Protocolos Básicos

Troca de Chaves

- Uma técnica de criptografia é uso de chave de sessão.
- Chave de sessão é assim chamada por ser utilizada uma única vez para uma comunicação particular.
- Chave de sessão somente existe durante a comunicação.

Protocolos Básicos

Troca de chaves com criptografia simétrica

$A \rightarrow T$: Requisição K_S

$T \rightarrow A : E_{KA}(K_S) \,||\, E_{KB}(K_S)$

$A : D_{KA}(K_S)$

$A \rightarrow B : E_{KB}(K_S)$

$B : D_{KB}(K_S)$

$A \leftarrow E_{KS}(N+1) \rightarrow B$

Protocolos Básicos

Troca de chaves com criptografia assimétrica

$A \rightarrow T$: Requisição KU_B

$T \rightarrow A : KU_B$

$A : \text{Gera } K_S$

$A \rightarrow B : E_{KU_B}(K_S)$

$B : D_{KR_B}(K_S)$

$$A \leftarrow E_{K_S}(N+1) \rightarrow B$$

Ataque do homem do meio

Protocolos Básicos

Interlock Protocol, Ron Rivest and Adi Shamir

$A \rightarrow B : KU_A$

$B \rightarrow A : KU_B$ $\qquad A : E_{KU_B}(M_A)$

$A \rightarrow B : \{ E_{KU_B}(M_A) \} / 2$ $\qquad B : E_{KU_A}(M_B)$

$B \rightarrow A : \{ E_{KU_A}(M_B) \} / 2$

$A \rightarrow B : \{ E_{KU_B}(M_A) \} / 2´$ $\qquad B : D_{KR_B}(1 / 2 \,||\, 1 / 2´)$

$B \rightarrow A : \{ E_{KU_B}(M_B) \} / 2´$ $\qquad A : D_{KR_A}(1 / 2 \,||\, 1 / 2´)$

Protocolos Básicos

Troca de chaves e Mensagens

$B \rightarrow A : KU_B$

A : Gera K_S

$A : E_{K_S}(M)$

$A \rightarrow B : E_{K_S}(M) \;||\; E_{KU_B}(K_S)$

$B : D_{KR_B}(K_S)$

$B : D_{K_S}(M)$

Protocolos Básicos

Troca de chaves e Mensagens Compartilhadas

A : Gera K_S

$A : E_{K_S}(M)$

$A \rightarrow B,C,D : E_{K_S}(M) \;||\; E_{KU_C}(K_S) \;||\; E_{KU_D}(K_S) \;||\; E_{KU_D}(K_S)$

$B : D_{KR_B}(K_S)$ $\quad B : D_{K_S}(M)$

$C : D_{KR_C}(K_S)$ $\quad C : D_{K_S}(M)$

$D : D_{KR_D}(K_S)$ $\quad D : D_{K_S}(M)$

Protocolos Básicos

Criptografia com múltiplas chaves públicas

Alice K_A
Bob K_B
Carol K_C
Dave $K_A \wedge K_B$
Ellen $K_B \wedge K_C$
Frank $K_A \wedge K_C$

$$M = D_{Kbc} [E_{Ka}[M]]$$
$$M = D_{Kab} [E_{Kc}[M]]$$
$$M = D_{Kac} [E_{Kb}[M]]$$

Protocolos Básicos

Assinaturas Múltiplas

RSA

$n = p\ q$

$K_1 K_2 \ldots K_t \equiv 1 \bmod ((p-1) (q-1))$

$M^{K_1 K_2 \ldots K_t} = M$

$$(1)\ M' = M^{K_1} \bmod n$$
$$(2)\ M = M'^{K_2 K_3} \bmod n$$
$$(3)\ M'' = M'^{K_2} \bmod n$$
$$(4)\ M = M''^{K_3} \bmod n$$

Protocolos Básicos

Particionamento de Segredos

T : Gera R (random bit string tamanho de M)

T : S = M ⊕ R

T → A : R

T → B : S

A ^ B : M = R ⊕ S

Problema perda de R ou S

Protocolos Básicos

Particionamento de Segredos entre N Pessoas

T : Gera R, S, T (random bit string tamanho de M)

T : U = M ⊕ R ⊕ S ⊕ T

T → A : R

T → B : S

T → C : T

T → D : U

A ^ B ^ C ^ D : M = R ⊕ S ⊕ T ⊕ U

Protocolos Básicos

Compartilhamento de Segredos

- Com simples uso de criptotografia assimétrica

T : Gera K_S
T : E_{K_S} (M)
T : $M_1 = E_{KU_A}(E_{KU_B}(K_S))$
: $M_2 = E_{KU_A}(E_{KU_C}(K_S))$
: . . . .
: $M_n = E_{KU_{n-1}}(E_{KU_n}(K_S))$
T → B,C,D : $E_{K_S}(M) \;||\; M_1 \;||\; M_2 \;||\; . . . \;||\; M_n$

