VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2017 Jaroslav Bošeľa

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

AUTENTIZACE NULOVOU ZNALOSTÍ
ZERO KNOWLEDGE AUTHENTICATION

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Jaroslav Bošeľa**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Dzurenda**
SUPERVISOR

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Teleinformatika**
Ústav telekomunikací

Student: Jaroslav Bošeľa ***ID:*** 173617
Ročník: 3 ***Akademický rok:*** 2016/17

NÁZEV TÉMATU:

Autentizace nulovou znalostí

POKYNY PRO VYPRACOVÁNÍ:

V rámci bakalářské práce student nastuduje základní problematiku autentizačních protokolů na bázi nulové znalosti a provede jejich srovnání. Následně student zvolí jednu autentizační metodu a tu implementuje do autentizačního systému pro přístupové systémy, který bude využívat pro autentizaci mobilní telefony a počítač Raspberry Pi. Komunikace mezi zařízeními bude realizována pomocí technologie Bluetooth.

DOPORUČENÁ LITERATURA:

[1] HAJNÝ, J. Autentizace pomocí Zero-Knowledge protokolů. Crypto- world, 2008, roč. 2008, č. 9, s. 7-13. ISSN: 1801- 2140.

[2] Menezes, A. J., van Oorschot, P. C., Vanstone, S. A.: Handbook of Applied Cryptography, CRC Press, 1997, ISBN 0-8493-8523-7

Termín zadání: 1.2.2017 ***Termín odevzdání:*** 8.6.2017

Vedoucí práce: Ing. Petr Dzurenda
Konzultant:

doc. Ing. Jiří Mišurec, CSc.
předseda oborové rady

ABSTRAKT

Táto práca sa venuje autentizácií nulovou znalosťou , jej princípom a základným rozdelením. Ďalej sa práca hlavne zameriava na Zero–Knowledge protokoly, teda protokoloy, ktoré pracujú s nulovou znalosťou, ich analýzou,základným princípom a pojednáva aj o konkrétnych protokoloch a popisuje ich výhody a vlastnosti. Ďalej sa práca zaobera technológiou Bluetooth a Bluetooth Low Energy, ich špecifikácie, využitie služieb a profilov pri prenose základných dát medzi počítačom Raspberry Pi 2 a Android mobilným telefónom. Praktická časť práce sa venuje implementácií Gatt Serveru pre komunikáciu BLE na Raspberry Pi 2 a developmentom základnej aplikácie pre BLE komunikáciu medzi Raspberry Pi 2 a smartfónom fungujúcom na systéme Android.

KĽÚČOVÉ SLOVÁ

autentizácia, Protokoly s nulovou znalosťou, Fiat-Shamir, Schnorr, Guillou-Quisquarter, Bluetooth Low Energy, Raspberry Pi, Android

ABSTRACT

This thesis looks to authentication, principle and basic divison. Another part of thesis looks closely to Zero–Knowledge protocols, which protocols with zero information, their analysis and base elements, types of this protocols and their advantages and disadvantages and attributes.Thesis also presents technology Bluetooth and Bluetooth Low Energy, specification of this technology usage of Bluetooth Services in transmission mode of simple data between computer Raspberry Pi 2 and mobile phone. The practical part of thesis works on implementation of Gatt Server for BLE transfer on Raspberry Pi 2 and also focuse on simple app development on smartphone based on Android system for BLE transfer between smartphone and Raspberry Pi 2.

KEYWORDS

authentication, Zero–Knowledge protocols,Fiat-Shamir, Schnorr, Guillou-Quisquarter, Bluetooth Low Energy, Raspberry Pi, Android

BOŠEĽA, Jaroslav. *Autentizace nulovou znalostí*. Brno, 2017, 41 s. Bakalárska práca. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedúci práce: Ing. Petr Dzurenda

VYHLÁSENIE

Vyhlasujem, že som svoju bakalársku prácu na tému „Autentizace nulovou znalostí“ vypracoval(a) samostatne pod vedením vedúceho bakalárskej práce, využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor(ka) uvedenej bakalárskej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto bakalárskej práce som neporušil(a) autorské práva tretích osôb, najmä som nezasiahol(-la) nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý(-á) následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákoníka Českej republiky č. 40/2009 Sb.

Brno ....

podpis autora(-ky)

POĎAKOVANIE

Rád by som poďakoval vedúcemu semestrálnej práce pánovi Ing. Petrovi Dzurendovi, za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Brno ....

podpis autora(-ky)

Faculty of Electrical Engineering
and Communication
Brno University of Technology
Purkynova 118, CZ-61200 Brno
Czech Republic
http://www.six.feec.vutbr.cz

POĎAKOVANIE

Výzkum popsaný v tejto bakalárskej práci bol realizovaný v laboratóriách podporených projektom SIX; registračné číslo CZ.1.05/2.1.00/03.0072, operačný program Výzkum a vývoj pro inovace.

Brno ....

podpis autora(-ky)

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OBSAH

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ÚVOD

V dnešnej dobe veľkoobjemovej dátovej prevádzky, rôznych elektronických služieb a činností je potrebné vo virtuálnom svete overovanie identity a autorizácie užívateľov k týmto službám a aplikáciam. S každodennou autentizáciou sa stretávame praktický všade napr.overnie platnosti šalinkarty a vlastníka na MHD, čipové karty na prístup do rôznych školských alebo pracovných priestorov a rovnako sa stretávame s digitálnym overovaním u veľkého mňožstva aplikácií a najmä v samotnom Intenete.

Za zmienku internetových služieb a aplikácií určite stoja cloudové služby, bankové služby–Internet banking, emailové služby, sociálne siete alebo rôzne dátové úložiska, kde nám systém overovania, certifikáty a autentizácia zabezpečuje ochranu osobných dát pred neželanými osobami a nevyžiadaným prístupom. Pri jednoduchých autentizačných sytémoch je nutné aby overovateľ poznal indentitu overovaného užívateľa , ktorú využije na verifikáciu pomocou daných verifikačných parametrov alebo faktorov. Behom jednoduchej autentizácie je útočník schopný heslo odchytiť a zneužiť preto sa pre dôležité služby a aplikácie ako napr. bankové, firemné aplikácie, zadávanie citlivých údajov a pod. používa viacprvkové overenie napr. overenie znalosťou(heslo) a zároveň aj vygenerovaným tokenom na klientskom zariadení.

Mnoho autentizačných protokolov vyžaduje veľké množstvo informácií behom procesu verifikácie , tým narastá riziko odchytenia alebo rozšifrovania takýchto informácií a je komplikované zabezpečiť ochranu týchto verifikačných informácií. Podobné problémy dokážu riešiť autentizačné systémy, ktoré sú založené na autenzizácií nulovou znalosťou, známe tiež ako protokoly nulovou znalosťou (Zero Knowledge Protocols). Protokoly nulovou znalosťou chránia súkromie užívateľov tým, že počas verifikácie neuvoľňujú nadbytočné informácie a protokol zisťuje len to, či overovaný užívateľ pozná tajnú informáciu a to len pomocou jedného bitu tejto informácie. Počas procesu verifikácie teda nie je vyzradené tajomstvo a tak nie je útočník schopný získať žiadne dôležité informácie.

Práca sa v teoretickej časti najprv zaoberá autentizáciou, prinicípmi autentizácie v kapitole 1.1 , ďalej je to autentizácia s nulovou znalosťou, protokoly s nulovou znalosťou a ich porovnanie s klasickou autentizáciou 1.2 . Neskôr je špecifikovaná technológia Bluetooth kapitola1.3 a jej podtechnológia Bluetooth Low Energy (BLE) 1.4 , ich opis, výhody a porovnanie, využitie Bluetooth Low Energy na zachytávanie a odosielanie jednoduchých správ, GATT profil, využitie Android telefónu na príjem alebo odoslanie jednotlivých správ pomocou Android aplikácie a popis systému Android 1.5, na konci sa práca venuje popisu minipočítača Raspberry Pi 2 1.6. Praktická časť práce sa zaoberá výberom protokolu nulovou znalosťou, prenosom jednoduchých príkazov pomocou BLE s využitím GATT profilu a vytvorením Android aplikácie pre prenos týchto jednoduchých príkazov/hodnôt.

