Segurança em Redes

Aula 02 - Introdução aos Mecanismos de Defesa

Apresentação

Nesta aula, você vai dquirir uma visão geral dos principais mecanismos de defesa utilizados para proteger os sistemas dos ataques estudados na Aula 1. Nas próximas aulas, cada um desses mecanismos será estudado mais detalhadamente. Sempre que preciso, lance mão da Aula 1 para acompanhar melhor os assuntos abordados nesta aula.

Vídeo 01 - Apresentação

Objetivos

- Identificar os principais mecanismos de segurança.
- Diferenciar a finalidade dos mecanismos de segurança.

Visão Geral

Até agora você conheceu alguns tipos de ataques e atacantes, e deve estar bem preocupado em como proteger o seu ambiente computacional. Nesta aula, você verá uma introdução aos diversos mecanismos de defesa existentes que, por sua vez, serão detalhados nas aulas subsequentes.

Na aula passada, você viu que **Confidencialidade**, **Integridade** e **Disponibilidade** são princípios fundamentais da segurança de sistemas computacionais. Você lembra o que vem a ser esses três princípios?

Relembrando

De forma resumida, Confidencialidade consiste na proteção da informação contra acessos (leitura ou escrita ou cópia) não autorizados. Integridade consiste em proteger as informações (dados, programas) de forma que elas permaneçam íntegras, ou seja, não sejam modificadas sem a expressa autorização do proprietário. Disponibilidade diz respeito à proteção dos serviços do sistema para que eles não sejam danificados e se tornem indisponíveis para os usuários.

Além desses, há outro princípio muito importante: a autenticidade, que consiste em verificar a identidade de um usuário. Por exemplo, em um computador da universidade Federal do Rio Grande do Norte (UFRN), um aluno, a partir de sua matrícula e senha, é capaz de se autenticar, ou seja, provar a sua identidade, para acessar e usar um computador.

Atenção

Não confundir autenticação com autorização! Uma pessoa autenticada não necessariamente está autorizada a fazer determinada ação. Por exemplo, um determinado usuário autentica-se para poder acessar um computador, mas tem autorização limitada para instalar e executar determinados programas. Outro exemplo seria de um aluno acessa alguns sistemas da UFRN, mas não tem autorização para realizar as mesmas ações que um professor.

Atividade 01

1. Pense e responda: fora do mundo dos computadores, existem outros exemplos claros de integridade e disponibilidade? Cite um exemplo de cada.

Mecanismos de Defesa e seus Princípios

Devido à existência de um ambiente inseguro nas redes de computadores, você deve estar se perguntando: como se defender dos *hackers* e dos tipos de ataques que aprendemos na Aula 1?

Em um ambiente coorporativo (empresas), com muitas informações sigilosas, podem ser utilizadas as **políticas de segurança**, ou seja, conjuntos de regras, normas e práticas de gestão que visam à proteção dos seus dados e sistemas. Para isso, primeiramente, para a criação da política de segurança, é necessário decidir sobre o que é importante ou não dentro daquela empresa, o que deve envolver vários profissionais de áreas técnicas, operacionais, administrativas etc. Por exemplo, se a preocupação da empresa é apenas proteger seus dados, uma vez que é a fonte de seu negócio, ela, provavelmente, vai adotar um conjunto de ações (política de segurança) para fazer com que a segurança dos dados seja a prioridade, nisso ela usará vários serviços de proteção para evitar acessos não autorizados ou outros tipos de ataques.

Um item comum na política de segurança são as regras para formação de senhas de acesso a sistemas. Nesse caso, o administrador estabelece as regras para sua criação ou alteração, por exemplo:

- Senhas têm de ter letras e números.
- Senhas têm de ter no mínimo 6 (seis) caracteres.
- Senhas devem ser mudadas a cada 30 dias.
- No caso da mudança de senha, o sistema não deixará que se use a mesma senha anterior ou as 4 últimas usadas.
- Não pode ser usada a mesma senha em vários serviços (por exemplo, para acessar um computador e um sistema corporativo).

