KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Nerijus Tamošauskas

Artimo lauko ryšio identifikacija panaudojant mobiliuosius telefonus

Magistro darbas

Darbo vadovas
Prof. Eligijus Sakalauskas

Kaunas, 2012

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Nerijus Tamošauskas

Artimo lauko ryšio identifikacija panaudojant mobiliuosius telefonus

Magistro darbas

Recenzentas
Doc. Saulius Japertas
2012-05-24

Vadovas
Prof. Eligijus Sakalauskas
2012-05-24

Atliko
IFN-0/3 gr. stud.
Nerijus Tamošauskas
2012-05-23

Kaunas, 2012

Turinys

Lentelių turinys:

Diagramų turinys:

Paveikslėlių turinys:

SUMMARY

In this work we will review what Near Field Communication (NFC) is and what standards it use. Which architecture is using to make NFC. How NFC is working between devices and services. We will evaluate threats between technology and devices.

After analyze identification algorithms we will choose one of identification method and we will remove its vulnerability. Then we will adjust in mobile phones with NFC. Algorithm will be chosen by mobile phones capability to compute hash functions. We will analyze which hash functions combinations are fasters. How much data between services and mobile device communications we will send.

Key words: NFC, security element, mobile phone, RFID, identification.

1 ĮVADAS

Informacinėms technologijoms vis labiau plečiantis kasdieniniame gyvenime, mes susiduriame su skirtingomis ir įvairiomis identifikacijomis. Jungiantis prie pamėgto socialinio tinklapio, elektroninio pašto ar kitų apribotų resursų mes naudojame kažkokį savęs identifikavimo raktą (slapyvardis, elektroninis paštas ar kitokie raktai), o jo patvirtinimui dažniausiai naudojame slaptažodį. Praėjimo kontrolėse naudojame identifikavimo korteles, biometrinius identifikavimus ir kitas identifikavimo priemones. Kuo labiau technologijos įsilieja į mūsų gyvenimus, tuo daugiau naudojame įvairesnes identifikacijas. Dažnai tų identifikavimo raktų reikia atsiminti ne vieną ir ne du, o jei norime jaustis saugesniais reikia atitinkamai ir kiekvienam identifikavimo raktui turėti ir skirtingą slaptažodį. Taigi natūralu, kad mes pradėsime naudoti tuos pačius slaptažodžius ar net identifikavimo raktus. Atsiranda poreikis kažkokiai globalesnei identifikavimo sistemai, su kurios pagalba mums nereikėtų atsiminti begalės identifikavimo raktų ir juos patvirtinančių slaptažodžių. Šiai problemai spręsti galima panaudoti mobiliuosius telefonus su Artimo Lauko Ryšio technologija.

Artimo Lauko Ryšys (angl. Near Field Communication) – yra trumpo nuotolio bevielė susijungimo technologija, kuri suteikia galimybę dviem elektroniniams prietaisams „bendrauti“ saugiu ir paprastu būdu, suteikdama vartotojams galimybę pasiekti skaitmeninę informaciją. ALR veikimas yra pagrįstas RFID bekontakčių kortelių skaitymo ir rašymo technologija, bei turi apibrėžtus ISO bendravimo standartus. Vienas iš standartų yra ISO 14443, kuris leidžia bekontaktę infrastruktūrą komunikuoti su RFID įrenginiais naudojant NXP Mifare bekontaktes korteles , ISO 15693 standartas naudojamas Vicinity kortelėms [1]. Tai buvo sugalvota Sony ir NXP Semiconductors įmonių 2002 metais ir standartizuota ISO/IEC 18092 (ECMA 340) standartu. Visos šios standartų kombinacijos sudaro Artimo Lauko Ryšio standartą, kuris leidžia NFC įrenginiams suderintai bendrauti su egzistuojančiomis RFID bekontaktėmis kortelėmis, žymenomis ir infrastruktūromis.

Be viso to, Artimo Lauko Ryšio technologija leidžia sukombinuoti skaitytuvo sąsają ir išmaniąją kortelę viename įrenginyje, taip leisdama mobiliesiems telefonams lengvai persijungti tarp pasyvių žymių skaitymo ar aktyvaus skaitytuvo skaitymo režimo.

Taigi šio *darbo tyrimo sritis* yra identifikavimo algoritmo pritaikymas ALR įrenginiams, o *tyrimo objektas* – mobilieji telefonai su ALR technologija. ALR technologija pasirinkta ne šiaip sau, o įvertinus, jog tai viena iš naujausių, sąlyginai paprasta, pradinėje masinio naudojimo

stadijoje ir potenciali tapti saugia technologija, o svarbiausia ją galima taikyti įvairiose srityse. Mobilusis telefonas šiais laikais yra vienas iš labiausiai žmonių naudojamų įrenginių, tad nenuostabu, kad naujų ir esamų paslaugų diegimą stengiamasi sieti su juo. Pažymėtina tai, jog diegti įvairias paslaugas į mobilųjį telefoną, naudojant ALR technologiją gali būti labai naudinga, kadangi viskas galėtų būti viename įrenginyje (skaitmeninis parašas; bankų, nuolaidų kortelės, praėjimo kortelės ir t.t.). Todėl šio *darbo tikslas* – pritaikyti kriptografinį identifikacijos algoritmą, tinkantį Artimo Lauko Ryšio įrenginiams.

Darbo tikslui pasiekti iškelti tokie uždaviniai:

- Pateikti ALR (angl. Near Field Communication) technologijos veikimo principus.
- Pateikti artimo lauko ryšio įrenginių apžvalgą.
- Išanalizuoti naudojamus ALR technologijos identifikacijos metodus ir nustatyti jų trūkumus.
- Įvertinti išanalizuotus metodų trūkumus ir vieną iš jų pasirinkus patobulinti, pašalinant jo trūkumą.
- Sukurti identifikacijos programinę įrangą ir ją išbandyti virtualioje aplinkoje.
- Įvertinti suprojektuotą sprendimą ir jo pritaikymo galimybes, pateikti rekomendacijas realizacijai.

Analizuojant mobiliuosius telefonus su Artimojo Lauko Ryšio technologija pastebėta, kad didžiausias saugumas galimas naudojant įterptinius saugumo elementus, nes naujausi įterptiniai saugumo elementai mobiliuosiuose telefonuose šiuo metu fiziškai palaiko tris vienkryptes funkcijas (MD5, SHA1 ir SHA-256)[20], praktiškai sunku juos klonuoti ar išgauti konfidencialią informaciją iš jos. Naudojantis šiomis funkcijomis buvo atliktas eksperimentinis tyrimas su patobulintu identifikavimo algoritmu bei išanalizuotas identifikavimo protokolas pagal saugumo srtitis.

Rezultatai parodė kurių vienkrypčių funkcijų kombinacijos yra sparčiausios identifikacijoje, kokios reikalingos duomenų saugojimo vietos įterptiniame saugumo elemente, koks perduodamas bendras duomenų kiekis ar atskiromis iteracijomis. Pateiktos rekomendacijos realizacijai priklausomai nuo reikiamo užtikrinti saugumo.

Darbo struktūra:

- Antrajame skyriuje apžvelgtos ALR technologijos, jų veikimo principai, duomenų perdavimo standartai, galimos grėsmės, saugos elemento klasifikacijos. Palyginti potencialiai galimi naudoti identifikavimo algoritmai ALR identifikavimo sistemose.
- Trečiajame skyriuje išsikeltas darbo tikslas, suformuluoti uždaviniai bei apsibrėžta metodo taikymo sritis bei pagrindiniai reikalavimai. Aprašyta ALR identifikacijos protokolo pagrindinė idėja bei pateikta vizuali identifikacijos algoritmo schema. Apsibrėžtos kokios vienkryptės funkcijos gali būti naudojamos saugumo elemente.
- Ketvirtajame darbo skyriuje aptarti ALR identifikavimo protokolo realizacijai reikalingi įrankiai, apsibrėžta, kas konkrečiai bus realizuojama, pristatytos pagalbinės naudojamos programinės priemonės. Taip pat pateikiamas realizuojamos dalies veikimo algoritmas, testavimo modelis.
- Penktasis skyrius skirtas eksperimentui. Apsibrėžtas eksperimento tikslas, siekiami atsakyti klausimai bei pati eksperimento eiga. Pateikiami gauti rezultatai ir jų analizė.

2 TECHNOLOGIJOS IR PANAUDOJIMO GALIMYBIŲ ANALIZĖ

Šiame skyriuje apžvelgiama ALR technologija, kuria remiantis siūlomi ir projektuojami kliento - serverio identifikacijos metodai mobiliajame telefone su ALR technologija. Taip pat pateikiamos šios technologijos panaudojimo sritys ir pritaikymo galimybės.

Atliekamas pagrindinių telefono ALR technologijos komponentų tyrimas, nagrinėjama, kaip galima tai panaudoti sprendžiant magistriniame darbe iškeltus uždavinius.

2.1 Tyrimo sritis, objektas ir problema

Informacija ir įvairūs specializuoti duomenų rinkiniai jau seniai tapo vienu iš svarbiausių dalykų šiuolaikinėje visuomenėje. O viena pagrindinių su jais susijusių problemų - saugumas. Ši problema yra aktuali tiek valstybinėms institucijoms, įmonėms, komercinėms įstaigoms tiek ir privatiems asmenims. Vis labiau technologijoms veržiantis į mūsų kasdieninį gyvenimą mums tenka susidurti su identifikacijomis. Jungiantis prie pamėgto socialinio tinklapio, elektroninio pašto, kompiuterizuotos darbo vietos, banko paslaugų valdymo sistemų, internetinių puslapių ar kitų apribotų resursų mes naudojame kažkokį savęs identifikavimo raktą (slapyvardis, elektroninis paštas ar kitokie raktai), o jo patvirtinimui naudojame paprasčiausią ir labiausiai įprastą raktą – slaptažodį, t.y. slapta simbolių seka. Tačiau pagrindinė tokių raktų problema pirmiausia ta, jog vartotojas juos turi atsiminti. Todėl neįvertinus galimų pasekmių sukeliamos saugumą mažinančios situacijos: naudojami labai lengvai atspėjami slaptažodžiai (vardas, gimimo metai, asmens kodas, telefono numeris), jeigu pasirenkamas sudėtingesnis – toks pat slaptažodis naudojamas keliose vietose arba užsirašomas. Visais atvejais rizika, jog asmeninius ar kitus slaptus duomenis galės peržiūrėti tretieji asmenys, smarkiai išauga, todėl moderniose sistemose slaptažodžių stengiamasi visiškai atsisakyti ir pereiti prie kitokių identifikavimo sistemų.

Egzistuoja ir tokių sistemų, kuriose jokio rakto atsiminti nereikia. Tačiau tuomet dažniausiai susiduriama su kita problema: jį reikia kažkur saugiai laikyti. Tam dažniausiai naudojamos *USB* atmintinės, protingosios kortelės (*angl. smart card*) ir kitokios laikmenos. Atsiradus ALR technologijai raktus galima saugoti ir įterptiniame saugumo elemente. Šiais atvejais niekas negali garantuoti, jog raktu visuomet naudosis tik savininkas, jis nebus pamestas ar nukopijuotas. Taip pat galimas ir šio bei anksčiau paminėto variantų derinys: vartotojas įveda slaptažodį (kurį reikia atsiminti), o sistema jam suteikia raktą (kuris saugomas sistemoje). Tokiu

atveju slaptažodis reikalingas tikrojo šifravimo ar kitokio slapto rakto atrakinimui. Tai turbūt yra vienas iš patikimesnių ir efektyvesnių apsaugos variacijų.

Taigi raktų valdyme egzistuoja dvi problemos: raktą reikia atsiminti arba kažkur saugiai laikyti. Nei vienas, nei kitas būdas nėra nei pakankamai patogus, nei patikimas. Todėl stengiamasi ieškoti būdų, kaip vartotojas būtų mažiausiai apkraunamas papildomais veiksmais ir informacija, o jo įsikišimas į sistemos veikimą (įvedant raktą) būtų minimalus arba pagal būtinybes net nereikalingas. Tam įgyvendinti bus naudojamas mobilusis telefonas su ALR technologija.

Taigi pagrindinė šiame darbe sprendžiama identifikavimo problema ALR įrenginiuose ir identifikacinių duomenų saugojimas. O esminį darbo klausimą galima suformuluoti taip: kaip identifikuoti asmenį (įrenginį), kuriam nereikėtų atsiminti daugelio slaptažodžių?

2.2 ALR Technologijos panaudojimo sritys

Didelis ALR technologijos lankstumas, paprastumas bei saugumas leidžia šią technologiją pritaikyti daugelyje sričių:

- **Kelių mokesčiams rinkti**- automobilyje įrengtas siųstuvas, gavęs skaitytuvo signalą, automatiškai įsijungia ir perduoda jam automobilio identifikacijos numerį. Pro tokį punktą važiuojanti transporto priemonė net neprivalo sumažinti greičio.
- **Automobilių apsauga nuo vagysčių** - prieš užvedant variklį, patikrinama raktelio tapatybė. Negavus tinkamo atsakymo iš raktelyje esančio RFID lusto, automobilio variklis blokuojamas.
- **Logistikoje**- prekių inventorizacija, sandėliavimas ir valdymas. Visos prekes su RFID žymenomis nuskenuojamos ir identifikuojamos tiesiog pravažiavus pro vartus, kuriuose įmontuoti skaitytuvai.
- **Mobilieji mokėjimai** - įrenginiai veikia kaip debetinės/kreditinės kortelės.
- **Lojalumo taškai ir kuponai** - įvairioms paslaugoms gali būti kaupiami lojalumo taškai. Taip pat galima naudoti kaip nuolaidų kuponus apsiperkant ir už prekes mokant su nuolaida.
- **„Protingas“ skelbimas** - mobilusis telefonas naudojamas RFID žymenų perskaitymui. Pavyzdžiui, perkeldamas informaciją apie skelbimą į mobilųjį telefoną, peržiūrint viešojo transporto tvarkaraščius, istorinę, turistinę informaciją arba prijungiant prie specialaus tinklapio.
- **Elektroniniai bilietai –** autobusų, lėktuvų, renginių bilietai ir kiti bilietai.

- **Asmens dokumentai** - pasas su RFID žyme leidžia nustatyti asmens tapatybę ir įrodyti paso autentiškumą.
- **Elektroniniai raktai** - automobilio, namų, ofiso, viešbučio raktai ir t.t.
- **Bibliotekose** - automatiškai išduodant knygas.
- **Gyvūnų identifikavimas**
- **Automobilių parkavimas**
- **Vaistų identifikavimas** - panaudojant vietoje kompensuojamų vaistų paso.

Tai tikrai ne visi ALR/RFID technologijos pritaikymo atvejai, tačiau daugeliui reikalingi saugūs duomenų apsikeitimai ar saugūs identifikacijos metodai.

2.3 ALR standartai

Artimo Lauko Ryšio technologija yra aukšto dažnio (radijo dažnis 13.56 MHz) bevielės komunikacijos technologija, kuri leidžia keistis duomenimis tarp įrenginių, ne didesniu nei 10 cm atstumu. ALR sąsaja ir komunikacijos protokolas tarp ypač arti esančių įrenginių (ne didesniu, nei 10 cm) gali būti standartizuojami ECMA-340 ir ISO/IEC 18092, dar kitaip vadinamais Artimo Lauko Ryšio Komunikacijos Sąsaja ir Protokolu-1 (angl. Near Field Communication Interface and Protocol-1 (NFCIP-1)). Šis standartas palaiko tris skirtingas perdavimo spartas: 106, 212 ir 424 kbit/s. Priklausomai nuo perdavimo spartos yra naudojamos skirtingos moduliacijos ir užkodavimo schemos.

Standartas taip pat apibrėžia ir komunikacijos režimus. ALR įrenginiai gali komunikuoti pasyviu arba aktyviu režimu. Pasyvus režimas yra ekvivalentiškas normalioms RFID tipo komunikacijoms, kur vienas įrenginys elgiasi kaip skaitytuvas, o kitas kaip pasyvi žymena (nuskaitomas objektas). Skaitytuvas radijo bangomis siunčia signalą, o žymena tuo tarpu indukavusi radijo bangas gražina skaitytuvui žymenas reikšmę. Aktyvus režimas yra tada, kai abu įrenginiai gali būti užmaitinami ir pakaitomis generuoja savo nuosavomis įterptinėmis žymių reikšmėmis, bei gali jas uždaryti (neperdavinėti reikšmių) kada laukia atsakymo. Šis režimas leidžia didesnę perdavimo spartą, nei prieš tai buvęs (t.y. 6,78 Mbit/s) [1].