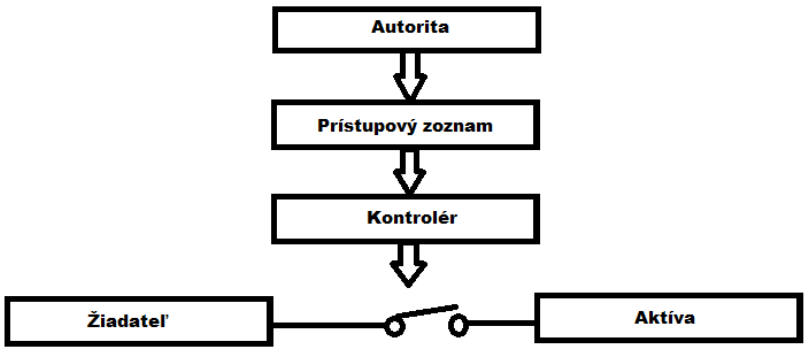
1 TEORETICKÁ ČASŤ

Teoretická časť práce sa zaoberá autentizáciou, jej princípmi, autentizačnými protokolmi, rozoberá autentizáciu s nulovou znalosťou a ich porovnanie. Ďalej sa zaoberá technológiou Bluetooth a jej rozširujúcou podtechnológiou Bluetooth Low Energy, pojednáva sa tu o princípoch týchto technológií, ich špecifikácie a schémy protokolej sady na prenos. Spolu s technológiou BLE je spomenutý aj mobilný systém Android, ktorý od istej verzie natívne podporuje technológiu BLE.

1.1 Autentizácia

Obecne je autentizácia proces, kde žiadateľ overuje svoje predložené identifikačné údaje, teda dochádza k overeniu jeho vyhlásenej identity a následnému prístupu k nejakej službe alebo dátam (aktívam). Hlavnou úlohou autentizácie je teda zamedzenie prístupu nepoverených osôb alebo útočníkov ku chráneným dátam alebo službám a umožnenie prístupu len overeným žiadateľom (osobám). Schému riadeného prístupu môžeme vidieť na obrázku 1.1, schéma obsahuje:

- **Žiadateľ** - osoba alebo zariadenie žiadajúce o prístup
- **Autorita** - systém alebo osoba, rozhodujúca kto môže k môže k aktívam (dátam) pristupovať
- **Prístupový zoznam** - zoznam identifikačných údajov ožívateľa spolu s ich právami
- **Kotrolér** - systém alebo osoba povoľujúca prístup k aktívam
- **Aktíva** - cenné informácie, dáta alebo nejaké zariadenia.[1]



Obr. 1.1: Schéma riadeného prístupu

Riadený prístup je založený na princípe: žiadateľ žiada o prístup k aktívam, pri tejto príležitosti posiela kontroléru svoje identifikačné údaje, kontrolér následne overuje, či tieto údaje patria danému užívateľovi. Ak údaje suhlásia, kontrolér nájde v prístupovom zozname daného užívateľa a zistí prístupové práva na prístup k aktívam. Ak údaje nesúhlasia, prístup je zamietnutý.

1.1.1 Typy autentizácie

Autentizáciu delíme na tri základné typy:

- **Autentizácia znalosťou**: žiadateľ svoju identitu dokazuje nejakou znalosťou (PIN kód, heslo)
- **Autentizácia predmetom**: žiadateľ identitu dokazuje predmetom (ID karta, Token, platobná karta, čipom, BLE náramok)
- **Autentizácia žiadateľom**: žiadateľ svoju identitu dokazuje svojími charakteristickými vlastnosťami (otlačok prsta, hlas, sken sietnice) [1]

1.1.2 Autentizácia znalosťou

Žiadateľ o prístup je pred povolením prístupu overovaný ma znalosť určitej informácie a na základe tejto znalosti je žiadateľový povolený prístup. Informáciu by mal poznať len autorizovaný užívateľ a informácia by mala byť držaná v tajnosti pred prípadnými utočníkmi. Heslo by malo ostať len v pamäti, nemalo by sa nikde zapisovať a nemalo by zhodné s iným heslom. Minimálne požiadavky na heslá:

- dlhé aspoň 8 znakov
- kombinácia malých, veľkých písmen, číslic a špeciálnych znakov
- pre každú službu (kontrolér) iné heslo
- heslo musí byť bez významu
- pravidene heslo meniť

Tento spôsob autentizace pre vyššie uvedené dôvody vytvára veľké bezpečnostné riziko, preto sa používa v kombinácií s inými spôsobmi autentizácie.

Druhou a silnejšie chránenou metódou pri autentizácií znalosťou je typ výzva–odpoveď. Princíp tejto metódy spočíva v tom, že žiadateľ potvrdzuje identitu vhodnou odpoveďou kontroléru na jeho výzvu. Bezpečnosť spočíva v tom, že kontrolér alebo overovacia autorita, posiela výzvu len jeden krát a nikdy nie rovnakú. [1]

Posledným známym typom je autentizácia s nulovou znalosťou. Základ tejto metódy je v tom, že žiadateľ preukazuje len znalosť určitej tajnej informácie ale žiadnu časť neposkytuje kontroléru a kontrolér heslo nepozná. Hlavným rozdielom medzi metódou autentizácie nulovou znalosťou a ostatnými popísanými metódami je v prenose hesla sieťou, kde pri metóde nulovou znalosť dochádza k rapídnemu nárastu bezpečnosti a to z dôvodu toho, že sieťou sa neprenáša šifrované heslo ani jeho časť

ale len bit informácie, ktorý je významný pre overovateľa (overovateľ heslo rovnako nepozná), ktorý ním overuje, že užívateľ pozná heslo ale odchytená informácia by nemala žiadny význam pre potencionálneho útočníka. Viac o autentizácií nulovou znalosťou v kapitole 1.2

1.2 Autentizácia nulovou znalosťou

V dnešnej dobe sú takmer všetky autentizačné protokoly založené na princípe overovania tajnej informácie prenosom po nezabezpečenej sieti. Prenos sieťou je teda najrizikovejšie miesto z hľadiska bezpečnosti a potencionálne najzranitelnejšie miesto pre útočníka. Znalosť tajnej informácie (hesla) je kľúčová teda kľúčová pre rozoznanie správneho užívateľa od potencionálneho útočníka . Väčšinou sa v moderných protokoloch používajú rôzne druhy šifrovania, avšak pri prenose hesla sieťou stále uniká určitá časť informácie. K overeniu užívateľa však nie je potrebné prenášať celé tajné heslo ale stačí preniesť iba informáciu, či toto tajné heslo užívateľ pozná. Takýmto spôsobom sa preniesie len 1 bit informácie. Protokoly takýmto spôsobom nepoznajú a pri prenose nedisponujú tajným heslom z toho dôvodu sa nazývajú protokoly s nulovou znalosťou. Heslo vlastní len užívateľ, nie server a to je dôležitá bezpečnostná vlastnosť tohto typu protokolov. V tejto kapitole uvedieme základný princíp a dôkazy týchto protokolov, rozoberieme nejaké konkrétne riešenia a popíšeme najznámejšie protokoly s nulovou znalosťou.

