INE5630 – Solução da Prova 2 – 21/11/2011

1. Embora navegadores Web sejam fáceis de usar, os servidores Web sejam relativamente fáceis de configurar e gerenciar, e o conteúdo da Web esteja cada vez mais fácil de se desenvolver, o software que dá suporte a tudo isso é extraordinariamente complexo. Esse software complexo pode ocultar muitas vulnerabilidades/falhas de segurança em potencial. A história da Web está repleta de exemplos de sistemas novos e atualizados, devidamente instalados, que são vulneráveis a uma série de ameaças/ataques à segurança (é só aplicar um analisador de vulnerabilidades num site conhecido, que as vulnerabilidades serão avisadas).

2. (Verdade/Falso) Quando um servidor Web está comprometido por algum ataque, um invasor pode ser capaz de obter acesso a dados ou sistemas que não fazem parte da Web, e que estão em máquinas conectadas localmente ao servidor Web. (Muitas vezes máquinas são comprometidas com ataques para o invasor poder chegar em outra máquina de interesse).

3. (Verdade/Falso) Os usuários não treinados em questões de segurança são clientes comuns de serviços na Web. Esses usuários (não) estão necessariamente cientes dos riscos de segurança e não possuem as ferramentas ou conhecimento para tomar contramedidas eficazes. (Muitas vezes são enganados por links constituindo ameaças que lhes são apresentados).

4. (Verdade/Falso) **Ataques passivos** incluem acesso não autorizado ao tráfego de rede entre o navegador e o servidor Web. (Constituindo uma escuta no meio de comunicação, sem que a mensagem seja adulterada). **Ataques ativos** incluem a simulação de outro usuário, a alteração de mensagens em trânsito entre cliente e servidor, e alteração de informações em um site Web.

5. (Verdade/Falso) Uma maneira de classificar ameaças de segurança na Web é em termos do local da ameaça: servidor web, navegador web ou no tráfego de rede entre navegador e servidor. As questões de segurança de servidor e navegador entram na categoria de segurança de rede (segurança de sistemas/aplicações) . As questões de segurança no tráfego entre servidor e navegador entram na categoria segurança de sistemas (segurança de redes).

6. (Verdade/Falso) A obtenção proposital de informações sobre a versão de um servidor Web é uma ameaça.

7. (Verdade/Falso) A obtenção proposital de informações sobre a versão de um servidor Web é um ataque (é uma ameaça).

8. (Verdade/Falso) A falsificação dos dados de autenticação de clientes de um servidor Web é uma ameaça à autenticação que pode ser evitada através do certificado do servidor (certificado do cliente).

9. (Verdade/Falso) A simulação de um site Web legítimo por um site falso é um ataque (mas pode ser uma ameaça, se o site foi simulado e o ataque em si não se concretizou com os dados dos clientes perante o site verdadeiro) que tem como conseqüência atingir ou alguém se beneficiar da: ( ) **Integridade** sobre a modificação de dados do usuário legítimo, por um navegador que apresenta um cavalo-de-tróia. (**X**) **Confidencialidade** de informações, sobre qual cliente se comunica com o servidor. ( ) Negação de um serviço verdadeiro por isolamento de uma máquina por ataque de DNS. (**X**) Autenticação por falsificação de dados do cliente. A contagem do valor da questão será considerada para as duas respostas (verdade/falso), considerando que o texto não mencionou claramente as condições de ameaça ou ataque. Sua nota poderá ser alterada se o valor não foi considerado.

10. (Verdade/Falso) Sobre a arquitetura em camadas do SSL: O protocolo SSL foi projetado para utilizar o protocolo TCP para oferecer um serviço seguro, confiável, entre um navegador e um servidor Web. Em particular, o protocolo HTTP oferece o serviço de interação cliente/servidor Web pode operar sobre o protocolo SSL, para se utilizar um serviço seguro.

11. (Verdade/Falso) O SSL (Secure Socket Layer) utiliza criptografia simétrica com cifra de bloco e os seguintes algoritmos podem ser usados: AES (128/256), IDEA (128), RC2 (40), DES (40/56), 3DES (168) ou Fortezza (80). Mas, o SSL, pode também usar criptografia com cifra de fluxo com o algoritmo RC4 (40/128). (RC4 é cifra de fluxo e é mais rápida do que cifra de bloco). O SSL v3 é a versão mais usada. O SSL v3.1 é o chamado TLS (Transport Layer Security).