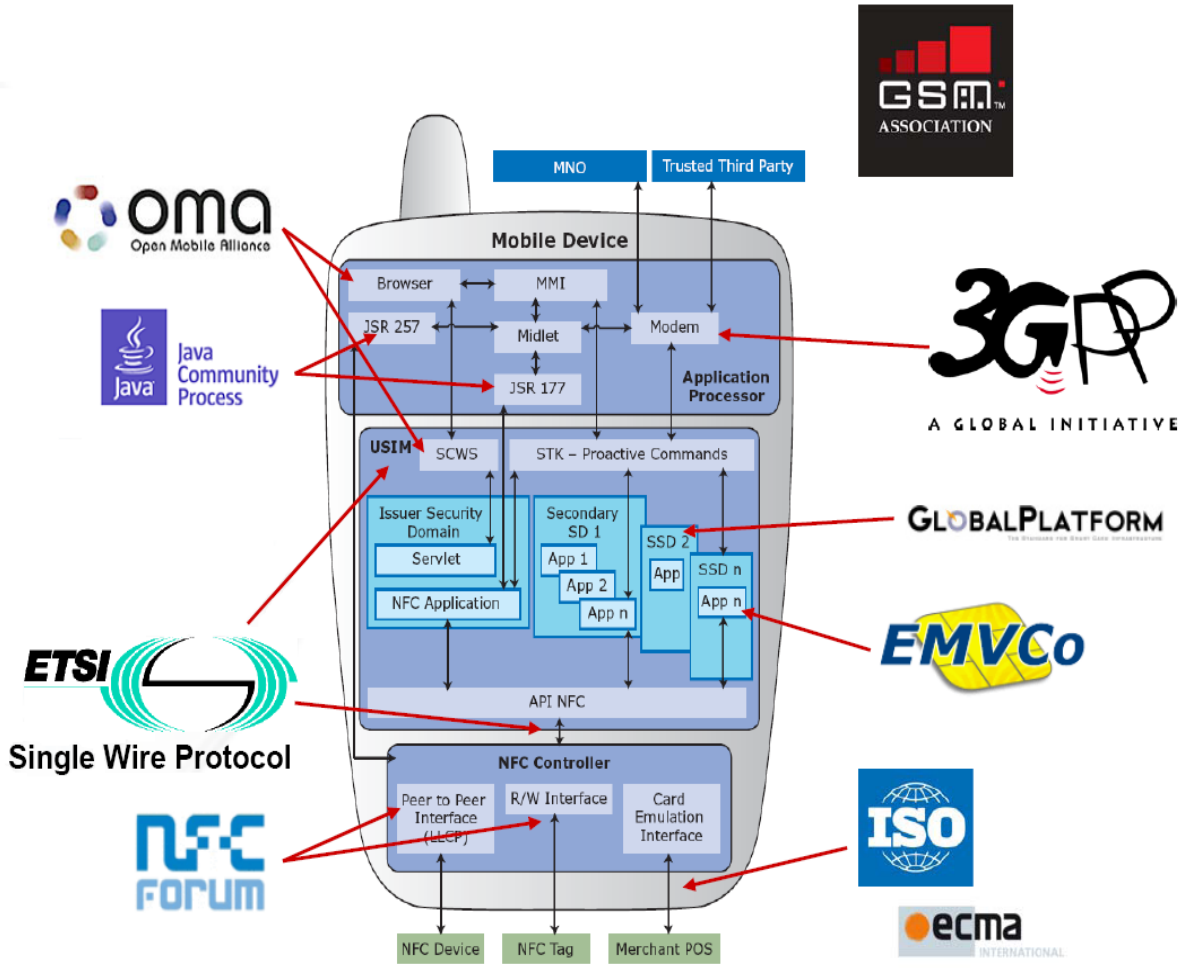
Vėliau NFCIP-1 standartas buvo išlėstas į ECMA-352 ir ISO/IEC 21481: NFCIP-2 (angl. Near Field Communication Interface and Protocol-2), integruoti NFCIP-1, ISO 14443 ir ISO 15693 standartai į vieną bendrą standartą. Šis globalus standartas apibrėžia vieną komunikacijos tipo aptikimo ir pasirinkimo mechanizmą iš trijų galimų apibrėžtų standartų[1].

Mobilusis telefonas su integruota ALR technologija gali veikti ir kaip aktyvus ir kaip

pasyvus prietaisas. Toks įrenginys turi tris pagrindinius operacijų režimus:

- **Kortelės Emuliacijos Režimas:** ALR įrenginys elgiasi kaip normali pasyvi bekontaktė kortelė (ISO 14443) [2], emuliuojama išmaniosios kortelės. Įrenginys yra pasyvus, taigi jis negeneruoja į radijo dažnio bangas (laukus). Šis režimas yra naudojamas apmokėjimuose ir bilietų pardavimuose.
- **Skaityti/Rašyti Režimas:** ALR įrenginys elgiasi kaip normalus aktyvus bekontaktis kortelių skaitytuvas. Telefonas generuoja radijo dažnio bangas (laukus), kad komunikuotų su bekontaktėmis kortelėmis, RFID žymenomis ar NFC Forum žymenomis. Gali nuskaityti informaciją esančią žymenose, bei įrašyti, pvz., kontaktinę informaciją, nuorodą į internetinį puslapį ar kitą nesudėtingą tekstinę informaciją į RFID žymeną, kurią palaiko telefonas.
- **Įrenginys su Įrenginiu Režimas:** Du ALR įrenginiai gali komunikuoti tarpusavyje (ISO 18092) [2]. Prietaisus priglaudus vienas prie kito, tarp jų galimas norimos informacijos apsikeitimas ar tarpusavio bendravimas.

  ISO 14443 (bekontaktėse išmaniosiose kortelėse) ir ISO 18092 (Įrenginys su Įrenginiu režime) standartuose nėra specifikuotas šifravimas ar apsauga tarp bekontakčių įrenginių komunikacijos [2]. Tai turėtų būti įdiegta ateityje: moduliai ar aplikacijos tų žmonių, kurie dirbs su tais įrenginiais ir kurs vienokias ar kitokias sistemas, kurios turės laikytis tam tikrų saugumo reikalavimų. Šiuo metu yra dvi pagrindinės firmos išmaniųjų kortelių, kurios vyrauja pardavimuose (NXP Semiconductors su savo produktu Mifare ir Sony su Felica produktu), kurios turi įgyvendintus produktus su patentuotais šifravimo algoritmais aukščiausio laipsnio komunikavimo saugumui užtikrinti.



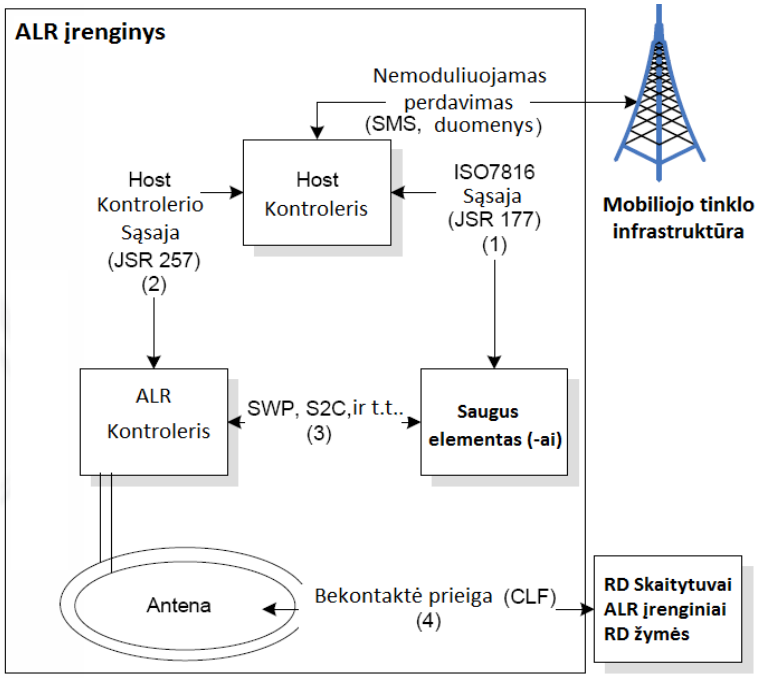
Pav. 1 ALR standartai mobiliajame telefone

2.4 Architektūra

ALR įrenginys (mobilusis telefonas) susideda iš keturių pagrindinių dalių: antenos, ALR kontrolerio, saugumo elemento ir pagrindinio kontrolerio (žiūrėti į Pav. 2). ALR kontroleris savyje turi analoginio skaitmeninio signalo konverterį duomenų perdavimui trumpu atstumu (iki 10 cm), bei ALR įrenginiai savyje turi apsaugotą išmaniosios kortelės mikroschemą. Ši integruota schema dar yra vadinama saugumo elementu (SE) iškviečiant žymenas emuliavimo operacijos režimui. Saugumo elementas yra sujungtas su ALR kontroleriu vykdyti artimoms operacijoms (išoriniu mokėjimo režimu už paslaugas ar pan.). Taip pat pagrindinis kontroleris turi galimybę keistis duomenimis su saugumo elementu (SE) (vidiniu režimu papildant pinigais išmaniąją kortele oro prieiga), tai iliustruota 2 Pav. . Fizinis ryšys tarp saugumo elemento ir ALR kontrolerio dar nėra apibrėžtas. Šiuo metu GSMA įvertina du skirtingus pasirinkimus: S2C (angl. Signal-in Signal-out Connection) ir SWP (angl. Single Wire Protocol, vieno laido protokolas),

tuo tarpu SWP yra labiausiai pasirenkamas ALR darbingume grupėse su GSMA. Skirtingos saugumo elemento realizacijos yra plačiai diskutuojamos čia [3].

ALR yra artimai susijęs su RFID (angl. Radio Frequency Identification). RFID yra daugiausiai naudojamas nuotoliniam stebėjimui ir identifikacijai daikto ar asmens taikomoje zonoje. ALR kai kuriuose vietose yra naudojamas labiau sudėtingesnės ir saugesnės operacijos kaip bevieliuose priėjimuose arba apmokėjimuose. Šios technologijos turi keleto sluoksnių ir prievadų principą, o tai atveria galimybes kai kurioms atakoms. [3]



Pav. 2 ALR integracijos schema mobiliajame telefone [3]

2.5 Mobilieji telefonai turintys ALR įrangą

Pats pirmasis komercinis mobilusis telefonas turintis ALR įrangą buvo Nokia 6131[13]. Tačiau bandomuosius telefonus su ALR įranga kūrė ir bandė ne vien Nokia, tai darė ir Motorola, Samsung, LG ir kitos įmonės užsiimančios mobiliųjų telefonų gamyba (pvz. Motorola L7 SLVR, LG 600V, Samsung SGH-X700N ir t.t.)

Šiuo metu turime jau keliolika telefonų su ALR technologija [13]. Pats naujausias mobilusis telefonas su NFC ir įterptiniu saugumo elementu yra **Samsung Galaxy S III.** Tai ne pirmas išleistas Samsung gaminys su įterptiniu saugumo elementu (pirmasis buvo Google Nexus S).

Nokia taip pat nenusileidžia Samsung gaminamiems telefonams ir išleido Nokia C7 [13] mobilųjį telefoną su ALR technologija, tačiau išleisti telefonai neturėjo dar programinės įrangos bendrauti su ALR įranga telefone. Tuo tarpu, Samsung telefonai su Android OS taip pat neturėjo priėjimo prie ALR įrangos, bet tai buvo greitai ištaisyta ir išleistos įdiegiamos programėlės, kurias galima parsisiųsti kiekvienam vartotojui.

Samsung išleistus telefonus (Nexus S ir Galaxy S II) vis dar gaubia Saugaus elemento paslapties šydas. Android kūrėjai teigia, jog šiuo metu kaip tik yra kuriama saugaus elemento pasiekiamumo technologija. Taigi, nors ir turėtume vieną iš šių telefonų liktumėme be galimybės naudotis šia funkcija. Telefonai su ALR išleisti tik Korėjos, Kinijos ir kai kurie modeliai Amerikos rinkoms, Europai dar teks kantriai luktelti šios technologijos. Belieka įsivaizduoti saugų elementą kaip vietą, kurioje bus laikomas parašytas tam tikras programos kodas (ar programėlė), teks taikyti šį principą, o kai jau bus išleista saugaus elemento specifikacija bus galima pakoreguoti identifikavimo programėlę.

2.6 ALR duomenų mainų formatas

Duomenų mainų Formatas (angl. NFC Data Exchange Format (NDEF)) [7] yra pagrindinis formatas, sukurtas tam, kad aprūpintų duomenis, nepriklausomus nuo užrašo ant kortelės tipo. NDEF duomenys yra kaupiami įrašuose ir žinutėse (žinutė apima vieno ar daugiau įrašų komplektą). Be tikrų duomenų, įrašas savyje turi informaciją apie duomenis, tokius kaip MIME tipas. NDEF apibrėžia duomenų tipus tokius kaip URI [8], Tekstas [9], ir Protingas Plakatas (angl. Smart poster) [10] įrašas. URI gali būti paprastu HTTP URL, ar daugiau telefoninio centrinio URI toks kaip telefonas ar sms. Teksto įraše yra patalpinta žmogaus informacija kartu su kalbos identifikatoriumi. Protingas Plakatas susideda iš daugialypių įrašų. Paprasčiausiu atveju SP (Protingas Plakatas), URI, ir Teksto įrašas. Papildomas tekstas ar atvaizdo įrašai yra galimi tuo metu, jei yra tik vienas URI įrašas, nes vienintelis Protingo Plakato tikslas yra suteikti papildomą informaciją apie URI vartotojui.

2.7 Java Card standartas

Java Card yra Java kalbos versija, kuri leidžia Java kalba parašytas programas vykdyti ribotų resursų sistemose, tokiose kaip mikroprocesorinės kortelės. Ši platforma plačiai naudojama mobiliųjų telefonų SIM kortelėse, įterpiniuose saugumo elementuose, banko kreditinėse bei debetinėse kortelėse. Java Card platforma leidžia rašyti objektiškai orientuotas programas, kurios palaikomos įvairiose mikroprocesorinėse kortelėse, todėl nereikia kiekvienai kortelei rašyti atskiros programos.

Programa veikianti Java Card platformoje yra vadinama apletu (angl. applet), o tokių apletų rinkinys yra vadinamas paketu. Kiekvienas apletas ir paketas turi unikalius identifikacijos numerius AID (angl. Application Identifier). Šio numerio pagalba galima trinti, diegti ir pasirinkti darbui atskirus apletus ir paketus. Java Card technologija nuo pirmos dienos buvo kuriama suteikiant didelę svarbą saugumui ir duomenų apsaugai. Kiekvienas apletas ir jam priklausantys duomenys yra atskirtas ugniasiene nuo kitų apletų ir izoliuotas nuo sistemos branduolio. Duomenys gali būti nuskaitomi ir perduodami tik per tam tikslui sukurtus specializuotus metodus (nėra tiesioginio priėjimo prie duomenų Java Card sistemoje). Kad galėtų veikti ribotų resursų sistemose, Java Card palaiko tik dalį Java kalbos:

- Java Card 3.0 versijoje palaikomi visi kintamųjų tipai išskyrus float ir double..
- Nepalaikomi daugiamačiai maysvai.
- Nepalaikomas dinaminis klasių užkrovimas, objektų serializacija ir klonavimas.
- Java Card 3.0 versijoje palaikomas šiūkšlių surinkimas (angl. Garbage Collector).
- Palaikomi paketai, klasės, interfeisai, paveldėjimas, virtualūs metodai, metodų perdengimas, išimčių valdymas.

Java Card platformos programos yra pirmiausia sukompiliuojamos ir sukuriami ’class’ failai, kaip ir naudojant standartinę Java SE platformą. Tuomet klasių failai yra konvertuojami ir sukuriamas .CAP failas, kuris apjungia visas klases. Konvertavimo tikslas yra patikrinti klasių tinkamumą ir optimizavus kodą, sukurti paketą, tinkantį Java Card platformai. Tuomet .CAP failas yra patalpinamas į Java Card kortelę ir gali būti naudojamas Java Card interpretatoriaus.

Dėl apribotų resursų sudėtingi kriptografiniai algoritmai yra realizuoti specialiai tam paruoštame kriptografiniame procesoriuje. Java Card yra realizuotas API skirtas darbui su kriptografinėmis funkcijomis ir modeliais. Darbui su kriptografiniais metodais klases galima rasti javacard.security ir javacardx.crypto paketuose.

- KeyBuilder - klasė skirta kriptografinių raktų generavimui.
- KeyPair - klasė skirta privataus ir viešo rakto poromos saugoti.
- MessageDigest - kriptografinės vienkryptės funkcijos (MD5, SHA-1, SHA-256 ir kitos).
- RandomData - klasė skirta atsitiktiniams skaičiams generuoti.
- Signature - DSA, RSA ir kitus algoritmus palakanti klasė, leidžianti pasirašyti duomenis.
- Cipher - RSA, AES ir kitus algoritmus palaikanti šifravimo klasė.

Java Card platformos trūkumas yra tai, kad nėra galimybės prieiti prie kriptografinio procesoriaus tiesiogiai, norint atlikti tokius veiksmus kaip modulinė daugyba. Dėl to labai apsunkinamas naujų kriptografinių modelių ir schemų diegimas į Java Card mikroprocesorines korteles.

2.8 Grėsmės

Kaip ir kiekviena technologija, taip ir ALR technologija turi tam tikro pobūdžio pažeidžiamumų kategorijas. Šiame skyriuje mes apžvelgsime egzistuojančius mobilių prietaisų pažeidžiamumus. Į tokius žmogaus faktorius kaip telefono ar PIN pametimo, atskleidimo, veiksmus neatsižvelgsime, nes tai nėra technologinė pusė, visa tai liečia socialinę duomenų sužinojimą ar tiesiog asmens aplaidumą saugojant svarbius daiktus ar duomenis.