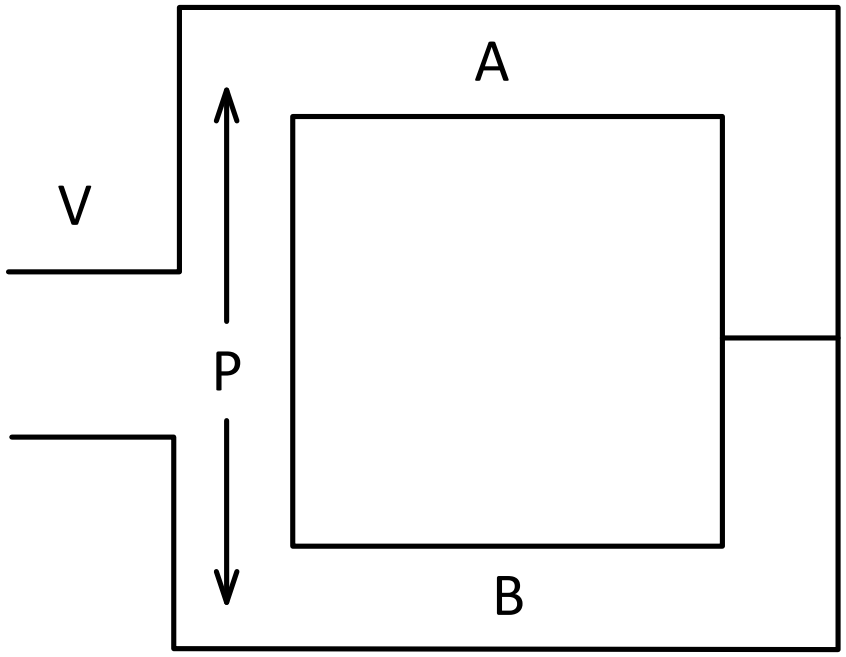
1.2.1 Základný princíp a dôkazy

V literatúre sa pre pochopenie základného princípu protokolov s nulovou znalosťou používa schématické znázornenie pomocou vstupu do jaskyne, niekedy uvádzána ako Alibabová jaskyna pre ľahšie pochopenie.[2] V tomto prípade vystupujú dva subjekty – užívateľ, ktorý vlastní tajnú informáciu (heslo) ku svojmu overeniu a server (overovacia autorita), ktorý ponúka a umožňuje pristupovať k určitým službám a aplikáciam, avšak až po overení tohto užívateľa. Často stretávame s pomenovaním subjektov užívateľa a serveru ako Alice (užívateľ) a Bob (server), avšak v prípade, že definujeme vlastníka a overovateľa v schéme je vhodnejšie použiť pomenovanie Prover (vlastník, držiteľ tajnej informácie – užívateľ, klient) a Verifier (overovacia autorita - server) , označení ako P a V. Na obrázkoch 1.2, 1.3, 1.4 , sú zobrazené tri situácie v jaskyni, kde na konci sú dvere, ktoré sa dajú otvoriť len pomocou tajného hesla. Princíp [3]:

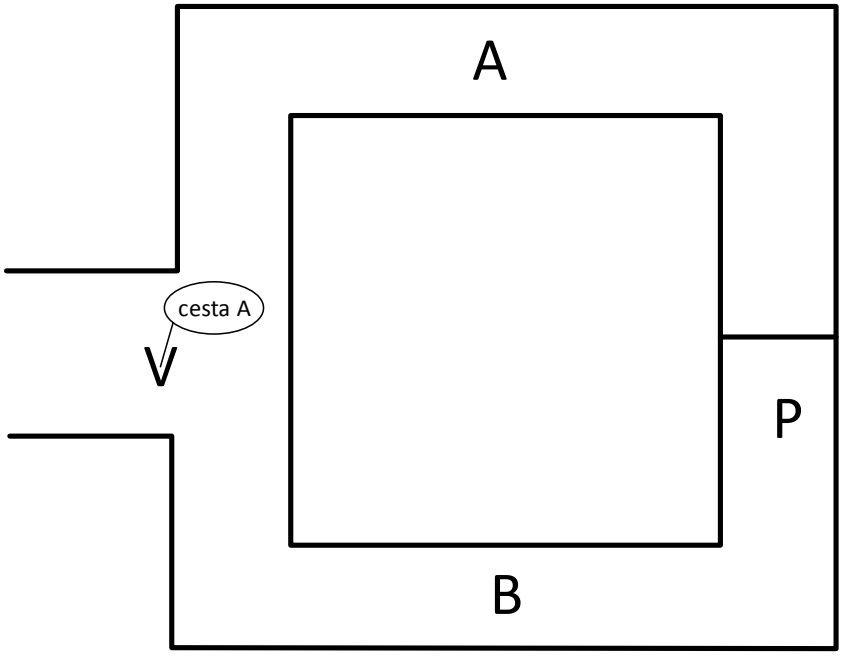
1. P – užívateľ vstúpi do jaskyne a vyberie si cestu ktorou pôjde hlbšie do jaskyne, V – overovateľ čaká vonku obr.1.2

2. V – overovateľ vstúpi do jaskyne, počká pred rozdvojením ciest a náhodne určí cestu pre P – užívateľa, ktorým smerom sa má užívateľ vrátiť obr.1.3

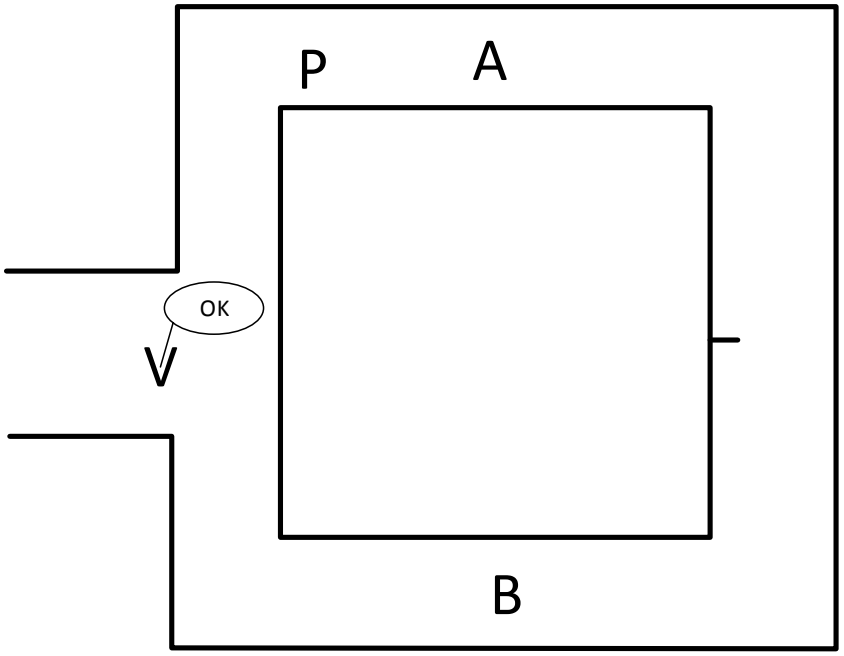
3. Teraz v tomto prípade môžu nastať dve situácie:
   - cesta vstupu P – užívateľa a požadovaná náhodne vygenerovaná cesta od overovateľa V je zhodná. Tým pádom sa užívateľ P vráti rovnakou cestou aj bez toho aby musel poznať tajné heslo.
   - cesta vstupu P – užívateľa a požadovaná vygenerovaná cesta sa líši - P teda vysloví tajné heslo k otvoreniu dverí a výstupi požadovanou stranou obr.1.4



Obr. 1.2: Princíp nulovej znalosti – voľba cesty



Obr. 1.3: Princíp nulovej znalosti – určenie cesty

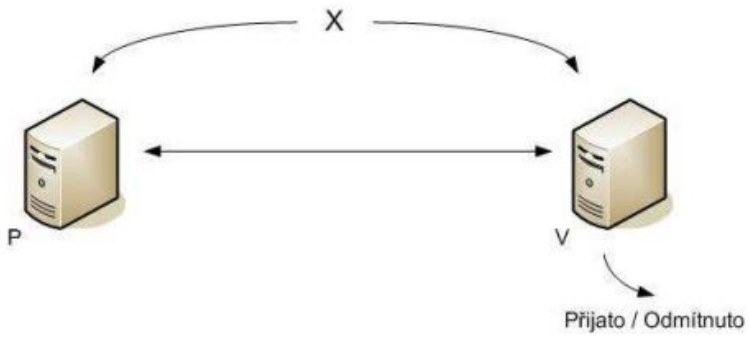


Obr. 1.4: Princíp nulovej znalosti – overenie cesty

Pre funkčnosť protokolu je nevyhutné jeho mnohonásobné opakovanie, potom

môžeme dôjsť k záveru, že pokiaľ P–užívateľ pozná tajné heslo, tak vystúpi z jaskyne vždy správnou cestou, ktorú V–overovateľ požaduje. Pokiaľ P heslo nepozná, tak je jeho úspešnosť len 50%, čo pri n-násobnom opakovaní protokolu dáva dostačujúcu malú pravdepodobnosť (2^{-n}), že užívateľ P oklame overovaciu autoritu V.

