Departamento de Informática
Faculdade de Ciências e Tecnologia
UNIVERSIDADE NOVA DE LISBOA

Curso de Engenharia Informática (2º Ciclo)

Segurança em Sistemas e Redes de Computadores

SSRC-0910-EN-1.1.A

1º Semestre 2009/2010

TESTE DE AVALIAÇÃO / FREQUÊNCIA Nº 1

07/11/09

Teste sobre os aspectos e tópicos relacionados com a realização do Trabalho Prático nº 2

Notas:

- O enunciado tem 2 Grupos:
  - PARTE I: Constituído por 3 questões sem consulta (10 valores)
  - PARTE II: Constituído por 3 questões com consulta (10 valores)
- Duração: 1 hora para cada uma das partes. As partes serão separadas por um intervalo de 10 min

---------- A preencher pelos alunos no final do teste ----------

Nº de aluno: _____ Nome: _____

Nº TOTAL de páginas entregues (exceptuando esta capa): _____

Obs: numere as páginas na forma nº da página /Nº TOTAL e coloque o nº e nome em cada folha.

---------- A preencher pelo docente ----------

Parte 1	Parte II 2)	Parte II 3)	Parte II 4)	TOTAL
1 2 3				

INF Controlo:

PARTE SEM CONSULTA (até 50 min no máximo)

Questão 1)

Considerando a terminologia e classificação da Framework OSI X.800, diga:
a) qual a diferença entre as noções de ataque activo e ataque passivo ?

b) Dê dois exemplos concretos de como se pode desencadear um ataque activo e um ataque passivo (pode ser qualquer um que entenda situar-se n domínio da classificação da Framework X.800) numa rede local com as características da rede local dos laboratórios do DI. Deve indicar preferivelmente como o ataque poderia ser lançado indicando exemplificadamente que ferramentas ou tipo de ferramentas poderia o atacante utilizar.

Nessa alínea não pode considerar o contexto da alínea c)

c) Considere a noção subjacente a um ataque do tipo Masquerade. Pode um ataque ao protocolo ARP estar na origem de um ataque activo do tipo Masquerade ? Justifique a resposta com base na explicação de um cenário que mostre que o ataque pode ou não pode ser feito (de acordo com a sua resposta).

Questão 2)

A seguinte tabela relaciona ataques e serviços, conforme a terminologia e conceptualização da Framework OSI X.800.

1.1	Release of message contents	Traffic analysis	Masquerade	Replay	Modification of messages	Denial of service
Peer entity authentication			Y			
Data origin authentication			Y			
Access control			Y			
Confidentiality	Y					
Traffic flow confidentiality		Y				
Data integrity				Y	Y	
Non-repudiation			Y			
Availability						Y

a) Qual a diferença entre "Traffic Analisys" e "Release of Message Contents" ?
b) Apresente outra tabela em que relacione a tipologia de ataques (como na tabela anterior) mas em que nas linhas, em vez de serviços coloque a tipologia de mecanismos da Framework X.800, pela seguinte ordem: Encipherment, Digital Signature, Access-Control, Data Integrity Checking, Authentication Exchange Protocol, Trafic-Padding, Routing Control, Notarization
c) Dos anteriores mecanismos, e ainda usando a terminologia e conceptualização X.800, quais considera serem mecanismos específicos ("specific security mechanisms") e quais considera serem mecanismos ditos permeados ("pervasive mechanisms") ?

