8. poglavje

Distribucija in uskladitev ključev

- Distribucija ključev
- Blomova shema
- Diffie-Hellmanova distribucija ključev
- Kerberos
- Uskladitev ključev
- Diffie-Hellmanova shema
- MTI protokoli
- Giraultova shema

Sistemi z javnimi ključi imajo prednost pred sistemi s tajnimi ključi, saj za izmenjavo tajnih ključev ne potrebujejo varnega kanala.

Večina sistemov z javnimi ključi (npr. RSA) je tudi do 100-krat počasnejša od simetričnih sistemov (npr. DES). Zato v praksi uporabljamo za šifriranje *daljših* besedil simetrične sisteme.

Obravnavali bomo več različnih protokolov za tajne ključe. Razlikovali bomo med *distribucijo ključev* in *uskladitvijo ključev*.

Sistem distribucije ključev je mehanizem, kjer na začetni stopnji verodostojna agencija generira in distribuira tajne podatke uporabnikom tako, da lahko vsak par uporabnikov kasneje izračuna ključ, ki je nepoznan ostalim.

Uskladitev ključev označuje protokol, kjer dva ali več uporabnikov sestavjo skupen tajni ključ, s komunikacijo po javnem kanalu. Vrednost ključa je določena s funkcijo vhodnih podatkov.

Center zaupanja

Imamo omrežje, ki ni varno in na katere
uporabnikov. V nekaterih shemah se pojavi a
ki je odgovorna za

- potrjevanje identitete (avtorizacijo),
- izbiro in prenos ključev
- itd.

Rekli ji bomo **center zaupanja** ali **verodo**
agencija (angl. Trusted Authority – TA ali
Third Party – TTP).

Uporabljali bomo kar oznako **TA**.

Obstaja potreba po zaščiti pred potencialnimi nasprotniki, tako pasivnimi kot tudi aktivnimi.

Pasivni sovražnik je osredotočen na prisluškovanje sporočilom, ki se pretakajo po kanalu.

Več nevšečnosti nam lahko naredi *aktivni* sovražnik:

- spreminjanje sporočil,
- shranjevanje sporočil za kasnejšo uporabo,
- maskiranje v uporabnika omrežja.

Naj bosta U in V uporabnika omrežja.

Cilj *aktivnega* sovražnika je lahko:

- prelisičiti U in V tako, da sprejmeta neveljaven ključ kot veljaven,
- prepričati U in V, da sta si izmenjala ključ, čeprav si ga v resnici nista.

Distribucija ključev

– omrežje z n uporabniki,
– agencija TA generira in preda enolično določen ključ vsakemu paru uporabnikov omrežja.

Potrebujemo varen kanal med TA in vsakim uporabnikom omrežja. Vsak posameznik dobi $n-1$ ključev, zahtevnost problema pa je vsaj $\mathcal{O}(n^2)$, zato ta rešitev ni praktična celo za relativno majhne n.

Želimo si boljšo rešitev, npr. z zahtevnostjo $\mathcal{O}(1)$.

Blomova shema

Naj bo javno p praštevilo večje od danega n
naj bo $k \in \mathbb{N}$ za katerega velja $k \leq n-2$.

TA pošlje po varnem kanalu $k+1$ elementov
osebi in nato si lahko vsak par $\{U, V\}$ izraču
ključ $K_{U,V} = K_{V,U}$.

Število k je velikost največje koalicije, proti k
shema še vedno varna.

Paul R. Halmos

"...the source of all great mathematics is the special case, the concrete example. It is frequent in mathematics that every instance of a concept of seemingly great generality is in essence the same as a small and concrete special case."

I Want to be a Mathematician, Washington: MAA Spectrum, 1985.

???

" Sometimes a research is a lot of hard work in looking for the easy way."

David Hilbert (-1900)

"The art of doing mathematics consists in finding that special case which contains all the germs of generality."

Najprej opišimo shemo v primeru, ko je $k = 1$.

