CENTRO PAULA SOUZA

GOVERNO DE SÃO PAULO

Sistemas Operacionais

Fatec Taubaté

Aula 10

Segurança de Sistemas

Profa. Divani Barbosa Gavinier divani.gavinier@fatec.sp.gov.br

Tópicos Complementares

Aula 10: Segurança de Sistemas

- Segurança de Sistemas
- Propriedades de Segurança
- Princípios de Segurança
- Conceitos: Ameaças, Vulnerabilidade, Ataque e *Malware*

Segurança de Sistemas

A segurança de um sistema computacional diz respeito à garantia de algumas propriedades fundamentais associadas as "informações" presentes nesse sistema.

Por "informação", compreenda todos os recursos disponíveis no sistema.

São os arquivos, áreas de memória, portas de entrada/saída, conexões de rede, registros de bancos de dados, etc.

3

Propriedades e Princípios de Segurança

A segurança de um sistema computacional pode ser expressa através de algumas propriedades fundamentais, sendo elas:

- Confidencialidade,
- Integridade,
- Disponibilidade,
- Autenticidade e
- Irretratabilidade

4

Propriedades de Segurança

Confidencialidade: os recursos presentes no sistema só podem ser consultados por usuários devidamente autorizados a isso;

Integridade: os recursos do sistema só podem ser modificados ou destruídos pelos usuários autorizados a efetuar tais operações;

Disponibilidade: os recursos devem estar disponíveis para os usuários que tiverem direito de usá-los, a qualquer momento;

5

Propriedades de Segurança

Irretratabilidade: Todas as ações realizadas no sistema são conhecidas e não podem ser escondidas ou negadas por seus autores;

Autenticidade: todas as entidades do sistema são autênticas ou genuínas;

Ou seja, todos os dados presentes no sistema computacional correspondem às informações do mundo real que elas representam, como as identidades dos usuários, a origem dos dados de um arquivo, etc.

6

Propriedades de Segurança

Essas propriedades podem estar sujeitas a violações decorrentes de:

- Erros de software,
- Usuários bem e
- Mal intencionados (maliciosos), internos ou externos ao sistema.

É função do SO garantir a manutenção das propriedades de segurança para todos os recursos sob sua responsabilidade.

7

Propriedades e Princípios de Segurança

Essas propriedades podem estar sujeitas a violações decorrentes de:

- Erros de software,
- Usuários bem e
- Mal intencionados (maliciosos), internos ou externos ao sistema.

Sendo assim, a construção de um SO seguro é pautada por uma serie de princípios que devem levar em conta:

- A construção do SO,
- O comportamento dos usuários e
- dos possíveis atacantes.

É função do SO garantir a manutenção das propriedades de segurança para todos os recursos sob sua responsabilidade.

8

Princípios de Segurança

Os princípios de segurança mais relevantes são:

1. Privilégio mínimo,
2. Mediação completa,
3. Default seguro,
4. Economia de mecanismo,
5. Separação de privilégios,
6. Compartilhamento mínimo,
7. Proteção adequada,
8. Facilidade de uso e
9. Eficiência

Princípios de Segurança

1. Privilégio mínimo: garantir que todos os usuários e programas devem operar com o mínimo possível de privilégios ou permissões de acesso.
Dessa forma, os danos provocados por erros ou ações maliciosas intencionais serão minimizados.

2. Mediação completa: garantir que todos os acessos a recursos, devem ser verificados pelos mecanismos de segurança.

3. Default seguro: o mecanismo de segurança deve identificar claramente os acessos permitidos; caso um certo acesso não seja permitido, ele deve ser negado.

4. Economia de mecanismo: o projeto de um sistema de proteção deve ser pequeno e simples, para que possa ser facilmente e profundamente analisado, testado e validado.

Princípios de Segurança

5. Separação de privilégios: sistemas de proteção baseados em mais de um controle são mais robustos, pois se o atacante conseguir burlar um dos controles, mesmo assim não terá acesso ao recurso.

Exemplo: O uso de mais de uma forma de autenticação para acesso ao sistema (como nos sistemas bancários onde se usa além de um cartão, uma senha).