Esse é um exemplo de norma que um administrador pode ter para garantir o uso de senhas adequadas, mantendo, assim, os dados da empresa em sigilo.

Mas, não é só nas empresas que as políticas de segurança podem ser aplicadas. Elas também devem ser aplicadas na sua casa ou na sua rede local. Existem várias forma de implementar as políticas de segurança e que chamamos de **mecanismos de segurança**.

Assim, você pode perceber que os **mecanismos de segurança** são técnicas usadas para assegurar a segurança de um sistema, de forma que apenas usuários e processos autorizados podem desempenhar ações no sistema. Alguns dos principais mecanismos de segurança são: criptografia, autenticação (assinatura digital, certificados digitais e sistemas biométricos) *firewall* e os Sistemas de Detecção de Intrusão (IDS). Em geral, **um ou mais mecanismos de segurança são combinados** para fornecer um serviço de segurança que implementam uma política específica.

Atividade 02

---

1. Crie suas próprias regras para definição de senhas, e as coloque em uso a partir de hoje.

Criptografia

Vídeo 02 - Criptografia

Criptografia é uma palavra vinda do Grego *kryptós*, que significa "escondido, secreto", e *gráphein*, "escrita". É, portanto, o estudo de princípios e técnicas para manter mensagens confidenciais. Normalmente, “disfarça-se” uma mensagem original para que ela só possa ser entendida pelo seu emissor e destinatário. Protocolos de criptografia definem formas de se “embaralhar” a informação. Uma forma bastante simples de se realizar criptografia é pela troca de todas as letras de um texto, conforme a regra a seguir:

Original:	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Muda Para:	Y R G K X O L N S Z T V W B E J A U D M C F H I P Q

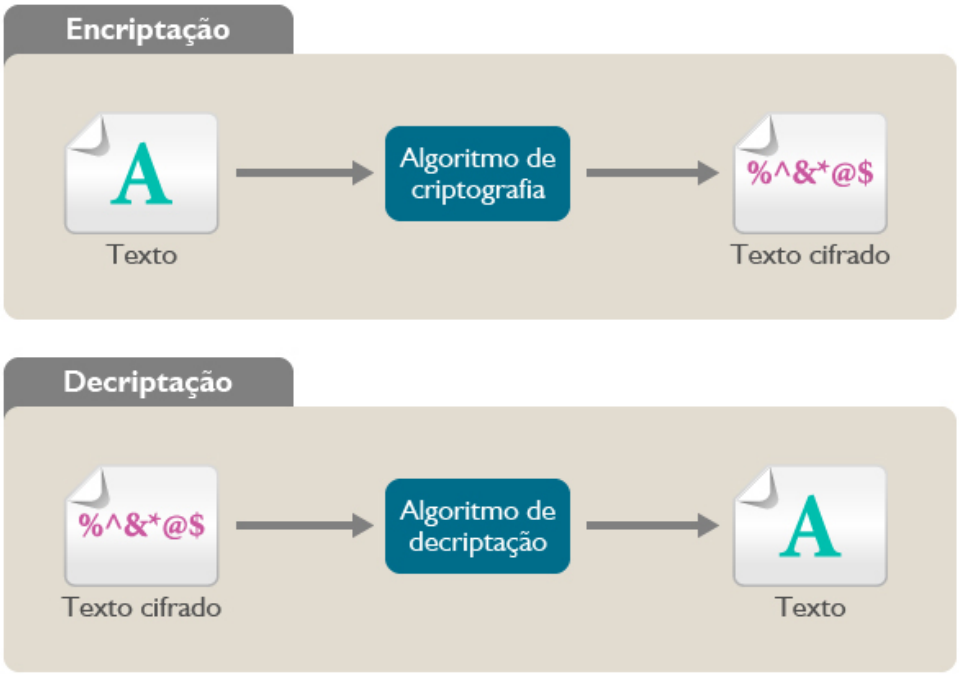
O texto original “leia-me se puder” seria transformado em “vxsy-wx dx jckxu”. Nesse exemplo, se eu e você conhecemos a regra de substituição das letras, conseguiremos nos comunicar com confidencialidade, bastando enviar apenas o texto “embaralhado”. No destino, de posse da regra, basta você fazer as substituições no sentido inverso, para obter o texto original. Uma terceira pessoa que não conhece a regra e copia nossa conversa não entenderá. Assim funciona o principio da criptografia, porém não se trata apenas de substituições simples de letras, mas sim de **complexos cálculos matemáticos**, pois, afinal, estamos tratando de informações importantes que, às vezes, valem fortunas.

