Segurança de Sistemas Computacionais
Teste de Frequência #1
Departamento de Informática, FCT/UNL
26/Outubro/2013

Nº		Nome	
Grupo		Nº Total de folhas (incluindo esta):	

Grelha de Avaliação (a preencher pelo docente)

PARTE I (1 - Sem consulta)									

PARTE II (2 - Com consulta)									

Duração do teste
Parte I (sem consulta): 10h00-11h15
Parte II (com consulta): 11h30-13h00

Parte I (respostas sem consulta)

Q1) Utilizando a terminologia e classificação de tipologia de ataques na arquitectura de segurança OSI X.800 e na base de normalização IETF (subjacente por exemplo à normalização RFC 2828), identifique tipos de ataques às comunicações do tipo activo e passivo, usando a seguinte tabela.

Ataques passivos

1)	
2)	

Ataques activos

1)	
2)	
3)	
4)	
5)	

Complete as seguintes frases de forma a traduzirem afirmações verdadeiras:

Um ataque do tipo _____ é em geral mais difícil de _____ mas fácil de prevenir, usando essencialmente mecanismos específicos da criptografia
Já um ataque do tipo _____ é em geral mais fácil de _____ sendo no entanto mais difícil de prevenir. De entre estes, por exemplo, um ataque do tipo _____ não pode ser prevenido mesmo combinando diferentes mecanismos, ferramentas e processos criptográficos.

Q2) Ainda utilizando a base conceptual e a terminologia na Framework X.800, qual a diference entre mecanismos específicos ou fundamentais de segurança e os mecanismos ditos permeados (ou *pervasive mechanisms*) de segurança ?

Mecanismos específicos:

São mecanismos que ...

Dê um exemplo de um mecanismo específico usado num serviço de segurança:

Mecanismos permeados:

São mecanismos que...

Dê um exemplo de um mecanismo permeado usado num serviço e segurança:

Q3) A categorização das propriedades de segurança na normalização FIPS 199, define os objectivos de segurança associados às propriedades de segurança dos sistemas computacionais através das seguintes propriedades fundamentais: confidencialidade, integridade e disponibilidade (CIA Triad). Isto significa que nesta base de normalização a autenticação não é considerada como propriedade fundamental de segurança num sistema computacional ?

Q4)

a) Considere um protocolo de segurança para estabelecimento de um canal seguro entre dois principais, com protecção das propriedades de autenticação, integridade e confidencialidade. Que diferença há em dizer-se que esse protocolo assegura autenticação dos principais comparativamente a dizer-se que garante autenticação das mensagens ?

Autenticação de principais consiste em...

Indique o que poderia utilizar como mecanismo específico de autenticação de principais:

Autenticação de mensagens consiste em ...

Para este efeito, indique o que poderia utilizar como mecanismo específico de autenticação de mensagens:

Q5) Um computador foi infectado por um *keylogger* que foi instalado na sequência de instalação descuidada de código de um servidor Web, algures na Internet. O descarregamento do programa foi feito por HTTPS (ou seja, uma conexão HTTP suportada em SSL), por um utilizador que usava o computador com privilégios de Administrador ou *Superuser*. Este programa, uma vez instalado, comprometeu o driver I/O e passou a interceptar entrada de dados do teclado, enviando esses dados para um sistema remoto controlado por um atacante (independentemente de, aparentemente, o funcionamento do teclado continuar a parecer correcto na utilização de todos os programas correctos que se executam nesse computador).

a) Indique, considerado estritamente a tipologia de ataques tal como definidos na Framework X.800, em que tipologia se enquadra o anterior ataque.

b) De acordo com a tipologia de propriedades e serviços de segurança estabelecidos pela Framework X.800, que mecanismos deveria ser usados para um serviço que actuasse como contra-medida desse ataque.

Q6) Na estrutura geral de um método criptográfico simétrico para cifra/decifra em cadeia para cifrar/decifrar *bit-a-bit* em tempo real, um dos componentes nucleares assenta numa função capaz de gerar uma sequencia pseudo-aleatória (PRF). Esta sequencia tem a forma de uma cadeia contínua de bits, de período maior do que a dimensão da cadeia a cifrar. Para conceber este algoritmo de cifra em cadeia, usou-se como PRF um algoritmo seguro de cifra de blocos (por exemplo, AES operado em modo CTR). Dessa forma, a segurança intrínseca do algoritmo de cifra em cadeia resultante será equivalente à segurança da cifra de blocos usada para "fabricar" a função PRF. Para o efeito, apenas se precisa de usar a implementação da operação de cifra do algoritmo AES (não sendo necessário usar a função de decifra AES).

a) Considera a afirmação VERDADEIRA ou FALSA_____

b) No caso de ter respondido VERDADEIRO a a) apresente um diagrama de blocos (e legenda que clarifique o diagrama) que concretize a solução indicada. No caso de ter respondido FALSO em a), justifique porque é que não considera possível ou válida a abordagem indicada.

Q7)

a) Num ataque por criptanálise a um algoritmo criptográfico, em que consiste um ataque do tipo "chosen text" (ou de escolha de texto) ?

b) Indique os dois critérios base, considerando as variáveis custo e tempo, através dos quais um método criptográfico simétrico é considerado na prática computacionalmente seguro (independentemente de não ser infinitamente seguro).

