SEGURANÇA DA INFORMAÇÃO E DE REDES

Prof. Milton Palmeira Santana

Firewall

- O **firewall de filtro de pacotes** controla o acesso à rede analisando os pacotes de saída e de entrada. Na prática, ele permite que um pacote passe ou seja bloqueado durante o caminho fazendo a comparação com critérios definidos antecipadamente.

- É ideal para redes pequenas, sendo mais complexa a análise em redes maiores.

- Esse tipo de firewall não pode impedir todos os tipos de ataques, pois ele não tem a capacidade de enfrentar os ataques que usam vulnerabilidades nas camadas de aplicativos e lutar contra ataques de falsificação.

Firewall

- Os **Firewalls de aplicação ou servidor proxy** são os tipos de firewall mais seguros. Eles podem proteger os recursos de rede de forma eficaz filtrando as mensagens, mascarando seu endereço IP e limitando os tipos de tráfego.

- Eles fornecem uma análise de segurança completa e com reconhecimento dos protocolos que suportam. Para as grandes empresas, os firewalls de aplicação oferecem a melhor experiência na internet e resultam nas melhorias de desempenho da rede.

Introdução

- Uma das definições de criptografia diz que ela é a arte de escrever ou resolver códigos. A criptografia deriva de duas palavras gregas: kryptos, que significa oculto, e graphien, que significa escrever. O objetivo da criptografia não é esconder a existência da mensagem, mas sim de apenas ocultar o seu significado.

- De um modo geral, se a mensagem cair nas mãos de um intruso, este, ao lê-la, não a compreenderá. Apenas o remetente e o destinatário, em princípio, com um acordo pré-estabelecido (as chaves), é que têm acesso ao significado da mensagem.

- O termo criptografia é usado muitas vezes como sinônimo de criptologia, abrangendo, desta forma, a criptanálise, que tem por função descobrir os segredos ou quebrar a confidencialidade entre emissor e receptor.

História – Criptografia clássica

- Historicamente, os métodos clássicos de criptografia são divididos em duas técnicas:
  - Cifras de substituição
  - Cifras de transposição
- Na transposição as letras das mensagens são simplesmente rearranjadas, gerando, efetivamente um anagrama.
- Para mensagens muito curtas, esse método é relativamente inseguro. Por exemplo, uma palavra de três letras só pode ser rearranjada de seis maneiras diferentes. Exemplo: ema, eam, aem, mea, mae, ame.

História – Criptografia clássica

- A alternativa para a transposição é a substituição.
- As cifras de substituição preservam a ordem dos símbolos no texto claro, mas disfarçam esses símbolos.
- Cada letra ou grupo de letras é substituído por outra letra ou grupo de letras, de modo a criar um “disfarce”.

História – Criptografia clássica

- O primeiro documento que usou uma cifra de substituição para propósitos militares aparece nas guerras da Gália de Júlio César.

- A Cifra de César, também conhecida como cifra de troca, código de César ou troca de César, é uma das mais simples e conhecidas técnicas de criptografia. É um tipo de cifra de substituição na qual cada letra do texto é substituída por outra, que se apresenta no alfabeto abaixo dela um número fixo de vezes.

- O nome do método é em homenagem a Júlio César, que o usou para se comunicar com os seus generais.

