DI/FCT/UNL
Mestrado Integrado em Engenharia Informática
Segurança de Redes e Sistemas de Computadores
2º Semestre, 2015/2016 (30/Maio/2016)

T2: Teste sobre tópicos teóricos do programa
Teste sem consulta, duração: 1h45m

Questão 1

Numa assinatura digital de chave pública emprega-se uma construção criptográfica composta por: um algoritmo assimétrico ou de chave pública (como por exemplo DSA, RSA ou ECC) e um algoritmo seguro de síntese (como por exemplo, funções da família SHA-1, SHA-2 ou SHA-3). Na normalização destas construções emprega-se ainda uma função de pré-processamento de *padding* (como por exemplo PKCS#1, OAEP ou MGF1).

a) Em que consiste, para que serve e qual a importância do processamento de *padidng* na robustez e garantias de segurança de uma assinatura digital ? Justifique, concretizando a a sua explicação com o processamento de uma assinatura usando o algoritmo RSA.

b) Uma possível instanciação da função de computação de *padding* consiste no padrão PKCS#1 Este processamento corresponde ao seguinte cálculo:

Padding(DATA) = 0x00 || 0x01 || F || DATA
Sendo F um *array* de bytes: 0xFF || 0xFF || 0xFF ... || 0x FF, de pelo menos 8 bytes

Note que este *padding (PKCS#1)* é o cálculo por defeito subjacente a uma assinatura digital que no caso de programação com o suporte JAVA-JCE corresponde às seguintes linhas de código

```
...
Signature signature = Signature.getInstance("SHA256withRSA”);
...
signature.initSign(keyPair.getPrivate());
...
signature.update(DATA);
```

Apresente um esquema (baseado num diagrama de blocos ou fluxograma) que explique o processamento de uma assinatura de DATA, com a sequência dos passos do processamento da assinatura digital subjacente à execução signature.update(DATA) no caso das linhas de código indicadas.

c) A assinatura do bloco de dados DATA de acordo com b) vai ser apresentada por um emissor a um destinatário. O emissor envia a assinatura conjuntamente com o bloco original e uma cadeia de certificação X509v3 que contem o certificado de chave pública do emissor (tendo a chave pública do certificado 2048 bits e não existindo na cadeia nenhum certificado com chaves públicas inferiores a 2048 bits). O destinatário pretende validar a assinatura. Apresente num esquema (diagrama de blocos ou fluxograma acompanhado de uma explicação clara e rigorosa) com todos os passos e todas as funções necessárias que devem ser executadas completamente pelo destinatário, para que a verificação da assinatura ocorra com segurança e com total confiança.

Nota: admita que o emissor e destinatário partilham uma base de confiança, possuindo e confiando ambos no certificado de chave pública que representa a raiz da cadeia de certificação enviada pelo emissor.

d) Suponha produz uma assinatura RSA-PKCS1, de acordo com o indicado em a) - usando uma função de síntese SHA-512. O par de chaves envolvido tem chaves RSA de 4096 bits, e os dados a assinar (DATA) são um bloco (ex., um *array* de bytes) com 256 bits. Do seu conhecimento teórico, qual vai ser o tamanho em bytes de DataSig ? Justifique.

e) Para que se possam garantir as propriedades de segurança de uma assinatura digital, enviada de A a B de acordo com a alínea c), é essencial do ponto de vista de segurança que o canal seja seguro, garantindo esse canal propriedades semelhantes às de um canal TLS ou SSL.

Comente a afirmação indicando se é correta ou incorreta, justificando a sua resposta.

f) O cálculo de *padding* nas operações criptográficas assimétricas (por exemplo usando RSA) é também importante noutros contextos de uso, por exemplo na construção de envelopes de distribuição de chaves secretas (para estabelecimento de chaves simétricas de sessão) ou no caso geral de se empregar cifras assimétricas para cifrar dados.

Que vantagens de segurança existem neste caso em usar um padrão de *padding* OAEP que utiliza o cálculos com funções de sínteses de segurança (neste caso MGF-1), comparativamente a usar padding PKCS#1 como referido em b) ? Justifique.

Questão 2

Pretende copiar ficheiros do disco do seu computador para uma *pen-drive*. Como receia perder a *pen-drive* decide usar criptografia RSA para cifrar cada ficheiro com uma chave pública. Guardará depois a chave privada do par em segurança, para poder recuperar os ficheiros. Os ficheiros têm dimensões variadas e vai cifrar cada ficheiro bloco a bloco, usando blocos de 2048 bits. A chave pública tem 1024 bits e não vai usar *padding* no processamento criptográfico. Do seu estudo teórico do processamento de cifras RSA, diga qual das seguintes afirmações é verdadeira, justificando a sua escolha.

AFIRMAÇÃO 1): Consegue cifrar os ficheiros de acordo com o descrito.

