



INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA

SEGURANÇA INFORMÁTICA

LICENCIATURA ENGENHARIA INFORMÁTICA E COMPUTADORES

FASE DE EXERCÍCIOS

Fase 1

Autores:

43552 - Samuel COSTA

43320 - André MENDES

Docente:

José SIMÃO

25 de Novembro de 2019

Conteúdo

| | | |
|-----|---------------------------------------|---|
| 1 | Introdução | 2 |
| 2 | Segunda série de exercícios | 3 |
| 2.1 | Exercício 1 | 3 |
| 2.2 | Exercício 2 | 3 |
| 2.3 | Exercício 3 | 3 |
| 2.4 | Exercício 4 | 3 |
| 2.5 | Exercício 5 | 3 |

1 Introdução

O trabalho realizado para esta fase pretende que os temas desenvolvidos durante as aulas sejam postos em prática. Para esta fase os exercícios focaram essencialmente a segunda parte da matéria.

- Autenticação baseadas em passwords
- Gestão de Identidade em Aplicações Web
- Modelos de Controlo de Acesso

Neste trabalho prático pretendemos responder aos vários exercícios propostos e implementar uma demonstração dos pontos referidos.

2 Segunda série de exercícios

2.1 Exercício 1

1.1

Um esquema de assinatura as chaves usadas são assimétricas o que permite a que autentica a mensagem usa a sua chave privada para o efeito e o recetor usa a chave publica do emissor para a autenticar essa mesma mensagem. Um esquema Mac como a chave é simétrica numa fase inicial através de um canal seguro teriam que ser trocadas para que desta forma ambos os intervenientes tenham a mesma chave para verificar a autenticidade da mensagem.

1.2

As recomendações do texto abordam fragilidades de segurança no caso de um atacante conseguir obter a chave privada de um servidor durante a sessão estabelecida entre o cliente e o servidor. No caso de um atacante obter a chave privada de um servidor passa a poder obter todas as mensagens dirigidas a ele, mas com a nova diretiva obriga a que a cada sessão durante a fase de *handshake* sejam estabelecidas novas chaves o que faz com que a chave do atacante deixe ter utilidade.

2.2 Exercício 2

O algoritmo simétrico para cifrar a *password* de um utilizador é criado através da função de *hash* com um valor aleatório unico a cada utilizador prevenindo assim que ataques de dicionario, ou seja, *passwords* iguais passam a ter valores de *hash* diferentes tornando a sua chave unica para cada utilizador. Para realizar a decifra realiza se o mesmo processo à *password* introduzida pelo utilizador, usa se o mesmo valor de *salt* e realiza se a comparação devolvendo um verdadeiro ou falso.

2.3 Exercício 3

2.4 Exercício 4

2.5 Exercício 5