

DI/FCT/UNL
Mestrado Integrado em Engenharia Informática
Segurança de Redes e Sistemas de Computadores
2º Semestre, 2016/2017
Teste de frequência nº 2 (14/Junho/2017)

Parte I (parte sem consulta) - Duração: 1h00

Questão 1

Quando se cifram dados com chaves públicas usando algoritmos criptográficos assimétricos (como por exemplo no caso de utilização do algoritmo RSA) podem usar-se parametrizações que envolvem processamento de *padding*. Este é o caso de configurações concretas, por exemplo, em implementações em JAVA:

```
Cipher cipher = Cipher.getInstance("RSA/NONE/PKCS1Padding")
```

ou...

```
Cipher cipher = Cipher.getInstance("RSA/NONE/OAEPWithSHA1AndMGF1Padding")
```

Para que serve e porque é importante usar *padding* do ponto de vista da segurança nas construções criptográficas de cifra com chaves públicas? Justifique.

Questão 2

Na segurança de uma assinatura digital RSA de uma mensagem M, estão envolvidos vários componentes: uma função de padding, uma função de síntese segura e a função de cifra que utiliza a chave privada.

- a) No processamento da assinatura obtida, o tamanho (em número de bytes) da assinatura (ciphertext) será dependente da função de síntese utilizada ou da função de *padding* usada ? Justifique.
- b) Concretizando a sua resposta à alínea a), se a mensagem M tinha originalmente 128 bits, estamos a usar uma chave privada de 2048 bits, a assinatura foi parametrizada para usar SHA-512 e o processamento de *padding* vai usar o padrão PSS (RSA-PSS), qual vai ser o tamanho concreto em bytes da assinatura calculada ? Porquê ?

Questão 3

Dois principais A e B precisam de estabelecer chaves de sessão com condições de segurança futura e passada perfeitas. Para isso vão usar o método de acordo de Diffie-Hellman.

A e B querem que o seu acordo seja imune a um ataque do tipo “homem-no-meio” face a adversários podem atuar no canal de comunicação usado por A e B, de acordo com as diversas tipologias de ataques tal como referenciadas na *framework* X.800.

Para o seu objetivo, A e B decidem trocar os números públicos de D-H que geram para estabelecer cada chave de sessão, enviando cada um o seu valor público cifrado com a chave pública do destinatário.

- a) Concorda com a decisão de A e B ? Justifique.
- b) Para mitigarem o uso prolongado da chave de sessão estabelecida, A e B decidem fazer uma operação de *rekeying* (refrescamento da chave), cada vez que A envia ou recebe um total de 100 mensagens, sendo estas trocadas a um throughput médio de 1 mensagem por segundo, o que leva a um processo de rekeying (em média) em cada 100 segundos.

B executa num telefone móvel e não gera novos números públicos para os parâmetros do algoritmo de Diffie-Hellman, pois pretende poupar energia, reutilizando sempre o mesmo número público inicialmente gerado. Assim, apenas A que executa num computador sem restrições de energia gera novos pares de números Diffie-Hellman em cada processo de *rekeying*.

Dado o comportamento de B isso cria uma fragilidade nas propriedades de segurança futura ou passada perfeitas do processo de *rekeying* ? Justifique.

Questão 4

- a) No processamento de uma mensagem Email utilizando PGP esta deve ser enviada e recebida com garantias de autenticação, confidencialidade e integridade. Vai também usar-se compressão. Na implementação decide-se usar compressão no final de todo o processamento criptográfico necessário e apenas antes do envio da mensagem. Parece-lhe que esta estratégia funciona? Justifique.
- b) No modelo de gestão de confiança de chaves públicas adoptado na concepção do sistema PGP, não é possível usar certificados de chaves públicas emitidas por CAs para efeitos de gestão de confiança das chaves públicas de emissores ou receptores de mensagens de Email. **Verdadeiro ou Falso ? Justifique.**

Questão 5

Porque é que no processamento TLS (ao nível do sub-protocolo RLP – Recor Layer Protocol) a compressão não pode ser aplicada após a obtenção da prova de autenticidade e integridade com MAC e antes da cifra de cada fragmento ? Justifique.

Obs) Note que no processamento TLS a compressão está definida como passo opcional. Tenha em conta que na definição do TLS, a compressão (se usada) é aplicada à fragmentação de pacotes TCP antes do processamento MAC e da cifra dos fragmentos com a chave de sessão estabelecida pelo handshake.

Questão 6

Considere a problemática da autenticação de utilizadores.

- a) Em que consiste um método de autenticação multi-fator e que vantagens encontra nesta abordagem para combater os problemas de autenticação com *passwords* e fragilidades exploradas por ataques às mesmas ?
- b) Como concretizaria um sistema do tipo do discutido em a) para autenticar utilizadores num sistema UNIX ou LINUX.
- c) Em que consiste uma autenticação com um fator do tipo Token-Based Authentication ? Argumente como este tipo de autenticação permite mitigar ataques do tipo *password-physhing* ?

