Criptografia MIECOM — 2006/2007

mbb @ di.uminho.pt 15 de Junho de 2007

1. Indique se considera cada uma das seguintes afirmações verdadeira (V) ou falsa (F). Justifique as suas respostas.

(a) Tipicamente, a complexidade computacional das cifras simétricas é várias ordens de grandeza superior á das cifras assimétricas, quando oferecem o mesmo nível de segurança. **F**
Justificação:
A complexidade computacional das cifras simétricas é inferior às cifras assimétricas, quando oferecem o mesmo nível de segurança, porque as últimas para comunicarem entre dois agentes é necessário dois pares (uma chave pública e uma privada), um por cada agente. A chave pública serve para codificar os dados e a chave privada descodifica.

(b) As chaves de sessão são utilizadas por peŕiodos de tempo muito curtos. **V**
Justificação:
As chaves de sessão são utilizadas por curtos períodos de tempo, pois chave só dura enquanto uma determinada comunicação estiver estabelecida.

(c) Os pares de chaves pública/privada associados aos algoritmos de cifra assimétrica são geralmente utilizados como chaves de sessão. **F**
Justificação:
As chaves de sessão quando associadas ao algoritmo de cifra assimétrica a chave da sessão é cifrada através da chave pública e decifrada através da chave privada.

(d) É comum a utilização de algoritmos de cifra simétrica num regime de partilha da mesma chave por mais do que dois agentes, por forma a reduzir o número total de chaves a gerir. **V**
Justificação:
As cifras simétricas usam a mesma chave para cifrar e decifrar informação, desta maneira redusse o número de chaves a gerir.

(e) Associado à utilização de algoritmos de cifra assimétrica está, geralmente, um esquema de certificação das chaves privadas dos agentes envolvidos. **F**
Justificação:
Esta afirmação é falsa porque as chaves privadas só são conhecidas pelo titular das mesmas.

(f) A certificação de chaves públicas não faz sentido sem que se estabeleça um *agente de confiança* aceite por todas as partes, uma vez que é este agente que fica encarregado da geração e gestão dessas mesmas chaves. **F**
Justificação:
Para certificados de chaves públicas não necessário existir um agente de confiança, pois estes tem um par de chaves (uma para cifrar outra para decifrar) e ainda tem uma autoridade de certificação que autentica o certificado. No entanto esta não consegue as chaves do dito certificado.

2. Recorde o que estudou sobre funções de Hash criptográficas e Message Authentication Codes (MACs).

(a) Porque é que um simples *checksum*, não pode ser utilizado como função de Hash criptográfica?
Resposta:
Uma função de Hash caracteriza-se por não criar colisões, cada mensagem passada numa função de hash gera um valor diferente. Também têm a particularidade que o valor de hash gerado funciona como uma impressão digital da mensagem invertível. Enquanto que no checksum a maior probabilidade de existir colisões é maior e é quase impossível associar o valor do checksum à mensagem.

(b) Explique as diferenças entre uma função de Hash criptográfica e um MAC, quer em termos de funcionamento, quer em termos de garantias fornecidas.
Resposta:
Um Mac usa uma chave secreta partilhada entre A e B, juntamente com a mensagem forma um valor, que só pode ser reproduzido por quem conhece o algoritmo e a chave, desta forma garante a integridade da mensagem. Uma função de Hash é um processo unidirecional que torna a mensagem num valor de Hash de tamanho fixo e muito menor que o da mensagem. O valor formando funciona com uma impressão digital da mensagem, pois é muito difícil duas mensagens formarem o mesmo valor de Hash .

3. Considere os Certificados de Chave Pública X.509:

(a) Comente a seguinte afirmação: "Nem todos os certificados de chave pública X.509 podem ser trocados livremente em canal aberto".

Resposta:

Os certificados da chave pública X.509 podem ser trocados livremente em canal aberto desde que haja confiança na autoridade de certicação (CA), isto é, encontrar um CA que autentique o certificado recebido e que se autentique a ela mesmo, as chamadas RA. Por vezes este processo leva a uma cadeia de autenticação de certificados.

(b) Descreva os passos necessários ao envio de uma mensagem com requisitos de confidencialidade com base em certificados de chave pública.

Resposta:

1. O emissor verifica que a identidade indicada pelo destinatário está de acordo com a identidade indicada no certificado.
2. O emissor valida o certificado e a identidade do destinatário;
    a. Que a assinatura do certificado é válida;
    b. Que foi efetuada por uma autoridade de certificação de confiança;
    c. Que o certificado está dentro do seu período de validade.
3. O emissor utiliza a chave pública contida no certificado para cifrar a informação;
4. O emissor envia a informação cifrada ao destinatário que a decifra com a sua chave privada.

(c) Em que circunstâncias deve um certificado ser revogado? Descreva o mecanismo previsto na PKI para efectuar esta operação.

Resposta:

Nesta circunstancias:

- chave privada comprometida;
- segurança da CA comprometida;
- alteração de filiação ou de privilégios;
- existência de uma versão mais recente do certificado;
- fim da operação da CA.

O processo revogação é realizado através de CRL's (Certificate Revocation Lists), enviadas pela Autoridade de Certificação periodicamente. Contêm uma lista dos certificados revogados dentro do período de validade. Tem também a data da emissão dessa CRL's e data da próxima CRL's a ser emitida. Desta forma garante-se que um certificado não seja usado depois de anulado.

4. No estabelecimento de uma sessão SSL são trocados certificados de chave pública.

(a) Descreva e justifique as propriedades destes certificados que são necessárias para que, numa ligação HTTPS típica, um *browser* consiga estabelecer a conexão com um servidor *web* sem a intervenção do utilizador.

Resposta:

- Caso seja utilizada autenticação do Servidor, este envia o seu certificado X.509 ao Cliente, que o valida. Além da validação habitual, o Cliente assegura-se de que o nome de domínio do Servidor, indicado no certificado, está correto;
- Parâmetros do Servidor específicos para acordo de chaves são enviados nesta fase (**Server Key Exchange**);
- Caso o Servidor autentique o Cliente, solicita o certificado correspondente (**Certificate Request**). Este pedido inclui um desafio para ser utilizado na autenticação do cliente.
- O Servidor termina esta fase da negociação enviando uma mensagem **Server Hello Done**.
- Conjuntamente com o certificado o Cliente tem de enviar uma assinatura digital do desafio que recebeu, comprovando assim a posse da chave privada associada ao certificado.
- Finalmente, o Cliente envia os seus parâmetros para acordo de chaves (**Client Key Exchange**), altera o seu estado de sessão, e envia uma primeira mensagem cifrada que indica o seu estado de prontidão (**finished**).
- O Servidor efectua o mesmo procedimento e a negociação termina tendo sido acordado o Master Secret da sessão.

(b) Pode um intruso ser bem sucedido se interceptar um desses certificados, fazendo-se passar mais tarde pela entidade associada? Justifique.

Resposta:

Um intruso podia editar as mensagens de hello trocadas entre Cliente e Servidor de forma a que ambos pensassem que o outro apenas conseguia funcionar com um nível de segurança reduzido. O resto da negociação decorria sem alterações e estabelecia-se uma ligação com um nível de segurança reduzido, mais vulnerável a ataques por parte do intruso. Este ataque era possível porque as mensagens de handshake não eram autenticadas!