INSTITUTO FEDERAL
Santa Catarina

Proteção e Segurança

Os mecanismos de proteção controlam o acesso a um sistema limitando os tipos de acesso a arquivos permitidos aos usuár
Além disso, a proteção deve assegurar que somente processos que tenham recebido autorização apropriada do sistema
operacional possam operar sobre segmentos de memória, a CPU e outros recursos.

Proteção é fornecida por um mecanismo que controla o acesso de programas, processos ou usuários aos recursos definidos
um sistema de computação. Esse mecanismo deve fornecer um meio para especificar os controles a serem impostos juntam
com um meio de exigi-los.

Segurança garante a autenticação de usuários dos sistemas para proteger tanto a integridade das informações armazenadas
sistema (dados e código) quanto os recursos físicos do sistema de computação. O sistema de segurança impede o acesso n
autorizado, a destruição ou alteração maliciosa de dados e a introdução acidental de inconsistências.

INSTITUTO FEDERAL
Santa Catarina

Objetivos de Proteção:

À medida que os sistemas de computação têm se tornando mais sofisticados e difusos em suas aplicações, a necessidade d proteger sua integridade também tem aumentado. A proteção foi concebida originalmente como um complemento dos sistem operacionais com multiprogramação para que usuários não confiáveis pudessem compartilhar seguramente um espaço lógic nomes comum, tal como um diretório de arquivos, ou um espaço físico de nomes comum, tal como a memória. Os conceitos modernos de proteção evoluíram para aumentar a confiabilidade de qualquer sistema complexo que faça uso de recursos compartilhados.

O papel da proteção em um sistema de computação é fornecer um mecanismo para a imposição das políticas que governam uso de recursos. Essas políticas podem ser estabelecidas de várias maneiras. Algumas são fixadas no projeto do sistema, enquanto outras são formuladas pelo gerenciamento de um sistema. Ainda outras são definidas pelos usuários individuais pa proteção de seus próprios arquivos e programas. Um sistema de proteção deve ter flexibilidade para impor uma variedade d políticas.

As políticas de uso de recursos podem variar por aplicação e podem mudar com o tempo. Por essa razão, proteção não é m preocupação apenas do projetista de um sistema operacional. O programador de aplicações também precisa usar mecanism proteção para proteger os recursos criados e suportados por um subsistema de aplicação contra a má utilização. Neste capí descrevemos os mecanismos de proteção que o sistema operacional deve fornecer, mas os projetistas de aplicações tambén podem usá-los no projeto de seu próprio software de proteção.

Lembre-se de que mecanismos são diferentes de políticas. Os mecanismos determinam como algo será feito; as políticas decidem o que será feito. A separação entre política e mecanismo é importante para a flexibilidade. As políticas podem muda um local para outro ou de tempos em tempos. No pior caso, cada mudança na política demandaria uma mudança no mecan subjacente. O uso de mecanismos gerais habilita-nos a evitar tal situação.

Princípios de Proteção

Frequentemente, um princípio geral pode ser usado em todo um projeto, como o projeto de um sistema operacional. Seguir es princípio simplifica decisões de projeto e mantém o sistema consistente e fácil de entender. Um princípio geral testado pelo ten e essencial para a proteção é o princípio do privilégio mínimo. Ele determina que programas, usuários e até sistemas recebam privilégios apenas suficientes para a execução de suas tarefas.

Um sistema operacional que siga o princípio do privilégio mínimo implementa seus recursos, programas, chamadas de sistema estruturas de dados de modo que uma falha ou comprometimento de um componente cause um dano mínimo e permita que u dano mínimo seja causado. O estouro de um buffer em um daemon do sistema pode causar a falha do processo, por exemplo, mas não deve permitir a execução do código da pilha do processo daemon que habilitaria um usuário remoto a obter privilégios máximos e acessar o sistema inteiro (como acontece com muita frequência, atualmente).

Um sistema operacional também fornece chamadas de sistema e serviços que permitem a programação de aplicações com controles de acesso refinados. Fornece mecanismos para habilitar privilégios, quando esses são necessários, e desabilitá-los quando não são mais necessários. Também é benéfica a criação de trilhas de auditoria para todo acesso a funções privilegiada trilha de auditoria permite que o programador, o administrador do sistema, ou o oficial responsável pelo cumprimento da lei rastreiem todas as atividades de proteção e segurança no sistema.

EXEMPLOS:

- Manter a integridade do SO;
- Proteger de usuários bizantinos;
- Proteger de usuários incompetentes;
- Aumenta confiabilidade detectando erros de interface.

Domínio de Proteção

Um sistema de computação é uma coleção de processos e objetos. Com objetos queremos nos referir tanto a objetos de hardware (tais como a CPU, segmentos de memória, impressoras, discos e drives de fita) quanto a objetos de software (t como arquivos, programas e semáforos). Cada objeto tem um nome exclusivo que o diferencia de todos os outros objetos sistema e pode ser acessado somente por meio de operações bem definidas e significativas. Objetos são, essencialment tipos abstratos de dados.

Um processo deve ter permissão para acessar apenas os recursos para os quais ele tenha autorização. Além disso, a qualquer momento, um processo deve ser capaz de acessar somente os recursos de que precisa para executar sua taref Esse segundo requisito, normalmente referenciado como princípio conhecer-o-necessário, é útil ao limitar o nível de dano um processo incorreto pode causar ao sistema. Por exemplo, quando o processo p invoca o procedimento A( ), o procedimento deve ser autorizado a acessar somente suas próprias variáveis e os parâmetros formais passados a ele; el deve ser capaz de acessar todas as variáveis do processo p.

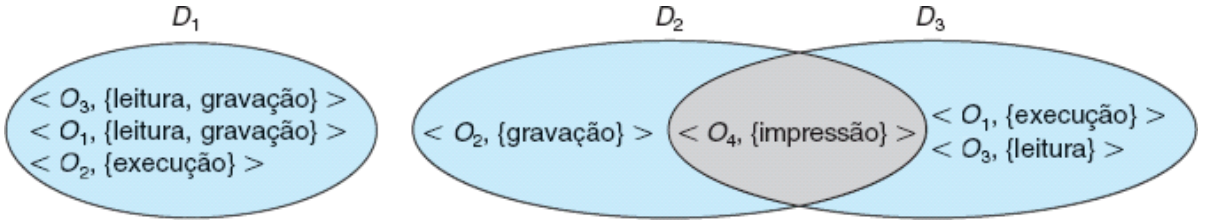
Exemplos de Domínios de Proteção:

Multics:

- Anéis de proteção:
  - cada anel é um domínio de proteção
  - Anéis vão de 0 a 7, 0 tem maior acesso
  - Anéis maiores são contidos em anéis menores.
- Modelo simplificado: dois anéis, 0: modo superusuário; 1: modo usuário.
- Sistema segmentado: cada segmento pertence a um anel.
- Além disto, cada segmento tem 3 bits rwx.
- Troca de domínio acontece quando um processo executando em um anel chama outro em um anel diferente.

Estrutura de Domínio

Para facilitar o esquema que acabamos de descrever, um processo opera dentro de um domínio de proteção, que especifica os recursos que ele pode acessar. Cada domínio define um conjunto de objetos e os tipos de operações que podem ser invocadas sobre cada objeto. A capacidade de executar uma operação sobre um objeto é o direito de acesso. Um domínio é um conjunto de direitos de acesso, cada um deles sendo um par ordenado <nome-do-objeto, conjunto-de-direitos>. Por exemplo, se o domínio D tem o direito de acesso <arquivo F,{leitura,gravação}>, então um processo, sendo executado no domínio D, tanto pode ler quanto gravar o arquivo F. Ele não pode, no entanto, executar qualquer outra operação sobre esse objeto.



Domínios podem compartilhar direitos de acesso. Por exemplo, na Figura 14.1, temos três domínios: D1, D2 e D3. O direito de acesso <O4, {impressão}> é compartilhado por D2 e D3 implicando que um processo em execução em um desses dois domínios pode imprimir o objeto O4. Observe que um processo deve estar sendo executado no domínio D1 para ler e gravar o objeto O1, enquanto apenas processos no domínio D3 podem executar o objeto O1.

exemplo: Multics

Anéis de proteção:

cada anel é um domínio de proteção, Anéis vão de 0 a 7, 0 tem maior acesso, Anéis maiores são contidos em anéis menores

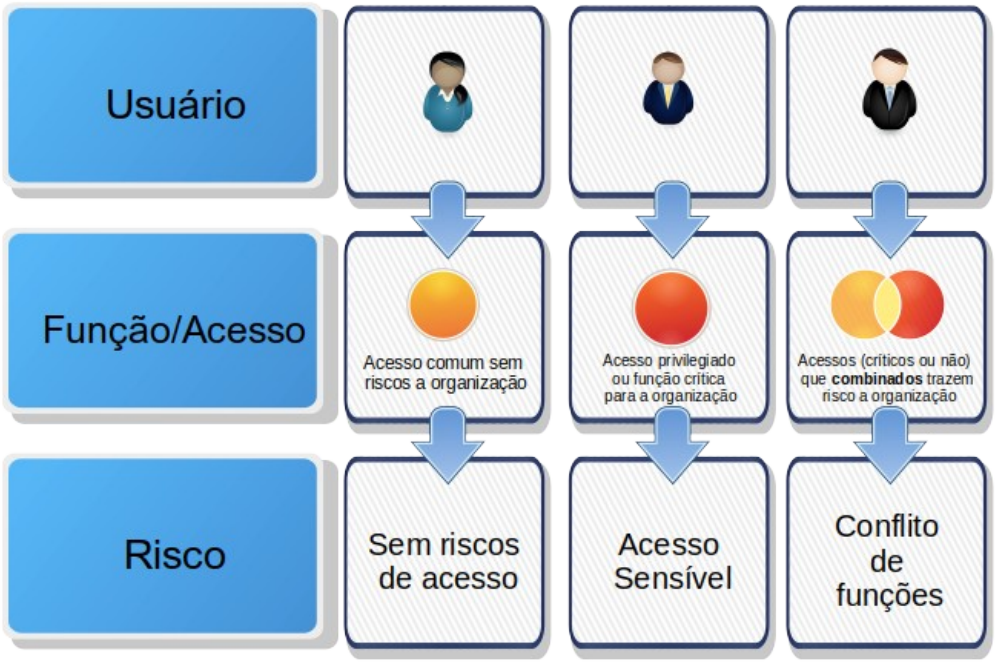
Além disto, cada segmento tem 3 bits rwx.

Matriz de Acesso

O esquema da matriz de acesso fornece-nos o mecanismo para a especificação de uma variedade de políticas. O mecanismo consiste na implementação da matriz de acesso e na garantia de que as propriedades semânticas que descrevemos são mantidas. Mais especificamente, devemos assegurar que um processo em execução no domínio Di pos acessar somente os objetos especificados na linha i, e somente conforme permitido pelas entradas da matriz de acesso.

A matriz de acesso pode implementar decisões políticas relacionadas com a proteção. As decisões políticas envolvem os direitos que devem ser incluídos na (i, j)-ésima entrada. Também devemos decidir o domínio em que cada processo é executado. Essa última política é usualmente decidida pelo sistema operacional.

Os usuários normalmente definem o conteúdo das entradas da matriz de acesso. Quando um usuário cria um novo objeto coluna é adicionada à matriz de acesso com as entradas de inicialização apropriadas, como definido pelo criador. O usuá pode decidir inserir alguns direitos em algumas entradas da coluna e outros direitos em outras entradas, conforme necessário.



INSTITUTO FEDERAL
Santa Catarina

Implementação da Matriz de Acesso

Seguindo o princípio do privilégio mínimo onde o intuito é definir o mínimo possível de acesso ao programa, sendo suficie
apenas para execução de suas tarefas e nada mais. As matrizes são montadas de forma a conceder as competências de
maneira eficiente e íntegra.

A forma como uma matriz é estruturada pode ser comparada à normalização de banco de dados, onde não há jeitos errad
de montar, apenas modos diferentes de executar a mesma função. Há 4 principais modos de montar a estrutura da matriz

- Tabela Global
- Lista de acesso para objetos
- Competências para Domínios
- Chave-Tranca

Antes de abordar estes métodos é necessário compreender alguns termos que serão utilizados:

- Domínio - É o conjunto de competências que o usuário / processo que recebe, essas competências estão relacionad
  a objetos;
- Objeto - É o destino ao qual as competências estão sendo aplicadas, um arquivo, uma pasta, um programa, etc;
- Competências - Conjunto de permissões que um domínio tem sobre determinado objeto.

INSTITUTO FEDERAL
Santa Catarina

Tipos de Matrizes

Tabela Global:

Os dados estão dispostos na tabela global por um conjunto de triplas ordenadas <domínio, objeto, competências>. Sempr
que uma operação é executada será verificado na tabela quais competências o domínio tem sobre o objeto.

Lista de acesso para objetos:

Cada objeto possui uma coluna na tabela, e nela há uma linha com um par ordenado de <domínio, conjunto de direitos>,
definindo todos os domínios com um conjunto não vazio de direitos de acesso para o objeto. Neste método é comum defi
um conjunto de direitos default, assim é mais rápido verificar primeiro os direitos default e em seguida a lista, caso a entra
não seja encontrada em nenhum dos dois o acesso é negado.

Lista de competências para domínios:

Neste modelo cada linha da matriz é representada por um domínio e cada uma recebe uma lista de competências, com a
informações de operações permitidas para cada objeto. A própria lista de competências é um objeto protegido, e apenas
indiretamente pelo usuário, assim mantendo bastante segura a lista de competências do domínio. Dentro da lista de
competências estão também presentes os objetos, que recebem uma etiqueta que denota se ele é um dado acessível ou
uma competência.

