Univerziteta v Ljubljani
Fakulteta za računalništvo
Smer IŠRM

Matej Ugrin 63040302

Overjeni protokoli za izmenjavo ključev

Seminarska naloga pri predmetu Kriptografija in teorija kodiranja 2

Abstract

V naslednjih straneh smo opisali značilnosti overjenih protokolov za izmenjevanje ključev, varnostne predpostavke in lastnosti, ki jih upoštevamo pri njihovem razvoju. V prvem delu seminarske naloge je podan pregled uporabe kriptografije javnih ključev, v drugem delu pa smo s prikazom napada na neoverjen protokol želeli prikazati njegove pomanjkljivosti. V nadaljevanju smo opisali štiri možne različice tristranskega TAK overjenega protokola in se prepričali ali izpolnjujejo lastnosti overjenih protokolov.

Cilj: Predstavitev overjenih protokolov za izmenjavo ključev, tristranski TAK protokol in njegove pomanjkljivosti

Predavatelj: prof. dr. Aleksandar Jurišić

š.l 2009/2010

Contents

1 Uvod

S povečevanjem internetnih aplikacij in storitev, se povečuje potreba po zaupnosti podatkov in avtentikaciji uporabnikov udeleženem v procesu. Izmenjevanje ključev je poleg ekripcije in digitalnih podpisov, eno izmed temeljnih gradnikov kriptografije. Takšni protokoli nam omogočajo, da se preko nezaščitenega komunikacijskega kanala odvija izmenjava in sporazum glede varnega ključa, s katerim lahko v naslednjih korakih zaščitimo povezavo. Poleg tega overjeni protokoli za izmenjavo omogočajo prepoznavenje avtentičnosti udeleženca. Pri razvoju takšnih protokolov lahko izberemo različne pristope izgradnje, ki pa posledično vplivajo na njihovo varnost in učinkovitost. Slednje je tudi glavni cilj pri njihovem razvoju, pozorni pa moramo biti tudi na izpolnjevanje varnostnih predpisov, ki jih bomo opisali v nadaljevanju.

Protokole kjer se dva udeleženca dogovarjata o skupnem ključu delimo na protokole, kjer ključ generira en udeleženec in nato ključ posreduje po varnem kanalu do drugega in na protokole kjer je sestava ključa odvisna od informacij, ki jih imajo v lasti udeleženci. V simetričnih protokolih udeleženca že vnaprej poznata skrivni ključ, medtem ko v asimetričnih protokolih poznata le javno overjene informacije, potrjene s strani izdajatelja.

Seminarsko nalogo predstavljajo trije deli. Prvi del obsega predstavitev javne kriptografije, njene začetke in različne načine uporabe. V drugem delu smo opisali značilnosti overjenih protokol, nanizali njihove definicije ter želene lastnosti, ki jih upoštevamo pri njihovem razvoju. V poglavju smo kot motivacijo podali napad na Jouxov protokol in opisali izboljšan overjen tristranski Al-Riyami-Petersonov protokol s štirimi različicami generiranja ključev. V nadaljevanju smo se osredotočili na protokola $TAK3$ in $TAK4$ in njuno analizo glede na najpogostejše ranljivosti v overjenih protokolih.

1.1 Uporaba kriptografije javnih ključev

Ena izmed želenih kriptografskih lastnosti v omrežju je ta, da podatke zaščitimo s pomočjo enkripcije. Omenjeno zaščito ponujajo algoritmi simetrične kriptografije, ki pa za svoje delovanje uporabljajo izmenjavo ključev preko zaščitenih kanalov. Z uporabo kriptografije javnih ključev se problemu zaščitenih kanalov izognemo, saj so za dogovor o ključu potrebne le javno dostopne informacije. Vsak izmed udeležencev ima na voljo javni in skrivni ključ. Skrivni je poznan le točno določenemu udeležencu, medtem ko je javni ključ poznam vsem, ki sodelujejo v izmenjavi. Ker je ključ javen, njegova delitev ne ogroža razkritja skrivnega ključa. Generanje skrivnega ključa lahko opravi zaupanja vredna avtoriteta ali ga generira udeleženec sam.
Za zaščiteno povezavo med dvema udeležencama moramo poznati njihova javna ključa. Pred tem pa se moramo prepričati ali sta ključa dejansko od pravih udeležencev. Rečemo torej lahko, da problem ni le varna izmenjava skrivnih ključev ampak tudi izmenjava overjenih javnih ključev.
Zagotavljanje informacijske varnosti s pomočjo matematičnih pristopkov, lahko v splošnem strnemo v naslednjih vodilih oz. ciljih:

- *Zaupnost* podatkov in njihovo varno hranjenje, ter dostopnost le avtoriziranim osebam.
- *Celovitost podatkov* ali zmožnost odkrivanja sprememb podatkov s strani nepooblaščenih oseb
- *Overjanje* v povezavi z identifikacijo udeležencev in podatkov. Deli se na dve poskupini:
  -*Overjanje oseb* oz. preverjanje identičnosti udeležencev
  -*Izvor podatkov* tj. skrb za preverjanje njihovega izvora
- *Neodklonljivost* ali preprečitev tajenja predhodno storjenih akcij

