Avaintenhallinta

- Avain on kryptografisten järjestelmien keskeinen osa.
- Avainten pitää olla **aitoja** ja salaisten avainten **salaisia**.
- Avaimia välitetään **avaintenhallintaprotokollilla**.
- Kryptografista protokollaa ei kannata itse suunnitella, jos ei ole pakko — aivan kuin algoritmiakaan.
- Avaintenvaihto, avaintenjakelu, *key establishment, key agreement, key distribution/transport*

  Protokollat käyttävät sekä salaisen että julkisen avaimen algoritmeja.

Istuntoavain

- Istuntoavain on (yleensä) salainen avain, jota käytetään vain **yhden istunnon ajan istunnon sisällön suojaamiseen.**

  Istuntoavaimista sovitaan tai ne jaetaan erityisillä avaintenjakeluprotokollilla.

  Istuntoavaimia voi olla useita eri tarkoituksiin, esim. salaukseen ja integriteettitarkistukseen eri suuntaisilla kanavilla.

  Istuntoavain generoidaan ja/tai välitetään salaisen **pääavaimen** tai julkisten avainten avulla.

- Istuntoavaimia tarvitaan, koska
  - tarvitaan jaettu salainen avain, eikä sitä ennestään ole
  - tarvitaan toistuvasti uusia avaimia tai useita avaimia eri tarkoituksiin
  - salataan suuria tietomääriä, jolloin kryptoanalyysi helpottuu.

- Istuntoavaimen paljastuminen ei saa vaarantaa pääavainta.

  Vanhojen istuntoavaimien paljastuminen ei saa vaarantaa uusia eikä uusien vanhoja.

  Parhaassa tapauksessa pääavaimelle ei ole saatavilla tunnettua selväkieltä.

Yksinkertainen yritelmä

- Alice haluaa yhteisen istuntoavaimen Bobin kanssa.

$$\boxed{1. \quad A \to B: \quad A, K_{SES}}$$

Hyvä?

- Salataan istuntoavain Alicen ja Bobin välisellä **pääavaimella** (*master key*) .

$$\boxed{1. \quad A \to B: \quad A, E_{AB}(K_{SES})}$$

Avaintenhallinnan ensimmäinen tavoite on salaisten avainten salassa pysyminen. Se saavutetaan salauksella.

Joko kelpaa?

Sanomien rakennusosat

A, ID_A, B, T	protokollaosapuolien nimet tai tunnisteet
R_A	A:n generoima satunnaisluku
N_A	A:n generoima nonssi
T_A	A:n aikaleima
K_{AB}, K_{SES}	istuntoavain
K_{AT}	A:n ja T:n välinen pääavain
K_A	A:n julkinen tai salainen avain
K_A^+, K_A^-	A:n julkinen ja yksityinen avain
$E_K(M)$	salaus avaimella K
$E_{AB}(M)$	salaus avaimella K_{AB}
$E_A(M)$	salaus A:n julkisella tai salaisella avaimella
$MAC_K(M)$	avaimella K laskettu MAC
$S_A(M)$	A:n allekirjoitus
$h(M)$	yksisuuntainen funktio

- Allekirjoistus liitetään sanoman perään $M, S_A(M)$ tai lähetetään erikseen $S_A(M)$.

  Allekirjoitettua sanomaa merkitään myös $S_A(M)$ tai $\{M\}_A$.

- Salausta merkitään monin tavoin:

  $E_{K_{A,B}}(sanoma) = E_{AB}(sanoma) = E_{K_{AB}}[sanoma] = E(K_{A,B}; sanoma) = (sanoma)_{K_{A,B}} = K_{A,B}(sanoma)$.

  Salauksen oletetaan usein estävän sanoman muuntelun.

Wide-mouth-frog

(Oletetaan salauksen E estävän sanoman hallitun muuntelun.)

1.	$A \rightarrow T:$	$A, E_A(T_A, B, K_{SES})$
2.	$T \rightarrow B:$	$E_B(T_T, A, K_{SES})$

Schneier ei näe protokollassa suurta vikaa. Entä sinä?

- Toistohyökkäys *Wide-Mouth Frog*-protokollaa vastaan:

$$
\begin{array}{ll}
A \rightarrow T: & A, E_A(T_A, B, K_{SES}) \\
T \rightarrow B: & E_B(T_T, A, K_{SES}) \\
M(B) \rightarrow T: & B, E_B(T_T, A, K_{SES}) \\
T \rightarrow M(A): & E_A(T_{T2}, B, K_{SES}) \\
M(A) \rightarrow T: & A, E_A(T_{T2}, B, K_{SES}) \\
T \rightarrow M(B): & E_B(T_{T3}, A, K_{SES}) \\
M(B) \rightarrow T: & B, E_B(T_{T4}, A, K_{SES}) \\
T \rightarrow M(A): & E_B(T_{T5}, B, K_{SES}) \\
\ldots & \\
M \rightarrow T: & A, E_B(T_{T1234}, A, K_{SES}) \\
T \rightarrow B: & E_B(T_{T1234}, A, K_{SES})
\end{array}
$$

Mallory voi pitää avaimen K_{SES} elossa mielivaltaisen pitkään.

Tuomas Aura TKK / Digitaalitekniikka

Salaisen avaimen Needham-Schröder

- Needham–Schröder-protokolla (1978–1981) oli ensimmäinen julkaistu salausta käyttävä avaintenhallintaprotokolla.

