Segurança em Redes

Aula 05 - Assinatura Digital

Apresentação

Nesta aula você vai estudar, mais detalhadamente, como é realizada a assinatura digital e quais as funções de segurança que são garantidas com o uso de assinatura digital.

Vídeo 01 - Apresentação

Objetivos

Ao final desta aula, você será capaz de:

- Descrever como é realizada a assinatura digital.
- Diferenciar assinatura digital de assinatura eletrônica.
- Conhecer os benefícios de segurança proporcionados pela assinatura digital.

Conceito de Assinatura Digital

Na Aula 4, você aprendeu que a autenticação não protege as duas partes uma contra a outra. Por exemplo, pode acontecer que:

1. Alguém consiga forjar uma mensagem e diga que foi enviada por outra pessoa.
2. Alguém negue o envio de uma mensagem, dizendo que ela foi forjada. Esse problema é resolvido pela assinatura digital!

A assinatura digital é um conjunto de *bits* calculado em função da mensagem sendo assinada. Ela identifica o seu autor e pode ser verificada por terceiros. Devemos ter cuidado com o termo assinatura eletrônica que, muitas vezes, é confundido com assinatura digital, mas tem um significado diferente. A assinatura eletrônica refere-se a qualquer mecanismo, não necessariamente criptográfico, para identificar o remetente de uma mensagem eletrônica.

Você lembra que na aula passada comentamos que o código MAC **não provê assinatura digital?** Lembram por quê? Porque com o código MAC tanto o receptor quanto o emissor da mensagem compartilham a mesma chave secreta, então, a mensagem pode ser enviada por qualquer um dos dois. A assinatura digital deve identificar, univocamente, um usuário. Portanto, as estratégias para assinatura digital baseiam-se, tipicamente, em criptografia assimétrica ou de chave pública. Mais uma vez, a criptografia é base de outros mecanismos de segurança!

Vale ressaltar que, na área de segurança, assim como na computação, os métodos e tecnologias evoluem constantemente. Portanto, novos métodos de assinatura digital, novos algoritmos de criptografia surgem no decorrer dos anos.

Vídeo 02 - Assinatura Digital

Mecanismo de Funcionamento da Assinatura Digital

O mecanismo de funcionamento típico da assinatura digital consiste em dois passos que serão estudados a seguir, detalhadamente. Ambos fazem uso da criptografia:

1. Cálculo do *hash* (resumo da mensagem).
2. Encriptação do *hash*.

Cálculo do *Hash*

Uma função *hash* aceita uma mensagem *"M"*, de tamanho qualquer, como entrada, e produz um código *hash* de tamanho fixo. O código *hash* "*H(M)"* é também chamado de *message digest*. O funcionamento básico de uma função *hash* é mostrada na Figura 1.

Figura 01 - Função *hash*

As propriedades fundamentais de uma função *hash* qualquer são:

1. Deve ser uma função não reversível (*one-way*), ou seja, dado o código *hash* de uma mensagem, "*H(M)"*, deve ser impossível achar a mensagem original *"M"* que o gerou. Ou seja, dada a saída, não é possível obter a entrada.

1. Deve ser computacionalmente inviável encontrar duas mensagens diferentes *"(M1, M2)"* com o mesmo código *hash "H(M1) = H(M2)"*. Por exemplo, em uma função *hash* que produza 128 *bits* de saída, seria necessário tentar 2128 mensagens diferentes para encontrar dois *hashs* iguais.

Além disso, é importante perceber que:

1. Como a função *hash* considera, em seu cálculo, todos os *bits* da mensagem de entrada *"M"*, a mudança em apenas um dos seus *bits* produz um código *hash* totalmente diferente.
2. Como a função *hash* não é secreta, alguma forma de proteção para o seu valor é necessária.
3. Funções *hash* não garantem autenticação nem confiabilidade, apenas integridade.

Alguns exemplos de algoritmos que, atualmente, são utilizados na prática para o cálculo de *hashs* são: MD4, MD5, SHA-1 etc. Uma grande vantagem das funções *hash* é o tempo de execução do algoritmo. São bem mais rápidos do que os algoritmos simétricos, por exemplo. Quando se aplica uma função *hash*, está se gerando uma espécie de "impressão digital" do conteúdo da mensagem, o que permite verificar sua integridade.

Vídeo 03 - Cálculo do Hash

Curiosidade

Devido ao seu conjunto de propriedades, outro uso bastante comum das funções *hash* é para o armazenamento de senhas. Quando um usuário tenta fazer *login* em um sistema, é gerado um *hash* da senha digitada e comparado com um previamente armazenado, quando o usuário criou a senha. Caso sejam iguais, o *login* é autorizado.

Atividade 01

1. Quais são as características fundamentais para uma função ser considerada hash?

Encriptação do Código *hash*

Após a geração do código *hash*, o próximo passo da assinatura digital é a encriptação desse código usando criptografia assimétrica.

Nesse caso, o *hash* deve ser encriptado usando a chave privada do emissor. Por exemplo, a Figura 2 mostra a geração de uma mensagem com assinatura digital por João para envio a Maria. Dada a mensagem *"M"* e seu código *hash "H(M)"* correspondente, esse código é criptografado usando-se a chave privada de João. O texto, junto com o *hash* encriptado, é enviado ao destino.