- *Izberemo javno praštevilo p.*
- *TA izbere tri naključne elemente $a, b, c \in \mathbb{Z}_p$ (ne nujno različne) in oblikuje polinom*

$$f(x, y) = a + b(x + y) + c\,xy \mod p.$$

- *Za vsakega uporabnika U izbere TA javni $r_U \in \mathbb{Z}_p$, tako da so le-ti medseboj različni.*

- *Za vsakega uporabnika U izračuna TA p*

$$g_U(x) = f(x, r_U) \bmod p$$

in mu ga pošlje po varnem kanalu.

Opomnimo, da je $g_U(x)$ linearen polinom, tak
lahko zapišemo v naslednji obliki

$$g_U(x) = a_U + b_U x,$$

kjer je

$$a_U = a + br_U \bmod p \quad \text{in} \quad b_U = b + cr_U$$

- *Za medsebojno komunikacijo osebi U in V uporabita ključ*

$$\begin{aligned} K_{U,V} = K_{V,U} &= f(r_U, r_V) \\ &= a + b(r_U + r_V) + c\,r_U r_V \bmod p. \end{aligned}$$

Uporabnika U in V izračunata svoja ključa $K_{U,V}$ in $K_{U,V}$ zaporedoma s

$$f(r_U, r_V) = g_U(r_V) \quad \text{in} \quad f(r_U, r_V) = g_V(r_U).$$

Izrek 1. *Blomova shema za $k = 1$ je brezpogojno varna pred posameznimi uporabniki.*

Dokaz: Recimo, da želi uporabnik W izračunati ključ

$$K_{U,V} = a + b(r_U + r_V) + c\,r_U r_V \bmod p.$$

Vrednosti r_U in r_V so javne, a, b in c pa ne.
Oseba W pozna vrednosti

$$a_W = a + br_W \bmod p \quad \text{in} \quad b_W = b + cr_W \bmod p,$$

ker sta to koeficienta polinoma $g_W(x)$, ki ju je dobila od agencije TA.

Pokažimo, da je informacija, poznana osebi W, konsistentna s poljubno vrednostjo $\ell \in \mathbb{Z}_p$ za ključ $K_{U,V}$, tj. W ne more izločiti nobene vrednosti za $K_{U,V}$.

Poglejmo si naslednjo matrično enačbo v $(\mathbb{Z}_p)$:

$$\begin{pmatrix} 1 & r_U + r_V & r_U\,r_V \\ 1 & r_W & 0 \\ 0 & 1 & r_W \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} \ell \\ a_W \\ b_W \end{pmatrix}.$$

Prva enačba vsebuje hipotezo, da je $K_{U,V} = \ell$, drugi dve enačbi pa sledita iz definicije števil a_W in b_W.

Determinanta zgornje matrike je

$$r_W^2 + r_U r_V - (r_U + r_V) r_W = (r_W - r_U)(r_W$$

Iz $r_W \neq r_U$ in $r_W \neq r_V$ sledi, da je deter
različna od nič in zato ima zgornji sistem
rešitev za a, b in c.

Koalicija uporabnikov $\{W, X\}$ pa ima štiri en
tri neznanke in od tod zlahka izračuna a, b
končno še polinom $f(x, y)$, s katerim dobi vsa

■

Posplošitev

Za splošno shemo (tj. shemo, ki je varna pred koalicijo velikosti k) je potrebna ena sama sprememba. Pri drugem koraku TA uporablja polinom $f(x, y)$ naslednje oblike

$$f(x, y) = \sum_{i=0}^{k} \sum_{j=0}^{k} a_{ij} x^i y^j \mod p,$$

kjer je $a_{ij} \in \mathbb{Z}_p$ za $0 \leq i, j \leq k$ in $a_{ij} = a_{ji}$ za vsak i, j. Ostali del protokola se ne spremeni.

Diffie-Hellmanova distribucija ključev

Delali bomo v $\mathbb{Z}_p$, p je praštevilo, z generatorjem α.

Naj bo ID(U) oznaka za določeno informacijo, ki enolično identificira osebo U (npr. ime, e-pošta, telefonska številka itd).

Vsak uporabnik si izbere tajni $a_U \in \{0, 1, \ldots, p-2\}$, in naj bo

$$b_U = \alpha^{a_U} \bmod p.$$

Agancija TA si izbere shemo za digitalni podpis z javnim algoritmom za preverjanje podpisov $\mathrm{ver}_{\mathrm{TA}}$ in tajnim algoritmom za podpisovanje $\mathrm{sig}_{\mathrm{TA}}$.