2.8.1 DoS ataka (angl. Denial of Service — „atsisakymas aptarnauti“)

DOS ataka gali būti naudojama norint suardyti, sunaikinti patikimą ryšį tarp kliento ir paslaugos tiekėjo. Tai liečia ir ALR įrenginius netgi su tuščiomis žymenomis, o priežastis yra reakcija į tuščią žymę. Tada įrenginys gauna netaisyklingas NDEF žinutes, kurios priverčia telefoną sutrikti ir persikrauti [4]. Netgi jei tai yra tik klaidos pranešimas, o tai jau yra lengviausias būdas užimti (užvaldyti) įrenginį. Reiškias turėtų būti koks nors kontrolės mechanizmas vartotojui, kuris leistų jam išjungti ALR skaitymo/rašymo funkcijas [2].

2.8.2 Phishing ataka

Tai tokia sukčiavimo forma prieš vartotojus kai pasinaudojant falsifikuotomis techninėmis priemonėmis, ištekliais ar dirbtiniais tiekėjo tvirtinimais, siekiama išgauti vartotojo privačius duomenis (telefono, banko sąskaitos numerius ir t.t.). Kliudymas priliesti žymę, nuskaityti mobiliuoju telefonu ar padaryti būsimą prisijungimą laidu yra tikriausia mažiausiai tikėtinas. Taigi ši phishing'o ataka gali būti lengvai įvykdoma modifikuojant ar pakeičiant žymę. Tai yra paprasčiausias ir nebrangiausias būdas apgauti vartotoją. Tačiau naudojant parašus žymenoms ir transportavimui turbūt tinkamiausias kelias išvengti šios problemos [2].

2.8.3 Leidimas pasiekti unikalų ID

Unikalus ID yra specifikuotas prieš susidūriminiame (andl. anti-collision) standarte, paprasčiausia aparatinė įranga kaip OpenPICC [5] leidžia patikrinti šią informaciją. Vadinasi taikomosios programos pagrįstos unikaliuoju ID išduoda unikalų ID ne vien tik privačiam savininkui, bet taip pat ir aplikacijoms bandančioms naudotis tuo. Taip pat ID gali būti įgytas, perimtas prarandant komunikacijos kanalą tarp skaitytuvo ir išmaniosios kortelės lusto jei tai nėra

šifruojama. Šis privatumas gali būti išsprendžiamas naudojant atsitiktinius skaičius prieš susidūrime (angl. anti-collision), kaip dabar naudojama ALR taikiniuose ir e-pase. Tačiau tai negali būti naudojama sekime ar identifikacijoje [2].

2.8.4 Nepatikima sąsaja

Daugeliu atvejų, saugumo klausimas susilieja į vieną, todėl, kad norima išsiaiškinti, ar iš tikrųjų egzistuoja vartotojų pasitikėjimo sąsaja. Kadangi kenkėjiškos programos ar virusai gali užpulti mobilius prietaisus, kurie tapo tokie pat sudėtingi kaip asmeniniai kompiuteriai, ši prielaida gali ne visada būti teisinga. Be to, yra daug programų susijusių su naršyklės pažeidžiamu. Tačiau, kai kuriais atvejais, kurie išvardinti toliau, mes manome, kad mobilus prietaisas apskritai yra saugesnis negu įprastas daiktas [6].

2.8.5 MITM ataka (angl. Man-in-the-middle-attacks)

Net geriausia apsauga prieš fizines atakas ir neįveikiamą užšifravimo planą nepadeda, jei protinga kortelė negali identifikuoti abiejų pusių. Ypač internetinio autentiškumo nustatymo atveju, kai informacija yra perduodama per daugelį kanalų, šis pažeidžiamumas tampa rimta svarstoma problema. Puolėjas gali įsiskverbti tarp serverio ir protingos kortelės. Net jei kanalas yra užkoduotas ir abi pusės mano, kad jie kalba su vienu kitu, tačiau puolėjas gali perimti, pašalinti ar pakeisti informaciją [6]. Paprasčiausias būdas apsisaugoti nuo šios rūšies atakų yra abipusis autentiškumo nustatymas.

2.8.6 Kriptografinis puolimas

Šios atakos išskirsto šifruotus algoritmus. Šie algoritmai yra nuolatos peržiūrimi mokslinės visuomenės. Šitos kriptografinės atakos ilgainiui ves į didesnių raktų būtinybę.

2.8.7 Šnipinėjimas (angl. Eavesdropping)

Vykstantį bendravimą ar perduodamą informaciją tarp dviejų prietaisų galima šnipinėti tam tikru atstumu. Šiuo atveju, puolėjas iš pradžių gali įrašyti informaciją būdamas kuo arčiau ir vėliau gali iššifruoti gautą informaciją su tinkama įranga. Populiariausias pavyzdys šiam pažeidžiamumui iliustruoti yra žinoma silpnybė pagrindinėje prieigos kontrolėje - (BAC) mechanizmas, išdėstytas elektroniniuose pasuose [6].

2.8.8 Sekimas

Daugeliu atvejų, sujungti prietaisai turi unikalų identifikavimo numerį (UID), kurį jie siunčia norėdami save identifikuoti. Tai leidžia sukurti sąlygas sekti asmenis, besinaudojančiais tokiais prietaisais. Pavyzdžiui, žmogus, besinaudojantis sujungtu su išore prietaisu (pavyzdžiui, ALR-

įgalintas mobilaus ryšio telefonu) eina pro ALR skaitytuvą (pavyzdžiui, integruotą į parduotuvių įėjimo vartus), stebėjimo sistema gali sukaupti UID duomenų bazėje [6]. Ilgainiui stebint būtų sukurtas specifinis asmens judėjimų profilis.

2.8.9 Duomenų įterpimas

Ši ataka gali būti įgyvendinta jei tik yra pakankamai laiko nusiųsti įterptą žinutę prieš tikrąjį prietaiso pradėjimą siųsti atsakymą. Jei įvyksta kolizija, duomenų apsikeitimas turi būti iškart sustabdytas . Norint apsisaugoti nuo tokio tipo atakų, prietaisas turi būti taip nustatytas, kad nesiųstų atsakymų su uždelsimu.

2.8.10 Klonavimas

Naujoji kortelė gali būti sukurta su tokiu pačiu turiniu kaip originalioji (tokios kaip Mifare Classic). Brangesnės kortelės (ar žymenos) gali turėti savyje logiką (veikimo principą), kuri neleidžia nuskaityti viso turinio, taip apsunkindama visiškai tikslų klonavimą/kopijavimą. Integruotas saugusis elementas gali būti pakeičiamas nauju, tačiau tam reikalingas fizinis priėjimas prie mobiliojo telefono pagrindinės mikroschemos.

Klonuotos žymenos nėra tokios įdomios puolėjui kaip klonuotos kortelės, tačiau turime būti atsargūs tikrindami ir tą pačią žymę.

2.9 Egzistuojantys RIFD identifikacijos/autentifikacijos metodai

Daugelyje šių laikų sistemose naudojami įvairūs identifikavimo ir autentifikavimo metodai, bei kriptografiniai algoritmai. Tačiau nereikia pamiršti, jog mobilieji telefonai dar nėra tokie spartūs, kaip dabartiniai mūsų kompiuteriai. Todėl autentifikacijos ir identifikacijos algoritmai ir metodai turi būti gerai pasverti ir apgalvoti, jog tenkintų keliamus saugumo reikalavimus, bei būtų įgyvendinti mobiliuosiuose telefonuose su ALR technologija. Mes apžvelgsime keletą autentifikacijos ir identifikacijos sistemų, kurios naudojamos telefonuose, jog susipažintumėme ir suprastume jų galimybes.

Lentelė Nr. 1 Išbandyti protokolai RFID sistemose su būdingais pažeidžiamumais

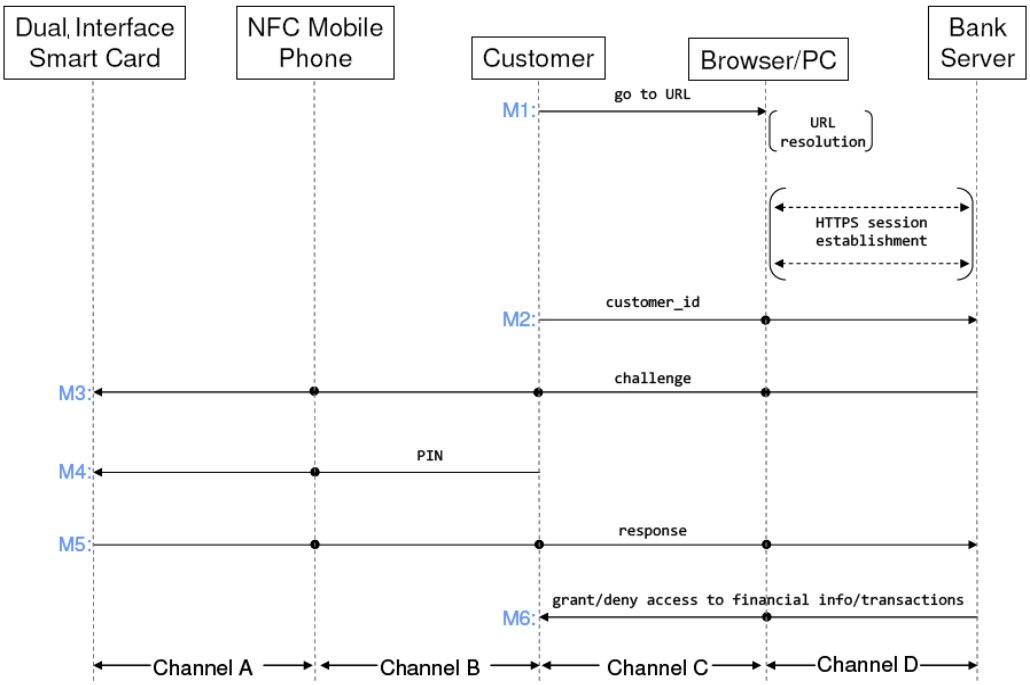
Atakos / Protokolai	Informacijos privatumo	Vietos privatumo	Pakartojamumo ataka	DOS ataka	Persiuntimo saugumas
Weise ir kitų aut. [15]	Nėra	Yra	Nėra	Nėra	Nėra
Ohkubo ir kitų aut. [16]	Nėra	Nėra	Yra	Nėra	Nėra
Chen ir kitų aut. [17]	Nėra	Yra	Yra	Nėra	Nėra
Molnar ir kitų aut. [18]	Nėra	Nėra	Nėra	Nėra	Yra
Li-Wang ir kitų aut. [19]	Nėra	Nėra	Nėra	Yra	Nėra

2.9.1 Bankinės autentifikacinės sistemos technologijos ir standartai

Tipinis e-Bankininkystės scenarijus gali būti apibrėžtas taip: klientas naudodamasis internetine naršykle, bei internetu gauna prieigą prie e-Bankininkystės portalo. Po to, kai jis yra sėkmingai autentifikuojamas jam yra pristatomas pasirinkimo meniu ekrane. Galiausiai, jis gali pradėti duomenų mainus užpildydamas formas ir vykdydamas reikiamus pasirinktus veiksmus. [11]

2.9.2 Kliento autentiškumo nustatymo protokolas

Panagrinėsime kliento autentiškumo nustatymo protokolą, kuris apibūdintas apačioje esančiame paveikslėlyje.



Pav. 3 Kliento autentiškumo nustatymo protokolas

1. Klientas įveda e-Banko svetainės adresą naršyklėje (M1).
2. Atidaromas e-Banko internetinė svetainė. HTTPS sesija yra nustatoma tarp banko ir naršyklės naudojant D kanalą.
3. Serveris siunčia formą naršyklei su vartotojo-ID lauku.
4. Vartotojas surenka savo vartotojo-ID naršyklėje, pavyzdžiui tai gali būti kažkoks pranešimas ar sutarties numeris (M2).
5. Serveris atsako į užklausą siųsdamas atsitiktinį skaičių, kuris susideda iš 6 ar maksimum 8 skaitmenų , taip susiedamas SSL ryšį ir kliento vartotojo-ID, kurį gavome ankstesniame (M3) žingsnyje.
6. Vartotojas pasileidžia MIDlet programinę įrangą telefone.
7. Vartotojas pasirenka Log-in režimą(MIDlet programoje) ir surenka gautą iš serverio atsitiktinį skaičių savo telefone. (M3)
8. Klientas suveda savo PIN į telefoną (M4).
9. Telefonas siunčia užklausą ir PIN į kortelę, už tai gaudamas kriptogramą mainais.
10. Vartotojas siunčia atsakymą serveriui, pateikdamas tai tinkamame WEB formos lauke.
11. Serveris tikrina, kad gautas atsakymas atitiktų prieš tai išsiųstą užklausą (Pav. 3). Jei atsakymas yra galiojantis, bankas perduoda klientui jo pranešimo reziume, kaip tinkamą duomenų perdavimo pasirinkimą (M6).

12. Vartotojas gali įvykdyti transakciją pasirinkdamas tinkamą pasirinkimą ir užpildydamas būtinus laukus. Joks tolimesnis autentifikavimas nevyksta, nebent praeina kiek nors laiko nieko nedarant (priklausomai nuo serverio nustatymų).[11]

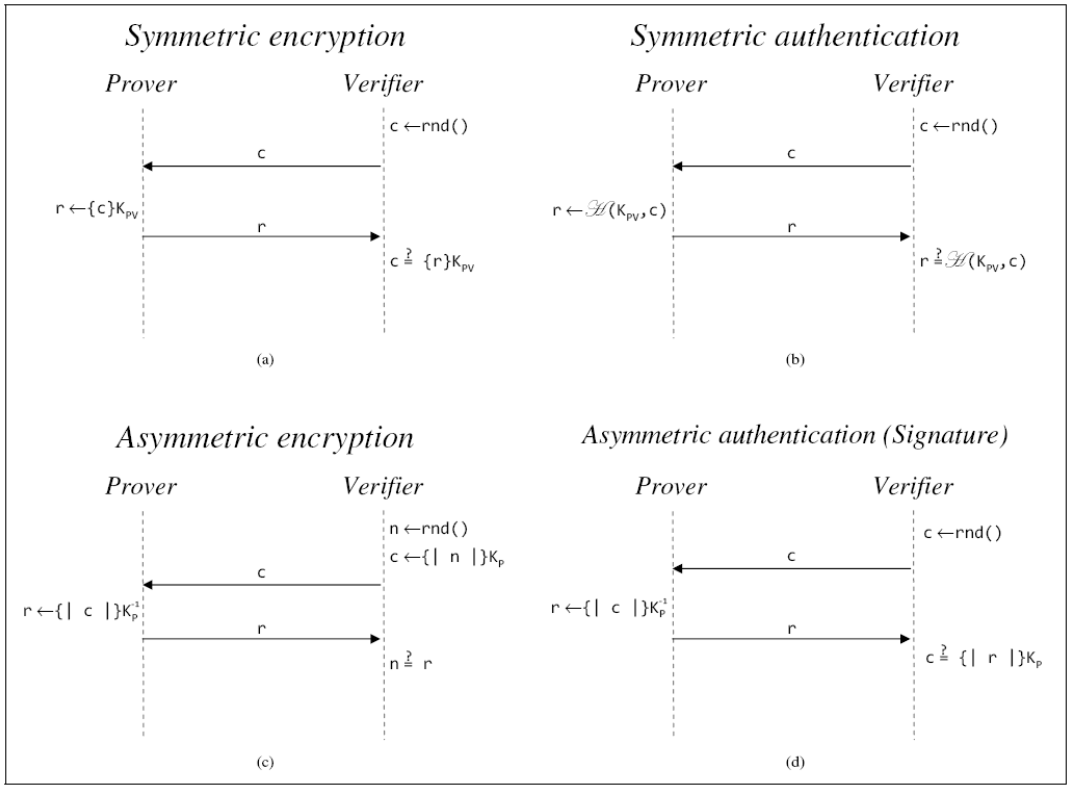
Aišku, kad kliento autentiškumą nustato bankas. Naudojamas Saugaus Kanalo Sluoksnis ir Transportinis Sluoksnio Saugumas(angl. SSL/TLS). Klientas įrodydamas, jog sugeba sukurti tinkamą atsakymą, atsitiktinei užklausai atsiųstai iš banko serverio, gali pradėti bendrauti su serveriu. O kad taip padarytų, jis turi pasinaudoti savo kortele ir jos atitinkamu PIN, kuris iš tikrųjų yra panaudotas, jog nustatytų kortelės autentiškumą. Taigi natūralu, jog vertinga informacija (objektai) turi būti apsaugoti, o tai yra PIN ir išmanioji kortelė. O apsaugai yra taikomi įvairiausi standartai, priklauso su kokiu telefono lygmeniu bendraujama (žiūrėti Pav. 1).

2.9.3 Autentifikacija

Yra du būdai pasiekti duomenų autentiškumą ir abu naudoja kriptografinę techniką. Pirmas sudaromas apskaičiuojant MAC informaciją, naudojant simetrišką raktą K pasidalintą tarp šalių: autentiškos informacijos vientisumo nustatančios ir vientisumą patikrinančios šalies. Antras būdas susideda iš skaitmeninio parašo (asimetrinė kriptografija), šiuo būdu duomenys yra pasirašyti, naudojant privatų raktą K, kuris yra saugomas sertifikuotų centrų.

