Aluno: Gabriel Paes

Professor: Fernando Buss

Ciência da Computação – Fundamentos de Sistemas distribuídos

28/06/2018

Sistemas Distribuídos: Importância da Segurança

A Segurança desempenha um papel fundamental em Sistemas Distribuídos, visto que uma variedade muito grande de políticas de segurança podem ser encontradas, deve-se entender que não faz sentido construir diversos tipos de mecanismos de segurança, sem ao menos conhecer seu funcionamento, sua qualidades e defeitos.

Basicamente sistemas distribuídos podem ser divididos em duas partes, comunicação entre usuários e processos por meio do uso de canais seguros na maioria dos casos, seguido pela segunda parte que trata principalmente dos direitos e recursos cabíveis a determinados processos.

Mas o que torna um sistema seguro?

Basicamente sistemas seguros são aqueles que nos garantem altos graus de confiabilidade (disponibilidade, capacidade de manutenção). Entretanto outros fatores são levados em consideração, podendo-se destacar:

- Confidencialidade

  Assegurando o acesso a informação somente aos autorizados;

- Integridade

  Deve garantir que em um sistema distribuído somente os autorizados tenham acesso a realizar alterações no sistema, sendo que toda alteração possa ser rastreada recuperável.

Um sistema distribuído deve estar apto a lidar com diversas situações que venham a causar problemas a harmonia da aplicação, que são as ameaças de segurança, são 4 os tipos de ameaças de segurança a se levar em consideração(Pfleeger.2003).

Tabela 1 – Ameaças de Segurança

Tipo	Características
Interceptação	Quando uma informação acaba por ser vista por um terceiro não autorizado devidamente, por exemplo acesso a uma pasta de arquivos que acabam por ser copiados ilegalmente
Interrupção	Acontece geralmente quando a comunicação se perde, deixando dados corrompidos, incompletos e até perdidos. Ataques de recusa de serviço entram nessa categoria
Modificação	A partir do momento que um sistema é alterado sem autorização para realizar uma tarefa que não deveria ele se enquadra nesta categoria. Por exemplo alterações em banco de dados ou o uso ilegal de softwares a partir do uso de ‘crack’

Invenção	Neste caso são geradas atividades extras as aplicações. Por exemplo a tentativa de adquirir senhas através de algum mecanismo que não deveria estar no sistema originalmente.

Portanto torna-se essencial o uso de políticas de segurança, para assegurar as atividades permitidas e as que são proibidas, a partir da delegação de cargos que as permitam ser executadas ou não.

A partir do momento que uma arquitetura de segurança é estipulada é irá focar em alguns mecanismos de segurança, deve-se destacar os seguintes: Criptografia, Autenticação, Autorização e Auditoria.

Um projeto de Sistema Distribuído deve contemplar diversas politicas de segurança, dando a diversas maneiras para que elas possam estar sendo implantadas.

Existem diversos focos de controle que podem ser utilizados pode-se focar em uma proteção direta, onde o foco é manter a integridade dos dados, garantindo que rotinas verifiquem todos os dados modificados.

Em uma outra abordagem temos mais rigidez nos controles de acesso, garantindo de uma forma mais eficiente, garantindo quais ações podem ser executadas. Estando fortemente ligado ao controle de acesso. Por exemplo garantindo os métodos que podem ser executados por uma outra aplicação dentro do sistema que esta sendo gerenciado.

Na terceira forma de abordagem é focar totalmente nos papéis ligados a cada usuário, garantindo desta forma que somente pessoas especificas tenham acesso a aplicação,

indiferente da ação que deseje executar. Podemos citar por exemplo acesso a informações restritas, como por exemplo informações pessoais em um sistema bancário, outro exemplo pode ser o de dados destinados somente a gerencia de uma empresa, sendo que o acesso a estas informações do banco de dados seja bastante restrita.