Nazadnje privzemimo še, da so vse informacije zgoščene z javno zgoščevalno funkcijo, preden jih podpišemo, vendar pa zaradi estetskih razlogov ne bomo omenjali zgoščevalne funkcije pri opisu protokolov.

Za osebo U bo agancija TA izdala naslednji **certifikat**:

$$C(U) = (\, \mathrm{ID}(U),\, b_U, \mathrm{sig}_{\mathrm{TA}}(\mathrm{ID}(U),\, b_U)\,)$$

(TA ne potrebuje a_U).

- *Izberemo javno praštevilo p in javen primitivni element $\alpha \in \mathbb{Z}_p^*$.*
- *Oseba V izračuna*

  $$K_{U,V} = \alpha^{a_U a_V} \bmod p \;=\; b_U^{a_V} \bmod$$

  z uporabo javne vrednosti b_U iz certifik
  osebe U in s svojo zasebno vrednostjo
- *Oseba U izračuna*

  $$K_{U,V} = \alpha^{a_U a_V} \bmod p \;=\; b_V^{a_U} \bmod$$

  z uporabo javne vrednosti b_V iz certifik
  osebe V in s svojo zasebno vrednostjo

Podpis agencije TA preprečuje osebi W, da spreminja certifikate, torej je dovolj preprečiti pasivne napade.

Ali lahko oseba W izračuna $K_{U,V}$, če je $W \neq U, V$, tj, če poznamo $\alpha^{a_U} \bmod p$ in $\alpha^{a_V} \bmod p$ ne pa tudi a_U ali a_V, ali je mogoče izračunati $\alpha^{a_U a_V} \bmod p$?

To bomo imenovali **Diffie-Hellmanov** problem.

Očitno je **Diffie-Hellmanova distribucija ključev** varna natanko tedaj, ko je varen **Diffie-Hellmanov** problem.

Izrek 2. *Razbitje ElGamalovega kriptosistema je ekvivalentno reševanju Diffie-Hellmanovega problema.*

Dokaz: Spomnimo se, kako potekata ElGamalovo šifriranje in odšifriranje. Ključ je $K = (p, \alpha, a, \beta)$, kjer $\beta = \alpha^a \bmod p$ (a je tajni in p, α in β so javni). Za tajno naključno število $k \in \mathbb{Z}_{p-1}$ je

$$e_K(x, k) = (y_1, y_2),$$

kjer $y_1 = \alpha^k \bmod p$ in $y_2 = x\beta^k \bmod p$.

Za $y_1, y_2 \in \mathbb{Z}_p^*$ je $d_K(y_1, y_2) = y_2(y_1^a)^{-1} \bmod p$.

Predpostavimo, da imamo algoritem A, ki reši Diffie-Hellmanov problem in podano ElGamalovo šifriranje (y_1, y_2). Z uporabo algoritma A na podatkih p, α, y_1 in β dobimo vrednost

$$A(p, \alpha, y_1, \beta) = A(p, \alpha, \alpha^k, \alpha^a) =$$
$$= \alpha^{ka} \bmod p = \beta^k \bmod p.$$

Potem odšifriranje (y_1, y_2) lahko enostavno izračunamo:

$$x = y_2(\beta^k)^{-1} \bmod p.$$

Predpostavimo, da imamo še algoritem B,
ElGamalovo odšifriranje. Torej B vzame
p, α, β, y_1 in y_2 in izračuna

$$x = y_2(y_1^{\log_\alpha \beta})^{-1} \bmod p.$$

Naj bodo p, α, β in γ podatki Diffie-Hellm
problema. Torej je $\beta = \alpha^b$ in $\gamma = \alpha^c$ za neka
ki nista poznana, pa vendar lahko izračunamo

$$(B(p, \alpha, \beta, \gamma, 1))^{-1} = (1(\gamma^{\log_\alpha \beta})^{-1})^{-1} \bmod$$
$$= \gamma^{\log_\alpha \beta} \bmod p = \alpha^{c \cdot b} \bmod p,$$

torej DH-ključ, kar smo tudi želeli.