Mecanismo de Chave-Tranca:

Cada objeto tem um padrão exclusivo de bits, chamado de tranca, e cada domínio tem um padrão de bits chamado de
chave. Se a chave do domínio corresponder à tranca do objeto, o acesso é garantido, caso contrário, é recusado. A lista d
chaves e trancas é gerenciada pelo sistema operacional apenas, mantendo a integridade dos dados.

INSTITUTO FEDERAL
Santa Catarina

Controle de Acesso

Para cada arquivo e diretório é atribuído um proprietário, um grupo e/ou uma lista de usuários, e para cada uma dessas entidades são atribuídas informações de controle de acesso, definindo os privilégios de cada um.

INSTITUTO FEDERAL
Santa Catarina

Revogação de Direitos de Acesso

Para alterar os direitos de um domínio é necessário realizar a revogação das competências, ao realizar este processo pode-se remover todo o conjunto ou apenas alguma competência específica (revogação seletiva), para isso depende do método aplicado.

A revogação pode ser feita de forma seletiva ou geral, no caso da seletiva pode-se excluir competências individualmente, selecionando aquela que se deseja remover, na geral, todas as competências do domínio são excluídas, precisando definir novamente as competências que não desejava excluir.

A dificuldade em revogar as competências se dá pelo fato de que estão distribuídas por todo o sistema, devemos encontrá-las antes de poder revogá-las. Alguns esquemas que realizam a revogação para competências são os seguintes:

Requisição:

Periodicamente as competências são excluídas de cada domínio, um processo pode tentar readquirir a competência, caso tenha sido revogado não conseguirá readquiri-la, assim permanecendo sem os direitos (revogação geral).

Ponteiros de retaguarda:

Uma lista de ponteiros é mantida com cada objeto, esses ponteiros apontam quais competências estão associadas a ele. Quando a revogação é requerida, podemos seguir esses ponteiros, alterando as competências conforme necessário (revogação seletiva).

Revogação de Direitos de Acesso

Endereçamento indireto:

Neste método de revogação as competências apontam indiretamente para o objeto. Cada competência aponta para uma entrada exclusiva em uma tabela global, que, por sua vez, aponta para o objeto. Para revogar as competências, é deletad o caminho da tabela global, assim não estará mais apontando para o objeto (revogação geral).

Chaves:

Uma chave mestra é associada a cada objeto, quando uma competência é criada o valor da chave mestra é associado a ela. Quando a competência é usada as chaves são comparadas, se coincidirem o acesso é garantido. A revogação substitui a chave mestra por outra, invalidando todas as competências desse objeto (sem revogação seletiva).
Para conseguir a revogação seletiva, é adicionado uma tabela de chaves ao objeto, cada competência é vinculada a uma chave exclusiva, assim podendo excluí-las individualmente.

Problemas de Segurança

Hoje, com a vasta utilização do meio digital, o contexto de segurança é um dos assuntos ais falados na área da informática, proteção de dados, integridade de sistemas e prevenção contra ataques são algumas das principais preocupações daqueles que utilizam do meio digital no dia a dia.

Ao contrário do que é comum pensar, a preocupação com a segurança no meio digital deve ser levada muito mais a sério, seja num contexto empresarial, comercial ou até mesmo midiático, uma brecha de segurança que vaze dados de qualquer fonte pode ser crucial para a integridade do sistema ou base de dados ser comprometida.

A seguir as principais formas de ameaças à segurança::

- **Brecha de Sigilo**: envolve a leitura não autorizada de dados, sendo esse o objetivo mais comum de acesso não autorizado a dados.
- **Brecha de Integridade**: envolve a modificação não autorizada de dados, podendo resultar na alteração do código fonte de um sistema ou na transferência de responsabilidade de terceiros.
- **Brecha de Disponibilidade**: envolve a destruição não autorizada de dados.
- **Roubo de Serviço**: envolve a utilização não autorizada de recursos
- **Recusa de Serviço**: impedimento do uso legítimo de recursos.

INSTITUTO FEDERAL
Santa Catarina

Proteção e Segurança

Os mecanismos de proteção controlam o acesso a um sistema limitando os tipos de acesso a arquivos permitidos aos usuár
Além disso, a proteção deve assegurar que somente processos que tenham recebido autorização apropriada do sistema
operacional possam operar sobre segmentos de memória, a CPU e outros recursos.

Proteção é fornecida por um mecanismo que controla o acesso de programas, processos ou usuários aos recursos definidos
um sistema de computação. Esse mecanismo deve fornecer um meio para especificar os controles a serem impostos juntam
com um meio de exigi-los.

Segurança garante a autenticação de usuários dos sistemas para proteger tanto a integridade das informações armazenadas
sistema (dados e código) quanto os recursos físicos do sistema de computação. O sistema de segurança impede o acesso n
autorizado, a destruição ou alteração maliciosa de dados e a introdução acidental de inconsistências.

INSTITUTO FEDERAL
Santa Catarina

Objetivos de Proteção:

À medida que os sistemas de computação têm se tornando mais sofisticados e difusos em suas aplicações, a necessidade d proteger sua integridade também tem aumentado. A proteção foi concebida originalmente como um complemento dos sistem operacionais com multiprogramação para que usuários não confiáveis pudessem compartilhar seguramente um espaço lógic nomes comum, tal como um diretório de arquivos, ou um espaço físico de nomes comum, tal como a memória. Os conceitos modernos de proteção evoluíram para aumentar a confiabilidade de qualquer sistema complexo que faça uso de recursos compartilhados.

O papel da proteção em um sistema de computação é fornecer um mecanismo para a imposição das políticas que governam uso de recursos. Essas políticas podem ser estabelecidas de várias maneiras. Algumas são fixadas no projeto do sistema, enquanto outras são formuladas pelo gerenciamento de um sistema. Ainda outras são definidas pelos usuários individuais pa proteção de seus próprios arquivos e programas. Um sistema de proteção deve ter flexibilidade para impor uma variedade d políticas.

As políticas de uso de recursos podem variar por aplicação e podem mudar com o tempo. Por essa razão, proteção não é m preocupação apenas do projetista de um sistema operacional. O programador de aplicações também precisa usar mecanism proteção para proteger os recursos criados e suportados por um subsistema de aplicação contra a má utilização. Neste capí descrevemos os mecanismos de proteção que o sistema operacional deve fornecer, mas os projetistas de aplicações tambén podem usá-los no projeto de seu próprio software de proteção.

Lembre-se de que mecanismos são diferentes de políticas. Os mecanismos determinam como algo será feito; as políticas decidem o que será feito. A separação entre política e mecanismo é importante para a flexibilidade. As políticas podem muda um local para outro ou de tempos em tempos. No pior caso, cada mudança na política demandaria uma mudança no mecan subjacente. O uso de mecanismos gerais habilita-nos a evitar tal situação.

Princípios de Proteção

Frequentemente, um princípio geral pode ser usado em todo um projeto, como o projeto de um sistema operacional. Seguir es princípio simplifica decisões de projeto e mantém o sistema consistente e fácil de entender. Um princípio geral testado pelo ten e essencial para a proteção é o princípio do privilégio mínimo. Ele determina que programas, usuários e até sistemas recebam privilégios apenas suficientes para a execução de suas tarefas.

Um sistema operacional que siga o princípio do privilégio mínimo implementa seus recursos, programas, chamadas de sistema estruturas de dados de modo que uma falha ou comprometimento de um componente cause um dano mínimo e permita que u dano mínimo seja causado. O estouro de um buffer em um daemon do sistema pode causar a falha do processo, por exemplo, mas não deve permitir a execução do código da pilha do processo daemon que habilitaria um usuário remoto a obter privilégios máximos e acessar o sistema inteiro (como acontece com muita frequência, atualmente).

Um sistema operacional também fornece chamadas de sistema e serviços que permitem a programação de aplicações com controles de acesso refinados. Fornece mecanismos para habilitar privilégios, quando esses são necessários, e desabilitá-los quando não são mais necessários. Também é benéfica a criação de trilhas de auditoria para todo acesso a funções privilegiada trilha de auditoria permite que o programador, o administrador do sistema, ou o oficial responsável pelo cumprimento da lei rastreiem todas as atividades de proteção e segurança no sistema.

EXEMPLOS:

- Manter a integridade do SO;
- Proteger de usuários bizantinos;
- Proteger de usuários incompetentes;
- Aumenta confiabilidade detectando erros de interface.

Domínio de Proteção

Um sistema de computação é uma coleção de processos e objetos. Com objetos queremos nos referir tanto a objetos de hardware (tais como a CPU, segmentos de memória, impressoras, discos e drives de fita) quanto a objetos de software (t como arquivos, programas e semáforos). Cada objeto tem um nome exclusivo que o diferencia de todos os outros objetos sistema e pode ser acessado somente por meio de operações bem definidas e significativas. Objetos são, essencialment tipos abstratos de dados.

Um processo deve ter permissão para acessar apenas os recursos para os quais ele tenha autorização. Além disso, a qualquer momento, um processo deve ser capaz de acessar somente os recursos de que precisa para executar sua taref Esse segundo requisito, normalmente referenciado como princípio conhecer-o-necessário, é útil ao limitar o nível de dano um processo incorreto pode causar ao sistema. Por exemplo, quando o processo p invoca o procedimento A( ), o procedimento deve ser autorizado a acessar somente suas próprias variáveis e os parâmetros formais passados a ele; el deve ser capaz de acessar todas as variáveis do processo p.

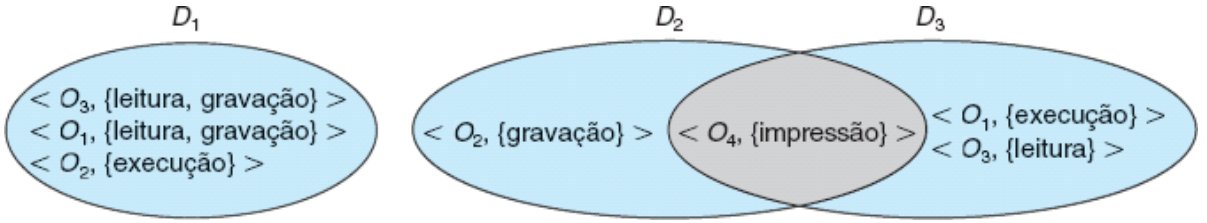
Exemplos de Domínios de Proteção:

Multics:

- Anéis de proteção:
  - cada anel é um domínio de proteção
  - Anéis vão de 0 a 7, 0 tem maior acesso
  - Anéis maiores são contidos em anéis menores.
- Modelo simplificado: dois anéis, 0: modo superusuário; 1: modo usuário.
- Sistema segmentado: cada segmento pertence a um anel.
- Além disto, cada segmento tem 3 bits rwx.
- Troca de domínio acontece quando um processo executando em um anel chama outro em um anel diferente.

Estrutura de Domínio

Para facilitar o esquema que acabamos de descrever, um processo opera dentro de um domínio de proteção, que especifica os recursos que ele pode acessar. Cada domínio define um conjunto de objetos e os tipos de operações que podem ser invocadas sobre cada objeto. A capacidade de executar uma operação sobre um objeto é o direito de acesso. Um domínio é um conjunto de direitos de acesso, cada um deles sendo um par ordenado <nome-do-objeto, conjunto-de-direitos>. Por exemplo, se o domínio D tem o direito de acesso <arquivo F,{leitura,gravação}>, então um processo, sendo executado no domínio D, tanto pode ler quanto gravar o arquivo F. Ele não pode, no entanto, executar qualquer outra operação sobre esse objeto.



Domínios podem compartilhar direitos de acesso. Por exemplo, na Figura 14.1, temos três domínios: D1, D2 e D3. O direito de acesso <O4, {impressão}> é compartilhado por D2 e D3 implicando que um processo em execução em um desses dois domínios pode imprimir o objeto O4. Observe que um processo deve estar sendo executado no domínio D1 para ler e gravar o objeto O1, enquanto apenas processos no domínio D3 podem executar o objeto O1.

exemplo: Multics

Anéis de proteção:

cada anel é um domínio de proteção, Anéis vão de 0 a 7, 0 tem maior acesso, Anéis maiores são contidos em anéis menores

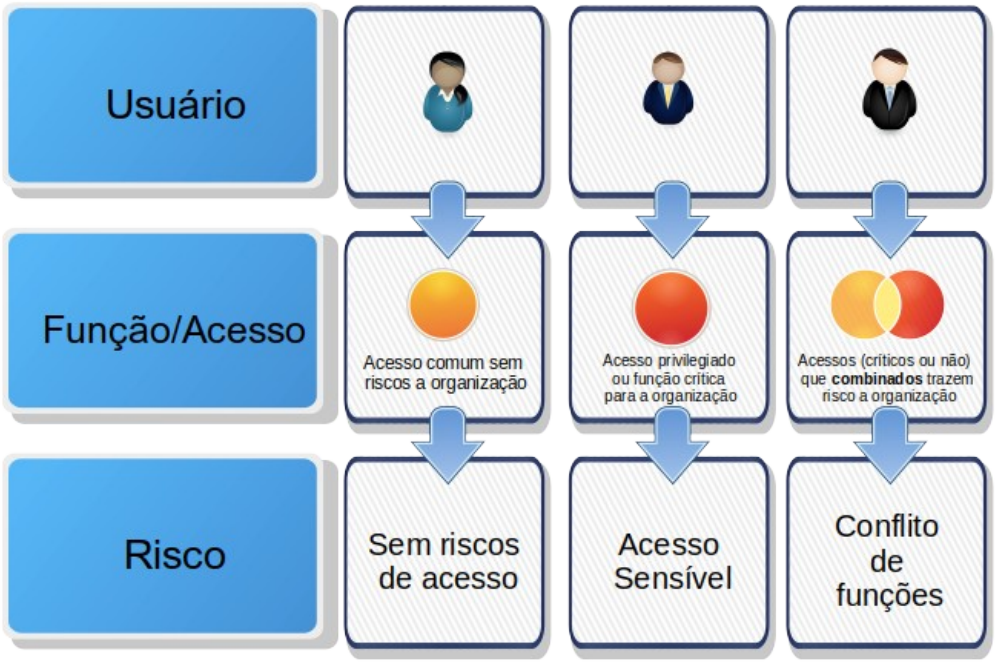
Além disto, cada segmento tem 3 bits rwx.