Deve estar clara também a diferença entre segurança e confiança nos Sistemas Distribuídos. Podemos assegurar um sistema seguro através de diversas técnicas de segurança, vários cálculos de probabilísticos entre outras técnicas, porém a confiança é na maioria das vezes algo emocional, todos os recursos de segurança que fogem ao essencial são devido ao nível de confiança que o cliente tem em relação a aplicação. Por exemplo protocolos de criptografia na troca de mensagens. Podemos citar alguns protocolos como o RPC e SSL por exemplo.

E como ocorre a distribuição de segurança em Sistemas Distribuídos?

Podemos citar principalmente a Criptografia, Autenticação e Delegação de Acesso, Firewall, Segurança em Código Móvel

O termo Criptografia surgiu da fusão das palavras gregas "Kryptós" e "gráphein", que significam "oculto" e "escrever", respectivamente. Trata-se de um conjunto de regras que visa codificar a informação de forma que só o emissor e o receptor consiga decifrá-la. Para isso várias técnicas são usadas, e ao passar do tempo modificada, aperfeiçoada e o surgimento de novas outras de maneira que fiquem mais seguras.

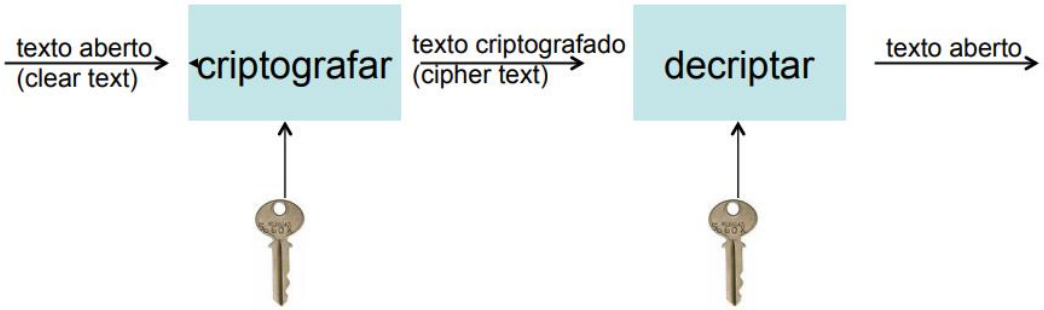

Figura 1 Criptografia

Autenticação e integridade sempre estão lado a lado, essas técnicas devem estar em harmonia, pois podem garantir a confidencialidade e qualidade dos dados.

Delegação de Recursos é de suma importância pois nos garantem que em um Sistema Distribuido, onde muitas máquinas diferentes possão executar suas tarefas sem problemas, desde que respeitando seus devidos privilégios, pois nesta interação vários processos estão acontencendo em diversos ambientes, é importante delegar estas autorizações para que o desempenho e melhor uso dos recursos seja aproveitado. Podendo até chegar até a operar em dominios administrativos diferentes.

Firewall, qu é um tipo especial de monitor de referência Controla os acesso aos recursos do sistema. Serve como uma proteção onde todo o tipo de comunicação, tanto de saída quanto de entrada, deve ser verificada para identificar sua autorização.

Segurança de Código Móvel onde o compartilhamento de códigos entre servidores provê uma quantidade de questões de segurança.

Diversos tópicos podem ser abordados em sistemas distribuidos levando em consideração o aspecto da segurança, em linhas gerais podemos concluir que a segurança de sistemas computacionais é um tópico universal em computação, com suas ideias e paradigmas aplicáveis nos mais diversos âmbitos e cenários, incluindo, claro, Sistemas

Distribuídos. Cada elemento do sistema não deve ser negligenciado, uma vez que, sem segurança, não se pode haver garantias do bom funcionamento do sistema como um todo. Nesse tipo de sistema, não podemos menosprezar a segurança, pois a informação é a peça central de todo o funcionamento do sistema a segurança se encontra no mesmo nível de segurança, já que o controle dessa informação distribuída lógica e geograficamente exige maior atenção e cuidado.Segurança não é, algo estático, segurança é antes de tudo uma ideologia de trabalho, que vive em constante evolução, e essencial para que possamos projetar cada vez sistemas que garantam mais integridade e confiabilidade aos usuários ao longo do tempo.