4 Pav. (a) dalyje yra parodytas simetrinio šifravimo protokolas, kuriame abi šalys dalinasi simetriniu raktu K_{PV}. Tikrintojas (Verifier) sugeneruoją atsitiktinį tekstą c ir siunčia asmeniui (Prover). Tas naudodamasis simetriniu K_{PV} raktu užšifruoja gautą žinutę ir siunčia tikrintojui (Verifier). Tikrintojas gavęs žinutę paveikia ją simetriniu raktu ir sutikrina ar pradinis tekstas atitinka iššifruotą tekstą. Taip patikrinama ar abi šalys naudojasi tuo pačiu simetriniu raktu. O toliau bendravimas vyksta kiekvieną žinutę užšifruoja/dešifruojant simetriniu K_{PV} raktu.

4 Pav. (b) dalyje yra parodytas simetrinės autentifikacijos protokolas, kuriame abi šalys taip pat naudojasi simetriniu raktu, tačiau jau yra pasitelkiama $H(K_{PV}, c)$ funkcija, kuri gražina žinutės autentifikavimo kodą. Sukūrus žinutės autentifikavimo kodą siunčiame tikrintojui. Tikrintojas (Verifier) panaudodamas funkciją patikrina ar ta žinutė yra nuo vartotojo.



Pav. 4 Užklausos/atsakymo protokolas

4 Pav. (c) dalyje yra parodytas asimetrinio šifravimo protokolas, kuriame tikrintojas sugeneruoją atsitiktinę žinutę ir pasirašo savo viešuoju raktu K_P. Tada tą žinutę gavęs asmuo nustato autentiškumą panaudodamas privatų raktą. Gavęs kažkokią reikšmę siunčia tikrintojui, jis tada patikrina ar asmuo gavo tokią pačią žinutę, kaip kad buvo išsiųsta.

4 Pav. (d) dalyje yra parodytas asimetrinės autentifikacijos protokolas, kuriame tikrintojas išsiunčia atsitiktinę žinutę asmeniui, kuris turi ją pasirašyti savo privačiuoju raktu ir siųsti atgal tikrintojui. Tikrintojas gavęs pasirašytą žinutę turi patikrinti ją ir nustatyti ar ji yra nuo to asmens.

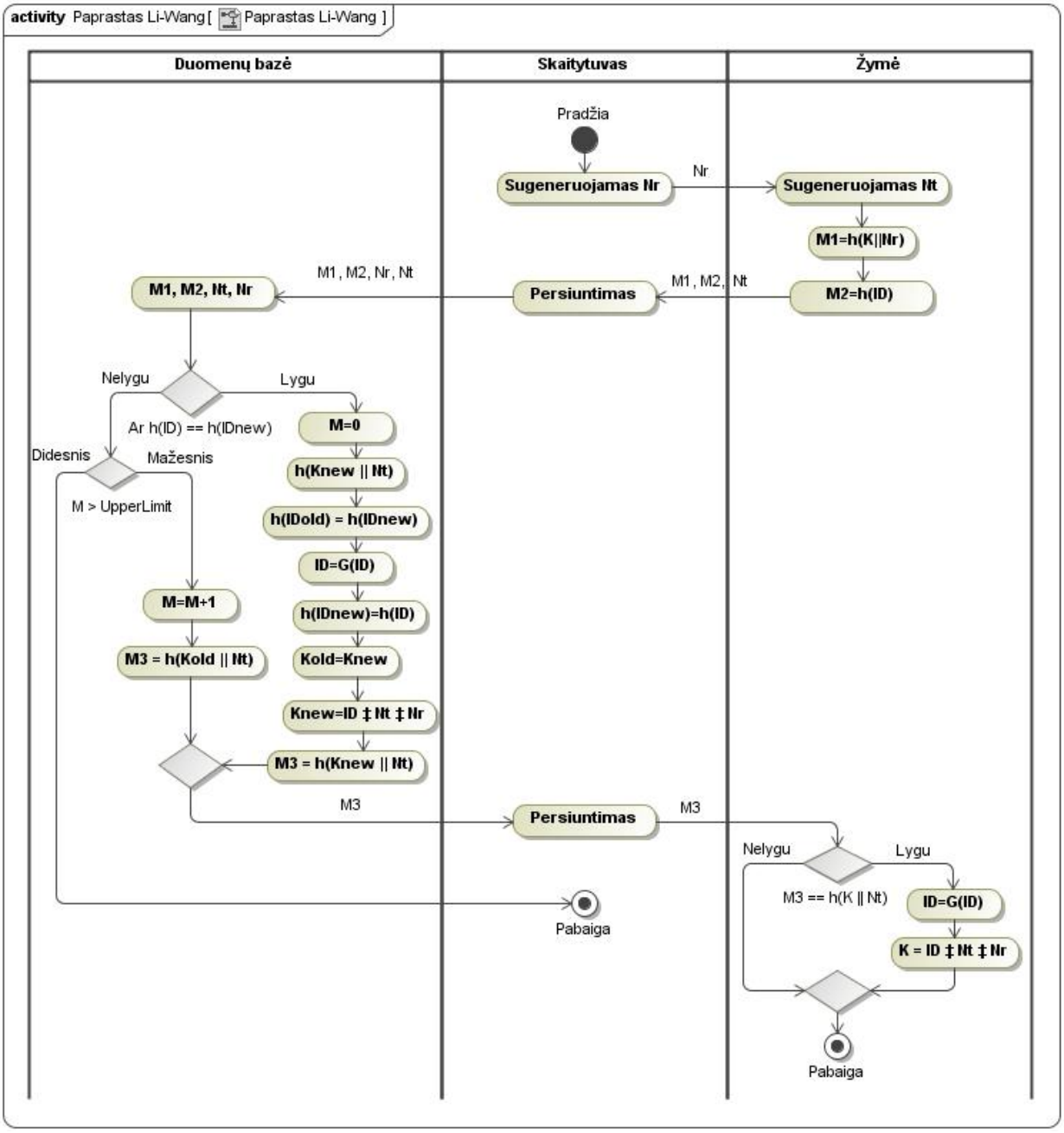
Simetrinio rakto sistema turi vieną minusą, reikia kažkaip pasikeisti tarp šalių simetriniu raktu K_{PV}, jog jis nebūtų niekam matomas. Asimetrinei autentifikacijai reikalingi sertifikavimo centrai, kurie saugotų informaciją apie asmenų privačiuosius raktus. Tokie autentifikacijos ir šifravimo principai yra taikomi mobiliuosiuose telefonuose jungiantis ar bendraujant su bankinėm sistemom.

2.9.4 Li-Wang protokolo apžvalga

Šis protokolas yra paremtas vienkryptėmis funkcijomis, naudojami žymėjimai yra aprašyti Priedas Nr. 1.

Susijungimas tarp serverio vyksta saugiu kanalu, o susijungimas tarp žymenos ir skaitytuvo vyksta nesaugiu kanalu, kuriuo pasinaudodamas atakuotojas gali klausytis perduodamos informacijos. Skaitytuvas turi pseudo atsitiktinių skaičių generatorių, žymena gali generuoti atsitiktinius skaičius ir apskaičiuoti vienkryptę (hash) funkciją. Identifikacijos procesas susideda ir penkių žingsnių (žiūrėti Pav. 5):

1. Skaitytuvas siunčia atsitiktinį skaičių N_R žymei.
2. Žymena generuoja N_T ir apskaičiuoja $M1=h(K||N_R)$ ir $M2 = h(ID)$, ir tada siunčia M1, M2 ir N_T skaitytuvui.
3. Po to , kai skaitytuvas gauna M1, M2 ir N_T iš žymenos, tada skaitytuvas persiunčia M1, M2, N_T ir N_R į serverį.
4. Serveris patikrina ar h(ID) yra lygi su $h(ID_{old})$ ar su $h(ID_{new})$. Serveris nustato M =0, paskaičiuoja $h(K_{new}||N_T)$ ir atnaujina duomenų bazės įrašus $h(ID_{old})=h(ID_{new})$, ID= G(ID), $h(ID_{new})=h(ID)$, $K_{old}=K_{new}$ ir $K_{new}=ID\oplus N_T\oplus N_R$ jei $h(ID_{new})$ lygi h(ID). Tada serveris apskaičiuoja M = M+1, $h(K_{old}||N_T)$ ir vis dar naudoja ID_{old} kadangi serveris neatnaujina duomenų bazės įrašų jei h (ID_{old}) lygus h (ID) ir M <*UpperLimit*. Čia *UpperLimit* apibrėžia saugumo lygį, kurį nustato sistemos administratorius. Kada *UpperLimit* yra maža reikšmė tada sistema turi aukštą saugumo lygį ir kada *UpperLimit* reikšmė yra maža, tada saugumo lygmuo yra žemas. Toliau serveris siunčia $h(K_{old}||N_T)$ ar $h(K_{new}||N_T)$ skaitytuvui.
5. Skaitytuvas persiunčia $h(K_{old}||N_T)$ ar $h(K_{new}||N_T)$ žymei kur nuspręsta $h(ID_{old})=h(ID)$ ar $h(ID_{new})=h(ID)$. Žymena apskaičiuoja $h(K||N_T)$ ir palygina tai su gauta reikšme iš serverio. Toliau žymena atnaujina ID=G(ID), $K=ID\oplus N_T\oplus N_R$ jei $h(K||N_T)$ yra lygi su gautąja reikšme.



Pav. 5 Li-Wang identifikacijos veiksmų diagrama

Saugumo specialistai teigia, jog Li-Wang protokolas turi tik DOS atakos pažeidžiamumą. Taip pat atakuotojas turi galimybę sugadinti sinchronizaciją tarp žymenos ir duomenų bazės įrašų, kurie saugo tam tikras reikšmes joje. Tai atlikus atsiranda galimybė įvykdyti DOS ataką, nes tarp duomenų bazės ir žymenos nebėra bendrų reikšmių (kintamųjų ID, K) [14].

2.10 Viešojo rakto infrastruktūra

Viešojo rakto infrastruktūra (angl. Private Key Infrastructure) susideda iš trijų sluoksnių: Sertifikatų Centro (SC), banko ir integruotos kortelės (išmanioji kortelė). SC turi raktų porą [P_{SC}, V_{SC}], kur privatus raktas P_{SC} naudojamas pasirašyti banko viešojo rakto sertifikatą. O banko privatus raktas P_B yra panaudojamas pasirašant integruotosios kortelės viešojo rakto sertifikatą.

Tuo tarpu integruotoji kortelė turi dvi sertifikuotas asociacijas su dviem raktų poromis: pirmasis viešojo rakto sertifikatas [C_{AUTH}]B siejamas su raktų pora [P_{AUTH}, V_{AUTH}] ir antrasis integruotoje kortelėje įdiegto PIN viešojo rakto sertifikatas [C]B siejamas su raktų pora [P_C,V_C]. Skirtumas tarp šių dviejų sertifikatų ir susietų rakto porų yra ta, kad pirma yra atliekamas kortelės autentifikacijos mechanizmas ir po to tik atliekamas PIN konfidencialumo mechanizmas.

2.11 Kriptografiniai algoritmai ir slapti raktai SIM kortelėje

Slapčiausia SIM kortelės informacija yra šifruojama A3, A5, A8 algoritmais ir naudojami slapti raktai Ki, PIN, PUK ir Kc. Praktiškai, A3 ir A8 yra dažniausiai įgyvendinami kartu (dar žinomi kaip A3/A8). A3, A8 algoritmas yra įrašytas į SIM kortelę gaminimo procese, ir dauguma žmonių negali perskaityti A3, A8 algoritmo. Srauto šifras dar žinomas kaip A5 algoritmas. Jis turi dar keletą skirtingo lygio šifravimą:

- A5/0: jokio užšifravimo.
- A5/1: originalus A5 algoritmas panaudotas Europoje.
- A5/2: silpnesnis užšifravimo algoritmas, sukurtas eksportui, perkėlimui.
- A5/3: stiprus užšifravimo algoritmas, sukurtas kaip dalis 3-iojo Generation Partnership Project (3GPP).[12]

SIM kortelė visada yra užrakinta, o norint pasiekti joje esančią informaciją (slaptus raktus ar algoritmus) reikia suvesti teisingą PIN kodą, kuris atrakina kortelę.

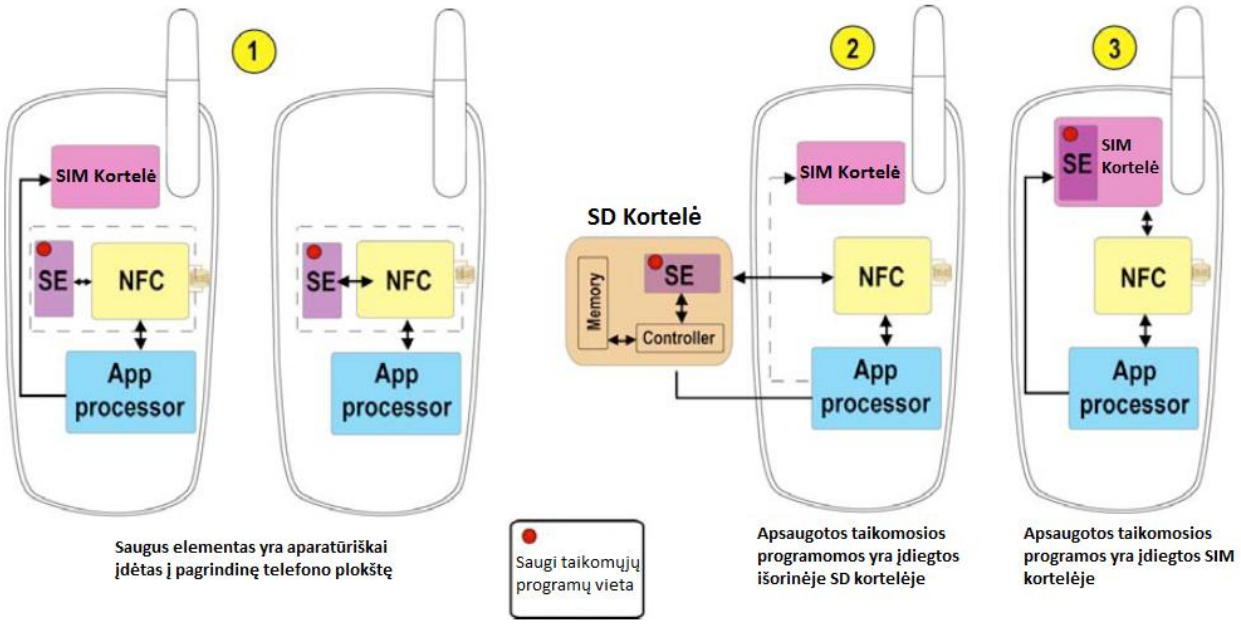
2.12 Saugus elementas

Saugus elementas (saugi atmintis ir vykdymo aplinka) yra dinamiška aplinka, kurioje taikomasis kodas ir taikomieji duomenys gali būti saugiai kaupiami, saugomi ir valdomi saugiai vykdant veiksmus.

Mobilusis telefonas su ALR technologija gali palaikyti trijų tipų saugumo elementus:

- Įdiegta fiziškai telefone - apsaugotos taikomosios programos ir raktai yra fiziškai įdiegti pagrindinėje telefono mikroschemoje (žiūrėti 5 paveikslėlį, 1-oje schemoje).

– SIM kortelėje - apsaugotos taikomosios programos ir raktai yra įdiegtos USIM/SIM telefono kortelėje (žiūrėti 5 paveikslėlį, 3-oje schemoje)..
– (micro)SD kortelėje - apsaugotos taikomosios programos ir raktai yra įdiegti (mikro)SD kortelėje (žiūrėti 6 paveikslėlį, 2-oje schemoje)..



Pav. 6 1-Įterptinė, 2-(mikro)SD, 3-USIM/SIM kortelėje saugaus elemento sprendimai

2.13 Išvados

1. Išanalizavome Artimo Lauko Ryšio technologiją, duomenų mainus tarp ALR įrenginių ir paslaugos tiekėjo.
2. Atlikome saugių elementų analizę ir padarėme išvadą, kad įterptinis saugumo elementas yra labiau apsaugotas nuo galimybės nepastebėtam pasisavinti duomenis ar juos klonuoti.
3. Apžvelgėme galimas grėsmės ALR technologijoje ir pasirinkome pašalinti Li-Wang identifikavimo algoritmo saugumo problemą: sugadinti sinchronizaciją tarp žymenos ir duomenų bazės.
4. Sužinojome, jog į įterptinius saugumo elementus galima įrašyti apletus , kuriuos apdoroja viena iš JAVA CARD OS modifikuotų versijų.

3 ALR IDENTIFIKACIJAI SKIRTAS PROTOKOLAS

Atsižvelgdami į informaciją, kurią gavome analizės etape siūlome Li-Wang identifikacijos protokolą, kuris tiktų vartotojo identifikavimui įvairiose elektroninėse paslaugose ir naudotų ALR technologiją. Protokolas taikytinas ir gali būti naudojamas telefone, nes nereikia atlikinėti itin sudėtingų skaičiavimo operacijų. Dinamiškai keičiasi raktai tiek pas klientą, tiek serveryje. Perduodami duomenys yra šifruojami vienkryptėmis funkcijomis.