Matriz de Acesso

O esquema da matriz de acesso fornece-nos o mecanismo para a especificação de uma variedade de políticas. O mecanismo consiste na implementação da matriz de acesso e na garantia de que as propriedades semânticas que descrevemos são mantidas. Mais especificamente, devemos assegurar que um processo em execução no domínio Di pos acessar somente os objetos especificados na linha i, e somente conforme permitido pelas entradas da matriz de acesso.

A matriz de acesso pode implementar decisões políticas relacionadas com a proteção. As decisões políticas envolvem os direitos que devem ser incluídos na (i, j)-ésima entrada. Também devemos decidir o domínio em que cada processo é executado. Essa última política é usualmente decidida pelo sistema operacional.

Os usuários normalmente definem o conteúdo das entradas da matriz de acesso. Quando um usuário cria um novo objeto coluna é adicionada à matriz de acesso com as entradas de inicialização apropriadas, como definido pelo criador. O usuá pode decidir inserir alguns direitos em algumas entradas da coluna e outros direitos em outras entradas, conforme necessário.



INSTITUTO FEDERAL
Santa Catarina

Implementação da Matriz de Acesso

Seguindo o princípio do privilégio mínimo onde o intuito é definir o mínimo possível de acesso ao programa, sendo suficie
apenas para execução de suas tarefas e nada mais. As matrizes são montadas de forma a conceder as competências de
maneira eficiente e íntegra.

A forma como uma matriz é estruturada pode ser comparada à normalização de banco de dados, onde não há jeitos errad
de montar, apenas modos diferentes de executar a mesma função. Há 4 principais modos de montar a estrutura da matriz

- Tabela Global
- Lista de acesso para objetos
- Competências para Domínios
- Chave-Tranca

Antes de abordar estes métodos é necessário compreender alguns termos que serão utilizados:

- Domínio - É o conjunto de competências que o usuário / processo que recebe, essas competências estão relacionad
  a objetos;
- Objeto - É o destino ao qual as competências estão sendo aplicadas, um arquivo, uma pasta, um programa, etc;
- Competências - Conjunto de permissões que um domínio tem sobre determinado objeto.

INSTITUTO FEDERAL
Santa Catarina

Tipos de Matrizes

Tabela Global:

Os dados estão dispostos na tabela global por um conjunto de triplas ordenadas <domínio, objeto, competências>. Sempr
que uma operação é executada será verificado na tabela quais competências o domínio tem sobre o objeto.

Lista de acesso para objetos:

Cada objeto possui uma coluna na tabela, e nela há uma linha com um par ordenado de <domínio, conjunto de direitos>,
definindo todos os domínios com um conjunto não vazio de direitos de acesso para o objeto. Neste método é comum defi
um conjunto de direitos default, assim é mais rápido verificar primeiro os direitos default e em seguida a lista, caso a entra
não seja encontrada em nenhum dos dois o acesso é negado.

Lista de competências para domínios:

Neste modelo cada linha da matriz é representada por um domínio e cada uma recebe uma lista de competências, com a
informações de operações permitidas para cada objeto. A própria lista de competências é um objeto protegido, e apenas
indiretamente pelo usuário, assim mantendo bastante segura a lista de competências do domínio. Dentro da lista de
competências estão também presentes os objetos, que recebem uma etiqueta que denota se ele é um dado acessível ou
uma competência.

Mecanismo de Chave-Tranca:

Cada objeto tem um padrão exclusivo de bits, chamado de tranca, e cada domínio tem um padrão de bits chamado de
chave. Se a chave do domínio corresponder à tranca do objeto, o acesso é garantido, caso contrário, é recusado. A lista d
chaves e trancas é gerenciada pelo sistema operacional apenas, mantendo a integridade dos dados.

INSTITUTO FEDERAL
Santa Catarina

Controle de Acesso

Para cada arquivo e diretório é atribuído um proprietário, um grupo e/ou uma lista de usuários, e para cada uma dessas entidades são atribuídas informações de controle de acesso, definindo os privilégios de cada um.

INSTITUTO FEDERAL
Santa Catarina

Revogação de Direitos de Acesso

Para alterar os direitos de um domínio é necessário realizar a revogação das competências, ao realizar este processo pode-se remover todo o conjunto ou apenas alguma competência específica (revogação seletiva), para isso depende do método aplicado.

A revogação pode ser feita de forma seletiva ou geral, no caso da seletiva pode-se excluir competências individualmente, selecionando aquela que se deseja remover, na geral, todas as competências do domínio são excluídas, precisando definir novamente as competências que não desejava excluir.

A dificuldade em revogar as competências se dá pelo fato de que estão distribuídas por todo o sistema, devemos encontrá-las antes de poder revogá-las. Alguns esquemas que realizam a revogação para competências são os seguintes:

Requisição:

Periodicamente as competências são excluídas de cada domínio, um processo pode tentar readquirir a competência, caso tenha sido revogado não conseguirá readquiri-la, assim permanecendo sem os direitos (revogação geral).

Ponteiros de retaguarda:

Uma lista de ponteiros é mantida com cada objeto, esses ponteiros apontam quais competências estão associadas a ele. Quando a revogação é requerida, podemos seguir esses ponteiros, alterando as competências conforme necessário (revogação seletiva).

Revogação de Direitos de Acesso

Endereçamento indireto:

Neste método de revogação as competências apontam indiretamente para o objeto. Cada competência aponta para uma entrada exclusiva em uma tabela global, que, por sua vez, aponta para o objeto. Para revogar as competências, é deletad o caminho da tabela global, assim não estará mais apontando para o objeto (revogação geral).

Chaves:

Uma chave mestra é associada a cada objeto, quando uma competência é criada o valor da chave mestra é associado a ela. Quando a competência é usada as chaves são comparadas, se coincidirem o acesso é garantido. A revogação substitui a chave mestra por outra, invalidando todas as competências desse objeto (sem revogação seletiva).
Para conseguir a revogação seletiva, é adicionado uma tabela de chaves ao objeto, cada competência é vinculada a uma chave exclusiva, assim podendo excluí-las individualmente.

Problemas de Segurança

Hoje, com a vasta utilização do meio digital, o contexto de segurança é um dos assuntos ais falados na área da informática, proteção de dados, integridade de sistemas e prevenção contra ataques são algumas das principais preocupações daqueles que utilizam do meio digital no dia a dia.

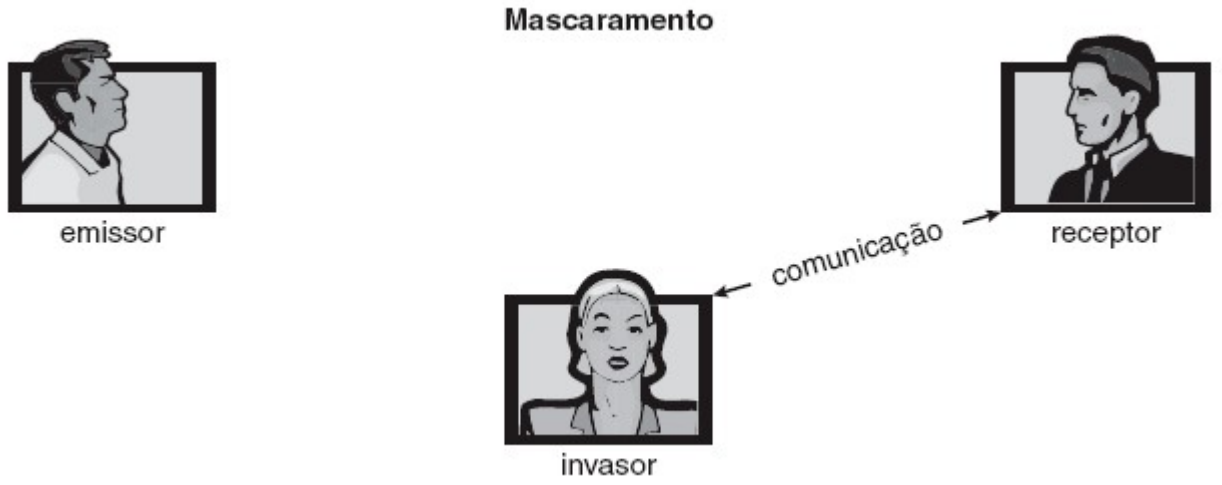
Ao contrário do que é comum pensar, a preocupação com a segurança no meio digital deve ser levada muito mais a sério, seja num contexto empresarial, comercial ou até mesmo midiático, uma brecha de segurança que vaze dados de qualquer fonte pode ser crucial para a integridade do sistema ou base de dados ser comprometida.

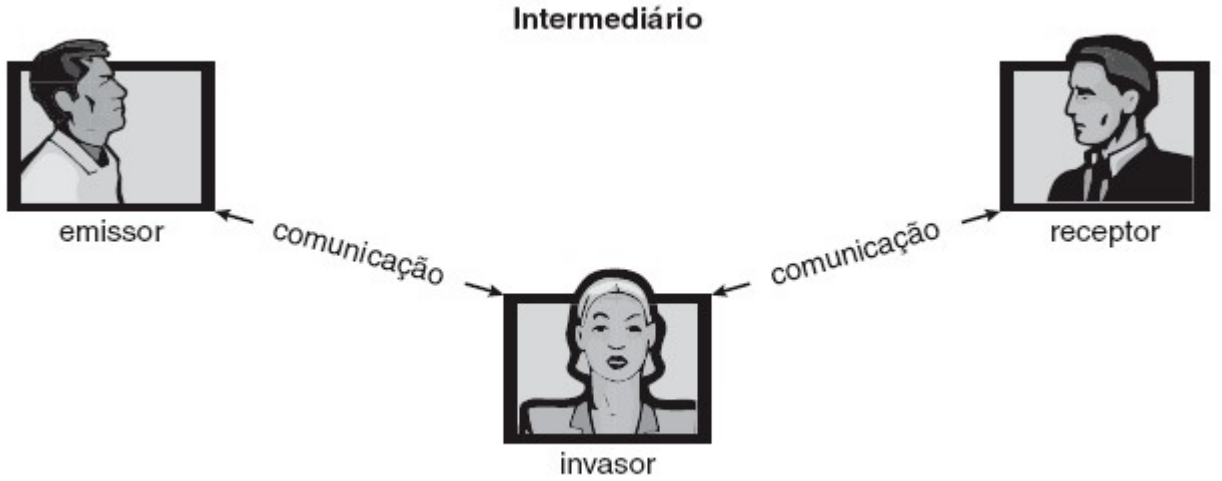
A seguir as principais formas de ameaças à segurança::

- **Brecha de Sigilo**: envolve a leitura não autorizada de dados, sendo esse o objetivo mais comum de acesso não autorizado a dados.
- **Brecha de Integridade**: envolve a modificação não autorizada de dados, podendo resultar na alteração do código fonte de um sistema ou na transferência de responsabilidade de terceiros.
- **Brecha de Disponibilidade**: envolve a destruição não autorizada de dados.
- **Roubo de Serviço**: envolve a utilização não autorizada de recursos
- **Recusa de Serviço**: impedimento do uso legítimo de recursos.

Outras formas de violação de segurança normais são:

- **Mascaramento**: o mascaramento acontece quando uma pessoa mal intencionada se passa por algum integrante válido do sistema e assim, tem acesso não autorizado a recursos e dados do sistema.
- **Intermediário**: o ataque do intermediário acontece quando um usuário não autorizado se instala no meio de um fluxo de dados(sequestro de sessão), agindo como intermediário desse fluxo e tendo acesso às informações que passam pelo mesmo





INSTITUTO FEDERAL
Santa Catarina

Fatores a serem considerados

É lógico considerar que mesmo tomando cuidado, é impossível ter uma segurança perfeita, são quase infinitos os casos que podem levar a uma brecha de segurança, sendo assim, para minimizar as chances do pior dos casos, são considerados 4 níveis de segurança:

- **Físico**: o lugar em que a base de dados (servidor) está instalada, levando em conta as condições do local, manutenção, acesso aos terminais, etc…
- **Humano**: é crucial para a segurança que apenas pessoal autorizado tenha acesso ao sistema, porém existe a possibilidade que esse pessoal seja influenciado por terceiros a permitir o acesso, o usuário pode ser enganado por sites e programas mal intencionados a dar suas credenciais ou ainda uma técnica usada chamada **dumpster diving** que consistem em coletar todos os “lixos” de informações do usuário na chance de encontrar alguma credencial ou dado importante em lugares como lixeiras, agendas, anotações, etc…
- **Sistema Operacional**: o sistema em si deve ter medidas de segurança a fim de prever, evitar e reparar brechas de segurança de origem interna, como erros de memória, estouros de pilha de processamento, integridade de credenciais, etc…
- **Rede**: um grande volume de dados percorre a rede tanto externa quanto interna, uma brecha de dados que se instale entre 2 ou mais pontos dessa rede deve ser considerada e evitada.

