Univerza v Mariboru

Fakulteta za elektrotehniko,
računalništvo in informatiko
Smetanova ulica 17
2000 Maribor, Slovenija

FERI

Matija Heričko

Klasifikacija varnostnih zahtev za overitvene protokole - sistematičen pregled literature

Magistrsko delo

Maribor, september 2015

Klasifikacija varnostnih zahtev za overitvene protokole - sistematičen pregled literature

Magistrsko delo

Študent:	Matija Heričko
Študijski program:	2. bolonjska stopnja – magistrski program
	Informatika in tehnologije komuniciranja
Mentor:	doc. dr. MARKO HÖLBL, univ. dipl. inž. rač. in inf.
Lektor:	Matic Pavlič, univ. dipl. komp. in spl. jez.

Univerza v Mariboru

Fakulteta za elektrotehniko,
računalništvo in informatiko
Smetanova ulica 17
2000 Maribor, Slovenija

Številka: E5016710
Datum in kraj: 29. 06. 2015, Maribor

Na osnovi 330. člena Statuta Univerze v Mariboru (Ur. l. RS, št. 46/2012)
izdajam

SKLEP O MAGISTRSKEM DELU

1. **Matiji Heričku,** študentu študijskega programa 2. stopnje INFORMATIKA IN TEHNOLOGIJE KOMUNICIRANJA, se dovoljuje izdelati magistrsko delo.

2. Tema magistrskega dela je pretežno s področja Inštituta za informatiko.

MENTOR: doc. dr. Marko Hölbl

3. Naslov magistrskega dela:
KLASIFIKACIJA VARNOSTNIH ZAHTEV ZA OVERITVENE PROTOKOLE - SISTEMATIČEN PREGLED LITERATURE

4. Naslov magistrskega dela v angleškem jeziku:
CLASSIFICATION OF SECURITY REQUIREMENTS FOR AUTHENTICATION PROTOCOLS - A SYSTEMATIC LITERATURE REVIEW

5. Magistrsko delo je potrebno izdelati skladno z »Navodili za izdelavo magistrskega dela« in ga do 29. 06. 2016 v 2 vezanih in 1 v spiralo vezanem izvodu oddati v pristojni referat za študentske zadeve.

V skladu z Navodili o pripravi in oddaji e-diplom je potrebno magistrsko delo oddati v Digitalno knjižnico Univerze v Mariboru.

Pravni pouk: Zoper ta sklep je možna pritožba na senat članice v roku 15 dni.

Obvestiti:
1. kandidata
2. mentorja
3. odložiti v arhiv

Dekan:
red. prof. dr. Borut Žalik

Klasifikacija varnostnih zahtev za overitvene protokole - sistematičen pregled literature

Ključne besede: overitveni protokoli, znani napadi, varnostne zahteve, klasifikacija

UDK: 004.77.056(043.2)

Povzetek

Overitveni protokoli so pomemben del storitev, ki zagotavljajo varnost komunikacij, saj nam potrjujejo, da je oseba, s katero se pogovarjamo, dejansko ta, za katero se izdaja. V magistrskem delu se je izvedel sistematičen pregled literature z namenom pridobitve pregleda nad overitvenimi protokoli, njihovimi napadi in varnostnimi zahtevami. Ugotovljenih je bilo 297 različnih protokolov, 27 različnih napadov in 20 različnih varnostnih zahtev. Na podlagi pridobljenega znanja so bila pripravljena tudi različna priporočila za snovalce novih overitvenih protokolov.

Classification of security requirements for authentication protocols - a systematic literature review

Key words: authentication protocols, known attacks, security requirements, classification

UDK: 004.77.056(043.2)

Abstract

Authentication protocols are an important part of the services that provide us with communication security, because they allow us to be sure that the person we are communicating with really is the person it claims to be. In this master thesis a systematic literature review was carried out with the intention of getting an overview of authentication protocols, their safety requirements and weaknesses. 297 different protocols were found, as well as 27 different attacks and 20 different security requirements. With this overview knowledge some recommendations for creators of new authentication protocols were also prepared.

KAZALO

1 UVOD ..... - 1 -

1.1 Identifikacija in opredelitev problema ..... - 1 -

1.2 Namen ..... - 2 -

1.3 Raziskovalna vprašanja ..... - 2 -

1.4 Raziskovalne hipoteze ..... - 2 -

2 OVERITEV IN OVERITVENE METODE ..... - 4 -

2.1 Informacijska varnost ..... - 4 -

2.2 Identifikacija in overitev ..... - 5 -

2.3 Overitvene metode ..... - 6 -

2.4 Overitveni protokoli ..... - 12 -

3 NAPADI IN VARNOSTNE ZAHTEVE ..... - 13 -

3.1 Napadi na overitvene protokole ..... - 13 -

3.2 Varnostne zahteve ..... - 20 -

4 PREGLED METODE - SISTEMATIČNI PREGLED LITERATURE ..... - 23 -

4.1 Potek sistematičnega pregleda literature ..... - 24 -

5 SISTEMATIČNI PREGLED LITERATURE OVERITVENIH PROTOKOLOV ..... - 32 -

5.1 Faza načrtovanja ..... - 32 -

5.2 Faza izvedbe ..... - 37 -

5.3 Odgovori na raziskovalna vprašanja ..... - 45 -

5.4 Omejitve ..... - 51 -

6 SKLEP ..... - 52 -

6.1 Preverjanje hipotez ..... - 52 -

6.2 Zaključek ..... - 53 -

VIRI IN LITERATURA ..... - 54 -

PRILOGE ..... - 59 -

Priloga A: Pomožna tabela protokolov, napadov in zahtev ..... - 59 -

Priloga B: Klasifikacija napadov in varnostnih zahtev ..... - 69 -

Priloga C: Viri SLR ..... - 85 -

KAZALO SLIK

Slika 5.1 Deleži ocen vseh raziskav ..... - 38 -
Slika 5.2 Deleži skupin overitvenih protokolov ..... - 40 -
Slika 5.3 Deleži protokolov glede na število faktorjev ..... - 41 -
Slika 5.4 Področja uporabe overitvenih protokolov ..... - 42 -

KAZALO TABEL

Tabela 5.1 PICOC kriterij ..... - 33 -
Tabela 5.2 Obrazec za izpis podatkov ..... - 36 -
Tabela 5.3 Rezultati iskanja ..... - 37 -
Tabela 5.4 Število primernih primarnih raziskav ..... - 38 -
Tabela 5.5 Primer pridobivanja podatkov ..... - 39 -
Tabela 5.6 Izsek iz pomožne tabele ..... - 39 -
Tabela 5.7 Seznam zahtev in njihovih pojavitev ..... - 42 -
Tabela 5.8 Seznam napadov in njihovih pojavitev ..... - 43 -
Tabela 5.9 Analiza varnosti protokolov glede na faktorje ..... - 45 -
Tabela 5.10 Analiza varnosti skupin overitvenih protokolov ..... - 46 -
Tabela 5.11 Število pojavitev kriterijev ..... - 47 -
Tabela 5.12 Splošna priporočila za preverjanje varnosti ..... - 48 -
Tabela 5.13 Seznam pojavov kriterijev pri protokolih z enim faktorjem ..... - 49 -
Tabela 5.14 Priporočila za preverjanje varnosti za protokole z enim faktorjem overjanja ..... - 50 -
Tabela 5.15 Seznam pojavov kriterijev pri protokolih z dvema faktorjema overjanja ..... - 50 -
Tabela 5.16 Priporočila za preverjanje varnosti za protokole z dvema faktorjema overjanja ..... - 51 -

1 UVOD

S hitrim razvojem brezžičnih komunikacijskih omrežij in aplikacij elektronskega trgovanja, kot sta elektronsko bančništvo in spletna trgovina, se veča tudi potreba po zagotavljanju varnosti in anonimnosti uporabnikov, saj se te storitve in viri distribuirajo po odprtih omrežjih, ki jih upravljajo razni ponudniki storitev. Takšne storitve omogočajo lažja vsakdanja opravila in večjo prenosljivost, saj so dostopne z različnih prenosnih naprav, kot so prenosniki, pametni telefoni in tablice, kar pa predstavlja tudi večje tveganje varnosti. V komunikacijskem sistemu strežnikov in odjemalcev so overitveni protokoli zaupanja vredna komponenta, ki z različnimi storitvami (kot so uporabniška zasebnost, overitev in druge) varuje občutljive podatke pred zlonamernimi osebami (Debiao, Jianhua, & Jin, 2012; Odelu, Das, & Goswami, 2015).

Overitev je ključen element tipičnega varnostnega modela. Je proces potrjevanja identitete uporabnika (bodisi osebe ali pa druge naprave), ki poskuša dostopati do določenega vira ali storitve. Obstaja veliko število različnih mehanizmov in protokolov, vendar je končen namen vseh enak. Želimo preveriti, ali je uporabnik, ki poskuša dostopati do virov, res tisti, za katerega se izdaja (Shinder, 2001).

Zgodnje overitvene sheme so temeljile zgolj na geslih. Z raziskavami so sčasoma ugotovili, da zgolj geslo ni dovolj varno v smislu izpolnjevanja varnostnih zahtev različnih aplikacij, ki so v korporacijskem in bančnem sektorju delovale na področju upravljanja baz podatkov. Temu je sledil razvoj (i) overitvenih shem s pomočjo pametnih kartic, kjer mora uporabnik ob geslu posedovati tudi pametno kartico, da se lahko overi v digitalnem svetu in (ii) shem, ki temeljijo na osnovi fizičnih lastnosti uporabnika – biometriji (Kumari, Khan, & Li, 2014).

1.1 Identifikacija in opredelitev problema

Izbira ustreznega overitvenega mehanizma je torej bistvenega pomena za zagotavljanje varnosti podatkov v določenem sistemu. Vendar ima vsak overitveni mehanizem svoje prednosti in slabosti. Teh se je potrebno zavedati in informacije o njih uporabiti pri izbiri in načrtovanju overitvenega protokola.

V magistrskem delu bomo s pomočjo sistematičnega pregleda literature izvedli analizo varnostnih zahtev in znanih napadov za overitvene protokole. Prav tako bomo pregledali

tudi ostale formalne in neformalne varnostne zahteve in iz pridobljenih podatkov pripravili klasifikacijo overitvenih protokolov.

Klasifikacija bo vsebovala podatke o varnostnih zahtevah in ranljivostih posameznih protokolov, tako, da bo lahko načrtovalec novega protokola uporabil klasifikacijo tudi pri ustvarjanju nekega inovativnega protokola, in sicer kot pomoč in nasvet, na kaj mora biti pozoren in pred katerimi napadi mora zaščititi svoj protokol.

1.2 Namen

Glavni namen raziskovalnega dela je pridobiti znanje in izvesti pregled o overitvenih protokolih, njihovih varnostnih zahtevah in znanih napadih. Ker je področje zelo obširno, bomo zajeli veliko literature, zato pričakujemo številne različne protokole in veliko različnih zahtev in napadov, ki jih bomo klasificirali. Na tej osnovi bomo oblikovali nekaj osnovnih priporočil za razvijalce novih overitvenih protokolov.

1.3 Raziskovalna vprašanja

Na osnovi identificiranega problema, namena raziskovalnega dela in pregledane literature smo oblikovali naslednja raziskovalna vprašanja:

- RV1: Kako število faktorjev overitvenih protokolov vpliva na njihove varnostne zahteve in ranljivosti?
- RV2: Kateri razredi oziroma skupine overitvenih protokolov obstajajo?
- RV3: Katera izmed skupin overitvenih protokolov v povprečju izkazuje manj varnostnih pomanjkljivosti in je posledično podvržena manj napadom?
- RV4: Ali obstaja klasifikacija napadov na overitvene protokole?
- RV5: Katere kriterije je treba upoštevati pri snovanju overitvenega protokola?

1.4 Raziskovalne hipoteze

Za potrebe magistrskega dela smo si pripravili tudi raziskovalne hipoteze, ki jih bomo sprejeli ali ovrgli, in s pomočjo katerih bomo usmerjali raziskovanje. Hipoteze se nanašajo na overitvene protokole, njihove ranljivosti in varnostne zahteve ter se večinoma skladajo z raziskovalnimi vprašanji. Hipoteze so sledeče:

H1: Overitveni protokoli z več faktorji overjanja imajo manj ranljivosti kot protokoli z enim faktorjem overjanja.

H2: Obstajajo tri skupine protokolov: ”overitev”, ”overitev in dogovor o ključu” ter ”dogovor o overjenem ključu”.

H3: Najbolj razširjena skupina je skupina ”overitev”.

H4: Najmanj ranljivosti ima skupina ”dogovor o overjenem ključu”.

H5: Klasifikacija napadov na overitvene protokole ne obstaja.

2 OVERITEV IN OVERITVENE METODE

2.1 Informacijska varnost

Informacije so v današnjem svetu pomemben del organizacij in posameznikov, pogosto imajo tudi denarno vrednost. Razkritje, poseganje v informacije ali njihova nerazpoložljivost organizaciji ali posamezniku lahko povzroči denarne stroške ali izgubo profita.

Zato je pomembno, da se informacije primerno zaščitijo pred grožnjami, ta naloga pa pripada IT varnosti. Organizacije in posamezniki imajo po navadi tri glavne zahteve za varovanje informacij. Te zahteve so:

- *Zaupnost*: lastnost, ki pomeni, da se vsebina informacije ne razkrije nepooblaščenemu uporabniku. Primeri informacij, ki potrebujejo zaščito pred razkritjem, so patenti, poslovne skrivnosti, vojaške informacije ipd.
- *Integriteta:* lastnost, ki zaščiti informacije pred namernim ali nenamernim spreminjanjem, ki bi lahko vplivalo na veljavnost podatkov. Primer informacij, ki potrebujejo integriteto, so finančne transakcije.
- *Razpoložljivost*: lastnost, ki pomeni, da so informacije in storitve za prikazovanje informacij uporabnikom na voljo, ko jih uporabniki potrebujejo.

Idealno bi za varnost informacij lahko uporabljali najboljšo tehnologijo, ki je na voljo, vendar običajno zaradi denarnih in drugih omejitev to žal ni mogoče. Ker vse informacije niso enako pomembne, zaupne oziroma vredne, pred izbiro primernega varovanja analiziramo zahteve za varnost in same informacije, ki jih varujemo. Na podlagi tega nato določimo ciljne vrednosti varovanja. Nazadnje na podlagi teh ciljnih vrednosti izberemo stroškovno najbolj učinkovit varnostni sistem, ki bo ob čim nižji ceni izpolnil ciljno vrednost varnosti.

Vendar pa se ne glede na nivo zaščite pojavljajo varnostne grožnje, večinoma zaradi nejasnih zahtev in varnostnih hib programske in strojne opreme. In ker varnostne ranljivosti obstajajo, obstaja tudi verjetnost, da zlonamerna oseba te ranljivosti izrabi in ogrozi varnostno zaščito informacij.

Tipičen pristop k upravljanju varnostne zaščite informacij je takšen, da se analizirajo tveganja ter grožnje informacijam in se ugotovljene grožnje ublažijo z različnimi

protiukrepi. Da se informacije ustrezno zaščitijo, morajo profesionalci za varnost vpeljati tudi varnostne sisteme, ki izvajajo različne varnostne kontrole.
Pri varnostnih kontrolah igrata identifikacija uporabnikov in overitev bistveni vlogi, saj potrdita identiteto uporabnika, preden mu podelita dostop do informacij.

Varnostni sistemi imajo tri glavne med seboj sodelujoče varnostne procese, ki zagotavljajo kontroliran dostop do virov. Ti procesi so:

- *Overitev* (angl. *authentication*): ugotavljanje in potrjevanje uporabnikove identitete.
- *Avtorizacija* (angl. *authorization*): dodeljevanje dostopa do virov, do katerih uporabniki lahko dostopajo – in preprečevanje dostopa do virov, do katerih nimajo dostopa.
- *Beleženje* (angl. a*ccounting*): sledenje uporabnikovih akcij. Občasno poimenovano tudi revizija.

V našem magistrskem delu se osredotočamo na prvi varnostni proces – overitev – in na metode ter protokole, ki se jih overitev poslužuje (Duncan, 2001; Syverson & Cervesato, 2001; Todorov, 2007).

2.2 Identifikacija in overitev

Overitev igra ključno vlogo pri varnosti porazdeljenih sistemov, izvede pa se s pomočjo overitvenih protokolov. Primarni cilj overitve je ta, da se vzpostavijo identitete sodelujočih entitet. Primeri sodelujočih entitet so uporabniki, delovne postaje, procesi, idr. Mnogi overitveni protokoli pa imajo tudi sekundarni namen razdelitve novega skritega sejnega ključa med sodelujočimi entitetami za namene komunikacije v prihodnosti (Woo & Lam, 1993).

Overitev sestoji iz dveh faz. Prva faza je identifikacija, druga pa overitev. Identifikacija poteka tako, da uporabnik varnostnemu sistemu poda svojo uporabniško identiteto, ki je večinoma predstavljena kot določen identifikator. Varnostni sistem pa nato v svoji bazi preveri, ali pozna objekt s tem identifikatorjem: če objekt s tem identifikatorjem najde, je identifikacija uspešno opravljena – če pa objekta ne najde, je identifikacija neuspešna.

Druga faza je overitev, ki je proces potrjevanja uporabniške identitete. To pomeni, da mora uporabnik tudi dokazati, da je dejansko tista entiteta, za katero se izdaja. To stori tako, da predloži dokaz, ki ga imenujemo poverilnica (angl. *credential*), ter tako dokaže svojo identiteto sistemu. Pri overitvi sistem preveri, ali se identiteta in poverilnica ujemata s shranjenima identiteto in poverilnico.

Poverilnice so različne in so odvisne od sistema. Določeni sistemi lahko zahtevajo celo več kot eno poverilnico. V računalniških sistemih je najbolj razširjena poverilnica uporabniško geslo, ki ga poznata le sistem in uporabnik. Ostali primeri poverilnic so certifikati, PIN številke, RFID značke, pametne kartice, biometrične lastnosti idr.

Pri overitvi večinoma sodelujejo tri komponente:

- *Prosilec*: entiteta v procesu overitve, ki se želi overiti in v ta namen predloži identiteto in poverilnico. Če sta identiteta in poverilnica ustrezni, je prosilec overjen. Drugi imeni za prosilca sta še stranka in uporabnik.
- *Overitelj*: entiteta v procesu overitve, ki uporabnika najprej overi, nato preveri, ali ima uporabnik dostop do virov, ter mu jih nazadnje posreduje. Drugo ime za overitelja je lahko tudi strežnik.
- *Varnostna baza*: shramba oziroma mehanizem za preverjanje uporabniških poverilnic. Baze so lahko različno kompleksne, od navadne datoteke na strežniku pa vse do skupine porazdeljenih strežnikov.

V najbolj preprostem primeru so vse tri entitete na istem računalniku, lahko pa je v lokalnem omrežju en računalnik namenjen overjanju, ostali pa so prosilci. V nekaterih primerih so celo vse tri entitete porazdeljene na več računalnikih na različnih geografskih lokacijah. Potrebno pa je zagotoviti, da lahko te tri entitete med seboj neodvisno komunicirajo (Todorov, 2007).

2.3 Overitvene metode

Overitev je proces preverjanja uporabniške identitete. Da sistem preveri identiteto, zahteva od uporabnika dokaz, ki mu rečemo poverilnica. V različnih okoljih se uporabljajo različni načini overitve, prav tako lahko en sistem zahteva več različnih dokazov, kot npr. v banki, kjer se je potrebno ob bančni kartici overiti še z osebnim dokumentom, na bankomatu pa sta potrebna bančna kartica in PIN koda. Zato je potrebno dobro premisliti, katera overitvena metoda je najbolj ustrezna za določeno okolje. Poverilnice se v osnovi delijo na tri skupine:

- »kar veš«: ta skupina predstavlja neko skrivnost, ki si jo delita uporabnik in overitveni sistem: Najbolj pogost primer je overitev s statičnim geslom.
- »kar imaš«: ta skupina predstavlja posedovanje nekega dejanskega objekta, ki mu rečemo overitveni žeton. Žetoni so različni, lahko so pametne kartice (angl. *smart cards*), usb ključek, obesek za ključe ali kaj drugega. Če prosilec poseduje takšen

žeton, je verjetno resnično tista oseba, za katero se izdaja, in ga sistem lahko overi.

- »kaj si«: ta skupina predstavlja neko biometrično lastnost, ki jo ima prosilec, in na podlagi katere overitelj overi prosilca. Biometrične lastnosti so prstni odtis, skeniranje obraza, mrežnice, način hoje in druge.

Večinoma se v overitvenih sistemih uporablja ena skupina, vendar samo ena skupina ne zagotavlja največje možne varnosti. Zato mnogi sistemi uporabljajo kombinacijo več overitvenih metod, kar poveča varnost. Hkrati pa se je potrebno zavedati, da uporaba več metod bistveno poveča tudi čas, ki ga uporabnik potrebuje, da se uspešno overi. Daljše trajanje overitve pa lahko povzroči, da se uporabniku poveča odpor do uporabe overitev z več metodami overjanja.

Posebna oblika overitve je vzajemna overitev, pri kateri prosilec in overitelj hkrati overjata drug drugega. Vzajemna overitev se po navadi uporablja, kadar želi prosilec zaupne podatke poslati na strežnik ali pa želi prejeti iz strežnika občutljive podatke, ki morajo biti nespremenjeni. Z vzajemno overitvijo se lahko uporabnik prepriča, da komunicira s pravim strežnikom in ne s sleparskim strežnikom. Različni overitveni mehanizmi različno podpirajo vzajemno overitev. Nekateri mehanizmi vzajemno overitev podpirajo samodejno, drugi jo podpirajo z uporabo dveh različnih overitvenih dialogov v obeh smereh, nekateri mehanizmi pa je sploh ne podpirajo (Schneier, 1996; Syverson & Cervesato, 2001).

2.3.1 Overitev z geslom

Gesla so najbolj razširjena metoda overitve, saj po navadi ne zahteva veliko procesorske moči in strojne opreme. Uporabniki podajo identifikator in vtipkajo geslo (skrivnost), ki si jo delita overitelj in uporabnik. Overitelj preveri identifikator in geslo med svojimi shranjenimi podatki in če sta identifikator in geslo pravilna, overitelj sklepa, da je uporabnik pristen – in overitev uspe. Obstajata dve vrsti gesel: statična gesla in enkratna gesla.

Statična gesla so najstarejša in najbolj razširjena uporabniška poverilnica. Statično geslo je skrivnost, ki si jo delita overitelj in prosilec, ter se ne spreminja prav pogosto. Da se dvigne nivo varnosti, morajo varnostni administratorji v podjetjih pripraviti priporočila oziroma navodila, na koliko časa naj se gesla zamenjajo, kakšne oblike naj bodo in iz nabora katerih simbolov naj bodo. Overitveni strežnik ima gesla shranjena v bazi, ki pa

mora biti ustrezno zavarovana. Statična gesla so priročna in ne potrebujejo posebne konfiguracije, ne na strani prosilca ne na strani overitvenega strežnika in ne na strani overitelja. Praktično vsaka platforma, aplikacija in operacijski sistem podpira overitev s pomočjo statičnih gesel. To pomeni, da se lahko na tak način uporabnik overja povsod in posledično od povsod dostopa do varovanih virov. Ker statična gesla uporabniku omogočajo veliko fleksibilnost glede lokacije, s katere lahko dostopa do varovanih virov, so zelo priljubljena in razširjena oblika overitve.

Vendar je enostavnost statičnih gesel hkrati tudi njihova največja slabost, saj so lahka tarča za napadalce. Moč overitve je odvisna od moči uporabljenega overitvenega mehanizma. In ker so po navadi overitveni mehanizmi, ki strežejo statična gesla, ranljivi na veliko število različnih napadov, ima posledično tudi overitev s takim geslom veliko ranljivosti. Primeri napadov, ki so primarno usmerjeni na statična gesla, so napad privzetih gesel, ugibanje gesla, izbrskanje v omrežju, napad ponovitve, napad vrinjene osebe, napad gledanja čez ramo, napad socialnega inženiringa in napad brskanja po smeteh. Večina teh napadov je bolj uspešnih, če so gesla šibka. Šibka gesla pa so posledica ljudi, ki si jih izbirajo tako, da so sestavljena iz nekih smiselnih besed, da si jih lažje zapomnijo. S tem olajšajo delo napadalcem, saj zmanjšajo zalogo vrednosti, ki jo lahko geslo zavzame. Strojno generirana gesla uporabljajo celoten nabor na tipkovnici, vendar so zaradi tega težje zapomnljiva. Kar pa lahko ponovno olajša delo napadalcem, saj si uporabnik v tem primeru geslo zapiše – pogosto kar na vidno mesto ob računalniku. Drug problem s strojno generiranimi gesli je ta, da so generirana s pomočjo psevdo-naključnih funkcij. Problem teh funkcij je, da se računalniki vedejo zelo predvidljivo in imajo le nekaj možnosti za naključnost. Majhno število možnosti pa lahko nekdo, ki dodobra pozna okolje, izrabi in ugane uporabljeno psevdo-naključno funkcijo. Zaključimo lahko, da so statična gesla zelo razširjena in zelo uporabljana metoda overitve z nizko do srednjo stopnjo varnosti.

Da bi se izognili ranljivostim statičnih gesel, so bila ustvarjena enkratna gesla. Enkratna gesla so skrivnosti, ki jih lahko uporabnik uporabi le enkrat oziroma le nekajkrat. Enkratnost gesel pomeni, da uporabnik ob vsakem overjanju uporabi novo geslo. Overitev z enkratnim geslom pa potrebuje posebno programsko ali strojno opremo na obeh straneh, torej na strežniku in na uporabniškem delu. Enkratna gesla lahko razdelimo v dve skupini. Prva deluje na podlagi seznama enkratnih gesel, druga pa na podlagi izziva in odgovora. Seznam enkratnih gesel deluje tako, da imata obe strani seznam gesel; ob uporabi gesla se geslo obkljuka in postane neprimerno. Naslednjič, ko se želi uporabnik overiti, zato uporabi naslednje geslo na seznamu. Ko se seznam izčrpa, se generira nov

seznam gesel. Takšen mehanizem je enostaven, vendar ni velikega zanimanja za uporabo; bolj so namreč uporabljani kompleksnejši mehanizmi, kot so S/KEY, OPIE in RSA SecurID (Acar, Belenkiy, & Küpçü, 2013; Duncan, 2001; Todorov, 2007).

2.3.2 Asimetrični ključi in poverilnice na podlagi certifikatov

Asimetrična kriptografija ali kriptografija javnega ključa temelji na kompleksnih matematičnih problemih, ki zahtevajo zelo specializirano znanje. Kriptografija uporablja dva ključa, javnega in privatnega, ki sta povezana prek zelo kompleksne matematične funkcije. Privatni ključ je skriven, javen ključ pa lahko razkrijemo vsem uporabnikom na internetu in ni skrivnost. Sam par asimetričnih ključev privzeto ne vsebuje podatka o tem, komu ključa pripadata. Vendar je v mnogih primerih zelo koristno, če lahko lastnika ključa identificiramo. Na ta način potrdimo, čigav je javni ključ, ter preverimo, da je dejansko od ustrezne osebe in ne od sleparja. Pri enem izmed takšnih pristopov se javni ključ uporabi za to, da se identificira uporabnika, privatni ključ pa se uporabi za to, da se overi uporabnika. Javni ključ je znan vsem in je zato lahko povezan z uporabnikovo identiteto. Privatni ključ pa je skrivnost in ga lahko posameznik uporabi za preverjanje identitete, saj sta javni in privatni ključ povezana med seboj. Vendar ima ta opcija omejeno uporabnost, saj ne podpira zapisa vseh podatkov, ki bi nas utegnili zanimati: npr. kdaj sta bila ključa ustvarjena, kako dolgo sta veljavna in za katere namene sta bila ustvarjena. Te podatke nam lahko podajo certifikati. Certifikat je zbirka javnih podatkov o uporabniku in javni ključ, potrjen s strani zaupanja vredne tretje osebe (izdajatelja digitalnih potrdil), ki zagotavlja verodostojnost teh podatkov. Certifikati se lahko uporabljajo za overitev uporabnikov, saj vsebujejo njihovo identiteto in njihov javni ključ. Ko zaupanja vredna tretja stranka certificira poverilnice, ki jih je uporabnik posredoval, podpiše javni ključ. Gostom, ki želijo dostopati do vira, ki ga ščiti podpisani javni ključ, podpis zagotavlja, da je bil lastnik preverjen in uspešno certificiran.

