Segurança em Redes

Aula 04 - Autenticação

Apresentação

Nesta aula, iremos estudar mais detalhadamente o que vem a ser autenticação, sua importância e como ela pode ser realizada.

Vídeo 01 - Apresentação

Objetivos

Ao final desta aula, você será capaz de:

- Diferencia os tipos de autenticação.
- Saber como a autenticação é realizada.
- Conhecer as vulnerabilidades de cada tipo de autenticação.

Visão Geral

Na segunda aula, nós vimos uma introdução aos mecanismos de segurança e aprendemos que a autenticação é a confirmação de que algo ou alguém é **autêntico**, **verdadeiro**. Comentamos sobre formas de autenticação simples, como login e senha, e mais sofisticadas, como sistemas biométricos.

O objetivo da autenticação é proteger as duas partes que trocam uma mensagem. A autenticação, no entanto, não protege as duas partes uma contra a outra. Por exemplo, pode acontecer que: (a) alguém forje uma mensagem e diga que foi enviada por outra pessoa; (b) alguém negue o envio de uma mensagem, dizendo que ela foi forjada. Esse problema é resolvido pela Assinatura Digital, que estudaremos mais adiante.

Você lembra, em aulas anteriores, que falamos que grande parte dos mecanismos usa criptografia? Pois é, a criptografia é a base dos principais mecanismos de autenticação. Lembra quando falamos que a criptografia ajuda a garantir autenticidade? Isso mesmo! A criptografia é usada na autenticação digital.

Por exemplo, se Maria vai se comunicar com João, e enviar alguns documentos, João precisa ter certeza que foi realmente Maria quem enviou, ou seja, que a mensagem vem mesmo de Maria. Autenticação é o mecanismo que garante isso.

Atividade 01

1. Que formas de autenticação você mais usa no dia a dia?

Funções da Autenticação

As principais funções da autenticação de uma mensagem são:

1. garantir quem enviou a mensagem;

2. garantir que a mensagem não teve seu conteúdo alterado.

Podemos distinguir a autenticação quanto ao elemento que deve ser autenticado, por exemplo:

1. **Autenticação de usuário**: em geral ocorre para a entrada do usuário em um sistema. A autenticação do usuário pode ser feita de várias formas, através de senhas, *smart cards*, biometria etc.

2. **Autenticação de máquinas**: pode ser feita com base em informações disponíveis na própria rede, como o endereço IP de cada máquina.

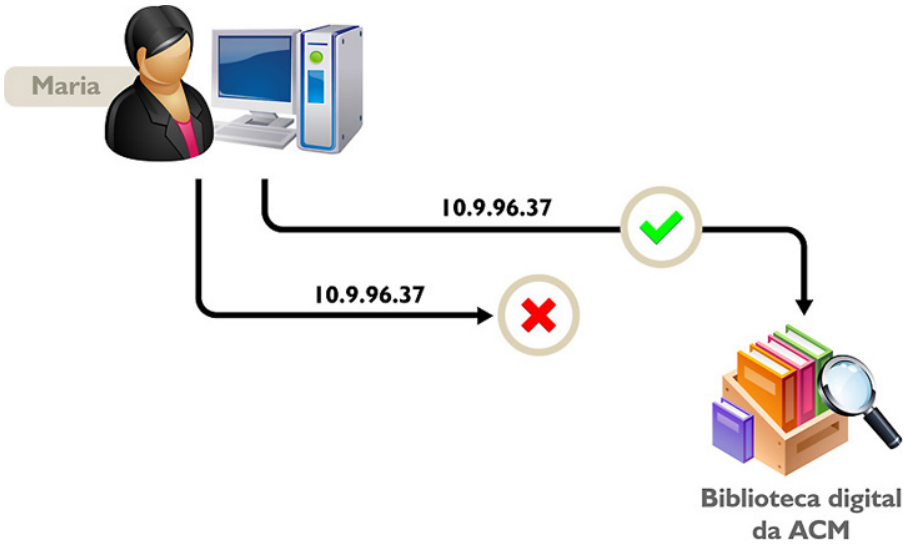
Métodos de Autenticação

Dentre os diversos métodos de autenticação que iremos estudar a seguir, podemos destacar três categorias:

1. **Baseados em senha**: o usuário ou programa autentica-se usando uma senha. Essa é a forma mais comum de autenticação, mas não muito segura, pois algum atacante pode, por exemplo, interceptar a transmissão da senha na rede.