INSTITUTO FEDERAL
Santa Catarina

Ameaças de Programas

Um objetivo comum dos hackers e crackers é o acesso a dados do usuário através de programas e linhas de código mal intencionadas, levando em consideração que um programa que crie um processo que rode junto ao kernel com capacidade de criar uma brecha de segurança seria capaz de derrubar o sistema por inteiro, roubar grandes volumes de informações ou ambos.

As ameaças por programas mais comuns são:

- **Cavalo de Tróia**: fazendo alusão ao mito grego, esse são programas que podem parecer legítimos e instalados pelo usuário porém em seu código fonte possui processos que copiam dados (podendo ser através de sistemas de login falsos, sistemas de busca, processos ocultos, etc…) e os mandam para uma base de dados separada, sendo de fácil acesso ao ladrão.
- **Alçapão**: é uma brecha de segurança “intencional” que o projetista do sistema deixa no código fonte para ter fácil acesso aos dados e processos do sistema burlando os sistemas de segurança locais.
- **Bomba Lógica**: é um pedaço de código embutido no programa que mesmo submetido a uma análise, em primeiro momento não faz nada, mas ao encontrar uma série de parâmetros pode iniciar uma brecha de segurança a partir de dentro do programa
- **Estouro de Pilha e Buffer**: é uma brecha de segurança onde o intruso envia a vários processos do sistema grandes volumes de dados sob uma grande quantidade de parâmetros (muitos mais do que o programa esperava) e assim quebra a pilha de processamento, levando ao erro de sistema e brecha de segurança.
- **Vírus**: são pedaços de código que podem ser facilmente enviados à terceiros a fim de “infectar” o sistema, vírus são autorreplicaveis e tem o principal objetivo de se espalhar pelo sistema destruindo, alterando e roubando dados em grandes quantidades, atualmente o termo “vírus” é o termo popular servindo de sinônimo de programas que causam brechas de segurança.

INSTITUTO FEDERAL
Santa Catarina

Ameaças de Sistema e Redes

São caracterizadas ameaças de sistema e redes aquelas que utilizam e abusam dos recursos das redes em que sistemas estão inseridos, podem ser consideradas de maior gravidade devido ao fato que em uma rede sempre existem várias máquinas em funcionamento com um tráfego de dados constante.

Exemplos comuns dessas ameaças são:

- **Vermes**: um verme é um processo que tem um mecanismo para se replicar e assim inunda a rede e os sistemas que fazem parte dela, podendo até mesmo interromper o tráfego de dados e trancando outros processos.
- **Varredura de Portas**: a varredura de portas em si não é maléfica para a rede e seus sistemas integrantes, mas sim uma ferramenta que um hacker ou cracker podem tentar fazer uma conexão TCP/IP e encontrar bugs e falhas nas portas em que a conexão é feita.
- **Recusa de Serviço**: a recusa de serviço em si não tem a intenção de acessar o sistema ou roubar dados, mas sim interromper o uso legítimo do sistema. Ataques de DDOS (distributed denial of service) acontecem quando um grande número de acessos é realizado de forma mal intencionada a fim de bloquear acessos legítimos em um sistema devido a “falta de espaço” para novos acessos, sobrecarregando a rede e os sistemas afetados.

INSTITUTO FEDERAL
Santa Catarina

Criptografia e a Segurança

Devido ao risco de brechas de segurança em redes e tráfego de dados internos, o jeito mais fácil de fazer esse transporte de dados de forma segura é não depender das medidas de segurança da rede e sim tornar a informação ilegível para aqueles sem as ferramentas necessárias para ler tal informação.

Um sistema criptográfico deve funcionar com base em:

- Um conjunto K de chaves.
- Um conjunto M de mensagens.
- Um conjunto C de textos cifrados.
- Uma função de criptografia E: K $\rightarrow$(M $\rightarrow$C). Isto é, para cada k $\in$ K, Ek é uma função de geração de textos cifrados a partir de mensagens. Tanto E quanto Ek para qualquer k devem ser funções eficientemente computáveis. Geralmente, Ek é um mapeamento randomizado de mensagens para textos cifrados.
- Uma função de descriptografia D: K $\rightarrow$ (C $\rightarrow$ M). Isto é, para cada k [K $\in$ Dk é uma função para a geração de mensagens a partir de textos cifrados. Tanto D quanto Dk, para qualquer k, devem ser funções eficientemente computáveis.

INSTITUTO FEDERAL
Santa Catarina

AUTENTICAÇÃO DE USUÁRIOS :

Portanto, um grande problema de segurança dos sistemas operacionais é a autenticação de usuários. O sistema de proteç depende da capacidade de identificação dos programas e processos em execução corrente que, por sua vez, depende da capacidade de identificação de cada usuário do sistema. Normalmente os usuários se identificam a si próprios. Como determinar se uma identidade de usuário é autêntica? Geralmente, a autenticação do usuário baseia-se em um ou mais do três aspectos a seguir: a posse de algo (uma chave ou cartão) por parte do usuário, o conhecimento de algo (um identifica e uma senha) pelo usuário, ou um atributo do usuário (impressão digital, padrão de retina ou assinatura).

SENHAS: A abordagem mais comum para a autenticação de uma identidade de usuário é o uso de senhas. Quando o usu se identifica pelo ID de usuário ou nome da conta, uma senha é solicitada. Se a senha fornecida pelo usuário coincidir com senha armazenada no sistema, este assumirá que a conta está sendo acessada pelo seu proprietário.

Na prática, a maioria dos sistemas exige apenas uma senha para que um usuário obtenha direitos totais. Embora, teoricamente, seja mais seguro o uso de mais senhas, tais sistemas tendem a não ser implementados em razão da clássic escolha entre segurança e conveniência. Se a segurança se torna algo inconveniente, então a segurança é frequentement ignorada ou então evitada.

INSTITUTO FEDERAL
Santa Catarina

VULNERABILIDADE DE SENHAS: Senhas são extremamente comuns porque são fáceis de entender e usar. Infelizmente, elas podem ser adivinhadas, acidentalmente expostas, rastreadas (lidas por um bisbilhoteiro) ou ilegalmente transferidas de um usuário autorizado para um usuário não autorizado, como mostramos a seguir.

Há duas maneiras comuns de adivinhar uma senha. Uma delas é o intruso (humano ou programa) conhecer o usuário ou ter informações sobre ele. Quase sempre, as pessoas usam informações óbvias (como os nomes de seus gatos ou cônjuges) c senhas. A outra maneira é o uso de força bruta, com tentativas de enumeração — ou uso de todas as combinações possívei caracteres de senha válidos (letras, números e pontuação em alguns sistemas) — até que a senha seja descoberta. Senhas curtas são particularmente vulneráveis a esse método. Por exemplo, uma senha de quatro caracteres fornece apenas 10.00 variações. Em média, 5.000 tentativas produziriam um acerto. Um programa que pudesse testar uma senha a cada milisseg levaria apenas cerca de 5 segundos para adivinhar uma senha de quatro caracteres. A enumeração é menos bem-sucedida os sistemas permitem senhas mais longas que incluam letras maiúsculas e minúsculas, junto a números e todos os caracter pontuação. Naturalmente, os usuários devem tirar partido do espaço de senha maior e não devem usar, por exemplo, apena letras minúsculas.

Além de adivinhadas, as senhas podem ser expostas como resultado de monitoramento visual ou eletrônico. Um intruso pod olhar por cima dos ombros de um usuário (surfista de ombros) quando este estiver fazendo login e descobrir facilmente a se observando o teclado. Alternativamente, qualquer pessoa com acesso à rede em que um computador resida pode adicionar, deixar vestígios, um monitor de rede que lhe permita rastrear, ou observar, todos os dados que estão sendo transferidos na r inclusive identificações e senhas de usuário. A criptografia do fluxo de dados que contém a senha resolve esse problema. No entanto, tal sistema ainda pode ter as senhas roubadas. Por exemplo, se é usado um arquivo para armazenar as senhas, ele poderia ser copiado para análise fora do sistema. Ou considere um programa cavalo de troia instalado no sistema que captu cada pressionamento de tecla antes de enviá-lo à aplicação.

A exposição é um problema particularmente grave se a senha é anotada onde possa ser lida ou perdida. Alguns sistemas for os usuários a selecionar senhas longas ou difíceis de lembrar, ou a alterar sua senha com frequência, o que pode fazer com o usuário anote a senha ou a reutilize. Como resultado, tais sistemas fornecem muito menos segurança do que sistemas que permitam aos usuários a seleção de senhas fáceis!

INSTITUTO FEDERAL
Santa Catarina

SENHAS DESCARTÁVEIS: Senha descartável ou senha de uso único (em inglês: *One-time password* - OTP) é uma senh
válida somente para uma sessão de login ou transação, em um sistema de computadores ou outros dispositivos digitais.[1] OTPs evita
série de deficiências que estão associadas às autenticações tradicionais (estáticas), baseada em uma senha; uma séries de impleme
também incorporam autenticação de dois fatores, garantindo que a senha de uso requer acesso a algo que uma pessoa tem (como u
pequeno chaveiro OTP ou um celular específico), bem como algo que a pessoa sabe (como um PIN).

Se porventura uma senha de acesso for capturada, ela não terá nenhum valor, já que para um novo acesso, uma nova senha d
ser informada, claro que diferente da atual. Isso acontece porque no momento que a conexão é aceita, automaticamente a senh
foi usada para autenticação é descartada, fazendo com que a próxima conexão seja informada uma senha diferente.

Existem varias formas de gerar senhas, sendo com o uso de calculadoras de senhas ou essas mesmas calculadoras implemen
em sistemas operacionais, PDA's, celulares ou até mesmo soluções multiplataformas, como Java, que permite o funcionamento
de navegadores convencionais. O uso desta calculadora melhora bastante a segurança, em geral causa pouco incomodo visto
podem estar disponíveis em um dispositivo que o usuário carrega consigo

BIOMETRIA: Os leitores de impressões digitais tornaram-se precisos e baratos e devem ser mais comuns no futuro. Esses disp
leem padrões de sulcos dos dedos e os convertem em uma sequência de números. Com o tempo, eles podem armazenar um c
de sequências de acordo com a localização do dedo no equipamento de leitura e outros fatores. O software poderá então exam
dedo no equipamento e comparar suas características com as sequências armazenadas para determinar se elas coincidem.
Naturalmente, múltiplos usuários podem ter perfis armazenados, mas a varredura consegue diferenciá-los. Um esquema de
autenticação com dois fatores muito preciso pode resultar da solicitação de uma senha, assim como de um nome de usuário e
varredura da impressão digital. Se essas informações forem criptografadas em trânsito, o sistema poderá ser muito resistente à
falsificação ou ao ataque de reexecução. A **autenticação com múltiplos fatores** é ainda melhor. Considere o nível de confiabil
autenticação com um dispositivo USB que precise ser conectado ao sistema, além de um PIN e uma varredura de impressão di
Exceto pelo fato de ser preciso inserir o dedo em um suporte e conectar o USB ao sistema, esse método de autenticação não é
conveniente do que o uso de senhas normais. Porém, lembre-se de que esse alto nível de confiança da autenticação por si só n
suficiente para garantir a identificação do usuário. Uma sessão autenticada ainda pode ser sequestrada se não for criptografada

INSTITUTO FEDERAL
Santa Catarina

Implementando Defesas de Segurança:

Assim como existem inúmeras ameaças à segurança de sistemas e redes, há muitas soluções de segurança. As soluç
vão da melhoria da educação do usuário ao uso de tecnologias e à criação de softwares sem bugs. A maioria dos
profissionais de segurança é adepta da teoria da defesa em profundidade, que declara que mais camadas de defesa s
melhores do que menos camadas. Naturalmente, essa teoria se aplica a qualquer tipo de segurança. Considere a segu
de uma casa sem uma fechadura, com uma fechadura e com uma tranca e um alarme. Nesta seção, examinamos os
principais métodos, ferramentas e técnicas que podem ser usados para melhorar a resistência a ameaças. (exemplo:
https://www.tecmundo.com.br/amp/backup/2556-como-proteger-arquivos-com-senha-no-linux-.htm)

Política de Segurança:

O primeiro passo em direção à melhoria da segurança de qualquer aspecto da computação é a existência de uma política de
segurança. As políticas variam muito, mas geralmente incluem uma definição do que está sendo protegido. Por exemplo, uma p
pode definir que todas as aplicações acessíveis no ambiente externo devem ter uma revisão do código antes de serem implant
que os usuários não devem compartilhar suas senhas ou que todos os pontos de conexão entre uma empresa e o ambiente ex
devem ter varreduras de portas executadas a cada seis meses. Sem uma política definida, é impossível que usuários e
administradores saibam o que é aceitável, o que é requerido e o que não é permitido. A política é um roteiro para a segurança;
sítio está tentando deixar de ser menos seguro para ser mais seguro, ele precisa de um roteiro para saber como chegar lá.

Uma vez que a política de segurança esteja definida, as pessoas que ela afeta devem conhecê-la bem. Ela deve ser seu guia.
política também deve ser um documento vivo, revisado e atualizado periodicamente, para assegurar que continue sendo pertin
seguido.