Kriptografija javnih ključev deluje tako, da uporabnik z njimi generira nekaj naključnih števil in jih pošlje strežniku kot sporočilo. Strežnik po prejetju sporočila na podlagi prvih naključnih števil generira nova naključna števila in jih vrne uporabniku. Uporabnik nato izračuna nove vrednosti in pošlje drugo sporočilo strežniku. Strežnik pa nato na podlagi javnega ključa preveri, ali so bile vrednosti izračunane s pomočjo zasebnega ključa uporabnika. Tako strežnik overi uporabnika, če pa želi uporabnik overiti strežnik, se vlogi preprosto zamenjata (Duncan, 2001; Todorov, 2007).

2.3.3 Biometrične poverilnice

Overjanje na podlagi biometrije je iz skupine »kaj si« in temelji na fizičnih lastnostih ali na obnašanju uporabnika. Ideja biometrije je v tem, da so merljive karakteristike uporabnika (kot so pisava, prstni odtis, mrežnica idr.) unikatne in se redko oziroma nikoli ne spremenijo – ter se zato lahko uporabijo za overitev uporabnika. Biometrija se lahko uporablja za overitev ali pa za identifikacijo in overitev. V obeh primerih mora biti baza napolnjena z biometričnimi profili vseh posameznikov, ki se bodo identificirali in overjali. Proces polnjenja baze se imenuje vpis (angl. *enrollment*), tekom katerega mora vsak uporabnik sistemu podati določen biometričen vzorec, po navadi tudi več vzorcev, da sistem kalibrira in shrani najbolj optimalen vzorec. Merili za natančnost in učinkovitost biometričnih naprav sta FAR (angl. *false acceptance rate*) in FRR (angl. *false rejection rate*) in pomenita odstotek napačno sprejetih uporabnikov oziroma odstotek napačno zavrnjenih uporabnikov. Kakovostne biometrične naprave imajo obe merili nizke vrednosti, hkrati pa je njihov sistem hiter in priročen. Kadar je biometrija uporabljena zgolj za overitev, mora uporabnik podati svojo uporabniško identiteto (ID) in nato še svoj biometrični vzorec, ki ga sistem primerja z njegovim vzorcem v bazi. V primeru, da se uporabnik želi identificirati in overiti z biometrijo, pa poda samo svoj biometrični vzorec, ki ga sistem primerja z vsemi vzorci v bazi; če najde ujemanje, je uporabnik identificiran in overjen. Potrebno je poudariti, da je lahko drugi način časovno zelo zamuden, predvsem če ima sistem velike baze podatkov. Kot primer takšnega iskanja lahko navedemo kriminaliste, ki v bazah iščejo osebe na podlagi njihovih prstnih odtisov.

Obstajata dve vrsti biometričnih poverilnic: statična biometrija in dinamična biometrija. Statična biometrija temelji na vzorcih biometričnih lastnosti, ki ostajajo enaki. Primeri takšnih vzorcev so prstni odtisi, mrežnica, poteze obraza idr., kjer sistem uporabnika overi tako, da vzorce shrani v obliki vektorske ali rastrske slike in potem primerja, ali se sliki ujemata. Dinamična biometrija pa temelji na obnašanju, kar pomeni, da prepoznava različno obnašanje, kot so dinamika pisave, barva in ton glasu, način tipkanja idr.

Biometrija ostaja dokaj malo uporabljana metoda, saj ima v primerjavi z drugimi visoke stroške. Na njeno priljubljenost vpliva tudi človeški faktor, saj imajo ljudje lahko zadržke pred uporabo biometrije. Dodatno oviro predstavlja natančnost, saj je lahko slika nejasna in posledično sistem ne razpozna značilnosti uporabnika (Duncan, 2001; Todorov, 2007).

2.3.4 Dokaz ničelnega znanja

Pri metodi overjanja s pomočjo dokaza ničelnega znanja poskuša uporabnik prepričati gostitelja, da mu odobri dostop do virov, ne da bi dejansko razkril kakšno skrivnost. Udeleženca v takšni metodi overjanja po navadi komunicirata večkrat, preden uspešno dokončata overitev. Uporabnik najprej ustvari težek naključen problem, ki ga reši na podlagi informacij, ki jih ima. Rešitev problema nato naloži in jo skupaj s problemom pošlje strežniku. Strežnik nato od uporabnika zahteva, da bodisi dokaže, da sta problema povezana, bodisi odpre rešitev in dokaže, da je to res rešitev. V večini primerov potrebujemo za uspešno overitev deset takšnih izmenjav. Vendar ima dokaz ničelnega znanja tudi svoje probleme, glavni izmed njih je napad vrinjene osebe (Duncan, 2001).

2.3.5 Hibridne overitvene metode na podlagi vstopnic

Overitev na podlagi vstopnic združuje enostavnejša overjanja (kot je na primer overjanje s statičnim geslom) z overjanji, ki temeljijo na kriptografiji. Overjanje na podlagi vstopnic uporablja zaupanja vredno tretjo osebo (varnostni strežnik), ki overi uporabnika in mu izda vstopnico. Uporabnik nato vstopnico predloži, ko želi dostopati do varovanih virov. Overitev poteka v naslednjih dveh fazah:

- *Uporabnikova overitev na overitvenem strežniku*: uporabnik, ki želi dostopati do virov se poveže na zaupanja vredno tretjo osebo (varnostni strežnik) in poda svojo poverilnico, npr. uporabniško ime in geslo. Strežnik nato preveri poverilnico, in če so podatki pravilni, overi uporabnika ter mu izda vstopnico. Vstopnica je podpisana in v nekaterih primerih tudi šifrirana s strani strežnika, zato da je uporabnik ne more spreminjati ali prebrati njene vsebine.
- *Uporabnikova overitev na strežniku virov*: s pridobljeno vstopnico lahko uporabnik poskuša dostopati do virov. To pa se zgodi tako, da na strežnik virov poda zahtevo po viru skupaj z vstopnico. Strežnik virov nato preveri podpis vstopnice in če gre za podpis overitvenega strežnika, ki mu strežnik virov zaupa, pregleda vstopnico, jo po potrebi dešifrira, preveri informacijo o identiteti in overitvi uporabnika ter na podlagi tega uporabniku dodeli ali zavrne dostop do vira.

Pri tej metodi overitve se lahko na overitvenem strežniku uporabi poljubna metoda overitve, kar pomeni, da se lahko uporabniki overjajo na overitvenem strežniku preko

gesel, biometrije, certifikatov in drugih overitvenih metod, saj jim izdana vstopnica zagotavlja, da so podali pravilne poverilnice. Hkrati strežnika virov ne zanima in mu ni potrebno vedeti, kako so se uporabniki overili, bistveno je le, da imajo veljavno vstopnico, na podlagi katere se jim dodeli dostop. Vstopnica je veljavna, če je podpisana s strani overitvenega strežnika; če je podpis pravilen, potem je vstopnica pristna. V nasprotnem primeru pa je bila vstopnica spremenjena in strežnik virov zavrne dostop. Strežnika med seboj ne komunicirata, saj strežnik virov lokalno preveri podpis na podlagi izračunov, uporabljata pa lahko tudi različne metode za podpisovanje in šifriranje, bodisi simetrične ali asimetrične (Todorov, 2007).

2.4 Overitveni protokoli

V porazdeljenem okolju se overitev izvede preko overitvenih protokolov. V idealnem svetu, kjer bi si vsaka naprava delila skriti ključ z vsemi drugimi napravami, s katerimi komunicira, in kjer ti ključi ne bi bili nikoli ogroženi, preklicani ali odjavljeni, bi bili overitveni protokoli morda odveč. Vendar je takšna situacija daleč od realnosti, saj so ključi pogosto ogroženi, preklicani in odjavljeni. Zato mora obstajati nek mehanizem, s katerim lahko dve entiteti, ki si ne delita skrivnega ključa, vzpostavita povezavo in ustvarita skriti ključ, da lahko varno komunicirata. Tukaj nastopijo overitveni protokoli.

Overitveni protokoli so izmenjava šifriranih sporočil, ki imajo določeno obliko in so namenjeni overitvi entitete. Velikokrat imajo tudi drugoten namen razdeljevanja sejnega ključa. Sporočila in ključi so pogosto šifrirani, bodisi s pomočjo simetričnega ali asimetričnega šifriranja. Kriptografija simetričnega ključa se zanaša na isti ključ za šifriranje in dešifriranje. Primera takšne kriptografije sta DES (angl. *data encryption standard*) in AES (angl. *advanced encryption standard*). Kriptografija asimetričnega ključa (ali tudi kriptografija javnega ključa) pa uporablja različna ključa za šifriranje in dešifriranje. Najbolj poznana kriptografija je RSA (ime je po avtorjih Rivest, Shamir in Adleman) (Syverson & Cervesato, 2001).

Overitev je v osnovi zagotovitev o tem, s kom komuniciraš, kar pa se lahko tudi bolj podrobno opredeli: npr. »želimo se prepričati, da so tisti, ki prejmejo sejni ključ, res tisti, za kogar se izdajajo«, »želimo biti prepričani, da entiteta, za katero mi mislimo, da si z njo delimo ključ, misli enako (torej misli, da si deli ključ z nami)«, »želimo biti prepričani, da oseba, za katero mislimo, da ima ključ, dejansko ima ključ« in podobno (Burrows, Abadi, & Needham, 1990; Syverson & Cervesato, 2001; Woo & Lam, 1993).

3 NAPADI IN VARNOSTNE ZAHTEVE

3.1 Napadi na overitvene protokole

Glavni namen identifikacije in overjanja je preverjanje uporabniške identitete. Računalniški sistemi potrebujejo overjanje zato, da lahko določijo, kateremu uporabniku omogočiti dostop do nekega vira in kateremu uporabniku ga onemogočiti. Napadalci želijo prevarati overitveni sistem in pridobiti dostop do virov, do katerih ne bi smeli imeti dostopa. To storijo tako, da vdrejo v informacijske sisteme in »zlomijo« overitvene mehanizme, ki ščitijo vire. Za dosego teh ciljev lahko zlonamerne osebe uporabijo različne načine. V tem poglavju bomo našteli in opisali nekaj znanih napadov, s katerimi smo se v sistematičnem pregledu literature srečali.

3.1.1 Obhod overitve

Če napadalec nima poverilnic (npr. uporabniškega imena in gesla) in se torej ne more overiti na strežniku, lahko poskuša obiti overjanje. Overjanju se lahko izogne na različne načine, odvisno od same aplikacije in od tipa dostopa do računalnika, na katerem ta aplikacija teče.

Če aplikacija teče lokalno na računalniku in ima napadalec fizični dostop do računalnika, lahko napadalec potencialno pridobi administrativne pravice. Te so lahko že dostopne ali pa si jih zagotovi s stopnjevanjem privilegijev. Ko ima napadalec enkrat administrativne pravice, lahko dostopa do vseh datotek in procesov, ki tečejo na računalniku, kar mu omogoča, da zažene procese v skrbniškem načinu ali pa da zamenja datoteke. S tem lahko zažene aplikacijo, ki izvaja overitev, v skrbniškem načinu. Potem lahko spremeni ukaze, ki primerjajo geslo, z ukazi, ki ne izvedejo ničesar, ali pa z ukazi, ki vrnejo uspešno overitev. Tako si zagotovi dostop do aplikacije. Napadalec lahko spreminja kodo, ki je že v spominu, ali pa zagonske datoteke, na katerih spremembe pričnejo veljati šele z naslednjim zagonom. Takšen način obhoda overitve je težje izvedljiv preko omrežja, razen če je strežnik ranljiv za napade, ki napadalcu omogočijo administrativni ali lokalni dostop. Vendar obstajajo tudi drugi načini obhoda overitve preko omrežja. Eden izmed teh pristopov je zloraba overite do spletnih virov. Ti viri so pogosto v

začetku objavljeni z anonimno overitvijo, nato pa se kasneje administratorji odločijo da želijo vire zaščititi. Zaščitijo pa jih tako, da za overitev pripravijo preprosto spletno stran s prijavnim oknom, kjer se zahtevata uporabniško ime in geslo. Ta pa sta lahko statično shranjena nekje v kodi ali pa sta shranjena v uporabniški podatkovni bazi. Ko se enkrat overimo na tej strani, pridobimo dostop do virov. Takšen dostop je lahek za implementacijo, a ima svoje slabosti. Ena izmed njih je ta, da če uporabnik ve ali uspe uganiti URL, ki je v ozadju, lahko potencialno dostopa do virov mimo strani z overitvijo. Da se reši ta problem je najbolje, da strežnik ustvarja zahteve za vir v imenu uporabnikov tako, da uporablja njihove prave uporabniške račune. Pogoj je seveda seznam pooblaščenih uporabnikov za vsak vir. Tako se anonimnim zahtevam onemogoči dostop do vira, saj OS zahteva prijavo (Dalton, Kozyrakis, & Zeldovich, 2009).

3.1.2 Privzeta gesla

Ena izmed glavnih šibkih točk varne overitve so privzeta gesla. Veliko ponudnikov strojne in programske opreme ima v svojih operacijskih sistemih, programih in strojni opremi nastavljena privzeta gesla. V primeru, da sistemski načrtovalci ne spremenijo gesel opreme in če napadalec ve ali ugane, katera oprema je bila uporabljena, lahko s pomočjo privzetega gesla pridobi dostop do omrežja ali naprave (Subramanian, Roth, Stoica, Shenker, & Katz, 2004).

3.1.3 Stopnjevanje privilegija

Ob prijavi v sistem se od uporabnika zahteva podatke. Te podatke lahko določeni procesi aplikacije uporabijo in poskušajo v imenu uporabnika izvesti overitev. V nekaterih primerih lahko zlonamerne osebe najdejo varnostno luknjo: pomanjkljivost v aplikaciji ali v operacijskem sistemu. Pogosto se aplikacija ali storitev izvaja na strežniku z lastnim uporabniškim računom, ki ima lahko različno omejen dostop. Napadalec lahko v aplikaciji spremeni overitveno logiko in prevzame njene poverilnice. To stori tako, da vnese v vnosna polja neveljaven vnos (daljši tekst kot je velikost medpomnilnika). Na ta način vnese svojo kodo v sistem, z njo spremeni program in ga prisili, da izvede kodo, ki jo je sam napisal. Grožnja tega napada se lahko zmanjša ali omili s strogim preverjanjem

uporabniških vnosov in z drugimi tehnikami pisanja varne kode (Davi, Dmitrienko, Sadeghi, & Winandy, 2011).

3.1.4 Ugibanje gesla

Eden izmed najstarejših napadov je ugibanje gesla. Uporabniško overjanje z uporabo uporabniškega imena in gesla je prisotno že od začetka IT, posledično tudi ugibanje gesla. Če sistem zahteva uporabniško ime in geslo za overitev uporabnika, lahko napadalec ugiba uporabniško ime in geslo in se overi kot dejanski uporabnik. Informacije o uporabniškem imenu lahko napadalec pridobi razmeroma lahko, v mnogih primerih je uporabniško ime enako prvemu delu naslova elektronske pošte. Napadalec lahko pozna logiko določanja uporabniških imen za nove uporabnike v določenem podjetju, prav tako ima lahko dostop do registra vseh uporabniških imen (če je napadalec znotraj podjetja). Napadalec izvede napad tako, da poizkusi eno ali več gesel, za katera je verjetno, da bi jih dejanski uporabnik uporabljal.

V primeru, da napadalec nima ideje, kakšno bi lahko bilo geslo, lahko uporabi napad surove sile. To pomeni to, da orodje za razbijanje gesel generira vsako možno kombinacijo gesla in preizkusi kombinacijo uporabniškega imena in gesla. Takšen napad lahko uspe pod pogojem, da ima dovolj časa in da uporabnik vmes ne spremeni gesla. Problem napada surove sile je ta, da je kombinacij ogromno. Težavnost (in s tem čas, ki je potreben za razbitje) je odvisna od števila in razpona znakov, ki jih lahko uporabimo v geslu. Če lahko uporabljamo številke, male in velike črke ter znake, je kombinacij ogromno. Prav tako lahko napad oteži, če ima podjetje stroga pravila za gesla in jih menjuje na krajši časovni interval, kot je čas, ki je potreben za preverbo vseh kombinacij z napadom surove sile. Zato je ta napad primeren samo za razbijanje kratkih gesel z omejenim naborom znakov.

Drug primer ugibanja gesla je napad s slovarjem, ki temelji na dejstvu, da so uporabniki ljudje in si zato izbirajo gesla, ki nekaj pomenijo – in si jih je zato lažje zapomniti in lažje uganiti. S to informacijo se namreč zelo zmanjša nabor vseh kombinacij. Napadalec pridobi seznam vseh besed in imen ter jih zbere skupaj v »slovar«. Program nato preizkusi vse kombinacije.

Napad surove sile potrebuje veliko časa in sistemskih virov. Čas, ki je potreben za razbitje gesla, se lahko zmanjša z uporabo mavričnih tabel z vnaprej izračunanimi vrednostmi. Ker orodju ni treba sproti računati vrednosti, se bistveno zmanjša čas

izvedbe. Da se omili grožnja napada z uporabo mavričnih tabel, lahko overitveni sistem uporabi shemo na podlagi izziva in odgovora, kot tudi dodajanje naključne vrednosti geslu (angl. *salting*). Tabele postanejo nepregledno velike, če morajo vsebovati vse kombinacije naključnih vrednosti ali pa se tabele vsakič ponovno računajo, kar njihovo učinkovitost zmanjša na nivo podoben napadu surove sile (Chuang & Chen, 2014; Hwang, Chong, & Chen, 2010; Xie et al., 2014).

3.1.5 Vohljanje poverilnic iz omrežja

Lahek način za napadalca, da pridobi uporabniško geslo ali druge poverilnice, predstavlja vohljanje prometa na omrežju (angl. *sniffing*) ali prisluškovanje (angl. *eavesdroping*). Mnogi starejši sistemi in aplikacije prenašajo uporabniške informacije in poverilnice čez omrežje v nešifrirani obliki. Primeri tega so FTP, HTTP in Telnet. V njihovi najbolj preprosti obliki ti protokoli dialoga med overitvijo ne šifrirajo. Če kdo vohlja po prometu na omrežju, lahko s tem pridobi uporabniško ime in geslo v navadnem besedilu. Da se zaščitimo pred tem napadom, mora biti overjanje primerno šifrirano (Hsieh & Leu, 2013; Moosavi, Nigussie, Virtanen, & Isoaho, 2014).

3.1.6 Ponovitveni napad

Drug popularen način napada na overitvene mehanizme je ponovitven napad (angl. *replay attack*). Za ta napad je potreben dostop napadalca do omrežja med uporabnikom in strežnikom, lahko pa da ima napadalec dostop tudi do kakšnega drugega načina motenja overitve. Ponovitveni napad je mehanizem, s katerim napadalec ne pridobi gesla v navadnem besedilu, ampak uporabi kar šifriran tekst za overitev. Napadalec prestreže šifrirano geslo, ki ga uporabnik pošlje strežniku, in ga sam pošlje strežniku.

Na ponovitven napad so najbolj ranljive sheme, ki uporabljajo statične overitvene parametre. Večina overitvenih protokolov pa uporablja izzive in odgovore, kar deluje tako, da strežnik generira naključno besedilo in ga pošlje uporabniku kot izziv. Uporabnik izvede neko akcijo nad besedilom, nato pa ga šifrira z uporabo gesla, s ključem na osnovi gesla ali pa izvede zgoščevalno funkcijo nad izzivom in geslom. V vsakem primeru je uporabljeno geslo za generiranje odgovora strežniku. Če napadalcu uspe zajeti celotno sejo, lahko vidi šifrirane odgovore uporabnika, ki so odvisni od izziva strežnika. Ko pa se

poskuša overiti še napadalec, dobi drugačen izziv in se ne more overiti, ne da bi poznal geslo. Vendar se moč overitve z izzivi in odgovori močno zanaša na naključnost izzivov, saj lahko napadalec v primeru, da mu strežnik poda isti izziv, ki ga je dal že uporabniku, ponovno uporabi isti šifriran odgovor. Da se zagotovi dodatna varnost pred ponovno uporabo, mnogo shem uporabi tudi druge parametre, kot je trenutni čas (Hafizul Islam & Biswas, 2013; Jiang, Wen, Li, Jin, & Zhang, 2015; Shen, Gao, He, & Wu, 2015).

3.1.7 Napad poosebljanja

Napad poosebljanja (angl. *impersonation attack*), ki je znan tudi pod imenom maškaradni napad (angl. *masquerading attack*) ali napad lažnega predstavljanja (angl. *spoofing*), predstavlja napad, kjer napadalec s pomočjo lažnih ali napačnih podatkov uspe prevarati osebo ali strežnik, da mu omogoči dostop do virov. Napad poosebljanja se lahko razlikuje odvisno od tega, katerega udeleženca napadalec pooseblja, tako da poznamo tudi napade poosebljanja strežnika. Primeri tega napada so prevara lokacije, prevara časa, prevara prijavne strani in prevara e-poštnega naslova, kjer napadalec ustvari lažno lokacijo, čas, prijavno stran ali e-poštni naslov in s tem prevara uporabnika, da izda skrivnosti (Cohen, 1997; Lu, Li, Peng, & Yang, 2015).

3.1.8 Zmanjševanje overitvene moči

Ta napad se po navadi uporablja na overitvenih protokolih, ki se z uporabnikom pogajajo o načinu overitve. Nekateri overitveni mehanizmi so lahko močnejši, drugi šibkejši. Uporabnik ali strežnik določi urejen seznam overitvenih mehanizmov, druga entiteta pa iz tega seznama izbere en mehanizem.

Če napadalec nekje vmes prestreže promet in uredi pakete, lahko spremeni seznam mehanizmov na tak način, da je šibkejša overitev bolj priljubljena, ali pa da je šibkejša overitev edina, ki jo oba podpirata. To prisili uporabnika in strežnik v uporabo šibkejšega overitvenega mehanizma, ki na primer prenaša geslo kot navadno besedilo preko omrežja, tako da ga napadalec zlahka prebere iz omrežja. Zaščita pred tem napadom je, da se zavaruje komunikacijski kanal med strežnikom in uporabnikom, preden začneta pogajanja o overitvenem mehanizmu. Prav tako lahko strežnik in uporabnika konfiguriramo tako, da uporabljata zgolj močne overitvene mehanizme (Todorov, 2007).

3.1.9 Sleparski strežniki

Napad sleparskega strežnika (angl. *server spoofing*) ali napad pooseblјanja strežnika (angl. *server impersonation attack*) se izvede tako, da se v omrežje vnese sleparski strežnik namesto pravega strežnika. Uporabnik se nato poskuša overiti na sleparskem strežniku, misleč, da je pravi strežnik. Uporabnik je tako zaveden in napadalcu poda svoje uporabniško ime in geslo ali druge poverilnice. Da se izognejo takšnim napadom, veliko overitvenih mehanizmov uporablja medsebojno overitev, kar pomeni, da se tudi strežnik overi uporabniku, ne samo uporabnik strežniku. Tako lahko uporabnik ugotovi, da je strežnik sleparski in konča overitveni proces (Kalra & Sood, 2015; Shen et al., 2015).

3.1.10 Napadi vrinjene osebe

Napad vrinjene osebe (angl. *man-in-the-middle-attack*) je ime za cel nabor napadov, kjer napadalec »sedi« oz. se nahaja nekje med uporabnikom in strežnikom ali pa med dvema entitetama, ki komunicirata. Napadalec je sposoben sprejemanja in pošiljanja sporočil od obeh sodelujočih. Zato ima napadalec moč, da pošlje dalje nespremenjeno sporočilo, ali pa da spremeni vsebino. Napadi vrinjene osebe so lahko učinkoviti pri uporabniški overitvi kot tudi pri dejanskem uporabniškem podatkovnem prometu. Takšni napadi se preprečujejo z uporabo medsebojnega overjanja, šifriranja kanala komunikacije in varovanja neokrnjenosti. Primeri so napad odboja (angl. *reflection attack*), napad modifikacije (angl. *modification attack*), napad vzporedne seje (angl. *parallel session attack*).

Eden izmed napadov vrinjene osebe je tudi ugrabitev seje (angl. *session hijacking*). Napadalec, ki izvaja ta napad, ima kontrolo nad komunikacijskim kanalom med uporabnikom in strežnikom. Pri napadu lahko napadalec počaka, da se uporabnik uspešno overi pri strežniku, nato pa lahko prestreže sporočila in jih pošlje dalje spremenjena oziroma jih sploh ne pošlje. Zaščita pred ugrabitvijo seje je ista kot za MITMA napade (Islam & Biswas, 2015; Todorov, 2007).

3.1.11 Vohunjenje čez ramo

Eden izmed netehnoloških napadov je vohunjenje čez ramo (angl. *shoulder surfing*). Čeprav ni IT napad, je vseeno lahko učinkovit. Kot je razvidno iz imena, pri tem napadu napadalec gleda oziroma vohuni čez ramo uporabnika, ko le ta vpisuje svoje geslo. Uporabniki se temu napadu izognejo tako, da se prepričajo, da jim nihče ne gleda čez ramo, prav tako so uporabna enkratna gesla (Todorov, 2007).

3.1.12 Beležniki tipkanja, trojanski in drugi virusi

Še en način, kako lahko napadalec pride do uporabniškega gesla, je, da na delovno postajo namesti beležnik tipkanja (angl. *keylogger*), ki predstavlja skrit program, ki v zapisnik shranjuje informacije o tipkah, ki jih uporabnik pritisne. Trojanski virus ali kakšen drug virus deluje podobno, vendar namesto beleženja pritisnjenih tip prestreza komunikacijo med uporabnikom in strežnikom in shranjuje dobljene informacije v bazo, ki jo lahko kasneje napadalec analizira (Todorov, 2007).

3.1.13 Nepovezani napadi

Nepovezani napadi (angl. *offline attacks*) se izvajajo tako, da poskuša napadalec pridobiti dostop do podatkovne baze poverilnic. Ta podatkovna baza je po navadi shranjena v datoteki na overitvenem strežniku in napadalec si jo poskuša prenesti na neko drugo lokacijo, kjer jo lahko analizira. Kraja te datoteke je možna, če ima napadalec administrativne pravice na računalniku, na katerem gosti overitveni strežnik, ali če ima napadalec fizični dostop do strežnika in lahko ponovno zažene računalnik z drugim operacijskim sistemom, na katerem ima poln dostop do sistema. Obstaja velika verjetnost, da nepovezan napad uspe, tudi če je datoteka z gesli šifrirana. Da se izognemo takšnemu napadu, je potrebno natančno in previdno načrtovanje fizičnega in administrativnega dostopa do overitvenega strežnika (Todorov, 2007).