2. **Baseado em endereço**: nesse tipo de autenticação o importante é o local onde o usuário ou programa se encontra. A identidade, nesse caso, é inferida baseada no endereço de rede do qual a mensagem se origina. Nesse caso, o computador destino tem um banco de endereços de quem pode ter acesso aos recursos. Por exemplo, suponha que todos os usuários que estejam em uma rede cujo endereço é 10.11.12.0/24 podem acessar os recursos da biblioteca digital da ACM (*Association for Computing Machinery* - http://www.acm.org). Então, se Maria utiliza a máquina cujo endereço é 10.11.12.46, que faz parte dessa rede, ela conseguirá entrar no site da biblioteca digital da ACM, que fará sua autenticação. No entanto, se Maria utiliza a máquina 10.30.77.40, ela não conseguirá ter acesso à biblioteca digital da ACM, porque essa rede não tem permissão, como demonstrado na **Figura 1**.

Figura 01 - Acesso com autenticação via endereço de rede.



Apesar da autenticação baseada em endereço não ter o problema da escuta por parte de um atacante, outros problemas de segurança podem acontecer. Por exemplo, a personificação do endereço de rede. O que seria isso? Seria um atacante enviar pacotes com endereço de outra rede, diferente da que ele se encontra.

3. **Baseado em criptografia**: nesse tipo de autenticação não importa a senha nem o local onde você está, mas um segredo gerado através de uma operação de criptografia.

Vídeo 02 - Tipos de Autenticação

Atividade 02

1. Qual o principal tipo de ataque que a autenticação baseada em senha pode sofrer?
2. Qual o principal tipo de ataque que a autenticação baseada em endereço pode sofrer?

Curiosidade!

Você já ligou para o atendimento de um banco ou operadora de telefonia e eles pediram para você confirmar uma série de dados, como endereço, identidade, CPF, nome da mãe etc.? Pois fique sabendo que isso é na verdade um mecanismo de autenticação. É dessa forma que a operadora de telefonia (por exemplo) "autentica" que é realmente você quem está falando ao telefone.

Mecanismos de Autenticação

Agora, vamos conhecer alguns mecanismos bastante usados para autenticação:

1. Usando criptografia assimétrica ou de chave pública;
2. Inserindo um código, chamado de código MAC (*Message Authentication Code*), que é calculado em função da mensagem e da chave, com criptografia simétrica.

Observe que há outros mecanismos também usados, como Sistemas Biométricos, que veremos na Aula 8.

Autenticação com Criptografia Assimétrica

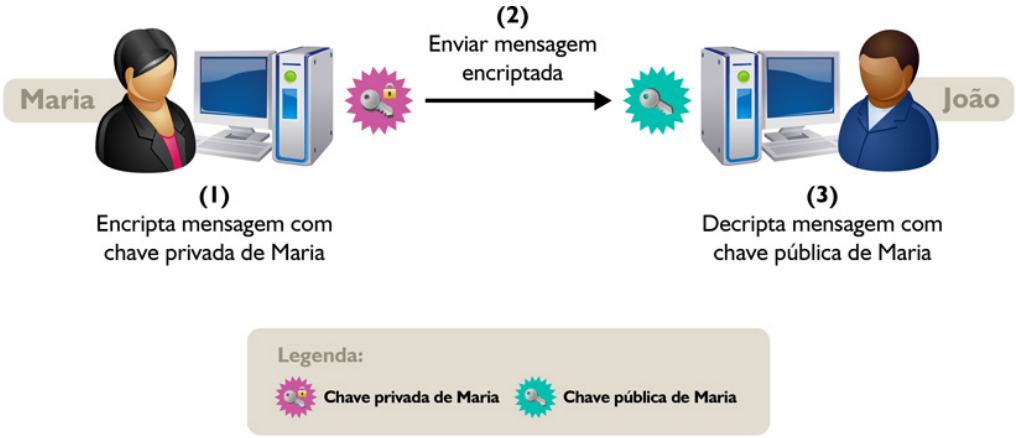
Você deve lembrar que já estudamos a criptografia assimétrica ou de chaves públicas na aula anterior. Vamos recordar: nesse tipo de criptografia, cada entidade possui um par de chaves, uma pública e uma privada. Tal mecanismo não serve apenas para garantir confidencialidade, mas também para autenticação.