12. (Verdade/Falso) No SSL, o protocolo de estabelecimento de sessão é usado antes que quaisquer dados da aplicação sejam transmitidos. Esse protocolo permite que servidor

e cliente se autentiquem um ao outro e negociem um algoritmo de criptografia e de MAC e chaves criptográficas a serem usadas para proteger dados enviados pelo protocolo de registro SSL. No estabelecimento da sessão, ocorre a negociação do método do acordo de chave secreta a ser compartilhada (ou seja, o meio pelo qual resulta em uma chave secreta fixa entre duas partes para a criptografia e MAC). Os métodos admitidos são os baseados em Diffie-Hellman e do RSA. A criptografia de chave pública RSA é usada no SSL, apenas como método de proteção da chave secreta compartilhada, quando esta é trocada. Neste caso, o servidor cria um par temporário de chaves pública/privada RSA e usa uma mensagem do próprio protocolo de sessão para enviar a sua chave pública para o cliente. Então, o cliente pode agora utilizar a chave pública do servidor para criptografar a chave secreta compartilhada, enviar essa chave secreta, e o servidor poderá abrir a chave secreta com sua chave privada.

13. Um código de autenticação de mensagem (MAC – Message Authentication Code) é uma técnica de assinatura de baixo custo, que autentica a comunicação entre duas partes A e B, com base em uma chave K, que é um segredo compartilhado. A gera uma chave aleatória K para usar e a distribui usando alguma forma segura para uma ou mais partes que autenticarão as mensagens recebidas de A. A única vantagem desta técnica é o seu desempenho em relação ao método de assinatura com chave pública, pois a técnica não envolve nenhuma criptografia, a não ser o uso de uma função Hash sobre a concatenação de uma mensagem M e uma chave K. Ao invés de se utilizar essa técnica para assinar mensagens, melhor é utilizá-la para verificar a integridade de mensagens transmitidas entre A e B. (A concatenação de ***M*** e ***K*** evita que ao ser ***M*** e o ***h(M)*** = ***h*** transmitidos, se um invasor puder capturar e alterar ***M***, ele possa capturar e alterar o resumo ***h,*** também. Isso é verdade, mas há duas maneiras de evitar isso: (1) uma é utilizar um HMAC (Hash Message Authentication Code) que usa uma chave-resumo, ou seja um resumo baseado numa chave. O que pode ser visto na questão 14. (2) A outra maneira de evitar isso é utilizar uma assinatura digital, Normalmente os HMACs são utilizados apenas para verificação da integridade de M, ou seja, se o conteúdo de M não foi alterado durante o trânsito. Um HMAC faz uma verificação instantânea de M e não se destina a ser um registro permanente relativo à M. Por essa razão, você precisa de uma outra maneira de criar assinaturas verificáveis e essa única maneira é cifrar o resumo h com a chave privada do assinante, como é no RSA ou no DSA).

14. (Verdade/Falso) Não existe nenhum motivo técnico pelo qual um algoritmo de criptografia de chave simétrica (chave secreta) não possa ser usado para gerar uma assinatura digital, mas para verificar tais assinaturas, a chave secreta precisa ser repassada. E isso pode causar alguns problemas. A exposição de uma chave secreta usada para assinar é indesejável. Por alguns motivos (*), o método de chave pública para geração e verificação de assinaturas oferece a solução mais conveniente na maioria das situações.