3.1.14 Napad notranje osebe

Napad notranje osebe (angl. *insider attack*) je vrsta napada, pri katerem je osnova to, da ima napadalec dostop ali privilegiran dostop do sistema. Napad notranje osebe je začetna stopnja napada, saj je sam dostop do sistema po navadi pridobljen legalno (npr. napadalec je zaposlen tam), napad pa se izvede z uporabo katere druge tehnike (prisluškovanje, prestrezanje). Drugo ime za napad notranje osebe je tudi napad privilegirane notranje osebe (angl. *privileged insider attack)* (Cohen, 1997; Das, 2014; Markantonakis, Tunstall, Hancke, Askoxylakis, & Mayes, 2009).

3.1.15 Napad na pametno kartico

Napad na pametno kartico (angl. *smart card attack*) ali napad ukradene pametne kartice (angl. *stolen smart card attack*) je napad, ki se pojavlja pod različnimi imeni (napad ukradene pametne kartice, vdor v pametno kartico), predstavlja pa napad, kjer napadalec pridobi pametno kartico uporabnika, nato pa vdre v njo. Vendar pa vdor v pametne kartice lahko izvedejo le tehnično zelo dobro podkovani posamezniki in za to potrebujejo veliko časovnih in tehničnih virov (Cohen, 1997; Mishra, 2015).

3.1.16 Brskanje po smeteh

Napad brskanja po smeteh (angl. *dumpster diving*) predstavlja napad, kjer napadalec v smeteh išče kakšne skrivnosti, saj se mnogokrat zgodi, da uporabnik dobi fizično izpisano začetno geslo za prijavo v sistem, se prijavi, nato pa pismo odvrže v smeti. Če napadalec v smeteh najde to pismo in če uporabnik ni pravočasno zamenjal gesla, lahko napadalec z lahkoto uporabi te podatke za prijavo v sistem in tako pridobi dostop do virov (Cohen, 1997; Duncan, 2001).

3.2 Varnostne zahteve

Varnostne zahteve predstavljajo različne lastnosti, ki jih morajo overitveni protokoli izpolnjevati, da dosežejo nek nivo varnosti. V tem poglavju jih bomo nekaj našteli in na

kratko opisali. Varnostne zahteve je potrebno definirati ob načrtovanju protokola in morajo biti definirane natančno (Deebak, Muthaiah, Thenmozhi, & Swaminathan, 2015; Ding, Zhou, Cheng, & Zeng, 2013; Farash, Kumari, & Bakhtiari, 2015; Gope & Hwang, 2015; Moosavi et al., 2014; Morshed, Atkins, & Yu, 2012; Zhu, 2015).

Poznamo naslednje overitvene zahteve:

- *Varnost pred limanico (angl. honeypot security)*: lastnost protokola, da je odporen na limanice (angl. *honeypots*).
- *Varnost shrambe (angl. storage security)*: lastnost protokola, da vsebuje skupino parametrov, s katerimi naredi vire razpoložljive pooblaščenim osebam in nerazpoložljive nepooblaščenim osebam.
- *Anonimnost (angl. anonymity)*: lastnost protokola, da zagotavlja anonimnost sodelujočih.
- *Nepovezljivost (angl. unlinkability)*: lastnost protokola, ki zagotavlja, da napadalec ne more identificirati preteklih izvedb protokola z istimi sodelujočimi.
- *Vzajemna overitev*: lastnost overitvenega protokola, da obema stranema omogoča vzajemno preverjanje identitete.
- *Varnost znanega ključa (angl. known key security)*: lastnost, ki zagotavlja da zlonamerna oseba iz ukradenega sejnega ključa ne more izračunati naslednjih sejnih ključev.
- *Popolna prihodnja varnost (angl. perfect forward secrecy)*: lastnost ki zagotavlja, da se ob razkritju ključa ne ogrozijo predhodna sporočila.
- *Varnost sejnega ključa (angl. session key security):* lastnost, ki zagotavlja, da zlonamerna oseba ne more pridobiti sejnega ključa brez posedovanja določenih skrivnosti.
- *Tajnost znanega ključa (angl. known key secrecy):* lastnost, ki zagotavlja da razkritje preteklega znanega ključa ne povzroči razkritja kakršnegakoli drugega ključa.
- *Tajnost sejnega ključa (angl. session key secrecy):* lastnost, ki zagotavlja, da se sejni ključ ne bo razkril nobenemu drugemu kot registracijskemu centru.
- *Privatnost RFID značke (angl. tag privacy):* lastnost protokola, da so sporočila značke dovolj naključna, da napadalec ne more razločiti sporočil ene značke od ostalih.
- *Anonimnost značke (angl. tag anonymity):* lastnost protokola, da zagotavlja varnost pred razkritjem informacij, ki bi lahko vodile do razkritja identifikatorja značke.

- *Brez verifikacijske tabele (angl. no verification table):* lastnost, ki zagotavlja, da protokol ne shranjuje tabele z zgoščenimi vrednostmi gesel ali kakršnihkoli drugih informacij.
- *Privatnost bralca (angl. reader privacy):* lastnost, ki zagotavlja, da je interakcija značke in bralca skrita pred strežnikom.
- *Dogovor o ključu:* lastnost protokola, da zagotavlja proces dogovora o ključu, kjer oba sodelujoča neodvisno drug od drugega vplivata na ključ.
- *Zaščita gesla (angl. password protection):* lastnost protokola, da nikoli ne pošlje nešifriranega gesla čez omrežje.
- *Nedavnost ključa (angl. key freshness):* lastnost protokola, da so vse naključne vrednosti, iz katerih se izračuna ključ, nedavne, kar pomeni, da je posledično tudi ključ nedaven.
- *Razpoložljivost (angl. availability):* lastnost RFID naprave, ki zagotavlja odpornost na napad ohromitve storitve, prav tako pa zagotavlja, da napadalec ne more vplivati na delovanje naprave.
- *Skalabilnost (angl. scalability):* lastnost RFID sheme, ki zagotavlja, da se računska zahtevnost ne veča skupaj s številom značk.
- *Brez nadzora ključa (angl. no key control):* lastnost, ki zagotavlja, da nobena sodelujoča entiteta nima popolnega nadzora nad sejnim ključem.

4 PREGLED METODE - SISTEMATIČNI PREGLED LITERATURE

Vsako znanstveno-raziskovalno delo vsebuje tudi empirični del, kjer so predstavljeni potek in rezultati izvedene empirične raziskovalne metode. Med različne empirične raziskovalne metode sodijo anketa, študija primera, eksperiment, intervju, sistematični pregled literature, idr. Mi bomo v našem magistrskem delu uporabili raziskovalno metodo sistematični pregled literature.

Sistematični pregled literature (angl. *SLR – systematic literature review*) je način prepoznavanja, vrednotenja in interpretiranja vsega dostopnega raziskovanja na izbranem raziskovalnem področju. Vse študije, ki jih pri sistematičnem pregledu literature odkrijemo, so *primarne* študije, sam sistematični pregled literature pa je tip *sekundarne* študije.

Poglavitni razlogi za izvedbo sistematičnega pregleda literature so lahko:

- Da povzamemo in združimo obstoječe raziskave iz področja, ki nas zanima.
- Da identificiramo pomanjkljivosti dosedanjih raziskav, da lahko priporočamo področja prihodnjim raziskavam.
- Da pripravimo primerno ogrodje oziroma ozadje, da se lahko bodoče raziskave primerno umestijo.
- Da preverimo raziskovalne hipoteze.
- Da nam pomaga pri snovanju raziskovalnih hipotez.

Glavne prednosti sistematičnega pregleda literature so dobro definirana metodologija, informacije iz širšega kroga empiričnih metod in pogojev ter v primeru kvantitativnih raziskav uporaba meta-analitičnih tehnik.

Dobro definirana metodologija zmanjša možnost pristranskosti študije, vendar se je potrebno zavedati, da so primarne študije še vedno lahko pristranske. Zaradi pregleda več raziskav, ki se med seboj razlikujejo, lahko opazujemo več različnih pogojev raziskav in različne raziskovalne metode. Če nam raziskave podajajo iste rezultate, pomeni, da je pojav, ki ga raziskujemo, robusten in prenosljiv, če pa so rezultati raziskav različni, lahko poskušamo najti vzrok za nedoslednost rezultatov. Uporaba meta-analitičnih metod nam poveča verjetnost odkritja pravih vzrokov, ki jih posamezne manjše študije ne zmorejo zaznati. Glavna slabost sistematičnega pregleda literature pa je, da je za tak pregled potrebno veliko več časa in truda kot za tradicionalni pregled literature: potrebno je

namreč točno določiti pogoje iskanja ter različne vključitvene in izključitvene kriterije (Keele, 2007).

Sistematičen pregled literature se od tradicionalnega pregleda literature loči v sledečih točkah:

- Sistematični pregledi se začnejo z definiranjem protokola pregleda, ki določa, na katera raziskovalna vprašanja odgovarjamo in katere metode bodo uporabljene za izvedbo pregleda.
- Sistematični pregledi temeljijo na določeni strategiji iskanja, s katero želimo odkriti čim več relevantne literature.
- Sistematični pregledi dokumentirajo strategijo iskanja, tako da lahko bralci ovrednotijo njihovo temeljitost, popolnost in ponovljivost.
- Sistematični pregledi potrebujejo eksplicitne vključitvene in izključitvene kriterije, s katerimi ocenimo primernost posameznih primarnih raziskav.
- Sistematični pregledi določajo informacije, ki jih pridobimo iz posamezne primarne raziskave, vključno s kriteriji kakovosti, s katerimi ovrednotimo primarne študije.

4.1 Potek sistematičnega pregleda literature

Sistematični pregled literature vključuje več različnih aktivnosti. Obstoječa priporočila se razlikujejo po količini in vrstnem redu izvajanja aktivnosti. Večina se jih strinja z glavnimi fazami, ki so: načrtovanje pregleda, izvajanje pregleda in poročanje o pregledu. Vsaka izmed glavnih faz pa se lahko dalje deli na več aktivnosti:

Načrtovanje pregleda:

- Identificiranje potrebe za pregled
- Naročilo pregleda
- Določanje raziskovalnih vprašanj
- Razvoj načrta pregleda
- Ocenjevanje načrta pregleda

Izvajanje pregleda:

- Identifikacija raziskave
- Izbira primarnih raziskav
- Ocenjevanje kvalitete raziskav

- Pridobivanje podatkov in nadzor
- Sinteza podatkov

Poročanje o pregledu:
- Določanje razširitvenih mehanizmov
- Formatiranje glavnega poročila
- Ocenjevanje poročila

Celotni postopek lahko izvajamo tudi iterativno. To pomeni, da se večina aktivnosti začne izvajati med načrtovanjem pregleda, nato pa se aktivnosti izpopolnijo med dejanskim izvajanjem pregleda (Keele, 2007).

4.1.1 Načrtovanje pregleda

Pri fazi načrtovanja pregleda je najprej potrebno ugotoviti, ali je res potreben pregled. Ko potrdimo potrebo po pregledu, je potrebno določiti raziskovalna vprašanja in pripraviti načrt pregleda.

Identificiranje potrebe za pregled

Potreba po SLR na nekem področju nastane, ko raziskovalci potrebujejo podrobno in nepristransko zbrane vse obstoječe informacije o nekem področju. Zbrani podatki se lahko nato uporabijo zato, da se postavijo bolj temeljiti in boljše podprti zaključki o nekem pojavu, kot pa se lahko določijo na podlagi ene same študije. Pogosto pa se SLR izvede kot osnova za neko nadaljnje delo na določenem področju.

Naročilo pregleda

Aktivnost se po naročilu izvaja zgolj, če organizacija sama nima časa izvajati SLR in zato najame zunanje sodelavce. Zunanjim sodelavcem organizacija preda predlogo SLR, po kateri zunanji sodelavci izvedejo SLR. Predloga vsebuje različne podatke o pregledu, kot so naslov, raziskovalna vprašanja, ozadje, proračun, itd.

Določanje raziskovalnih vprašanj

Aktivnost določanja raziskovalnih vprašanj je najpomembnejša aktivnost vsakega SLR, saj so raziskovalna vprašanja temelj pregleda in vodijo celoten pregled. Raziskovalna vprašanja se s pregledom povezujejo na sledeče načine:

- Proces iskanja mora identificirati primarne študije, ki odgovarjajo na raziskovalna vprašanja.
- Ko iz primarnih študij izvlečemo podatke, morajo ti podatki odgovarjati na raziskovalna vprašanja.
- Sinteza podatkov mora združiti podatke tako, da lahko na njeni podlagi odgovorimo na raziskovalna vprašanja.

Za določitev raziskovalnih vprašanj se lahko opremo na PICOC kriterij (angl. *Population, Intervention, Comparison, Outcome, Context*), pri čemer je ta kriterij v kontekstu programskega inženirstva.

Populacija se torej lahko nanaša na kriterije naše raziskave, ki predstavljajo predmet naše raziskave. Raziskava je lahko usmerjena na zelo določen profil, npr. na določeno vlogo (tester, nadzornik), določeno kategorijo ljudi (novinec ali izkušen), področje uporabe (IT sistemi ali nadzorni sistemi) ali del industrije (srednje velika IT podjetja).

Izvedba se nanaša na metodologijo, tehnologijo, orodje ali postopek, ki naslavlja določen problem.

Primerjava se nanaša na metodologijo, tehnologijo, orodje ali postopek, s katerim je posredovanje primerjano.

Rezultati se nanašajo na dejavnike, ki jih zaznamo kot pomembne pri uporabnikih, kot sta zanesljivost in uporabnost.

Kontekst pa se nanaša na ozadje, v katerem se je raziskava izvedla. Ozadje se nanaša na okolje (akademsko ali industrijsko), udeležence (študenti ali delavci) in na opravila, ki se izvajajo.

Razvoj načrta pregleda

Načrt pregleda določa metode, ki bodo uporabljene za izvedbo SLR. Vnaprej določen načrt je potreben zato, da se zmanjša možnost pristranskosti izvajalca. Načrt je sestavljen iz elementov pregleda in načrtovanja, kot so ozadje, raziskovalna vprašanja, strategija iskanja, kriteriji za izbor raziskav, postopki izbora raziskav, postopki in kontrolni seznam kvalitete raziskav, strategija pridobivanja podatkov iz raziskav, sinteza dobljenih podatkov, strategija razširitve podatkov in časovni načrt izvajanja SLR.

Ocenjevanje načrta pregleda

Načrt je kritičen del vsakega pregleda, zato je pomembno, da se raziskovalci strinjajo na postopku za ocenjevanje načrta. Če obstaja ta možnost (primerna sredstva), je celo optimalno, da se načrt da zunanjim strokovnjakom v pregled, ki lahko kasneje tudi pregledajo končno poročilo. Za ocenjevanje načrta se lahko uporabijo osnovna vprašanja za SLR, kot tudi nekaj dodatnih postavk, kot so:

- Iskalni niz izhaja iz raziskovalnih vprašanj.
- Pridobljeni podatki se primerno nanašajo na raziskovalna vprašanja.
- Postopek analize podatkov je primeren za pridobivanje odgovorov na raziskovalna vprašanja.

Ko torej končamo fazo načrtovanja pregleda, moramo imeti dobro razdelano strategijo pregleda in določena raziskovalna vprašanja (Keele, 2007).

4.1.2 Izvedba pregleda

Ko smo določili načrt pregleda, se lahko dejanski SLR prične, pri čemer je priporočljivo, da raziskovalci poskusijo izvesti vse aktivnosti.

Identifikacija raziskave

Glavni namen SLR je z uporabo nepristranske strategije najti čim več primernih primarnih raziskav, ki se nanašajo na izbrano področje. Strogost in doslednost sta dve lastnosti, ki ločita SLR od klasičnega pregleda literature.

Pri tej prvi aktivnosti izvedbe poskušamo preučiti področje, na katerem želimo izvesti SLR in zagotoviti, da takšne raziskave še ni. To storimo tako, da najprej pripravimo strategijo iskanja. Strategijo iskanja izvajamo iterativno, in sicer s sledečimi postopki:

- Predhodno iskanje, ki je namenjeno temu, da najdemo obstoječe preglede in da pridobimo oceno o številu potencialno primernih raziskavah.
- Poskusna iskanja z različnimi kombinacijami iskalnih pojmov in fraz.
- Primerjanje testnih iskalnih nizov s seznamom že znanih primarnih raziskav.
- Posvet s strokovnjaki iz področja.

Dobra praksa priprave strategije iskanja je, da se raziskovalna vprašanja razčlenijo na manjše dele po kriteriju PICOC, kot smo že omenili. Ko imamo ključne besede, lahko na podlagi le teh pripravimo iskalni niz, kjer ključne besede med seboj povežemo z logičnima izrazoma AND in OR. Začetno iskanje lahko začnemo v digitalni knjižnici, vendar samo to

ne zadostuje za popoln SLR. Dokaze in raziskave je potrebno najti tudi v drugih virih, kot so seznami referenc primarnih virov, različne revije in dnevniki, konferenčni članki, internet ipd.

Pri SLR se je potrebno tudi zavedati pristranskosti publikacij glede na njihovo dosegljivost. To pomeni, da bomo hitreje in lažje zbrali oziroma opazili raziskave, ki imajo pozitiven rezultat, kot pa tiste, ki imajo negativen rezultat. Za zmanjšanje pristranskosti je pametno pregledati tudi sivo literaturo (kjer se nahajajo dela v nastajanju), konferenčne članke, prav tako pa lahko poiščemo in izprašamo tudi strokovnjake.

Sam pregled literature je potrebno tudi ustrezno dokumentirati. Z dobro dokumentacijo pregleda dosežemo transparentnost in ponovljivost pregleda. Dokumentacija mora biti dovolj podrobna, da lahko bralci ocenijo temeljitost pregleda, mora biti točna in jo moramo spreminjati, ko spreminjamo samo raziskavo. Prav tako pa morajo biti nefiltrirani rezultati shranjeni za morebitno ponovno analizo.

Izbira primarnih raziskav

Ko sestavimo seznam potencialno primernih raziskav, je potrebno te raziskave pregledati in oceniti njihovo pomembnost. Pomembnost jim določamo na podlagi vključitvenih in izključitvenih kriterijev. Kriteriji nam pomagajo najti primarne raziskave, ki nam podajo neposredne dokaze o raziskovalnih vprašanjih. Da se zmanjša pristranskost, je priporočljivo, da se kriteriji določijo v fazi načrtovanja, vendar se lahko naknadno preuredijo v fazi izvajanja. Izbor raziskav je večstopenjski proces. V prvi stopnji se kriterijev držimo bolj svobodno; če raziskave eksplicitno ne moremo izključiti glede na povzetek in naslov, jo vključimo in pridobimo celoten tekst. Na področju IT je priporočljivo pregledati tudi zaključek, saj povzetki pogosto kaj pomembnega izpustijo. Naslednja stopnja je uporaba različnih vključitvenih kriterijev glede na praktične izkušnje, kot so jezik, revija, avtor, leto objave, sodelujoči, metoda in podobno. Včasih pa se izvaja tudi tretja stopnja, kjer raziskovalci vključujejo raziskave na podlagi še bolj podrobno razdelanih kriterijev.

Ocenjevanje kvalitete raziskav

Poleg vključitvenih in izključitvenih kriterijev je pomembna določitev »kvalitete« primarnih raziskav, saj nam pomaga pri:

- določanju bolj podrobnih vključitvenih in izključitvenih kriterijev,
- ugotovljanju ali kvaliteta vpliva na različne izide raziskav,
- določanju teže podatkov, pridobljenih iz raziskav pri sintezi podatkov,

- interpretaciji zaključkov in
- izdelavi priporočil za nadaljnje raziskave.

Težava pri tem je, da ne obstaja enoten kriterij kvalitete pri raziskavah. Da lahko ocenimo kvaliteto raziskav, je potrebno pripraviti kvalitetne inštrumente, ki so seznami faktorjev, katere moramo oceniti za vsako raziskavo. Seznami so po navadi izpeljani iz množice faktorjev, ki bi lahko ogrozili nepristranskost raziskave. Velikokrat se ponavljajo štiri skupine pristranskosti: pristranskost izbire, pristranskost izvedbe, pristranskost meritve in pristranskost izključitve. Te faktorje lahko predelamo in tako dobimo kvaliteten inštrument, ki vsebuje dve skupini faktorjev: splošne in specifične. Splošni faktorji se nanašajo na lastnosti metode dela v določeni raziskavi, specifični faktorji pa se nanašajo na področje raziskave.

Seznami so sestavljeni tudi s premislekom o pristranskostih in problemih veljavnosti, ki lahko nastanejo v različnih fazah empirične raziskave (pri načrtovanju, izvedbi, analizi in zaključku). Posledično obstaja veliko različnih seznamov kvalitete za različne tipe empiričnih raziskav, težava pa je v tem, da se seznami med seboj razlikujejo in ni dogovorjenega enotnega nabora vprašanj. Ko si raziskovalci enkrat pripravijo seznam kvalitete, je potrebno določiti še, kje in kako bo uporabljen. Lahko je uporabljen za pomoč pri izbiri primarnih raziskav ali pa za pomoč pri analizi in sintezi podatkov. Pomanjkljivost ocenjevanja kvalitete je, da so lahko raziskave tudi slabo opisane in torej ne vsebujejo vseh podatkov, ki jih potrebujemo za oceno kvalitete: čeprav je nekaj mogoče bilo izvedeno v raziskavi, ni opisano v samem članku.

Pridobivanje podatkov

Namen te aktivnosti je, da se načrtuje način pridobivanja podatkov iz raziskav in da se pripravi obrazce za zapisovanje pridobljenih podatkov. Da se zmanjša vpliv pristranskosti, se priporoča, da se obrazci določijo, ko se določi protokol izvedbe SLR. Obrazci za pridobivanje podatkov morajo biti oblikovani tako, da zajemajo vse podatke, ki so potrebni za odgovarjanje na raziskovalna vprašanja in vprašanja o kvaliteti raziskave. Obrazci po navadi zajamejo nekaj splošnih informacij, kot so ime izvajalca, datum pridobivanja podatkov, naslov raziskave, avtorji ipd., kot tudi vse podatke, ki jih potrebujemo za odgovore na raziskovalna vprašanja.

Postopek pridobivanja podatkov je priporočljivo izvesti s strani dveh ali več raziskovalcev. Kasneje se podatki primerjajo, morebitni nesporazumi pa se morajo razrešiti. Za primere, kjer to ni mogoče (je le en raziskovalec), se uporabijo druge tehnike preverjanja.

Ena izmed pomembnejših stvari, na katere moramo biti pozorni pri SLR, je podvajanje publikacij istih podatkov, saj bi le to resno ogrozilo nepristranskost rezultatov. V primeru podvajanj je potrebno pri avtorjih preveriti, ali gre dejansko za iste raziskave. Če gre dejansko za dvojnike, je najboljša izbira uporaba najbolj dodelane raziskave.

Sinteza podatkov

Sinteza podatkov predstavlja primerjanje in povzetek rezultatov primarnih raziskav. Sinteza je lahko kvantitativna ali opisna, lahko pa je tudi oboje. Kvantitativno sintezo lahko izvedemo s statističnimi tehnikami, kar poimenujemo meta-analiza. Način in aktivnosti sinteze se predvidoma zapišejo v strategijo izvajanja pregleda.

Pri opisni sintezi je priporočljivo, da se podatki, pridobljeni iz raziskav, zapišejo v tabelo tako, da se upoštevajo raziskovalna vprašanja. Tabela naj bo pripravljena tako, da se poudarjajo razlike in podobnosti med rezultati raziskav, saj je pomembno, da ugotovimo, ali so rezultati dosledni ali ne.

Pri kvantitativni sintezi je prav tako priporočljivo rezultate zapisati v tabelo, pri čemer se po navadi zapisujejo (i) podatki o velikosti vzorca za posamezno izvedbo, (ii) ocena velikosti učinka za vsako izvedbo s standardno napako učinka, (iii) razlika med povprečji vsake izvedbe in (iv) enote, uporabljene za merjenje učinka. Da lahko različne raziskave primerjamo med seboj, morajo biti rezultati raziskav predstavljeni na primerljiv način. Za primerljivost se glede na število možnih rezultatov uvedejo različne spremenljivke. Če imamo dva možna rezultata, se lahko uvede razmerje, tveganje, razmernostno tveganje, relativno tveganje ali pa absolutno zmanjšanje tveganja. Če imamo več možnih rezultatov, se lahko uvede razlika povprečja, obtežena razlika povprečja ali standardizirana razlika povprečja. Vsako od teh ima svoje prednosti in slabost, zato mora izvajalec SLR pretehtati in določiti, katera je najbolj ustrezna za njegov pregled.

Pri kvalitativni sintezi poskušamo integrirati raziskave, ki so sestavljene iz rezultatov in zaključkov v naravnem jeziku. Težava lahko nastane, ko različni raziskovalci v rahlo različnih pomenih uporabljajo določene besede.

Če pa se raziskovalci ukvarjajo s pregledom, ki vsebuje tako kvantitativne kot kvalitativne raziskave, je potrebno sintetizirati kvantitativne in kvalitativne raziskave posebej, šele nato lahko poskusimo integrirati rezultate skupaj, tako, da se s pomočjo kvalitativnih razložijo kvantitativne (Keele, 2007).

4.1.3 Poročanje o pregledu

Zadnja faza pregleda vključuje popis dobljenih rezultatov pregleda in razširitev teh rezultatov vsem potencialnim interesentom.

Določanje razširitvenih mehanizmov

Rezultate SLR je potrebno razširiti učinkovito, zato večina smernic priporoča načrtovanje razširjanja rezultatov že v fazi načrtovanja. Najbolj razširjen način širjenja rezultatov je objava v reviji ali v konferenčnem zborniku. Vendar so v določenih primerih (npr. kadar želimo vplivati na ljudi, ki so v stiku s področjem, ki smo ga raziskovali) potrebni tudi drugi načini širjenja: revije za izvajalce, izjave za javnost, kratki informativni letaki, posterji, spletne strani in neposredna komunikacija.

Formatiranje glavnega poročila

Po navadi so SLR predstavljeni v dveh oblikah: v tehničnem poročilu ali delu raziskovalnega dela (magistrsko delo ali doktorat) ter v reviji ali konferenčnem zborniku.

Zaradi omejitve glede dolžine, ki jo imajo revije in zborniki, morajo avtorji določene dele pregleda pogosto izpustiti. Posledično lahko pride do težav, ko želijo bralci oceniti temeljitost pregleda. Zato je priporočljivo, da avtorji v članku podajo referenco na tehnično poročilo, ki vsebuje vse podatke.

Ocenjevanje poročila

Ocenjevanje poročila je potrebno zato, da se zagotovi njegovo visoko kvaliteto. Določeni tipi publikacij imajo že ustaljene postopke ocenjevanja (recenzija članka ali pregled magistrske oziroma doktorske disertacije s strani strokovnjakov). Tehnična poročila pa nimajo ustaljenega postopka ocenjevanja, zato je priporočljivo, da nam kolegi ocenijo poročilo, preden rezultate prestavimo javnosti (Keele, 2007).

5 SISTEMATIČNI PREGLED LITERATURE OVERITVENIH PROTOKOLOV

V predhodnem poglavju smo teoretično opisali metodo dela, ki smo jo uporabili – sistematični pregled literature. Namen SLR je poiskati vse relevantne raziskave na področju overitvenih protokolov, odgovoriti na raziskovalna vprašanja ter pridobiti temeljno znanje o overitvenih protokolih. Kot rezultat pregleda pa želimo izdelati tudi klasifikacijo overitvenih protokolov. Ker je bil SLR izveden z zgolj enim raziskovalcem, je tudi postopek SLR prilagojen za eno osebo. Sledi opis izvedenih faz in opis izvedbe sistematičnega pregleda literature.