Výhodou protokolu s nulovou znalosťou je možnosť dokázať ich bezpečnosť. K tomuto účelu sa zavádza tzv. *interaktívny dôkazový systém*, ktorý prevádza predošlý abstraktný model s jaskyňou do matematickej roviny a popisuje komunikáciu P a V ako komunikáciu dvoch Turingových strojov vzájomne prepojených komunikačnou páskou obr.1.5 [4]



Obr. 1.5: Interaktívny dôkazový systém

Oba stroje získajú spoločný vstup X. Potom nasleduje beh a vzájomná interakcia na jej konci je výsledok „Prijaté/Odmietnuté“, vychádzajúce od V. Týmto beh systému skončí. Výsledok je teda, že pár (P, V) príjme X alebo ho odmietne. V tomto prípade môže byť X výrok, ktorého pravdivosť vedie k odmietnutiu alebo prijatiu. Pre interaktívne dôkazové systémy musia teda platiť dve základné vlastnosti:

- **Úplnosť**: Pokiaľ $X \in L$ (je pravdivé), potom pravdepodobnosť, že (P, V) odmietne X je zanedbateľná dĺžkou X.
- **Spoľahlivosť**: Pokiaľ $X \notin L$ (nie je pravdivé), potom pravdepodobnosť, že (P*, V) príjme X je zanedbateľná s dĺžkou X, pričom P* je akýkoľvek klient.

Ak by sme tento systém použili pre overenie identity klienta, ktorého tajomstvo je dôkaz pravdivosti výroku, klient by bol do systému vpustený takmer vždy, pokiaľ by bolo tvrdenie pravdivé(vďaka úplnosti – klient má dôkaz) a takmer nikdy, pokiaľ toto tvrdenie pravdivé nie je (vďaka spoľahlivosti – klient dôkaz nemôže mať). Systém takto poskytuje overnie klienta ale žiadným spôsobom nešpecifikuje, ktoré infromácie budú odoslané verejne. Tento dôvod spôsobuje to, že systém zatiaľ nie je zabezpečený proti odhaleniu tajomstva ktoré drží klient P. Protokoly založené na interaktívnom dôkazovom systéme môžu naviac obsahovať vlastnosť Zero Knowledge, čiže nulovú znalosť informácie. V tejto súvislosti potom môžeme o týchto

protokoloch hovoriť ako o Zero Knowledge protokoloch. Požiadavok na utajenie súkromných informácií klienta môžeme špecifikovať ako požiadavok na existenciu simulátora, tento simulátor bude simulovať pribeh protokolu bez prítomnosti klienta P. Potom môžeme predpokladať, že ak existuje stroj, ktorý vygeneruje celý výstup protokolu bez prístomnosti klienta P, nie je teda žiadne tajomstvo známe len klientovi P, ktoré bolo v protokole odhalené a to z dôvodu, že simulátor tajomstvo samozrejme nepozná.[4]

1.2.2 Protokoly

Protokoly Nulovou Znalosťou(ZK-zero knowledge) musia spĺňať tri vlastnosti; úplnosť, dôkladnosť a nulovú znalosť. Vlastnosť úplnosť znamená to, že ak prehlásenie je pravda, poctivý overovateľ-verifier bude o tom presvedčený týmto faktom od poctivej overovanej entity - provera. Dôkladnosť znamená, že ak je vyhlásenie nepravdivé, žiaden podvadzajúci prover(klient) nemôže presvedčiť poctivého overovateľa-verifier, že je to pravda s výnimkou malej pravdepodobnosti. Vlastnosť nulová znalosť znamená, že ak vyhlásenie je pravda, žiaden podvádzajúci overovateľ-verifier sa nenaučí nič iné ako tento fakt. Väčšina Zero Knowledge protokolov sú tri preukázané protokoly, to znamená že tri správy sú prenášané medzi A a B(P-prover a V-verifier); záväzok, výzva(challange), a odpoveď(response). Náhodnosť a načasovanie sú súčasťou ostatných vlastností typický spojených s Zero Knowledge protokolmi. Náhodnosť v záväzku a výzva sú použité k zakrytiu utajenej informácie. Načasovanie(časovanie) je použitý k prevencií protistranu na príliš dlhú dobu na vypočítanie odpovede.[5]

Najznámejšie sú tri protokoly nulovou znalosťou : Fiat-Shamir, Guillou-Quisquarter (GQ) a Schorr protokoly.

Fiat-Shamir identifikačný protokol Je jeden z najznámejších protokolov s nulovou znalosťou. Protokol bol publikovaný už roku 1986. Účelom tohto protokolu je zaistiť aby sa užívateľ (prover–P) mohol identifikovať akémukoľvek overovateľovi (verifer–V) a to za splnenia podmienky nulovej znalosti, kde tajné heslo pozná len užívateľ–P a overovateľ sa ho nedozvie. Bezpečnosť je zaistená obtiažnou faktorizáciou RSA modulu. Priebeh protokolou sa skladá z dvoch častí: inicializácie a vlastný beh protokolu.

Inicializácia: Dôveryhodná autorita (napríklad bezpečnostný server) vygeneruje k-bitový RSA modul $n = p \cdot q$, kde p a q sú rôzne veľké prvočísla, ktoré sú stále držané v tajnosti. Užívateľ P si vyberie svoj tajný kľúč s z množiny Z_n a vypočíta $v = s^2 \ mod \ n$, kde mod značí operáciu modulo, a následne pošle v autorite, ktorá zverejní $(n, \ v)$.

Beh protokolu: Ak sa užívateľ P chce identifikovať overovateľovi V, musia sa pred začatím overovania dohodnúť na počte priebehu protokolu t (obvykle $t \geq 80$).

- P zvolí náhodné r $\in Z_n$(záväzok), P ďalej spočíta $x = r^2$ *mod n (dôkaz)* a pošle x overovateľovi V.
- overovateľ V zvolí náhodný bit $b \in (0, 1)$ a pošle to späť užívateľovi P.
- P vypočíta $y = (r \cdot s^b)$ *mod n (odpoveď)* a pošle späť overovateľov.
- V overí $y^2 \equiv x \cdot v^b$ (mod n). Pokiaľ zhoda platí, overovateľ V tento cyklus akceptuje, v opačnom prípade ho odmietne.

Ak je protokol akceptovaný vo všetkých t-cykloch, môžeme teda protokol považovať za úspešne ukončený a užívateľ P tak bol overený overovaciou autoritou V. Protokol však musí spĺňať podmienky úplnosti, spoľahlivosti a musí existovať simulátor S. [6]

Guillou-Quisquarter(GQ) protokol Cieľom protokolu Guillou-Quisquarter (GQ) protokolu je umožniť A klientovi preukázať znalosť B overovateľovi v **t** vykonaniach. Toto je pravdepodobnostný protokol s pravdepodobnosťou v^{-t} pre protistranu aby zmiatla overovateľa. Od možného rozsahu **e** hodnôt rozsah od 1 do **v** s tým, že **v** sa môže stať veľmi veľké sa pravdepodobnosť,že protistrana môže zmiasť overovateľa stáva veľmi malá. GQ je rozšírenie Fiat-Shamir protokolu, ktorý závisí od ťažkosti faktoringu. [5]

- **Systémové parametre**
  1. Dôveryhodné centrum(T) vyberie RSA - modulus n=pq, n-verejný, **p** a **q** tajný
  2. T vyberie exponent v, v>=3 a gcd(v,ϕ)=1 kde ϕ=(p-1)(q-1), s = v^{-1} mod ϕ, v-verejné, s-tajné
- **Jednotlivé užívateľské parametre**
  1. Entita A má dohodnutú jedinečnú identitu I_A
  2. Redundantná identita J_A=f(I_A) kde 1<J_A<n ktoré implikuje gcd(J_A,ϕ)=1, f-verejná funkcia
  3. T udeľuje A: $s_A = {J_A}^{-s}$ mod n, s_A - tajné
- **Protokol**
  1. **A** vyberie náhodný záväzok r, 1<=r<=n-1
  2. **A** pošle **B** (1): I_A, x=r^v mod n
  3. **B** pošle **A** (2): náhodné **e**,1<=e<=v
  4. **A** pošle **B** (3): $y = r \cdot {s_A}^e$ mod n
- **Verifikácia**
  1. **B** vytvára J_A = f(I_A)
  2. **B** počíta $z = {J_A}^e \cdot y^v$ mod n
  3. **B** odmieta if z = 0
  4. **B** akceptuje if z = x, odmietne inak

Schnorr protokol Cieľom tohto protokolu je umožniť A klientovi preukázať znalosť overovateľovi B. Schnorr je trojprechodný protokol, ktorý sa odvíja od náročnosti počítania diskrétneho logaritmu.