Varnostna infrastruktira oz. celoten sistem za uporabo varnostnih metod na podlagi asimetrične kriptografije imenujemo infrastruktura javnih ključev ali Public Key Infrastructure(PKI). Sistem nam omogoča podpisovanje certifikatov, sledenje zavrnjenih certifikatov, distribucijo ključev in ostalo. Najbolj znana metoda delitve overjenih ključev je deljenje s pomočjo zaupanja vredne tretje osebe (Trusted authority - TA). Udeleženec za registracijo svojega javnega ključa zaprosi TA, katera udeleženca overi in z izdajo digitalnega certifikata zagotovi njegov ključ. Alternativa upravljanja javnih ključev je lahko tudi uporaba protokolov, katerih izmenjava ključev temelji na identiteti udeleženca. V takem okolju prisotnost certifikatov ni potrebna, vseeno pa je za generiranje privatnih ključev potrebna prisotnost zaupanja vredne tretje osebe, ki ima v teh protokolih vlogo generatorja privatnih ključev (PKG). Za pridobitev ključa udeleženc zaprosi PKG, slednji pa udeleženca overi in generira skrivne ključe na podlagi njegove identite.
V spodnjih odstavkih je zbrano nekaj najpogosteje uporabljenih infrastruktur izmenjave ključev:

Infrastruktura javnih ključev z uporabo certifikatov

Običajno avtentičnost javnih ključev zagotavlja certifikatna agencija (CA). S svojim podpisom povezuje identiteto udeleženca z njegovim javnim ključen in zagotavlja njegovo avtentičnost. Javni ključ, skupaj z identiteto udeleženca in podpisom CA tvori digitalni certifikat, katerega lahko preveri vsak, ki ima v lasti javni ključ agencije. Certifikat lahko dodatno hrani informacije o imenu udeleženca, veljavnosti certifikata, uporabljenem algoritmu pri podpisovanju, možnosti uporabe

(npr. enkripcija, podpisovanje), omejitve in dodatna polja, ki služijo uporabi in upravljanju certifikata. Strukturo in vsebino certifikata določajo različni standardi. Primer enega izmed bolj razširjenih je standard X.509.
V infrastrukturi javnih ključev z uporabo certifikatov igra osrednjo vlogo certifikatna agencija. Osnovni elementi take infrastrukture predstavljajo servisi, procesi in varnostni predpisi/politike, kateri določajo upravljanje, distribucijo, uporabo, hranjenje in preklic digitalnih certifikatov.

Infrastruktura javnih ključev na temelju identitete

V prejšnjem odstavku smo lahko videli, da upravljanjanje infrastrukture javnih ključev lahko zahteva veliko sredstev. Kljub temu ni verjetno, da bodo protokoli na temelju identitete, izpodrinili uveljavljeno infrastrukturo javnih ključev, ampak bodo uporabni kot možna alternativa[2]. Njihova značilnost je ta, da lahko problem avtentičnosti uporabnika rešimo tudi brez uporabe certifikatov. Javna vrednost je tako informacija, ki udeleženca enolično identificira (npr. emšo ali email naslov). Poenostavitev upravljanja certifikatov v email sistemih je prvi predstavil avtor Shamir leta 1984, nekaj let kasneje pa sta Boneh in Franklin vpeljala prvo enkripcijsko shemo na temelju identitete s pomočjo Weilovega parjenja. Primer, ki ga je Shamir opisal obsega pošiljanje zaščitenega sporočila udeleženca *Alice* udeležencu *Bob*. Za pošiljanje *Alice* ne potrebuje *Bob*-ovega certifikata, ampak sporočilo zašifrira le z njegovim javno dostopnim ključem *bob@podjetje.si*. Ko *Bob* prejme sporočilo, kontaktira tretjo osebo, ki opralja vlogo generatorja skrivnih ključev (Public Key Generator - PKG). Njegova naloga je izdajanje skrivnih ključev udeležencem glede na njihovo javno vrednost, s katerimi lahko udeleženci odšifrirajo prejeto sporočilo. Pred tem se mora *Bob* centru avtenticirati. Za generiranje skrivnega ključa PKG uporablja glavni skrivni master ključ kateri je znan le njemu.

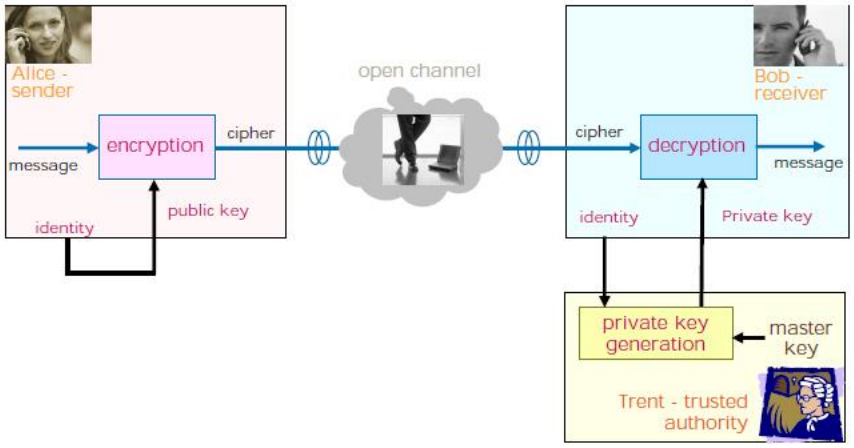

Figure 1: Shamirjeva enkripcija na temelju identitete

Navkljub temu, da opisana infrastruktura ne potrebuje certifikatov, ima nekatere pomankjlivosti. Ena izmed njih je naprimer hranjenje in varnost glavnega ključa PKG, s katerim se generirajo skrivni ključi udeležencev. Problem takega pristopa se pojavi tudi v zaupnosti PKG-ja saj ima slednji z dešifriranjem možnost vpogleda v vsa šifrirana sporočila. Podobno ima PKG v shemah za podpisovanje možnost ponarejanja podpisov, tako da taka infrastruktura ne omogoča zagotavljanja

popolne preprečitve tajenja izvedene komunikacije, kot to poznamo pri PKI. Kompromitiranje glavnega ključa PKG bi v tem sistemu povzročilo veliko škode, zato je takšna infrastruktura uporabna predvsem v manjših, zaprtih skupinah ali v aplikacijah z omejenimi varnostnimi zahtevami [9].