5.1 Faza načrtovanja

Identificiranje potrebe za pregled

Prva aktivnost faze načrtovanja je identifikacija potreb za izvajanje SLR. To pomeni, da je bilo potrebno ugotoviti, kakšni so cilji SLR, in preveriti, ali že obstaja takšen pregled. Preiskali smo baze ScienceDirect, IEEExplore ter SpringerLink in nismo našli literature, ki bi vsebovala ključno besedo sistematični pregled literature s področja overitvenih protokolov. Iskalni niz, ki smo ga uporabili za iskanje podobnih raziskav, je bil:

("authentication" OR "authentication protocols" OR "authenticated key agreement"
OR "authentication and key agreement")
AND
("systematic literature review" OR "systematic review" OR
"systematic survey" OR "systematic research")

Rezultatov, ki so bili vrnjeni na podlagi tega iskalnega niza, je bilo 374, od tega na ScienceDirect 185, na SpringerLink 185 in na IEEExplore 4. Od tega jih je nekaj imelo v naslovu oziroma ključnih besedah izraz "sistematični pregled literature", vendar smo po pregledu ugotovili, da gre za raziskave na drugih področjih. Dejstvo, da nismo našli raziskave, nam potrjuje, da naša raziskava še ni bila izvedena in da jo lahko izvedemo mi.

Naročilo pregleda

To opcijsko aktivnost smo izpustili, saj smo SLR izvedli sami in ne zunanja skupina raziskovalcev.

Določitev raziskovalnih vprašanj

Kot smo že opisali v teoretičnem pregledu metode, so dobro zastavljena raziskovalna vprašanja bistvenega pomena za raziskavo. S kriterijem PICOC, ki je prikazan v tabeli 5.1, smo si pomagali pri pripravi raziskovalnih vprašanj.

Tabela 5.1 PICOC kriterij

Populacija	*Overitveni protokoli*
Izvedba	*Varnostne zahteve in znani napadi*
Primerjava	*/*
Rezultat	*Pregled overitvenega protokola*
Kontekst	*Pregled overitvenih protokolov, njihovih znanih napadov in varnostnih zahtev*

Sledeča pa so naša raziskovalna vprašanja:

- RV1: Kako število faktorjev overitvenih protokolov vpliva na njihove varnostne zahteve in ranljivosti?
- RV2: Kateri razredi oziroma skupine overitvenih protokolov obstajajo?
- RV3: Katera izmed skupin overitvenih protokolov v povprečju izkazuje manj varnostnih pomanjkljivosti in je posledično podvržena manj napadom?
- RV4: Ali obstaja klasifikacija napadov na overitvene protokole?
- RV5: Katere kriterije je treba upoštevati pri snovanju overitvenega protokola?

Razvoj načrta pregleda

Razvoj načrta pregleda je pomemben del faze načrtovanja, saj je potrebno pred izvedbo SLR določiti načrt dela. S tem se zagotovi ponovljivost SLR in zmanjša pristranskost, kar je v našem primeru bistvenega pomena, saj SLR izvaja zgolj en raziskovalec.

Ozadje pregleda

Število overitvenih protokolov se vztrajno veča, s tem pa se veča tudi njihova nepreglednost. Prav tako se odkrivajo nove ranljivosti in pomanjkljivosti teh protokolov, ki jih nadgradnje morda spregledajo in jih zato ne odpravijo z novo verzijo. Zaradi teh razlogov želimo izvesti sistematični pregled literature in pripraviti klasifikacijo overitvenih protokolov z namenom smiselne kategorizacije posamezne varnostne zahteve in znanih napadov na overitvene protokole. S tem bi pomagali načrtovalcem novih overitvenih protokolov, da bi na enem mestu imeli zbrane podatke o tem, na katere lastnosti in ranljivosti morajo biti posebej pozorni pri načrtovanju novega protokola. Prav tako želimo s sistematičnim pregledom literature pridobiti osnovno znanje in pregled nad overitvenimi protokoli in njihovimi varnostnimi zahtevami ter ranljivostmi.

Raziskovalna vprašanja

Raziskovalna vprašanja smo definirali v prejšnjem poglavju, na njihovi podlagi pa smo pripravili iskalni niz, ki je sledeč:

("authentication" OR "authenticated key agreement"
OR "authentication and key agreement")
AND ("security properties" OR "known attacks" OR "security attributes")
AND ("survey" OR "overview" OR "cryptanalysis" OR "review")

Iskalni niz bomo nato uporabili v treh digitalnih knjižnicah: ScienceDirect, SpringerLink in IEEExplore.

Vključitveni in izključitveni kriteriji

Za vključevanje in izključevanje raziskav v seznam primarnih raziskav bomo uporabili različne kriterije, ki bodo določili, ali je neka raziskava primerna za naš pregled ali ne. Kriterije bomo uporabili nad meta podatki (naslov, podatki o avtorju, datum objave, revija itd.), nad povzetkom in zaključkom, po potrebi pa še nad celotno vsebino. Vključitveni/izključitveni kriteriji, na podlagi katerih bomo izbirali primarne raziskave, so:

- Raziskave v angleškem jeziku.
- Raziskave v obliki članka.
- Raziskave na področju računalništva in informacijskih tehnologij.
- Raziskave, ki opisujejo overitvene protokole.
- Raziskave, ki prikazujejo varnostne pomanjkljivosti overitvenih protokolov.

- Raziskave, ki izvajajo preglede nad overitvenimi protokoli.
- Kriptoanalize overitvenih protokolov.
- Raziskave, ki opisujejo varnostne zahteve overitvenih protokolov.
- Raziskave, ki so bile objavljene med leti 2010 in 2015.
- Raziskave, do katerih imamo dostop preko omrežja UM.

Postopek izbora raziskav

Izbira primarnih raziskav bo potekala tako, da bomo vse rezultate prenesli na računalnik naenkrat, da ne pride do razlik v rezultatih iskanja, šele nato bomo izbrali primerne raziskave. Primarne raziskave bomo izbrali tako, da bomo najprej izbrali ustrezne na podlagi naslova, v primeru da naslov ni ustrezen, pa bomo pregledali še povzetek, uvod in zaključek. Če raziskava nikjer ne ustreza vključitvenim kriterijem, bomo raziskavo zavrnili.

Postopek in kontrolni seznam kvalitete raziskav

V našem primeru gre za SLR, s katerim želimo pridobiti čim bolj širok pregled nad vsemi overitvenimi protokoli, prav tako pa uporabljamo baze kvalitetnih člankov in zato zaupamo v postopke revizije raziskav. Zaradi teh prepričanj bomo obravnavali vse podatke enakovredno in posledično ne bomo ocenjevali kvalitete raziskav.

Strategija pridobivanja podatkov iz raziskav

Podatke bomo iz raziskav pridobivali tako, da bo raziskovalec prebral najprej naslov, povzetek, uvod in zaključek, nato pa bo preletel še celoten članek in bil pri tem pozoren na sledeče stvari:

1.) Za kateri overitven protokol gre (naziv)?
2.) V katero skupino overitvenih protokolov spada?
3.) Pred katerimi znanimi napadi je protokol varen?
4.) Kakšne so varnostne zahteve protokola?
5.) Katere so varnostne ranljivosti protokola?
6.) V katerem področju se uporablja protokol?
7.) Koliko faktorjev ima overitven protokol?

Za lažje pridobivanje podatkov iz raziskav smo pripravili tabelo 5.2, ki jo bo raziskovalec izpolnjeval, kar bo hkrati olajšalo tudi analizo dobljenih podatkov.

Tabela 5.2 Obrazec za izpis podatkov

Podatek	***Vrednost***
Naslov članka	*Izpisan naslov članka*
Naziv protokola	*Izpisan naziv oziroma identifikator protokola*
Skupina protokolov	*Izpisana skupina, v katero spada protokol. V primeru, da skupina ni izpisana, raziskovalec sam dodeli skupino*
Varno pred napadi	*Izpisani napadi, pred katerimi je protokol varen*
Izpolnjene varnostne zahteve	*Izpisane izpolnjene varnostne zahteve protokola*
Varnostne ranljivosti (znani napadi)	*Izpisane ranljivosti (znani napadi protokola in neizpolnjene zahteve)*
Področje uporabe protokola	*Izpisana tehnologija oziroma področje, na katerem se protokol uporablja*
Število faktorjev protokola	*Izpisano število faktorjev overitvenega protokola*

Sinteza dobljenih podatkov

Sinteza podatkov bo potekala tako, da bomo pregledali vse zbrane podatke in jih povezali s tem, da bomo iskali ponavljanja v vseh tabelah. Nato pa bomo rezultate predstavili v analizi in na koncu pripravili priporočila za snovalce novih protokolov.

Strategija razširitve podatkov

Rezultate našega pregleda bomo objavili kot magistrsko delo v digitalni knjižnici Univerze v Mariboru.

Časovni načrt izvajanja pregleda

Časovni načrt izvajanja sistematičnega pregleda literature smo pripravili glede na oceno, da za vsako fazo ne bi smeli potrebovati več kot dva tedna dela. Ker SLR obsega fazo načrtovanja, fazo izvedbe in fazo poročanja, časovni načrt za celoten pregled obsega šest tednov dela.

S tem smo končali fazo načrtovanja, naslednja faza je izvedba SLR.

5.2 Faza izvedbe

Ko smo zaključili fazo načrtovanja SLR, smo se lotili izvedbe. Kot smo že omenili v teoretičnem pregledu metode SLR, faza izvedbe vsebuje naslednje aktivnosti: identifikacijo raziskave, izbiro primarnih raziskav, ocenjevanje kvalitete raziskav, pridobivanje podatkov in sintezo podatkov.

Identifikacija raziskave

Preliminarno iskanje smo izvedli že v času načrtovanja pregleda in z njim preizkusili nekaj različnih iskalnih nizov. Po premisleku smo uporabili tistega, ki je zapisan v načrtu SLR. Iskalni niz smo uporabili v digitalnih knjižnicah ScienceDirect, SpringerLink in IEEExplore. Za vsako bazo bomo opisali postopek iskanja.

Prvo iskanje smo izvedli v bazi ScienceDirect, kjer smo izbrali opcijo iskanja za strokovnjake, ki omogoča vnos lastnega iskalnega niza. Ko smo vpisali niz, smo označili opcijo iskanja člankov ter iskanje od leta 2010 naprej.

Sledilo je iskanje v bazi SpringerLink, kjer smo iskalni niz vpisali v iskalnik in nato postopoma aplicirali filtre. Izbrali smo, da ne želimo rezultatov, kjer je možen samo pregled, da želimo samo članke, da so članki na področju računalništva in da so bili članki izdani med leti 2010 in 2015.

Nazadnje smo iskali še v bazi IEEExplore, kjer smo izbrali opcijo naprednega iskanja z nizom. Nato smo vpisali iskalni niz in dodali časovni filter. Končni rezultati iskanja so zapisani v tabeli 5.3.

Tabela 5.3 Rezultati iskanja

Baza	Datum	Število zadetkov
ScienceDirect	03.08.2015	516
SpringerLink	03.08.2015	371
IEEExplore	03.08.2015	9

Izbira primarnih raziskav

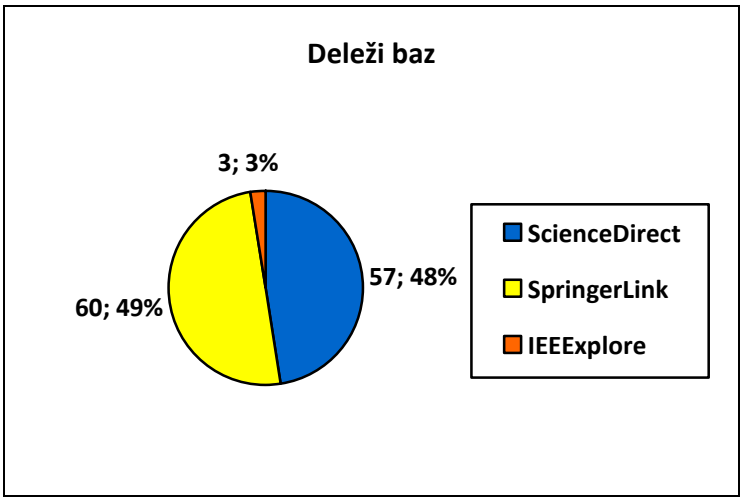
Ker je iskanje vrnilo tudi nekatere raziskave, ki se ne nanašajo na želeno področje, smo morali preveriti njihovo primernost. Primernost smo preverjali v dveh stopnjah. V prvi stopnji smo ločili neprimerne in primerne raziskave tako, da smo pregledovali, ali se

raziskave vsaj ohlapno nanašajo na overitev in overitvene protokole. Tako smo pridobili seznam potencialnih primarnih raziskav, ki je obsegal 195 raziskav iz baze ScienceDirect, 165 raziskav iz baze SpringerLink in 7 raziskav iz baze IEEExplore. Te potencialne primarne raziskave smo nato še podrobneje pregledali in ugotavljali, ali raziskave obravnavajo temo overitvenih protokolov. Rezultati izbire primarnih raziskav so predstavljeni v tabeli 5.4.

Tabela 5.4 Število primernih primarnih raziskav

Baza	Število zadetkov	Število potencialnih primarnih raziskav	Število primarnih raziskav
ScienceDirect	516	195	57
SpringerLink	371	165	60
IEEExplore	9	7	3
Skupaj rezultatov	**896**	**367**	**120**

Skupno smo torej kot primerne ocenili 120 raziskav, od tega 57 iz baze ScienceDirect, 60 iz baze SpringerLink in 3 iz baze IEEExplore. Odstotki zastopanosti baz, iz katerih so bili pridobljeni viri, so prikazani na sliki 5.1.



Slika 5.1 Deleži ocen vseh raziskav

Pridobivanje podatkov

Po izboru primarnih raziskav, ki naj jih SLR zajema, smo s pomočjo tabele za pridobivanje podatkov iz vsake raziskave poskušali pridobiti podatke, ki smo jih potrebovali. Vsi pridobljeni podatki so zajeti v prilogi B.

Za lažji končni pregled smo uporabili dodatne tabele, kamor smo zapisovali protokole, znane napade in varnostne zahteve, v glavno tabelo pa smo zaradi boljšega pregleda in sinteze zapisovali zgolj identifikatorje. Samo pridobivanje podatkov je potekalo tako, da smo v članku poiskali vse overitvene protokole, o katerih je avtor pisal, vse njihove ranljivosti in prednosti. Pridobljene podatke smo sproti beležili v glavno tabelo. Kadar smo se srečali z že obstoječim protokolom, smo dodali podatke, če pa smo se v raziskavi srečali z novim protokolom, novim znanim napadom ali novo varnostno zahtevo, smo dodali nov vnos v ustrezno tabelo. Primer pridobivanja podatkov je v tabeli 5.5.

Tabela 5.5 Primer pridobivanja podatkov

ID raziskave	PR22
Naziv protokola	P51
Skupina protokola	authentication
Varno pred napadi	N06, N08, N09, N13, N21
Izpolnjene varnostne zahteve	Z05, Z15
Področje uporabe protokola	Brezžično senzorsko omrežje
Varnostne ranljivosti	N22, N23, N24, Z03, Z10
Število stopenj	1

V tabeli 5.6 pa imamo prikazan primer pomožne tabele, ki vsebuje samo sezname parov identifikator-celoten naziv. Celotna tabela vseh protokolov je v prilogi A, tabeli napadov in zahtev pa se nahajata pod zaporedno številko 5.7 in 5.8.

Tabela 5.6 Izsek iz pomožne tabele

ID	**Naziv protokola/napada/zahteve**
P51	Yoo et al.'s security-performance-balanced user authentication scheme for wireless sensor networks
P52	Sun et. Al.'s security and improvement of a two-factor user authentication scheme in wireless sensor networks

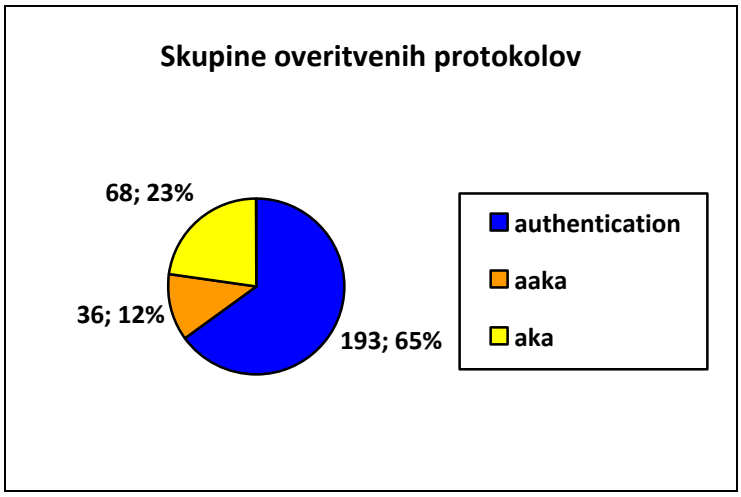
Sinteza podatkov

Ko smo imeli vse podatke zbrane v tabelah, smo lahko pričeli z analizo in sintezo podatkov. Z analizo in sintezo podatkov smo želeli pridobiti odgovore na raziskovalna vprašanja, prav tako pa smo poskušali pridobiti osnovni pregled nad overitvenimi protokoli. S pomočjo zbranih in analiziranih podatkov smo sproti pripravljali klasifikacijo overitvenih protokolov, s pomočjo katere smo pripravili priporočila za snovanje novih overitvenih protokolov.

Kakšni tipi overitvenih protokolov obstajajo? Za potrebe tega raziskovalnega vprašanja smo v tabeli za pridobivanje podatkov namenili vrstico, kamor smo vpisovali tip oziroma skupino overitvenega protokola. Skupno smo zaznali tri glavne tipe overitvenih protokolov:

- Overitev (angl. *authentication*)
- Overitev in dogovor o ključu (angl. *authentication and key agreement*)
- Dogovor o overjenem ključu (angl. *authenticated key agreement*)

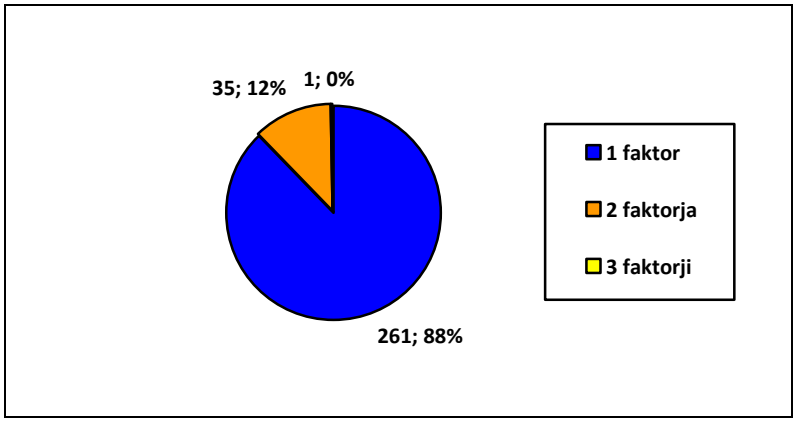
V tabeli rezultatov smo overitev označevali z »*authentication*«, overitev in dogovor o ključu z »*aaka*« in dogovor o overjenem ključu »*aka*«. Na sliki 5.2 imamo prikazano, v kakšnem deležu se pojavlja posamezna skupina. Od skupno 297 različnih protokolov, ki smo jih zabeležili, v skupino overitev sodi 193 protokolov, v skupino overitev in dogovor o ključu 36 protokolov ter v skupino dogovor o overjenem ključu 68 protokolov. Največ protokolov je v skupini *overitev*, verjetno zato, ker so najpreprostejše sheme izmed vseh treh.



Slika 5.2 Deleži skupin overitvenih protokolov

Druga stvar, ki smo jo pregledovali, je bilo število faktorjev posameznega protokola. Pri tem smo odkrili, da je od skupno 297 protokolov 261 protokolov z enim faktorjem

overjanja, 35 protokolov z dvema faktorjema overjanja in 1 protokol s tremi faktorji overjanja. Deleži so prikazani na sliki 5.3.

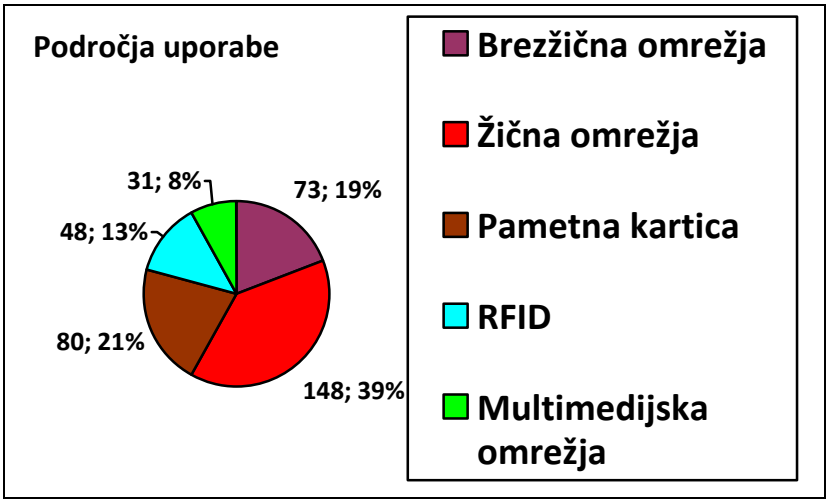


Slika 5.3 Deleži protokolov glede na število faktorjev

Tretja stvar, ki nas je zanimala, je bila tehnologija oziroma področje, na katerem se uporablja določen overitveni protokol. Tukaj je bilo več razlikovanja v odgovorih, saj se overitveni protokoli uporabljajo v najrazličnejših tehnologijah, shemah in omrežjih ter uporabljajo različne mehanizme. Področja, ki smo jih zasledili:

- *Brezžična omrežja*: tukaj so se pojavljale različne vrste omrežij, kot so brezžično zankasto omrežje (angl. *wireless mesh network*), brezžično senzorsko omrežje (angl. *wireless sensor network*), navadna brezžična omrežja, kot tudi mobilna omrežja
- *Multimedijska omrežja*: tukaj sta se pojavila internetna telefonija (angl. *VoIP - voice over IP*) in protokol za vzpostavitev seje (angl. *SIP - session initiation protocol*)
- *Žična omrežja*: tukaj so se pojavljala klasična omrežja strežnik-odjemalec, odjemalec-odjemalec, okolja z več strežniki ipd.
- *RFID* (angl*. radio frequency identification*)
- *Pametna kartica* (angl. *smart card*)

Nekateri protokoli delujejo na več področjih, tako da je vseh podatkov skupno več kot 297. Največja skupina je skupina *žična omrežja* s 148 primerki, nato je skupina *pametna kartica* z 80 primerki, sledi skupina *brezžična omrežja* s 73 primerki, sledi skupina *RFID* z 48 primerki in na koncu še skupina *multimedijska omrežja* z 31 primerki. Deleži so prikazani na sliki 5.4.



Slika 5.4 Področja uporabe overitvenih protokolov

Nadalje smo obravnavali varnostne zahteve overitvenih protokolov. Po pregledu raziskav smo zabeležili sledeče zahteve: varnost pred limanico, varnost shrambe, anonimnost, nepovezljivost, vzajemna overitev, varnost poznanega ključa, popolna prihodnja varnost, varnost sejnega ključa, tajnost poznanega ključa, tajnost sejnega ključa, privatnost značke, anonimnost značke, brez verifikacijske tabele, privatnost bralca, dogovor o ključu, zaščita gesla, nedavnost ključa, razpoložljivost, skalabilnost in brez kontrole ključa.

V tabeli 5.7 so zapisani podatki o tem, kolikokrat se je posamezna zahteva pojavila. Modro obarvana polja označujejo zahteve Z12, Z13, Z16, Z23 in Z24, ki zadevajo zgolj določeno skupino protokolov, in sicer tiste, ki delujejo v področju RFID (teh je 48). Iz tabele je razvidno, da nobena zahteva ne prevladuje pri vseh protokolih, kar pomeni, da si avtorji zelo različno izbirajo zahteve, ki naj bi jih njihov protokol izpolnjeval. Največ se pojavlja vzajemna overitev, pa še to zgolj v 63 %.

Tabela 5.7 Seznam zahtev in njihovih pojavitev

ID	Naziv zahteve	Pojavov	Odstotek	Izpolnjena zahteva	Ranljivost
Z01	varnost pred limanico	1	0 %	1	0
Z02	varnost shrambe	1	0 %	1	0
Z03	anonimnost	145	49 %	71	74
Z04	nepovezljivost	8	3 %	4	4

Z05	vzajemna overitev	188	63 %	152	36
Z06	varnost poznanega ključa	43	14 %	37	6
Z07	popolna prihodnja varnost	163	55 %	115	48
Z08	varnost sejnega ključa	69	23 %	49	20
Z09	tajnost poznanega ključa	12	4 %	11	1
Z11	tajnost sejnega ključa	6	2 %	4	2
Z12	privatnost značke	16	33 %	9	7
Z13	anonimnost značke	17	35 %	14	3
Z14	brez verifikacijske tabele	27	9 %	25	2
Z16	privatnost bralca	1	2 %	1	0
Z17	dogovor o ključu	11	4 %	8	3
Z18	zaščita gesla	2	1 %	2	0
Z22	nedavnost ključa	2	1 %	2	0
Z23	razpoložljivost	10	21 %	6	4
Z24	skalabilnost	5	10 %	1	4
Z26	brez kontrole ključa	18	6 %	18	0

Potem smo se lotili preverjanja napadov na protokole. Iz pregleda raziskav smo izpisali napade, predstavljene v tabeli 5.8.

Tudi v tem primeru smo prešteli, kolikokrat se posamezen napad pojavlja, in izračunali, v kakšnem deležu od vseh 297 protokolov se pojavlja. Ponovno so posebnost modro obarvane vrstice, ki označujejo napade, ki so možni zgolj na določeno skupino protokolov. Tako je pri napadu N15 skupno 80 protokolov, ki delujejo na področju pametnih kartic, pri napadih N19, N23 in N27 pa gre za protokole, ki delujejo na področju senzorskih omrežij, skupno jih je 22. Prav tako so v tabeli 5.8 prikazani podatki za število pojavitev napada, število pojavitev kot zahteva in kot ranljivost.

Tabela 5.8 Seznam napadov in njihovih pojavitev

ID	Naziv	Pojavov	Odstotek	Varen pred	Ranljivost
N1	Nepovezan napad ugibanja identitete	7	2 %	4	3
N2	Nepovezan napad ugibanja	159	54 %	92	67

	gesla				
N3	Strežniški maškaradni napad	71	24 %	44	27
N4	Napad poosebljanja	226	76 %	136	90
N5	Napad ponovitve	196	66 %	158	38
N6	Napad modifikacije	45	15 %	39	6
N7	Napad ukradenega verifikatorja	90	30 %	75	15
N8	Napad vrinjene osebe	109	37 %	73	36
N9	Napad prisluškovanja	13	4 %	12	1
N10	Povezan napad ugibanja gesla	26	9 %	14	12
N11	Napad s poznanim sejnim ključem	36	12 %	33	3
N12	Napad odseva	29	10 %	22	7
N13	Napad desinhronizacije	99	33 %	59	40
N14	Napad notranje osebe	127	43 %	63	64
N15	Napad ukradene pametne kartice	74	93 %	47	27
N16	Napad ugibanja identitete	5	2 %	1	4
N17	Napad sledenja	5	2 %	1	4
N18	Napad vzporedne seje	34	11 %	18	16
N19	Napad obhoda prehodnega vozlišča	10	46 %	3	7
N20	Denning-Sacco napad	26	9 %	20	6
N21	Napad ukradene identitete	7	2 %	2	5
N22	Napad poosebljanja ključa	6	2 %	3	3
N23	Napad poosebljanja senzorskega vozlišča	5	23 %	3	2
N24	Napad več vpisanih oseb z istim identifikatorjem	12	4 %	7	5
N25	Napad repliciranja ključa	19	6 %	4	15
N26	Napad specifičnega znanja seje	25	8 %	19	6
N27	Napad ugrabljanja vozlišča	9	41 %	4	5

Če izvzamemo napade, ki so specifični za določeno skupino protokolov (N15, N19, N23 IN N27), lahko ugotovimo, da je večina napadov slabo zastopana v analizah, največji odstotek je 76 %, kar je več od odstotka najbolj prisotne varnostne zahteve, vendar so napadi v splošnem prisotni v premajhnih odstotkih. Razlog za takšen odstotek je ponovno v tem, da ne obstaja enoten seznam napadov, ki naj bi jih razvijalci preverili.