Questão 7

- a) Qual a diferença entre um modelo de controlo de acesso MAC (Mandatory Access Control) e um modelo de controlo de acesso DAC (*Discretionary Access Control*) ?
- b) Considerando os modelos MAC ou DAC, como caracterizaria o modelo de controlo de acesso que foi implementado no trabalho prático N° 2 pelo seu servidor que implementa a política de controlo de acesso ?

Parte II (parte com consulta) - Duração: 1h00**Questão 8**

- O cumprimento do **princípio dos mínimos privilégios** impõe que as entidades ativas existentes num sistema computacional (por exemplo, utilizadores / processos) apenas tenham, num dado momento, acesso à informação ou recursos que são estritamente necessários para os seus legítimos objetivos nesse momento. Nas alíneas seguintes discute-se se este princípio é seguido em várias situações num sistema operativo multi-utilizador como o Linux.
- a) O CPU tem de ter dois modos de utilização (utilizador / sistema). Explique porque é que o CPU tem dois modos e diga se é válido nesta decisão o princípio dos mínimos privilégios. Justifique.
 - b) Considere o sistema de controlo de acesso no sistema de permissões de ficheiros UNIX. Trata-se de um modelo do tipo MAC, DAC ou RBAC. Justifique.
 - c) O funcionamento do modelo de controlo de acessos que descreveu em b) respeita o princípio dos mínimos privilégios? Justifique a resposta.
 - d) Como é sabido, existe nos sistemas UNIX um utilizador com nome *root*; processos associados a este utilizador têm todos os privilégios; processos pertencentes a outros utilizadores têm muito menos privilégios. Quais são os perigos associados a esta situação e diga, justificadamente se, ou em que condições, o princípio dos mínimos privilégios é neste caso aplicado.
 - e) Um ficheiro executável pode ter um bit chamado *setuid bit*. Diga como funciona este bit e para que é que é usado e se este uso põe em causa o princípio dos mínimos privilégios. Justifique.

Questão 9

Como procede no concreto para verificar se um dado certificado X509v3 que pretende validar não se encontra numa *Certification Revocation List* em que possa ter sido dado como revogado. Explique todos os passos necessários desde que recebe o certificado e como indexa e faz a verificação do mesmo na respetiva CRL utilizada.

Questão 10

- a) O protocolo TLS não tem nos seus objetivos a cobertura de contra-medidas contra ataques de negação de serviço. Estes podem ser desencadeados, por exemplo, por atacantes que lançam ataques do tipo “SYN-Flooding” sobre servidores HTTPS (provocando abertura incompleta de conexões TCP no processo de *3-way handshake* na abertura de conexões TCP). Estes ataques são ainda mais amplificados no caso do estabelecimento de sessões TLS ? Sim ou Não ? Justifique.
- b) A partir do traço capturado pela ferramenta wirehsark que mostra um trecho de tráfego (21 pacotes TCP – alguns dos quais encapsulando TLSv1.2) trocados entre um computador numa rede privada doméstica, com endereço 192.168.1.10, e um servidor HTTPS com endereço público 216.58.214.174 (correspondente ao nome domínio DNS mad01s26-in-f174.1e100.net), responda às seguintes questões:
 - B1) A autenticação TLS subjacente é cliente-only, server-only ou mutual cliente/server ? Porquê?
 - B2) Que porto TCP está a ser usado pelo cliente para enviar os records TLS (Recor Layer Protocol) subjacente à pilha TLS ?

- B3) Após qual dos pacotes no traço indicado o cliente já calculou a chave de sessão e está apto a receber records RLP cifrados enviados pelo servidor ? Porquê ?
- B4) Após qual dos pacotes no traço indicado o servidor já calculou a chave de sessão e está apto a receber records RLP cifrados enviados pelo cliente ? Porquê ?
- B5) Sabendo que o detalhe da mensagem trocada no instante ... 14.495544 é a que consta no anexo, diga qual a ciphersuite que vai ser adoptada pelo cliente e servidor neste handshake e qual a chave de sessão que no final irá suportar a troca de mensagens do protocolo HTTPS. Justifique.