Infrastruktura javnih ključev brez uporabe certifikatov

Kritografija javnih ključev brez uporabe certifikatov se je razvila predvsem iz potrebe po zmanjševanju kompleksnosti upravljanja s certifikati in odprave možnosti vpogleda v skrivne ključe s strani PKG. Tako kot prejšnji se tudi ta sistem za generirnaje skrivnih ključev še vedno poslužuje tretje osebe oz. centra za generiranje ključev (KGC). Razlikuje se v tem da udeležencu A ne posreduje celotnega skrivnega ključa ampak le del D_A, ki ga izračuna s pomočjo identifikatorja udeleženca ID_A in glavnega master ključa. Nato udeleženec A delni skrivni ključ D_A združi z določeno skrivno informacijo in izračuna dejanski skrivni ključ S_A. Na takšen način je skrivni ključ poznan le udeležencu. Poleg skrivnega udeleženec izračuna tudi javni ključ P_A, katerega izračuna s pomočjo skrivne informacije in javnih parametrov KGC. Opisan sistem se tako razlikuje od sistemov, ki temeljijo na identiteti udeleženca saj za izračun javnega ključa udeleženca ni le potrebna njegova identiteta, ampak tudi skrivna informacija, ki jo ima vsak udeleženec.

Javni ključ udeleženca A je lahko dostopen ostalim udeležencem, tako da se ga pošlje skupaj s sporočilom ali pa se ga shrani v javni direktorij. Za dešifriranje in preverjanje podpisov med udeležencema A in B, slednji uporablja P_A in ID_A.

2 Overjeni protokoli za izmenjavo ključev

V nadaljevanju drugega poglavja bomo spoznali kakšne so lahko posledice protokola, ki ni overjen. Neoverjen protokol udeležencem izmenjave ne omogoča preveranje identitet ostalih udeležencev, s čimer omogoča napadalcu možnost pridobitve skupnega skrivnega ključa. Overitev ključev lahko opišemo kot lastnost, kjer se lahko udeleženec prepriča da noben drug poleg točno identificiranih preostalih udeležencev nima dostopa do skrivnega ključa. Protokol, ki podpira omenjeno lastnost imenujejo overjen protokol za izmenjavo ključev.

Naj bosta A in B poštena udeleženca, katera izvajata korake določenega protokola za izmenjavo ključev. Protokol pravimo da zagotavlja *implicitno overitev kljucev* če je udeleženec A prepričan, da znanje o vrednosti skrivnega ključa pozna le udeleženec B in noben drug. Protokol, ki obojestransko zagotavlja *implicitno overitev kljucev* imenujemo overjen protokol za izmenjavo ključev (authenticated key agreement protocol). Če poleg implicitne overitve ključev protokol od udeležencev zahteva tudi izrecno potrdilo o dejansko generiranem ključu, tak protokol imenujemo overjen protokol za izmenjavo ključev s potrditvijo ključa (authenticated key agreement with key confirmation).

Veliko načinov obstaja kako lahko napadalec razbije protokol za izmenjevanje ključev zato je pomembno, da pri njegovem kreiranju vemo na katere napade je odporen in katere ni. Spodaj je naštetih nekaj izmed pomembnejših in bolj zaželenih varnostnih atributov, katere bi moral vsebovati vsak protokol za izmenjavo ključev. Njihova prisotnost je ključnega pomena pri preprečevanju napadov.

Želene lastnosti protokolov:

- **Varnost ob razkritju sejnih ključev - Known session key security**
  Protokol ima omenjeno lastnost, če poznavanje prejšnjih sejnih ključev napadalcu ne omogoča kompromitiranja prejšnjih in bodočih sejnih ključev.
- **Poudarjena zaupnost - Perfect forward secrecy**
  Protokol ima poudarjeno zaupnost, ko izguba dolgotrajnega ključa enega ali več udeležencev ne vpliva na varnost prejšnjih sej v prisotnosti pasivnega napadalca.
- **Odpornost na poosebljanja pri uporabi kompromitiranih ključev - Key-compromise impersonation resilience**
  Predpostavimo da je udeležencev skrivni ključ razkrit. Z znanjem skrivnega ključa ga lahko napadalec pooseblja, saj prav skrivni ključ določa identiteto udeleženca. Protokol je odporen na poosebljanja pri uporabi kompromitiranih ključev, ko izguba skrivnega ključa ne omogoča poosebljanja tudi preostalih udeležencev.
- **Neznana delitev ključa - Unknown key-share resilience**
  Pri napadu z neznano delitvijo ključa napadalec skupino udeležencev prepriča, da komunikacija poteka med njim in skupino, čeprav skupina komunicira s tretjo osebo.
- **Onemogočena kontrola nad ključi - No key control**
  Protokol za izmenjavo ključev ima to lastnost takrat, ko nobeden izmed udeležencev nima vpliva na izbiro vrednosti sejnega ključa ali pa možnosti njenega napovedovanja.

3 Tristranski overjeni protokoli za izmenjavo ključev z enim obhodom (TAK)

Eden izmed pomembnejših tristranskih protokolov za izmenjavo ključev je Jouxov protokol iz leta 2004. Protokol uporablja parjenje na eliptičnih krivuljah, vsaka entiteta pa mora sporočilo poslati vsem udeležencem v izmenjavi. V zadnjih letih smo lahko zasledili nemalo protokolov, ki temeljijo na njem. Primer take razširitve protokola je npr. nadgradnja protokola za izmenjavo ključev v skupini ali pa primer tristranskega overjenega protokola (TAK), s katerim so avtorji odpravili pomanjkljivost napada srednjega moža. V poglavju 3.3 smo poleg TAK protokola opisali štiri možnosti izračuna sejnega ključa. TAK protokol temelji na Jouxovem protokolu, nekatere ideje pa so avtorji črpali iz protokola MTI in MQV.