5.3 Odgovori na raziskovalna vprašanja

- RV1: Kako vpliva število faktorjev overitvenih protokolov na njihove varnostne zahteve in ranljivosti?

Da smo lahko odgovorili na prvo raziskovalno vprašanje, smo iz podatkov prešteli število izpolnjenih zahtev in ranljivosti za vsak protokol. Te podatke smo nato ločili glede na število faktorjev posameznega protokola (1 faktor oziroma več faktorjev) in na koncu izračunali povprečne vrednosti izpolnjenih zahtev in ranljivosti za vsako skupino posebej. Vrednosti so prikazane v tabeli 5.9.

Tabela 5.9 Analiza varnosti protokolov glede na faktorje

Skupina protokolov	Povprečje izpolnjenih zahtev	Povprečje ranljivosti	Razlika
Protokoli z enim faktorjem	4.9	2.4	2.5
Protokoli z več faktorji	6.3	3.7	2.6

Kot lahko vidimo iz tabele, imajo protokoli z več faktorji v povprečju več izpolnjenih zahtev z 6.3 izpolnjenimi zahtevami proti 4.9 izpolnjenim zahtevam protokolov z enim faktorjem. Vendar imajo tudi večje število ranljivosti, saj imajo povprečno kar 3.7 ranljivosti proti 2.4 ranljivosti protokolov z enim faktorjem. Kar pomeni, da je končna razlika 0.1 povprečne točke minimalna, zato tudi ne moremo z gotovostjo trditi, da ima več faktorjev kakšen vpliv na večjo varnost protokola.

- RV2: Kateri razredi / skupine overitvenih protokolov obstajajo?

Med izvajanjem pregleda smo izluščili tri skupine oziroma razrede overitvenih protokolov, ki so zastopane v naši bazi člankov, in sicer so to (i) overitev, (ii) overitev in dogovor o ključu in (iii) dogovor o overjenem ključu.

- RV3: Katera izmed skupin overitvenih protokolov v povprečju izkazuje manj varnostnih pomanjkljivosti in posledično manj napadov?

Podatki o napakah so zbrani v tabeli 5.10, kjer imamo povprečno število izpolnjenih zahtev in odpornosti na napade, povprečno število ranljivosti in razliko med tema dvema številoma. Večja kot je pozitivna razlika, varnejša je skupina.

Tabela 5.10 Analiza varnosti skupin overitvenih protokolov

Skupina protokolov	Povprečje izpolnjenih zahtev	Povprečje ranljivosti	Razlika
Overitev	5.0	2.6	2.4
Overitev in dogovor o ključu	5.9	1.6	4.3
Dogovor o overjenem ključu	4.6	2.8	1.8

Iz tabele lahko vidimo, da ima v povprečju največ izpolnjenih zahtev in odpornosti na napade skupina overitev in dogovor o ključu s 5.9 izpolnjenimi zahtevami, druga največ jih ima skupina overitev s 5.0 izpolnjenimi zahtevami, najmanj pa skupina dogovor o overjenem ključu s 4.6 izpolnjenimi zahtevami. Prav tako ima v povprečju najmanj ranljivosti skupina overitev in dogovor o ključu s povprečno 1.6 ranljivostmi, druga najmanj jih ima skupina overitev s povprečno 2.6 ranljivostmi in na zadnjem mestu skupina dogovor o overjenem ključu s povprečno 2.8 ranljivostmi. Tako da so razlike med izpolnjenimi zahtevami in ranljivostmi za skupino overitev 2.4, za skupino overitev in dogovor o ključu 4.3 in za skupino dogovor o overjenem ključu 1.8, kar pomeni, da je najboljša skupina overitev in dogovor o ključu. Takšen končen rezultat nas je presenetil, saj smo pričakovali bolj enakomerno porazdeljene rezultate, predvsem pa smo pričakovali, da bo skupina dogovor o overjenem ključu imela več izpolnjenih zahtev in manj ranljivosti. Prav tako smo v vseh skupinah pričakovali večje povprečje preverjenih napadov in izpolnjenih zahtev, saj je varnostnih zahtev in napadov, ki smo jih zajeli, preko

50 (zagotovo pa smo kakšnega tudi izpustili). To pomeni, da je v povprečju posamezna skupina protokolov preverjena s približno 10 % vseh zahtev.

- RV4: Ali obstaja klasifikacija napadov na overitvene protokole?

Klasifikacija napadov na overitvene protokole še ne obstaja.

- RV5: Katere kriterije je treba upoštevati pri snovanju overitvenega protokola?

Kot smo že omenili pri odgovoru na raziskovalno vprašanje RV3, ne obstaja enotni seznam zahtev ali priporočil, katerih naj bi se avtorji držali, zato smo tudi tukaj pripravili lasten seznam pomembnejših kriterijev, ki jih je potrebno upoštevati ob snovanju novega overitvenega protokola. Kriterije, ki smo jih preverjali, smo pridobili iz naših seznamov napadov in varnostnih zahtev. Potem smo preverjali, v kolikih primerih se posamezen kriterij pojavlja pri protokolih (ne glede na način, kako se pojavlja; upoštevali pa smo tako varnostne zahteve kot ranljivosti). Prav tako smo izračunali odstotek pojavljanja, in sicer tako, da smo število pojavitev delili z 297 (število vseh protokolov) v vseh primerih razen za kriterije N15, N19, N23, N27, Z12, Z13, Z16, Z23 in Z24. Te kriterije smo delili s številom posamezne skupine protokolov. Število pojavov kriterijev N19, N23 in N27 smo delili z 22, saj je toliko protokolov, ki delujejo na področju senzorskih omrežij, število pojavov kriterija N15 smo delili z 82, saj je toliko protokolov ki delujejo na področju pametnih kartic, število pojavov kriterijev Z12, Z13, Z16, Z23 in Z24 pa smo delili z 48, saj je toliko protokolov, ki delujejo na področju RFID. Menimo, da se tako pridobi najboljša ocena pomembnosti kriterijev. V tabeli 5.11 so zapisani rezultati. Kot lahko vidimo iz rezultatov, se zgolj pet kriterijev pojavlja v več kot polovici protokolov, pri čemer sta dva od teh posebna kriterija, ki ju preverjamo na manjši skupini protokolov.

Tabela 5.11 Število pojavitev kriterijev

ID	Pojavov	Odstotek	ID	Pojavov	Odstotek	ID	Pojavov	Odstotek
N1	7	2 %	**N17**	5	2 %	**Z6**	43	14 %
N2	159	54 %	**N18**	34	11 %	**Z7**	163	55 %
N3	71	24 %	**N19**	10	46 %	**Z8**	69	23 %
N4	226	76 %	**N20**	26	9 %	**Z9**	12	4 %
N5	196	66 %	**N21**	7	2 %	**Z11**	6	2 %

N6	45	15 %	**N22**	6	2 %	**Z12**	16	33 %
N7	90	30 %	**N23**	5	23 %	**Z13**	17	35 %
N8	109	37 %	**N24**	12	4 %	**Z14**	27	9 %
N9	13	4 %	**N25**	19	6 %	**Z16**	1	2 %
N10	26	9 %	**N26**	25	8 %	**Z17**	11	4 %
N11	36	12 %	**N27**	9	41 %	**Z18**	2	1 %
N12	29	10 %	**Z1**	1	0 %	**Z22**	2	1 %
N13	99	33 %	**Z2**	1	0 %	**Z23**	10	21 %
N14	127	43 %	**Z3**	145	49 %	**Z24**	5	10 %
N15	74	90 %	**Z4**	8	3 %	**Z26**	18	6 %
N16	5	2 %	**Z5**	188	63 %			

Na podlagi teh podatkov smo pripravili priporočila za snovanje overitvenih protokolov, ki so prikazana v tabeli 5.12. Odločili smo se, da bomo na osnovi pojavitev pripravili tudi priporočila. Kriteriji so razdeljeni še na področje uporabe, kar pomeni, da so napadi in zahteve v stolpcih RFID, pametna kartica in senzorska omrežja veljavni le za te določene protokole. Seveda je najboljše, če razvijalec novega protokola preveri vse napade in zadosti vsem varnostnim zahtevam, vendar v primeru, da to ne gre, priporočila razdelimo glede na odstotek pojavljanja, tako da priporočamo, da se napadi in zahteve preverjajo od najpogostejšega do najredkejšega kriterija. Prav tako priporočamo pregled vseh specifičnih kriterijev za to skupino, če se razvija protokol, ki deluje na tem področju.

Tabela 5.12 Splošna priporočila za preverjanje varnosti

Pojavitev	**Kriteriji**			
	Vsa področja	**RFID**	**Pametna kartica**	**Senzorska omrežja**
Nad 40 %	N2, N4, N5, N14, Z3,Z5,Z7		N15	N19, N27
Nad 20 %	N3, N7, N8, N13, Z8	Z12, Z13, Z23		N23
Nad 10 %	N6, N11, N12, N18, Z6	Z24		
Pod 10 %	N1, N9, N10, N16, N17, N20, N21, N22, N24, N25, N26, Z1, Z2, Z4, Z9, Z11, Z14, Z17, Z18, Z19, Z22, Z26	Z16		

Nato smo pregledali tudi pojavljanje kriterijev glede na faktorje overitve. Postopek dela je enak kot pri splošnih priporočilih, le da smo tukaj razdelili vse protokole v dve skupini glede na število faktorjev overitve, nato pa smo izvedli analizo pojavov kriterijev in izdelali tabelo priporočil za vsako skupino posebej. V tabeli 5.13 so prikazani rezultati analize pojavov za protokole z enim faktorjem overjanja.

Tabela 5.13 Seznam pojavov kriterijev pri protokolih z enim faktorjem

ID	Pojavov	Odstotek	ID	Pojavov	Odstotek	ID	Pojavov	Odstotek
N1	6	2 %	**N17**	2	1 %	**Z6**	43	16 %
N2	129	49 %	**N18**	23	9 %	**Z7**	151	58 %
N3	55	21 %	**N19**	4	37 %	**Z8**	61	23 %
N4	196	75 %	**N20**	22	8 %	**Z9**	12	5 %
N5	168	64 %	**N21**	7	3 %	**Z11**	6	2 %
N6	38	15 %	**N22**	6	2 %	**Z12**	16	33 %
N7	72	27 %	**N23**	2	18 %	**Z13**	17	35 %
N8	97	37 %	**N24**	12	5 %	**Z14**	24	9 %
N9	13	5 %	**N25**	19	7 %	**Z16**	1	2 %
N10	16	6 %	**N26**	24	9 %	**Z17**	7	3 %
N11	27	10 %	**N27**	4	37 %	**Z18**	2	1 %
N12	23	9 %	**Z1**	1	0 %	**Z22**	2	1 %
N13	84	32 %	**Z2**	1	0 %	**Z23**	10	21 %
N14	101	39 %	**Z3**	121	46 %	**Z24**	5	10 %
N15	54	100 %	**Z4**	8	3 %	**Z26**	18	7 %
N16	2	1 %	**Z5**	157	60 %			

Iz tabele lahko vidimo, da do večjih odstopanj ne prihaja, kar pomeni, da sta tabeli priporočil podobni, loči ju le nekaj razlik glede pogostosti posameznega napada ali zahteve. Pripravili smo tudi priporočila za protokole z enim faktorjem overjanja, ki so prikazana v tabeli 5.14.

Tabela 5.14 Priporočila za preverjanje varnosti za protokole z enim faktorjem overjanja

Pojavitev	Kriteriji			
	Vsa področja	RFID	Pametna kartica	Senzorska omrežja
Nad 40 %	N2, N4, N5, Z3, Z5, Z7		N15	
Nad 20 %	N3, N7, N8, N13, N14, Z8	Z12, Z13, Z22		N19, N27
Nad 10 %	N6, N11, Z6	Z23		N23,
Pod 10 %	N1, N9, N10, N12, N16, N17, N18, N20, N21, N22, N24, N25, N26, Z1, Z2, Z4, Z9, Z11, Z14, Z17, Z18, Z19, Z24, Z26	Z16		

Nato smo analizirali še protokole z dvema faktorjema overjanja in prišli do rezultatov, ki so prikazani v tabeli 5.15.

Tabela 5.15 Seznam pojavov kriterijev pri protokolih z dvema faktorjema overjanja

ID	Pojavov	Odstotek	ID	Pojavov	Odstotek	ID	Pojavov	Odstotek
N1	1	3 %	**N17**	3	9 %	**Z6**	0	0 %
N2	30	86 %	**N18**	11	31 %	**Z7**	12	34 %
N3	16	46 %	**N19**	6	55 %	**Z8**	8	23 %
N4	30	86 %	**N20**	4	11 %	**Z9**	0	0 %
N5	28	80 %	**N21**	0	0 %	**Z11**	0	0 %
N6	7	20 %	**N22**	0	0 %	**Z12**	0	0 %
N7	18	51 %	**N23**	3	27 %	**Z13**	0	0 %
N8	12	34 %	**N24**	0	0 %	**Z14**	3	9 %
N9	0	0 %	**N25**	0	0 %	**Z16**	0	0 %
N10	10	29 %	**N26**	1	3 %	**Z17**	4	11 %
N11	9	26 %	**N27**	5	45 %	**Z18**	0	0 %
N12	6	17 %	**Z1**	0	0 %	**Z22**	0	0 %
N13	15	43 %	**Z2**	0	0 %	**Z23**	0	0 %
N14	26	74 %	**Z3**	24	69 %	**Z24**	0	0 %
N15	20	71 %	**Z4**	0	0 %	**Z26**	0	0 %
N16	3	9 %	**Z5**	31	89 %			

Pri protokolih z dvema faktorjema overjanja je prišlo do večjih razlik, saj so tukaj avtorji izpuščali veliko napadov, ki so jih avtorji protokolov z enim faktorjem overjanja preverjali. Zato je tudi v priporočilih izpuščenih veliko napadov in zahtev, kot lahko vidimo v tabeli 5.16.

Tabela 5.16 Priporočila za preverjanje varnosti za protokole z dvema faktorjema overjanja

Pojavitev	**Kriteriji**			
	Vsa področja	**RFID**	**Pametna kartica**	**Senzorska omrežja**
Nad 40 %	N2, N3, N4, N5, N7, N13, N14, Z3, Z5		N15	N19, N27
Nad 20 %	N6, N8, N10, N11, N18, Z7, Z8			N23
Nad 10 %	N12, N20, Z17			
Pod 10 %	N1, N16, N17, N26, Z14			

5.4 Omejitve

Potrebno pa je tudi opisati omejitve, s katerimi smo se srečali pri izdelavi magistrskega dela in izvedbi sistematičnega pregleda literature.

Pri teoretičnem pregledu metode sistematičnega pregleda literature smo ugotovili, da se priporoča izvedba sistematičnega pregleda literature vsaj v paru, če že ne v skupini, da se zagotovi visok nivo nepristranskosti. Tega priporočila se nismo mogli držati, tako da je SLR izvedel zgolj en raziskovalec.

Druga omejitev je bila omejitev glede virov raziskav. Omejili smo se na knjižnice Science Direct, Springer Link in IEEExplore, in sicer na podlagi preliminarnega iskanja. Ostale knjižnice, ki smo jih pregledali, so vrnile neprimerne rezultate.

Tretja omejitev je bila omejitev glede iskalnega niza. Uporabili smo niz, ki nam je vrnil do 500 zadetkov, vendar smo ga za to morali okrniti, kar je morda izločilo kakšne relevantne raziskave.

Četrta omejitev je bila ta, da smo za prost dostop do člankov potrebovali omrežje Univerze v Mariboru. Če so bili članki v tem omrežju vseeno plačljivi, smo jih izločili.

Zadnja omejitev pa je ta, da smo izpustili nekaj faz sistematičnega pregleda literature. Načrta sistematičnega pregleda nismo preverili pri zunanjih osebah, prav tako nismo vrednotili kvalitete člankov, saj to ni bilo potrebno. Prav tako nismo izvajali sekundarnega iskanja virov, kar pomeni, da nismo pregledovali vseh referenc primarnih virov.

6 SKLEP

6.1 Preverjanje hipotez

H1: Overitveni protokoli z več faktorji overjanja imajo manj ranljivosti kot protokoli z enim faktorjem overjanja.

Iz tabele 5.9 lahko vidimo, da imajo protokoli z več faktorji overjanja več znanih napadov, zato hipotezo 1 ovržemo in sprejmemo ničelno hipotezo, ki pravi, da imajo protokoli z enim faktorjem overjanja manj znanih napadov.

H2: Obstajajo 3 skupine protokolov: »overitev«, »overitev in dogovor o ključu«, ter »dogovor o overjenem ključu«.

Kot smo že zapisali v odgovoru na raziskovalno vprašanje 2, nismo našli dovolj podatkov, ki bi dovolj podrobno in specifično opisovali še kakšno drugo skupino poleg skupine overitev, overitev in dogovor o ključu in dogovor o overjenem ključu. Ker smo ugotovili samo te 3 skupine, lahko hipotezo 2 potrdimo.

H3: Najbolj razširjena skupina je skupina »overitev«.

Izmed vseh 297 protokolov smo jih kar 193 uvrstili v skupino overitev, kar potrjuje našo tretjo hipotezo.

H4: Najmanj ranljivosti ima skupina »dogovor o overjenem ključu«.

Iz tabele 5.10 je razvidno, koliko ranljivosti ima določena skupina protokolov. V tabeli je zapisano, da ima skupina overitev in dogovor o ključu najmanj ranljivosti s povprečno 1.6 ranljivostmi. Skupina dogovor o overjenem ključu je na tretjem mestu s povprečno 2.8 ranljivostmi. Na podlagi teh podatkov hipotezo 4 zavrnemo in sprejmemo alternativno hipotezo, da ima najmanj ranljivosti skupina overitev in dogovor o ključu.

H5: Klasifikacija napadov na overitvene protokole ne obstaja.

Glede na prelimirani pregled, ki smo ga izvedli, smo ugotovili, da klasifikacija ne obstaja, zato na podlagi teh podatkov hipotezo 5 sprejmemo.

6.2 Zaključek

V magistrskem delu smo se lotili pregleda področja overitvenih protokolov. Želeli smo pridobiti osnovno znanje o različnih overitvenih protokolih, o metodah, ki jih uporabljajo, o njihovih varnostnih zahtevah in znanih napadih. Za dosego tega cilja smo uporabili metodo sistematičnega pregleda literature. Po pregledu metodologije smo pripravili načrt izvedbe, nato pa smo na osnovi iskalnega niza poiskali primerne vire. Po končanem postopku izločanja virov glede na vključitvene kriterije nam je ostal seznam 120 različnih raziskav, ki smo jih nato pregledali in iz njih pridobili podatke, ki so nas zanimali.

Na podlagi analize pridobljenih podatkov smo nato odgovorili na raziskovalna vprašanja. Zanimalo nas je, katere vrste overitvenih protokolov obstajajo, katera izmed vrst je najbolj varna (ima najmanj ranljivosti in največ izpolnjenih varnostnih zahtev), kakšen je vpliv stopnje na varnost overitvenih protokolov, če že obstaja klasifikacija napadov in varnostnih zahtev ter kakšna so priporočila za snovanje novega overitvenega protokola. Ugotovili smo: (i) da obstajajo skupine overitev, overitev in dogovor o ključu in dogovor o overjenem ključu, (ii) da je najbolj varna izmed teh overitev in dogovor o ključu, (iii) da več stopenjsko overjanje samo po sebi ne predstavlja večje varnosti protokola in (iv) da klasifikacija še ne obstaja. Na tej osnovi smo pripravili tudi priporočila za snovanje novih protokolov.

S sistematičnim pregledom literature smo pridobili potrebno osnovno znanje o področju in lahko nadaljujemo raziskovanje v tej smeri. Prav tako smo pripravili priporočila in klasifikacijo, kar bi lahko snovalec novega overitvenega protokola uporabil kot referenco za iskanje in odpravo ranljivosti svojega novega protokola.

Menimo, da je področje kljub temu še vedno zelo neurejeno in neenotno, zato predlagamo nove raziskave, kjer bi se pripravil splošen formalni model overitvenih protokolov, njihovih varnostnih zahtev, ter znanih napadov.

VIRI IN LITERATURA

Acar, T., Belenkiy, M., & Küpçü, A. (2013). Single password authentication. *Computer Networks*, *57*(13), 2597–2614. http://doi.org/10.1016/j.comnet.2013.05.007

Burrows, M., Abadi, M., & Needham, R. (1990). A logic of authentication. *ACM Transactions on Computer Systems*, *8*(1), 18–36. http://doi.org/10.1145/77648.77649

Chuang, M.-C., & Chen, M. C. (2014). An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics. *Expert Systems with Applications*, *41*(4), 1411–1418. http://doi.org/10.1016/j.eswa.2013.08.040

Cohen, F. (1997). Information system attacks: A preliminary classification scheme. *Computers & Security*, *16*(1), 29–46. http://doi.org/10.1016/S0167-4048(97)85785-9

Dalton, M., Kozyrakis, C., & Zeldovich, N. (2009). Nemesis: Preventing Authentication & Access Control Vulnerabilities in Web Applications. In *USENIX Security Symposium* (pp. 267–282).

Das, A. K. (2014). A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks. *Peer-to-Peer Networking and Applications*. http://doi.org/10.1007/s12083-014-0324-9

Davi, L., Dmitrienko, A., Sadeghi, A.-R., & Winandy, M. (2011). Privilege Escalation Attacks on Android. In M. Burmester, G. Tsudik, S. Magliveras, & I. Ilić (Eds.), *Information Security* (Vol. 6531, pp. 346–360). Berlin, Heidelberg: Springer Berlin Heidelberg.

Debiao, H., Jianhua, C., & Jin, H. (2012). An ID-based client authentication with key agreement protocol for mobile client–server environment on ECC with provable

security. *Information Fusion*, *13*(3), 223–230. http://doi.org/10.1016/j.inffus.2011.01.001

Deebak, B. D., Muthaiah, R., Thenmozhi, K., & Swaminathan, P. I. (2015). Analyzing three-party authentication and key agreement protocol for real time IP multimedia server–client systems. *Multimedia Tools and Applications*. http://doi.org/10.1007/s11042-015-2542-4

Ding, Y., Zhou, X., Cheng, Z., & Zeng, W. (2013). Efficient Authentication and Key Agreement Protocol with Anonymity for Delay Tolerant Networks. *Wireless Personal Communications*, *70*(4), 1473–1485. http://doi.org/10.1007/s11277-012-0760-x

Duncan, R. (2001). An Overview of Different Authentication Methods and Protocols. *Report Submitted to SANS Institute*.

Farash, M. S., Kumari, S., & Bakhtiari, M. (2015). Cryptanalysis and improvement of a robust smart card secured authentication scheme on SIP using elliptic curve cryptography. *Multimedia Tools and Applications*. http://doi.org/10.1007/s11042-015-2487-7

Gope, P., & Hwang, T. (2015). A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system. *Computers & Security*. http://doi.org/10.1016/j.cose.2015.05.004

Hafizul Islam, S., & Biswas, G. P. (2013). Design of improved password authentication and update scheme based on elliptic curve cryptography. *Mathematical and Computer Modelling*, *57*(11-12), 2703–2717. http://doi.org/10.1016/j.mcm.2011.07.001

Hsieh, W.-B., & Leu, J.-S. (2013). A Time and Location Information Assisted OTP Scheme. *Wireless Personal Communications*, *72*(1), 509–519. http://doi.org/10.1007/s11277-013-1026-y

Hwang, M.-S., Chong, S.-K., & Chen, T.-Y. (2010). DoS-resistant ID-based password authentication scheme using smart cards. *Journal of Systems and Software*, *83*(1), 163–172. http://doi.org/10.1016/j.jss.2009.07.050

Islam, S. H., & Biswas, G. P. (2015). Design of Two-Party Authenticated Key Agreement Protocol Based on ECC and Self-Certified Public Keys. *Wireless Personal Communications*, *82*(4), 2727–2750. http://doi.org/10.1007/s11277-015-2375-5

Jiang, P., Wen, Q., Li, W., Jin, Z., & Zhang, H. (2015). An anonymous and efficient remote biometrics user authentication scheme in a multi server environment. *Frontiers of Computer Science*, *9*(1), 142–156. http://doi.org/10.1007/s11704-014-3125-7

Kalra, S., & Sood, S. K. (2015). Advanced password based authentication scheme for wireless sensor networks. *Journal of Information Security and Applications*, *20*, 37–46. http://doi.org/10.1016/j.jisa.2014.10.008

Keele, S. (2007). Guidelines for performing systematic literature reviews in software engineering. In *Technical report, Ver. 2.3 EBSE Technical Report. EBSE*.

Kumari, S., Khan, M. K., & Li, X. (2014). An improved remote user authentication scheme with key agreement. *Computers & Electrical Engineering*, *40*(6), 1997–2012. http://doi.org/10.1016/j.compeleceng.2014.05.007

Lu, Y., Li, L., Peng, H., & Yang, Y. (2015). A secure and efficient mutual authentication scheme for session initiation protocol. *Peer-to-Peer Networking and Applications*. http://doi.org/10.1007/s12083-015-0363-x

Markantonakis, K., Tunstall, M., Hancke, G., Askoxylakis, I., & Mayes, K. (2009). Attacking smart card systems: Theory and practice. *Information Security Technical Report*, *14*(2), 46–56. http://doi.org/10.1016/j.istr.2009.06.001

Mishra, D. (2015). Design and Analysis of a Provably Secure Multi-server Authentication Scheme. *Wireless Personal Communications*. http://doi.org/10.1007/s11277-015-2975-0

Moosavi, S. R., Nigussie, E., Virtanen, S., & Isoaho, J. (2014). An Elliptic Curve-based Mutual Authentication Scheme for RFID Implant Systems. *Procedia Computer Science*, *32*, 198–206. http://doi.org/10.1016/j.procs.2014.05.415

Morshed, M. M., Atkins, A., & Yu, H.-N. (2012). An efficient and secure authentication protocol for RFID systems. *International Journal of Automation and Computing*, *9*(3), 257–265. http://doi.org/10.1007/s11633-012-0642-4

Odelu, V., Das, A. K., & Goswami, A. (2015). An efficient ECC-based privacy-preserving client authentication protocol with key agreement using smart card. *Journal of Information Security and Applications*. http://doi.org/10.1016/j.jisa.2015.01.001

Schneier, B. (1996). *Applied cryptography: protocols, algorithms, and source code in C* (2nd ed). New York: Wiley.

Shen, H., Gao, C., He, D., & Wu, L. (2015). New biometrics-based authentication scheme for multi-server environment in critical systems. *Journal of Ambient Intelligence and Humanized Computing*. http://doi.org/10.1007/s12652-015-0305-8

Shinder, D. (2001, August 28). Understanding and selecting authentication methods.

Subramanian, L., Roth, V., Stoica, I., Shenker, S., & Katz, R. (2004). Listen and whisper: Security mechanisms for BGP. In *Proc. First Symposium on Networked Systems Design and Implementation (NSDI)* (p. 11).

Syverson, P. F., & Cervesato, I. (2001). *The Logic of Authentication Protocols*. Berlin ; New York: Springer.

Todorov, D. (2007). *Mechanics of user identification and authentication: Fundamentals of identity management*. CRC Press.

