DI/FCT/UNL
Mestrado Integrado em Engenharia Informática

Segurança de Redes e Sistemas de Computadores
2º Semestre, 2015/2016
(12/Abril/2016 TP1C)

T1-P: Teste Prático (C1)
Enquadramento e Desenvolvimento do Trabalho Prático nº 1
Duração: 45 minutos

Questão 1 (Fase 1)

Na implementação de referencia do enunciado do trabalho, indicava-se que deveria ser implementado um formato universal de segurança para suportar todas as mensagens do protocolo de suporte à aplicação (*Chat*/*Messaging*).

Usando uma notação formal contendo as várias partes constituintes desse formato de mensagens, o formato era o seguinte:

HEADER || DADOS || MAC

Em que:
HEADER = Phase || Vers || LEN // informação enviada em claro (ou *plaintext*)

DADOS: corresponde à parte da mensagem enviada cifrada com um algoritmo criptográfico simétrico de acordo com as parametrizações criptográficas, na forma:

DADOS = { TYPE || uID || r1 || r2 || Dados da mensagem || MAC_{Kh} }$_{Ks}$

Como sabe, MAC_{Kh} corresponde à prova de integridade e de autenticidade da mensagem, com base na chave Kh (supostamente implementada por funções do tipo HMAC ou CMAC, também de acordo com as parametrizações criptográficas utilizadas). K_s é a chave de sessão usada para proteção de confidencialidade das mensagens.

a) Qual o valor que corresponde a uID na sua implementação ? Indique no seu código onde é que este valor é colocado quando está a enviar as mensagens (emissor) e em que local é verificado no processamento (pelo receptor). Indique ao nível das instruções especificamente envolvidas e não mais do que essas.

b) Para que servem os valores r1 e r2 e como foram utilizados na sua implementação da fase 1 ? Indique no código onde estes valores são utilizados e como são processados, indicando a lógica do processamento e verificação para o efeito pretendido. Indique ao nível das instruções especificamente envolvidas e não mais do que essas.

Questão 2 (Fase 1)

a) Diga se na sua implementação e parametrizações, utilizou ou ensaiou funções do tipo CMAC como possibilidade de parametrizar a função MAC no formato da mensagem ? Se SIM diga quais. Se NÃO indique simplesmente que funções do tipo MAC foram utilizadas e que podem ser suportadas na sua implementação.

b) **Nota:** *Responda a esta alínea, apenas se não utilizou funções CMAC para a implementação de MAC*

   No caso de responder negativamente a a) indique ainda assim, como procederia à parametrização de uma função CMAC para o efeito, indicando como a poderia suportar a partir da sua implementação.

c) **Nota:** *Responda a esta alínea, independentemente de ter ou não utilizado funções do tipo CMAC para a implementação de MAC*

   Independentemente de ter ou não ter utilizado funções CMAC, que vantagens práticas e repercussões na sua implementação argumentaria como vantagens ou desvantagens de utilizar CMACs como funções MAC em vez de funções do tipo HMAC.

Questão 3 (Fase 1)

Dado o formato de segurança da mensagem e a proteção dos dados (indicado na questão 1), suponha que se iria usar um formato diferente, como a seguir se indica

DADOS = { TYPE || uID || r1 || r2 || Dados da mensagem }$_{Ks}$ || MAC$_{Kh}$

c) Indique no seu código (ou a partir do seu código) onde e como alteraria a sua implementação para passar a suportar o formato indicado. Indique ao nível das instruções especificamente envolvidas e não mais do que essas.

d) Diga se a sua implementação continuaria a assegurar as mesmas propriedades de segurança caso adoptasse este formato. Justifique.

Questão 4 (Fase 2)

a) Na discussão das especificações para a Fase 2 de implementação do trabalho foram discutidas duas diferentes variantes possíveis para concretização do modelo baseado no protocolo de Needham-Schroeder, tendo em vista a distribuição e estabelecimento de parametrizações criptográficas na entrada de utilizadores numa sessão segura de Chat/Messagging.

   Qual das variantes foi usada ? Indique com base nas variantes indicadas a que foi usada, representando o protocolo.

e) Indique no seu código, onde é que o SSOServer está a enviar as parametrizações criptográficas a um cliente que vai entrar numa sessão, após ter verificado o controlo de acesso. Indique ao nível das instruções especificamente envolvidas e não mais do que essas.