Segurança Informática e nas Organizações

Teste Intermédio
11 de Novembro de 2015

João Alegria | 68661

Segurança Informática e nas Organizações
1º Semestre, 2015/16

Teste Intermédio
11 de novembro de 2015

- Todas as perguntas têm a mesma cotação.
- Todas as respostas devem ser justificadas.
- A duração total do exame é de 1h 30.

1. Considere o seguinte código SQL, em que `user` e `password` são variáveis com dados de autenticação.
   `"SELECT * FROM users WHERE uname='"+user+"' secret='"+MD5(password)+"'";`
   a. Identifique a vulnerabilidade, descreva um ataque prático e uma medida de prevenção.

2. Descreva, exemplificando, em que medida as medidas de desencorajamento, as medidas de ilusão e as medidas de deteção se relacionam com os ataques informáticos.

3. Qual o perigo dos *Zero Day Attacks*, em que medida podem ser evitados e quais as limitações das proteções para estes ataques?

4. Considerando os modos de uma cifra por blocos, explique, exemplificando com pelo menos dois modos, como a escolha do modo é um aspeto vital para a paralelização do processo de cifra.

5. Explique, recorrendo a um exemplo, como o período de um gerador de uma cifra contínua tem impacto no secretismo de um criptograma.

6. Qual razão pela qual são necessárias cifras assimétricas para a implementação correta de assinaturas digitais?
   a. Considere como exemplo o caso de N interlocutores trocando mensagens assinadas.

7. Considerando a necessidade de cifrar um texto de dimensão N por uma cifra com tamanho de bloco B, em que N não é múltiplo de B, descreva o processo que permite a correta operação da cifra.
   a. Exemplifique como se processaria a cifra e decifra de um texto arbitrário.

8. Tanto as assinaturas digitais como as *Message Authentication Code* (MAC), podem ser utilizadas para validar a integridade de uma mensagem. Descreva, exemplificando o processo de criação e verificação, em que cenários pode ser utilizado cada um dos métodos.

9. Porquê uma entidade certificadora expõe informação semelhante via CRL, Delta-CRL e OCSP?
   a. Refira o propósito de cada método, limitações e vantagens.

10. No contexto do cartão de cidadão, qual a necessidade de adicionar o certificado de chave pública de um cidadão a um documento que tenha sido assinado por ele?

Segurança 2015/2016
1º teste - 11 novembro 2016

1. Considere o seguinte código SQL, em que user e password são variáveis com dados de autenticação

"SELECT * FROM users WHERE uname = '" + user + "' secret = '" MD5(password) + "'";

a. Identifique a vulnerabilidade, descreva um ataque prático e uma medida de prevenção.

A vulnerabilidade descrita acima é o SQL Injection, uma falha que se aproveita de falhas de sistemas que interagem com a base de dados via SQL.

Os possíveis ataques práticos são:

- exposição de dados contidos na BD / consultar informação
- modificação de dados contidos na BD (através de read, update, delete)
- falsa autenticação em sistemas de Login

Uma medida de prevenção é a utilização de stored procedures. / Limitar privilégios de acesso / Parametrizar consultas

2. Descreva, exemplificando, em que medida as medidas de desencorajamento, as medidas de ilusão e as medidas de deteção se relacionam com os ataques informáticos.

As medidas de desencorajamento dificultam os ataques, uma vez que são implementadas barreiras de segurança, como firewalls e processos de autenticação.

As medidas de ilusão desviam os ataques. Ou seja, são simuladas possíveis falhas ao sistema baseado no histórico de falhas anteriores ou a partir de honey.

As medidas de deteção descobrem falhas, através de sistemas de deteção de intrusões.

3. Qual é o perigo dos zero Day Attacks, em que medida podem ser evitados e quais as limitações das proteções para estes ataques?

Os ataques "zero day attacks" são assim denominados uma vez que o autor da aplicação tem zero dias para planear qualquer forma de evitar esse ataque (como por exemplo: aconselhamento de soluções). Ou seja, o ataque explora vulnerabilidades desconhecidas e, uma vez que não existem quaisquer soluções conhecidas para por fim, possibilita o acesso a dados e a informações confidenciais.

Uma medida de resistir a este ataque é apostar na diversidade de sistemas operativos para qual o software pode ser lançado, ou bloquear com defesas em profundidade com auxílio de firewalls, ou utilizar mecanismos de proteção com análise comportamental (honeypots).

4. Considerando os modos de cifra por blocos, explique, exemplificando com pelo menos dois modos, como a escolha do modo é um aspeto vital para a paralelização do processo de cifra.
A paralelização possibilita o acesso aleatório ao conteúdo do ficheiro.
Por exemplo, no modo ECB o acesso aleatório é possível tanto na cifra como na decifra, mas no modo CBC só é possível na decifra (ou seja, no ficheiro cifrado)

5. Explique, recorrendo a um exemplo, como o período de um gerador de uma cifra contínua tem impacto no secretismo de um criptograma.
O período de uma cifra contínua pode ter impacto no secretismo de um criptograma através da repetição de padrões que se façam sentir nesse período do texto original.
Ou seja, se 23% dos caracteres forem A, então no criptograma 23% dos caracteres serão o substituto de A.⊗ Isto acontece uma vez que a cifra contínua usa apenas um alfabeto de substituição.

6. Qual a razão pela qual são necessárias cifras assimétricas para a implementação correta de assinaturas pessoais.
a. Considere como exemplo o caso de N interlocutores trocando mensagens assinadas
A assinatura digital de um documento consiste em autenticar o conteúdo do documento e autenticar o seu assinante. Para tal, a criptografia assimétrica é a melhor que se adequa a este fim, uma vez que os pares de chaves têm um cariz pessoal. A assinatura digital de um documento consiste na cifra do mesmo com a chave privada do autor. O criptograma resultante não serve para esconder o documento original mas sim para garantir, a quem o decifrar com a chave pública correspondente, que o texto recuperado seja igual ao original, está correto e foi assinado pelo detentor da chave pública.
Em modo de conclusão, uma mensagem digitalmente assinada deverá ser associável a uma e uma só entidade.