- **Systémové parametre**
  1. Vyber **p** ktorý **p**-1 je deliteľný ďalším prvočíslom **q**(p = 2^{1024}, q>=2^{160}), p, q - verejné
  2. Vyber *beta*, 1 <= β <=p-1, majúci príkaz q, α je generátor mod p, $\beta = \alpha^{(p-1)/q}$
  3. Vyber **t**, **t**>=40, 2^t < q
- **Jednotlivé užívateľské parametre**
  1. **A** zvolí tajný kľúč a, 0<= a <=q-1
  2. **A** vypočíta v = β^{-a} mod p
- **Protokol**
  1. **A** zvolí náhodný záväzok r, 1<= r <=q-1
  2. **A** pošle **B**(1): x= β^t mod p
  3. **B** pošle **A**(2): náhodné e, 1 <= e <= 2^t < q
  4. **A** pošle **B**(3): $y = a \cdot e$ + r mod q
- **Verifikácia**
- **B** počíta $z = \beta^y \cdot v^e$ mod p
- **B** akceptuje if z = x, odmietne inak

Porovnanie protokolov

- Komunikácia
- Výpočty
- Pamäť
- Bezpečnostné záruky
- Dôvera požadovaná treťou stranou

Komunikácia je počet správ, ktoré sa vymieňajú medzi preverovanou entitou-klientom a overovateľom.Výpočty sú počet modulárnych násobkov pre obidvoch, pre provera-klienta ako aj pre verifiera-server(overovateľ). Rovnako je počet on-line a off-line výpočtov. Veľkosť pamäte používana k ukladaniu tajných kľúčov a ostatných hodnôt je ďalšie porovnávacie kritérium. Bezpečnostná záruka je úroveň ochrany proti falšovaniu a zverejňovaniu tajných informácií. Nakoniec je požadovaná dôvera treťou stranou. Rozličné predpoklady dôvery môžu byť vytvorené medzi rozdielnými protokolmi.

Komunikácia Fiat-Shamir požaduje 20 až 40 kôl trojcestného protokolu, teda 60 až 120 jednotlivých správ. Toto je zďaleka najväčší z týchto troch protokolov, uvedených v tejto práci. Guillou-Quisquarter(GQ) protokol a Schnorr potrebujú len jedno kolo protokolu.

Výpočty Fiat-Shamir protokol má hranice vo výpočtovej efektivite, zatiaľ čo Schnorr má tú výhodu, že požaduje iba jediné on-line modulárne násobne od proveraklienta, existujú však značné výpočty, ktoré si vyžaduje verifikátor-server v porovnaní s protokolmi Fiat-Shamir alebo Guillou-Quisquarter (GQ).

Šírka pásma(Bandwidth) a Pamäť Guillou-Quisquarter umožňuje znížiť pamäť a aj šírku pásma oproti Fiat-Shamir protokolu.

Bezpečnostné predpoklady Fiat-Shamir je založený na obtiažnosti extrakcie štvorcových koreňov mod n(Factoring). GQ(Guillou-Quisquarter) je rovnako založený na factoringu ale vyžaduje si extrakciu vth koreňa mod n. Schnorr je založený na obtiažnosti výpočtu disktétnych záznamov mod p. Ako sme videli v šifrovacích protokoloch, bitová úroveň pre relatívnu bezpečnosť pre faktoringový problém je mierne vyššia ako požiadavka na diskrétne záznamy.[5]

Útoky Niektoré z hlavných útokov , ktoré sa používajú na prelomenie Zero Knowledge protokolov:

1. Zosobnenie
2. Opakovanie
3. Prekladanie
4. Reflexia
5. Nútené oneskorenie
6. Zvolený text

Zosobnenie je tam kde jedna entita predstiera, že je iná. Opakovanie je takýto typ útoku a používa zosobnenie, ktoré zahŕňa použitie informácií z jedného alebo viacerých predchádzajúcich protokolov. Realizácie(executions) sú útokom prekladania(interleaving), ktorý zahŕňa zasielanie informácií z predchádzajúceho spúšťania protokolu späť na pôvodcu. Protivník, ktorý zachytil správu a uvoľní ju neskôr používa nútený oneskorený útok(forced delay). Napokon útok na vybraný text je keď protivník vyberá špecifické výzvy v snahe získať informácie o tajomstve.

Záver z protokolov

Protokoly Nulovou Znalosťou umožňujú overovanej entite(prover) dokázať overovateľovi(verifier), že vie tajomstvo aj bez odhaľujúcich informácií ktoré by mohgli byť zneužité. Porovnaním hodnôt medzi záväzkom a odpoveďou si môže overovateľ(verifier) dopočítať, či odpoveď zodpovedá očakávanej hodnote. Toto umožňuje overovateľovi overiť informácie bez toho aby mal vedomosti o súkromnom tajomstve overovanej entity(prover). Zero Knowledge protokoly môžu byť použité na umožnenie anonymnej autentifikácie v zariadeniách , ako napríklad RFID tagy, alebo cestovné pasy s RFID čipom, na ktorom by bežal takýto ZK protokol. Takýto protokol by bol použitý na ochranu osobných informácií pričom na overenie pravosti osoby by sa stále použil pas.

1.3 Bluetooth

Technológia Bluetooth je štandard na pripojenie bezdrôtových zariadení na krátku vzdialenosť, medzinárodné označený tiež ako IEEE 802.15.1. Bluetooth sa radí do kategórie osobných počítačových sietí tzv. PAN (Personal Area Network) , ktoré pracujú na krátku vzdialenosť , rádovo jednotky až desiatky metrov. Bluetooth technológia začala vznikať ako požiadavka firmy Ericson na prepojenie mobilných telefónov bezdrôtovo okolo roku 1994 . Bluetooth pracuje v okolí frekvenčného pásma 2,4 GHz s metódou FHSS, čo je skoková metóda na prelaďovanie medzi frekvenciami, konkrétne 79 frekvencií s odstupom 1 MHz. Použitie tohto mechanizmu zvyšuje odolnosť spojenia voči rušniu na rovnakej frekvencií. Pri štandarde Bluetooth máme definovaných viacero výkonových úrovní (1 mW, 10 mW, 100 mW) pomocou ktorých môžeme dosiahnúť komunikáciu od niekoľko metrov až do vzdialenosti 100 metrov vo voľnom priestore, v zastavanom priestore dosah značne klesá. Prvá známejšia verzia Bluetooth pre mobilné zariadenie prišla ako štandard 2.1 + EDR v roku 2007 s teoretickou prenosovou rýchlosťou na úrovni 3 Mbit/s , ďalej bolo oproti verzií 1.2 implementované jednoduché bezpečné párovanie (SSP - Simple Secure Pairing). V roku 2009 prišla verzia v3.0 + HS ktorá priniesla spojenie štandardu Bluetooth a technológie WiFi, čo prineslo teoretické rýchlosti pri prenose až 24 Mbit/s , pričom prenos nie je realizovaný priamo cez rozhranie Bluetooth ale využíva štandard 802.11 známe ako WiFi . Cez štandard Bluetooth sa nadviaže spojenie a dôjde k odoslaniu dôležitých údajov o prenose. Ďalšia zásadnejšia aktualizácia technológie Bluetooth, ktorá je známa ako špecifikácia pod označením 4.0 prišla v roku 2010 a hlavnou črtou tejto aktualizácie je implementovanie technológia BLE z toho plynúce zníženie spotreby a zameranie sa na nízko energetické zariadenia ako napríklad nositeľná elektronika, senzorické zariadenia, handsfree súpravy a iné zariadenia s nízkou spotrebou energie.[7] Podstatnou časťou špecifikácie Bluetooth 4.0 je technológia BLE (Bluetooth Low Energy), ktorá sa využíva aj v tejto práci k prenosom medzi vývojovou doskou Raspberry Pi 2 a telefónom Android.

