Você sabia que seu material didático é interativo e multimídia?
Ele possibilita diversas formas de interação com o conteúdo, a qualquer hora e de qualquer lugar. Mas na versão impressa, alguns conteúdos interativos são perdidos, por isso, fique atento! Sempre que possível, opte pela versão digital.
Bons estudos!

Imprimir

# Sistemas Distribuídos

Segurança em sistemas distribuídos

Unidade 4 – Seção 1

Frequentemente vemos ameaças, como vírus, tentando infiltrar em algum programa de senha. Assim, nessa essa webaula vamos conhecer algumas características importantes sobre a segurança em sistemas distribuídos.

## Características da segurança de sistemas distribuídos

Todo sistema distribuído implementado têm, como um dos principais e mais importantes, aspectos de projeto a segurança, conforme estudado anteriormente. Em um sistema distribuído temos uma série de componentes de hardware e software, físicos ou virtualizados, que se comunicam para a execução das aplicações distribuídas. Por conta disso vários tipos de ameaças podem afetar a segurança de nossos sistemas.

Podemos dividir a parte de segurança de sistemas distribuídos em duas: Permissão de acessos a serviços e recurso disponíveis no sistema e comunicação entre máquinas que contém mais de um processo e usuários diferentes (GOODRICH e TAMASSIA, 2012).

Podemos relacionar a segurança de um sistema distribuído aos seguintes fatores:

Confidencialidade: significa que a informação só estará disponível para os usuários ou máquinas autorizadas. Uma das formas de se garantir confidencialidade das mensagens é através do uso de Autenticação baseada em chave privada.

Aplicando esses fatores, que acabamos de conhecer, temos o objetivo de proteger o canal de comunicação de nossas aplicações, tornando assim canais seguros em nossos sistemas distribuídos. O grande objetivo de nossa aplicação distribuída é que ela possa se comunicar, ou seja, trocar dados, com confiabilidade, integridade e autenticidade. Portanto, uma das principais formas de proteção é deixar a comunicação permitida apenas em máquinas e por usuários autenticados em nosso sistema e com as permissões necessárias.

## Ameaças ao sistema distribuído

Para produzir um sistema que seja seguro contra diversas ameaças, precisamos aprender classificar essas ameaças e entender seus os métodos de ataque. As ameaças aos sistemas distribuídos podem ser divididas nas seguintes classes (COULOURIS et al, 2013):

| |
|---|
| Leakage (vazamento) |
| Acesso a informação por agentes não autorizados. |
| Tampering (falsificação) |
| Vandalism (vandalismo) |

Para que o invasor consiga violar um sistema através de algumas das estratégias apresentadas anteriormente, é necessário acessá-lo. Geralmente, todas as máquinas que compõem um sistema distribuído têm canais de comunicação para acesso autorizado às suas facilidades, e através desses canais de comunicação que o acesso não autorizado pode ocorrer.

As estratégias de violações de segurança em sistemas distribuídos dependem da obtenção de acesso aos canais de comunicação de nosso sistema, ou do estabelecimento de canais que escondem conexões, com a autoridade desejada. Fazem parte destas estratégias:

Eavesdropping | Masquerading | Message tampering | Replaying

Acesso a cópias de mensagem sem autorização. Geralmente essa estratégia funciona através da captura de mensagens da rede. Por exemplo, usando a Internet um computador pode se passar por outro, quando configurado com o endereço de rede de outro, desta forma ele pode receber as mensagens endereçadas a outro destinatário.

Para os invasores conseguirem acesso ao sistema é utilizado um método simples de infiltração que pode ser o uso de programas de quebra de senhas para obter as chaves de acesso de algum usuário do sistema. Além desta forma simples e não muito eficaz de invasão, existem outras maneiras mais sutis, que estão se tornando bem conhecidas:

Cavalo de Tróia
(*Trojan Horse*)

Vírus

Worm

Spyware

Keyloggers

Backdoor

Adware

Exploits

Hoax

Estudamos alguns tipos de ameaças em sistemas distribuídos. Para complementar seu conhecimento, acesse o livro didático.