6. Compartilhamento mínimo: mecanismos compartilhados entre usuários são fontes potenciais de problemas de segurança, devido à possibilidade de fluxos de informação imprevistos entre usuários. Por isso, o uso de mecanismos compartilhados deve ser minimizado.

Princípios de Segurança

7. Proteção adequada: cada recurso computacional deve ter um nível de proteção coerente com seu valor intrínseco.

Exemplo: o nível de proteção requerido em um servidor Web de serviços bancário é bem distinto daquele de um terminal público de acesso à Internet.

8. Facilidade de uso: o uso dos mecanismos de segurança deve ser fácil e intuitivo, caso contrário eles serão evitados pelos usuários.

9. Eficiência: os mecanismos de segurança devem ser eficientes no uso dos recursos computacionais, de forma a não afetar significativamente o desempenho do sistema ou as atividades de seus usuários.

Princípios de Segurança

Esses princípios devem pautar a construção, configuração e operação de qualquer sistema computacional com requisitos de segurança

A maioria dos problemas de segurança dos sistemas atuais provém da não observação desses princípios

13

Ameaças

A ameaça seria qualquer ação que coloca em risco as Propriedades de Segurança.

Confidencialidade, Integridade, Disponibilidade, Autenticidade e Irretratabilidade

Sendo assim, as ameaças podem ou não se concretizar, dependendo da serie de Princípios de Segurança levados em consideração durante a construção do SO.

14

Ameaças

Tipos e exemplos de ameaças:

Ameaças à confidencialidade: um processo vasculhar as áreas de memória de outros processos, arquivos de outros usuários, tráfego de rede nas interfaces locais ou áreas do núcleo do sistema, buscando dados sensíveis como números de cartão de crédito, senhas, e-mails privados, etc.;

Ameaças à integridade: um processo alterar as senhas de outros usuários, instalar programas, drives ou módulos de núcleo maliciosos, visando obter o controle do sistema, roubar informações ou impedir o acesso de outros usuários;

Ameaças à disponibilidade: um usuário alocar para si todos os recursos do sistema, como a memória, o processador ou o espaço em disco, para impedir que outros usuários possam utilizá-lo.

15

Vulnerabilidades

Uma vulnerabilidade é um defeito ou problema (intencional ou não) presente no código de um aplicativo ou do próprio SO, que possa ser explorado para violar as Propriedades de Segurança.

16

Vulnerabilidades

Alguns exemplos de vulnerabilidades são:

1. Um erro de programação no serviço de compartilhamento de arquivos, que permita a usuários externos o acesso a outros arquivos do computador local, além daqueles compartilhados;

2. Uma conta de usuário sem senha, ou com uma senha pré-definida pelo fabricante, que permita a usuários não-autorizados acessar o sistema;

3. Ausência de quotas de disco, permitindo a um único usuário alocar todo o espaço em disco para si e assim impedir os demais usuários de usar o sistema.

17

Ataques

Um Ataque é o ato de utilizar (ou explorar) uma vulnerabilidade para violar uma Propriedade de Segurança.

Existem 4 tipos de ataques, sendo eles:

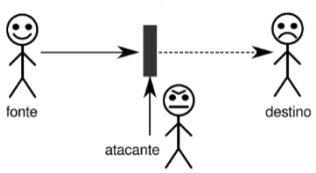
1. Interrupção
   Ataque a disponibilidade do sistema
2. Interceptação
   Ataque à confidencialidade do sistema
3. Fabricação
   Ataque à autenticidade do sistema
4. Modificação

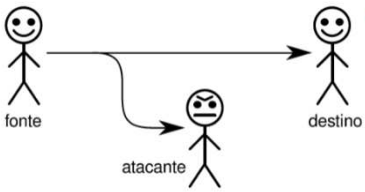
18

Ataques

1. Interrupção (ataque à disponibilidade do sistema)

Consiste em impedir o fluxo normal das informações ou acessos.