3.1 Darbo tikslas ir uždaviniai

Kaip alternatyvą įvairiems slaptažodžiams ir kitokiems raktams saugoti galima naudoti mobiliuosius telefonus su įterptiniais saugumo elementais ir ALR technologija. Taigi ryšio užmezgimo pradžioje ALR skaitymo terminalas aptikęs įrenginį siųs pranešimą mobiliajam įrenginiui, kuriame bus nurodytas identifikavimo aplikacijos pavadinimas (identifikavimo programėlės kodinis pavadinimas). Tada telefone esantis ALR užklausų apdorojimo servisas išrinks tinkamą identifikavimo aplikaciją iš visų palaikomų telefone. Telefonas, išsirinkęs aplikaciją inicijuos identifikaciją. Taip pradės vykti duomenų perdavimas/priėmimas, po kurių vartotojas bus identifikuojamas arba neidentifikuojamas sistemoje.

3.1.1 Darbo tikslas

Pritaikyti Li-Wang identifikavimo protokolą mobiliuosiuose telefonuose su ALR technologija ir pašalinti sinchronizacijos tarp žymenos ir duomenų bazės problemą.

3.1.2 Uždaviniai

Kadangi literatūra jau išnagrinėta, naudojami identifikavimo metodai aptarti, apžvelgtos naudojamos technologijos, uždavinius formuluojame tolesnėms šio darbo dalims.

- Apsibrėžti sudaromo identifikacijos protokolo taikymo sritį
- Apsibrėžti, kokius reikalavimus turi tenkinti sudaromo protokolo realizacija
- Aprašyti Li-Wang protokolo pakeitimus identifikavimo algoritme
- Aprašyti apsikeitimo pranešimus tarp sistemų ir sistemoje esančių komponentų
- Nurodyti saugume elemente ir duomenų serveryje saugomus duomenis
- Programiniu būdu realizuoti sudarytą protokolą eksperimentui atlikti

- Eksperimento metu nustatyti sudaryto protokolo efektyvumą pagal užsiduotus kriterijus
- Pagal gautus rezultatus parašyti darbo išvadas

3.2 Taikymo sritis ir reikalavimai identifikavimo protokolui

Taikymo sritį galima numanyti iš darbo pavadinimo ir analizės dalyje nagrinėtų problemų bei technologijų. Identifikacijos algoritmą taikysime naujausioje srityje: mobiliuosiuose telefonuose su ALR technologija panaudojime. Identifikacijos neapsieina be specialių algoritmų ir juose naudojamų vienkrypčių funkcijų ir raktų.

Rakto saugumas yra tiesiog proporcingas jo ilgiui ir skirtingų simbolių kiekiui, iš kurių jis sudarytas. Vadinasi kuo ilgesnis ir kuo iš įvairesnių simbolių sudarytas raktas, tuo jis saugesnis ir sunkiau atspėjamas ar nulaužiamas.

Apsibrėžę taikymo sritį ir norimą gauti rezultatą, nustatykime pagrindinius reikalavimus, kuriuos turi tenkinti sudaromas identifikavimo algoritmas. Reikalavimų šioje dalyje labai nedetalizuojame – tai padarysime projektinėje dalyje. Taigi tobulinamas identifikavimo turi tenkinti šiuos reikalavimus:

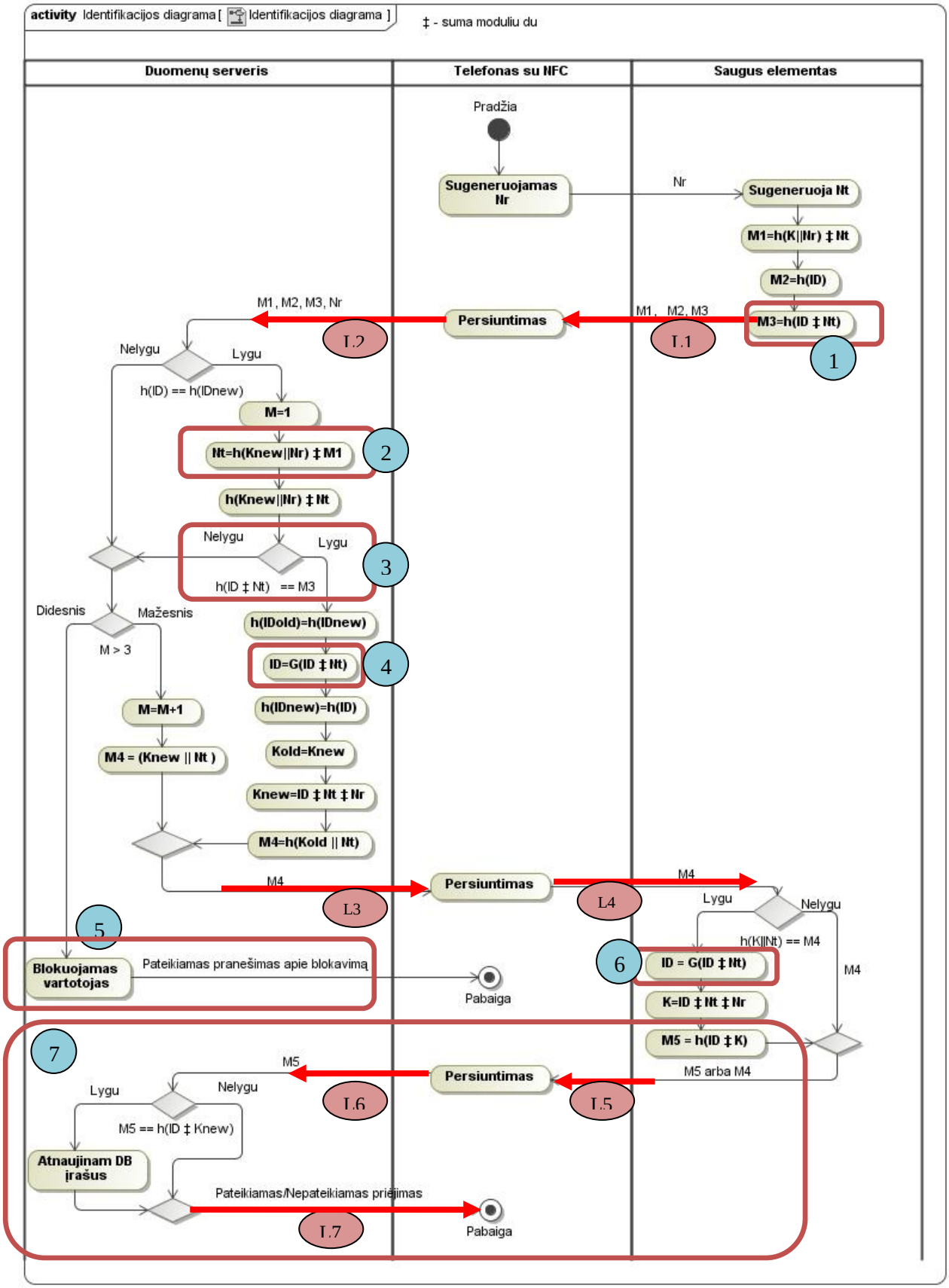
- atsitiktinio skaičiaus generavimui turi būti naudojami aparatiniai generatoriai ir atitikti mažiausiai FIPS 140 saugumo reikalavimus.
- naudojamos dvi skirtingos vienkryptės funkcijos
- svarbi metodo sparta, todėl reikia vengti ypatingai sudėtingų iteracijų ir skaičiavimų
- pašalinti Li-Wang algoritmo duomenų sinchronizacijos problemą tarp žymenos ir duomenų serverio
- reikalingi identifikacijai būtini duomenys turi būti saugomi saugumo elemente

3.3 Pritaikyto Li_Wang protokolo pakeitimai ALR identifikavimo algoritme apžvalga

Išanalizavus paprastą Li-Wang protokolą ir atsižvelgus į specialistų pastebėjimus kaip jį pagerinti buvo suprojektuotas identifikavimo protokolas (žiūrėti į 7 paveikslėlį).

Patobulintos 7 vietos identifikaciniame protokole (patobulintos vietos apibrauktos raudonai ir pažymėtos numerėliais mėlyname fone).

1. Nenorint atviru tekstu neperduoti Nt reikšmės (kaip kad buvo daroma pagrindinėje identifikavimo schemoje) ji buvo sudedama su ID reikšme suma moduliu du ir paveikta vienkrypte funkcija (h() funkcija) ir tik tada perduodama išsiuntimui.
2. Kadangi Nt reikšmė perduota užšifruota, ją reikalinga išsiskaičiuoti iš gautų pranešimų pasinaudojant duomenų bazėje saugoma K_{new} reikšme.
3. Pridėtas papildomas patikrinimas ar teisingai išskaičiuota Nt reikšmė ir tikrinama su gautąja M2 reikšme.
4. Papildomai pridėtas ID apskaičiavimo metodas, jog nauja ID reikšmė taptų daugiau priklausoma nuo keleto kintamųjų, nei, kad buvo senajame algoritme.
5. Apibrėžta ką daryti su tais vartotojais kurie bandė nesėkmingai identifikuotis daugiau kaip 3 kartus (blokuoti juos sistemoje).
6. Saugumo elemente taip pat ID apskaičiavimo metodas turi būti toks, koks yra apibrėžtas 4-oje pataisoje.
7. Šis punktas apibrėžia sėkmingą identifikaciją ir nurodo duomenų bazėje atnaujinti reikiamus įrašus, bei priklausomai nuo aplikacijos identifikuotam vartotojui leidžiama naudotis sistemoje apibrėžtais resursais.



Pav. 7 Siūlomos identifikacijos protokolo schema

3.4 Apsikeitimo pranešimai tarp sistemų ir sistemoje esančių komponentų

Kai yra užtikrinamas bendras prievadas tarp duomenų bazės serviso ir telefono galima atlikti ir identifikaciją, kuri susideda iš tokių žingsnių (žiūrėti į 7 paveikslėlį, raudonas rodykles su numeracija):

L1. Telefonas sugeneruoja atsitiktinį skaičių N_R ir siunčia į saugumo elementą.

L2. Saugumo elementas generuoja N_T ir apskaičiuoja $M_1=h(K||N_R)\oplus N_T$, $M_2=H(ID)$ ir $M_3=h(ID\oplus N_T)$ ir siunčia M_1, M_2, M_3 telefonui.

L3. Po to, kai telefonas priima M_1, M_2 ir M_3 iš saugumo elemento, telefonas persiunčia M_1, M_2, M_3 ir N_R duomenų bazės komunikavimo servisui.

L4. Duomenų bazės servisas patikrina ar h(ID) yra lygi $h(ID_{old})$ ar $h(ID_{new})$. Jei h(ID) lygi $h(ID_{new})$ tada yra nustatoma M=0, apskaičiuoja $N_T = h(K_{new}||N_R)\oplus M_1$, $h(K_{new}||N_R)\oplus N_T$ su apskaičiuotąja N_T, panaudojame N_T nustatyti ar $h(ID\oplus N_T)$ yra lygu gautajai M_3 reikšmei. Jei lygi, tada atliekame veiksmus sekančiai $h(ID_{old})=h(ID_{new})$, $ID=G(ID\oplus N_T)$, $h(ID_{new}) = h(ID)$, $K_{old}=K_{new}$, $K_{new}=ID\oplus N_T\oplus N_R$. Jei h(ID) nelygi $h(ID_{new})$ arba $h(ID\oplus N_T)$ yra nelygi gautajai M_3 reikšmei, tai padidiname M reikšmę M=M+1, ir siunčiame telefonui $h(K_{old}||N_T)$. Taip pat duomenų bazės servisas patikrina ar M reikšmė nėra didesnė už 3 (M *>3)*, taip padidiname saugumo lygį iki trejų neteisingų bandymų identifikuotis. Jei būtų bandoma identifikuotis 4 kartą, tai sistema turėtų blokuoti tokį vartotoją.

L5. Telefonas gavęs M4 pranešimą persiunčia jį saugumo elementui, kuris apskaičiuoja $h(K||N_T)$ ir palygina ją su gautąja reikšme iš telefono. Tada saugus elementas atnaujina $ID=G(ID\oplus N_T)$, $K = ID\oplus N_T\oplus N_R$, paskaičiuoja $M5=h(ID\oplus K)$ ir siunčia jį telefonui.

L6. Telefonas gavęs M5 persiunčia jį duomenų bazės servisui.

L7. Servisas gavęs M5 pranešimą paskaičiuoja $h(ID\oplus K)$ ir patikrina su gautąją reikšme. Jei paskaičiuotoji ir gautos reikšmės sutampa, tada duomenų bazės įrašai yra atnaujinami ir vartotojui yra pateikiamas priėjimas prie sistemos resursų. Priešingu atveju duomenų bazės įrašai nėra išsaugomi ir vartotojui yra pateikiama informaciją apie neteisingą prisijungimą.

3.5 Saugumo elemente saugomi duomenys

Saugumo elemente saugomos ID ir K reikšmės. Kiti kintamieji po identifikacijos, sėkmingos arba nesėkmingos, nėra niekur įrašomi ar naudojami. Saugumo elemente naudojamos dvi skirtingas vienkryptės funkcijos, kurių pagalba realizuojamas ir užtikrinamas identifikavimas. Keičiantis kortelės kriptografinių algoritmų palaikymui, galimas identifikacinio algoritmo modifikavimas, pakeičiant geresnėmis, greitesnėmis vienkryptėmis funkcijomis. Tai tektų pakeisti tiek serverio tiek mobiliojo įrenginio sistemose.

3.6 Duomenų serveryje saugomi duomenys

Duomenų serveryje tik saugomos ID_{old}, ID_{new}, K_{old} ir K_{new} reikšmės. Kiti kintamieji po identifikacijos nėra niekur įrašomi ar naudojami. Papildomos reikšmės (ID_{old} ir K_{old}) duomenų bazėje saugomos, todėl, kad esant nesėkmingai identifikacijai būtų galima prisijungti su senais duomenimis.

Paminėti duomenys duomenų bazėje gali būti papildomai apsaugomi specialiu kodu, kad priėjimas prie jų būti suteiktas tik pateikus teisingą apsaugos kodą. Papildoma duomenų apsauga specialiu saugos kodu priklauso nuo teikiamos paslaugos. Tačiau papildomai duomenis apsaugant specialiu kodu pailgėtų identifikacijos protokolo laikas, tačiau padidėtų duomenų saugumas.

3.7 Išvados

1. Šiame skyriuje apsibrėžtas darbo tikslas, iškelti uždaviniai, nustatyta sudaromo protokolo taikymo sritis ir jam keliami reikalavimai.
2. Sumodeliavome identifikavimo protokolą skirtą telefonui su ALR technologija ir pašalinome duomenų sinchronizacijos galimybę.
3. Protokole rekomenduojame naudoti dvi skirtingas vienkryptes funkcijas. Šiuo metu yra galimos trys vienkryptės funkcijos (SHA-1, SHA-256 ir MD5)[20], nes saugiojo elemento techninės specifikacijos apsprendė, jog tos funkcijos yra palaikomos saugumo elemente.
4. Peržiūrėjus saugiojo elemento specifikacijas [21] nustatyta, kad saugumo elementas aparatiškai generuoja atsitiktinius skaičius ir jis atitinka FIPS 140-2 saugumo keliamus reikalavimus.

4 ALR IDENTIFIKAVIMO PROTOKOLO EMULIATORIAUS MODELIS

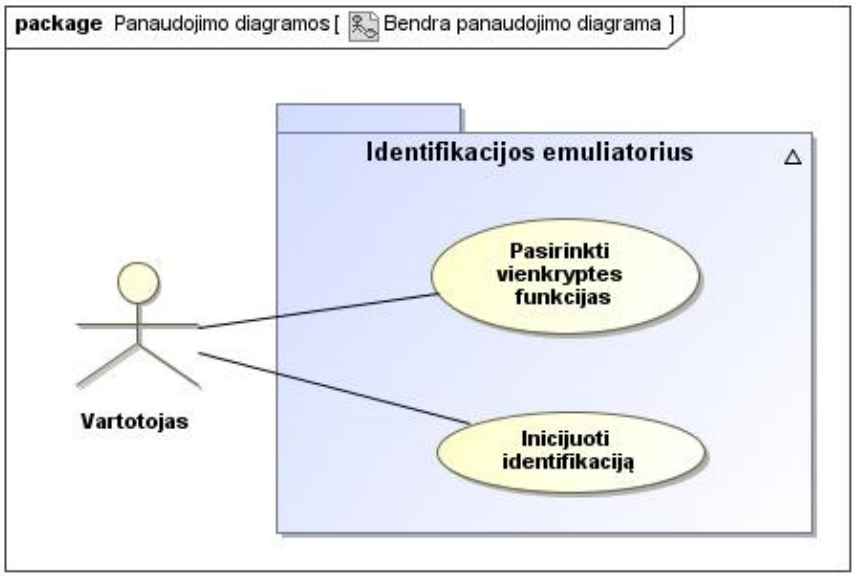
Šiame skyriuje aprašoma programinė ir techninė įranga kuri bus naudojama eksperimentui atlikti. Eksperimentas realizuojamas programine įranga, realus mobilusis įrenginys su artimojo lauko ryšio technologija ir realus artimojo lauko ryšio skaitytuvo terminalas nebus naudojami. Architektūros prasme eksperimentas yra kliento-serverio architektūros programinė įranga, kur klientas atitinka telefoną su artimojo lauko ryšio technologija su saugumo elementu, o serveris atitinka artimojo lauko ryšio skaitytuvo terminalą su pasiekiama duomenų baze.