Se Maria e João querem confidencialidade na troca de mensagens, Maria cifra a mensagem com a chave pública de João, e ela tem certeza que apenas João consegue decifrá-la com a chave privada que pertence a ele. Nesse caso, a confidencialidade foi garantida, mas a autenticação não foi, uma vez que João não

tem certeza de que a mensagem foi enviada por Maria. Qualquer pessoa poderia cifrar a mensagem com a chave pública de João, já que ela é pública. Portanto, a mensagem poderia ter sido enviada por Maria ou por qualquer outra pessoa.

Para garantir autenticação, Maria deve cifrar a mensagem com sua chave privada, que apenas ela conhece, e João (ou qualquer outra pessoa) pode decifrá-la com a chave pública de Maria, conforme mostrado na Figura 2. Dessa forma se teria a garantia de que a mensagem realmente veio de Maria. Autenticação realizada! Nesse caso, não há garantia de confidencialidade, porque qualquer pessoa pode decifrar a mensagem com a chave pública de Maria. Isso quer dizer que a criptografia assimétrica só garante confidencialidade ou autenticação? Ainda bem que não! Ela pode garantir as duas coisas!

Figura 02 - Autenticação com criptografia.



Para garantir confidencialidade e autenticação, dois passos de criptografia devem ser aplicados, conforme mostrado na Figura 3.

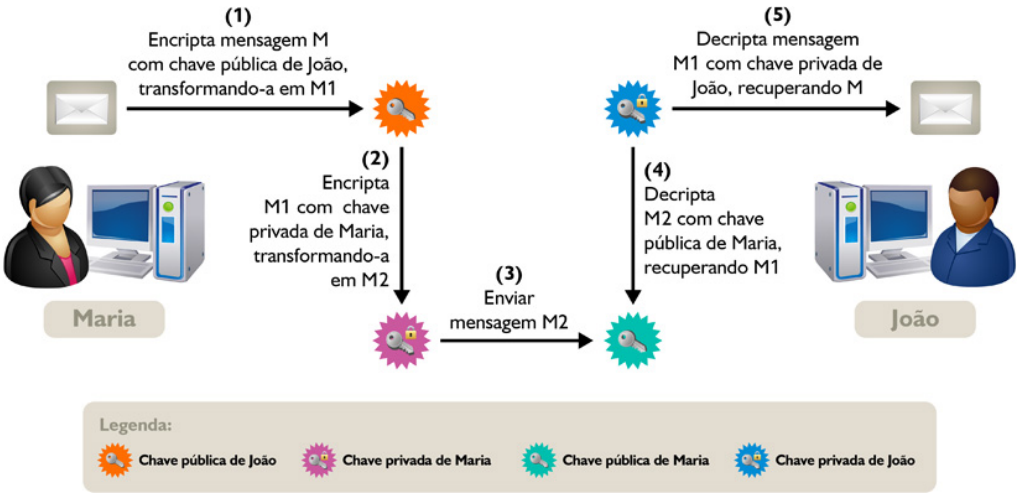
Passo 1 (confidencialidade): Maria cifra a mensagem M com a chave pública de João. Somente João conseguirá decifrá-la! Vamos chamar essa mensagem cifrada de M1.

Passo 2 (autenticação): Maria cifra novamente a mensagem M1 com sua chave privada, de forma a garantir a autenticidade. Vamos chamar essa mensagem de M2. Ela é que será enviada para João.

Passo 3: João decifra M2 usando a chave pública de Maria, obtendo novamente M1 e garantindo autenticação.

Passo 4: João decifra M1 usando sua chave privada, obtendo novamente M e garantindo a confidencialidade.

Figura 03 - Confidencialidade e autenticação com criptografia.