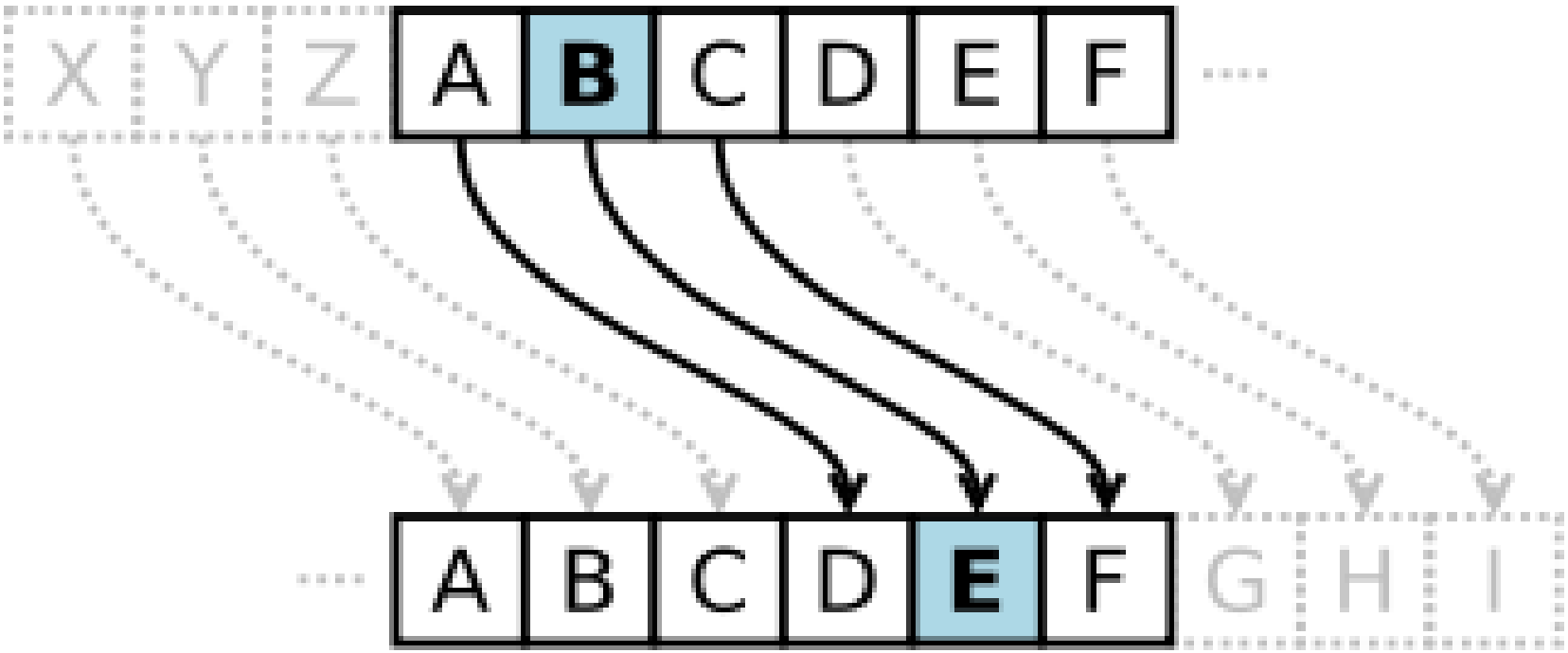
História – Criptografia clássica

- Considerando as 26 letras do alfabeto

  (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),

- Neste método, **a** se torna **D**, **b** se torna **E**, **c** se torna **F**, … …, **z** se torna **C**.

História – Criptografia clássica



História – Criptografia clássica

- EXEMPLO:

C O M P U T A C A O

F R P S X W D F D R

Criptografia de chave privada

- O sistema de **chave privada ou única** consiste em encriptar uma mensagem usando uma chave criptográfica secreta, que é apenas conhecida pelo emissor e pelo receptor da mensagem.

- Esse sistema inspirou um tipo de criptografia chamado de criptografia simétrica.

- O termo simétrico é dado porque nos dois lados da transmissão a chave que é usada para **encriptar** é a mesma usada para **decriptar** uma mensagem.

Criptografia de chave privada

- A criptografia de chave simétrica, quando comparada com a de chaves assimétricas, é a mais indicada para garantir a confidencialidade de grandes volumes de dados, pois seu processamento é mais rápido. Todavia, quando usada para o compartilhamento de informações, se torna complexa e pouco escalável, em virtude da:
  - necessidade de um canal de comunicação seguro para promover o compartilhamento da chave secreta entre as partes (o que na Internet pode ser bastante complicado) e;
  - dificuldade de gerenciamento de grandes quantidades de chaves (imagine quantas chaves secretas seriam necessárias para você se comunicar com todos os seus amigos).

Criptografia de chave privada

- A criptografia simétrica é uma forma simples e fácil de criptografar, porém, muito vulnerável, pois se uma rede não é segura o suficiente para não permitir que algum indivíduo acesse a mensagem enviada também não será suficientemente segura para transferir uma chave.

- Outro problema é que neste tipo de criptografia a chave não é de conhecimento exclusivo do emissor, sendo assim, como garantir que a mensagem foi realmente enviada por ele?

- Exemplos de métodos criptográficos que usam chave simétrica são: AES, Blowfish, RC4, 3DES e IDEA.

Criptografia de chave pública

- Também conhecida como criptografia de chave **assimétrica**, utiliza duas chaves distintas: uma pública, que pode ser livremente divulgada, e uma privada, que deve ser mantida em segredo por seu dono.

- Quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la. Qual chave usar para codificar depende da proteção que se deseja, se confidencialidade ou autenticação, integridade e não-repúdio. A chave privada pode ser armazenada de diferentes maneiras, como um arquivo no computador, um smartcard ou um token.

Criptografia de chave pública

- Exemplo: tanto o usuário do computador A quanto o usuário do computador B possuem suas chaves públicas e privadas.

- Se o usuário da máquina A quiser enviar uma mensagem para o usuário da máquina B, basta utilizar a chave pública do usuário B para codificar a mensagem. A decodificação fica a cargo da chave privada que é de conhecimento APENAS do usuário B.