3.1 Izmenjeva ključev z uporabo parjenja

V tem poglavju bomo opisali postopek združevanja oz. parjenja (bilinear mapping) in njegove lastnosti.

Naj bo $\mathbb{G}_1$ aditivna grupa reda q in $\mathbb{G}_2$ multiplikativna grupa enakega reda q, kjer je q praštevilo. Predpostavimo da obstaja bilinearna preslikava $\hat{e}$, za katero velja da slika iz $\mathbb{G}_1 \times \mathbb{G}_1$ v $\mathbb{G}_2$. Za grupo $\mathbb{G}_1$ tipično velja da je podgrupa grupe točk na eliptični krivulji nad končnim obsegom medtem ko za $\mathbb{G}_2$ velja, da je podgrupa multiplikativne grupe nad končnim obsegom. Preslikavo $\hat{e}$ dobimo s pomočjo Weil ali Tail parjenja na eliptični krivulji za katero veljajo naslednje lastnosti:

- Bilinearnost:
  Če $Q, W, Z \in \mathbb{G}_1$ potem velja $\hat{e}(Q, W+Z) = \hat{e}(Q, W) \cdot \hat{e}(Q, Z)$ in $\hat{e}(Q+W, Z) = \hat{e}(Q, Z) \cdot \hat{e}(W, Z)$

  Posledično če $P, Q \in \mathbb{G}_1$ in $a, b \in \mathbb{Z}_q^*$ potem $\hat{e}(aQ, bW) = \hat{e}(Q, W)^{ab} = \hat{e}(abQ, W) = \hat{e}(Q, abW) = \hat{e}(bQ, W)^a$, kjer oznaka aQ označuje skalarno množenje Q z a.

- Ne-degenerativnost: $\hat{e}(P, Q) \neq 1$ kjer je 1 enota grupe $\mathbb{G}_2$

- Učinkovitost: Preslikavo $\hat{e}$ je možno učinkovito izračunati (v polinomskem času).

3.2 Motivacija (primer napada na neoverjen tristranski Jouxov protokol)

Z napadom na Jouxov protokol smo želeli prikazati njegove pomanjkljivosti, ki jih z overjenim tristranskim protokolom odpravimo. Skupni skrivni ključ se izračuna v enem obhodu. Sestavljen je tako, da je komunikacija med udeleženci čim bolj enostavna. Protokol uporablja parjenje na eliptični krivulji in od vsakega udeleženca zahteva po eno pošiljanje sporočila preostalim udeležencem (broadcast).
Element P je generator grupe $\mathbb{G}_1$ katerega red je enak praštevilu q medtem, ko $a, b, c \in \mathbb{Z}_q^*$ izberejo udeleženci A, B, C enakomerno naključno. Po končanem obhodu protokola lahko vsi udeleženci na podlagi javnih sporočil preostalih udeležencev izračunajo vrednost skrivnega ključa. Vrstni red sporočil ni pomemben in vsak izmed udeležencev je lahko pobudnik za izmenjavo.

Jouxov protokol:

$A \rightarrow B, C : aP \quad (1)$
$B \rightarrow A, C : bP \quad (2)$
$C \rightarrow A, B : cP \quad (3)$

Opis Protokola: Ko se komunikacija zaključi lahko vsak izmed udeležencev izračuna svoj skrivni ključ, ki je zaradi bilinearnosti enak za vse tri udeležence $K_{ABC} = K_a = K_b = K_c$. Udeleženec A izračuna $K_a = \hat{e}(bP, cP)^a$, B izračuna $K_b = \hat{e}(aP, cP)^b$, in C izračuna $K_c = \hat{e}(aP, bP)^c$. Skupen ključ je tako $K_{ABC} = \hat{e}(P, P)^{abc}$
Uspešnost opisane izmenjave oz. kreiranja ključa med udeleženci z ozirom na pasivnega napadalca sloni na težkosti Bi-linearnega Diffie-Hellmanovega problema (BDHP) za grupi $\mathbb{G}_1$,$\mathbb{G}_2$. Problem je določen sledeče:

S podanim P, aP, bP, cP, kjer je a, b, c izbran nakljucno iz $\mathbb{Z}_q^*$ izračunaj $\hat{e}(P, P)^{abc}$

Podobno kot neoverjen dvostranski Diffie-Hellmanov protokol je tudi Jouxov protokol ranljiv z napadom srednjega napadalca, ki napdalcu omogoča maskiranje v vsakega izmed udeležencev. Napad je opisan v naslednjem poglavju.

Napad srednjega napadalca na Jouxov protokol:

Podobno kot neoverjen dvostranski Diffie-Hellmanov protokol je tudi Jouxov protokol varen le pred pasivnim napadalcem. Ko je napadalec aktiven sta tako Jouxov kot Diffi-Hellmanov protokol ranljiva, saj ne omogočata overjanja udeležencev. Protokol napadalcu omogoča spremljanje mrežnega prometa in maskiranje, kar pomeni da se lahko vsakemu izmed udeležencev predstavi

kot nekdo drug.