4.1 Reikalingi įrankiai

Programinė įranga bus programuojama JAVA programavimo kalba, nes dabartiniai rinkoje atsirandantys telefonai su įterptiniais saugumo elementais ir artimojo lauko ryšio technologija, naudoja Android operacinę sistemą (privaloma didesnė nei 2.3 operacinės sistemos versija). Naudosime JAVA 1.6 JDK, Android SDK r17 programavimo paketo versijas. Naudojami programavimo įrankiai: Eclipse (Galileo versiją), Android virtual device programinis paketas.

4.2 Panaudos atvejai

Iš vartotojo pusės programa nėra labai interaktyvi. Kaip ir realiu atveju, vartotojas gali atlikti tik vieną veiksmą – inicijuoti identifikaciją, tai būtų tiesiog telefono priartinimas prie ALR skaitytuvo terminalo (tarp telefono ir ALR skaitytuvo terminalo turi būti ne daugiau kaip 10 cm atstumas, jog būtų vykdoma identifikacija). Tyrimo dėlei vartotojui bus papildomai leidžiama pasirinkti kokios vienkryptės funkcijos bus naudojamos identifikacijoje.



Pav. 8 Projekto panaudojimo atvejai

Taigi žiūrint iš vartotojo pusės programa turi būti labai paprasta. Programos sudėtingumas atsiskleidžia protokolo realizavime.

4.3 Reikalavimai projektui

Šiame skyriuje išdėstomi reikalavimai kuriamai programinei įrangai. Reikalavimus suskirstyme į tris grupes: funkcinius, nefunkcinius, techninius ir programų reikalavimus.

4.3.1 Nefunkciniai reikalavimai sistemai

Kadangi sistemos pagrindinis tikslas yra identifikuoti vartotoją panaudojant mobiliuosius telefonus su artimo lauko ryšio technologija, tai vartotojas ir turi turėti galimybę identifikuotis (prisijungti prie sistemos) tolimesnių vartotojo veiksmų sistemoje mes neapibrėšime.

- Programa turi turėti paprastą vartotojo sąsają
- Konfigūruojamų parametrų skaičius turi būti minimalus, kad kuo labiau supaprastinti programos naudojimąsi
- Programa turi tinkamai dirbti, kol vyksta identifikavimo procesas

4.3.2 Funkciniai reikalavimai sistemai

- Vartotojas prieš pradėdamas identifikavimo procesą turi turėti galimybę pasirinkti kokias vienkryptes funkcijas naudos identifikacijoje.
- Vartotojas turi turėti galimybę bet kada uždaryti programą net ir nesibaigus identifikavimo procesui.
- Po sėkmingo/nesėkmingo identifikavimo ekrane turi matytis tai pažymintis pranešimas.
- Programa turi realizuoti siūloma identifikavimo protokolą.
- Klientui pasirinkus vykdyti identifikavimą telefonu su ALR įranga ir saugumo elemento programa turi automatiškai prisijungti prie imituojantį ALR skaitymo terminalo ir įvykdyti identifikaciją be vartotojo įsikišimo.
- Turi būti skaičiuojamas laikas kiek trunka identifikacijos procesas ir rezultatas parodomas ekrane.
- Identifikacijos protokole turi būti naudojamos dvi skirtingos vienkryptės funkcijos
- Identifikacijos protokole turi būti generuojamas FIPS 140 saugumą atitinkantis atsitiktinių skaičių generatorius.

4.3.3 Techniniai reikalavimai sistemai

Norint analizuoti vartotojo identifikaciją užtenka dvejų, tačiau mes naudosime tris technines priemones, šiuo atveju tai būtų:

- Mobilusis telefonas
- Kompiuteris
- Duomenų bazė serveris

Mobilusis telefonas turi turėti įdiegta Android operacinę sistemą.

Duomenų bazės serveryje gali būti instaliuota bet kuri duomenų bazė, svarbiausia, jog būtų galima prie jos prisijungti naudojant JDBC tvarkykles. Taip pat ji gali būti fiziškai atskirame kompiuteryje (rekomenduotina). Šiame projekte mes naudosime MySql duomenų bazę ir reikiamas JDBC tvarkykles prie jos prisijungti.

Kompiuteris turi turėti tokius arba geresnius parametrus:

- 1 GHz Pentium arba greitesnis
- 512 MB RAM atmintis arba daugiau
- ~20 Gb talpos kietąjį diską ar daugiau (priklausomai nuo operacinės sistemos).

4.3.4 Privalomų programų reikalavimai sistemai

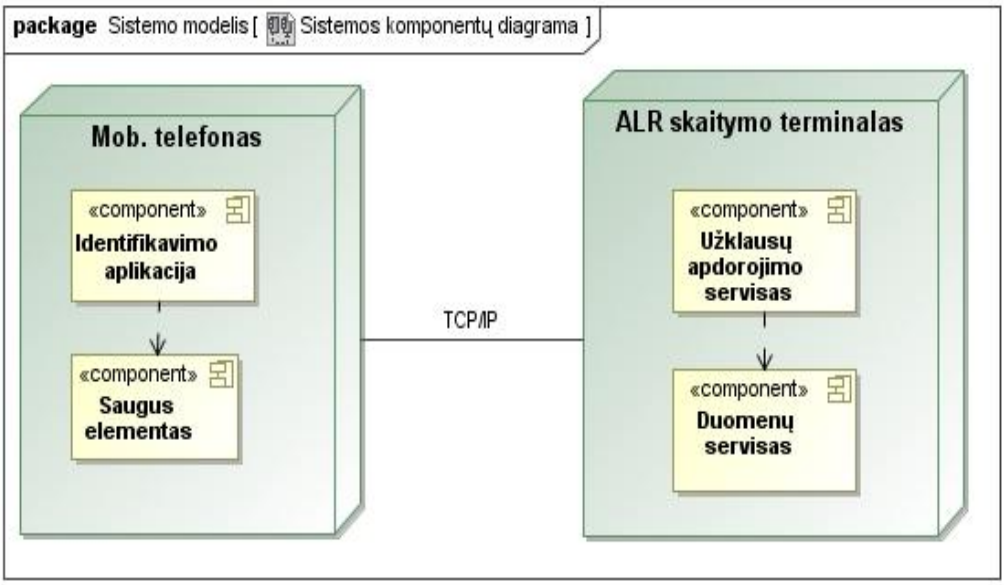
Mobiliajame telefone turi būti įdiegta bent Android 2.1 versijos operacinė sistema, gali būti ir geresnė versija.

Duomenų bazės serveryje turi būti įdiegta MySql duomenų bazė (versija neturi jokio funkcinio skirtumo) ir turėti galimybę ją pasiekti naudojantis IP/TCP protokolu.

Kompiuteryje turi būti įdiegta JAVA JDK 1.6 versija, bei atviras 8000 prievadas.

4.4 Identifikacinės sistemos architektūrinė schema

Kaip jau buvo minėta programa bus realizuojama kliento-serverio architektūros principu. Sistema susideda iš dviejų dalių: mobilaus telefono ir ARL skaitymo terminalo sistemų (žiūrėti 9 paveikslėlį). Klientas mūsų atveju atitiks mobilųjį telefoną su įterptiniu saugumo elementu, o serveris – ALR skaitymo terminalas. Kadangi klientas turi siųsti ir gauti pranešimus serveriui reikalinga komunikacijos terpė. Komunikacijos terpę panaudosime TCP/IP susijungimą (angl. socket).



Pav. 9 Identifikacinės sistemos architektūrinė schema

4.4.1 Mobiliojo telefono sistema

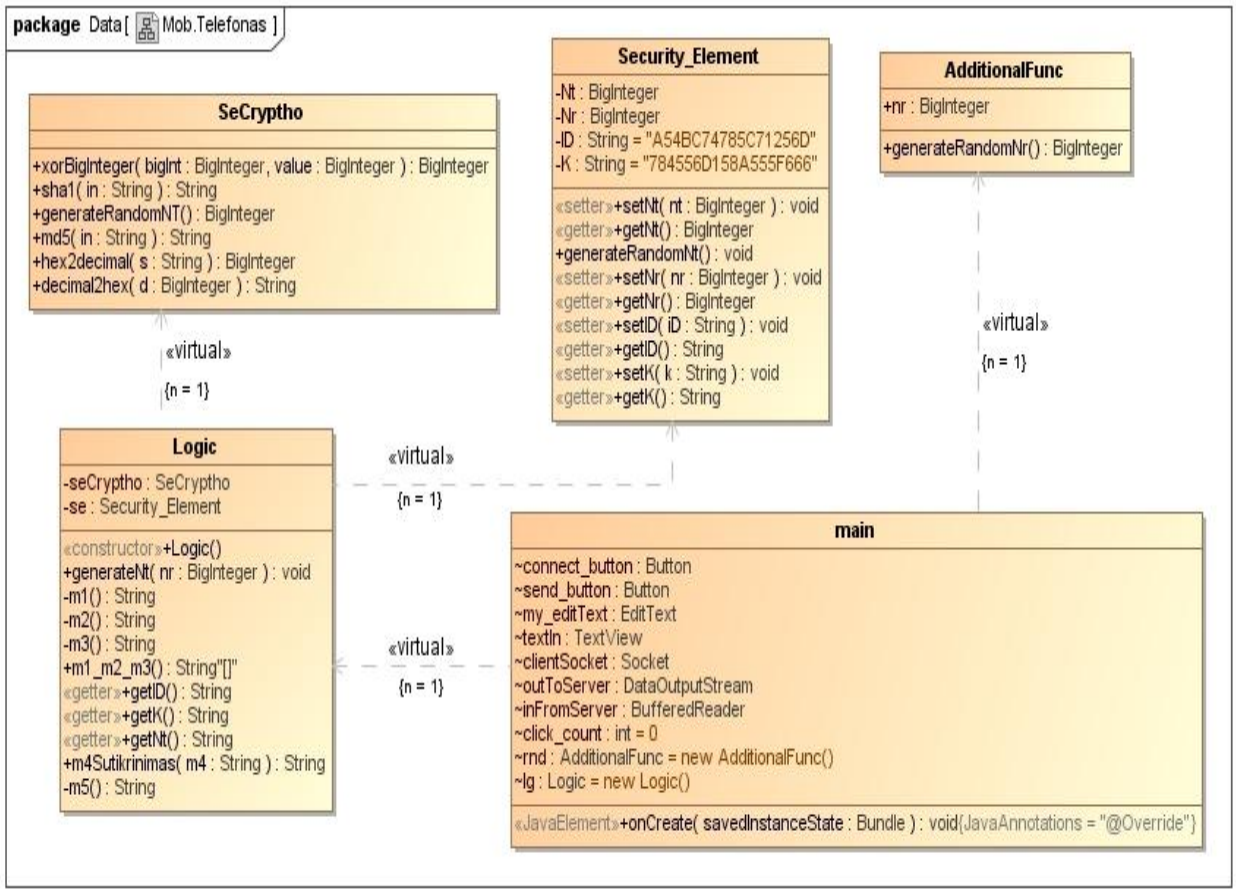
Telefone esanti identifikavimo aplikacija bendrauju su saugumo elementu, kuris savyje saugo identifikacijai reikalingus duomenis. Bendravimas tarp sistemų vyksta IP/TCP protokolu.

4.4.2 ALR skaitymo terminalo sistema

ALR terminalas susideda iš užklausų apdorojimo serviso ir duomenų serviso, kuris pateikia reikiamus duomenis užklausų servisui. Duomenų bazėje saugomos keturios slaptos reikšmės. Dvi unikalios K senoji ir K naujoji reikšmės, bei dvi unikalios ID reikšmės (senoji ir naujoji reikšmė).

4.5 Kliento klasių diagrama

Žemiau pateikta kliento dalies klasių diagramos ir trumpi svarbiausių klasių apibūdinimai.



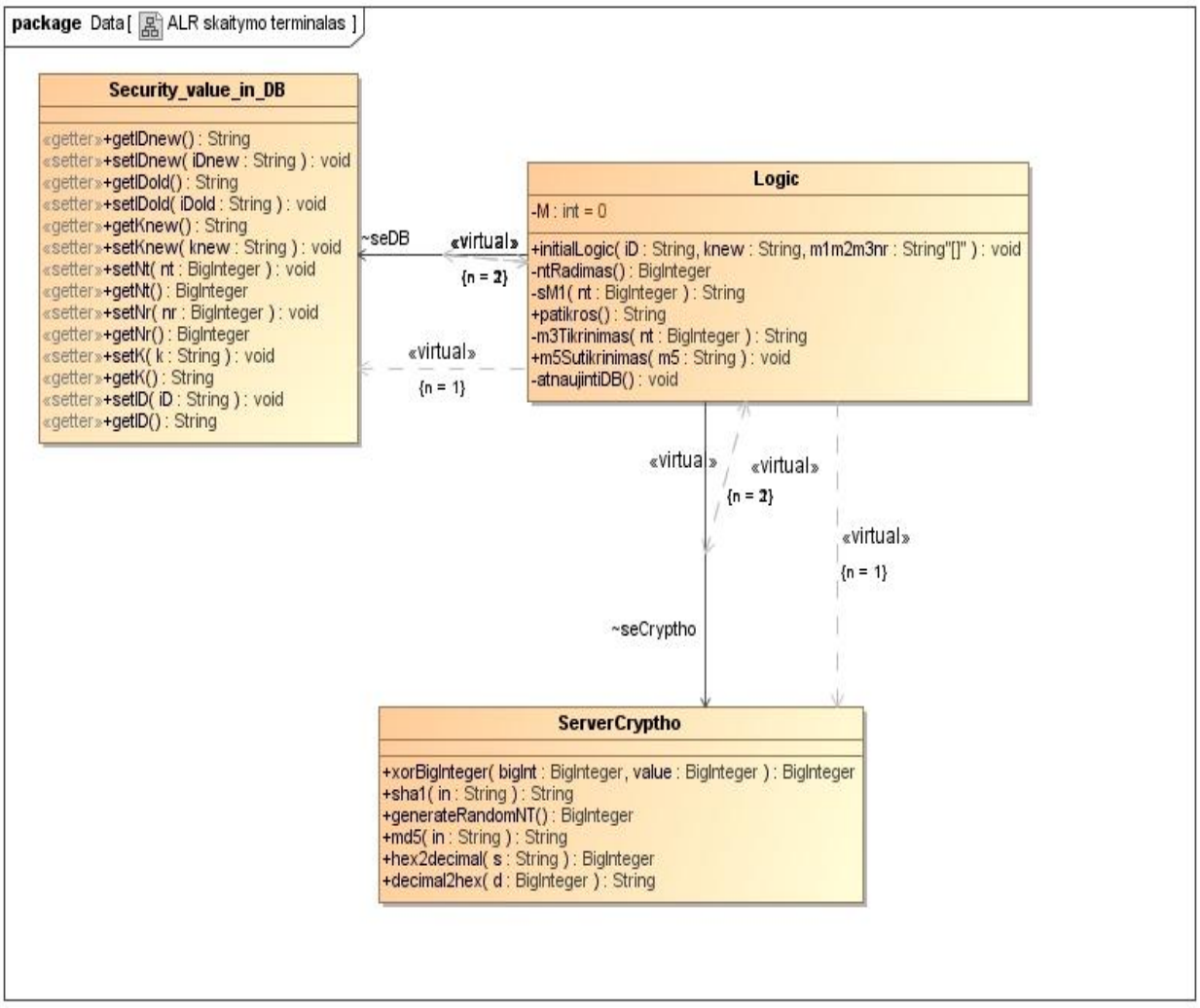
Pav. 10 Kliento dalies klasių diagrama

Svarbiausių kliento klasių trumpas apibūdinimas:

- Main – pagrindinė grafinės mobiliosios Android aplikacijos klasė.
- AdditionalFunkc – klasė, kuri atsakinga už atsitiktinio skaičiau generavimą.
- Logic – klasė, kurioje realizuota visa identifikacinio algoritmo loginė realizacija.
- SeCryptho – klasė, atsakinga už kriptografinines funkcijas.
- SecurityElement – klasė, skirta saugoti, gauti ID ir K reikšmes, bei papildomas reikšmes.

4.6 Serverio klasių diagrama

Žemiau pateikta serverio dalies klasių diagramos ir trumpi svarbiausių klasių apibūdinimai.



