Instituto Superior de Engenharia de Lisboa

Licenciatura em Engenharia Informática e de Computadores

Licenciatura em Engenharia Informática, Redes e Telecomunicações

Segurança Informática

Primeira série de exercícios, Semestre de Inverno de 18/19

Entregar até 21 de outubro de 2018

---

1. Considere a existência de um ataque à função de *hash* SHA1, baseado num algoritmo eficiente para: dado x, obter $x' \neq x$ tal que $H(x') = H(x)$. Quais as implicações deste ataque caso esta função seja usada num esquema de assinatura digital.

2. Considere o esquema CI para cifra e autenticidade de mensagens, onde $||$ representa a concatenação de bits e $X_{1..L}$ representa os primeiros L bits de X.

$$CI(m) = T(k_1)(m)||E_s(T(k_1)(m)_{1..L})(m)$$

   T é um esquema de *message authentication code* (MAC). E_s é um esquema simétrico de cifra, cuja dimensão da chave é L bits. Porque motivo este esquema não cumpre os objectivos?

3. Considere um novo modo de operação definido por:

   - Seja $x = x_1, \ldots, x_L$ a divisão nos blocos x_i do texto em claro x.
   - RV é um vector aleatório, com a dimensão do bloco, gerado por cada texto em claro x.
   - Seja $y_i = E(k)(x_i \oplus RV)$, para $i = 1, \ldots, L$, onde E é a operação de cifra, $\oplus$ denota o ou-exclusivo bit a bit.

   3.1. Defina o algoritmo de decifra para este modo de operação.

   3.2. Compare este modo de operação com o modo CBC quanto a: *a)* padrões do texto em claro passarem para o texto cifrado, *b)* capacidade de paralelizar a cifra.

4. Considere as infraestruturas de chave pública baseadas em certificados X.509.

   4.1. Considere uma cadeia de certificados composta pelos certificado folha C, os intermédios I_1, I_2, $\ldots$ I_n e a raiz R. Alguma das chaves privadas dos certificados intermédios é usada para validar o certificado C?

   4.2. Considere que a Alice tem o certificado C e a correspondente chave privada K_d. A Alice pode emitir novos certificados usando este material criptográfico? Se não, porquê, se sim, os certificados são válidos?

5. Considere o exercício "MD5 Collision Attack Lab" [3] dos laboratórios SEED [4]. Realize e apresente os resultados das tarefas 2.1, 2.2 e 2.3. Nas tarefa 2.2 e 2.3 inclua na entrega os dois ficheiros diferentes mas com valores iguais de MD5.

   Para este exercícios faça download da máquina virtual `SEEDUbuntu16.04.zip` *[1] e siga os passos indicados para a configuração da imagem no Virtual Box [2].*

6. Realize em Java uma implementação do esquema simétrico de cifra autenticada, cujo processo de proteção é descrito em seguida:

$$AE(k, m) = E(k)(m)||T(k)(E(k)(m))$$

   Para garantir confidencialidade use o algoritmo DES em modo *CBC* com padding *PKCS#5*, e o HMAC-SHA1 para autenticidade. A aplicação recebe na linha de comandos a opção para cifrar (`-cipher`) ou decifrar (`-decipher`), o ficheiro a proteger/desproteger (m), e um ficheiro com a chave (k). A aplicação produz o ficheiro protegido/desprotegido, e no caso da decifra deve também indicar se a mensagem é autêntica ou não. Na entrega inclua este enunciado cifrado e a chave utilizada.

7. Realize em Java uma implementação de um esquema de assinatura digital com a primitiva RSA. A aplicação recebe na linha de comandos a opção para assinar (`-sign`) ou verificar (`-verify`), a função de *hash* (`-sha1` ou `-sha256`) e o ficheiro para assinar/verificar.

   No modo de assinatura recebe i) *keystore* com a chave privada ii) `password` para aceder à *Keystore*; e produz um ficheiro só com a assinatura.

   No modo de verificação recebe i) ficheiro com a assinatura ii) certificado de quem assinou; e indica se a assinatura é válida ou não.

   Use o material criptográfico em anexo. Na entrega inclua a assinatura deste enunciado usando as chaves privadas de $Alice_1$ e Bob_2.

Referências

[1] http://www.cis.syr.edu/~wedu/seed/lab_env.html

[2] http://www.cis.syr.edu/~wedu/seed/Labs_16.04/Documents/SEEDVM_VirtualBoxManual.pdf

[3] http://www.cis.syr.edu/~wedu/seed/Labs_16.04/Crypto/Crypto_MD5_Collision/

[4] http://www.cis.syr.edu/~wedu/seed/Labs_16.04/