7. Considerando a necessidade de cifrar um texto de dimensão N por uma cifra com tamanho de bloco B, em que N não é múltiplo de B, descreva o processo que permite a correta operação de cifra.
a. Explique como se processaria a cifra e a decifra de um texto arbitrário.
As cifras por blocos, em alguns modos (ECB, CBC) têm de se aplicar a textos com dimensões múltipla do tamanho do bloco. Existem vários métodos para aumentar a dimensão do texto de forma previsível e reversível, tais como Cypher Text Stealing, Pkcs#5 e Pkcs#7. A este processo dá-se o nome de padding.

⊗ Da mesma forma, podem-se detetar construções características da linguagem, como digramas (consoantes dobradas RR e SS em português).

• O ciphertext stealing é um método em que se roubam N bytes do final do penúltimo bloco cifrado, sendo que são adicionados estes bytes ao último bloco de texto de forma a tornar o texto múltiplo do tamanho do bloco.
O último bloco é depois cifrado e enviado como penúltimo bloco (troca-se a ordem entre o último e penúltimo). O resultado é que a cifra ocorre normalmente mas o tamanho do criptograma não aumenta. No entanto, necessita que o texto ocupe um mínimo de 2 blocos.
Na decifra, depois de se decifrar o penúltimo bloco do criptograma, roubam-se de volta os bytes suficientes para compor o último bloco. Este é depois decifrado e volta-se a trocar a sua ordem (último com penúltimo). De notar que, os bytes "roubados" são sempre cifrados e decifrados duas vezes. Não entanto, o número de blocos cifrados ou decifrados não se altera.
Este método é o mais complexo. Os outros métodos são mais simples mas têm o inconveniente de aumentar sempre o tamanho do criptograma.
• O PKCS#7 funciona adicionando bytes com o valor dos bytes em falta. Ou seja, se o último bloco tiver 5 bytes em falta para ser múltiplo do tamanho do bloco, são adicionados 5 bytes com o valor 5.
• O PKCS#5 é igual mas foi definido apenas por blocos de 8 bytes (DES).

8. Tanto as assinaturas digitais como as Message Authentication Code (MAC), podem ser utilizadas para validar a integridade de uma mensagem. Descreva, exemplificando o processo de criação e verificação, em que cenários pode ser utilizada cada um dos métodos.
As assinaturas digitais e o MAC permitem validar a integridade de uma mensagem, a primeira a partir de um par de chaves assimétricas e a segunda através de uma chave simétrica partilhada.
As assinaturas digitais utilizam um par de chaves, onde a chave privada é utilizada para cifrar a síntese do documento. Esta cifra não se destina a esconder o conteúdo original do documento mas sim para garantir a autenticidade e integridade do autor. Posteriormente, uma vez que a chave pública do par pode ser partilhada, será com esta que se procederá ao método de verificação, o que implicará gerar uma nova síntese, decifrar a assinatura e comparar.
No caso do MAC - autenticadores de mensagens - é produzido um valor a partir da síntese de uma mensagem e de uma chave simétrica partilhada pelo emissor e pelo recetor da mesma. Assim, um MAC apenas pode ser gerado e validado por estas duas entidades, o que não acontece nas assinaturas digitais, uma vez que, qualquer um que detenha a chave pública do par de chaves pode verificar a autenticidade da mensagem.
O MAC apenas garante que a mensagem é integra para os participantes envolvidos.

9. Porquê uma entidade certificadora expõe informação semelhante via CRL, delta CRL e OCSP?

a. Refira o propósito de cada método, Limitações e vantagens.

O CRL é uma lista de certificados revogados. Tal define uma lista disponibilizada publicamente por uma PKI X.509v3 com todos os certificados que foram revogados e cujo prazo de validade ainda não expirou, onde em cada entrada da lista é apresentada informação relevante do mesmo, como a razão para a sua revogação e a sua data.

A informação pode então ser apresentada a partir do CRL, como a partir do delta-CRL onde só irá constar informação de entrada e saída de um CRL de referência.

As principais diferenças entre os elementos que constituem uma CRL completa e uma delta CRL é que esta última pode referir a remoção de entradas (ou seja, de certificados de revogação) e tem sempre de referir o identificador da CRL completa de referência.

Por último, a informação ainda pode ser consultada por OCSP, ou seja, um protocolo simples de pergunta-resposta onde é questionado o certificado a consultar através do seu número de série.

10. No contexto do cartão de cidadão, qual a necessidade de adicionar o certificado de chave pública de um cidadão a um documento que tenha sido assinado por ele?

O cartão de cidadão é detentor de um par de chaves assimétricas, composto por uma chave pública e outra privada. Este par de chaves pode ter fins destintos, ou seja, permite a confidencialidade dos dados se for utilizada a chave pública na cifragem do documento ou para fins de autenticação dos conteúdos e a sua autoria, caso a cifragem passe através da chave privada.

Assim, e de modo a que outros intervenientes possam comprovar a integridade do documento e a autoria do mesmo é necessária uma distribuição prévia da chave pública do autor para que seja possível realizar o processo inverso.

Em jeito de conclusão, os certificados presentes no cartão de cidadão têm três objetivos:

- Identificar o dono do cartão
- Possibilitar o dono autenticar outras pessoas com cartões semelhantes
- Possibilitar o cartão autenticar clientes com certificados semelhantes