Woo, T. Y., & Lam, S. S. (1993). Verifying authentication protocols: Methodology and example. In *Network Protocols, 1993. Proceedings., 1993 International Conference on* (pp. 36–45). IEEE.

Xie, Q., Liu, W., Wang, S., Hu, B., Dong, N., & Yu, X. (2014). Robust password and smart card based authentication scheme with smart card revocation. *Journal of Shanghai Jiaotong University (Science)*, *19*(4), 418–424. http://doi.org/10.1007/s12204-014-1518-2

Zhu, H. (2015). Cryptanalysis and Improvement of a Mobile Dynamic ID Authenticated Key Agreement Scheme Based on Chaotic Maps. *Wireless Personal Communications*. http://doi.org/10.1007/s11277-015-2896-y

PRILOGE

Priloga A: Pomožna tabela protokolov, napadov in zahtev

ID	Naziv protokola
P01	Single password authentication - SPA
P02	Extensible authentication protocol
P03	Hsieh-Leu authentication scheme
P04	Amin-Biswas authentication protocol
P05	Jiang et. Al.'s authentication and key agreement scheme
P06	Yeh et al.'s Robust smart card secured authentication scheme on SIP using Elliptic Curve Cryptography
P07	Arshad-Nikooghdam two factor authentication and key agreement scheme
P08	Irshad et. Al.'s authentication and key agreement scheme
P09	Arshad-Nikooghdam authentication and key agreement scheme for SIP
P10	Tsai's authentication scheme for SIP
P11	Arshad et. Al.'s Elliptic curve cryptography based mutual authentication scheme for session initiation protocol
P12	Shen et. Al.'s Security enhancement for the timestamp-based password authentication
P13	Awasthi et. Al.'s improved timestamp-based remote user authentication scheme
P14	DRCEP (Denial-of-service Resistant Call Establishment Protocol)
P15	Buttyan et. Al.'s certificate based authentication protocol
P16	Cao et. Al's authentication scheme
P17	Li et. Al's password authenticated key-agreement
P18	Chang et. Al.'s authenticated key agreement
P19	Tsai et. Al.'s Efficient multi-server authentication scheme based on one-way hash function without verification table
P20	Wang et. Al.'s User authentication scheme with privacy-preservation for multi- server environment
P21	Chen et. Al.'s authentication scheme for multi-server environments
P22	LLT protocol
P23	ILLT
P24	VLYK protocol
P25	improved VLYK protocol
P26	Doss et al.'s Rabin cryptosystem-based RFID authentication scheme
P27	Chien et. Al.'s novel Rabin cryptosystem authentication scheme
P28	New Password-Based Authenti- cated Diffie-Hellman Key Agreement Scheme
P29	Guo et al.'s three-party password-based authenticated key exchange (G-3PAKE) protocol
P30	Chou's mutual authentication RFID scheme
P31	Godor et al.'s Elliptic curve cryptography basedmutual authentication protocol for

	lowcomputational capacityRFIDsystems-performance analysis by simulations
P32	O'neill and Robshaw Low-cost digital signature architecture suitable for radio frequency identification tags.
P33	Lee et. Al.'s Anti-counterfeiting, untraceability and other security challenges for RFID systems: public-key-based protocols and hardware
P34	Batina et. Al. Public-key cryptography for RFID-tags
P35	Tuyls et. Al.'s RFID-tags for Anti-Counterfeiting
P36	lightweight mutual authentication mechanism (LMAM)
P37	Chuang et. Al.'s anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics
P38	Yoon and yoo biometrics-based multi-server authentication with key agreement scheme
P39	yang and yang biometric password based multi-server authentication scheme
P40	li and hwang's efficient biometrics-based remote user authen- tication scheme using smart cards
P41	xu et. Al. Fingerprint based remote user authentication scheme
P42	khan et. Al. Fingerprint biometric remote user authentication scheme
P43	lin and laj biometrics remote user authentication scheme
P44	Liao and wang's A secure dynamic id-based remote user authentication scheme for multi-server environment
P45	Tsai's multi server authentiction scheme
P46	Chang and lee's An efficient and secure multi-server password authentication scheme using smart cards
P47	Juang's Efficient multi-server password authenticated key agreement using smart cards
P48	Jiang et. Al.'s efficient two factor user authentication scheme
P49	Das's A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks
P50	Das's Two-factor user authentication in wireless sensor networks
P51	Yoo et al.'s A security-performance-balanced user authentication scheme for wireless sensor networks
P52	Sun et. Al.'s security and improvement of a two-factor user authentication scheme in wireless sensor networks
P53	Xue et. Al.'s A temporal-credential- based mutual authentication and key agreement scheme for wireless sensor networks
P54	An's biometric based remote user authentication scheme
P55	Das's robust anonymous biometric-based remote user authentication scheme
P56	Das's biometric based remote user authentication scheme
P57	Li et. Al's biometric based remote user authentication scheme
P58	Li-Hwang biometric based remote user authentication scheme
P59	Deebak's Mutual Adaptive User Authentication Scheme (S-Cum-EMAUA)
P60	Vaidya et. Al.'s Two-factor mutual authentication with key agreement
P61	Nyang and lee's Improvement of Das's two-factor authentication protocol
P62	He et al.'s An enhanced two-factor user authentication scheme in wireless sensor networks
P63	Khan et al.'sCryptanalysis and security improvements of Two-factor user authentication in wireless sensor networks
P64	Chen and Shih's robust mutual authentication protocol

P65	Xue et al.'s A temporal-credential-based mutual authentication and key agreement scheme
P66	Deebak's proposed 3-PAKE protocol
P67	Xie et al.'s three-party password-based key exchange protocol
P68	Xiong et al.'s three-party password authenticated key exchange protocols
P69	Tallapally's n simple three partyPAKEprotocol
P70	Hsieh et al.'s An improvement of Saeednia's identity based key exchange protocol
P71	Tseng's efficient two-party identity-based key exchange protocol
P72	Ding et al.'s Efficient Authentication and Key Agreement Protocol with Anonymity for Delay Tolerant Networks
P73	Doss et al.'s practical quadratic residues based scheme for authentication
P74	Wong et al.'s authentication on RFID tags
P75	Chien et chen's Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards
P76	Chen et al.'s novel mutual authentication scheme based on quadratic residues for RFID systems
P77	Yeh et al.'s Improvement of the RFID authentication scheme based on quadratic residues
P78	Lo et al.'s efficient mutual authentication scheme for EPCglobal Class-1 Generation-2 RFID systems
P79	Yeh et al.'s Securing RFID systems conforming to EPC Class 1 Generation 2 standards
P80	Chen and Deng's RFID system with mutual authentication
P81	Liu et al.'s privacy and authentication protocol for passive RFID tags
P82	Cho et al.'s a hash based RFID mutual authenication protocol using a secret value
P83	Doss et al.'s minimum disclosure approach to authentication and privacy in RFID systems
P84	O-FRAP and O-RAP
P85	O-FRAP+ and O-RAP+
P86	A2-MAKE: An efficient anonymous and accountable mutual authentication and key agreement protocol for WMNs
P87	Farash's Security analysis and enhancements of an improved authentication for session initiation protocol with provable security
P88	Tu et al.'s password-based authen- ticated key agreement protocol
P89	Farash's efficient client–client password-based authentication scheme with provable security
P90	Tso's three-party password-based authenticated key exchange (3PAKE) protocol
P91	Pu et al.'s Secure verifier-based three-party password-authenticated key exchange
P92	Yang et al.'s Provably secure three-party authenticated key agreement protocol using smart cards
P93	Youn et al.'s Efficient three-party key exchange protocols with round efficienc
P94	Chang et al.'s communication-efficient three-party password authenti- cated key exchange protocol
P95	Farash's new efficient authenticated multiple-key exchange protocol from bilinear pairings
P96	Cheng et Ma's Analysis and improvement of an authenticated multiple key exchange protocol
P97	Farash et al.'s Cryptanalysis and improvement of a robust smart card secured authentication scheme on SIP using elliptic curve cryptography
P98	Zhang et al.'s Efficient and flexible password authenticated key agreement for Voice over Internet Protocol Session Initiation Protocol using smart card

P99	Zhang et al.'s Cryptanalysis and improvement of password authenticated key agreement for session initiation protocol using smart cards
P100	Tu et al.'s An improved authentication protocol for session initiation protocol using smart card
P101	Farash et al.'s efficient user authentication and key agreement scheme for heterogeneouswireless sensor network tailored for the Internet of Things environment
P102	Turkanovič et al.'s novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor net- works, based on the internet of things notion
P103	Fu et al.'s GHAP: An Efficient Group-based Handover Authentication Mechanism for IEEE 802.16m Networks
P104	Fu et al.'s Fast and Secure Handover Authentication Scheme Based on Ticket forWiMAX andWiFi Heterogeneous Networks
P105	Fu et al.'s efficient handover authentication scheme with privacy preservation for IEEE 802.16m network
P106	Gope and Hwang's Enhanced Secure Mutual Authentication and Key Agreement Scheme Preserving User Anonymity in Global Mobile Networks
P107	Qi et al.'s enhanced authentication schemewith privacy preservation for roaming services in global mobility networks
P108	Wen et al.'s secure and effective user authentication scheme for roaming ser- vice in global mobility networks
P109	Gope and Hwang's realistic lightweight authentication protocol preserving strong anonymity for securing RFID system
P110	Yang et al.'s Mutual authentication protocol for low-cost RFID
P111	Tan et al.'s Secure and server-less RFID authentication and search protocols
P112	Cai et al.'s Attacks and improvements to an RFID mutual authentication protocol
P113	Cho et al.'s a hash-based radio-frequency identification (RFID) tag mutual authentication protocol
P114	Guo et al.'s Analysis and Improvement of 'Chaotic Map Based Mobile Dynamic ID Authenticated Key Agreement Scheme
P115	Lin'smobile dynamic IDauthenticated scheme
P116	Lee et al.'s extended chaotic maps-based key agreement protocol with user anonymity
P117	Xue and Hong's Security improvement on an anonymious key agreement protocol based on chaotic maps
P118	Habibi and Aref's Security and Privacy Analysis of Song–Mitchell RFID Authentication Protocol
P119	Song and Mitchell's Scalable RFID security protocols supporting tag ownership transfer
P120	Islam and Biswas's improved password authentication and update scheme based on elliptic curve cryptography
P121	Lin and Hwang's password authentication scheme with secure password updating
P122	Peyravian and Zunic's Methods for protecting password transmission
P123	Hwang and Yeh's Improvement on Peyravian–Zunic's password authentication schemes
P124	Zhu et al.'s Improvement upon mutual password authentication scheme
P125	He et al.'s strong user authentication scheme with smart cards for wireless communications
P126	Wu et al.'s secure authentication scheme with anonymity for wireless communications
P127	Hsiang and Shih's Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment
P128	Holbl et al.'s improved two-party identity-based authenticated key agreement protocol using pairings
P129	Hsieh and Leu's Time and Location Information Assisted OTP Scheme
P130	Kerberos

P131	S/KEY OTP
P132	Hsu et al.'s Novel Remote User Authentication Scheme from Bilinear Pairings Via Internet
P133	Manik et al.'s novel remote user authentication scheme using bilinear pairings
P134	Fang and Huang's Improvement of recently proposed remote user authentication schemes
P135	Hwang et al.'s DoS-resistant ID-based password authentication scheme using smart cards
P136	Kim et al.'s . Id-based password authentication scheme using smart cards and fingerprint
P137	Islam and Biswas'simproved pairing-free identity-based authenticated key agreement protocol based on ECC
P138	Cao’s ID-2PAKA protocol
P139	Islam and Biswas's more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem
P140	Yang and Chang's ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem
P141	Yoon and yoo's Robust ID-based remote mutual authentication with key agreement scheme for mobile devices on ECC
P142	Chen et al.'s An advanced ECC ID-based remote mutual authentication scheme for mobile devices
P143	Islam and Biswas's Two-Party Authenticated Key Agreement Protocol Based on ECC and Self-Certified Public Keys (2-PAKA)
P144	Chen and Kudla's Identity based key agreement protocols from pairings
P145	Choie et al.'s Efficient identity-based authenticated key agreement protocol from pairings
P146	Holbl et Welzer's Two improved two-party identity-based authenticated key agreement protocols
P147	McCullagh and Baretto's two-party identity-based authenticated key agree- ment
P148	Kudla and Patterson's Modular security proofs forkeyagreementprotocols
P149	Ryu et al.'s efficient ID-based authenticated key agreement protocol from pairings
P150	Shim's Efficient ID-based authenticated key agreement protocol based onWeil pairing
P151	Smart's An identity based authenticated key agreement protocol based on theWeil pairing
P152	Xie's Cryptanalysis of Noel McCullagh and Paulo S.L.M. Barreto’s two-party identity-based key agreement
P153	Cao et al's A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges
P154	Cao et al's Identity-based authentication key agreement protocols without bilinear pairings
P155	Zu-Hua's Efficient authenticated key agreement protocol using self-certified public keys from pairings
P156	Ni et al.'s Strongly secure identity-based authenticated key agreement protocols in the escrow mode
P157	Wang et al.'s Efficient identity-based authenticated key agreement protocol with PKG forward secrecy
P158	Tsaur's Several security schemes constructed using ECC-based self-certified public key cryptosystems
P159	Jiang et al.'s anonymous and efficient remote biometrics user authentication scheme in amulti server environment
P160	Kim et al.'s Cryptanalysis and improvement of a biometrics-based multi-server authentication with key agreement scheme
P161	Li et al.'s Cryptanalysis and improve- ment of a biometric-based remote authentication scheme using smart cards
P162	Yoon and yoo's Robust biometrics-based multi-server authenti- cation with key agreement scheme for smart cards on elliptic curve cryptosystem

P163	Jiang et al.'s Efficient Ticket Based Authentication Protocol with Unlinkability forWireless Access Networks
P164	Hsieh and Leu's anonymous mobile user authentication protocol using self- certified public keys based on multi-server architectures
P165	Chen et al.'s practical authentication protocol with anonymity for wireless access networks
P166	Kalra and Sood's Advanced remote user authentication protocol for multi-server architecture based on ECC
P167	Sood et al.'s A secure dynamic identity based authentication protocol for multi-server architecture
P168	Kalra and Sood's Advanced password based authentication scheme for wireless sensor networks
P169	Yeh et al.'s A secured authentication protocol for wireless sensor networks using elliptic curves cryptography
P170	Song's Advanced smart card based password authentication protocol
P171	Xu et al.'s An improved smart card based password authentication scheme with provable security
P172	Wong et al.'s A dynamic user authentication scheme for wireless sensor networks
P173	Kang's Cryptanalysis and improvement on an IC-card-based remote login mechanism
P174	Cheng et al.'s Security enhancement of an IC-card based remote login
P175	Karuppiah and Saravanan's secure remote user mutual authentication scheme using smart cards
P176	Ku and Chen's Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards
P177	Yoon et al.'s Further improvement of an efficient password based remote user authentication scheme using smart cards
P178	Liao et al.'s password authentication scheme over insecure networks
P179	Wang et al.'s Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards
P180	Sood et al.'s An improvement of Xu et al.'s authentication scheme using smart cards
P181	Chen et al.'s Robust smart-card-based remote user password authentication scheme
P182	Khan et al.'s An Authentication and Key Establishment Scheme for the IP-BasedWireless Sensor Networks (6LoWPAN)
P183	Kim's Location-based authentication protocol for first cognitive radio networking standard
P184	Mun et al.'s Enhanced secure anonymous authentication scheme for roaming service in global mobility networks
P185	Zhu and Mu's A new authentication scheme with anonymity for wireless environments
P186	Lee et al.'s Security enhancement on a new authentication scheme with anonymity for wireless environments
P187	Das et al.'s A dynamic password-based user authentication scheme for hierarchical wireless sensor networks
P188	Huang et al.'s Enhancement of two-factor user authentication in wireless sensor networks
P189	Vaidya et. Al.'s Two-factor mutual authentication with key agreement
P190	Fan et al.'s A secure and efficient user authentication protocol for two-tieres wireless sensor networks
P191	Lai et al.'s SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks
P192	Lee and Lai's Secure Anonymous Authentication Scheme for Roaming Service in Global Mobility Networks Another Secure Anonymous Authentication Scheme for Roaming Service in Global Mobility Networks
P193	Chang et al.'s A secure authentication scheme with anonymity for wireless communications

P194	He et al.'s Design and validation of an efficient authentication scheme with anonymity for roaming service in global mobility networks
P195	Li and Lee's A novel user authentication and privacy preserving scheme with smart cards for wireless communications
P196	Lee's Enhancing the security of password authenticated key agreement protocols based on chaotic maps
P197	Li et al.'s Secure User Authentication and User Anonymity Scheme based on Quadratic Residues for the Integrated EPRIS
P198	Li et al.'s New Dynamic ID-Based User Authentication Scheme Using Mobile Device
P199	Tsai et al.'s New dynamic ID authentication scheme using smart cards
P200	Wen and Li's An improved dynamic ID-based remote user authentication with key agreement scheme
P201	Lin's Efficient mobile dynamic ID authentication and key agreement scheme without trusted servers
P202	Li et al.'s novel smart card and dynamic ID based remote user authentication scheme for multi-server environments
P203	Lee et al.'s A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards
P204	Liao and Hsiao's novel multi-server remote user authentication scheme using self-certified public
P205	Tseng et al.'s pairing-based user authentication scheme for wireless clients with smart card
P206	Geng and Zhang's dynamic ID-based user authentication and key agreement scheme for multi-server using bilinear pairing
P207	Lu et al.'s secure and efficient mutual authentication scheme for session initiation protocol
P208	Zhang et al.'s secure authentication scheme with anonymity for session initia- tion protocol using elliptic curve cryptography
P209	Yoon et al.'s Robust mutual authen- tication with a key agreement scheme for the session initiation protocol
P210	Xie's new authenticated key agreement for session initiation protocol
P211	He et al.'s secure mutual authentica- tion scheme for session initiation protocol using elliptic curve cryptography
P212	Farash and Attari's enhanced authenticated key agreement for session initiation protocol
P213	Pelaez et al.'s Security Improvement of Two Dynamic ID-based Authentication Schemes by Sood-Sarje-Singh
P214	Sood et al's improvement of Wang et al.'s authentication scheme using smart cards
P215	Sood et al's Improvement of Liao et al.'s Authentication Scheme using Smart Cards
P216	Mir and Nikooghadam's Secure Biometrics Based Authentication with Key Agreement Scheme in Telemedicine Networks for E-Health Services
P217	Yan et al.'s secure biometrics-based authentication scheme for telecare medicine information systems
P218	Mishra's Design and Analysis of a Provably Secure Multi-server Authentication Scheme
P219	Sood et al.'s secure dynamic identity based authentication protocol for multi-server architecture
P220	Li et al.'s An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards
P221	Wang and Ma's smart card based efficient and secured multi-server authentication scheme
P222	Pippal et al.'s Robust smart card authentication scheme for multi- server architecture
P223	Yeh's provably secure multi-server based authentication scheme
P224	Mishra et al.'s secure and efficient ECC-based user anonymity-preserving session initiation authentication protocol using smart card

P225	Irshad et al.'s single round-trip SIP authentication scheme for voice over internet protocol using smart card
P226	Jiang et al.'s Cryptanalysis of smart-card-based pass- word authenticated key agreement protocol for session initiation protocol of Zhang et al.
P227	Kumar et al.'s improved authentication protocol for session initiation protocol using smart card
P228	Mishra et al.'s design of a lightweight two-factor authentication scheme with smart card revocation
P229	Li et al.'s enhanced smart card based remote user password authentication scheme
P230	Mishra et al.'s secure password-based authentication and key agreement scheme using smart cards
P231	Jiang et al.'s Improvement of robust smart-card-based password authentication scheme
P232	Mishra et al.'s secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards
P233	Moosavi et al.'s Elliptic Curve-based Mutual Authentication Scheme for RFID Implant Systemsa
P234	Zhang et al.'s ECDLP-Based Randomized Key RFID Authentication Protocol
P235	Liao and Hsiao's secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol
P236	Moradi et al.'s Security Analysis and Strengthening of an RFID Lightweight Authentication Protocol Suitable for VANETs
P237	Caballero-Gil et al.'s Lightweight authentication for RFID used in VANETs
P238	Morshed et al.'s efficient and secure authentication protocol for RFID systems (ESAP)
P239	HIDV
P240	LCAP
P241	OHLCAP
P242	YA-TRAP*
P243	Tan's enhanced three-party authentication key exchange protocol for mobile commerce environments
P244	Lim et al.'s Cryptanalysis of improved one-round Lin–Li's tripartite key agreement protocol
P245	Chen et al.'s round- and computation-efficient three-party authenticated key exchange proto- col
P246	Odelu et al.'s Effective and Robust Secure Remote User Authenticated Key Agreement Scheme Using Smart Cards in Wireless Communication Systems
P247	Islam's Design and analysis of an improved smartcard-based remote user password au- thentication scheme
P248	Odelu et al.'s efficient ECC-based privacy-preserving client authentication protocol with key agreement using smart card
P249	Li's new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card
P250	Wang's Analysis and enhancement of a password authentication and update scheme based on elliptic curve cryptography
P251	Xie et al.'s Robust Password and Smart Card Based Authentication Scheme with Smart Card Revocation
P252	Xie's Improvement of a security enhanced one-time two-factor authentication and key agreement scheme
P253	Chen et al.'s Security enhance- ment on an improvement on two remote user authen- tication schemes using smart cards
P254	Holbl et al.'s Attacks and improvement of an efficient remote mutual authentication and key agreement scheme
P255	Li and Lee's robust remote user authentication scheme using smart card

P256	Deng et al.'s Tree-LSHB+: An LPN-based lightweight mutual authen- tication RFID protocol
P257	Qian et al.'s revised Tree-LSHB+
P258	Ryu et al.'s KCI-resilient anonymous wireless link-layer authentication protocols
P259	Shen et al.'s New biometrics-based authentication scheme for multi-server environment in critical systems
P260	Shim's round-optimal three-party ID-based authenticated key agreement protocol
P261	Sun et al.'s security and improvement of a two-factor user authentication scheme in wireless sensor networks
P262	Khan and Alghathtbar's Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks'
P263	Tang and Liu's improved Arshad et al.'s ECC-based mutual authentication scheme for session initiation protocol
P264	Teng et al.'s ID-based authenticated dynamic group key agreement with optimal round (DAGKA)
P265	Tsai et al's New Password-Based Multi-server Authentication Scheme Robust to Password Guessing Attacks
P266	Tu et al.'s strongly secure pairing-free certificateless authenticated key agreement protocol suitable for smart media and mobile environments
P267	Wang and Ma's Cryptanalysis and security enhancement of a remote user authentication scheme using smart cards
P268	Wang et al.'s Efficient and provably secure two-factor authentication scheme with user anonymity
P269	Wen et al.'s Analysis and Improvement on a Biometric-Based Remote User Authentication Scheme Using Smart Cards
P270	Wen et al.'s Secure and Effective Anonymous User Authentication Scheme forRoaming Service in Global Mobility Networks
P271	Wu et al.'s improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks
P272	Lee and Hwang's Simple password-based three-party au- thenticated key exchange without server public keys
P273	Xue et al.'s lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture
P274	Yang et al.'s Improved Two-Party Authentication Key Exchange Protocol for Mobile Environment
P275	Chou et al.'s ID-based authenticated schemes with key agreement for mobile environments
P276	Yeh's lightweight authentication scheme with user untraceability
P277	Yeh et al.'s Analysis and design of a smart card based authentication protocol
P278	Chang and Cheng's robust and efficient smart card based remote login mechanism for multi-server ar- chitecture
P279	Yi et al.'s Gen2 Based Security Authentication Protocol for RFID System
P280	Yoon et al.'s secure and efficient SIP authentication scheme for converged VoIP networks
P281	Wu et al.'s new provably secure authentication and key agreement protocol for SIP using ECC
P282	Durlanik and Sogukpinar's SIP authentication scheme using ECDH
P283	Yang et al.'s Secure authentication scheme for session initiation protoco
P284	Yoon et al.'s Robust deniable authentication protocol
P285	Zhang et al.'s Provably secure one-round identity-based authenticated asymmetric group key agreement protocol
P286	Zhang et al.'s Simulatable certificateless two-party authenticated key agreement protocol
P287	Zhou and Xu's Provable secure authentication protocol with anonymity for roaming service

	in global mobility networks
P288	Zhu's Cryptanalysis and Improvement of a Mobile Dynamic ID Authenticated Key Agreement Scheme Based on Chaotic Maps
P289	Lin's Chaotic map based mobile dynamic ID authenticated key agreement scheme
P290	Zhuang et al.'s New Ultralightweight RFID Protocol for Low-Cost Tags
P291	Deebak et al.'s three-party authentication and key agreement
P292	Tso's security analysis and improvements of a communication-efficient three-party password authenticated key exchange protocol
P293	Wu et al.'s Cryptanalysis of a communication-efficient three-party password authenticated key exchange protocol
P294	Tallapally's Security enhancement on simple three party PAKE protoco
P295	Chang et al.'s Security design for three-party encrypted key exchange protocol using smart cards
P296	Yoon and Yoo's Token-based authenticated key establishment protocols for three-party communi- cation
P297	Juang's Efficient three-party key exchange using smart cards

Priloga B: Klasifikacija napadov in varnostnih zahtev

ID raziskave	Naziv protokola	Skupina protokola	Varno pred napadi	Izpolnjene varnostne zahteve	Področje uporabe protokola	Varnostne ranljivosti	Faktorjev
PR 1	P01	authentication		Z1, Z2, Z3, Z4	cloud, mobile,		1
PR 2	P02	authentication			Wi-Fi networks		1
PR 3	P03	authentication			multi server environment	N1, N2, N3, N4	1
	P04	aaka	N2,N4	Z3, Z5	multi server environment		1
PR 4	P05	aka			smart card, SIP	N4	1
	P06	authentication	N3, N5, N6,N7, N8, N11, N13, N14	Z5, Z7, Z8, Z9, Z14	SIP, smart card	N2, N4, N15, Z3	1
	P07	aaka		Z5, Z6, Z7	SIP		1
PR 5	P08	aaka			SIP	N4,	1
	P09	aaka	N2, N4, N14	Z5, Z7, Z8, Z9	SIP		1
PR 6	P10	authentication	N5, N6, N7	Z5, Z8	SIP	N2, N7, N8, Z9, Z7	1
	P11	authentication	N3, N5, N6, N7, N8	Z5, Z7, Z8, Z9	SIP	N2, N4, N14	1
PR 7	P12	authentication			network	N4	1
	P13	authentication		Z5, Z7	network		1
PR 8	P14	aaka	N6, N9	Z7	VoIP		1
PR 9	P15	authentication	N13	Z5, Z22, Z23	wireless mesh networks		1
PR 10	P16	authentication	N4, N8	Z5, Z7	mobile network		1
PR 11	P17	aka			smart card	N2, N10	1

	P18	aka	N11	Z3, Z5, Z7	mobile network		1
PR 12	P19	authentication			multi server environment, smart card	Z7, Z8, N3, N4	1
	P20	authentication	N3, N4, N5, N7	Z3, Z5	multi server environment, smart card	Z7, Z11	1
	P21	authentication	N5, N7, N3, N4, N8	Z7, Z11	multi server environment, smart card		1
PR 13	P22	aka		Z7	wireless networks	N4, Z3	1
	P23	aka	N4	Z7, Z3	wireless networks		1
PR 14	P24	aka			wireless mobile networks	N12	1
	P25	aaka	N12		wireless mobile networks		1
PR 15	P26	authentication	N4, N5, N13	Z3	RFID	N5, Z7	1
	P27	authentication	N2	Z5, Z7, Z12, Z13	low end devices, RFID	N4, Z3	1
PR17	P 28	aka	N2,N4, N5, N8, N11	Z7	smart card		1
PR18	P29	aka	N3, N4, N5, N7	Z3, Z5, Z7, Z11	network	N2	1
PR19	P30	authentication	N4, N5, N7	Z5, Z3, Z12	RFID		1
	P31	authentication	N5, N7, N8, N13	Z3, Z5,Z14	RFID	N3, N4, Z7, Z11	1
	P32	authentication	N4, N5, N8		RFID	N13	1
	P33	authentication	N4, N5, N8	Z12	RFID	N13	1
	P34	authentication	N5, N9	Z23	RFID	N4, N8, N13, Z3, Z5, Z7	1
	P35	authentication	N4, N5		RFID	N8, N13	1
PR 20	P36	authentication	N3, N5, N6, N7	Z5	wireless networks		1
PR21	P37	aka	N1, N2, N5, N6, N10, N11, N14	Z3, Z5	multi server environment, smart card	N3, N4, N8, N13, N15	2