$E : a', b' \in \mathbb{Z}_q^*;\ a'P, b'P \in \mathbb{G}_1$ (1)
$A \rightarrow E_B, C : aP$ (2) A je pobudnik izmenjave, njegovo sporočilo B-ju prestreže E
$E_A \rightarrow B, C : a'P$ (3) E je pobudnik nove izmenjave z udeležencema B, C
$B \rightarrow E_A, C : bP$ (4)
$C \rightarrow E_A, B : cP$ (5)
$E_B \rightarrow A : b'P$ (6)
$E_C \rightarrow A : cP$ (7)
$B, C : K_{E_ABC} = \hat{e}\left(P, P\right)^{a'bc}$ (8)
$A : K_{AE_BC} = \hat{e}\left(P, P\right)^{ab'c}$ (9)
E : lahko izračuna K_{E_ABC} in K_{AE_BC} (10)

Ker ima napadalec nadzor nad omrežjem in lahko prestreza ter usmerja promet, se lahko s pridobljenimi informacijami izdaja za udeleženca A,B ali C. V primeru, ko se napadalec E izdaja za udeleženca C v komunikaciji z udeležencem A, pri tem uporablja oba ključa. Ključ K_{AE_BC} uporablja pri povezavi z udeležencem A, ključ K_{E_ABC} pa pri povezavi z udeležencem C. Rešitev te težave je podana v naslednjem poglavju, kjer smo opisali overjeno verzijo tega protokola.

3.3 Opis tristranskega overjenega protokola

Dobra lastnost Jouxovega tristranskega protokola je ta, da za izračun skrivnega ključa potrebujemo le en obhod, kljub temu pa smo videli, da ima nekatere pomanjkljivosti. V poglavju bomo predstavili overjeno različico protokola s štirimi možnostmi generiranja ključev. Med izvajanjem protokola potrebujemo certifikate, katere s strani overitelja potrjujejo verodostojnost entitet in jih povezujejo s pripadajoči ključi. Oblika certifikatov je sledeča:

$$Cert_A = (I_A \,||\, \mu_A \,||\, P \,||\, S_{CA}\left(I_A \,||\, \mu_A \,||\, P\right))$$

kjer I_A niz predstavlja identiteto A-ja, operacijo $||$ opisuje konkatenacijo posameznih elementov, S_{CA} pa predstavlja podpis overitelja certifikata. Javni ključ A-ja je enak $\mu_A = xP$, kjer je $x \in \mathbb{Z}_q^*$ njegov dolgotrajni skrivni ključ. Podobno so tudi $Cert_B$ in $Cert_C$ certifikati za udeleženca B in C z javnimi ključi $\mu_B = yP$ in $\mu_C = zP$. Certifikati lahko vsebujejo dodatne informacije, kot npr. datum veljavnosti.

Opis protokola:

Trenutni ključi $a, b, c \in \mathbb{Z}_q^*$ so izbrani enakomerno naključno za vsak obhod protokola posebej.
$A \rightarrow B, C : aP \,||\, Cert_A$ (1)
$B \rightarrow A, C : bP \,||\, Cert_B$ (2)
$C \rightarrow A, B : cP \,||\, Cert_C$ (3)

Udeleženec A pošlje preostalim udeležencem B in C svojo trenutni javno vrednost aP skupaj s svojim certifikatom $CertA$, ki vsebuje A-jev javni ključ. Sporočila s svojim certifikatom in trenutno vrednosti pošljeta preostalim udeležencem tudi B in C. Potek sporočil je enak kot pri Jouxovem protokolu, s to razliko, da so sporočilom dodani certifikati. Vsak izmed udeležencev ob sprejemu

sporočila preveri avtentičnost obeh certifikatov, ki ju je prejel od ostalih udeležencev. Če pri preverjanju pride do napake se protokol prekine. V nasprotnem primeru se izvede generiranje ključev na enega izmed spodaj naštetih načinov. Funkcija H predstavlja zgoščevalno funkcijo.

Generiranje ključev:

Tip 1 (TAK1)

$$K_A = H\left(\hat{e}\left(bP, cP\right)^a \,||\, \hat{e}\left(yP, zP\right)^x\right)$$
$$K_B = H\left(\hat{e}\left(aP, cP\right)^b \,||\, \hat{e}\left(xP, zP\right)^y\right)$$
$$K_C = H\left(\hat{e}\left(aP, bP\right)^c \,||\, \hat{e}\left(xP, yP\right)^z\right)$$

Zaradi bilinearnosti je skupen ključ $K_{ABC} = H\left(\hat{e}\left(P, P\right)^{abc} \,||\, \hat{e}\left(P, P\right)^{xyz}\right)$

Tip 2 (TAK2)

$$K_A = \hat{e}\left(bP, zP\right)^a \cdot \hat{e}\left(yP, cP\right)^a \cdot \hat{e}\left(bP, cP\right)^x$$
$$K_B = \hat{e}\left(aP, zP\right)^b \cdot \hat{e}\left(xP, cP\right)^b \cdot \hat{e}\left(aP, cP\right)^y$$
$$K_C = \hat{e}\left(aP, yP\right)^c \cdot \hat{e}\left(xP, bP\right)^c \cdot \hat{e}\left(aP, bP\right)^z$$

Sejni ključ je enak $K_{ABC} = \hat{e}\left(P, P\right)^{(ab)z+(ac)y+(bc)x}$

Tip 3 (TAK3)

$$K_A = \hat{e}\left(yP, cP\right)^x \cdot \hat{e}\left(bP, zP\right)^x \cdot \hat{e}\left(yP, zP\right)^a$$
$$K_B = \hat{e}\left(xP, cP\right)^y \cdot \hat{e}\left(aP, zP\right)^y \cdot \hat{e}\left(xP, zP\right)^b$$
$$K_C = \hat{e}\left(xP, bP\right)^z \cdot \hat{e}\left(aP, yP\right)^z \cdot \hat{e}\left(xP, zP\right)^c$$