  (Oletetaan salauksen E estävän sanoman hallitun muuntelun.)

1.	$A \rightarrow T:$	A, B, N_A	
2.	$T \rightarrow A:$	$E_A(N_A, B, K_{SES}, E_B(K_{SES}, A))$	
3.	$A \rightarrow B:$	$E_B(K_{SES}, A)$	
4.	$B \rightarrow A:$	$E_{K_{SES}}(N_B)$	haaste
5.	$A \rightarrow B:$	$E_{K_{SES}}(N_B + 1)$	vaste

Sanomilla 4 ja 5 Bob varmistuu, että Alice tuntee avaimen (*key confirmation*) .

- Toistohyökkäys: Mallory nauhoittaa sanoman $E_B(K_{SES}, A)$. Myöhemmin hän saa haltuunsa vanhan istuntoavaimen K_{SES}.

$$
\begin{array}{ll}
M(A) \rightarrow B: & E_B(K_{SES}, A) \\
B \rightarrow M(A): & E_{K_{SES}}(N'_B) \\
M(A) \rightarrow B: & E_{K_{SES}}(N'_B + 1)
\end{array}
$$

Denning–Sacco

- Denning–Sacco-protokollassa (1981–1994) Alice pyytää Trentiltä sertifikaatin omalle ja Alicen julkiselle avaimelle.

  DS käyttää julkisen avaimen algoritmeja.

$$
\begin{array}{lll}
1. & A \to T: & A, B \\
2. & T \to A: & B, K_B, S_T(B, K_B),\ A, K_A, S_T(A, K_A) \\
3. & A \to B: & E_B(T_A, K_{SES}, S_A(T_A, K_{SES})), \\
 & & \quad B, K_B, S_T(B, K_B),\ A, K_A, S_T(A, K_A)
\end{array}
$$

Normaalin protokolla-ajon jälkeen Bob jatkaa:

$$
\begin{array}{ll}
B \to T: & B, C \\
T \to B: & C, K_C, S_T(C, K_C),\ B, K_B, S_T(B, K_B) \\
B(A) \to C: & E_C(T_A, K_{SES}, S_A(T_A, K_{SES})), \\
 & \quad C, K_C, S_T(C, K_C),\ A, K_A, S_T(A, K_A)
\end{array}
$$

Charlie luulee nyt, että K_{SES} on hänen ja Alicen yhteinen avain. Tosiasiassa se on Bobin ja Charlien välinen.

Meyer–Matyas

- Meyer–Matyas-protokollassa palvelin kertoo pyynnöstä julkisen avaimen. Avain liitetään pyyntöön nonssilla. Yksinkertaistettu versio:

$$
\begin{array}{lll}
1. & A \to T: & A, B, N_A \\
2. & T \to A: & S_T(K_B, N_A)
\end{array}
$$

- Henkilön nimeä ei ole kunnolla liitetty avaimeen.

$$
\begin{array}{ll}
A \to T: & A, B, N_A \\
T \to M(A): & S_T(K_B, N_A) \\
M(A) \to T: & A, M, N_A \\
T \to A: & S_T(K_M, N_A)
\end{array}
$$

Mallory voi esiintyä Alicelle Bobina. Jos hän myös esiintyy Bobille Alicena, on kyseessä *man-in-the-middle*-hyökkäys.

Julkisen avaimen Needham-Schröder

- Julkisen avaimen NS-protokollassa (1978–1995) Alice ja Bob hankkivat toistensa julkiset avaimet Trentiltä ja vaihtavat avainmateriaalia N_A, N_B.

1.	$A \longrightarrow T$	A, B
2.	$T \longrightarrow A$	$K_B^+, B, S_T(K_B^+, B)$
3.	$A \longrightarrow B$	$E_B(N_A, A)$
4.	$B \longrightarrow T$	B, A
5.	$T \longrightarrow B$	$K_A^+, A, S_T(K_A^+, A)$
6.	$B \longrightarrow A$	$E_A(N_A, N_B)$
7.	$A \longrightarrow B$	$E_B(N_B)$

Istuntoavain voidaan generoida nonsseista: $K_{SES} = h(N_A, N_B)$.

Heikkous 1: Trentiltä saadut sertifikaatit voivat olla vanhoja.

- Oletetaan Alicen ja Bobin jo tuntevan toistensa julkiset avaimet:

1.	$A \longrightarrow B$	$E_B(N_A, A)$
2.	$B \longrightarrow A$	$E_A(N_A, N_B)$
3.	$A \longrightarrow B$	$E_B(N_B)$

Heikkous 2: Hyökkääjä pystyy siirtämään A:n autentikoinnin B:lle.

$$A \longrightarrow M: \quad E_M(N_A, A) \quad (1)$$
$$M(A) \longrightarrow B: \quad E_B(N_A, A) \quad (1')$$
$$B \longrightarrow M(A): \quad E_A(N_A, N_B) \quad (2')$$
$$M \longrightarrow A: \quad E_A(N_A, N_B) \quad (2)$$
$$A \longrightarrow M: \quad E_M(N_B) \quad (3)$$
$$M \longrightarrow B: \quad E_B(N_B) \quad (3')$$

Bob luulee olevansa yhteydessä Alicen kanssa, mutta onkin yhteydessä Malloryn kanssa. Mallory myös tuntee nonssit ja niistä generoitavan istuntoavaimen.