No destino a assinatura pode ser verificada com os passos seguintes:

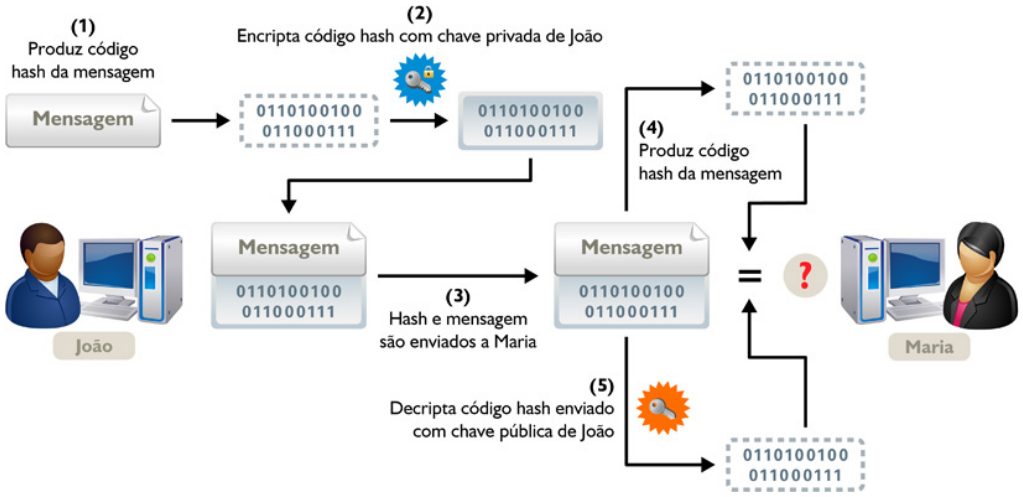
1. O *hash* recebido é decriptado, usando-se, para tanto, a chave pública de João. Obtém-se, então, o *hash "H1"* que foi gerado na origem da mensagem;

2. Também se deve calcular novamente o *hash* a partir da mensagem recebida *"H(M) = H2"*. Daí compara-se os dois. Se o *hash "H1"* (que foi obtido a partir da decriptação) for igual a *"H2"* (calculado pelo receptor), então, a mensagem está íntegra, ou seja, não foi modificada. Também podemos garantir que a mensagem foi enviada realmente por João (integridade e autenticação).

Isso é muito importante, porque significa que nada foi modificado na mensagem, depois de assinada. Portanto, a assinatura digital usando recursos criptográficos garante tanto autenticidade quanto integridade.

Vale ressaltar que todo esse processo é feito de forma automática pelo *software* de assinatura digital, que também faz a verificação.

Figura 02 - Geração de Assinatura Digital.



Atividade 02

1. Quais princípios fundamentais da segurança de sistemas computacionais são garantidos com o uso de assinatura digital? Por quê?

Assinatura Digital no Brasil

No Brasil, a criação da ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira), pela medida provisória 2.200-2/2001, foi um marco para a adoção de assinatura digital em documentos oficiais. Desde então, a substituição de documentos físicos pelos correspondentes documentos eletrônicos vem crescendo. Por exemplo, a lei 11.419, de dezembro de 2006, trata da informatização do processo judicial. Um documento assinado digitalmente tem que ter um certificado emitido por uma autoridade certificadora credenciada à ICP-Brasil. Você vai conhecer mais detalhes sobre como funciona a ICP-Brasil na próxima aula, sobre Certificados Digitais. A Figura 3 mostra o RIC, novo documento que irá substituir nossa identidade, CPF, título de eleitor, carteira de motorista etc. e possui uma assinatura digital.

Figura 03 - RIC – Registro de Identidade Civil.

Fonte: http://www.dnt.adv.br/noticias/publicado-o-decreto-que-regulamenta-o-registro-de-identidade-civil-ric/ Acesso em: 29 ago. 2012.

Vídeo 04 - Garantindo a Integridade

Leitura Complementar

Saiba mais sobre assinatura digital:

https://www.tecmundo.com.br/web/941-o-que-e-assinatura-digital-.htm

Atividade 03

Agora pesquise

1. Você sabia que a assinatura digital pode ser utilizada juntamente com o serviço de e-mail, para evitar diversos problemas de segurança como o phising? Pesquise sobre PGP.

Resumo

Nesta aula você aprendeu que o objetivo da assinatura digital é garantir o não repúdio, ou seja, é impossível para um remetente negar a autoria de uma mensagem. Viu também que juntamente com o não repúdio também se garante a integridade da mensagem, assim como sua autenticação. E você aprendeu que **não** é objetivo da assinatura digital garantir confidencialidade da mensagem. Você aprendeu que o mecanismo mais usado para gerar uma assinatura digital utiliza funções *hash* juntamente com criptografia assimétrica. Por fim, vimos que a assinatura digital está cada vez mais sendo usada no setor público do Brasil, onde os documentos governamentais estão, cada vez mais, utilizando assinatura digital.

Autoavaliação

1. Qual serviço de segurança a assinatura digital não garante?
2. Por que as funções hash são chamadas de one-way?

3. Assinale com V ou F, V para verdadeiro ou F para falso:
   ( ) A assinatura digital garante integridade.
   ( ) O código hash é criptografado com a chave pública do usuário que envia uma mensagem assinada.
   ( ) O uso da criptografia assimétrica é obrigatória na assinatura digital.
   ( ) Ao receber um documento com assinatura digital, o destinatário, primeiramente, encripta seu código hash.

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.