Tab. 1.1: Výkonové triedy Bluetooth

Výkonová trieda	**Maximálny výkon**	**Maximálny dosah**
1	100 mW (20 dBm)	100 m
2	2,5 mW (4 dBm)	10 m
3	1 mW (0 dBm)	1 m
4	0,5 mW (-3 dBm)	0,5 m

1.4 Bluetooth Low Energy

Bluetooth Low Energy(BLE) často označovaný tiež ako Bluetooth Smart bol implementovaný ako hlavná časť špecifikácie Bluetooth 4.0. Cieľom vývoja tejto špecifikácie bolo priniesť menšiu, vysoko optimalizovanú technológiu klasického rozhrania Bluetooth. V podstate je však BLE značne odlišné od klasickej technológie Bluetooth a táto technológia bola vytvorená pre úplne iné ciele ako pôvodná technológia Bluetooth. Predtým ako si technológiu osvojila spoločnosť Bluetooth Special Interest Group (BSIG), bola technológia vyvýjaná spoločnosťou Nokia pod názvom Wibree. Autori technológie sa nepokúšali od začiatku vyvinúť nový bezdrôtový štandard, ktorý by vyriešil všetky problémi ale zamerali sa na vývoj rádiového komunikačného štandardu, ktorý disponuje najmenšiou možnou mierou spotreby energie, je nízkonákladový a nie je zložitý na implementovanie. Tieto ciele sú evidentné už pri hlavnej špecifikácií, ktorá definovala BLE ako originálny nízkoenergetický štandard navrhnutý pre implementáciu veľkými výrobcami. BLE by sa mohlo v budúcnosti stať svetovou široko osvojenou technológiou, ktorá definuje štandard na dlhší čas.[8] Platformy podporujúce Bluetooth Low Energy[9]:

- iOS5+(iOS7+ preferovaný)
- Android 4.3 (od verzie 5.0 periférny mód)
- Apple OS X 10.6+
- Windows 7 a novšie
- GNU/Linux Vanilla BlueZ 4.93+

1.4.1 Pripojenie BLE

Pripojenie znamená výmenú dát v oboch smeroch na dvoch zariadeniach a je potrebné v prípade ak chceme posielať dáta periodicky a len medzi dvoma spárovanými zariadeniami. Takéto pripojenie a spárovanie zariadení výrazne obmedzuje odchytávanie komunikácie ako v prípade jednorázového posielania dát bez spárovania kedy zariadenie ktoré vysiela dáta bez zabezpečenia a tak sa zväčšuje šanca takto vysielané dáta odchytiť. Pripojenie zahŕňa dva separované módy zariadení:

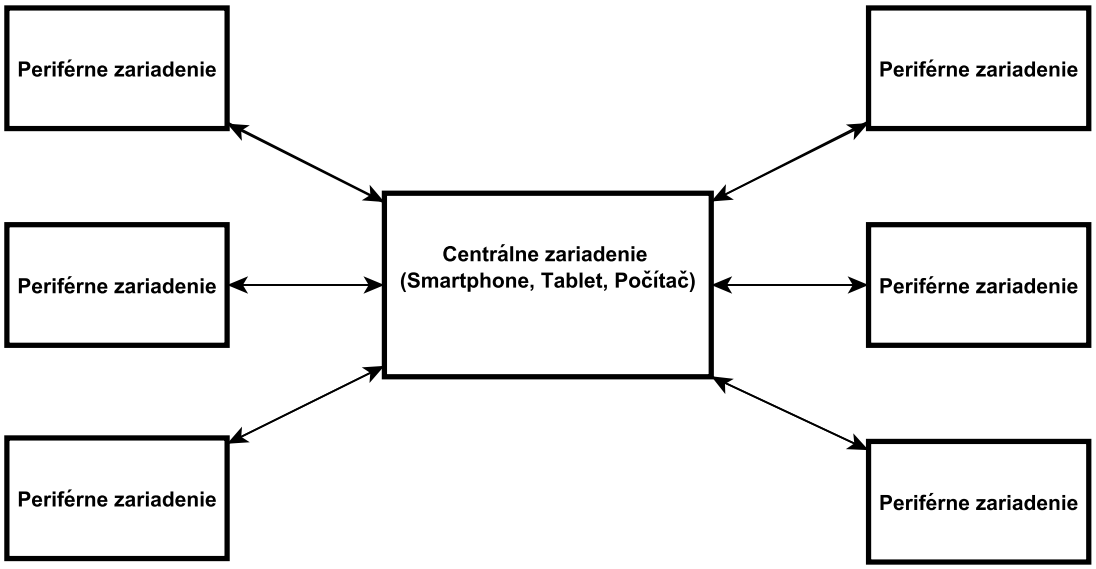
Centrálne zariadenie(master)

Opakovanie kontroluje predložené frekvencie kde sa snaží zachytiť pakety, ktoré oznamujú pripojenie na vysielacie zariadenie. Keď tieto pakety odchytí a zistí, že sú vyhovujúce nadviaže pripojenie. Pri aktívnom spojení, centrálne zariadenie nastaví časovanie a začne sa periodická výmená dát.

Periférne zariadenie(slave)

Je zariadenie, ktoré periodický vysiela pakety pre nadviazanie spojenia s iným zariadením a akceptuje prichádzajúce pripojenia. Ak je spojenie aktívne, periférne

zariadenie používa časovanie centrálneho zariadenia a vymieňa si s ním pravidelne dáta.
Na začatie komunikácie, musí centrálne zariadenie prijať paket incializovaný pripojenie, ktorý vysiela periférne zariadenie. Po tomto kroku centrálne zariadenie pošle na periférne zariadenie žiadosť o vytvorenie tzv. exkluzívneho pripojenia medzi dvoma zariadeniami. V okamihu keď je pripojenie nadziazané, prestáva periférne zariadenie vysielať incializačné pakety a pripojené zariadenia začnú medzi sebou komunikovať v oboch smeroch.[8]



Obr. 1.6: Topológia pripojenia BLE

Vo špecifikácií verzie 4.0 boli obmedzenia pre pripojenie prefiérneho a centrálneho zariadenie a ich kombinácií, s aktualizáciou na verziu 4.1 boli tieto obmedzenia odstránené, detailne v podkapitole 1.4.2.

1.4.2 Verzia Bluetooth 4.1

Prišla v roku 2013 a vytvára cestu pre použitie Bluetooth ako obecného komunikačného rozhrania pre širokú škálu elektronických zariadení pripojených k sietí, tzv. „internetu vecí“ (IoT–Internet of things). Bluetooth 4.1 teda prináša prvotnú podporu pre sieťovú komunikáciu prostredníctvom protokolu IPv6, čo je jeden z najzákladnejších protokol pre prenos v samotnom Internete. V štandarde je pre túto komunikáciu vyhradený špeciálny kanál, ktorý v budúcnosti zabezpečí komunikáciu veľkého množstva rôznych zariadení, senzorov, vypínačov ale aj spotrebičov.[10] Verzia 4.1 odstránila obmedzenia pri kombinovaní centrálneho a periférneho módu pri pripojení a umožňuje [8] :

- Zariadenie môže fungovať ako v centrálnom tak aj v perifémom móde v jednom čase
- Centrálne zariadenie môže byť pripojené na viacero perifémych zariadení
- Periférne zariadenie môže byť pripojené na viacero centrálnych zariadení

To prináša výhody v podobe toho, že napríklad inteligentné hodinky sú pripojené k telefónu ako periférium ale zároveň dokážu ako hostiteľ prijímať informácie od externého senzora s podporou BLE.[10] Verzia 4.1 je plne kompatibilná s verziou 4.0 avšak zariadenie BLE nemôže komunikovať s iným zariadením nižšej verzie ako je 4.0 a to z dôvodu, odlišnej hornej vrstvy protokolu.

1.4.3 Verzia Bluetooth 4.2

Priniesla oproti verzií 4.1 pár nových vylepšení najväčšiou výhodou oproti verzií 4.1 bolo umožnila čipom použiť Bluetooth na priamu prístup pomocou protokolu IPv6, verzia 4.2 v menšej miere vylepšila rýchlosť a ochranu komunikácie pri využití Bluetooth.[11] Do dnešnej doby je to zatiaľ posledná implementácia Bluetooth na jadro 4.0. V roku 2017 bude implementovaná do zariadení nová technológia Bluetooth, ktorej jadro bude založené na verzií 5.0 a z väčšej časti sa zameriava na Internet of Things technológie. Mala by priniesť štvornásobný dosah a dvojnásobnú rýchlosť pri nižšej spotrebe energie.[12]

IoT schopnosti pri verzií BLE 4.2

- Nízkoenergetické IP (IPv6/6LoWPAN)
- Bluetooth Smart Internet Gateways

S technológiou BLE 4.2 sú Bluetooth Smart senzory schopné preniesť dáta internetom.