Avaliação de Vulnerabilidades: A avaliação de riscos, por exemplo, tenta estimar os bens da entidade em questão (
programa, uma equipe de gerenciamento, um sistema ou uma instalação) e determinar as chances de um incidente de segurar
afetar a entidade e diminuir seu valor. Quando as chances de ocorrer uma perda e o montante da perda potencial são conheci
pode ser investido um valor na tentativa de segurar a entidade. A atividade fundamental da maioria das avaliações de
vulnerabilidades é um teste de penetração, em que a entidade é vasculhada em busca de vulnerabilidades conhecidas. Já que
livro refere-se aos sistemas operacionais e aos softwares que são executados sobre eles, concentramo-nos nesses aspectos d
avaliação de vulnerabilidades.
Varreduras de vulnerabilidades são feitas em momentos em que o uso do computador é relativamente baixo, para minimizar se
impacto. Quando apropriado, elas são feitas em sistemas de teste, em vez de em sistemas de produção, porque podem provoc
um comportamento indesejado nos sistemas-alvo ou dispositivos de rede.
Uma varredura dentro de um sistema individual pode verificar uma variedade de aspectos do sistema:

•Senhas curtas ou fáceis de adivinhar

•Programas privilegiados não autorizados, como os programas setuid

•Programas não autorizados em diretórios do sistema

•Processos de execução inesperadamente longa

•Proteções de diretório inapropriadas em diretórios do sistema e dos usuários

•Proteções inapropriadas em arquivos de dados do sistema, tais como o arquivo de senhas, drivers de dispositivos, ou o própri
kernel do sistema operacional

•Alterações em programas do sistema detectadas com valores de somas de verificação

INSTITUTO FEDERAL
Santa Catarina

Detecção de Invasões:

•O momento em que a detecção ocorre. A detecção pode ocorrer em tempo real (enquanto a invasão está ocorrendo) ou após o

•Os tipos de entradas examinadas para a detecção de atividade intrusiva. Eles podem incluir comandos de shell de usuário, cha
de sistema de processos e cabeçalhos ou conteúdos de pacotes de rede. Alguns tipos de invasão podem ser detectados somen
comparação de informações de várias dessas fontes.
•O conjunto de recursos de resposta. Tipos simples de resposta incluem alertar um administrador para a possível invasão ou int
de alguma forma a atividade potencialmente invasora — por exemplo, encerrando um processo empenhado nessa atividade. Em
sofisticado de resposta, um sistema pode desviar transparentemente a atividade de um intruso para um pote de mel — um recu
exposto ao invasor. O recurso parece real ao invasor e habilita o sistema a monitorar e obter informações sobre o ataque.

Esses graus de liberdade no espaço de projetos para detecção de invasões têm gerado uma extensa gama de soluções conhec
como sistemas de detecção de invasões (IDSs — intrusion-detection systems) e sistemas de prevenção de invasões (IDPs — in
prevention systems). Os sistemas IDS acionam um alarme quando uma invasão é detectada, enquanto os sistemas IDP atuam
roteadores, direcionando o tráfego, exceto quando uma invasão é detectada (momento em que esse tráfego é bloqueado).
Mas o que constitui exatamente uma invasão? Definir uma especificação adequada de invasão acaba sendo muito difícil, e port
IDSs e IDPs automáticos de hoje aceitam, tipicamente, uma entre duas abordagens menos ambiciosas. Na primeira, chamada d
baseada em assinatura, as entradas do sistema ou o tráfego de rede são examinados em busca de padrões de comportamento
específicos conhecidos (ou assinaturas) que indiquem ataques. Um exemplo simples de detecção baseada em assinatura é a v
de pacotes de rede em busca da string /etc/passwd/ destinada a um sistema UNIX. Outro exemplo é um software de detecção d
que promova varreduras em binários ou pacotes de rede em busca de vírus conhecidos.
A segunda abordagem, normalmente chamada detecção de anomalias, tenta detectar por meio de várias técnicas um comporta
anômalo dentro dos sistemas de computação. É claro que nem toda atividade anômala no sistema indica uma invasão, mas a p
é de que as invasões costumem provocar comportamento anômalo. Um exemplo de detecção de anomalias é o monitoramento
chamadas de sistema de um processo daemon para detectar se o comportamento da chamada de sistema desvia-se dos padrõ
normais, possivelmente indicando que um estouro de buffer foi explorado no daemon para corromper seu comportamento. Outr
exemplo é o monitoramento de comandos do shell para a detecção de comandos anômalos de determinado usuário, ou a detec
uma hora de login anômala de um usuário, os dois podendo indicar que um invasor foi bem-sucedido em obter acesso à conta d
usuário.

INSTITUTO FEDERAL
Santa Catarina

Proteção contra Vírus

Peraí, Linux precisa de antivírus?

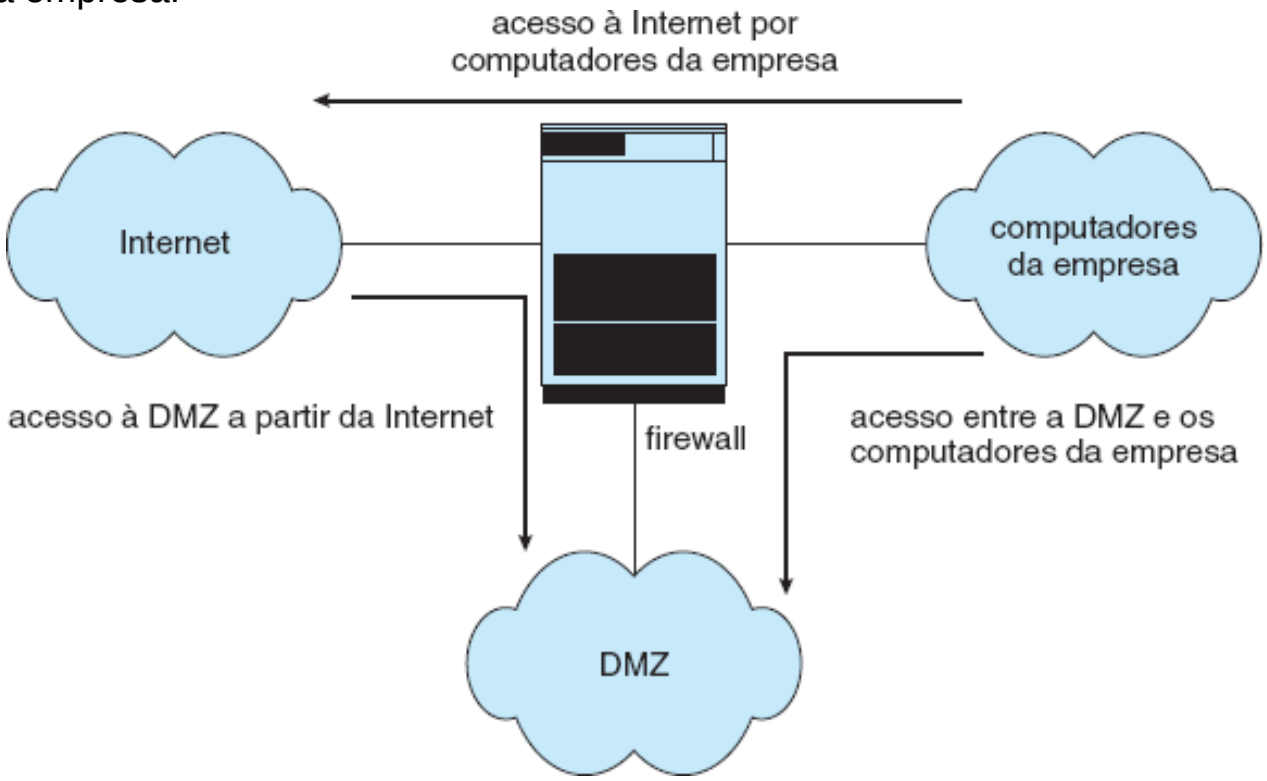
Por ter uma estrutura de segurança baseada em permissões, contar com uma arquitetura modular e ser permanentemente at
o Linux é bastante seguro. Por esse motivo, a maioria de seus usuários dispensa a instalação de antivírus no sistema operac
Mas nenhum sistema pode garantir 100% de segurança. É por isso que algumas pessoas e organizações recorrem a antivíru
Linux, não necessariamente como um cuidado obrigatório, mas como uma camada adicional de segurança.
É por isso que, a seguir, selecionamos cinco soluções de antivírus, além de um “bônus”. Note que há opções para uso domés
corporativo

ClamAV: Comecemos por uma opção clássica e gratuita. O ClamAV (Clam AntiVirus) é um antivírus lançado em 2007. M
pela Cisco, essa solução tem versões para Linux, sistemas BSD, Windows e macOS. Apesar disso, o antivírus é mais conhec
usuários de distribuições Linux. Há boas razões para isso. A primeira é que o ClamAV tem código-fonte aberto. A segunda: é
usá-lo tanto via interface gráfica (instalada à parte) quanto por linha de comando.
Terceira razão: o antivírus costuma ser bastante eficiente na detecção de malwares presentes em arquivos que acabaram de
baixados. Há até quem o use, no Linux, para analisar arquivos suspeitos direcionados ao Windows.
As orientações para instalação no Ubuntu, Debian e outras distribuições estão no site oficial do ClamAV.

Comodo Antivirus:

O Comodo Antivirus é outra opção gratuita para Linux, embora não tenha código-fonte aberto. A característica mais marcante
opção é a sua capacidade de fazer análise comportamental com base nas nuvens.
Em outras palavras, a ferramenta pode barrar arquivos potencialmente maliciosos ao identificar atividades suspeitas. Esse re
útil para isolar vírus e outros malwares novos, que ainda não aparecem no banco de dados do antivírus.
Há versões para Ubuntu, Debian, Mint e outras distribuições na página do Comodo Antivirus.

Usando um Firewall para Proteger Sistemas e Redes: Enfocamos, a seguir, a questão de como um comput
confiável pode ser conectado seguramente a uma rede não confiável. Uma solução é o uso de um firewall para separar sistem
confiáveis e não confiáveis.
Na verdade, um firewall de rede pode separar uma rede em múltiplos domínios. Uma implementação comum tem a Internet co
domínio não confiável; uma rede semiconfiável e semissegura, chamada zona desmilitarizada (DMZ — demilitarized zone), co
domínio; e os computadores de uma empresa como um terceiro domínio (Figura 15.10). Conexões são permitidas da Internet p
computadores da DMZ e dos computadores da empresa para a Internet, mas não são permitidas da Internet ou de computador
DMZ para os computadores da empresa. Opcionalmente, comunicações controladas podem ser permitidas entre a DMZ e um
computadores da empresa. Por exemplo, um servidor web na DMZ pode precisar consultar um servidor de banco de dados na
empresa. Com um firewall, no entanto, o acesso é contido, e qualquer sistema da DMZ que tenha sido invadido será incapaz d
acessar os computadores da empresa.



Windows 7

Windows 7 é uma versão do Microsoft Windows, uma série de sistemas operativos produzidos pela Microsoft para uso em computadores pessoais, incluindo computadores domésticos e empresariais, *laptops*, *tablets* e PCs de centros de mídia, ent outros, A Microsoft diz que o Windows 7 é o sistema operacional da plataforma Windows mais seguro já criado até hoje.

RECURSOS DE SEGURANÇA:

- **Proteção do core:**
  O kernel é o coração de um sistema operacional e, por isso mesmo, principal alvo para todo tipo de praga e outros tipo ataques. Basicamente, caso um cracker possa acessar ou manipular o kernel do sistema operacional, ele será capaz d executar códigos maliciosos em um nível que não é detectável por outras aplicações ou mesmo pelo sistema operacion propriamente dito. A Microsoft desenvolveu um modo de proteção do kernel para evitar que processos não autorizados tenham acesso ao núcleo do Windows 7.

- **Navegação segura:**

A primeira delas é o modo de navegação privativa ou anônima (InPrivate Browsing) proporciona a opção de surfar na web se deixar rastros. Quando a funcionalidade é ativada, o IE deixa de registrar qualquer informação relacionada com o que se faz web. Isso significa que nada do que é digitado é registrado no cache, nada de histórico dos sites visitados. A função é particularmente útil quando se compartilha um computador ou utiliza-se uma máquina em lugar público, como uma lan house biblioteca na escola.

Outra melhoria notável do IE8 é o Modo Protegido e que está relacionado a componentes de segurança do Windows 7 para impedir que códigos maliciosos ou não autorizados sejam executados dentro do navegador. Esta funcionalidade não permite exemplo, que a simples visita a um site contaminado possa baixar e instalar códigos maliciosos no computador.

INSTITUTO FEDERAL
Santa Catarina

- **Proteção que adoramos odiar:**

  O controle de contas de usuário (UAC pela sigla em inglês) é, provavelmente, a característica mais odiada e ao mesm tempo amada do Vista. No Windows 7, o UAC continua lá, mas a Microsoft adicionou um recurso que dá mais contro do nível de proteção ao usuário e, em decorrência, do número de pop-ups solicitando permissão para acesso ou execução de algum processo. Além disso, os pop-ups são apenas um aspecto do que o UAC proporciona. Muitos usuários simplesmente desabilitaram o UAC completamente no Vista. O problema é que ao fazer isso no Vista, eles também estavam desativando o modo de proteção do Internet Explorer além de outros recursos de proteção do siste operacional. O controle variável disponível no Windows 7 também faz o mesmo, mas o usuário tem melhor controle sobre o que desabilitar a partir de ajustes no Painel de Controle.

- **Ferramentas de segurança e aplicativos:**

Por conta do modo de proteção do kernel e das mudanças que a Microsoft fez para gerenciar, as aplicações são autorizad interagir com funcionalidades core do sistema operacional, antivírus e outros aplicativos de segurança mais antigos não sã compatíveis com o Windows 7.

TREND MICRO™

Symantec™ by Broadcom Software

McAfee™

- Tal fornecedores tem total compatibilidade com o windows, sendo assim fica a dica para quem quer deixar seu siste com segurança e proteção a mais.