...	14.452530	192.168.1.10	216.58.214.174	TCP	78	51408-443 [SYN]	Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=86110471 TSecr=0 SACK_PERM=
...	14.471320	216.58.214.174	192.168.1.10	TCP	74	443-51408 [SYN, ACK]	Seq=0 Ack=1 Win=42408 Len=0 MSS=1380 SACK_PERM=1 TSval=206162885
...	14.471389	192.168.1.10	216.58.214.174	TCP	66	51408-443 [ACK]	Seq=1 Ack=1 Win=131328 Len=0 TSval=86110489 TSecr=206162885
...	14.472518	192.168.1.10	216.58.214.174	TLSv1.2	280	Client Hello	
...	14.493951	216.58.214.174	192.168.1.10	TCP	66	443-51408 [ACK]	Seq=1 Ack=215 Win=43520 Len=0 TSval=206162908 TSecr=86110490
...	14.495544	216.58.214.174	192.168.1.10	TLSv1.2	1484	Server Hello	
...	14.496490	216.58.214.174	192.168.1.10	TCP	1484	[TCP segment of a reassembled PDU]	
...	14.496550	192.168.1.10	216.58.214.174	TCP	66	51408-443 [ACK]	Seq=215 Ack=2837 Win=129632 Len=0 TSval=86110512 TSecr=206162909
...	14.496664	216.58.214.174	192.168.1.10	TCP	1484	[TCP segment of a reassembled PDU]	
...	14.496666	216.58.214.174	192.168.1.10	TLSv1.2	285	CertificateServer Key Exchange, Server Hello Done	
...	14.496688	192.168.1.10	216.58.214.174	TCP	66	51408-443 [ACK]	Seq=215 Ack=4474 Win=129408 Len=0 TSval=86110513 TSecr=206162909
...	14.551502	192.168.1.10	216.58.214.174	TLSv1.2	141	Client Key Exchange	
...	14.551503	192.168.1.10	216.58.214.174	TLSv1.2	72	Change Cipher Spec	
...	14.551503	192.168.1.10	216.58.214.174	TLSv1.2	111	Encrypted Handshake Message	
...	14.563485	192.168.1.10	74.125.71.188	TCP	54	51076-443 [ACK]	Seq=1 Ack=1 Win=4096 Len=0
...	14.569467	216.58.214.174	192.168.1.10	TCP	66	443-51408 [ACK]	Seq=4474 Ack=296 Win=43520 Len=0 TSval=206162984 TSecr=86110567
...	14.573277	216.58.214.174	192.168.1.10	TLSv1.2	117	Change Cipher Spec, Hello Request, Hello Request	
...	14.573357	192.168.1.10	216.58.214.174	TCP	66	51408-443 [ACK]	Seq=341 Ack=4525 Win=131008 Len=0 TSval=86110587 TSecr=206162987
...	14.581216	192.168.1.10	216.58.214.174	TLSv1.2	578	Application Data	
...	14.581270	192.168.1.10	216.58.214.174	TCP	1434	[TCP segment of a reassembled PDU]	
...	14.581271	192.168.1.10	216.58.214.174	TLSv1.2	944	Application Data	

▶ Frame 55: 1484 bytes on wire (11872 bits), 1484 bytes captured (11872 bits) on interface 0
 ▶ Ethernet II, Src: HitronTe_bb:6d:d5 (00:05:ca:bb:6d:d5), Dst: Apple_8c:a8:5a (60:03:08:8c:a8:5a)
 ▶ Internet Protocol Version 4, Src: 216.58.214.174, Dst: 192.168.1.10
 ▶ Transmission Control Protocol, Src Port: 443, Dst Port: 51408, Seq: 1, Ack: 215, Len: 1418
 ▼ Secure Sockets Layer
 ▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
 Content Type: Handshake (22)
 Version: TLS 1.2 (0x0303)
 Length: 350
 ▼ Handshake Protocol: Server Hello
 Handshake Type: Server Hello (2)
 Length: 346
 Version: TLS 1.2 (0x0303)
 ▶ Random
 Session ID Length: 32
 Session ID: b6388ec2b3ed6db4d7f5f4c73787349c796eff67a96e7892...
 Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
 Compression Method: null (0)
 Extensions Length: 274
 ▶ Extension: renegotiation_info
 ▶ Extension: signed_certificate_timestamp
 ▶ Extension: Application Layer Protocol Negotiation
 ▶ Extension: ec_point_formats

- c) No handshake TLS um dos elementos determinantes da complexidade computacional imposta aos endpoints é a necessidade de computações envolvendo exponenciais modulares (ou exponenciais-módulo), com números de grande dimensão (conforme as dimensões de chaves envolvidas).

Num handshake com autenticação mútua que vai usar estabelecimento de chaves de sessão com base no modo Ephemeral Diffie-Hellman com os números públicos Diffie-Hellman enviados assinados com assinaturas RSA, quantas exponenciais modulares serão canceladas por cada endpoint durante o processo de handshake ? Justifique.

Nota) Não conte com verificações de assinaturas dos certificados trocados, devendo apenas ter em conta as exponenciais necessárias para a geração, autenticação e verificação dos parâmetros de Diffie-Hellman para geração da chave de sessão.