	P38	aaka	N2, N3, N5, N6, N7, N15	Z5, Z6, Z7, 14	multi server environment	N4, N14	1
	P39	authentication	N2, N4, N5, N6, N7	Z5	network	N14	1
	P40	authentication	N2, N4, N5, N6, N7	Z14	network, smart card	N8, N14, Z3, Z5	2
	P41	authentication	N2, N4,N5, N6, N7	Z5	network	N14	1
	P42	authentication	N2, N4, N5, N6, N7	Z5	network	N14	1
	P43	authentication	N2, N4, N5, N6, N7		network	N14	1
	P44	authentication	N2, N7, N14	Z3, Z14	multi server environment, smart card	N3, N4, N5, N15, Z5, Z7, Z11	1
	P45	authentication	N2, N4, N5, N7	Z5	multi server environment		1
	P46	authentication	N2, N7	Z5	multi server environment, smart card	N4, N5, N15	1
	P47	aka	N2, N3, N7	Z5, Z14	multi server environment, smart card	Z7, N4, N5, N14	1
PR22	P48	authentication	N2, N4, N5, N7, N8, N10, N15, N16, N17	Z3, Z5, Z8	network, smart card	N14	2
	P49	authentication	N2, N7, N8, N10, N14		network, smart card	N4, N5, N15	2
	P50	authentication	N3, N5		wireless sensor networks, smart card	N2,N4, N7, 19, N14, N15, N16, N17, N27, Z3, Z5, Z8, Z17	2
	P51	authentication	N2, N4,N5, N7, N14	Z5, Z8	wireless sensor networks, smart card	N15, N16, N17, Z3	1
	P52	authentication	N2, N4,N5, N7, N14, N15	Z8	wireless sensor networks, smart card	N16, N17, Z3, Z5	2
	P53	authentication	N2, N4, N5, N7	Z5, Z8	multi server environment, smart card	N14, N15, N16, N17 Z3	1
PR23	P54	authentication	N13, N15		network, smart card	N1, N2, N4, N5, N8, N14	1
	P55	authentication	N1, N2, N4, N5, N8, N13, N14, N15		network, smart card		1

	P56	authentication	N5, N8, N13		network, smart card	N1, N2, N4, N14, N15	1
	P57	authentication	N1, N2, N4, N5, N8, N13, N15		network, smart card	N14	1
	P58	authentication	N1, N2, N4, N13		network, smart card	N5, N8, N14, N15	1
PR24	P59	aaka			wireless sensor networks		1
	P60	authentication	N2, N5, N7, N15	Z5	wireless sensor networks, smart card	Z3, N4, N14, N18, N19	2
	P61	authentication	N4, N18, N5, N7		wireless sensor networks, smart card	N2, N13, N14, N15, N27, N19, Z3, Z5	2
	P62	authentication	N2, N7, N18		wireless sensor networks, smart card	N4, N5, N13, N14, N15, N19, N27, Z3, Z5, Z17	2
	P63	authentication	N4, N7		wireless sensor networks, smart card	Z3, Z5, N2, N3, N5, N14, N15, N18, N19	2
	P64	authentication	N5, N7, N18	Z5	wireless sensor networks, smart card	Z3, N2, N4, N13, N14, N15, N19, N27	1
	P65	aaka	N4, N5, N7, N15, N18	Z5	wireless sensor networks, smart card	Z3, N2, N14, N19	1
PR25	P66	aaka	N2, N4, N6, N8, N13, N14, N18, N20, N21, N22	Z3, Z5, Z6, Z7	multimedia network		1
	P67	aka	N4, N20	Z7, Z6	network	N2, N6, N8, N13, N14, N18, N21, N22, Z3, Z5	1
	P68	aka			network	N2, N4, N6, N8, N13, N14, N18, N20, N21, N22, Z3, Z5, Z6, Z7	1
	P69	aka	N4	Z6, Z7	multi server environment	N2, N6, N8, N13, N14, N18, N20, N21, N22, Z3, Z5	1
	P70	aka	N12, N22, N26	Z6, Z7, Z26	network	N2, N4, N6, N8, N13, N14, N18, N20, N21, N25, Z3, Z5, Z7, Z8	1
	P71	aka	N22	Z6, Z7	network	N2, N4, N6, N8, N13, N14, N18, N20, N21,	1

						Z3, Z5	
PR26	P72	aaka	N5	Z5, Z8,	network		1
PR27	P73	authentication	N4, N5, N13	Z7, Z12, Z13, Z8	RFID		1
	P74	authentication	N13	Z7, Z13	RFID	Z12, Z8, N4, N5	1
	P75	authentication	N4	Z13	RFID	Z7, Z12, Z8, N5, N13	1
	P76	authentication	N4, N13	Z7, Z13	RFID	Z12, Z8, N5	1
	P77	authentication	N4, N5, N13	Z7, Z12, Z13	RFID	Z8	1
	P78	authentication	N5	Z7, Z13	RFID	Z12, Z8, N4, N13	1
	P79	authentication	N3, N5	Z7, Z12, Z13	RFID	N4, N13	1
	P80	authentication	N5, N13		RFID	Z12, Z13, Z8, N4	1
	P81	authentication		Z7	RFID	Z7, Z12, Z13, Z8, N4, N5	1
	P82	authentication	N5	Z7, Z12, Z13, Z8	RFID	N4, N13	1
PR28	P83	authentication	N4, N13	Z5, Z7, Z12, Z13	RFID		1
PR29	P84	authentication		Z5, Z7	RFID	Z12, N13	1
	P85	authentication		Z5, Z7, Z12	RFID	N13, Z3	1
PR30	P86	aaka		Z3, Z7	wireless mesh networks		1
PR31	P87	authentication	N3		SIP		1
	P88	aka			network	N3	1
PR32	P89	authentication	N2, N4, N5, N6, N11, N20	Z7	client-client, network		1
	P90	aka	N5, N6, N11, N20	Z7	network	N2, N4	1
	P91	aka	N2, N5, N6, N11, N20	Z7	network	N4	1
	P92	aka	N2, N4, N5, N6, N11, N20	Z7	network, smart card		1

	P93	aka	N2, N5, N6, N11, N20	Z7	network	N4	1
	P94	aka	N5, N6, N11, N20	Z7	network	N2, N4	1
PR33	P95	aka	N4		network		1
	P96	aka			network	N4	1
PR34	P97	authentication	N2,N4, N5, N6, N7, N15	Z3, Z5, Z7, Z9, Z14	SIP, smart card		1
	P98	aka	N5, N6, N7, N8, N11, N13	Z5, Z7, Z9, Z14	VoIP, SIP, smart card	N2,N4, N14, N15, Z3	1
	P99	aka	N2,N5, N6, N7, N15	Z5, Z7, Z9, Z14	SIP, smart card	N4, Z3,	1
	P100	authentication	N2, N5, N6, N7, N8, N14, N15	Z5, Z7, Z9, Z14	SIP, smart card	N4, Z3	1
PR35	P101	aaka	N4, N5, N7, N8, N13, N14, N15, N23, N19, N24	Z3, Z5, Z17, Z18	wireless sensor networks		1
	P102	aaka	N4, N5, N7, N13, N14, N19, N24	Z5, Z17, Z18	wireless sensor networks, smart card	Z3, N8, N15, N23	1
PR36	P103	authentication	N5, N8	Z5, Z17	wireless networks		1
PR37	P104	authentication	N5, N8	Z5, Z22	wireless networks		1
PR38	P105	authentication		Z5, Z16, Z17	wireless networks, RFID		1
PR39	P106	aaka	N4, N9, N15	Z3, Z5	mobile network, smart card		1
	P107	authentication		Z3, Z5	mobile network	N4	1
	P108	authentication		Z5	mobile network	Z3, N4	1
PR40	P109	authentication	N4, N5, N13	Z5, Z7, Z23, Z24	RFID	Z3	1
	P110	authentication			RFID	Z3, Z5, Z7, Z23, Z24	1
	P111	authentication		Z7	RFID	Z3, Z5, Z23, Z24	1
	P112	authentication		Z5	RFID	Z3, Z7, Z23, Z24	1

	P113	authentication		Z5, Z7	RFID	N4, N13, Z3, Z23, Z24	1
PR41	P114	aka	N2, N3, N4, N5, N8, N14, N21		mobile network		1
	P115	aka	N2, N5, N8, N14		mobile network	N3, N4, N13	1
	P116	aka	N2, N5, N8, N14		network	N4	1
	P117	aka	N2, N3, N4, N5, N14		network	N8	1
PR42	P118	authentication	N13	Z3	RFID		1
	P119	authentication			RFID	N13, Z3	1
PR44	P120	authentication	N3, N4, N5, N11, N14, N24, N26	Z3, Z5, Z7, Z13	RFID	N2, N7, N13	1
	P121	authentication	N3, N4, N13	Z5, Z7, Z13	RFID	N2,N5, N7, N11, N14, N24	1
	P122	authentication	N4	Z5, Z13	RFID	N2,N3, N5, N13, N14, N24	1
	P123	authentication	N3	Z5, Z13	RFID	N2,N4, N5,N11, N13, N14, N24, Z7	1
	P124	authentication	N2,N3, N4, N13, N14, N24	Z5	RFID	N5, Z13	1
PR45	P125	authentication	N2, N4, N5, N14	Z5, Z14	wireless networks, smart card	Z3, Z7	1
	P126	authentication		Z14	wireless networks	N2, N4, N5, N14, Z3, Z5, Z7	1
	P127	authentication	N7, N14	Z14	multi server environment, smart card	N3, N4, N5, N15, Z3, Z5, Z7	1
PR46	P128	aka		Z6, Z7	network	N4, N14	1
PR47	P129	authentication	N2,N4, N5, N8, N9		network	N9	1
	P130	authentication	N5, N9		network	N2,N4, N8	1
	P131	authentication	N4, N5, N9		network	N2,N8	1
PR48	P132	authentication	N2, N4, N5, N14		network		1
	P133	authentication	N5		network	N2, N4, N14	1

	P134	authentication	N2, N4, N5, N14		network		1
PR49	P135	authentication	N2, N4, N5, N10	Z5	network, smart card		2
	P136	authentication	N2, N5, N10		network, smart card	N4, Z5	2
PR50	P137	aka			network	N11, N25	1
	P138	aka	N11, N12, N25	Z7	network		1
PR51	P139	aaka	N4, N5, N7, N14, N24, N26	Z3, Z5, Z7	mobile network		1
	P140	aaka	N7, N14	Z5	mobile network	N4, N5, N24, N26, Z3, Z7	1
	P141	aaka	N4, N7, N14	Z5	mobile network	N5, N24, N26, Z3, Z7	1
	P142	authentication	N4, N7, N14, N24	Z5	mobile network	N5, N26, Z3, Z7	1
PR52	P143	authentication	N4, N8, N12, N25, N26	Z6, Z7, Z8, Z9, Z26	network		1
	P144	aka	N4, N8, N12, N26	Z6, Z7, Z8, Z26	network	N25	1
	P145	aka	N4, N8, N12, N25, N26	Z6, Z7, Z8, Z26	network		1
	P146	aka	N8, N26	Z6, Z7, Z26	network	N4, N25, Z8	1
	P147	aka	N4, N8, N12, N26	Z6, Z7, Z26	network	N25, Z8	1
	P148	authentication	N4, N8, N12, N26	Z6, Z7, Z8,Z26	network	N25	1
	P149	aka	N4, N8, N26	Z6, Z7, Z26	network	N12, N25, Z8	1
	P150	aka	N4, N12, N26	Z6, Z7, Z8,Z26	network	N8, N25	1
	P151	aka	N4, N8, N12, N25, N26	Z6, Z26	network	N25, Z7, Z8	1
	P152	aka	N4, N12, N26	Z6, Z7, Z26	network	N8, N25, Z8	1
	P153	aka	N4, N8, N12	Z6, Z7, Z8,Z26	network	N25, N26	1
	P154	aka	N4, N8, N12	Z6, Z7, Z8, Z26	network	N25, N26	1
	P155	aka	N4, N8, N12, N26	Z6, Z7, Z8,Z26	network	N25	1
	P156	aka	N4, N8, N12, N26	Z6, Z7, Z8, Z26	network	N25	1
	P157	aka	N4, N8, N12, N26	Z6, Z7, Z8,Z26	network	N25	1

	P158	authentication	N4, N8, N12	Z6, Z8, Z26	network	N25, N26, Z7	1
PR53	P159	authentication	N2, N4, N5, N8, N15	Z3, Z5, Z7, Z8, Z9, Z14, Z26	multi server environment		1
	P160	aaka	N2, N3, N4, N5, N10, N11, N14, N15	Z14	multi server environment	Z3, Z5, N8	1
	P161	authentication	N8	Z5, Z14	network, smart card	N2, N4, N5, Z3	2
	P162	aaka	N3, N5, N10, N11, N13	Z5, Z7, Z14	multi server environment, smart card	N2, N4, N8, N14, N15, Z3	2
PR54	P163	authentication	N2,N4, N5, N7, N8, N13, 21	Z3, Z4, Z5, Z8	wireless networks		1
	P164	authentication	N2,N4, N5, N7, N8	Z5, Z8	multi server environment, mobile networks	N13, N14, Z3, Z4	1
	P165	authentication	N2,N4, N5, N7, N8	Z3, Z5, Z8	wireless networks	N13, N14, Z4	1
PR55	P166	authentication	N2,N4, N5, N8, N13, N15, N18		multi server environment		1
	P167	authentication	N2	Z3, Z5	multi server environment	N4, N5, N15	1
PR56	P168	authentication	N3, N4, N5, N14, N15	Z5, Z17	wireless sensor networks		1
	P169	authentication	N5, N15	Z5, Z17	wireless sensor networks	N3, N4, N14	1
	P170	authentication	N5, N6, N7, N11, N13, N20	Z5, Z8,Z17	network, smart card	N2, N3, N4, N5, N10, N12, N14, N15, N18, Z3, Z7	2
	P171	authentication	N2, N3, N5, N6, N7, N11, N13, N14, N15, N18, N20	Z3, Z5, Z8, Z17	network, smart card	N4, N5, N12, N18, Z7	2
	P172	authentication	N4, N5, N15		wireless sensor networks	N3, N10, N13, N14, N27, Z5, Z17	1
PR57	P173	authentication	N2, N18	Z8	network		1
	P174	authentication			network	N2, N18, Z8	1

PR58	P175	authentication	N2, N3, N4, N5, N6, N7, N12, N13, N14, N15, N18	Z3, Z5, Z7	network, smart card		1
	P176	authentication	N2, N3, N6, N7, N15	Z3, Z5, Z7	network, smart card	N4, N5, N12, N13, N14, N18	2
	P177	authentication	N2, N3, N5, N6, N7, N12, N15	Z3, Z5, Z7	network, smart card	N4, N13, N14, N18	2
	P178	authentication	N2, N3, N4, N5, N6, N7, N14	Z3, Z5	network	Z7, N12, N13, N15, N18	1
	P179	authentication	N2, N5, N6, N7, N13, N14, N15	Z3, Z5	network, smart card	Z7, N3, N4, N12, N18	1
	P180	authentication	N4, N5, N6, N7, N11, N12, N13, N15, N18	Z3	network, smart card	Z5, Z7, N2, N3, N10, N14	1
	P181	authentication	N5, N6, N7, N11, N12, N13, N15, N18	Z3, Z5	network, smart card	Z7, N2, N3, N4, N10, N14	2
PR59	P182	aaka	N7, N9, N13		wireless networks		1
PR60	P183	authentication		Z5, Z7	radio network		1
PR61	P184	authentication	N4, N5, N8	Z3, Z5, Z7	mobile network		1
	P185	authentication	N5		wireless networks	Z3, Z5, Z7, N8	1
	P186	authentication	N5		wireless networks	Z3, Z5, Z7, N8	1
PR62	P187	authentication	N13, N27	Z5,	wireless sensor networks		1
	P188	authentication	N27		wireless sensor networks	N13, Z5	2
	P189	aaka	N13, N27	Z5	wireless sensor networks		2
	P190	authentication	N13	Z5	wireless sensor networks	N27	1
PR63	P191	aaka	N8, N13	Z5,	mobile network		1
PR64	P192	authentication	N2, N4, N5, N14	Z3, Z5, Z7, Z14	mobile network		1
	P193	authentication	N4, N5	Z5	wireless network	N2, N14, Z3, Z7, Z14	1
	P194	authentication			mobile network	N2, N4, N5, N14, Z3, Z5, Z7, Z14	1

	P195	authentication	N2, N4, N14	Z3, Z5, Z7, Z14	wireless network	N5	1
PR65	P196	aka	N2, N5, 15	Z3, Z5, Z6, Z7, Z8	network		1
PR66	P197	authentication	N4, N14, N15	Z3	network		1
PR67	P198	authentication	N2,N4, N5, N14, N15	Z3, Z5, Z6, Z7	mobile network		1
	P199	authentication	N2,N4, N5, N15	Z5, Z3	network, smart card	N13, N14	1
	P200	aaka	N5	Z5	network	N2,N4, N13, N14, N15, Z3	1
	P201	aaka	N2,N5, N14		mobile network	N4, N13, N15, Z5, Z3	1
PR68	P202	authentication	N3, N4, N5, N15	Z5, Z7, Z9	multi server environment, smart card		1
	P203	authentication	N5, N11, N13, N14, N15	Z3, Z14	multi server environment, smart card	Z5, Z7, N2, N3, N4, N8	1
PR69	P204	authentication	N3, N4, N5, N14	Z5, Z7, Z14	multi server environment		1
	P205	authentication		Z14	wireless network, smart card	Z3,Z5, Z7, N2,N3, N4, N5, N14	1
	P206	aaka		Z5, Z7, Z14	multi server environment	N2,N3, N4, N5, N14	1
PR70	P207	authentication	N2, N4, N5, N7, N8, N14	Z3, Z5, Z7, Z8	SIP		1
	P208	authentication	N2, N5, N7, N8, N20	Z3, Z6, Z7, Z8	SIP	N14, Z5	1
	P209	aaka	N4, N5, N8	Z5, Z7, Z8	SIP	N2, N7, N14, Z3	1
	P210	aka	N4, N5, N7, N20	Z5, Z6, Z7, Z8	SIP	N2, N8, N14	1
	P211	authentication	N2, N4, N5, N7, N8	Z5, Z7	SIP	N14, Z3	1
	P212	aka	N2, N4, N5, N7, N8, N20	Z5, Z6, Z7, Z8	SIP	N14, Z3	1
PR71	P213	authentication	N2, N3, N4, N5, N13, N15, N18	Z3, Z4, Z5	network		1
	P214	authentication		Z3, Z5	network, smart card	N2, N3, N4, N5, N13,	1

						N15, N18, Z4	
	P215	authentication		Z3, Z5	network, smart card	N2, N3, N4, N5, N13, N15, N18, Z4	1
PR72	P216	aaka	N2, N4, N5, N7, N10, N13, N14, N24	Z3, Z5, Z3	network		1
	P217	authentication			network	Z5, N2, N4,	1
PR73	P218	authentication	N2, N3, N4, N5, N8, N11, N13, N14, N15	Z3, Z5, Z7	multi server environments		1
	P219	authentication	N3, N5, N8, N11, N13, N14, N15	Z3, Z5	multi server environments	N2, N4, Z7	1
	P220	authentication	N5, N11, N13, N14, N15	Z3, Z5	multi server environments, smart card	N2, N3, N4, N8, Z7	2
	P221	authentication	N2, N5, N11, N13, N14, N15	Z5	multi server environments	N3, N4, N8, Z3, Z7	1
	P222	authentication	N5, N11, N13, N15	Z5	multi server environments	N2, N3, N4, N8, N14, Z3, Z7	1
	P223	authentication	N3, N5, N8, N11, N13, N15, N18	Z5, Z14, Z8	multi server environments	N2, N4, N14, Z3, Z7	1
PR74	P224	authentication	N2, N3, N4, N5, N8, N11, N13, N14, N15	Z3, Z5	SIP, smart card		1
	P225	authentication	N3, N4, N5, N8, N11, N13, N14, N15	Z5	SIP, smart card	N2, Z3	1
	P226	aka	N3, N4, N5, N8, N11, N13, N14, N15	Z5	SIP, smart card	Z3	2
	P227	authentication	N2, N5, N11, N13, N14, N15	Z5	SIP, smart card	N3, N4, N8, Z3	1
PR75	P228	authentication	N2, N3, N4, N5, N8, N14	Z5	network, smart card		2
	P229	authentication	N3, N4, N5, N8	Z5, Z7	network, smart card	N2, N14, N15, Z3, Z8	2
PR76	P230	aaka	N2, N3, N4, N5, N10, N11, N14	Z3, Z5, Z7	network, smart card		2

	P231	authentication	N2, N3, N4, N5, N10, N11, N14	Z5, Z7	network, smart card	N2, N4, N10, N14, Z3	1
PR77	P232	aka	N2, N3, N4, N5, N8, N10, N11, N14, N15	Z3, Z5	multi server environment, smart card		2
PR78	P233	authentication	N4, N5, N9	Z3, Z5, Z7, Z23	RFID		1
	P234	authentication	N4, N5, N9	Z3, Z7, Z23	RFID	Z5	1
	P235	authentication	N4, N5, N9	Z3, Z5, Z7, Z23	RFID		1
PR79	P236	authentication	N4, N13	Z3	RFID		1
	P237	authentication			RFID	N4, N13, Z3	1
PR80	P238	authentication	N4, N5	Z3	RFID		1
	P239	authentication			RFID	N4, N5, Z3	1
	P240	authentication	N5	Z3	RFID	N5	1
	P241	authentication			RFID	N4, N5, Z3	1
	P242	authentication	N4, N5		RFID	Z3	1
PR81	P243	aka			mobile network	N4, N8	1
	P244	aka			network	N4, N8	1
	P245	aka			network	N4	1
PR83	P246	aka	N14, N15	Z3, Z5, Z7, Z8	wireless network, smart card		1
	P247	authentication	N14	Z5, Z7	network	N15, Z3, Z8	1
PR84	P248	aaka	N2, N7, N13, N26	Z3, Z5	network, smart card		1
	P249	authentication	N26	Z3, Z5	network, smart card	N2, N7, N13, Z3	2
	P250	authentication	N13, N26	Z5	network, smart card	N2, N7, Z3	1
PR85	P251	authentication	N2, N4, N5, N7, N18, N20	Z5, Z7, Z8	network, smart card		2
	P252	aaka	N2,N4, N5, N7, N18, N20	Z5, Z7, Z8	network		2
	P253	authentication	N4, N5, N7, N18	Z5	network, smart card	N2, N20, Z7, Z8	1

	P254	aaka	N5, N7, N20	Z5, Z7, Z8	network	N2,N4, N18	1
	P255	authentication	N4, N5, N7, N18, N20	Z5, Z8	network, smart card	N2, Z7	1
PR86	P256	authentication			RFID	N6, N9, N13, Z3	1
	P257	authentication	N6, N9, N13	Z3	RFID		1
PR87	P258	authentication	N4	Z4, Z7	wireless networks		1
PR89	P259	authentication	N3, N4, N5, N6, N7, N14, N15	Z5, Z7	multi server enivronment, smart card		1
P90	P260	aka	N4, N14	Z7	network		1
P92	P261	authentication	N14, N23, N19		wireless sensor networks		2
	P262	authentication			wireless sensor networks	N14, N23, N19	2
PR93	P263	authentication	N2, N4, N5, N6, N7, N8, N20	Z5, Z7, Z8	SIP		1
PR94	P264	aka		Z7	network		1
PR95	P265	authentication		Z7	multi server environment	N2, N3, N4, N5, N10	1
PR96	P266	aka	N2, N4		network, mobile networks		1
PR98	P267	authentication	N2, N7, N4, N3, N5, N18, N13	Z3, Z5, Z7,Z8	network, smart card		1
PR99	P268	authentication	N2, N4, N5, N7, N8, N12	Z3	network	Z7	2
PR101	P269	authentication	N2, N3, N4, N14, N15	Z5	network, smart card		2
PR102	P270	authentication	N5, N7, N13	Z3, Z5	mobile network, smart card		1
PR103	P271	authentication	N2, N4, N13, N14, N23	Z3, Z5	wireless sensor		2

					networks		
PR104	P272	aka	N14		network	N2	1
PR105	P273	aaka	N4, N5, N9, N13, N14	Z5, Z3	multi server enviornment		1
PR106	P274	aka	N4, N5, N8	Z5, Z7	mobile network		1
	P275	aaka	N5, N8	Z5, Z7	mobile network	N4	1
PR108	P276	authentication	N3, N4, N5, N8	Z3, Z5	network		1
PR109	P277	authentication	N3, N4, N5	Z7, Z8, Z8	network, smart card		1
	P278	authentication	N5		multi server environment, smart card	N3, N4, Z7, Z8, Z8	1
PR110	P279	authentication	N5	Z3, Z5, Z7	RFID		1
PR112	P280	authentication	N2,N5, N6, N7, N8, N20	Z5, Z6, Z7, Z8	VoIP, SIP		1
	P281	aaka	N5, N6, N8, N20	Z5, Z6, Z7, Z8	SIP	N2, N7	1
	P282	authentication	N2,N5, N6, N8	Z5, Z6, Z7, Z8	SIP	N7, N20	1
	P283	authentication	N2,N5, N6, N8	Z5	SIP	N7	1
PR113	P284	authentication	N8	Z5	network		1
PR114	P285	aka		Z6, Z9, Z11	network		1
PR115	P286	aka		Z7	network		1
PR117	P287	authentication	N4, N15	Z3, Z5, Z11	mobile network, smart card		1
PR118	P288	aka	N2, N4, N5, N7, N8, N10	Z5, Z6, Z7, Z8, Z14	network, mobile network		1
	P289	aka	N5, N7, N8	Z5, Z6, Z7, Z8, Z14,	network, mobile networks	N2, N4, N10	1
PR119	P290	authentication	N5, N8, N13	Z5, Z7	RFID		1

PR120	P291	aaka	N2, N5, N7, N8, N10, N14	Z3, Z5, Z6, Z7	network		1
	P292	aka			network	Z3, Z5, Z6, Z7, N2, N5, N7, N8, N10, N14	1
	P293	aka			network	Z3, Z5, Z6, Z7, N2, N5, N7, N8, N10, N14	1
	P294	aka	N5, N10	Z5, Z6	network	Z3, Z7, N2, N7, N8, N14	1
	P295	aka			network, smart card	Z3, Z5, Z6, Z7, N2, N5, N7, N8, N10, N14	1
	P296	aka			network	Z3, Z5, Z6, Z7, N2, N5, N7, N8, N10, N14	1
	P297	authentication			network, smart card	Z3, Z5, Z6, Z7, N2, N5, N7, N8, N10, N14	1

Priloga C: Viri SLR

[1] T. Acar, M. Belenkiy, and A. Küpçü, “Single password authentication,” *Comput. Networks*, 2013.