Sejni ključ je enak $K_{ABC} = \hat{e}\left(P, P\right)^{(xy)c+(xz)b+(yz)a}$

Tip 4 (TAK4)

$$K_A = \hat{e}\left(bP + H\left(bP \,||\, yP\right) yP, cp + H\left(cP \,||\, zP\right) zP\right)^{a+H(aP||xP)x}$$
$$K_B = \hat{e}\left(aP + H\left(aP \,||\, xP\right) xP, cp + H\left(cP \,||\, zP\right) zP\right)^{b+H(bP||yP)y}$$
$$K_C = \hat{e}\left(aP + H\left(aP \,||\, xP\right) xP, bp + H\left(bP \,||\, yP\right) yP\right)^{c+H(cP||zP)z}$$

Skupni ključ je enak $K_{ABC} = \hat{e}\left(P, P\right)^{(a+H(aP||xP)x)(b+H(bP||yP)y)(c+H(cP||zP)z)}$

Opombe:

Jouxov in zgoraj opisane različice TAK protokola so ranljive proti napadom "manjših podgrup". Za preprečitev takih napadov mora vsaka entiteta prejeta sporočila preveriti ali so res elementi grupe $\mathbb{G}_1$.

Za generiranje skupnega skrivnega ključa se vsak izmed udeležencev poslužuje svojega trenutnega in javnega kluča. Pri tem noben izmed udeležencev nima vpliva nad izbiro skupnega ključa in ker so trenutni ključi a, b, c izbrani enakomerno naključno je tudi skupni skrivni ključ iz grupe $\mathbb{G}_2$ naključen. Zakasnjeno sprejemanje sporočil ni dopuščeno, saj bi tako lahko udeleženec poznal vse entite, ki v obhodu sodelujejo in imel možnost pridobitve skupnega ključa.

Vse štiri različice protokola pošiljajo enaka sporočila, kar pomeni da je promet, ki ga ustvarijo enak pri vseh. Vseeno pa za protokol $TAK1$ porabimo več računskih operacij kot pri protokolu $TAK2$ in $TAK3$. Tako imamo pri $TAK1$ dvoje parjenj, medtem ko imamo pri $TAK2$ in $TAK3$ le dve. Najmanj parjenj lahko zasledimo $TAK4$, kjer uporabimo le eno operacijo parjenja.

3.4 Analiza protokolov TAK3 in TAK4

V sledečem poglavju bomo opisali različne napade na TAK protokole z ozirom na lastnosti, ki smo jih opisali v poglavju overjenih protokolov. Večina napadov ima izvor iz dvostranskih protokolov MTI, nekaj pa jih je podal avtor KyungAh Shim v članku [7], kjer je ugotovil da trenutno noben izmed naštetih različic protokola ne zadošča varni izmenjavi ključev. S predelavo Jouxovega protokola in dodanimi certifikati je v protokolih zagotovljena implicitna izmenjava klučev. Kljub temu pa protokol $TAK2$ ne zadošča tej predpostavki, saj zanj poznamo ranljivost srednjega napadalca. V naslednjih straneh bomo podrobneje pogledali $TAK3$ in računsko najmanj potraten protokol $TAK4$. Povzetek vseh napadov na TAK protokole je zbran na koncu poglavja. Ranljivosti protokolov $TAK1$ in $TAK2$ lahko najdemo v [6] in [7].

3.4.1 Napad poosebljanja z uporabo kompromitiranih ključev $TAK3$, $TAK4$ - Key-compromise impersonation

Predstavili bomo kaj se zgodi v primeru, ko napadalec E pride v posest enega izmed dolgotrajnih ključev udeleženca in podali primere poosebljanja.

- Napad na protokol TAK3
  Predpostavimo, da napadalec pozna dolgotrajni skrivni ključ x. Videli bomo, da ob poznavanju dolgotrajnega ključa napadalec E_C lahko pooseblja udeleženca C udeležencu B. Napad ni popoln, saj napadalec ne more izračunati ključa K_A, iz česar sledi da poosebljanje C-ja A-ju ni mogoče:

  Med pošiljanjem sporočil E prestreže sporočili $P_A = aP$ in $P_B = bP$, izbere nov a' in b' ter ju zamenja z $P_A^{'} = a'P$ in $P_B^{'} = b'P$. Hkrati naključno izbere c' in ga pošlje preostalim udeležencem.

  $$A : P_A = aP, Cert_A \rightarrow P_A = a'P, Cert_A \quad (1)$$
  $$B : P_B = bP, Cert_B \rightarrow P_B = b'P, Cert_B \quad (2)$$
  $$E_C : P_C = c'P, Cert_C \quad (3)$$

  Udeleženec A in B nato izračunata sejna ključa K_A in K_B:

  $$K_A = \hat{e}\left(yP, c'P\right)^x \cdot \hat{e}\left(b'P, zP\right)^x \cdot \hat{e}\left(yP, zP\right)^a = \hat{e}\left(P, P\right)^{xyc' + xzb' + yza}$$
  $$K_B = \hat{e}\left(xP, c'P\right)^y \cdot \hat{e}\left(a'P, zP\right)^y \cdot \hat{e}\left(xP, zP\right)^b = \hat{e}\left(P, P\right)^{yza' + xyc' + xzb}$$

  Ker E lahko izračuna $\hat{e}\left(zP, yP\right)^{a'} \cdot \hat{e}\left(xP, yP\right)^{c'} \cdot \hat{e}\left(zP, bP\right)^x$ s tem pridobi ključ K_B. Kljub temu pa E ne pozna ključa K_A, saj ne more izračunati njegovega zadnjega člena $\hat{e}\left(P, P\right)^{yza}$. Kar sledi je to da E ne more poosebljati udeležence A-ju, saj ne pozna K_A s katerim bi lahko šifriral sporočila. Napad tako omogoča le poosebljanje C-ja B-ju in pridobitev ključa K_B.

