SEMINAR IZ KRIPTOGRAFIJE

Porazdelitev in uskladitev ključev (nadaljevanje)

Erik Schlegel

FMF

15. junij, 1998

Na zadnjem seminarju:

- Porazdelitev ključev
  - Blomova shema
  - Diffie-Hellmanova shema
  - Kerboros
- Reševanje nalog

Današnji načrt

- Uskladitev ključev
  - Diffie-Hellmanova shema
  - MTI protokoli
  - Giraultova shema
- Reševanje nalog

Diffie-Hellmanova izmenjava ključa

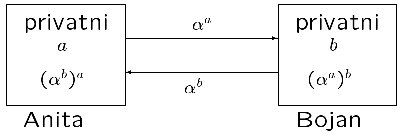
- U izbere naključen a_U, $0 \leq a_U \leq p-2$.
- U izračuna $\alpha^{a_U} \bmod p$ in pošlje V-ju.
- V izbere naključen a_V, $0 \leq a_V \leq p-2$.
- V izračuna $\alpha^{a_V} \bmod p$ in pošlje U-ju.
- U izračuna

$$K = (\alpha^{a_V})^{a_U} \bmod p$$

in V izračuna

$$K = (\alpha^{a_U})^{a_V} \bmod p.$$

IZMENJAVA KLJUČEV
(Diffie-Hellman)



Anita in Bojan si delita skupni element grupe: $(\alpha^a)^b = (\alpha^b)^a = \alpha^{ab}$.

Varnost Diffie-Hellmanovega protokola

Protokol ni varen pred aktivnim sovražnikom, ki uporablja napad vrinjenja na sredino. S tem prestreže sporočila in jih nadomesti s svojimi. Uporabnika hočeta biti sigurna v medsebojno izmenjavo sporočil, zato potrebujeta ločljiv protokol za medsebojno identifikacijo. Dobro je, da poteka identifikacija istočasno z uskladitvijo ključa, saj je s tem aktivnost aktivnega sovražnika onemogočena.

Overitev uskladitve ključa

Protokol od uporabnika do uporabnika je protokol overitve uskladitve kjuča in je modifikacija Diffie-Hellmanove izmenjave ključa.

Vsak uporabnik ima certifikat

$$C(U) = (ID(U), ver_U, sig_{TA}(ID(U), ver_U)),$$

kjer je shranjena identifikacija uporabnika.

Poenostavljen protokol od uporabnika do uporabnika

- U izbere naključen a_U, $0 \leq a_U \leq p-2$.
- U izračuna $\alpha^{a_U} \bmod p$ in pošlje V-ju.
- V izbere naključen a_V, $0 \leq a_V \leq p-2$.
- V izračuna $\alpha^{a_V} \bmod p$.
  Potem izračuna

$$K = (\alpha^{a_U})^{a_V} \bmod p$$

in

$$y_V = sig_V(\alpha^{a_V}, \alpha^{a_U}).$$

- V pošlje $(C(V), \alpha^{a_V}, y_V)$ U-ju.

- U izračuna

$$K = (\alpha^{a_V})^{a_U} \bmod p.$$

Preveri y_V z uporabo ver_V in $C(V)$ z uporabo ver_{TA}.
- U izračuna

$$y_U = sig_U(\alpha^{a_U}, \alpha^{a_V})$$

in pošlje $(C(U), y_U)$ V-ju.
- V preveri y_U z uporabo ver_U in $C(U)$ z uporabo ver_{TA}.

Varnost protokola STS

Poenostavljen STS protokol je varen pred sovražnikom, ki uporablja sredinski napad. Izkaže se, da aktivni sovražnik ne more izračunati podpisa, ker ne pozna podpisnega algoritma uporabnika na liniji.
Še nekaj, tako oblikovan protokol ne vsebuje potrditve ključa, kot je to narejeno v Kerborosovi shemi. Protokol, v katerem je vključena potrditev ključa, se imenuje STS protokol.