CONCLUSÃO

Proteção é um problema interno. Segurança, por outro lado, deve considerar tanto o sistema de computação quanto o amb
— pessoas, prédios, empresas, objetos de valor e ameaças — dentro do qual o sistema é usado.

Os dados armazenados no sistema de computação devem ser protegidos contra acesso não autorizado, destruição ou alteração maliciosa e introdução acidental de inconsistências. É mais fácil se proteger contra a perda acidental da consistê dos dados do que se proteger contra o acesso malicioso aos dados. A proteção absoluta das informações armazenadas em sistema de computação contra abuso malicioso não é possível; mas o custo para o infrator pode ser suficientemente alto pa deter quase todas (quando não todas) as tentativas de acesso a essas informações sem autorização apropriada.

Vários tipos de ataques podem ser lançados contra programas e contra computadores individuais ou coletivos. Técnicas de estouro de pilha e de buffer permitem que invasores bem sucedidos alterem seu nível de acesso ao sistema. Vírus e verme são autoperpetuáveis e às vezes infectam milhares de computadores. Ataques de recusa de serviço impedem o uso legítim sistemas-alvo.

A criptografia limita o domínio de receptores de dados enquanto a autenticação limita o domínio de emissores. A criptografia usada para fornecer sigilo aos dados que estão sendo armazenados ou transferidos. A criptografia simétrica requer uma ch compartilhada, enquanto a criptografia assimétrica fornece uma chave pública e uma chave privada. A autenticação, quand combinada com o hashing, pode comprovar que os dados não foram alterados.

Os métodos de autenticação de usuários são usados para identificar os usuários legítimos de um sistema. Além da proteçã padrão com nome de usuário e senha, vários métodos de autenticação são usados. As senhas descartáveis, por exemplo, mudam de uma sessão para outra para evitar ataques de reexecução. A autenticação com dois fatores requer dois tipos de autenticação, tal como uma calculadora em hardware junto com um PIN de ativação. A autenticação com múltiplos fatores u três tipos ou mais. Esses métodos diminuem muito a chance de falsificação da autenticação.

Os métodos de prevenção ou detecção de incidentes de segurança incluem os sistemas de detecção de invasões, os softw antivírus, a auditoria e o registro em log de eventos do sistema, o monitoramento de alterações em softwares do sistema, o monitoramento de chamadas de sistema e firewalls.

INSTITUTO FEDERAL
Santa Catarina

QUESTIONÁRIO

1: O que é matriz de acesso?

2: De que recursos de hardware um sistema de computação precisa para a manipulação eficiente de competências? Esses recursos podem ser usados para proteção da memória?

3: Uma senha pode se tornar conhecida por outros usuários de várias maneiras, diga os métodos simples:

4: como proteger arquivos com senhas no linux?

1: A matriz de acesso é um modelo teórico usado para mapear os acessos dentro de uma organização. Foi criado em 2013 pelo profissional de TI Ticiano Benetti, com o objetivo de apresentar as questões de segurança da informação de forma mais segmentada para gerentes de uma empresa.

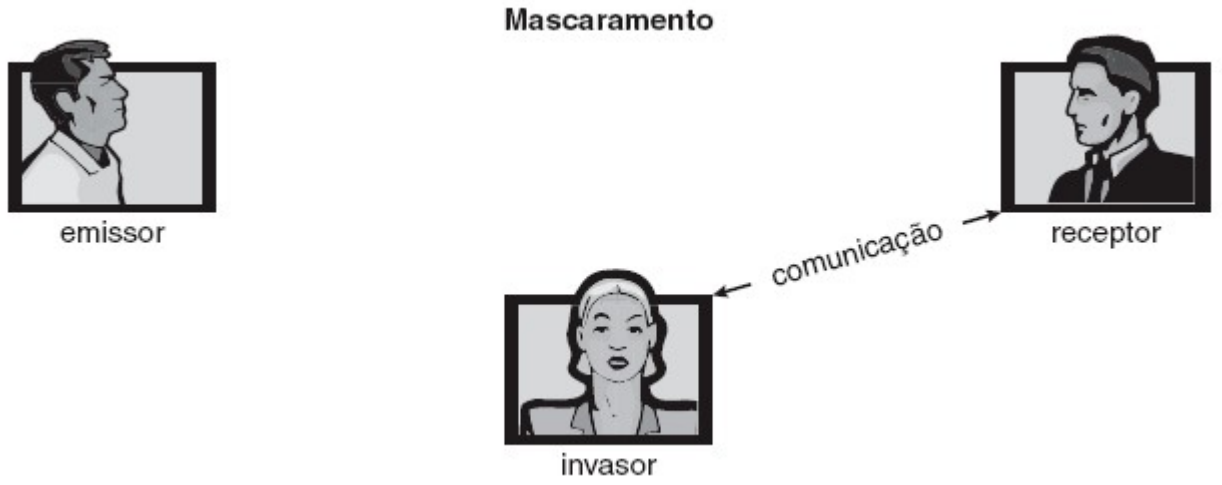
2:Um TPM (Trusted Platform Module) foi projetado para fornecer funções relacionadas à segurança baseadas em hardware e ajudar a evitar adulterações indesejadas. Os TPMs fornecem benefícios de segurança e privacidade para hardware do sistema, proprietários de plataforma e usuários. Um chip TPM é um processador de criptografia seguro que ajuda com ações como gerar, armazenar e limitar o uso de chaves criptográficas. Muitos TPMs incluem vários mecanismos de segurança física para torná-lo resistente a adulterações e impedir que o software mal-intencionado altere as funções de segurança do TPM.

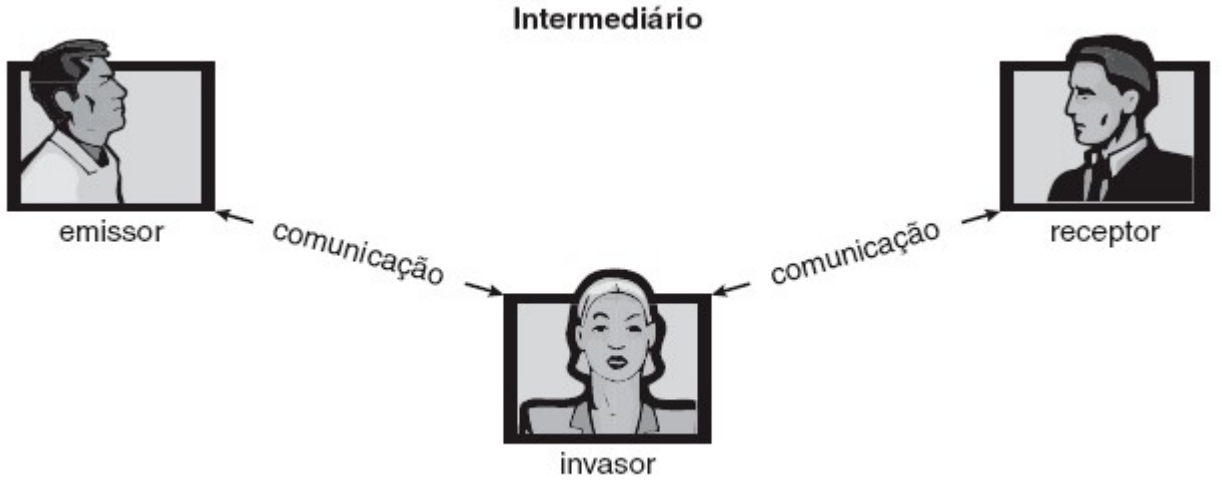
3: Há duas maneiras comuns de adivinhar uma senha. Uma delas é o intruso (humano ou programa). uma senha de quatro caracteres fornece apenas 10.000 variações. Em média, 5.000 tentativas produziriam um acerto. Um programa que pudesse testar uma senha a cada milissegundo levaria apenas cerca de 5 segundos para adivinhar uma senha de quatro caracteres. tipo de comprometimento da senha, a transferência ilegal, é resultado da natureza humana.

4: prático (link no slide **Implementando Defesas de Segurança**)

Outras formas de violação de segurança normais são:

- **Mascaramento**: o mascaramento acontece quando uma pessoa mal intencionada se passa por algum integrante válido do sistema e assim, tem acesso não autorizado a recursos e dados do sistema.
- **Intermediário**: o ataque do intermediário acontece quando um usuário não autorizado se instala no meio de um fluxo de dados(sequestro de sessão), agindo como intermediário desse fluxo e tendo acesso às informações que passam pelo mesmo





INSTITUTO FEDERAL
Santa Catarina

Fatores a serem considerados

É lógico considerar que mesmo tomando cuidado, é impossível ter uma segurança perfeita, são quase infinitos os casos que podem levar a uma brecha de segurança, sendo assim, para minimizar as chances do pior dos casos, são considerados 4 níveis de segurança:

- **Físico**: o lugar em que a base de dados (servidor) está instalada, levando em conta as condições do local, manutenção, acesso aos terminais, etc…
- **Humano**: é crucial para a segurança que apenas pessoal autorizado tenha acesso ao sistema, porém existe a possibilidade que esse pessoal seja influenciado por terceiros a permitir o acesso, o usuário pode ser enganado por sites e programas mal intencionados a dar suas credenciais ou ainda uma técnica usada chamada **dumpster diving** que consistem em coletar todos os “lixos” de informações do usuário na chance de encontrar alguma credencial ou dado importante em lugares como lixeiras, agendas, anotações, etc…
- **Sistema Operacional**: o sistema em si deve ter medidas de segurança a fim de prever, evitar e reparar brechas de segurança de origem interna, como erros de memória, estouros de pilha de processamento, integridade de credenciais, etc…
- **Rede**: um grande volume de dados percorre a rede tanto externa quanto interna, uma brecha de dados que se instale entre 2 ou mais pontos dessa rede deve ser considerada e evitada.

INSTITUTO FEDERAL
Santa Catarina

Ameaças de Programas

Um objetivo comum dos hackers e crackers é o acesso a dados do usuário através de programas e linhas de código mal intencionadas, levando em consideração que um programa que crie um processo que rode junto ao kernel com capacidade de criar uma brecha de segurança seria capaz de derrubar o sistema por inteiro, roubar grandes volumes de informações ou ambos.

As ameaças por programas mais comuns são:

- **Cavalo de Tróia**: fazendo alusão ao mito grego, esse são programas que podem parecer legítimos e instalados pelo usuário porém em seu código fonte possui processos que copiam dados (podendo ser através de sistemas de login falsos, sistemas de busca, processos ocultos, etc…) e os mandam para uma base de dados separada, sendo de fácil acesso ao ladrão.
- **Alçapão**: é uma brecha de segurança “intencional” que o projetista do sistema deixa no código fonte para ter fácil acesso aos dados e processos do sistema burlando os sistemas de segurança locais.
- **Bomba Lógica**: é um pedaço de código embutido no programa que mesmo submetido a uma análise, em primeiro momento não faz nada, mas ao encontrar uma série de parâmetros pode iniciar uma brecha de segurança a partir de dentro do programa
- **Estouro de Pilha e Buffer**: é uma brecha de segurança onde o intruso envia a vários processos do sistema grandes volumes de dados sob uma grande quantidade de parâmetros (muitos mais do que o programa esperava) e assim quebra a pilha de processamento, levando ao erro de sistema e brecha de segurança.
- **Vírus**: são pedaços de código que podem ser facilmente enviados à terceiros a fim de “infectar” o sistema, vírus são autorreplicaveis e tem o principal objetivo de se espalhar pelo sistema destruindo, alterando e roubando dados em grandes quantidades, atualmente o termo “vírus” é o termo popular servindo de sinônimo de programas que causam brechas de segurança.

INSTITUTO FEDERAL
Santa Catarina

Ameaças de Sistema e Redes

São caracterizadas ameaças de sistema e redes aquelas que utilizam e abusam dos recursos das redes em que sistemas estão inseridos, podem ser consideradas de maior gravidade devido ao fato que em uma rede sempre existem várias máquinas em funcionamento com um tráfego de dados constante.

Exemplos comuns dessas ameaças são:

- **Vermes**: um verme é um processo que tem um mecanismo para se replicar e assim inunda a rede e os sistemas que fazem parte dela, podendo até mesmo interromper o tráfego de dados e trancando outros processos.
- **Varredura de Portas**: a varredura de portas em si não é maléfica para a rede e seus sistemas integrantes, mas sim uma ferramenta que um hacker ou cracker podem tentar fazer uma conexão TCP/IP e encontrar bugs e falhas nas portas em que a conexão é feita.
- **Recusa de Serviço**: a recusa de serviço em si não tem a intenção de acessar o sistema ou roubar dados, mas sim interromper o uso legítimo do sistema. Ataques de DDOS (distributed denial of service) acontecem quando um grande número de acessos é realizado de forma mal intencionada a fim de bloquear acessos legítimos em um sistema devido a “falta de espaço” para novos acessos, sobrecarregando a rede e os sistemas afetados.

INSTITUTO FEDERAL
Santa Catarina

Criptografia e a Segurança

Devido ao risco de brechas de segurança em redes e tráfego de dados internos, o jeito mais fácil de fazer esse transporte de dados de forma segura é não depender das medidas de segurança da rede e sim tornar a informação ilegível para aqueles sem as ferramentas necessárias para ler tal informação.

Um sistema criptográfico deve funcionar com base em:

- Um conjunto K de chaves.
- Um conjunto M de mensagens.
- Um conjunto C de textos cifrados.
- Uma função de criptografia E: K $\rightarrow$(M $\rightarrow$C). Isto é, para cada k $\in$ K, Ek é uma função de geração de textos cifrados a partir de mensagens. Tanto E quanto Ek para qualquer k devem ser funções eficientemente computáveis. Geralmente, Ek é um mapeamento randomizado de mensagens para textos cifrados.
- Uma função de descriptografia D: K $\rightarrow$ (C $\rightarrow$ M). Isto é, para cada k [K $\in$ Dk é uma função para a geração de mensagens a partir de textos cifrados. Tanto D quanto Dk, para qualquer k, devem ser funções eficientemente computáveis.