Questão 3

Diga como se pode implementar um processo de cifra em cadeia (bit-a-bit), que pudesse ser usado, por exemplo, para transmitir um fluxo cifrado de video-streaming em real-time, tendo como componente de base uma implementação de um algoritmo de cifra de blocos, como por exemplo o AES, com uma chave de 256 bits. Apresente apenas o processo esquematicamente e justifique como funcionariam os processos de cifra e decifra da cadeia

Parte COM CONSULTA (até 80 min no MÁXIMO)

Questão 1 (20 min)

Nota: de acordo com o enunciado, deve responder a a) e dependendo da resposta de a), deve responder a b) ou c)

Suponha o seguinte protocolo de autenticação. Neste protocolo, pretende-se apenas garantir a propriedade de autenticação entre A e B, supondo que previamente, A e B partilham uma chave secreta k que foi estabelecida de forma segura, por exemplo a partir de um protocolo como o protocolo Needham-Schroeder e que estabeleceu previamente a chave k. Na e Nb são "nonces" gerados por A e B, respectivamente, durante o presente protocolo.

A>B {Na}k
B>A {Nb}k, Na
A>B {Nb}

Assuma que:

(i) O protocolo vai ser suportado em UDP e cada mensagem corresponde ao envio de um único datagrama
(ii) No ambiente computacional em causa, o protocolo pode ser desempenhado por quaisquer pares de N principais A, B, C, D, E, F, …. ec
(iii) O protocolo pode correr entre quaisquer pares de principais, de forma assíncrona e em paralelo.

a) Considera que este protocolo garante a propriedade de autenticação ? Justifique argumentando se sim ou não e se não como é que o protocolo poderia ser atacado por um principal X que actuasse de forma maliciosa.
b) **Se respondeu sim em a)** , diga como garantiria adicionalmente suporte para garantir a propriedade da integridade sem suporte orientado à conexão. Se respondeu não à questão anterior não responda a esta alínea.
c) Se respondeu não em a), diga como se proporia resolver o problema de garantir de facto autenticação entre A e B, a partir do protocolo indicado.

Questão 2 (20 min)

Analise o protocolo anexo (Beller-Yacobi) para compeender o seu funcionamento esperado e interprete o ataque considerado que consegue explorar na verdade uma vulnerabilidade do protocolo.

Apresente uma correcção ao protocolo, de maneira a evitar o ataque considerado.

Na sua argumentação de análise do ataque (no entendimento do anexo fornecido) e na correcção proposta, apresente as considerações que achar convenientes para argumentar sobre a eficácia da sua correcção.

Questão 3 (40 min)

É obrigatório fazer a)
É obrigatório fazer b) ou c)
É obrigatório fazer d)
Mas se fizer c) e d) não precisa de fazer a) nem b)

Considere o contexto do seu trabalho prático n 1.

a) Apresente num diagrama temporal, de forma completa e rigorosa, o protocolo que desenvolveu para a fase 2 do trabalho.

b) Indique uma solução para o estabelecimento da chave de sessão, com base num esquema PBE Encryption combinando com um esquema do tipo One Time Pad (ou One Time Password) subjacente à geração da chave. De preferência apresente a especificação com base num diagrama temporal, ilustrando qual o processamento intermédio do cliente e servidor com base numa legenda associada aos estados de execução no fluxo do protocolo.

c) Apresente uma especificação (com recurso a um diagrama temporal) para especificar de forma CLARA, RIGOROSA e COMPLETA, como desencadeia o protocolo Needham-Schroeder com criptografia assimétrica, e como complementaria o mesmo com um esquema contributivo de acordo de chaves com base no método D-H (Diffie-Hellman), de modo a estabelecer a chave de sessão entre o cliente e o servidor com base em garantias de segurança passada e futura perfeitas.

d) Suponha que o cliente do seu trabalho prático executa num telefone móvel (com base numa aplicação JAVA c/suporte MIDP e que interage com o servidor utilizando uma infra-estrutura 802.11 WLAN. A aplicação só utiliza http/1.0 na interacção com o servidor. A solução de b) seria a mais desejável ? Como poderia avançar uma idea inicial para especificação (abordagem inicial) de um esquema de estabelecimento de chave de sessão contributiva que fosse mas adequado a este "*setting*". Discuta as vantagens e eventuais *tradeofs* da solução que propõe.