Em termos gerais, a criptografia é feita em duas etapas: a cifragem (em inglês: *encryption*) e a decifragem (em inglês: *decryption*). A cifragem é o processo de tornar a mensagem original ilegível. Podemos chamar também de cifrar, criptografar ou, ainda, encriptar. A decifragem transforma a mensagem cifrada (ilegível) na

mensagem original (novamente legível). Podemos chamar também de decriptar. A criptografia é um dos mecanismos de segurança mais completos, possuindo ferramentas que garantem a confidencialidade, integridade, autenticação e não repúdio. Você sabe o que é não repúdio? Logo mais você estudará esse assunto.

Na figura 1, ilustramos, de forma simples, o processo de encriptação e decriptação. Na encriptação, um texto original é submetido a um algoritmo de criptografia e obtém-se um texto cifrado. Na decriptação, o texto cifrado é submetido a um algoritmo de decriptação que faz processo inverso do anterior, obtendo-se o texto original.

Figura 01 - Processo de Encriptação e Decriptação



Curiosidade

Você sabia que a Criptografia não é uma invenção da era dos computadores? Ela está presente na história dos povos desde a antiguidade!!! Era usada para garantir que informações confidenciais, fórmulas secretas, entre outras informações, não se tornassem públicas ou chegassem às mãos de inimigos.

Autenticação

É a confirmação de que algo ou alguém é autêntico, verdadeiro. A autenticação tem o papel de validar a identificação dos usuários da rede e/ou sistemas. Uma das formas mais simples de autenticar um usuário é pela solicitação de um nome de usuário (*login)* e a senha.

Contudo, existem outras formas mais sofisticadas, que iremos estudar na Aula 4, de realizar autenticação. Em alguns casos, é usada uma combinação de dois ou mais métodos de autenticação. Por exemplo: algumas empresas utilizam uma combinação de um cartão pessoal, com um código de barras, mais uma senha, para autenticar um funcionário, e permitir o seu acesso a uma sala em particular.

Existem tipos bastante sofisticados de autenticação como os certificados digitais, amplamente utilizados pelos sites de bancos ou de comércio eletrônico, e os meios biométricos como impressão digital e padrões de voz. Você sabe o que são meios biométricos? Ainda nesta aula você saberá mais sobre isso.

Após a autenticação, o sistema irá conceder um conjunto de autorizações de acesso a recursos. Essa autorização é atribuída pelo administrador aos usuários e, normalmente, é definida com base em três métodos: (a) no que o usuário sabe (como, por exemplo, uma senha de acesso); (b) no que o usuário tem (cartão de identificação com código de barra, por exemplo); (c) em alguma característica do usuário (sistemas biométricos). Quanto mais métodos envolvidos para determinar a autenticação e autorização, maior o nível de segurança.

A autenticação é fundamental não só em Sistemas Computacionais, mas em qualquer área, para identificar quem é o autor de um ato e impedir que o legítimo autor negue que fez algo por arrependimento ou por má fé. Ou seja, a autenticação garante o **não repúdio**, isto é, impede que o autor de um ato negue que o tenha feito. Por exemplo, a assinatura de um documento com registro em cartório garante a identificação da pessoa que assinou o documento e que ela está ciente do conteúdo do documento.

Vídeo 03 - Mecanismos de Autenticação

Atividade 03

1. Liste mecanismos de autenticação que você já utilizou na internet e no mundo real.
2. Dê exemplo de autorizações que você não possui no sistema da Metrópole Digital.