INSTITUTO FEDERAL
Santa Catarina

AUTENTICAÇÃO DE USUÁRIOS :

Portanto, um grande problema de segurança dos sistemas operacionais é a autenticação de usuários. O sistema de proteç depende da capacidade de identificação dos programas e processos em execução corrente que, por sua vez, depende da capacidade de identificação de cada usuário do sistema. Normalmente os usuários se identificam a si próprios. Como determinar se uma identidade de usuário é autêntica? Geralmente, a autenticação do usuário baseia-se em um ou mais do três aspectos a seguir: a posse de algo (uma chave ou cartão) por parte do usuário, o conhecimento de algo (um identifica e uma senha) pelo usuário, ou um atributo do usuário (impressão digital, padrão de retina ou assinatura).

SENHAS: A abordagem mais comum para a autenticação de uma identidade de usuário é o uso de senhas. Quando o usu se identifica pelo ID de usuário ou nome da conta, uma senha é solicitada. Se a senha fornecida pelo usuário coincidir com senha armazenada no sistema, este assumirá que a conta está sendo acessada pelo seu proprietário.

Na prática, a maioria dos sistemas exige apenas uma senha para que um usuário obtenha direitos totais. Embora, teoricamente, seja mais seguro o uso de mais senhas, tais sistemas tendem a não ser implementados em razão da clássic escolha entre segurança e conveniência. Se a segurança se torna algo inconveniente, então a segurança é frequentement ignorada ou então evitada.

INSTITUTO FEDERAL
Santa Catarina

VULNERABILIDADE DE SENHAS: Senhas são extremamente comuns porque são fáceis de entender e usar. Infelizmente, elas podem ser adivinhadas, acidentalmente expostas, rastreadas (lidas por um bisbilhoteiro) ou ilegalmente transferidas de um usuário autorizado para um usuário não autorizado, como mostramos a seguir.

Há duas maneiras comuns de adivinhar uma senha. Uma delas é o intruso (humano ou programa) conhecer o usuário ou ter informações sobre ele. Quase sempre, as pessoas usam informações óbvias (como os nomes de seus gatos ou cônjuges) c senhas. A outra maneira é o uso de força bruta, com tentativas de enumeração — ou uso de todas as combinações possívei caracteres de senha válidos (letras, números e pontuação em alguns sistemas) — até que a senha seja descoberta. Senhas curtas são particularmente vulneráveis a esse método. Por exemplo, uma senha de quatro caracteres fornece apenas 10.00 variações. Em média, 5.000 tentativas produziriam um acerto. Um programa que pudesse testar uma senha a cada milisseg levaria apenas cerca de 5 segundos para adivinhar uma senha de quatro caracteres. A enumeração é menos bem-sucedida os sistemas permitem senhas mais longas que incluam letras maiúsculas e minúsculas, junto a números e todos os caracter pontuação. Naturalmente, os usuários devem tirar partido do espaço de senha maior e não devem usar, por exemplo, apena letras minúsculas.

Além de adivinhadas, as senhas podem ser expostas como resultado de monitoramento visual ou eletrônico. Um intruso pod olhar por cima dos ombros de um usuário (surfista de ombros) quando este estiver fazendo login e descobrir facilmente a se observando o teclado. Alternativamente, qualquer pessoa com acesso à rede em que um computador resida pode adicionar, deixar vestígios, um monitor de rede que lhe permita rastrear, ou observar, todos os dados que estão sendo transferidos na r inclusive identificações e senhas de usuário. A criptografia do fluxo de dados que contém a senha resolve esse problema. No entanto, tal sistema ainda pode ter as senhas roubadas. Por exemplo, se é usado um arquivo para armazenar as senhas, ele poderia ser copiado para análise fora do sistema. Ou considere um programa cavalo de troia instalado no sistema que captu cada pressionamento de tecla antes de enviá-lo à aplicação.

A exposição é um problema particularmente grave se a senha é anotada onde possa ser lida ou perdida. Alguns sistemas for os usuários a selecionar senhas longas ou difíceis de lembrar, ou a alterar sua senha com frequência, o que pode fazer com o usuário anote a senha ou a reutilize. Como resultado, tais sistemas fornecem muito menos segurança do que sistemas que permitam aos usuários a seleção de senhas fáceis!

INSTITUTO FEDERAL
Santa Catarina

SENHAS DESCARTÁVEIS: Senha descartável ou senha de uso único (em inglês: *One-time password* - OTP) é uma senh
válida somente para uma sessão de login ou transação, em um sistema de computadores ou outros dispositivos digitais.[1] OTPs evita
série de deficiências que estão associadas às autenticações tradicionais (estáticas), baseada em uma senha; uma séries de impleme
também incorporam autenticação de dois fatores, garantindo que a senha de uso requer acesso a algo que uma pessoa tem (como u
pequeno chaveiro OTP ou um celular específico), bem como algo que a pessoa sabe (como um PIN).

Se porventura uma senha de acesso for capturada, ela não terá nenhum valor, já que para um novo acesso, uma nova senha d
ser informada, claro que diferente da atual. Isso acontece porque no momento que a conexão é aceita, automaticamente a senh
foi usada para autenticação é descartada, fazendo com que a próxima conexão seja informada uma senha diferente.

Existem varias formas de gerar senhas, sendo com o uso de calculadoras de senhas ou essas mesmas calculadoras implemen
em sistemas operacionais, PDA's, celulares ou até mesmo soluções multiplataformas, como Java, que permite o funcionamento
de navegadores convencionais. O uso desta calculadora melhora bastante a segurança, em geral causa pouco incomodo visto
podem estar disponíveis em um dispositivo que o usuário carrega consigo

BIOMETRIA: Os leitores de impressões digitais tornaram-se precisos e baratos e devem ser mais comuns no futuro. Esses disp
leem padrões de sulcos dos dedos e os convertem em uma sequência de números. Com o tempo, eles podem armazenar um c
de sequências de acordo com a localização do dedo no equipamento de leitura e outros fatores. O software poderá então exam
dedo no equipamento e comparar suas características com as sequências armazenadas para determinar se elas coincidem.
Naturalmente, múltiplos usuários podem ter perfis armazenados, mas a varredura consegue diferenciá-los. Um esquema de
autenticação com dois fatores muito preciso pode resultar da solicitação de uma senha, assim como de um nome de usuário e
varredura da impressão digital. Se essas informações forem criptografadas em trânsito, o sistema poderá ser muito resistente à
falsificação ou ao ataque de reexecução. A **autenticação com múltiplos fatores** é ainda melhor. Considere o nível de confiabil
autenticação com um dispositivo USB que precise ser conectado ao sistema, além de um PIN e uma varredura de impressão di
Exceto pelo fato de ser preciso inserir o dedo em um suporte e conectar o USB ao sistema, esse método de autenticação não é
conveniente do que o uso de senhas normais. Porém, lembre-se de que esse alto nível de confiança da autenticação por si só n
suficiente para garantir a identificação do usuário. Uma sessão autenticada ainda pode ser sequestrada se não for criptografada

INSTITUTO FEDERAL
Santa Catarina

Implementando Defesas de Segurança:

Assim como existem inúmeras ameaças à segurança de sistemas e redes, há muitas soluções de segurança. As soluç
vão da melhoria da educação do usuário ao uso de tecnologias e à criação de softwares sem bugs. A maioria dos
profissionais de segurança é adepta da teoria da defesa em profundidade, que declara que mais camadas de defesa s
melhores do que menos camadas. Naturalmente, essa teoria se aplica a qualquer tipo de segurança. Considere a segu
de uma casa sem uma fechadura, com uma fechadura e com uma tranca e um alarme. Nesta seção, examinamos os
principais métodos, ferramentas e técnicas que podem ser usados para melhorar a resistência a ameaças. (exemplo:
https://www.tecmundo.com.br/amp/backup/2556-como-proteger-arquivos-com-senha-no-linux-.htm)

Política de Segurança:

O primeiro passo em direção à melhoria da segurança de qualquer aspecto da computação é a existência de uma política de
segurança. As políticas variam muito, mas geralmente incluem uma definição do que está sendo protegido. Por exemplo, uma p
pode definir que todas as aplicações acessíveis no ambiente externo devem ter uma revisão do código antes de serem implant
que os usuários não devem compartilhar suas senhas ou que todos os pontos de conexão entre uma empresa e o ambiente ex
devem ter varreduras de portas executadas a cada seis meses. Sem uma política definida, é impossível que usuários e
administradores saibam o que é aceitável, o que é requerido e o que não é permitido. A política é um roteiro para a segurança;
sítio está tentando deixar de ser menos seguro para ser mais seguro, ele precisa de um roteiro para saber como chegar lá.

Uma vez que a política de segurança esteja definida, as pessoas que ela afeta devem conhecê-la bem. Ela deve ser seu guia.
política também deve ser um documento vivo, revisado e atualizado periodicamente, para assegurar que continue sendo pertin
seguido.

Avaliação de Vulnerabilidades: A avaliação de riscos, por exemplo, tenta estimar os bens da entidade em questão (
programa, uma equipe de gerenciamento, um sistema ou uma instalação) e determinar as chances de um incidente de segurar
afetar a entidade e diminuir seu valor. Quando as chances de ocorrer uma perda e o montante da perda potencial são conheci
pode ser investido um valor na tentativa de segurar a entidade. A atividade fundamental da maioria das avaliações de
vulnerabilidades é um teste de penetração, em que a entidade é vasculhada em busca de vulnerabilidades conhecidas. Já que
livro refere-se aos sistemas operacionais e aos softwares que são executados sobre eles, concentramo-nos nesses aspectos d
avaliação de vulnerabilidades.
Varreduras de vulnerabilidades são feitas em momentos em que o uso do computador é relativamente baixo, para minimizar se
impacto. Quando apropriado, elas são feitas em sistemas de teste, em vez de em sistemas de produção, porque podem provoc
um comportamento indesejado nos sistemas-alvo ou dispositivos de rede.
Uma varredura dentro de um sistema individual pode verificar uma variedade de aspectos do sistema:

•Senhas curtas ou fáceis de adivinhar

•Programas privilegiados não autorizados, como os programas setuid

•Programas não autorizados em diretórios do sistema

•Processos de execução inesperadamente longa

•Proteções de diretório inapropriadas em diretórios do sistema e dos usuários

•Proteções inapropriadas em arquivos de dados do sistema, tais como o arquivo de senhas, drivers de dispositivos, ou o própri
kernel do sistema operacional

•Alterações em programas do sistema detectadas com valores de somas de verificação

INSTITUTO FEDERAL
Santa Catarina

Detecção de Invasões:

•O momento em que a detecção ocorre. A detecção pode ocorrer em tempo real (enquanto a invasão está ocorrendo) ou após o

•Os tipos de entradas examinadas para a detecção de atividade intrusiva. Eles podem incluir comandos de shell de usuário, cha
de sistema de processos e cabeçalhos ou conteúdos de pacotes de rede. Alguns tipos de invasão podem ser detectados somen
comparação de informações de várias dessas fontes.
•O conjunto de recursos de resposta. Tipos simples de resposta incluem alertar um administrador para a possível invasão ou int
de alguma forma a atividade potencialmente invasora — por exemplo, encerrando um processo empenhado nessa atividade. Em
sofisticado de resposta, um sistema pode desviar transparentemente a atividade de um intruso para um pote de mel — um recu
exposto ao invasor. O recurso parece real ao invasor e habilita o sistema a monitorar e obter informações sobre o ataque.

Esses graus de liberdade no espaço de projetos para detecção de invasões têm gerado uma extensa gama de soluções conhec
como sistemas de detecção de invasões (IDSs — intrusion-detection systems) e sistemas de prevenção de invasões (IDPs — in
prevention systems). Os sistemas IDS acionam um alarme quando uma invasão é detectada, enquanto os sistemas IDP atuam
roteadores, direcionando o tráfego, exceto quando uma invasão é detectada (momento em que esse tráfego é bloqueado).
Mas o que constitui exatamente uma invasão? Definir uma especificação adequada de invasão acaba sendo muito difícil, e port
IDSs e IDPs automáticos de hoje aceitam, tipicamente, uma entre duas abordagens menos ambiciosas. Na primeira, chamada d
baseada em assinatura, as entradas do sistema ou o tráfego de rede são examinados em busca de padrões de comportamento
específicos conhecidos (ou assinaturas) que indiquem ataques. Um exemplo simples de detecção baseada em assinatura é a v
de pacotes de rede em busca da string /etc/passwd/ destinada a um sistema UNIX. Outro exemplo é um software de detecção d
que promova varreduras em binários ou pacotes de rede em busca de vírus conhecidos.
A segunda abordagem, normalmente chamada detecção de anomalias, tenta detectar por meio de várias técnicas um comporta
anômalo dentro dos sistemas de computação. É claro que nem toda atividade anômala no sistema indica uma invasão, mas a p
é de que as invasões costumem provocar comportamento anômalo. Um exemplo de detecção de anomalias é o monitoramento
chamadas de sistema de um processo daemon para detectar se o comportamento da chamada de sistema desvia-se dos padrõ
normais, possivelmente indicando que um estouro de buffer foi explorado no daemon para corromper seu comportamento. Outr
exemplo é o monitoramento de comandos do shell para a detecção de comandos anômalos de determinado usuário, ou a detec
uma hora de login anômala de um usuário, os dois podendo indicar que um invasor foi bem-sucedido em obter acesso à conta d
usuário.