Vídeo 03 - Autenticação Assimétrica

Atividade 03

1. Você entendeu por que são necessários dois passos para se garantir confidencialidade e autenticação? Explique!

Autenticação com Código MAC

O código MAC (*Message Authentication Code*), ou código de autenticação da mensagem, é gerado através de criptografia simétrica. Usando-se uma chave secreta, compartilhada entre as entidades comunicantes:

1. A origem da mensagem gera um bloco de dados pequeno e de tamanho fixo, o qual chamaremos de "*MAC_origem*", que é anexado à mensagem. Transmite-se a mensagem junto com o código *"MAC_origem"*, para ser validado no destino.

2. O destino da mensagem usa a chave secreta que ele compartilha com o da origem e gera novamente o MAC, agora chamado de "*MAC_destino*" e o compara com o "*MAC_origem*", que foi recebido junto com a mensagem.

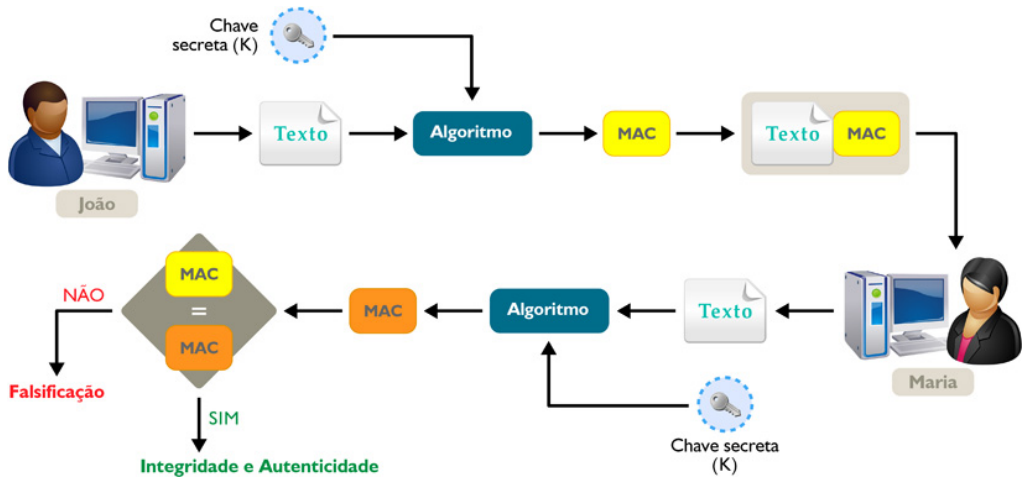
Se forem iguais, a autenticação é realizada! Além da autenticação, essa estratégia também garante integridade porque, se o MAC obtido foi o mesmo, isso significa que a mensagem não foi alterada, está íntegra, já que a mensagem é um dos parâmetros do cálculo do MAC. Legal, hein? Duas funções de segurança em um único mecanismo!

Podemos expressar essa função da seguinte forma:

MAC = Encriptação(M,K), onde M = Mensagem e K = chave secreta

Veja a ilustração na Figura 4. João e Maria têm uma chave secreta (K) compartilhada. Para autenticar o texto enviado, João usa um algoritmo de criptografia simétrica e gera o código MAC. Esse código é enviado para Maria junto com o texto. Quando Maria recebe, ela recupera o texto e aplica, sobre ele, o mesmo algoritmo para gerar o MAC. Depois compara o MAC gerado com o MAC recebido. Se forem iguais, a mensagem não foi alterada e ela tem certeza que foi enviada por João. Caso contrário, houve alguma falsificação. Ou seja, a mensagem foi adulterada e deve ser descartada.

Figura 04 - Autenticação com código MAC.



Observe que esse processo garante integridade e autenticação, mas **não garante confidencialidade**, uma vez que a mensagem é enviada sem estar criptografada. Todos podem ver a mensagem, mas não podem alterá-la! Isso é útil em aplicações que não têm interesse em manter mensagens em segredo, mas

quando o importante é autenticar a mensagem. Por exemplo, em aplicações com muito processamento e que exigem apenas autenticação, usar função MAC é mais econômico que cifrar/decifrar toda a mensagem.