Assinatura digital

Também chamada de **firma digital**, a assinatura digital é uma técnica que garante a **integridade** e **autenticidade** de uma informação digital. A assinatura digital permite comprovar que uma mensagem ou arquivo não foi alterado por terceiros e que foi assinada pela pessoa que está ali representada. Ela é equivalente à assinatura feita no papel, no entanto, é composta por um conjunto de operações criptográficas. Uma assinatura digital deve ter as seguintes características:

1. *Autenticidade* – o receptor da informação deve ser capaz de confirmar que a assinatura foi feita pelo emissor.
2. *Integridade* – qualquer alteração na informação faz com que a assinatura deixe de ser válida.
3. *Não repúdio* – o emissor não pode negar a o envio ou autenticidade da mensagem.

Curiosidade

O termo **assinatura eletrônica**, às vezes, é confundido com **assinatura digital**, mas assinatura eletrônica tem um significado diferente: refere-se a qualquer mecanismo, não necessariamente criptográfico, para identificar o remetente de uma mensagem eletrônica.

Sistemas Biométricos

Biometria deriva de (*bios* = vida, *metron* = medida). É realizada pelo uso de características biológicas em mecanismos de autenticação. Esses métodos analisam características físicas ou comportamentais do usuário para determinar sua identificação. As duas características mais comumente utilizadas em sistemas biométricos são a impressão digital e a íris do olho. Contudo, existem outras características biológicas usadas na identificação, tais como:

- Retina.
- Voz.
- Palma da mão.
- DNA etc.

O uso dessas características para identificação é segura, uma vez que elas são únicas. Por exemplo, não há como existir duas pessoas com a mesma impressão digital.

Curiosidade

Você sabia que a biometria não é um conceito novo? A sua aplicação na computação é que é algo recente. Os faraós do Egito usavam características físicas dos indivíduos (arcada dentária, cicatrizes) para diferenciá-los.

Firewalls

Em português, significa “muro corta-fogo”. É o nome dado ao dispositivo responsável por controlar e autorizar a entrada e saída de tráfego na rede, tornando-a mais resistente a invasões e, consequentemente, a ataques. O nome é esse porque o *firewall* atua como uma “parede”, evitando que programas ou usuários externos não autorizados acessem sistemas ou computadores internos da rede.

Quais os sistemas ou computadores ele evita alcançar? Isso depende da política do *firewall,* que é estabelecida pelo seu administrador. Veremos detalhes sobre isso na nossa aula exclusiva sobre *firewalls*, a Aula 8.

Alguma vez já apareceu na tela do seu navegador, em redes internas, como em escolas ou universidades, uma mensagem dizendo que a página está bloqueada e pedindo para entrar em contato com o administrador da rede? Em caso afirmativo, você foi pego pelo *firewall*!

Um *firewall* pode ser um dispositivo de *hardware*, um *software*, ou ambos. Assim, em uma definição mais formal, o *firewall* é um conjunto de componentes e funcionalidades que utilizam uma ou mais tecnologias de filtragem para proteger uma rede contra ataques e acessos indevidos.

Vídeo 04 - *Firewalls*

Sistemas de Detecção de Intrusão (IDS)

São sistemas capazes de detectar ataques e intrusões, pelo monitoramento do ambiente computacional em busca de **atividades suspeitas ou impróprias**. O IDS trabalha como um alarme, identificando possíveis intrusões a partir de um desvio de comportamento na rede, ou pelo conhecimento da forma de um ataque.

Ao identificar ou reconhecer um determinado ataque, os administradores da rede e/ou sistemas são alertados. Esse tipo de alerta fornecido pelo IDS permite a melhoria nas defesas contra possíveis ataques, principalmente os internos, que podem passar despercebidos ao *firewall*.

Auditoria

Em sistemas computacionais, a auditoria tem como uma de suas funções avaliar os procedimentos de controle e segurança. Para isso, o auditor examina se os sistemas estão em conformidade com a política de segurança da organização e se estão protegidos das ameaças do mundo digital. São vários os aspectos analisados na auditoria. Um exemplo comum é verificar se existem cópias dos dados para situações de emergência (por exemplo, perda de arquivos, incêndios etc.). Todo usuário deve ser capaz de "auditar" o seu próprio ambiente computacional, de forma simples, verificando, por exemplo, se possui cópias de todos os arquivos importantes em *pen-drives* ou outro meio externo de armazenamento, como CDs ou DVDs graváveis.