Protocolos Básicos

Compartilhamento de Segredos

- Esquema do limiar (***m***, ***n***) (qualquer ***m*** partes de um total de ***n***)

Interpolação Polinômial

p - número primo escolhido, onde
p > número de partes e *p* > maior segredo

Exemplo: (3, n)

$F(x) = (ax^2 + bx + M) \bmod p$

Partes: $k_i = F(x_i)$, para *n* pontos

polinômio de grau *m* – 1
a,b randômicos e descartados

Protocolos Básicos

Compartilhamento de Segredos

$F(x) = (7x^2 + 8x + 11) \bmod 13$

Partes

$k_1 = F(1) = 7 + 8 + 11 \equiv 0 \pmod{13}$
$k_2 = F(2) = 28 + 16 + 11 \equiv 3 \pmod{13}$
$k_3 = F(3) = 63 + 24 + 11 \equiv 7 \pmod{13}$
$k_4 = F(4) = 112 + 32 + 11 \equiv 12 \pmod{13}$
$k_5 = F(5) = 175 + 40 + 11 \equiv 5 \pmod{13}$

$a.2^2 + b.2 + M \equiv 3 \pmod{13}$
$a.3^2 + b.3 + M \equiv 7 \pmod{13}$
$a.5^2 + b.5 + M \equiv 5 \pmod{13}$

Protocolos Básicos

Esquemas de autenticação

são métodos através dos quais alguém pode provar sua identidade, sem revelar conhecimentos importantes e que possam ser usados de forma maliciosa no futuro.

A → S : senha
S : Hash (senha)
S : compara com valor previamente armazenado

ataque do dicionário

Protocolos Básicos

Autenticação com chave compartilhada “K”

$A \rightarrow B : N_A$

$B \rightarrow A : N_B \;||\; V = E_K (N_A \;||\; N_B \;||\; ID_B)$

$A : V == E_K (N_A \;||\; N_B \;||\; ID_B) ?$

$A \rightarrow B : Q = E_K (N_B \;||\; ID_A)$

$B : Q == E_K (N_B \;||\; ID_A) ?$

Protocolos Básicos

Autenticação arbitrada “T”

$A \rightarrow T : ID_A \;||\; E_{KA} (T_A \;||\; K_S \;||\; ID_B)$

$T \rightarrow B : E_{KB} (T_B \;||\; K_S \;||\; ID_A)$

KA e KB compartilhadas com T

Protocolos Básicos

Yahalom

$A \rightarrow B : ID_A \,||\, N_A$

$B \rightarrow T : ID_B \,||\, E_{KB}(ID_A, N_A, N_B)$

$T \rightarrow A : E_{KA}(ID_B, K_S, N_A, N_B) \,||\, E_{KB}(ID_A, K_S)$

$A \rightarrow B : E_{KB}(ID_A, K_S) \,||\, E_{KS}(N_B)$

$B : D_{KB}(E_{KB}(ID_A, K_S))$

$D_{KS}(E_{KS}(N_B))$

Protocolos Básicos

Needham-Schroeder

$A \rightarrow T : ID_A \,||\, ID_B \,||\, N_A$

$T \rightarrow A : E_{KA}(N_A \,||\, ID_B \,||\, K_S) \,||\, E_{KB}(K_S \,||\, ID_A)$

$A \rightarrow B : E_{KB}(K_S, ID_A)$

$B \rightarrow A : E_{KS}(N_B)$

$A \rightarrow B : E_{KS}(N_B - 1)$

Protocolos Básicos

Kerberos

$A \rightarrow T : ID_A, ID_B$

$T \rightarrow A : E_{KA} (N \,||\, K_S \,||\, ID_B) \,||\, E_{KB} (N \,||\, K_S \,||\, ID_A)$

$A \rightarrow B : E_{KS} (ID_A, N) \,||\, E_{KB} (N \,||\, K_S \,||\, ID_A)$

$B \rightarrow A : E_{KS} (N+1)$

Protocolos Básicos

Autenticação com chave pública

$A \rightarrow B : N$

$B \rightarrow A : E_{KR_B} (N) \;||\; ID_B$

$A : N == D_{KU_B} (E_{KR_B} (N)) ?$

Ataque do homem do meio