AFIRMAÇÂO 2): Só consegue cifrar os ficheiros se usar *padding*

AFIRMAÇÃO 3): A operação de cifra só é possível se as chaves envolvidas tiverem 2048 bits ou mais de modo a não usar *padding*

AFIRMAÇÃO 4): A operação de cifra não é possível como descrito, só sendo possível com chaves de 2048 bits e tendo obrigatoriamente que usar *padding*

Questão 3

Em anexo pode encontrar a especificação dos fluxos do protocolo Kerberos, nas versões V4 e V5, possuindo estas diferenças importantes.

a) Do seu estudo teórico (background) e tendo em conta a informação fornecida, identifique todas as melhorias na V5 em relação a V4? Justifique as melhorias e vantagens.

b) Num dado domínio de autenticação Kerberos, qual dos servidores (AS, TGS e servidores finais) partilham chaves derivadas das passwords dos clientes autenticados no domínio ? Justifique.

c) Tendo em conta o modelo de entidades no sistema Kerberos: Clientes, Servidores finais, AS (*Authentication Server*) e TGS (*Ticket Grantong Server*), qual destas entidades terá que ter

chaves partilhadas com entidades homólogas de outro domínio num contexto de autenticação multi-domínio (ou *multi-realm*) ? Justifique

d) Uma das fragilidades no sistema Kerberos tem a ver com a derivação de chaves simétricas a partir de passwords dos utilizadores (clientes). Quais as diferenças entre V4 e V5 em relação a esta possível vulnerabilidade e como se proporia melhorar este aspecto, tomando como referência a versão V5? Justifique.

Questão 4

Como sabe o protocolo TLS pode ser usado com diferentes configurações, que dão origem a propriedades de segurança muito diferentes. Entre essas diferenças uma das configurações corresponde ao modo de autenticação (anónima, unilateral ou mútua). Outra repercute-se no tipo de autenticação subjacente à *CIPHERSUITE* usada. Como é sabido do estudo teórico do protocolo e seu impacto na prática, as configurações possuem impacto na operação do sub-protocolo *HANDSHAKE*, nomeadamente no fluxo de mensagens e máquina de estado de processamento por parte dos *endpoint*s.

No caso de uso de *CIPHERSUITES* que envolvem o algoritmo *Diffie-Hellman* (em diversas versões do protocolo) é possível estabelecer chaves de sessão nos modos "*EDH - Ephemeral Diffie-Hellman*", "*FDH - Fixed Diffie-Hellman*" ou "*ADH - Anonymus DIffie-Hellmen*".

a) Qual a diferença entre esses modos ? Justifique, discutindo os níveis de segurança de cada um desses modos.

b) No caso de *CIPHERSUITES* usando o modo EDH com autenticação unilateral do servidor, o que permite proteger um ataque de impersonificação dos endpoints por interposição de um adversário do tipo "homem-no-meio" ? Justifique.

c) Se a *ciphersuite* escolhida usar EDH e o modo de autenticação for mútua, então o cliente e o servidor não podem usar certificados de chaves públicas DSA. Verdadeiro ou Falso ? Justifique.

d) Suponha que lhe fornecem um *trace* do protocolo Handshake-TLS (por exemplo obtido com uma ferramenta do tipo *wireshark*).

   D1) Como reconhece que se verificou autenticação unilateral só do cliente ?

   D2) Como reconhece que o fluxo TLS (*endpoint* cliente e servidor) não está invertido, comparando com o cliente que pediu a conexão e o servidor que aceitou a conexão ?

e) Um servidor HTTPS está a usar o protocolo TLS (numa configuração considerada segura, ex: TLSv1.2, autenticação mútua com o servidor impondo uma *ciphersuite* considerada segura, por exemplo: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

   Os clientes e o servidor usam cadeias de certificados que só usam chaves de tamanho igual ou superior a 2048 bits. Neste caso, seria possível um cliente (necessariamente autenticado) explorar uma vulnerabilidade do tipo Heartbleed – caso esta vulnerabilidade exista do lado do referido servidor HTTPS. Justifique a sua resposta.

Questão 5

a) Considere os diversos modelos ou tipologias de controlo de acessos: MAC (*Mandatory Access Control*), RBAC (*Role Based Access Control)* e ABAC (*Attribute-Based Access Control*). Explique em que consistem e como se diferenciam.

b) No caso do sistema de ficheiros UNIX (ou LINUX), qual o modelo de controlo de acessos subjacente ao modelo de permissões de operações sobre ficheiros ? Porquê ?

c) Que diferença tem estabelecer as seguintes permissões numa diretoria ?

rwxr-xr-x ou rwxrw----

Podem os elementos do grupo do utilizador dono da diretoria em causa listar a diretoria nos dois casos ? Explique.