Pav. 11 Serverio dalies klasių diagrama

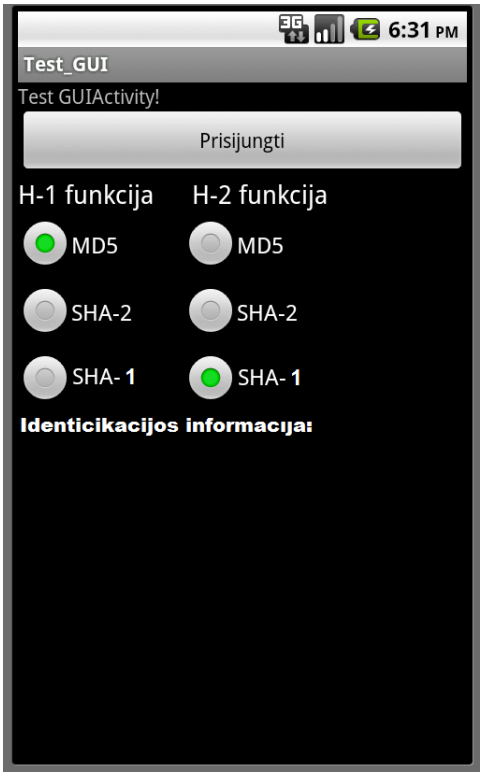
Svarbiausių serverio klasių trumpas apibūdinimas:

- Security_value_in_DB – klasė skirta saugoti duomenis duomenų bazėje
- Logic – klasė, kurioje realizuota visa identifikacinio algoritmo loginė realizacija.
- ServerCryptho — klasė, atsakinga už kriptografinines funkcijas.

4.7 Grafinė kliento sąsaja

Kliento programa buvo realizuojama kaip grafinė sąsaja. Toks sprendimas buvo pasirinktas, todėl, kad būtų galima paprastai ir patogiai atvaizduoti rezultatus ekrane (sėkminga/nesėkminga identifikacija, identifikacijos laikas). Taip pat panaudojant grafinę sąsają lengvai realizuotas protokole naudojamų vienkrypčių funkcijų pasirinkimas.

Žemiau pateikiama grafinė kliento sąsaja ir trumpi sąsajos apibūdinimai:



Pav. 12 Kliento grafinė sąsaja

Kliento vartotojo sąsaja sudaro keturi komponentai: identifikavimo inicijavimo mygtukas „Prisijungti“, protokole naudojamų dviejų funkcijų pasirinkimai ir vieta identifikacijos vykdymo informacijos išvedimo vieta. Teksto išvedimo vietoje parodomos slaptos reikšmės po sėkmingo/ nesėkmingo identifikavimo ir kiti tarpiniai kriptografiniai kintamieji būdingi pasirinktam protokolui bei testavimui.

4.8 Konsolinė serverio sąsaja

Konsolinė serverio sąsaja skirta atvaizduoti prisijungusius vartotojus prie serverio, tarpiniai kriptografiniai kintamieji bei reikalinga informacija testavimui.

4.9 Realizavimo detalės

Šiame skyriuje pateikiamos realizavimo detalės, kurios nebuvo paminėtos ankstesniuose skyriuose.

- Paleidus serverį jis pereina į klausimosi būseną ir klausosi 8000 TCP/IP prievado, tiesiog paleidžiame serverį. Jeigu paleidimo metu prievadas yra užimtas (tą prievadą naudoja kita ar kitos programos) bus parodomas klaidos pranešimas, jog serveris negali dirbti 8000 prievadu. Tuomet reikia uždaryti programą kuri užėmė prievadą ir serverį paleisti iš naujo.
- Kliento programoje paspaudus „Prisijungti“ mygtuką programa automatiškai jungiasi į vietinį kompiuterį, kurio IP yra 192.168.0.100 ir 8000 prievadą. Norint, jog sėkmingai įvyktu identifikavimas turi būti paleista serverio programa. Jeigu mygtuko paspaudimo metu nebus paleista serverio sistema, tai bus parodomas klaidos pranešimas, jog nepavyko prisijungti prie 192.168.0.100:8000 adreso.
- Serveris palaiko multiklientinį aptarnavimą, bei realizuotas taip, jog klientų užklausų būtų laukiama nuolatos.
- Kliento – serverio programose įrašytos vienodos pradinės reikšmės reikalingos identifikacijai. Išjungus klientą ar serverį reikėtų viską pradėti iš naujo, nes to paties serverio ar kliento naudojimas (pasikeitusios kintamųjų reikšmės) sukels sistemos neveikimą.

4.10 Išvados

1. ALR identifikacinio protokolo emuliatoriaus projektui buvo suformuluoti reikalavimai, ir suprojektuota programinė įranga atitinkanti keliamus reikalavimus.
2. Projektas realizuojamas kliento ir serverio architektūros programine įranga. Klientas atitinka telefoną su ALR įranga ir integruotu saugumo elementu, serveris – ALR skaitymo terminalą su pasiekiamu duomenų serveriu.
3. Pateikta klasių diagrama, grafinė vartotojo sąsaja su paaiškinimais.

5 ALR IDENTIFIKACIJOS PROTOKOLO TYRIMAS

Eksperimento metu bus atliekamas įrenginių turinčių ALR technologiją identifikacija serveryje su sukurta simuliacine programa virtualioje erdvėje.

Šio eksperimento esmė yra išanalizuoti siūlomo identifikacijos protokolo atsparumą prieš informacijos paskelbimą, ID reikšmių atskleidimą, pranešimo pakartojimą, DOS ataką, sekančio žingsnio apskaičiavimą. Paskaičiuoti identifikacijos laiką, saugomų ir perduodamų duomenų kiekius.

Eksperimentas bus vykdomas taip: paleidus serverį ir klientą bus bandoma identifikuoti klientą ir po to bus lyginamos slaptos reikšmės abejuose klientuose (kliento, serverio). Jeigu raktai visais atvejais gaunami vienodi reiškias protokolas ir jo realizacija yra teisingai veikianti. Reikiamas reikšmes tyrimui išvesime ekrane (mobiliojo įrenginio aplikacijoje), serverio dalyje reikiamas reikšmes išvesime konsolėje, visur pateiksime paveikslėlius kur bus matomi slapti raktai. Tuomet vizualiai sutikrinę reikšmes matysime ar reikšmės sutampa ar ne. Taip pat turi sutapti ID ir K reikšmės abejuose pusėse (kliento, serverio).

5.1 ALR identifikavimo protokolo teorinis saugumo tyrinėjimas atskiromis sritimis

Šioje dalyje mes paanalizuosime pasiūlyto protokolo saugumą pagal sritis.

5.1.1 Atsparumas informacijos paskelbimui

Siūlomame protokole atakuotojas gali sekti visas operacijas tarp žymenos ir skaitytuvo. Žinutės su perduodama informacija M1, M2, M3,M4 ir M5 gali būti perimtos, tačiau jos nieko naudingo atakuotojui nepateiks, nes jos yra apsaugotos vienkryptėmis funkcijomis. Jeigu atakuotojas pabandytu paprašyti pakartoti veiksmus, jis vis tiek negaus jokios naudingos informacijos iš to.

5.1.2 Atsparumas ID atskleidimui

Patobulintame protokole yra siunčiamas pranešimas M2=h(ID), kuriame yra sąlyginai užšifruota ID reikšmė. Atakuotojui perimant M2 žinutę ir ją mėginant iššifruoti, tai jam padaryti yra neįmanoma, nes pati ID reikšmė yra šifruojama vienkryptės funkcijos ir be viso to ID yra dinamiškai keičiamas po kiekvienos sėkmingos identifikacijos. Taigi norint surasti užšifruotą ID reikšmę tektų spręsti diskretinio logaritmo problemą.

5.1.3 Atsparumas pranešimo pakartojimui

Patobulintame protokole yra perduodami 5 pranešimai (M1, M2, M3, M4 ir M5). M1, M2 ir M4 pranešimuose yra naudojamas saugaus elemento sugeneruotas atsitiktinis skaičius.

Atakuotojui bandant priverstinai pakartoti tuos pačius pranešimus ir norint sužinoti atsitiktinai sugeneruotą skaičių yra neįmanoma, nes M1, M4 pranešimuose yra apsaugotas vienkryptės funkcijos, bei po sėkmingos identifikacijos visos reikšmės vėl keičiasi. M2 ir M5 pranešimuose šis skaičius net nefigūruoja. Be viso to, šis saugiame elemente sugeneruotas skaičius kas kartą yra pakeičiamas naujai sugeneruotu atsitiktiniu skaičiumi. Atsitiktinio skaičiaus generatorius atitinka FIPS 140-2 keliamiems reikalavimams.

5.1.4 Atsparumas DOS atakai

Atakuotojas gali mėginti pakeisti M5 žinutę, taip norėdamas sutrukdyti išsaugoti naujas reikšmes duomenų bazėje, nes naujos reikšmės jau yra išsaugotos saugiajame elemente. Nors jei atakuotojas ir pakeistų žinutę, tačiau bandantis vėl prisijungti prie sistemos būtų galima, nes sistemoje yra saugomi nauji ir seni duomenys reikalingi identifikacijai (K_{old} ir $h(ID)_{old}$). Taigi atakuotojas negali sunaikinti duomenų sinchronizacijos.

5.1.5 Atsparumas sekančio žingsnio apskaičiavimui

Norint apskaičiuoti sekančią žingsnio reikšmę atakuotojas turi žinoti saugaus elemento ID reikšmę. Bet kuriuo atveju tai yra sudėtinga, nors ir žinant esamų ID, M ir K reikšmes. Be to, ID reikšmė yra keičiama kiekvieną sesiją vis nauja, kuri paskaičiuojama naudojantis atskira vienkrypte funkcija $ID=G(ID \oplus N_T$.

5.2 ALR identifikavimo protokolo veikimo tyrimas

Patobulintas Li-Wang identifikavimo protokolas įgyvendintas emuliatoriuje ir atlikti vienkrypčių funkcijų kombinacijų duomenų perdavimo ir identifikacijos trukmės tyrimai.

5.2.1 Naudoti skaičiavimo resursai

Patobulintas Li-Wang kliento-serverio identifikavimo protokolas buvo testuojamas su mobiliuoju įrenginiu ir asmeniniu kompiuteriu.

Mobiliojo įrenginio charakteristikos:

- RAM 384MB
- CPU 600 MHz

Asmeninio kompiuterio charakteristikos:

- RAM 1,5 GB
- CPU 2,08 GHz

5.2.2 Perduodamų duomenų kiekis

Sukurtoje identifikacijoje duomenys yra perduodami tris kartus:

- Pirmajame duomenų perdavime galimi 6 skirtingi vienkrypčių funkcijų panaudojimai, o tai įtakoja perduodamą maksimalų duomenų kiekį kiekvienu atveju. Šiuo atveju duomenų siuntimą inicijuoja klientas (šiuo atveju telefonas).

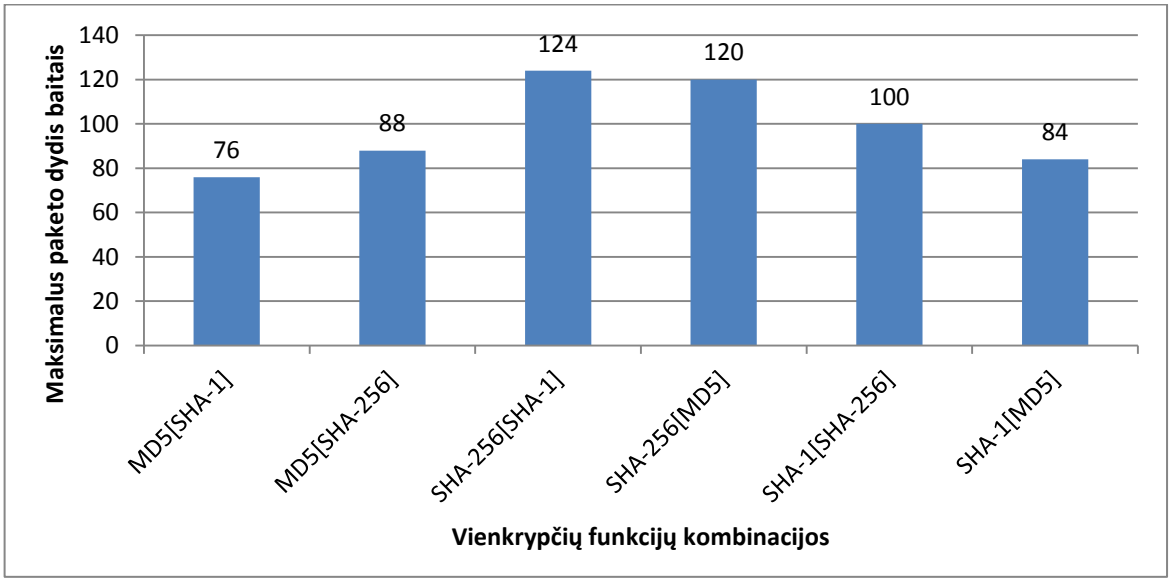


Diagrama Nr. 1 Pirmosios informacijos siuntimo duomenų kiekiai baitais priklausomai nuo naudojamų vienkrypčių funkcijų kombinacijų

- Antrajame ir trečiajame duomenų perdavime galimi 3 skirtingi vienkrypčių funkcijų panaudojimai, o tai įtakoja perduodamą duomenų kiekį kiekvienu atveju. Antrajame siuntime duomenų siuntimą inicijuoja serveris, o trečiajame – klientas (šiuo atveju telefonas).

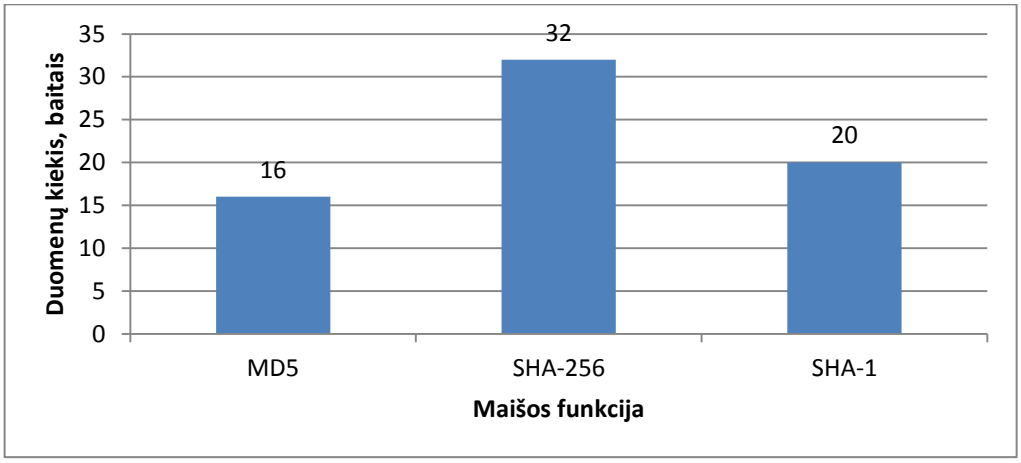


Diagrama Nr. 2 Antrosios informacijos siuntimo duomenų kiekiai baitais priklausomai nuo naudojamų vienkrypčių funkcijų

Bendras maksimalus duomenų perdavimo dydis identifikacijoje pagal vienkrypčių funkcijų kombinacijas yra skirtingas, nuo 108 iki 188 baitų dydžio. Šį dydį tiesiogiai įtakoja naudojamos vienkryptės funkcijos.

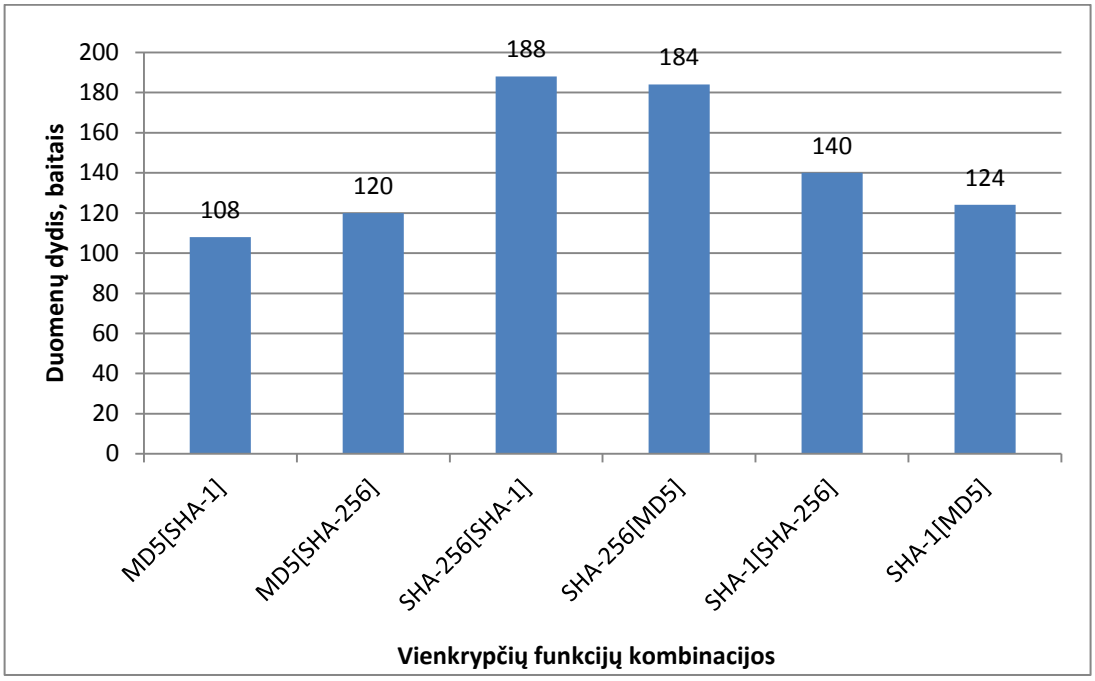


Diagrama Nr. 3 Maksimalus duomenų perdavimo dydis identifikacijoje baitais priklausomai nuo naudojamų vienkrypčių funkcijų

5.2.3 Identifikavimo trukmė

Naudojamame identifikavimo algoritme pasirinktinai galima panaudoti dvi skirtingas maišos funkcijas iš trejų palaikomų saugumo elemente (MD5, SHA-1 ir SHA-256). Taigi, buvo atliktas tyrimas, kiek laiko užtrunka kiekviena maišos funkcija paskaičiuoti santrauką. Bandymai buvo atliekami trejuose kategorijose (100, 1000 ir 10000 kartų). Kiekvienai kategorijai buvo atlikta po 10 bandymų ir paskaičiuotas vidurkis, bei paskaičiuotas visų kategorijų bendras vidurkis kiekvienai maišos funkcijai. Pateikta diagrama Nr. 4 vaizdžiai parodo kiekvienos funkcijos, vienos santraukos paskaičiavimo vidurkinį pasiskirstymą laike milisekundėmis.