A auditoria pode ser:

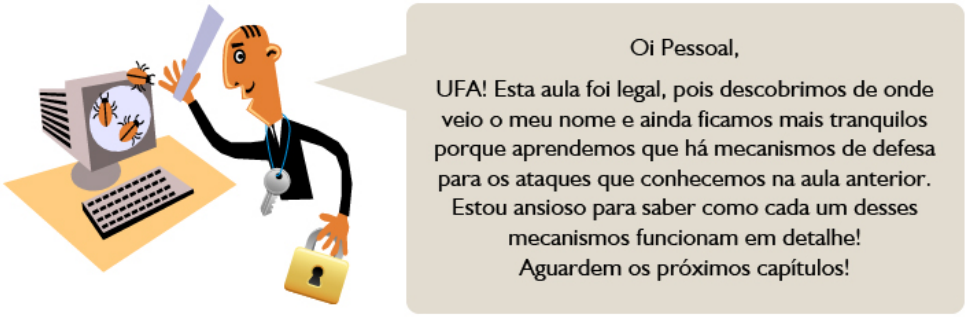
- **Preventiva**: para prevenir ataques e realizar melhorias na política de segurança.
- **Detectiva**: para detectar vulnerabilidades existentes, passíveis de serem exploradas.
- **Corretiva**: para corrigir vulnerabilidades já exploradas e reduzir a possibilidade de novos ataques a ela relacionados.

Você sabia que o auditor de um sistema computacional precisa ser um profissional muito dedicado, estar sempre ligado nos novos tipos de ataques e nas estratégias de defesa?

Curiosidade

Você se lembra dos white hats? Você sabia que, normalmente, eles são contratados pelas empresas para fazer testes e simulações para medir o nível de segurança das redes? Ou seja, para fazer uma auditoria!

Conclusão



Leitura Complementar

Sobre Mecanismos de Segurança:

- <http://www.oficinadanet.com.br/>

Atividade 04

1. Você sabe o que são certificados digitais? Pesquise!

Resumo

Na aula anterior, você soube da existência de diversos tipos de ameaças, ataques e atacantes que aumentam a importância de proteger o seu ambiente computacional. Para isso, nesta aula, você aprendeu que é possível usar políticas de segurança, ou seja, um conjunto de regras, normas e práticas de gestão que, apoiados por diversos mecanismos de defesa, visam proteger sistemas computacionais. Você viu também que a escolha de uma política depende do nível de segurança que se deseja obter. Por exemplo, em um ambiente que se deseja obter muita segurança, é necessário usar vários mecanismos para alcançar o nível de proteção desejado. Dentre os principais mecanismos podem ser destacados a criptografia, autenticação, assinatura digital, sistemas biométricos, *firewalls* e IDSs, sendo a criptografia a base para vários outros mecanismos.

Autoavaliação

1. Regras para definição de senhas fazem parte da política ou dos mecanismos de segurança? Por quê?
2. O que é criptografia? Para que servem as operações de encriptar e decriptar?

3. O que é não repúdio? Cite um mecanismo de segurança que o garanta.
4. Para que serve um Firewall? Qual a sua diferença para um IDS?
5. Qual a importância de se realizar auditorias de segurança no dia a dia de uma empresa?

Referências

CERT.BR. **Práticas de Segurança para Administradores de Redes Internet**. Disponível em: <http://www.cert.br/docs/seg-adm-redes/>. Acesso em: 1 mar. 2012.

NAKAMURA, E.; GEUS, P. L. **Segurança em redes em ambientes cooperativos**. São Paulo: Novatec, 2007.

STALLINGS, W. **Cryptography and network security**: principles and practice. 5th ed. New York: Prentice Hall, 2010. 744 p.