[2] K. M. Ali and A. Al-Khalifah, “A comparative study of authentication methods for Wi-Fi networks,” in *Proceedings - 3rd International Conference on Computational Intelligence, Communication Systems and Networks, CICSyN 2011*, 2011.

[3] R. Amin and G. P. Biswas, “Design and Analysis of Bilinear Pairing Based Mutual Authentication and Key Agreement Protocol Usable in Multi-server Environment,” *Wirel. Pers. Commun.*, 2015.

[4] H. Arshad and M. Nikooghadam, “Security analysis and improvement of two authentication and key agreement schemes for session initiation protocol,” *J. Supercomput.*, vol. 71, pp. 3163–3180, 2015.

[5] H. Arshad and M. Nikooghadam, “An efficient and secure authentication and key agreement scheme for session initiation protocol using ECC.”

[6] R. Arshad and N. Ikram, “Elliptic curve cryptography based mutual authentication scheme for session initiation protocol,” *Multimed. Tools Appl.*, 2013.

[7] A. K. Awasthi, K. Srivastava, and R. C. Mittal, “An improved timestamp-based remote user authentication scheme,” *Comput. Electr. Eng.*, vol. 37, pp. 869–874, 2011.

[8] P. Battistello, J. Garcia-Alfaro, and C. Delétré, “Transaction-based authentication and key agreement protocol for inter-domain VoIP,” *J. Netw. Comput. Appl.*, 2012.

[9] L. Buttyán, L. Dóra, F. Martinelli, and M. Petrocchi, “Fast certificate-based authentication scheme in multi-operator maintained wireless mesh networks,” *Comput. Commun.*, 2010.

[10] J. Cao, M. De Ma, and H. Li, “Handover authentication between different types of eNBs in LTE networks,” *J. China Univ. Posts Telecommun.*, 2013.

[11] C. C. Chang, H. D. Le, and C. H. Chang, “Novel untraceable authenticated key agreement protocol suitable for mobile communication,” *Wirel. Pers. Commun.*, 2013.

[12] T.-Y. Chen, C.-C. Lee, M.-S. Hwang, J.-K. Jan, T.-Y. Chen, C.-C. Lee, M.-S. Hwang, and J.-K. Jan, “Towards secure and efficient user authentication scheme using smart card for multi-server environments Towards secure and efficient user authentication scheme using smart,” *J Supercomput*, vol. 66, pp. 1008–1032, 2013.

[13] Q. F. Cheng, C. G. Ma, and F. S. Wei, “Analysis and improvement of a new authenticated group key agreement in a mobile environment,” *Ann. des Telecommun. Telecommun.*, 2011.

[14] Q. Cheng and C. Ma, “Analysis and improvement of an authenticated multiple key exchange protocol,” *Comput. Electr. Eng.*, 2011.

[15] H. Y. Chien, “Combining Rabin cryptosystem and error correction codes to facilitate anonymous authentication with un-traceability for low-end devices,” *Comput. Networks*, 2013.

[16] H. Chien, “Cryptanalysis on RFID authentications using minimum disclosure approach,” in *Proceedings - 2013 8th Asia Joint Conference on Information Security, AsiaJCIS 2013*, 2013.

[17] H.-Y. Chien, “Provably Secure Authenticated Diffie-Hellman Key Exchange for Resource-Limited Smart Card,” vol. 19, no. 4, pp. 436–439, 2014.

[18] S. B. Choi and E. J. Yoon, “Cryptanalysis of Guo et al.’s three-party password-based authenticated key exchange (G-3PAKE) protocol,” in *Procedia Engineering*, 2011.

[19] J.-S. Chou, “An efficient mutual authentication RFID scheme based on elliptic curve cryptography,” *J Supercomput*, vol. 70, pp. 75–94, 2014.

[20] M. C. Chuang and J. F. Lee, “A lightweight mutual authentication mechanism for network mobility in IEEE 802.16e wireless networks,” *Comput. Networks*, 2011.

[21] M.-C. Chuang and M. C. Chen, “An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics,” *Expert Syst. Appl.*, vol. 41, pp. 1411–1418, 2014.

[22] A. K. Das and A. K. Das, “A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks.”

[23] A. K. Das and A. Goswami, “A robust anonymous biometric-based remote user authentication scheme using smart cards,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 27, pp. 193–210, 2015.

[24] B. David Deebak, “Secure and Efficient Mutual Adaptive User Authentication Scheme for Heterogeneous Wireless Sensor Networks Using Multimedia Client–Server Systems,” *Wirel. Pers. Commun.*

[25] B. D. Deebak, R. Muthaiah, K. Thenmozhi, and P. Swaminathan, “Evaluating Three Party Authentication and Key Agreement Protocols Using IP Multimedia Server–Client Systems,” *Wirel. Pers. Commun.*, 2014.

[26] Y. Ding, X. Zhou, Z. Cheng, and W. Zeng, “Efficient Authentication and Key Agreement Protocol with Anonymity for Delay Tolerant Networks,” *Wireless Personal Communications*. 2012.

[27] R. Doss, S. Sundaresan, and W. Zhou, “A practical quadratic residues based scheme for authentication and privacy in mobile RFID systems,” *Ad Hoc Networks*, 2013.

[28] R. Doss, W. Zhou, S. Sundaresan, S. Yu, and L. Gao, “A minimum disclosure approach to authentication and privacy in RFID systems,” *Comput. Networks*, 2012.

[29] D. N. Duc and K. Kim, “Defending RFID authentication protocols against DoS attacks,” *Comput. Commun.*, 2011.

[30] A. O. Durahim and E. Savaş, “A2-MAKE: An efficient anonymous and accountable mutual authentication and key agreement protocol for WMNs,” *Ad Hoc Networks*. 2011.

[31] M. S. Farash, “Security analysis and enhancements of an improved authentication for session initiation protocol with provable security,” *Peer-to-Peer Netw. Appl.*, 2014.

[32] M. S. Farash and M. A. Attari, “An efficient client–client password-based authentication scheme with provable security,” *J Supercomput*, vol. 70, pp. 1002–1022, 2014.

[33] M. S. Farash, M. A. Attari, R. E. Atani, and M. Jami, “A new efficient authenticated multiple-key exchange protocol from bilinear pairings,” *Comput. Electr. Eng.*, 2013.

[34] M. S. Farash, S. Kumari, and M. Bakhtiari, “Cryptanalysis and improvement of a robust smart card secured authentication scheme on SIP using elliptic curve cryptography,” *Multimed. Tools Appl.*, 2015.

[35] M. S. Farash, M. Turkanoví, S. Kumari, and M. Hölbl, “ARTICLE IN PRESS An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment,” *Ad Hoc Networks*, vol. 13, no. 000, pp. 52–1, 2015.

[36] A. Fu, G. Zhang, Y. Zhang, and Z. Zhu, “GHAP: An efficient group-based handover authentication mechanism for IEEE 802.16m networks,” *Wirel. Pers. Commun.*, 2013.

[37] A. Fu, G. Zhang, Z. Zhu, Y. Zhang, A. Fu, G. Zhang, Z. Zhu, and Y. Zhang, “Fast and Secure Handover Authentication Scheme Based on Ticket for WiMAX and WiFi Heterogeneous Networks,” *Wirel. Pers Commun*, vol. 79, pp. 1277–1299, 2014.

[38] A. Fu, Y. Zhang, Z. Zhu, Q. Jing, and J. Feng, “An efficient handover authentication scheme with privacy preservation for IEEE 802.16m network,” *Comput. Secur.*, 2012.

[39] P. Gope and T. Hwang, “Enhanced Secure Mutual Authentication and Key Agreement Scheme Preserving User Anonymity in Global Mobile Networks,” *Wirel. Pers. Commun.*, 2015.

[40] P. Gope and T. Hwang, “A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system,” *Comput. Secur.*, 2015.

[41] D. Guo, Q. Wen, W. Li, H. Zhang, and Z. Jin, “Analysis and Improvement of ‘Chaotic Map Based Mobile Dynamic ID Authenticated Key Agreement Scheme,’” *Wirel. Pers. Commun.*, vol. 83, pp. 35–48, 2015.

[42] M. H. Habibi and M. R. Aref, “Security and privacy analysis of song-mitchell RFID authentication protocol,” *Wirel. Pers. Commun.*, 2013.

[43] M. H. Habibi, M. R. Aref, M. H. Habibi, and M. R. Aref, “Attacks on Recent RFID Authentication Protocols,” *J Sign Process Syst*, vol. 79, pp. 271–283, 2015.

[44] S. K. Hafizul Islam and G. P. Biswas, “Design of improved password authentication and update scheme based on elliptic curve cryptography,” *Math. Comput. Model.*, 2013.

[45] D. He, M. Ma, Y. Zhang, C. Chen, and J. Bu, “A strong user authentication scheme with smart cards for wireless communications,” *Comput. Commun.*, 2011.

[46] M. Hölbl, T. Welzer, and B. Brumen, “An improved two-party identity-based authenticated key agreement protocol using pairings,” in *Journal of Computer and System Sciences*, 2012.

[47] W. Bin Hsieh and J. S. Leu, “A time and location information assisted OTP scheme,” *Wirel. Pers. Commun.*, 2013.

[48] C.-L. Hsu, Y.-H. Chuang, and C. Kuo, “A Novel Remote User Authentication Scheme from Bilinear Pairings Via Internet,” *Wirel. Pers. Commun.*, 2015.

[49] M. S. Hwang, S. K. Chong, and T. Y. Chen, “DoS-resistant ID-based password authentication scheme using smart cards,” *J. Syst. Softw.*, 2010.

[50] S. K. H. Islam and G. P. Biswas, “An improved pairing-free identity-based authenticated key agreement protocol based on ECC,” in *Procedia Engineering*, 2012.

[51] S. H. Islam and G. P. Biswas, “Design of Two-Party Authenticated Key Agreement Protocol Based on ECC and Self-Certified Public Keys,” *Wirel. Pers. Commun.*, 2015.

[52] S. H. Islam and G. P. Biswas, “A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem,” *J. Syst. Softw.*, 2011.

[53] P. Jiang, Q. Wen, W. Li, Z. Jin, and H. Zhang, “An anonymous and efficient remote biometrics user authentication scheme in a multi server environment,” *Front. Comput. Sci*, vol. 9, no. 1, pp. 142–156, 2015.

[54] Q. Jiang, J. Ma, G. Li, and L. Yang, “An efficient ticket based authentication protocol with unlinkability for wireless access networks,” *Wirel. Pers. Commun.*, 2014.

[55] S. Kalra and S. Sood, “Advanced remote user authentication protocol for multi-server architecture based on ECC,” *J. Inf. Secur. Appl.*, vol. 18, pp. 98–107, 2013.

[56] S. Kalra and S. K. Sood, “Advanced password based authentication scheme for wireless sensor networks,” *J. Inf. Secur. Appl.*, 2014.

[57] B. Kang, J. Han, and Q. Wang, “Cryptanalysis and improvement on an IC-card-based remote login mechanism,” in *ICCET 2010 - 2010 International Conference on Computer Engineering and Technology, Proceedings*, 2010.

[58] M. Karuppiah and R. Saravanan, “A secure remote user mutual authentication scheme using smart cards,” *J. Inf. Secur. Appl.*, vol. 19, pp. 282–294, 2014.

[59] S. U. Khan, C. Pastrone, L. Lavagno, and M. A. Spirito, “An Authentication and Key Establishment Scheme for the IP-Based Wireless Sensor Networks,” *Procedia Computer Science*. 2012.

[60] H. S. Kim, “Location-based authentication protocol for first cognitive radio networking standard,” *J. Netw. Comput. Appl.*, 2011.

[61] J. S. Kim and J. Kwak, “Improved secure anonymous authentication scheme for roaming service in global mobility networks,” *Int. J. Secur. its Appl.*, 2012.

[62] A. Kumar, P. Sharma, S. Chatterjee, and J. Kanta, “Journal of Network and Computer Applications A dynamic password-based user authentication scheme for hierarchical wireless sensor networks,” *J. Netw. Comput. Appl.*, 2012.

[63] C. Lai, H. Li, R. Lu, and X. (Sherman) Shen, “SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks,” *Comput. Networks*, 2013.

[64] C. Lee and Y. Lai, “Another Secure Anonymous Authentication Scheme for Roaming Service in Global Mobility Networks Another Secure Anonymous Authentication Scheme for Roaming Service in Global Mobility Networks Abstract,” *Rev. Lit. Arts Am.*

[65] T.-F. Lee, “Enhancing the security of password authenticated key agreement protocols based on chaotic maps,” *Inf. Sci. (Ny).*, 2015.

[66] C.-T. Li, C.-Y. Weng, C.-C. Lee, and C.-C. Wang, “ScienceDirect Secure User Authentication and User Anonymity Scheme based on Quadratic Residues for the Integrated EPRIS,” *Procedia - Procedia Comput. Sci.*, vol. 52, pp. 21–28, 2015.

[67] X. Li, B. Junguo Liao, B. Saru Kumari, B. Wei Liang, J. Liao, S. Kumari, W. Liang, F. Wu, and M. Khurram Khan, “A New Dynamic ID-Based User Authentication Scheme Using Mobile Device: Cryptanalysis, the Principles and Design,” *Wirel. Pers. Commun.*

[68] X. Li, J. Ma, W. Wang, Y. Xiong, and J. Zhang, “A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments,” *Math. Comput. Model.*, 2013.

[69] Y. P. Liao and C. M. Hsiao, “A novel multi-server remote user authentication scheme using self-certified public keys for mobile clients,” *Futur. Gener. Comput. Syst.*, 2013.

[70] Y. Lu, L. Li, H. Peng, and Y. Yang, “A secure and efficient mutual authentication scheme for session initiation protocol.”

[71] R. Martínez-Peláez, F. Rico-Novella, J. Forné, and P. Velarde-Alvarado, “Security Improvement of Two Dynamic ID-based Authentication Schemes by Sood-Sarje-Singh,” *J. Appl. Res. Technol.*, 2013.

[72] O. Mir and M. Nikooghadam, “A Secure Biometrics Based Authentication with Key Agreement Scheme in Telemedicine Networks for E-Health Services,” *Wirel. Pers. Commun.*, 2015.

[73] D. Mishra, “Design and Analysis of a Provably Secure Multi-server Authentication Scheme,” *Wirel. Pers. Commun.*

[74] D. Mishra, ·. Ashok, K. Das, S. Mukhopadhyay, D. Mishra, S. Mukhopadhyay, and A. K. Das, “A secure and efficient ECC-based user anonymity-preserving session initiation authentication protocol using smart card.”

[75] D. Mishra, A. Chaturvedi, and S. Mukhopadhyay, “Design of a lightweight two-factor authentication scheme with smart card revocation,” *J. Inf. Secur. Appl.*, 2015.

[76] D. Mishra, A. K. Das, A. Chaturvedi, and S. Mukhopadhyay, “A secure password-based authentication and key agreement scheme using smart cards,” *J. Inf. Secur. Appl.*, 2015.

[77] D. Mishra, A. K. Das, and S. Mukhopadhyay, “A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards,” *Expert Syst. Appl.*, 2014.

[78] S. R. Moosavi, E. Nigussie, S. Virtanen, and J. Isoaho, “An elliptic curve-based mutual authentication scheme for RFID implant systems,” in *Procedia Computer Science*, 2014.

[79] F. Moradi, H. Mala, and B. T. Ladani, “Security Analysis and Strengthening of an RFID Lightweight Authentication Protocol Suitable for VANETs,” *Wirel. Pers. Commun.*

[80] M. M. Morshed, A. Atkins, and H.-N. Yu, “An efficient and secure authentication protocol for RFID systems,” *International Journal of Automation and Computing*. 2012.

[81] L. Ni, G. L. Chen, J. H. Li, and Y. Y. Hao, “Strongly secure identity-based authenticated key agreement protocols in the escrow mode,” *Sci. China Inf. Sci.*, 2013.

[82] P. Nose, “Security weaknesses of authenticated key agreement protocols,” *Inf. Process. Lett.*, 2011.

[83] V. Odelu, @bullet Ashok, K. Das, @bullet Adrijit Goswami, A. K. Das, and A. Goswami, “An Effective and Robust Secure Remote User Authenticated Key Agreement Scheme Using Smart Cards in Wireless Communication Systems,” *Wirel. Pers. Commun.*

[84] V. Odelu, A. K. Das, and A. Goswami, “An efficient ECC-based privacy-preserving client authentication protocol with key agreement using smart card,” *J. Inf. Secur. Appl.*, 2015.

[85] X. Qi, W.-H. Liu, S.-B. Wang, N. Dong, and X.-Y. Yu, “Robust Password and Smart Card Based Authentication Scheme with Smart Card Revocation,” vol. 19, no. 4, pp. 418–424, 2014.

[86] X. Qian, X. Liu, S. Yang, and C. Zuo, “Security and Privacy Analysis of Tree-LSHB+ Protocol,” *Wirel. Pers Commun*, vol. 77, pp. 3125–3141, 2014.

[87] E. K. Ryu, H. S. Kim, and K. Y. Yoo, “KCI-resilient anonymous wireless link-layer authentication protocols,” *Math. Comput. Model.*, 2012.

[88] M. Safkhani, P. Peris-Lopez, J. C. Hernandez-Castro, and N. Bagheri, “Cryptanalysis of the Cho et al. protocol: A hash-based RFID tag mutual authentication protocol,” *J. Comput. Appl. Math.*, 2014.

[89] H. Shen, “New biometrics-based authentication scheme for multi-server environment in critical systems,” *J. Ambient Intell. Humaniz. Comput.*

[90] K. A. Shim, “A round-optimal three-party ID-based authenticated key agreement protocol,” *Inf. Sci. (Ny).*, 2012.

[91] S. K. Sood, A. K. Sarje, and K. Singh, “A secure dynamic identity based authentication protocol for multi-server architecture,” *J. Netw. Comput. Appl.*, 2011.

[92] D.-Z. Sun, J.-X. Li, Z.-Y. Feng, Z.-F. Cao, and G.-Q. Xu, “On the security and improvement of a two-factor user authentication scheme in wireless sensor networks,” *Personal and Ubiquitous Computing*. 2012.

[93] H. Tang and X. Liu, “Cryptanalysis of Arshad et al.’s ECC-based mutual authentication scheme for session initiation protocol,” *Multimed. Tools Appl.*, 2013.

[94] J. K. Teng, C. K. Wu, and C. M. Tang, “An ID-based authenticated dynamic group key agreement with optimal round,” *Sci. China Inf. Sci.*, 2012.

[95] J. L. Tsai, N. W. Lo, and T. C. Wu, “A new password-based multi-server authentication scheme robust to password guessing attacks,” *Wirel. Pers. Commun.*, 2013.

[96] H. Tu, N. Kumar, J. Kim, and J. Seo, “A strongly secure pairing-free certificateless authenticated key agreement protocol suitable for smart media and mobile environments,” *Multimed. Tools Appl.*, 2015.

[97] B. Wang and M. Ma, “A smart card based efficient and secured multi-server authentication scheme,” *Wirel. Pers. Commun.*, 2013.

[98] D. WANG and C. MA, “Cryptanalysis and security enhancement of a remote user authentication scheme using smart cards,” *The Journal of China Universities of Posts and Telecommunications*. 2012.

[99] D. Wang, N. Wang, P. Wang, and S. Qing, “Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity,” *Inf. Sci. (Ny).*, vol. 321, pp. 162–178, 2015.

[100] D. Wang and P. Wang, “On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions,” *Comput. NETWORKS*, vol. 73, pp. 41–57, 2014.

[101] F. Wen, W. Susilo, and G. Yang, “Analysis and Improvement on a Biometric-Based Remote User Authentication Scheme Using Smart Cards,” *Wirel. Pers. Commun.*, 2014.

[102] F. Wen, W. Susilo, and G. Yang, “A Secure and Effective Anonymous User Authentication Scheme for Roaming Service in Global Mobility Networks,” *Wirel. Pers Commun*, vol. 73, pp. 993–1004, 2013.

[103] F. Wu, B. Lili Xu, B. Saru Kumari, and B. Xiong Li, “An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks,” *Multimed. Syst.*

[104] □ Xu Chungen and Y. Yanjiong, “Off-Line Dictionary Attack on Password-Based Authenticated Key Exchange Protocols,” vol. 17, no. 6, pp. 468–472, 2012.

[105] K. Xue, P. Hong, and C. Ma, “A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture,” in *Journal of Computer and System Sciences*, 2014.

[106] H. Yang, B. Jianhua Chen, and B. Yuanyuan Zhang, “An Improved Two-Party Authentication Key Exchange Protocol for Mobile Environment,” *Wirel. Pers. Commun.*

[107] K.-H. Yeh, “A Provably Secure Multi-server Based Authentication Scheme,” *Wirel. Pers Commun*, vol. 79, pp. 1621–1634, 2014.

[108] K.-H. Yeh, “A lightweight authentication scheme with user untraceability,” *Yeh / Front Inf. Technol Electron Eng*, vol. 16, no. 4, pp. 259–271, 2015.

[109] K.-H. Yeh, K.-Y. Tsai, and J.-L. Hou, “Analysis and design of a smart card based authentication protocol,” *J. Zhejiang Univ. Sci. C*, 2013.

[110] X. Yi, L. Wang, D. Mao, and Y. Zhan, “An Gen2 Based Security Authentication Protocol for RFID System,” *Physics Procedia*. 2012.

[111] E. J. Yoon and K. Y. Yoo, “Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem,” *J. Supercomput.*, 2013.

[112] E. J. Yoon, K. Y. Yoo, C. Kim, Y. S. Hong, M. Jo, and H. H. Chen, “A secure and efficient SIP authentication scheme for converged VoIP networks,” *Comput. Commun.*, 2010.

[113] E. J. Yoon, K. Y. Yoo, S. S. Yeo, and C. Lee, “Robust deniable authentication protocol,” *Wirel. Pers. Commun.*, 2010.

[114] L. Zhang, Q. Wu, B. Qin, and J. Domingo-Ferrer, “Provably secure one-round identity-based authenticated asymmetric group key agreement protocol,” *Inf. Sci. (Ny).*, 2011.

[115] L. Zhang, F. Zhang, Q. Wu, and J. Domingo-Ferrer, “Simulatable certificateless two-party authenticated key agreement protocol,” *Inf. Sci. (Ny).*, 2010.

[116] Z. Zhang, Q. Qi, N. Kumar, N. Chilamkurti, H.-Y. Jeong, Z. Zhang, Q. Qi, N. Kumar, N. Chilamkurti, and H. <y Jeong, “A secure authentication scheme with anonymity for session initiation protocol using elliptic curve cryptography,” *Multimed Tools Appl*, vol. 74, pp. 3477–3488, 2015.

[117] T. Zhou and J. Xu, “Provable secure authentication protocol with anonymity for roaming service in global mobility networks,” *Comput. Networks*, 2011.

[118] H. Zhu, “Cryptanalysis and Improvement of a Mobile Dynamic ID Authenticated Key Agreement Scheme Based on Chaotic Maps,” *Wirel. Pers. Commun.*

[119] X. Zhuang, Y. Zhu, and C.-C. Chang, “A New Ultralightweight RFID Protocol for Low-Cost Tags: R ^{2} 2 AP,” *Wirel. Pers. Commun.*, 2014.

[120] B. D. Deebak, R. Muthaiah, K. Thenmozhi, and P. Swaminathan, “Analyzing three-party authentication and key agreement,” *Multimed Tools Appl*, 2015.

Univerza v Mariboru

Fakulteta za elektrotehniko,
računalništvo in informatiko
Smetanova ulica 17
2000 Maribor, Slovenija

FERI

IZJAVA O AVTORSTVU

Spodaj podpisani/-a **Matija Heričko**

z vpisno številko **E5016710**

sem avtor/-ica magistrskega dela z naslovom:

KLASIFIKACIJA VARNOSTNIH ZAHTEV ZA OVERITVENE PROTOKOLE - SISTEMATIČEN PREGLED LITERATURE

S svojim podpisom zagotavljam, da:

- sem magistrsko delo izdelal/-a samostojno pod mentorstvom (naziv, ime in priimek)

  doc. dr. Marko Hölbl

- so elektronska oblika magistrskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko magistrskega dela.
- soglašam z javno objavo elektronske oblike magistrskega dela v DKUM.

V Mariboru, dne 9.9.2015

Podpis avtorja/-ice:

Univerza v Mariboru

Fakulteta za elektrotehniko,
računalništvo in informatiko
Smetanova ulica 17
2000 Maribor, Slovenija

FERI

IZJAVA O USTREZNOSTI ZAKLJUČNEGA DELA

Podpisani mentor :

MARKO HÖLBL

(ime in priimek mentorja)

in somentor (eden ali več, če obstajata):

(ime in priimek somentorja)

Izjavljam (-va), da je študent

Ime in priimek: MATIJA HERIČKO

Vpisna številka: E50169710

Na programu: Informatika in tehnologije komuniciranja MAG

izdelal zaključno delo z naslovom:

KLASIFIKACIJA VARNOSTNIH ZAHTEV ZA OVERITVENE PROTOKOLE – SISTEMATIČEN PREGLED LITERATURE

(naslov zaključnega dela v slovenskem in angleškem jeziku)

CLASSIFICATION OF SECURITY REQUIREMENTS FOR AUTHENTICATION PROTOCOLS - A SYSTEMATIC LITERATURE REVIEW

v skladu z odobreno temo zaključnega dela, Navodilih o pripravi zaključnih del in mojimi (najinimi oziroma našimi) navodili.

Preveril (-a, -i) in pregledal (-a, -i) sem (sva, smo) poročilo o plagiatorstvu.

Datum in kraj: 9.9.2015, Maribor

Podpis mentorja:

Datum in kraj:

Podpis somentorja (če obstaja):

UNIVERZA V MARIBORU

Fakulteta za elektrotehniko, računalništvo in informatiko

IZJAVA O ISTOVETNOSTI TISKANE IN ELEKTRONSKE VERZIJE ZAKLJUČNEGA DELA IN OBJAVI OSEBNIH PODATKOV MAGISTRANTOV

Ime in priimek magistranta-tke: Matija Heričko

Vpisna številka:

Študijski program: INFORMATIKA IN TEHNOLOGIJE KOMUNICIRANJA

Naslov magistrskega dela: KLASIFIKACIJA VARNOSTNIH ZAHTEV ZA OVERITVENE PROTOKOLE - SISTEMATIČEN PREGLED LITERATURE

Mentor: Marko Hölbl

Somentor:

Podpisani-a Matija Heričko **izjavljam, da sem za potrebe arhiviranja oddal elektronsko verzijo zaključnega dela v Digitalno knjižnico Univerze v Mariboru. Magistrsko delo sem izdelal-a sam-a ob pomoči mentorja. V skladu s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovoljujem, da se zgoraj navedeno zaključno delo objavi na portalu Digitalne knjižnice Univerze v Mariboru.**

Tiskana verzija magistrskega dela je istovetna elektronski verziji, ki sem jo oddal za objavo v Digitalno knjižnico Univerze v Mariboru.

Zaključno delo zaradi zagotavljanja konkurenčne prednosti, varstva industrijske lastnine ali tajnosti podatkov naročnika:
ne sme biti javno dostopno do _____ **(datum odloga javne objave ne sme biti daljši kot 3 leta od zagovora dela).**

Podpisani izjavljam, da dovoljujem objavo osebnih podatkov vezanih na zaključek študija (ime, priimek, leto in kraj rojstva, datum magistriranja, naslov magistrskega dela) na spletnih straneh in v publikacijah UM.

Datum in kraj: Maribor, 09.09.2015

Podpis magistranta-tke:

Podpis mentorja
(samo v primeru, če delo ne sme biti javno dostopno):

Podpis odgovorne osebe naročnika in žig:
(samo v primeru, če delo ne sme biti javno dostopno)