> O código MAC **não é uma assinatura digital** porque tanto o receptor quanto o emissor da mensagem compartilham a mesma chave secreta.

Um algoritmo muito usado para calcular o MAC é uma variante do DES (*Data Encription Standard*). Uma importante diferença entre a geração de MAC e a criptografia diz respeito às funções de MAC, que são irreversíveis, ou seja, a partir do MAC não há nenhuma forma de se obter o texto original.

Atividade 04

1. Você viu que o MAC provê integridade e autenticidade. Dada uma mensagem com o MAC associado, o que você faria para adicionar também confidencialidade?

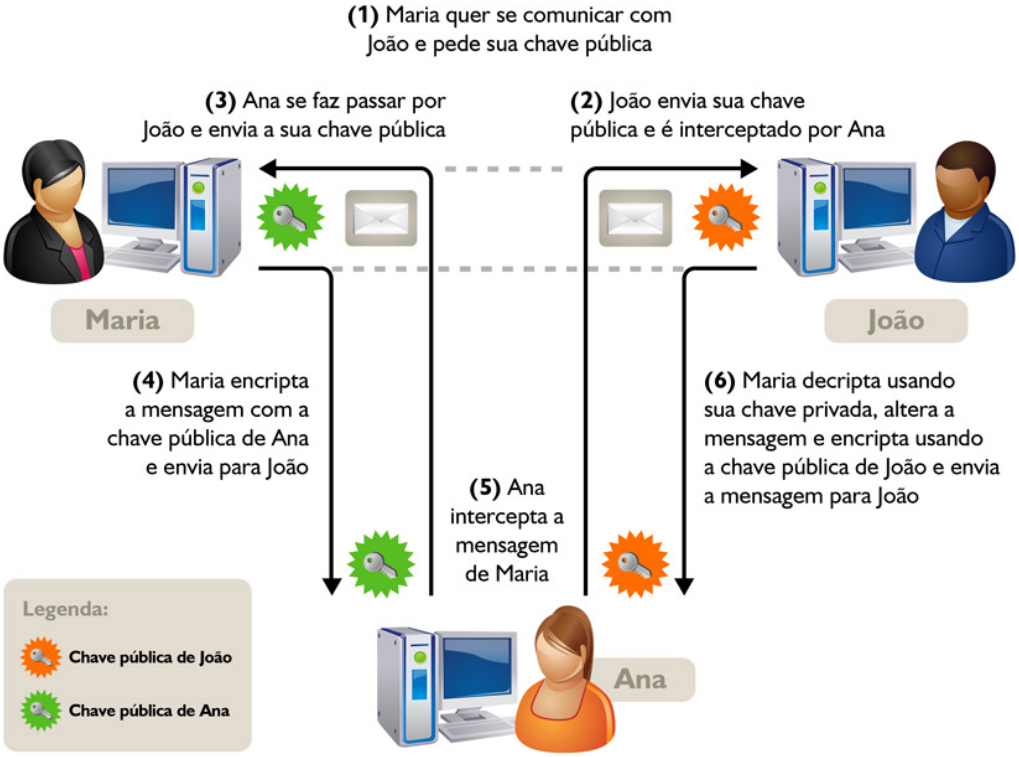
Autenticação com Arbitragem

Um dos potenciais problemas com a autenticação é conhecido como o ataque “homem-no-meio” ou *(man-in-the-middle)*, em que há um elemento no meio da comunicação interceptando mensagens e fazendo-se passar por outra pessoa.

Suponha que Maria deseja se comunicar com João, e Ana deseja interceptar essa conversação, possivelmente para enviar mensagens falsas. Primeiramente, Maria pergunta a João qual a sua chave pública. Quando João responde, Ana intercepta a resposta e então começa o ataque “homem-no-meio”. Ana envia uma mensagem a Maria, passando-se por João, incluindo a sua chave pública (de Ana). Maria acredita que é a chave pública de João e cifra mensagens com a chave pública de Ana, enviando as mensagens cifradas para João. Ana intercepta novamente as

mensagens, decifra usando sua chave privada, altera a mensagem, e as cifra novamente usando a chave pública de João. Quando João recebe a mensagem, ele acredita que veio de Maria. Essa sequência está ilustrada na Figura 5.