- Se o usuário da máquina B quiser enviar uma mensagem para o usuário da máquina A, basta utilizar a chave pública do usuário A para codificar a mensagem. A decodificação fica a cargo da chave privada que é de conhecimento APENAS do usuário A.

Criptografia de chave pública

- Exemplos de métodos criptográficos que usam chaves assimétricas são: RSA, DSA, ECC e Diffie-Hellman.

- A criptografia de chaves assimétricas, apesar de possuir um processamento mais lento que a de chave simétrica, resolve os problemas anteriores citados visto que facilita o gerenciamento (pois não requer que se mantenha uma chave secreta com cada um que desejar se comunicar) e dispensa a necessidade de um canal de comunicação seguro para o compartilhamento de chaves.

Criptografia de chave pública

- Para aproveitar as vantagens de cada um destes métodos, o ideal é o uso combinado de ambos, onde a criptografia de chave simétrica é usada para a codificação da informação e a criptografia de chaves assimétricas é utilizada para o compartilhamento da chave secreta (neste caso, também chamada de chave de sessão). Este uso combinado é o que é utilizado pelos navegadores Web e programas leitores de e-mails. Exemplos de uso deste método combinado são: SSL, PGP e S/MIME.

Função Hash

- Uma função de resumo é um método criptográfico que, quando aplicado sobre uma informação, independente do tamanho que ela tenha, gera um resultado único e de tamanho fixo, chamado hash.

- Exemplos de utilização:
  - verificar a integridade de um arquivo armazenado em seu computador ou em seus backups;
  - verificar a integridade de um arquivo obtido da Internet (alguns sites, além do arquivo em si, também disponibilizam o hash correspondente, para que você possa verificar se o arquivo foi corretamente transmitido e gravado);
  - gerar assinaturas digitais

Função Hash

- Exemplos de métodos de hash são: SHA-1, SHA-256 e MD5.

Esteganografia

- A diferença entre a criptografia e esteganografia é que a primeira oculta o significado da mensagem, enquanto a segunda oculta a existência da mensagem.

- Exemplo de utilização:
  - Marcas d'água visíveis em cédulas de dinheiro.

Aspectos não tecnológicos em segurança da informação

- Iremos discutir três categorias gerais de aspectos não tecnológicos (ISO 27001, 2013; ISO 27005, 2011) que são os aspectos físicos, humanos e naturais.
- Desastres
- Acidentes
- Falhas
- Engenharia Social
- Terrorismo

Políticas de Segurança

- A política de segurança é composta por um conjunto de documentos ou capítulos que devem ser lidos, compreendidos e seguidos pelos respectivos responsáveis.

- Há as diretrizes, as normas, os processos e os procedimentos de segurança da informação.

- A política de segurança protege a empresa, por isso, todos devem segui-la.

- A política tem o foco em pessoas, prevenindo os usuários de serem vítimas de phishing, que leva ao roubo de credenciais de acesso, por exemplo.

Políticas de Segurança

- Um dos assuntos importantíssimos tratados na política de segurança é a senha.

- Criação de regras como tamanho mínimo e tempo de validade, a política de senhas deve ser implementada na medida certa para não ser um obstáculo aos usuários e para não criar insegurança na empresa.
  - O usuário têm que escolher uma senha forte e adiciona: M!nH@$0dm31kxç1? Que pode ser uma senha extremamente forte.
  - Mas ele têm problemas para lembrar, por isso anota em um post it que deixa colado no monitor de seu computador de trabalho. ☺

EXERCÍCIOS REVISÃO

1) O que significa encriptar e decriptar?

2) Por que a criptografia simétrica é vulnerável?

3) Com a criptografia assimétrica, como garantir a confidencialidade?

4) Com a criptografia assimétrica, como garantir o não-repúdio?

REFERÊNCIAS

MACHADO, Felipe Nery Rodrigues. **Segurança da Informação: princípios e controle de ameaças**. [S. l.]: ÉRICA, 2014.

FONTES, Edison. **Segurança da Informação**: O usuário faz a diferença. [S. l.]: SARAIVA, 2007.

SMULDERS, André; BAARS, Hans; HINTZBERGEN, Jule; HINTZBERGEN, Kees. **Fundamentos de Segurança da Informação**: com base na ISO 27001 e na ISO 27002. [S. l.]: BRASPORT, 2018.

BASTA, Alfred; BASTA, Nadine; BROWN, Mary. **Segurança de computadores e teste de invasão**. [S. l.]: Cengage Learning, 2014.

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à Segurança de Computadores**. [S. l.]: Bookman Editora, 2013.

STALLINGS, WILLIAM. **Criptografia e Segurança de Redes**: Princípios e práticas. 6. ed. [S. l.]: Pearson Universidades, 2014.

SINGH, Simon. **O livro dos códigos**: A ciência do sigilo – do antigo Egito à criptografia quântica. [S. l.]: Record, 2001.


Anhanguera