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 (Sem tolerância)

Questão 1

Quando se cifram dados com chaves públicas usam-se habitualmente parametrizações que envolvem processamento de *padding*. Este é o caso de configurações concretas, por exemplo, em implementações em JAVA para construção de envelopes de chave pública usando RSA, por exemplo:

- Cipher cipher = Cipher.getInstance("RSA/NONE/PKCS1Padding")
- Cipher cipher Cipher.getInstance("RSA/NONE/OAEPWithSHA1AndMGF1Padding"

Para que serve e porque é importante usar *padding*? Justifique.

O padding serve para …

A sua utilização é importante porque …

Questão 2

Na segurança de uma assinatura digital RSA de uma menagem M, estão envolvidos vários componentes: uma função de *padding*, uma função de síntese segura e a função de cifra que utiliza a chave privada. No processamento da assinatura obtida, o tamanho (em número de bytes) da assinatura (ciphertext) é dependente da função de síntese utilizada e da função de *padding* escolhida.

A afirmação é verdadeira ou falsa ? _____

Justificação:

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 ? _____

Justificação:

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 receba 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*.

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

Questão 4

No envio de uma mensagem de E-Mail por parte de um Mail User Agent que utiliza o formato seguro PGP, a mensagem será enviada com garantias de autenticação, confidencialidade e integridade. Vai também usar-se compressão.

Na implementação a compressão é feita no final de todo o processamento criptográfico necessário e antes do envio da mensagem.

Parece-lhe que esta estratégia funciona? Sim ou Não ? _____

Porquê ?

Questão 5

Tenha em conta os modelos de controlo de acesso estudados. E considere o sistema de controlo de acesso estabelecido pelo controlo de permissões no sistema de ficheiros UNIX

a) . Trata-se de um modelo do tipo MAC, DAC, RBAC. Ou ABAC ? _____

Justificação:

b) Considerando os modelos de controlo de acesso anteriores, como caracteriza o modelo de controlo de acesso que implementou no trabalho prático Nº 2 no servidor que implementa a política de controlo de acesso ? _____

Justificação:

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) 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* ?

c) Como concretizaria um sistema do tipo do discutido em b) num processo de autenticação multi-fator para autenticar os utilizadores de um sistema UNIX ?

Parte II (parte com consulta) - Duração: 1h00 (+ 20 min para questão 10 sobre o TP2)

Questão 7

Considere o **princípio dos mínimos privilégios** Num modelo de um sistema de controlo de acessos..

a) O funcionamento do modelo de controlo de acessos do sistema de ficheiros no sistema operativo UNIX respeita o princípio dos mínimos privilégios? Justifique a resposta.

Sim ou Não ? _____

Justificação:

b) 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.

Perigos:

Justificação sobre se e em que condições o princípio é respeitado:

Questão 8

a) No sistema PGP os utilizadores podem ter associado a cada conta de E-Mail (ou endereço E-Mail por si usados) mais do que um par de chaves (pública-privada), podendo usar indiscriminadamente qualquer par para envio ou recepção de mensagens autenticadas e confidenciais. Porque é que isso é possível ? Justifique.

b) Na arquitetura e segurança do sistema de Email Internet (Internet Mail Architecture), explique o papel da solução DKIM e argumente em que medida essa solução é importante para mitigar ataques do tipo Mail-Spam.

c) Como é que um servidor SMTP envolvido no encaminhamento de mensagens de Email adquire dinamicamente as chaves públicas que terá que usar para verificar as assinaturas DKIM ? Acha que o procedimento é confiável ou advogaria condições complementares para aumentar a segurança dessa verificação ? Quais ?

Questão 9

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 em anexo capturado pela ferramenta wireshark que mostra um trecho de tráfego (21 pacotes TCP – alguns dos quais encapsulando TLSv1.2) trocados entre um computador numa rede privada doméstica (endereço 192.168.1.10) e um servidor HTTPS (endereço público 216.58.214.174) correspondente ao nome DNS mad01s26-in-f174.1e100.net), responda às seguintes questões B1 a B5

B1) A autenticação TLS subjacente é cliente-only, server-only ou mutual cliente/server ? Porquê?

A autenticação é: _____
porque:

B2) Que porto TCP está a ser usado pelo cliente para enviar os records TLS (Recor Layer Protocol) subjacente à pilha TLS ? _____

Porquê ?

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 ?

Após se ter verificado o pacote temporalmente identificado por: _____

Porque:

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 ?

Após se ter verificado o pacote temporalmente identificado por: _____

Porque:

B5) Sabendo que o detalhe da mensagem trocada no instante temporalmente identifidado po ... 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 vai ser estabelecida para troca de mensagens do protocolo HTTPS.

A cipersuite é: _____
O algoritmo simétrico que vai ser usado na sessão HTTPS para proteger as mensagens encapsuladas no formato do sub-protocolo RLP (do TLS) é: _____, e irá ser usada uma chave de sessão de _____ bits.

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 canculadas 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.

O cliente fará _____ exponenciais modulares.

O servidor fará _____ exponenciais modulares

Justificação:

Questão 10
// Questão a considerar para avaliação individual sobre a avaliação de grupo doa implementação doTP2

a) Quando um cliente se autentica no servidor de autenticação (Parte I do trabalho) para efeitos de poder depois iniciar o acordo Diffie-Hellman face ao grupo de participantes que se encontra numa sessão multicast-chat (funcionalidade da PARTE II do trabakho) precisará de provar que foi previamente autenticado e obteve permissões de controlo de acesso para o efeito. Qual a prova que tem do servidor de autenticação e controlo de acesso e como é que a mesma pode ser comprovada pelos participantes que estão na sessão, quando o novo utilizador entrar ?

Responda justificadamente, referindo qual o conteúdo da prova criptográfica verificável que o participante obteve no protocolo de autenticação e controlo de acesso. De prefer~encia deve usar uma representação formalizada dessa prova criptográfica.

b) Na sua implementação qual a garantia de que os números públicos nos parâmetros Diffie-Hellman enviados (na saída ou entrada de participantes) para negociação de novas chaves de sessão em grupo são enviados por participantes autênticos e não podem ser replayed

c) No contexto de entrada ou saída de um participante , com a consequente renegociação de uma nova chave de sessão com base num acordo Diffie-Hellman, qual a garantia que qualquer um dos participantes na sessão (como membro correto do grupo que vai usar a nova chave de sessão) pode ter e comprovar que a nova chave gerada e estabelecida também tem necessariamente a sua contribuição individual, podendo ser considerada como uma chave de sessão segura com salvaguarda de segurança futura ou passada perfeita

ANEXO: para resposta da questão 9

…	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
```