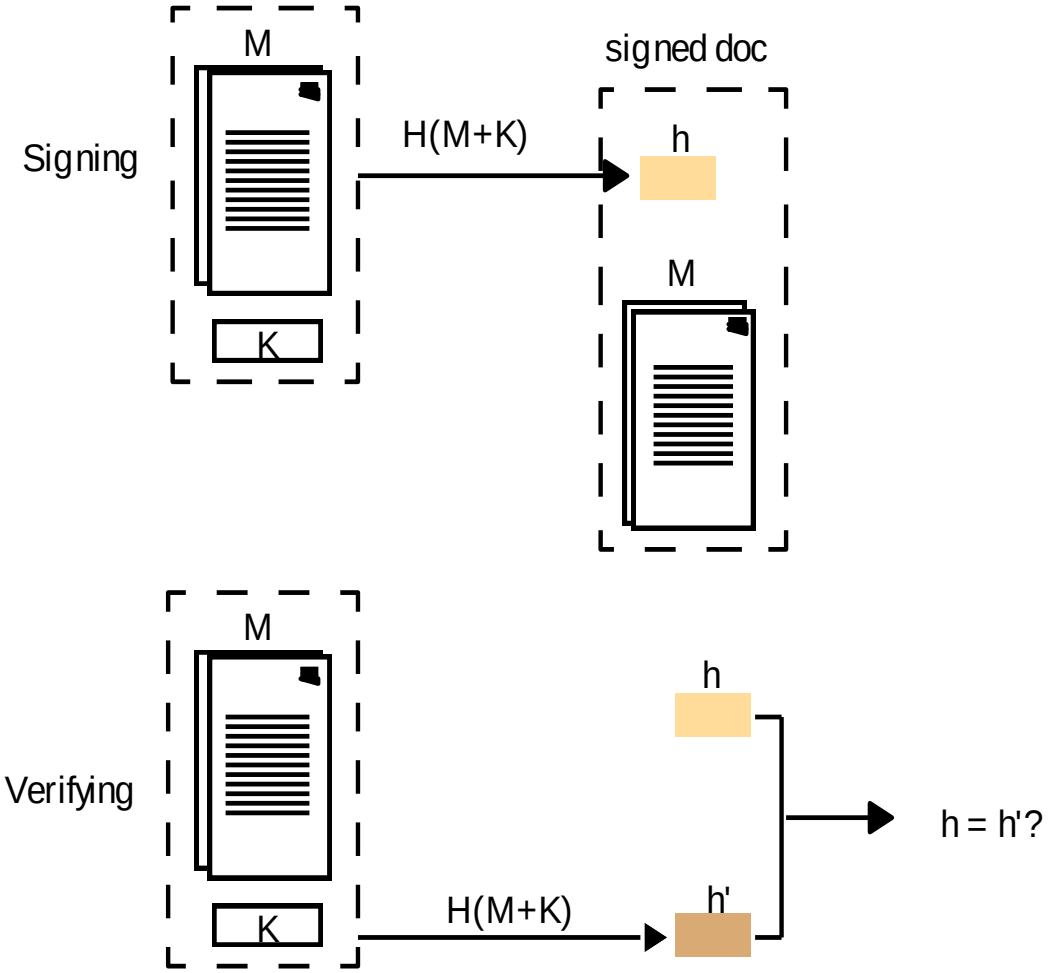
    (*) (a) Quem assina deve preparar para o verificador receber a chave secreta, usada para assinatura, com segurança. (b) Talvez precise verificar uma assinatura em vários contextos e em diferentes momentos e no momento da assinatura, quem assina pode não saber a identidade de quem irá verificar a assinatura. Para resolver isso, a verificação pode ser delegada a um terceiro confiável que possua as chaves secretas de todos os signatários, mais isso aumenta a complexidade do modelo de segurança e exige uma comunicação segura com o terceiro confiável. E um problema estrutural em usar criptografia de chave secreta para assinaturas digitais é que todo mundo tem que confiar no "terceiro confiável", pois este lê todas as mensagens assinadas. Os candidatos mais lógicos para ser esse terceiro confiável podem ser governo, bancos ou por exemplo, uma ordem de advogados. Porém essas organizações não inspiram total confiança de todos os cidadãos. (c) A exposição da chave secreta usada para assinar é indesejável, pois isso enfraquece a segurança das assinaturas feitas com essa chave, porque uma assinatura poderia ser falsificada por um possuidor da chave que não seja o proprietário dela. Por estes motivos, o método de chave pública para geração e verificação de assinaturas oferece a solução mais conveniente na maioria das situações.

    Um exceção surge quando um **canal seguro é usado para transmitir mensagens não cifradas**, **mas com a necessidade de verificar a autenticidade das mensagens**. Este é o caso chamado de **códigos de autenticação de mensagem** – MAC (**Message Authentication Code**) para termos uma solução para tal exceção com propósito mais limitado. Um MAC autentica a comunicação entre pares com base em um segredo compartilhado que é uma chave. Note que no método MAC não existe criptografia, a não ser uma Função Hash que é usada para fazer o hash de uma mensagem M concatenada com uma chave K. Códigos MAC autenticam a comunicação entre pares, com base em um segredo compartilhado que é uma chave.

Mas, os custos de processamento da criptografia de chave pública são altos demais até para cifrar mensagens de tamanho médio, normalmente encontradas no comércio eletrônico. **A solução adotada é usar um esquema de criptografia misto**, no qual a **criptografia de chave pública é usada para autenticar as partes e para cifrar a troca de chaves secretas**, as quais são usadas para toda a comunicação subseqüente. Lembre do que foi explicado sobre o envelope digital, que junta a criptografia de chave pública para criptografar chaves de sessão e a criptografia simétrica para cifrar a informação transmitida.

Uma técnica de **assinatura de baixo custo**, **baseada em uma chave secreta compartilhada**, que tem segurança adequada para muitos propósitos é que segue:

1. **A** gera uma chave aleatória ***K*** e a **distribui usando canais seguros** para uma ou mais entidades, que precisam autenticar (verificar a integridade) mensagens recebidas de A.
2. Para qualquer documento ***M*** que **A** deseje enviar, **A** concatena ***M*** com ***K***, computa o resumo (digest) ***h = H(M+K)*** , enviando o documento assinado **[** ***M*** **]**$_k$ ***= M, h*** para uma entidade **B** desejando verificar os dados ***M***. O resumo ***h*** é um **MAC** (representa ***M+K***). O resumo ***h*** depende da mensagem ***M*** e da chave **k** e dessa forma um invasor teria de saber o que a chave ***K*** é para alterar a mensagem ***M***. A chave ***K*** não será comprometida pela revelação de ***h***, visto que a função ***h*** oculta o seu valor totalmente.
3. O receptor **B** recebe o documento **[** ***M*** **]**$_k$ ***= M, h***, concatena a chave secreta compartilhada ***K*** recebida, **cifrada pela chave pública do receptor B** (**o método depende da existência de um canal seguro pelo qual a chave *K* compartilhada possa ser distribuída**), decifra esta com sua chave privada, *e* com o documento ***M recebido*** e computa o resumo ***h' = h(M+K)***. A integridade de ***M*** é verificada se ***h = h'***. A figura abaixo mostra o método para assinaturas de baixo custo com uma chave secreta compartilhada.



15. Escolhendo o certificado digital: O primeiro passo para a escolha de um certificado é saber exatamente qual vai ser a aplicação do certificado. Com a utilização de um certificado de servidor, o cliente de uma loja virtual pode verificar se o site para o qual está enviando dados é realmente a página da loja esperada. Com a utilização de certificados para assinar códigos executáveis, empresas desenvolvedoras de software podem impedir que outras pessoas modifiquem códigos executáveis. Esses certificados também previnem que usuários usem software de procedência duvidosa. Certificados de uso pessoal (certificado de cliente) destinados à assinatura e ao sigilo de documentos e e-mail são utilizados para autenticar clientes.

16. Depois de escolher a aplicação do certificado, o próximo passo a saber é a infra-estrutura em que o certificado será usado. Existem casos, em que um sistema exige certificados emitidos na hierarquia/relação de confiança sob a raiz da ICP-Brasil. Mas também um sistema pode exigir certificados emitidos por uma determinada AC que só atende no âmbito de uma corporação. Depois de considerar estes fatores, a pessoa ou empresa que deseja adquirir um certificado precisa escolher uma AC de confiança.

17. O que determina a qualidade da AC é a compatibilidade com as políticas e práticas que ela se compromete a cumprir (por exemplo, segue as normas da ICP-Brasil). Se for estritamente necessária uma verificação on-line da validade do certificado/validade da chave pública no certificado, então é indicado a procura de ACs que suportem tal serviço (que usa o protocolo OCSP, usado na infra-estrutura de chave pública mostrada nos slides).

18. Armazenamento de certificados: Existem duas formas de armazenar certificados digitais: certificados armazenados em software ou certificados armazenados em hardware. Atualmente, existem dois dispositivos padrões para armazenamento de certificados e chaves: *smartcard* e tokens USB . Seja qual for o padrão escolhido, com certeza será mais seguro do que armazenar o certificado em software. Para impossibilitar que pessoas que se apossem indevidamente de um dispositivo, utilizar o certificado ou as chaves contidas nele, é comum nesses dispositivos haver proteção de acesso (normalmente através de códigos PIN e PUK). Se uma pessoa, proprietária ou não do dispositivo, que está tentando acessar o conteúdo desses não conseguir entrar com os códigos de acesso, então o dispositivo é inutilizado/descartado e nesse caso a pessoa, se for a proprietário do dispositivo deverá requerer a emissão de outro certificado.

19. As premissas de uma VPN com segurança são: confidencialidade ou privacidade, autenticidade e integridade. Mas, o que uma VPN não protege ? A idéia sobre falhas numa VPN, na verdade, está diretamente ligada ao risco envolvido em determinadas configurações, em função do investimento feito na solução. Por exemplo, colocar em um gateway VPN, serviços que não fazem parte do contexto de segurança, pode reduzir custos, mas compromete a segurança. Outra falha que uma VPN não protege, diz respeito a ataques internos direcionados a servidores ou máquinas de funcionários dentro da empresa.

20. (Verdade/Falso) Sobre uma Função Hash: Existem infinitas mensagens M, mas um número finito de resumos (hashes) que pode ser gerado, por exemplo, com 20 bytes de resumo do algoritmo SHA-1. Portanto, a quantidade total de resumos (hashes) finita e igual a 2^{160} resumos que podem ser obtidos (este é uma arranjo com repetição de dois elementos, 0 e 1, tomados 160 a 160, onde a ordem dos elementos 0 e 1 nos resumos, importa, ou seja mudando-se os valores de dois bits tem-se que o resumo é outro). Isto significa que existem muitos resumos que podem ser produzidos, mas isso também significa que existem algumas mensagens que terão o mesmo resumo (por causa da finitude). Isto não deve trazer preocupações, em termos práticos, pois é extremamente raro que duas mensagens tenham, computacionalmente, o mesmo resumo (hash). Mais importante é o fato de não ser possível modificar uma mensagem e ainda assim produzir o mesmo resumo que a original.