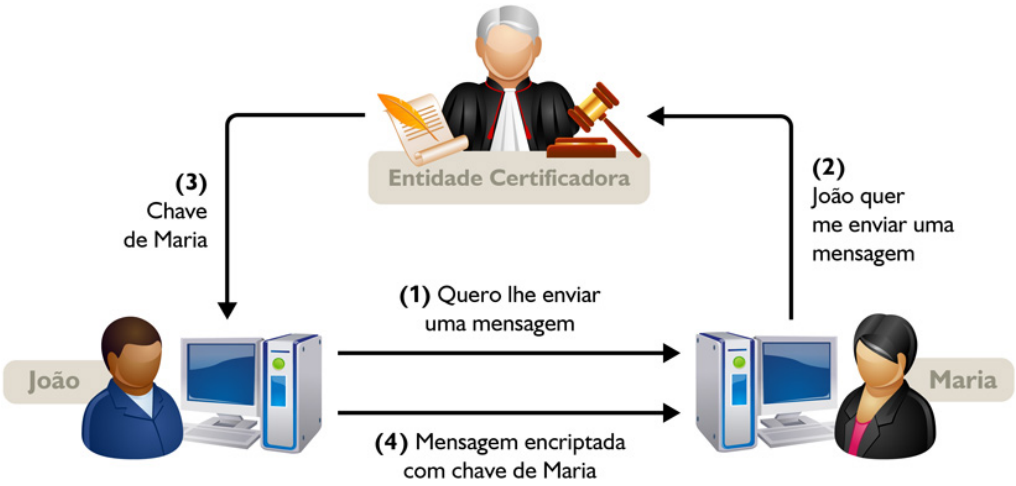
Figura 05 - Ataque homem-no-meio.



Existem algumas maneiras de se evitar esse tipo de ataque. Uma delas é o uso de um árbitro, um juiz que é intermediário no processo de distribuição de chaves. Esse tipo de autenticação se chama autenticação arbitrada. Na Aula 6, você verá detalhes sobre as Autoridades Certificadoras, que têm esse papel de distribuir chaves em certificados digitais. A Figura 6 ilustra um exemplo simples de autenticação arbitrada.

Nesse tipo de autenticação, o árbitro, denominado de Entidade Certificadora, é um intermediário da comunicação que distribui as chaves. Então, se João quer enviar uma mensagem a Maria, ele avisa a Maria que vai enviar uma mensagem. Maria, por sua vez, comunica isso à entidade certificadora. A entidade certificadora envia a chave para comunicação entre João e Maria. De posse dessa chave, João cifra a mensagem e envia a Maria. Nesse caso, a mensagem tem confidencialidade – somente Maria pode decifrá-la e Maria sabe que foi João quem enviou porque a entidade certificadora concedeu a chave para comunicação entre João e Maria.

Figura 06 - Autenticação arbitrada.



Vídeo 04 - Autenticação com Arbitro

Leitura Complementar

<http://pt.wikipedia.org/wiki/Autenticação>

Nesse site, você encontrará vários detalhes e links sobre autenticação. Vale a pena conferir!

Atividade 05

Pesquisa

Você já ouviu falar em autenticação usando *smart cards*?

Pesquise e escreva um texto explicando como funciona esse tipo de autenticação!

Resumo

Nesta aula, você viu que o objetivo da autenticação é proteger as duas partes que trocam uma mensagem. Você estudou diferentes tipos de autenticação e como eles são realizados. E também aprendeu um pouco sobre as principais vulnerabilidades de cada um dos tipos de autenticação.

Autoavaliação

1. A autenticação sempre garante integridade? Justifique.
2. Quais as situações em que a autenticação baseada em senha é indicada?
3. A autenticação por código MAC usa que tipo de criptografia?
4. Descreva o que é o ataque *man-in-the-middle*?

5. O código MAC garante o não repúdio? Justifique.

Referências

NAKAMURA, E.; GEUS, P. L. **Segurança em redes em ambientes cooperativos**. Rio de Janeiro. : Editora Novatec, 2007.

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