Q8)

Suponha que num protocolo de comunicações seguras, para proteger confidencialidade das mensagens, utiliza criptografia 3DES operando o algoritmo no modo CFB (Cipher Feedback Mode). A operação deste modo pode representar-se da seguinte forma, em que Ci representa a sequencia de blocos cifrados de cada mensagem enviada no canal e Pi representa os blocos em claro dessa mensagem:

$$C1 = P1 \text{ xor } Ss(\{IV\}_k) \quad , \quad Ci = Pi \text{ xor } Ss(\{C_{i-1}\}_k)$$

Sendo Ss(B) uma função que dado um bloco B de b bits de entrada, retorna os s bits mais significativos desse bloco, sendo s<b e sendo s o número de bits de P1 ou Pi.

Dado o anterior, indique como escreveria as expressões para calcular P1 e Pi na operação de decifra.

P1 = _____, Pi= _____

Parte II (respostas com consulta)

Q9

Considere o protocolo de distribuição de chaves de Needham-Schroeder para estabelecimento de chaves de sessão entre dois principais A e B, na variante que usa criptografia simétrica. Suponha que em vez de utilizar *Nonces* na implementação do protocolo (nas várias mensagens e fases do protocolo), alguém decidiu usar *timestamps* (ou estampilhas temporais). Ou seja, no lugar dos *Nonces* de desafio ou de resposta, os principais envolvidos (KDC, A e B) utilizam *timestamps* obtidos dos seus relógios locais, no momento da geração das mensagens que enviam. A ideia é que cada destinatário controlará esses *timestamps* para testar se as mensagens são "frescas", isto é, se as mesmas não resultam de retransmissões ilícitas por parte de um atacante.

Que problemas identifica com esta abordagem em relação à utilização de *Nonces*?

Q10

Considere o contexto do seu trabalho prático nº 1.
De acordo com a sua implementação que medidas destacaria na sua implementação que tiveram em vista minimizar a possibilidade de ataques do tipo DoS que podem ser desencadeados contra os clientes (proxies da aplicação de visualização VLC)), contra o servidor de autenticação e contra o servidor de *streaming,* tendo em conta as operações de processamento criptográfico das mensagens por parte de cada um desses servidores.

Se considera que não implementou nenhuma medida que tenha em vista reduzir ataques de negação de serviço, sugira algumas medidas de melhoria dos protocolos que poderiam minimizar esse tipo de ataque que possa ser desencadeado por um atacante que actua no canal.

Q11

Suponha que pretende guardar os seus ficheiros na *Dropbox* (ou numa solução similar de um repositório de ficheiros numa nuvem de armazenamento, ex., *GoogleDrive*, *Box*, etc), deixando de ter esses ficheiros no sistema de ficheiros local do seu computador, de forma a usufruir das vantagens dessas soluções. Para evitar a exposição dos ficheiros em claro (por querer controlar a privacidade da informação que guarda em alguns dos seus ficheiros e temer que pessoal do provedor possa aceder indevidamente aos mesmos), decide que cada vez que transfere um ficheiro F para a *Dropbox*, processa antes o ficheiro de forma a protegê-lo numa cápsula de segurança, sendo então as cápsulas guardadas na nuvem do provedor da solução que usa (Dropbox ou outra).

Cada cápsula C de um ficheiro F será obtida através de uma função C(F) como a seguir se indica (usando a notação habitual utilizada nas aulas):

$$X(F) = [\ \{Ks\}Kpub \,||\, \{F\}Ks \,||\, \{\ H1(F)\ \}Kpriv$$
$$C(F) = H2(N) \,||\, X(F) \,||\, HMAC_K(\ X(F)\ )$$

As cápsulas serão então guardadas como ficheiros na nuvem, cujos nomes são calculados a partir do nome N original dos ficheiros na forma H2(N), em que H2 é uma função de síntese segura capaz de gerar sínteses de tamanho razoável (ex., 512 bits).

Para calcular as cápsulas acima utilizará: criptografia assimétrica RSA com chaves (pública e privada) de 2K, criptografia simétrica AES em modo CBC com chaves Ks de 256 bits (geradas de forma única para cada ficheiro guardado na nuvem) e assinaturas RSA com síntese SHA-1. Na cápsula, o papel do HMAC servirá como prova rápida de autenticidade e integridade da cápsula, sendo a chave K do HMAC calculada a partir de uma síntese SHA-1 do nome original do ficheiro.

No seu computador (*file system* local) apenas manterá uma lista dos nomes dos ficheiros que guardou na nuvem, e o par chave pública chave privada (embora a chave pública pudesse também ser guardada na nuvem, por exemplo, dentro de um ficheiro em claro, cujo nome poderia ser H2(Kpub).

Para efeitos de resiliência (com receio que alguém apague na nuvem o seu repositório), tudo o que guarda numa nuvem, duplica também noutra nuvem (usando por exemplo simultaneamente a Dropbox e o GoogleDrive, por exemplo, ou quaisquer outras duas soluções congéneres).

a) Mostre, sob a forma de um algoritmo em pseudo-código (ou descrito um fluxograma), como faz para recuperar um ficheiro cujo nome é "nome".

b) Na cápsula acima, várias funções de síntese são usadas: H1(), H2(), bem como as funções de síntese subjacentes ao HMAC.

   De todas essas funções de síntese, diga quais as que exigem "*Strong Collision Resistance*" e quais as que apenas poderiam exigir "*Weak Collision Resistance*" se considerar que pode haver ataques à integridade na nuvem. Justifique.