivos.

- **Interrupção** - ocorre quando um dado ou um serviço é colocado indisponível. Ataques deste tipo são comumente denominados *Deny Of service* (negação de serviço).

- **Modificação** - consiste na alteração não autorizadas dos dados. Esta vulnerabilidade poderia ser realizada pela interceptação, modificação e retransmissão dos dados em uma rede de computadores, por exemplo.

- **Fabricação** - realizada através da criação de atividades e dados que não existam. Um intruso poderia, por exemplo, inserir entradas em um arquivo de senhas ou em tabelas de banco de dados.

Em função destas ameaças, definiu-se preliminarmente as seguintes políticas de segurança [4]:

- A comunicação entre os processos dos nós participantes do cluster e o seu gerenciador (veja a arquitetura do InteGrade em [Kon04]), deverá garantir confidenciabilidade e integridade dos dados;

[3] Laboratórios do LCPD e Eclipse do IME-USP

[4] Possivelmente estas políticas poderão ser revistas ao longo da execução do trabalho

- Caberá somente ao usuário do sistema, garantir a segurança da aplicação submetida a grade;
- Um determinado usuário e/ou sua aplicação deverá ser identificado de maneira inequívoca e assinada na grade;
- Um determinado nó poderá definir o nível de acesso que será obtido pelos processos a ele submetido ou aos recursos nas máquinas hospedeiras (nó ou gerenciador);
- Os eventos gerados pelos sistemas de segurança serão divididos em níveis e poderão, se assim desejado, ser registrados.

  Diante deste contexto, notamos que o InteGrade necessita de uma implementação de segurança que proteja os seus dados das ameaças listadas a posteriori, segundo as políticas previamente definidas. Sabemos, no entanto, que implementar todas essas políticas carece de tempo e uma árdua pesquisa. Durante este trabalho consideramos a somente a implementação do terceiro ítem das políticas listadas.

4 Objetivos, atividades e cronograma

Objetiva-se neste trabalho, uma implementação de segurança no Integrade de forma a permitir que usuários e aplicações sejam identificados de maneira inquestionável. Tal definição impedirá, ou tornará muito difícil, que usuários mal intencionados desconhecidos possam submeter aplicações indevidas a grade, causando prejuízos aos seus usuários.

As atividade realizadas durante o trabalho serão:

1. Definição das necessidades de segurança
2. Estudo sobre a implementação de segurança nas grades computacionais existentes.
3. Definição da solução
4. Implementação

O cronograma abaixo apresenta como estas atividades serão realizadas no espaço de quatro meses.

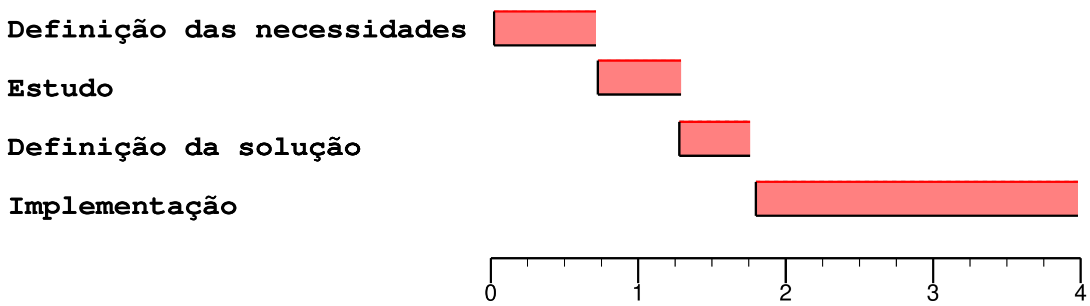

Figura 1: Diagrama de Entidade e Relacionamento.

Referências

[For94] W. Ford. *Computer Communications Security - Principles, Standard Protocols and Techniques*. Prentice-Hall, 1994.

[Gro03] Object Management Group. CORBA Security Service. http://www.omg.org/, 10 2003.

[GS96a] Simson Garfinkel and Gene Spafford. *Practical UNIX & Internet Security*. OŔeilly & Associates, Inc., 1996.

[GS96b] Simson Grafinkel and Gene Spafford. *Practical UNIX and Internet Security*. O'Reilly & Associates, Inc, 1996.

[Kon04] Fabio Kon. Integrade. http://gsd.ime.usp.br/Integrade, Abril 2004.

[TS02] Andrew S. Tanenbaum and Maarten Van Steen. *Distributed Systems. Principles and Paradigms*. Prentince Hall, 2002.