- Napad na protokol TAK4
  Enak napad lahko opišemo tudi za protokol $TAK4$:

  $$A : P_A = aP, Cert_A \rightarrow P_A = a'P, Cert_A \quad (1)$$
  $$B : P_B = bP, Cert_B \rightarrow P_B = b'P, Cert_B \quad (2)$$
  $$E_C : P_C = c'P, Cert_C \quad (3)$$

  Nato A in B izračunata ključe K_A in K_B:

  $$K_A = \hat{e}\left(P, P\right)^{(a + H(aP||xP)x)\left(b' + H\left(b'P||yP\right)y\right)\left(c' + H\left(c'P||zP\right)z\right)}$$

$$K_B = \hat{e}\left(P,P\right)^{\left(a'+H\left(a'P||xP\right)x\right)\left(b+H(bP||yP)y\right)\left(c'+H\left(c'P||zP\right)z\right)}$$

Ker ima napadalec na voljo vrednosti P_A, P_B in skrivne vrednosti a',b',c' in x lahko s spodnjim izračunom ugotovi ključ K_B:

$$K_B = \hat{e}\left(bP,P\right)^{a'c'}\cdot\hat{e}\left(bP,H\left(c'P\,||\,zP\right)zP\right)^{a'}\cdot\hat{e}\left(P,H\left(bP\,||\,yP\right)yP\right)^{a'c'}\cdot\hat{e}\left(H\left(bP\,||\,yP\right)yP,H\left(c'P\,||\,zP\right)zP\right)^{a'}\cdot$$
$$\hat{e}\left(bP,H\left(a'P\,||\,xP\right)xP\right)^{c'}\cdot\hat{e}\left(H\left(a'P\,||\,xP\right)bP,H\left(c'P\,||\,zP\right)zP\right)^{x}\cdot\hat{e}\left(H\left(a'P\,||\,xP\right)xP,H\left(bP\,||\,yP\right)yP\right)^{c'}\cdot$$

$$\hat{e}\left(H\left(bP\,||\,yP\right)yP,H\left(c'P\,||\,zP\right)zP\right)^{xH\left(a'P||xP\right)}$$

Kljub temu E ne more izračunati K_A saj ne zna izračunati člena $K_B = \hat{e}\left(P,P\right)^{ayzH\left(b'P||yP\right)H\left(c'P||zP\right)}$.
Tako kot v prejšnem napadu lahko E pooseblja le udeleženca C udeležencu B.

3.4.2 Pomanjkljiva poudarjena zaupnost protokola $TAK3$ - Forward security weakness

Protokol ima poudarjeno zaupnost, ko izguba dolgotrajnega ključa enega ali več udeležencev ne vpliva na varnost prejšnjih sej, ki so bile vzpostavljene med poštenimi udeleženci (v našem primeru so to ključi x,y ali z).

V primeru protokola $TAK4$ je ta lastnost zagotovljena, saj če pogledamo in razvijemo skupni ključ $K_{ABC} = \hat{e}\left(P,P\right)^{(a+H(aP||xP)x)(b+H(bP||yP)y)(c+H(cP||zP)z)}$ opazimo, da ključ vsebuje izraz $\hat{e}\left(P,P\right)^{abc}$ katerega reševanje je enako reševanju Bilinearnemu Diffie-Hellmanovemu problemu.

Za protokol $TAK3$ lastnost poudarjene zaupnosti ne velja, saj s pridobitvijo dveh dolgotrajnih ključev lahko napadalec ugotovi ključ prejšnje seje. V naslednjem primeru predpostavimo, da napadalec pozna javne vrednosti aP,bP,cP in dva dolgotrajna ključa x,y. Vrednosti xP,yP in zP so na voljo v certifikatih udeležencev. Za razkritje ključa mora napadalec izračunati $K_{ABC} = \hat{e}\left(P,P\right)^{(xy)c+(xz)b+(yz)a}$, kar stori na sledeči način:

$$K_{ABC} = \hat{e}\left(yP,cP\right)^{x}\cdot\hat{e}\left(zP,bP\right)^{x}\cdot\hat{e}\left(zP,aP\right)^{y}$$

Protokol $TAK3$ bi lahko spremenili v varnega, če bi ključ K_{ABC} dodatno pomnožili z $\hat{e}\left(P,P\right)^{abc}$, kar pa bi pomenili dodatno računsko operacijo in počasnitev protokola.

3.4.3 Napad neznane delitve ključa - Unknown key share attack

V poglavju bomo predstavili dva tipa napada. Osnovni napad z zamenjavo pride v poštev pri vseh TAK protokolih, saj izkorišča pomankljivost kreiranja certifikatov pri prijavi javnih ključev.
Napadalec E pri overitelju registrira A-jev javni ključ μ_A za svojega in tako pridobi certifikat $Cert_E = (I_E\,||\,\mu_A\,||\,P\,||\,S_{CA}\left(I_E\,||\,\mu_A\,||\,P\right))$. Nato prisluškuje omrežju in sporočila s strani A-ja zamenjuje s svojim certifikatom. Napadalec dolgotrajnega ključa x ne pozna in skupnega sejnega ključa K_{ABC} ne more izračunati. Kljub temu pa sta udeleženca B in C zavedena, saj mislita da si izmenjujeta ključ z E-jem, čeprav ga z A-jem. Rešitev problema bi predstavljajo preverjanje ključev s strani overitelja, ki bi za vsako zahtevo registracije ključev preveril njegovo enoličnost. Če bi ugotovil da se zahtevani ključ ponavlja bi podpis zavrnil. Kljub temu pa bi takšen pristop predstavljal težave pri večjih oz. distribuiranih sistemih. Druga možna rešitev je podana kasneje.