2. Interceptação (ataque à confidencialidade do sistema)

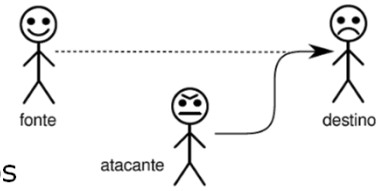
Consiste em obter acesso indevido a um fluxo de informações, sem necessariamente modificá-las.

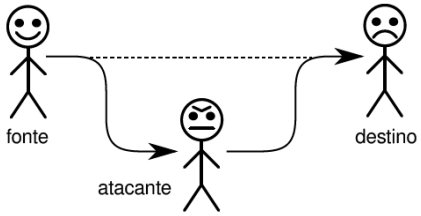
19

Ataques

3. Fabricação (ataque à autenticidade do sistema)

Consiste em produzir informações falsas ou introduzir módulos ou componentes maliciosos no sistema.





4. Modificação

Consiste em modificar de forma indevida informações ou partes do sistema, violando sua integridade.

20

Malwares

Malware é todo programa cuja intenção é realizar Ataques.

Existe uma grande diversidade de *malwares*, destinados às mais diversas finalidades, que podem ser divididos em diferentes categorias.

21

Malwares

Categorias de *Malwares*:

Vírus

É um trecho de código que se infiltra em programas executáveis existentes no SO, usando-os como suporte para sua execução e replicação.

Quando um programa "infectado" é executado, o vírus também se executa, infectando outros executáveis e eventualmente executando outras ações danosas.

22

Malwares

Worm

Ao contrário de um vírus, um "verme" é um programa autônomo, que se propaga sem infectar outros programas.

Uma vez instalado em um sistema, o verme pode instalar *Spywares* ou outros programas nocivos.

Programas construídos com a finalidade de se realizar ataques de interceptação, consistem em obter acesso indevido ao fluxo de informações (ataque a confidencialidade do sistema).

23

Malwares

Trojan

Ou "cavalo de Tróia" é um programa com duas funcionalidades:
uma funcionalidade lícita conhecida de seu usuário e outra ilícita, executada sem que o usuário a perceba.

Muitos cavalos de Tróia são usados como vetores para a instalação de outros *malwares*.

24

Malwares

Exploit

Um programa escrito para explorar vulnerabilidades conhecidas de algum SO.

Essa exploração pode ser realizada como:

- Prova de conceito (atividade licita) ou
- Parte de um ataque (atividade ilícita).

Os *exploits* podem estar incorporados a outros *malwares* (como *worm* e *trojans*) ou fazerem parte de alguma ferramenta autônoma, usadas em ataques manuais.

25

Malwares

Keylogger

Software dedicado a capturar e analisar as informações digitadas pelo usuário na máquina local, sem seu conhecimento.

Essas informações podem ser transferidas a um computador remoto periodicamente ou em tempo real, através da rede.

Packet Sniffer

Um "farejador de pacotes" captura pacotes de rede do próprio computador ou da rede local, analisando-os em busca de informações sensíveis como senhas e dados bancários.

26

Malwares

Rootkit

Um conjunto de programas destinado a ocultar a presença de um intruso no SO.

Como princípio de funcionamento, ele modifica os mecanismos do SO que mostram os processos em execução, arquivos nos discos, portas e conexões de rede, etc., para ocultar o intruso.

Versões mais elaboradas de *rootkits* substituem bibliotecas do SO ou modificam partes do próprio núcleo, o que torna complexa sua detecção e remoção.

27

Malwares

Backdoor

Ou "porta dos fundos" é um programa que facilita a entrada posterior do atacante em um sistema já invadido.

Geralmente a porta dos fundos é criada através um processo servidor de conexões remotas.

Muitos *backdoors* são instalados a partir de *trojans*, *worm* ou *rootkits*.

28

Atividades - Aula 10

62. Quais são as cinco propriedades fundamentais de segurança de um sistema computacional? Descreva a função de cada uma delas.
63. Descreva ameaça, vulnerabilidade, ataque e malware.
64. Quais são e no que consiste os quatro diferentes tipos de ataque?
65. Qual a diferença entre vírus, worm e trojan?
66. Qual a diferença entre exploit, rootkit e backdoor?