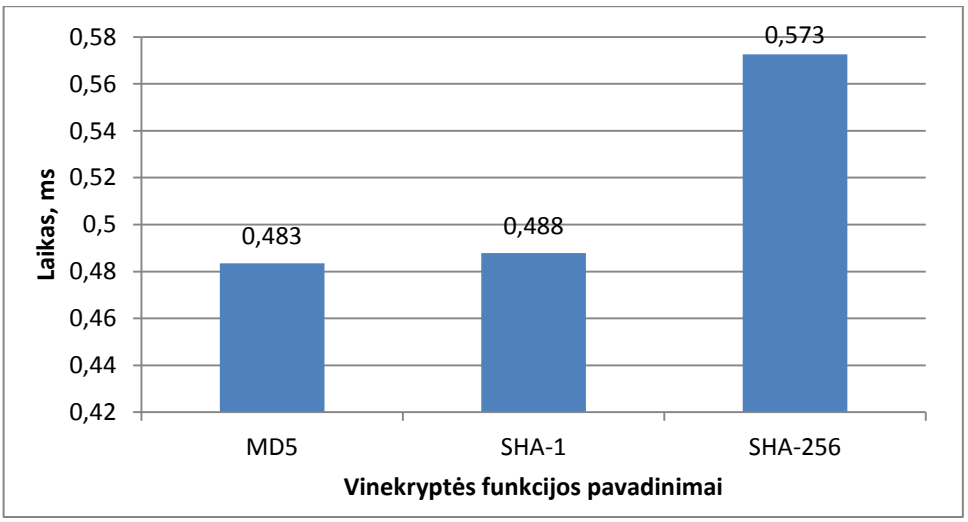


Diagrama Nr. 4 Santraukos paskaičiavimo vidurkinis pasiskirstymas laike priklausomai nuo vienkrypčių funkcijų

Pasinaudojant sukurtu emuliatoriumi buvo ištirti identifikavimo laikai priklausomai nuo naudojamų vienkrypčių funkcijų kombinacijų. Kiekviena kombinacija buvo bandoma 100 kartų ir vedamas jos vidurkis. Diagramoje Nr. 5 pavaizduoti gauti rezultatai įvertinus greičiausią, lėčiausią ir vidurkinę identifikacijos laikus.

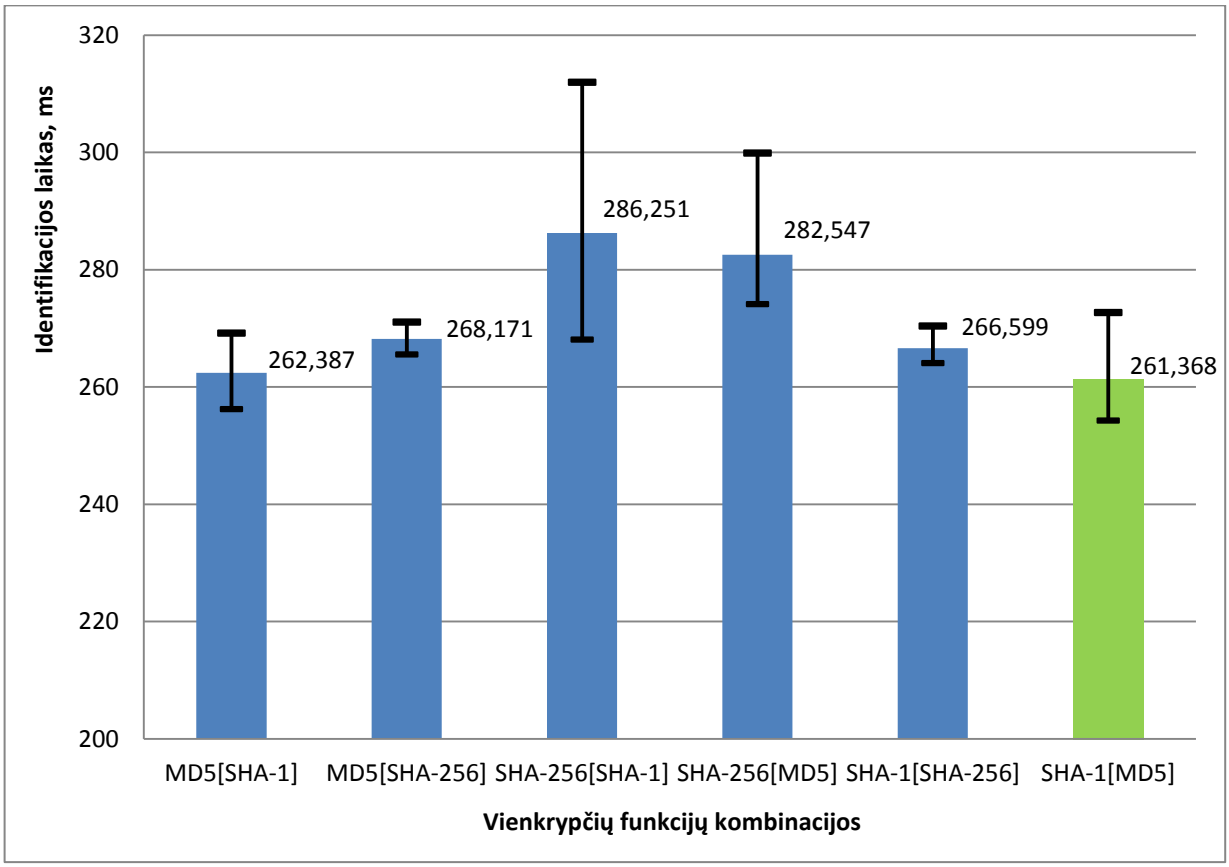


Diagrama Nr. 5 Identifikavimo laikai milisekundėmis priklausomai nuo naudojamų vienkrypčių funkcijų kombinacijų

5.3 Išvados

1. Suprojektuotas emuliatorius prieš pradedant identifikaciją leidžia pasirinkti vienkryptes funkcijas, bei gauti identifikacijos trukmės rezultatą.
2. Tyrime buvo atliktas identifikacinio protokolo loginis ir funkcinis tyrimas bei nustatyta, jog siūlomas algoritmas atitinka saugumo keliamus reikalavimus: yra atsparus informacijos paskelbimui, ID reikšmių atskleidimui, pranešimo pakartojimui, DOS atakai, sekančio žingsnio apskaičiavimui.
3. Nustatyta, kad saugumo elemente saugomos reikšmės gali užimti nuo 36 iki 52 baitų vietos, priklausomai nuo pasirinktos vienkrypčių funkcijų kombinacijos.
4. Nustatyta, kad greičiausia vienkryptė funkcija yra MD5 ir jos skaičiavimo laikas yra 0,483 ms vienai santraukai.
5. Tyrimai parodė, kad trumpiausias identifikavimo laikas: 261 ms, pasirinkus pirmajai funkcijai SHA-1 ir antrajai funkcijai MD5 vienkryptes funkcijas.

IŠVADOS

1. Nustatyta, kad Li-Wang identifikavimo protokolas tenkina pagrindinius saugumo reikalavimus: yra atsparus informacijos paskelbimui, ID reikšmių atskleidimui, pranešimo pakartojimui, sekančio žingsnio apskaičiavimui, tačiau nėra atsparus DOS atakoms.
2. Nustatyta, kad siūlomas identifikavimo protokolas yra saugesnis už Li-Wnag protokolą ir yra atsparus DOS atakoms, bei tenkina pagrindinius saugumo reikalavimus.
3. Nustatyta, kad siūlomas identifikavimo protokolas gali būti efektyviai realizuojamas ALR įrenginiuose. Skaičiavimams atlikti reikalingos dvi skirtingos vienkryptės funkcijos, kurias būtų galima naudoti tiek saugumo elemente, tiek serveryje.
4. Nustatyta, kad greičiausiai identifikacijai reikėtų saugumo elemente turėti mažiausiai 52 baitus laisvos vietos saugoti dinamines reikšmes, kurie leidžia atlikti identifikaciją tarp ALR įrenginių.
5. Tyrimai parodė, kad trumpiausias identifikavimo laikas yra 261 ms, pasirinkus pirmajai funkcijai SHA-1 ir antrajai funkcijai MD5 vienkryptes funkcijas.
6. Identifikacijos protokolo greitaveikos tyrimas parodė, kad vienkrypčių funkcijų kombinacijų pasirinkimas turi didžiulę įtaką greitaveikai. Kuo santraukos bitų skaičius didesnis naudojamoje vienkryptėje funkcijoje tuo identifikacija yra lėtesnė. Taigi renkantis kokios vienkryptės funkcijos turėtų būti naudojamos identifikavimui reikėtų pagalvoti ar tikrai reikia didelio saugumo, gal galima naudoti mažiau saugias vienkryptes funkcijas ir turėti greitesnį identifikavimo protokolą.

Technologija yra perspektyvi bei sparčiai plintanti visame pasaulyje ją pritaikant naujose srityse. Atliktas darbas leido geriau suprasti ALR technologiją ir ypač mobiliojo ALR telefono panaudojimo galimybes. Identifikacinis algoritmas gali būti panaudotas tolimesniems mobiliųjų telefonų su ALR technologija tyrimams ar įgyvendinimui realiuose projektuose.

LITERATŪROS SĄRAŠAS

[1] Van Damme G. and Wouters K. Practical Experiences with NFC Security on mobile Phones. Workshop on RFID Security, 2009.

[2] Madlmayr G. and Langer J. NFC Devices: Security and Privacy. The Third International Conference on Availability, Reliability and Security, 2008.

[3] Bishwajit C. and Juha R., Mobile Device Security Element. Mobey Rorum, 2005

[4] Mulliner C. Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones. 2009 International Conference on Availability, Reliability and Security.

[5] Welte H. "OpenPCD" [Interaktyvus], [žiūrėta 2010-12]. Prieiga per internetą: <www.openpcd.org>

[6] Dinne H. & Mandava K. Knyga: Two Way Mobile Authentication System. 2010

[7] Technical Specification. Iš NFC Forum. NFC Data Exchange Format (NDEF)[Interaktyvus], [žiūrėta 2010-12]. Prieiga per internetą: <http://www.nfc-forum.org>

[8] Techninė specifikacija. Iš NFC Forum. URI Record Type Definition[Interaktyvus], [žiūrėta 2012-12] Prieiga per internetą: <http://www.nfc-forum.org>

[9] Technical Specification. Iš NFC Forum. Text Record TypeDefinition [Interaktyvus], [žiūrėta]. Prieiga per internetą: <http://www.nfc-forum.org>

[10] Technical Specification. Iš NFC Forum. Smart Poster Record Type Definition [Interaktyvus], [žiūrėta 2010-11] Prieiga per internetą: <http://www.nfc-forum.org>

[11] *Diego Alejandro Ortiz-Yepes. Knyga:* Enhancing authentication in eBanking with NFC enabled mobile phones. 2008

[12] He S. SIM Card Security. Chair for Communication Security. 2007

[13] NXP Semiconductors N.V. (NASDAQ:NXPI) [Interaktyvus], [žiūrėta 2011-06] Prieiga per internetą: <http://www.nearfieldcommunicationsworld.com/nfc-phones-list/>

[14] Jie Li, Yunfeng Wang, Baoying Jiao, and Yong Xu, An authentication protocol for secure and efficient RFID communication" iš *International Conference on Logistics Systems and Intelligent Management*, pp. 1648 - 1651, Harbin, Jan. 9-10, 2010.

[15] Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels, Security and privacy aspects of low-cost radio frequency identification systems," in *Proceedings of International Conference on Security in Pervasive Computing*, p. 201 - 212, 2003.

[16] M. Ohkubo, K. Suzuki, and S. Kinoshita, Efficient hash-chain based RFID privacy protection scheme," *Ubcomp 2004 workshop*.

[17] Yalin Chen, Jue-Sam Chou, and Hung-Min Sun, A novel mutual authentication scheme based on quadratic residues for RFID systems," *Computer Networks*, vol. 52, no. 12, p. 2373-2380, 2008.

[18] Jie Li, Yunfeng Wang, Baoying Jiao, and Yong Xu, "An authentication protocol for secure and eeffcient RFID communication," *International Conference on Logistics Systems and Intelligent Management*, p. 1648 - 1651, Harbin, Jan. 9-10, 2010.

[19] Chia-Hui, Wei Min-Shiang ,Hwang Augustin, Yeh-hao Chin "An Improved Li-Wang authentication protocol for secure and efficient in RFID communication", Department of Management Information Systems National Chung Hsing University. 2010.12

[20] NXP Semiconductors: JCOP 2.4.1 specification [Interaktyvus], [žiūrėta 2011-09]. Prieiga per internetą: < http://www.usmartcards.com/media/downloads/492/NXP%20P5CX012%2002X%2040%2073%2080%20144%20%20%202011.pdf>

[21] NXP Semiconductors: P5CN072 Secure Dual Interface PKI Smart Card Controler [Interaktyvus], [žiūrėta 2011-08]. Prieiga per internetą: <http://www.pansuninfo.com/UploadFiles/P5CN072.pdf>

[22] BlueZ Secure Systems: JCOP – The IBM GlobalPlatform JavaCardTM implementation, [Interaktyvus], [žiūrėta 2011-09]. Prieiga per internetą: <ftp://ftp.software.ibm.com/software/pervasive/info/JCOP_Family.pdf>

TERMINŲ IR SANTRUMPŲ ŽODYNAS

Identifikacija - tai asmens tapatybės nustatymas ir pripažinimas, sutapatinimas.

ALR - Artimo Lauko Ryšys.

AID - Aplikacijos identifikavimo numeris (angl. *Aplication Identification*)

APDU - ryšio protokolas, perduodantis duomenis tarp skaitytuvo ir kortelės (angl. *Application Protocol Data Unit*)

Bluetooth - belaidžio ryšio gamybinė specifikacija leidžianti keistis informacija.

DoS - atsisakymas aptarnauti ataka (angl. Denial of Service).

GPRS - mobiliojo ryšio technologija, skirta duomenų perdavimui (angl. *General Packet Radio Service*)

ISO - tarptautinė standartizacijos organizacija (angl. *International Organization for Standardization*)

JAVA - programavimo kalba

kbps - kilobitai per sekundę

NFC - trumpo nuotolio beviele technologija (ALR), (angl. *Near Field Communication*)

OTA - oru (angl. *Over The Air*)

PIN - asmeninis identifikavimo numeris (angl. *Personal identification number*)

P2P - prietaisų susijungimo tinklas (angl. *Peer-to-Peer*)

RFID – radijo dažnių identifikavimas (angl. *Radio-frequency identification*)

UID – unikalus kortelės identifikacijos numeris (angl. *Unique Identificarion*)

Wi-Fi – bevielio ryšio technologija

JDBC – tvarkyklė, kurios pagalba galima prisijungti prie duomenų bazės serverio

FIPS – Federalinis Informacijos Apdorojimo Standartas (angl. *Federal Information Processing Standards*)

PRIEDAS

Priedas Nr. 1 Li-Wang identifikavimo algoritme naudojami žymėjimai

Lentelė Nr. 2 Li-Wang identifikavimo algoritme naudojami žymėjimai

$\oplus$ arba ‡	Suma moduliu 2
||	Kankatinacijos operacija
h()	Vienkryptė funkcija
G()	Vienkryptė funkcija
K	Slapta reikšmė padalinta tarp serverio ir žymenos
ID	Unikalus žymenos identifikatorius
M	Kiek kartų žymena neatnaujino ID ir K reikšmių
ID_{old} arba IDold	Ankstesnė unikali žymenos identifikatorius
ID_{new} arba IDnew	Naujas unikalus žymenos identifikatorius
K_{old} arba Kold	Ankstesnė slapta reikšmė
K_{new} arba Knew	Nauja slapta reikšmė
N_T arba Nt	Žymenos sugeneruotas atsitiktinis skaičiaus
N_R arba Nr	Skaitytuvo sugeneruotas atsitiktinis skaičius