INSTITUTO FEDERAL
Santa Catarina

Proteção contra Vírus

Peraí, Linux precisa de antivírus?

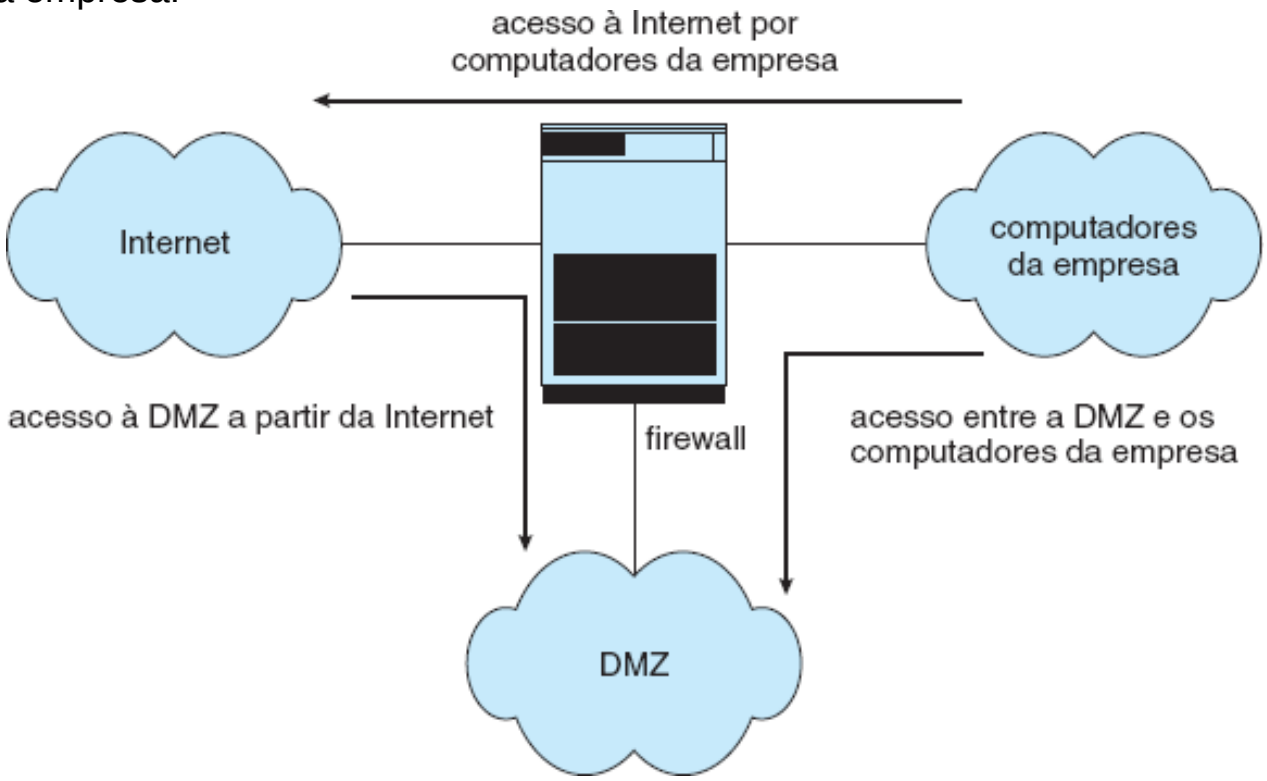
Por ter uma estrutura de segurança baseada em permissões, contar com uma arquitetura modular e ser permanentemente at
o Linux é bastante seguro. Por esse motivo, a maioria de seus usuários dispensa a instalação de antivírus no sistema operac
Mas nenhum sistema pode garantir 100% de segurança. É por isso que algumas pessoas e organizações recorrem a antivíru
Linux, não necessariamente como um cuidado obrigatório, mas como uma camada adicional de segurança.
É por isso que, a seguir, selecionamos cinco soluções de antivírus, além de um “bônus”. Note que há opções para uso domés
corporativo

ClamAV: Comecemos por uma opção clássica e gratuita. O ClamAV (Clam AntiVirus) é um antivírus lançado em 2007. M
pela Cisco, essa solução tem versões para Linux, sistemas BSD, Windows e macOS. Apesar disso, o antivírus é mais conhec
usuários de distribuições Linux. Há boas razões para isso. A primeira é que o ClamAV tem código-fonte aberto. A segunda: é
usá-lo tanto via interface gráfica (instalada à parte) quanto por linha de comando.
Terceira razão: o antivírus costuma ser bastante eficiente na detecção de malwares presentes em arquivos que acabaram de
baixados. Há até quem o use, no Linux, para analisar arquivos suspeitos direcionados ao Windows.
As orientações para instalação no Ubuntu, Debian e outras distribuições estão no site oficial do ClamAV.

Comodo Antivirus:

O Comodo Antivirus é outra opção gratuita para Linux, embora não tenha código-fonte aberto. A característica mais marcante
opção é a sua capacidade de fazer análise comportamental com base nas nuvens.
Em outras palavras, a ferramenta pode barrar arquivos potencialmente maliciosos ao identificar atividades suspeitas. Esse re
útil para isolar vírus e outros malwares novos, que ainda não aparecem no banco de dados do antivírus.
Há versões para Ubuntu, Debian, Mint e outras distribuições na página do Comodo Antivirus.

Usando um Firewall para Proteger Sistemas e Redes: Enfocamos, a seguir, a questão de como um comput
confiável pode ser conectado seguramente a uma rede não confiável. Uma solução é o uso de um firewall para separar sistem
confiáveis e não confiáveis.
Na verdade, um firewall de rede pode separar uma rede em múltiplos domínios. Uma implementação comum tem a Internet co
domínio não confiável; uma rede semiconfiável e semissegura, chamada zona desmilitarizada (DMZ — demilitarized zone), co
domínio; e os computadores de uma empresa como um terceiro domínio (Figura 15.10). Conexões são permitidas da Internet p
computadores da DMZ e dos computadores da empresa para a Internet, mas não são permitidas da Internet ou de computador
DMZ para os computadores da empresa. Opcionalmente, comunicações controladas podem ser permitidas entre a DMZ e um
computadores da empresa. Por exemplo, um servidor web na DMZ pode precisar consultar um servidor de banco de dados na
empresa. Com um firewall, no entanto, o acesso é contido, e qualquer sistema da DMZ que tenha sido invadido será incapaz d
acessar os computadores da empresa.



Windows 7

Windows 7 é uma versão do Microsoft Windows, uma série de sistemas operativos produzidos pela Microsoft para uso em computadores pessoais, incluindo computadores domésticos e empresariais, *laptops*, *tablets* e PCs de centros de mídia, ent outros, A Microsoft diz que o Windows 7 é o sistema operacional da plataforma Windows mais seguro já criado até hoje.

RECURSOS DE SEGURANÇA:

- **Proteção do core:**
  O kernel é o coração de um sistema operacional e, por isso mesmo, principal alvo para todo tipo de praga e outros tipo ataques. Basicamente, caso um cracker possa acessar ou manipular o kernel do sistema operacional, ele será capaz d executar códigos maliciosos em um nível que não é detectável por outras aplicações ou mesmo pelo sistema operacion propriamente dito. A Microsoft desenvolveu um modo de proteção do kernel para evitar que processos não autorizados tenham acesso ao núcleo do Windows 7.

- **Navegação segura:**

A primeira delas é o modo de navegação privativa ou anônima (InPrivate Browsing) proporciona a opção de surfar na web se deixar rastros. Quando a funcionalidade é ativada, o IE deixa de registrar qualquer informação relacionada com o que se faz web. Isso significa que nada do que é digitado é registrado no cache, nada de histórico dos sites visitados. A função é particularmente útil quando se compartilha um computador ou utiliza-se uma máquina em lugar público, como uma lan house biblioteca na escola.

Outra melhoria notável do IE8 é o Modo Protegido e que está relacionado a componentes de segurança do Windows 7 para impedir que códigos maliciosos ou não autorizados sejam executados dentro do navegador. Esta funcionalidade não permite exemplo, que a simples visita a um site contaminado possa baixar e instalar códigos maliciosos no computador.

INSTITUTO FEDERAL
Santa Catarina

- **Proteção que adoramos odiar:**

  O controle de contas de usuário (UAC pela sigla em inglês) é, provavelmente, a característica mais odiada e ao mesm tempo amada do Vista. No Windows 7, o UAC continua lá, mas a Microsoft adicionou um recurso que dá mais contro do nível de proteção ao usuário e, em decorrência, do número de pop-ups solicitando permissão para acesso ou execução de algum processo. Além disso, os pop-ups são apenas um aspecto do que o UAC proporciona. Muitos usuários simplesmente desabilitaram o UAC completamente no Vista. O problema é que ao fazer isso no Vista, eles também estavam desativando o modo de proteção do Internet Explorer além de outros recursos de proteção do siste operacional. O controle variável disponível no Windows 7 também faz o mesmo, mas o usuário tem melhor controle sobre o que desabilitar a partir de ajustes no Painel de Controle.

- **Ferramentas de segurança e aplicativos:**

Por conta do modo de proteção do kernel e das mudanças que a Microsoft fez para gerenciar, as aplicações são autorizad interagir com funcionalidades core do sistema operacional, antivírus e outros aplicativos de segurança mais antigos não sã compatíveis com o Windows 7.

TREND MICRO™

Symantec™ by Broadcom Software

McAfee™

- Tal fornecedores tem total compatibilidade com o windows, sendo assim fica a dica para quem quer deixar seu siste com segurança e proteção a mais.

CONCLUSÃO

Proteção é um problema interno. Segurança, por outro lado, deve considerar tanto o sistema de computação quanto o amb
— pessoas, prédios, empresas, objetos de valor e ameaças — dentro do qual o sistema é usado.

Os dados armazenados no sistema de computação devem ser protegidos contra acesso não autorizado, destruição ou alteração maliciosa e introdução acidental de inconsistências. É mais fácil se proteger contra a perda acidental da consistê dos dados do que se proteger contra o acesso malicioso aos dados. A proteção absoluta das informações armazenadas em sistema de computação contra abuso malicioso não é possível; mas o custo para o infrator pode ser suficientemente alto pa deter quase todas (quando não todas) as tentativas de acesso a essas informações sem autorização apropriada.

Vários tipos de ataques podem ser lançados contra programas e contra computadores individuais ou coletivos. Técnicas de estouro de pilha e de buffer permitem que invasores bem sucedidos alterem seu nível de acesso ao sistema. Vírus e verme são autoperpetuáveis e às vezes infectam milhares de computadores. Ataques de recusa de serviço impedem o uso legítim sistemas-alvo.

A criptografia limita o domínio de receptores de dados enquanto a autenticação limita o domínio de emissores. A criptografia usada para fornecer sigilo aos dados que estão sendo armazenados ou transferidos. A criptografia simétrica requer uma ch compartilhada, enquanto a criptografia assimétrica fornece uma chave pública e uma chave privada. A autenticação, quand combinada com o hashing, pode comprovar que os dados não foram alterados.

Os métodos de autenticação de usuários são usados para identificar os usuários legítimos de um sistema. Além da proteçã padrão com nome de usuário e senha, vários métodos de autenticação são usados. As senhas descartáveis, por exemplo, mudam de uma sessão para outra para evitar ataques de reexecução. A autenticação com dois fatores requer dois tipos de autenticação, tal como uma calculadora em hardware junto com um PIN de ativação. A autenticação com múltiplos fatores u três tipos ou mais. Esses métodos diminuem muito a chance de falsificação da autenticação.

Os métodos de prevenção ou detecção de incidentes de segurança incluem os sistemas de detecção de invasões, os softw antivírus, a auditoria e o registro em log de eventos do sistema, o monitoramento de alterações em softwares do sistema, o monitoramento de chamadas de sistema e firewalls.

INSTITUTO FEDERAL
Santa Catarina

QUESTIONÁRIO

1: O que é matriz de acesso?

2: De que recursos de hardware um sistema de computação precisa para a manipulação eficiente de competências? Esses recursos podem ser usados para proteção da memória?

3: Uma senha pode se tornar conhecida por outros usuários de várias maneiras, diga os métodos simples:

4: como proteger arquivos com senhas no linux?

1: A matriz de acesso é um modelo teórico usado para mapear os acessos dentro de uma organização. Foi criado em 2013 pelo profissional de TI Ticiano Benetti, com o objetivo de apresentar as questões de segurança da informação de forma mais segmentada para gerentes de uma empresa.

2:Um TPM (Trusted Platform Module) foi projetado para fornecer funções relacionadas à segurança baseadas em hardware e ajudar a evitar adulterações indesejadas. Os TPMs fornecem benefícios de segurança e privacidade para hardware do sistema, proprietários de plataforma e usuários. Um chip TPM é um processador de criptografia seguro que ajuda com ações como gerar, armazenar e limitar o uso de chaves criptográficas. Muitos TPMs incluem vários mecanismos de segurança física para torná-lo resistente a adulterações e impedir que o software mal-intencionado altere as funções de segurança do TPM.

3: Há duas maneiras comuns de adivinhar uma senha. Uma delas é o intruso (humano ou programa). uma senha de quatro caracteres fornece apenas 10.000 variações. Em média, 5.000 tentativas produziriam um acerto. Um programa que pudesse testar uma senha a cada milissegundo levaria apenas cerca de 5 segundos para adivinhar uma senha de quatro caracteres. tipo de comprometimento da senha, a transferência ilegal, é resultado da natureza humana.

4: prático (link no slide **Implementando Defesas de Segurança**)