MTI protokoli

Matsumoto, Takashima, Imai - avtorji

Modifikacije Diffie-Hellmanove izmenjave ključa.

Uporabniki ne računajo podpisov, dvo prehodni protokoli.

Eden od njih je naslednji (osnovne predpostavke so iste kot pri Diffie-Hellmanovi porazdelitvi ključa): vsak uporabnik bo imel svoj certifikat oblike

$$C(U) = (ID(U), b_U, sig_{TA}(ID(U), b_U)).$$

MTI protokol

- U izbere naključen r_U, $0 \leq r_U \leq p-2$ in izračuna

$$s_U = \alpha^{r_U} \bmod p.$$

- U pošlje $(C(U), s_U)$ V-ju.
- V izbere naključen r_V, $0 \leq r_V \leq p-2$ in izračuna

$$s_V = \alpha^{r_V} \bmod p.$$

- V pošlje $(C(V), s_V)$ U-ju.
- U izračuna

$$K = s_V^{a_U} b_V^{r_U} \bmod p,$$

kjer je vrednost b_V iz $C(V)$.
V izračuna

$$K = s_U^{a_V} b_U^{r_V} \bmod p,$$

kjer je vrednost b_U iz $C(U)$.

Varnost protokola MTI

Pred pasivnimi sovražniki je enako varen kot Diffie-Hellmanov problem.

Varnost pred aktivnimi sovražniki je bolj vprašljiva. Brez uporabe podpisnega algoritma nismo varni pred sredinskimi napadi.

Ključ komunicirajočih uporabnikov je težko izračunati, ker je v ozadju težko izračunljiv diskretni logaritem.

Lastnost implicitne overitve ključa.

Uskladitev ključa z uporabo ključev za osebno overitev

Shema ne zahteva certifikatov. Javni kjuč in identiteta lastnika implicitno razlikuje uporabnike.

Giraultova shema vsebuje poteze sheme RSA in diskretnega logaritma.

Uporabnik ima identifikacijsko besedo ID. Javni ključ za osebno overitev dobi od strežnika TA.

Javni ključ za osebno overitev

- U izbere tajni eksponent a_U in izračuna

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

- U da a_U in b_U strežniku TA.
- TA izračuna

$$p_U = (b_U - ID(U))^d \bmod n.$$

- TA da p_U U-ju.

$n = p\,q$, kjer je $p = 2p_1 + 1$, $q = 2q_1 + 1$, in p, q, p_1, q_1 so velika praštevila.

$$(\mathbb{Z}_n^*, \cdot) \simeq (\mathbb{Z}_p^* \times \mathbb{Z}_q^*, \cdot)$$

$\alpha \in \mathbb{Z}_n^*$ reda $2p_1q_1$. Ciklična podgrupa v $\mathbb{Z}_p^*$ z generatorjem α je primerna zasnova za problem diskretnega logaritma.

n, α javni, p, q, p_1, g_1 tajni. e, javni RSA šifrirni eksponent, izbere ga TA. $d = e^{-1} \bmod \Phi(n)$, tajni dešifrirni eksponent.

Giraultov protokol uskladitve ključa

- U izbere naključen r_U in izračuna
$$s_U = \alpha^{r_U} \bmod n.$$
- U pošlje ID(U), p_U in s_U V-ju.
- V izbere naključen r_V in izračuna
$$s_V = \alpha^{r_V} \bmod n.$$
- V pošlje ID(V), p_V in s_V U-ju.
- U izračuna $K = s_V^{a_U}(p_V^e + ID(V))^{r_U} \bmod n$;
V izračuna $K = s_U^{a_V}(p_U^e + ID(U))^{r_V} \bmod n$.

Varnost Giraultovega protokola

Ključ za osebno overitev varuje pred sovražniki.

Protokol vsebuje implicitno overitev ključa, torej smo varni pred sredinskimi napadi.

Strežnik TA je prepričan, da uporabnik pozna vrednost a predno izračuna ključ za osebno overitev.