$TAK3$ protokol pa je ranljiv še na drugačen način, kljub preverjanju overitelja. Napadalec pri registriranju certifikata overitelju pošlje v overjanje ključ μ_E, ki pa je nek večkratnik ključa μ_A. S tem je napadalcu omogočeno da v izvajanju protokola lahko s prireditvijo trenutnega ključa in

vzpostavitvijo dveh sej zavede udeleženca B, in C da je sporočilo prišlo od udeleženca A (potek napada [6]).

V obeh napadih napadalec nima dostopa do dolgotrajnih ključev udeležencev, zato bi lahko napada preprečili s tem, da bi overitelj ob registriranju javnega ključa zahteval potrdilo o imetju dolgotrajnega skrivnega ključa.

3.4.4 Ranljivost ob razkritju sejnih ključev protokola $TAK3$- Known key attack

Kot smo opisali v lastnostih overjenih protokolov mora bit protokol odporen na razkritje sejnih ključev protola, kar pomeni da razkritje informacij sej napadalcu ne koristijo. Videli bomo da v primeru protokola $TAK3$ temu ni tako. Napadalec E je vsiljivec in pozna A-jev dolgotrajni skrivni ključ x. Z vzpostavitvijo dveh sej in vsiljenjem javnih informacij prve seje v drugo, napadalec doseže razkritje sejnega ključa začetne seje. Napad ob razkritju ključev poteka sledeče:

1. Napadelec E prisluškuje komunikaciji udeležencev A,B,C v začetni seji:

   $A : P_A = aP, Cert_A \quad (1)$
   $B : P_B = bP, Cert_B \quad (2)$
   $C : P_C = cP, Cert_C \quad (3)$

2. Napadalec E vzpostavijo novo sejo z B in C, kjer pooseblja A. Označimo ga kot E_A. Ko B in C odpošljeta vrednosti nove seje $b'P$ in $c'P$, ju E prestreže in nadomesti z vrednostima iz prejšnje seje bP in cP, hkrati pa E_A pošlje vrednost aP.

   $E_A : P_A = aP, Cert_A \quad (1)$
   $B : P_B = b'P, Cert_B \rightarrow P_B = bP, Cert_B \quad (2)$
   $C : P_C = c'P, Cert_C \rightarrow P_C = cP, Cert_B \quad (3)$

3. Če imamo dostop do novo izračunanega ključa udeleženca C, je slednji zaradi sprememb v prejšnji točki enak $K_C^{'} = \hat{e}\,(P,P)^{ayz+xbz+xyc'}$. Kar pa pomeni da lahko z informacijami iz začetne seje na spodnji način izračunamo njen sejni ključ:

$K_{ABC} = K_C^{'} \cdot \left[\hat{e}\,(yP, c'P)^x\right]^{-1} \cdot \hat{e}\,(yP, cP)^x = \hat{e}\,(P,P)^{ayz+bxz+xyc'} \cdot \hat{e}\,(P,P)^{-xyc'} \cdot \hat{e}\,(P,P)^{xyc} = \hat{e}\,(P,P)^{ayz+bxz+xyc}$

Povzetek protokolov je povzet v spodnji tabeli. Tabela prikazuje ali je protokol odporen na določeno vrsto napada, katere smo opisali med želenimi lastnostmi overjenih protokolov za izmenjavo ključev.

Protokol	Forward secrecy	Key-compromise impersonation	Known key	Unknown key share
TAK3	Ne	Ne	Ne	Da
TAK4	Da	Ne	Da	Da

*Napade na protokole $TAK1$ in $TAK2$ lahko najdemo v [6] in [7]

4 Zaključek

V seminarski nalogi je bila predstavljena uporaba javne kriptografije, njeni cilji in najpogostejše strukture za njeno delovanje. V nadaljevanju smo opisali overjene protokole, ki temeljijo na enem izmed prej opisanih infrastruktur ter predstavili tristranski overjen protokolov za izmenjavo ključev

avtorja Al-Riyami in ostalih. S štirimi primeri generiranja ključev smo videli kako različni kombinacije izračunov parjenj na eliptični krivulji vplivajo na varnost protokola in njegove lastnosti.
Po analizi protokola $TAK3$ in $TAK4$ je razvidno, da trenutno še nobena izmed štirih možnosti protokola ni popolnoma varna. Obe različici nista odporni na poosebljanja, če so ključi kompromitirani, protokol $TAK3$ pa ima še dodatni pomankljivosti ob razkritju sejnih ključev in ranljivost ob izgubi dolgotrajnih sejnih kljlučev.

References

[1] Hölbl M., Development of Identity-Based Authenticated Key Agreement Protocols, University of Maribor, 2009

[2] Hölbl M., Welzer T., Brumen B., Comparative Study of Tripartite Identity-Based Authenticated Key Agreement Protocols, Informatica, Journal of Computing, Vol. 33, No. 3, pp. 347-355, 2008

[3] Stinson, D., Cryptography: Theory and Practice, Second Edition, CRC Press, 2002

[4] Blake-Wilson S., Johnson D., Menezes A., Key Agreement Protocols and their Security Analysis, 1997

[5] Dutta R., Barua R., Overview of Key Agreement Protocols, Cryptology ePrint Archive, No. 289, 2005

[6] Al-Riyami S. S., Paterson K. G.: Tripartite Authenticated Key Agreement Protocols from Pairings. IMA Int. Conf., pp. 332-359, 2003

[7] Shim K., Woo S. S., Cryptanalysis of tripartite and multi-party authenticated key agreement protocols, Inf. Sci. 177(4), 1143-1151, 2007

[8] Chen L., Identity-based Cryptography, Hewlett-Packard Laboratories, 2006

[9] Al-Riyami S.S., Paterson K. G., Certificateless public key cryptography. In Proc. Asiacrypt 2003, pp. 452–473. Springer-Verlag, 2003.