Bezpečnosť

- LE Ochrana 1.2
- LE Zabezpečené spojenie

Pri implementovaní nových bezpečnostných štandardov BLE 4.2, je zabezpečené že len overený užívatelia môžu sledovať lokáciu zariadenia (senzoru) a spárovať sa so zariadením.

Rýchlosť

- 250% rýchlejšie
- 10x Viac prenosovej kapacity [11]

1.4.4 Komunikačné protokoly a profily BLE

Od prestavenia Bluetooth špecifikácie bol pevne dané rozdiely medzi protokolmi a profilmi:

Protokoly

Vytvorené bloky ktoré sú používané všetkými zariadeniami podriadenými pod špecifikáciou Bluetooth. Protkoly sú vrstvy, ktoré implementujú rozličné formáty paketov, zabezpečujú smerovanie, kódovanie a dekódovanie ktoré zaisťuje efektívny prenos medzi spojenými bodmi.

Profily

„Vertikálne rezy“, ktoré funkcionalitou buď pokrývajú základné módy vyžadovaných operácií pri pripojení všetkých zariadení (Generic Access Profile, Generic Attribute Profile) alebo je ich funkcia využitá v špecifických prípadoch použitia Bluetooth (Proximity Profile, Glucose Profile), kde v týchto prípadoch profily definujú akým spôsobom majú byť protokoly použité k dosiahnutiu čiastočného cieľa spojenia, či už všeobecného alebo špecifického.

Všeobecné Profily (Generic Profiles) sú definované špecifikáciou, dva z nich sú základným prvkom zaisťujúcim kooperáciu medzi BLE zariadeniami od rôznych výrobcov, týmito profilmi sú:

1. *Generic Access Profile (GAP)* – Pokrýva model použitia nízkoúrovňových rádio protokolov na definovanie rolí, procedúr a módov, ktoré umožňujú zariadeniam vysielať dáta, objaviť zariadenia, nadviazať spojenie, spravovať spojenia a vyjednávať bezpečnostné úrovne medzi zariadeniami. GAP je v základe najvyššia kontrolná vrstva BLE. Všetky zariadenia BLE musia spĺňať tento profil a je pre ne záväzný.
2. *Generic Attribute Profile (GATT)* – Pri narábaní s výmenou dát v BLE, GATT definuje základné dátové modely a procedúry, ktoré zaisťujú zariadeniam odhaľovať, čítať, prepisovať a pretlačiť dátove prvky medzi nimi. GATT je v základe najvyššia dátová vrstva v BLE.

Špecifický použiteľné profily

V dnešnej dobe sú špecifický použiteľné profily limitované do profilov so základom v GATT. Znamená to, že všetky profily, procedúry a operačné módy GATT sú základom pre tvorenie blokov všetkých ďalších rozšírení. Zatiaľ nie sú známe špecifické profily bez základu v GATT ale predstavenie L2CAP kanálov orientovaných na pri-

pojenie vo verzií 4.1, predostrelo verziu, že v budúcnosti by mohli vznikať špecifické profily, ktoré by mali menší základ v GATT protokole, vznikali by tzv. GATT-less profily.

Špecifické profily založené na GATT profile

Špeciálna záujmová skupina pre Bluetooth (SIG) priniesla viacero špecifických profilov, ktoré majú základ v GATT profile a plne pokrývajú všetky procedúry a dátové formáty, ktoré sú vyžiadané a implementované do širokého spektra špecifikého použitia, patria sem nasledujúce najznámejšie profily [8]:

- *Nájdi ma profil (Find me Profile)* – Umožňuje zariadeniam fyzicky lokalizovať iné zariadenia (nájdenie telefónu v miestnosti pomocou Bluetooth).
- *Profil blízkosti – (Proximity Profile)* Vhodné na dekteciu prítomnosti alebo neprítomnosti blízkych zariadení (pípnutie zariadenia v prípade opustenia izby a poklesu signálu).
- *Zariadenia komunikujúce s človekom cez GATT profil (HID over GATT Profile)* – Posiela dáta z klávesníc alebo ovládacích prvkov cez BLE.
- *Profil Glukózy (Glucose Profile)* – Bezpečné posielanie úrovní glukózy cez BLE, vhodné napríklad ako senzor pre diabetikov.
- *Profil teplomeru(Health Thermometer Profile)* – Profil vhodný na sledovanie telesnej teploty pomocou BLE.
- *Rýchlosť a rytmus bicyklovania (Cycling Speed and Cadence Profile)* – Umožňuje senzoru na bicykli posielať rýchlosť a rytmus bicyklovania do smartfónu alebo tabletu.

Špecifické profily výrobcov (Vendor-Specific Profiles)

Špecifikácia Bluetooth umožňuje aj výrobcom zariadení definovať ich vlastne profily pre špecifické použitie, ktoré nie sú pokryté skupinou profilov definovanou Bluetooth SIG. Tieto profily môžu byť držané v tajnosti a výrobcovia zariadení ich môžu používať napríklad na komunikáciu medzi svojím zdravotným príslušenstvom a aplikáciou v mobile alebo môžu byť publikované výrobcom a ich základ môže byť využitý na implementáciu do iných profilov.

Príklad špecifického profilu výrobcu je iBeacon, ktorý umožňuje lokáciu iOS vo vnútri budov kde nie je k dispozícií dobrý signál GPS. Základ iBeaconu môže slúžiť ako oznamovací prostriedok predajcu k zákazníkový pomocou Bluetooth, môže taktiež slúžiť na posielanie informácií k expozíciam v múzeu alebo ako informácie o blízkych udalostiach.[8]

Protokolová základňa BLE

Pri použití Bluetooth Low Energy sa užívatelia väčšinou stretnú len v hornými vrstvami BLE protokolovej základne, avšak protokoly a profily sa v BLE zariadeniach delia do troch častí, tieto častí sú zobrazené na obrázku 1.7.

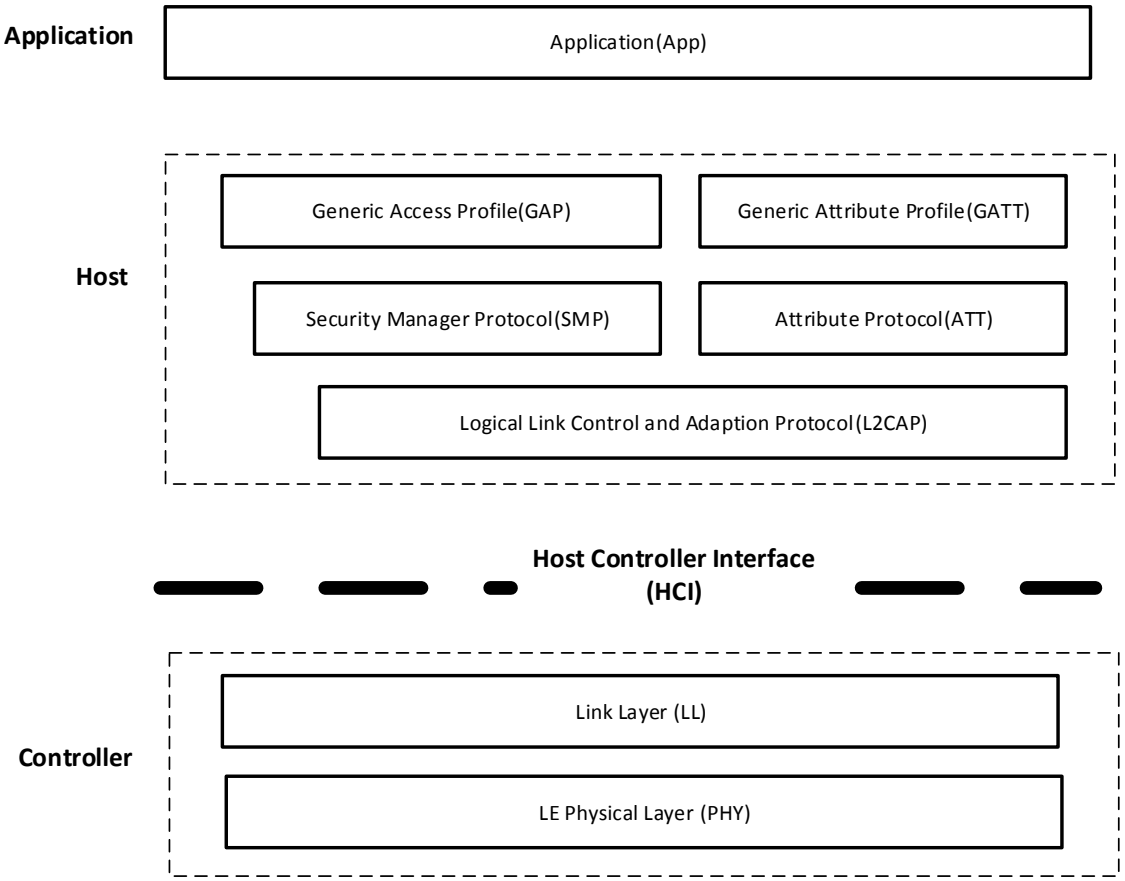
Každý stavebný blok protokolovej sady je rozdelený do niekoľko vrstiev, ktoré

zabezpečujú funkcionalitu požadovanú pri obsluhe:

1. **Aplikácia**
   Aplikácia je tak ako v iných systémoch, najvyššie postavená vrstva obsahujúca logiku, zodpovedná za používateľske rozhrania, narábanie s dátami a všetkým čo aplikácia pri použití implementuje. Architektúra aplikácie je závislá na každom čiastočnom prevedení.

2. **Hostiteľ**
   Obsahuje nasledujúce vrstvy:
   - Generic Access Profile (GAP)
   - Generic Attribute Profile (GATT)
   - Logical Link Control and Adaption Protocol (L2CAP)
   - Attribute Protocol (ATT)
   - Security Manager (SM)
   - Host Controller Interface (HCI), Host side

3. **Kontrolér**
   Obsahuje nasledujúce vrstvy:
   - Host Controller Interface (HCI), Controller side
   - Link Layer (LL)
   - Physical Layer (PHY)



Obr. 1.7: Protokolová sada BLE

1.5 Systém Andriod

Časť pojednávajúca o operačnom systéme Android, jeho stručný opis a opis verzie 6.0, ktorá beží na telefóne ktorý používame na spojenie s Raspeberry Pi 2.

1.5.1 System Android a Bluetooth Low Energy

V polke roku 2013 bol vypustený Android API 18, verzia 4.3 ktorá predstavila podporu pre Bluetooth Low Energy. Bluetooth Low Energy bol navrhnutý pre podobnú komunikáciu ako klasický Bluetooh ale s oveľa nižšiou spotrebou energie z toho dôvodu môžu byť BLE zariadenia prepnuté do sleep módu a prebudiť sa len pre pokus nazviazania spojenia alebo inú udalosť. V tejto verzií však podporoval len centrálnu rolu BLE.[13] Od verzie 5.0 prináša Android podporu pre BLE aj ako periférne zariadenie alebo periférna rola. Do vydania tejto mohli inteligentné telefóny fungovať len ako centrálne zariadenie, ktoré sa pripájalo na periférne zariadenie, avšak po vydaní verzie 5.0 fungujú už aj ako periférne, ktoré môže vysielať oznamovacie pakety a pripájať sa na iné centrálne zariadenia, rovnako môže posielať Beacon a iBeacon

pakety. Rovnako sa vylepšilo posielanie oznamovacích paketov a zlepšila sa oneskorovacia doba pri posielaní týchto paketov, vylepšené bola aj skenovanie zariadení, ktoré bolo veľkým problémom pri starších verziách, kde pri prechode zariadenia do standby módu dochádzalo k rýchlemu vybíjaniu batérie a tým bola eliminovaná hlavná výhoda Bluetooth Low Energy, čo mala byť nízka spotreba energie, s príchodom Androidom 5 (Lollipop), bol skenovací proces BLE presunutý na nižšie vrsty, ktoré dovoľovali telefónu nastaviť BLE na mód spánku, tým pádom nedochádzalo k veľkému vybíjaniu počas toho ako bolo BLE neaktívne. [14] Verzia 6.0 beží na mobilnom telefóne ktorý používame na pripojenie k minipočítaču Raspberry Pi 2 pomocou BLE rozhrania. Verzia 6.0 oproti prechádzajúcej verzií prináša radu vylepšení a to hlavne udeľovanie práv aplikáciam, integrovanú podporu pre čítačky odtlačkov prstov, mobilné platby, automatické zálohovanie, nové menu aplikácií, vylepšené notifikácie, pokročilejšie fungovanie úložiska alebo väčšiu výdrž batérie.[15]

1.6 Raspberry Pi 2

Raspberry Pi je zrejme najpopulárnejší vývojový a edukačný minipočítač na svete. Vyrábaný je spoločnosťou Raspberry Pi Foundation od roku 2012 za cenu približne 35$ a s veľkosťou 8,8 x 5,6 cm. Táto práca pojednáva o modely Raspberry Pi 2, ktorý bol v práci použitý na prenos dát medzi mobilným telefónom a minipočítačom pomocou BLE.

Raspberry Pi 2 je oproti predošlej verzií Raspberry Pi približne šesťkrát výkonnejší. Základom je nová štvorjadrová platforma Broadcom BCM2836, ktorá obsahuje štyri procesorové jadrá ARMv7 Cortex A7 na frekvencií 900 MHz, otvára sa tu však aj možnosť pretaktovania maximálne na 1,1 GHz. Výrazne sa zvýšila operačná pamäť a to na 1 GB LPDDR2 oproti predošlej verzií, ktorá disponovala 256 MB alebo 512 MB operačnou pamäťou.[17]

2 PRAKTICKÁ ČASŤ

V praktickej časti práce je definovaný výber autentizačného protokolu ktorý by mal byť implementovaný na overenie. Vytvorenie GATT BLE servera a GATT custom services a vytváranie Android aplikácie pomocou Android studia.

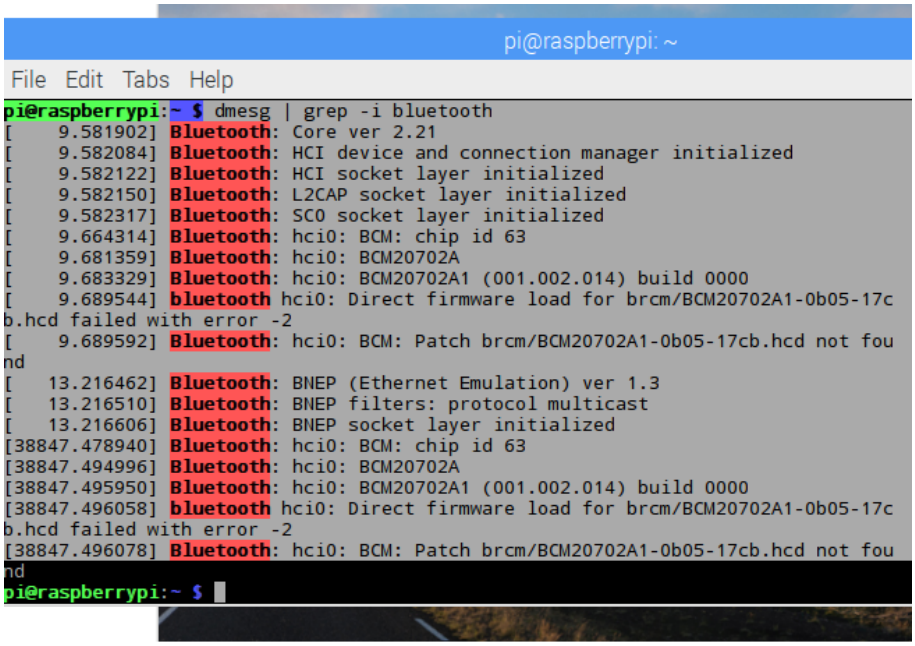
2.1 Návrh Autentizačného Protokol

Autentizačný protokol bude bežať na mobilnom telefóne na ktorom bola vytvorená Android aplikácia. Mobilný telefón sa bude pripájať na dosku Raspberry Pi 2 pomocou BLE rozhrania a svoju autentizáciu overovať pomocou autentizačného protokolu, ktorý je založený na báze **protokolov nulovou znalosťou**. Overenie telefónu bude prebiehať bezdrôtovo na rozhraní BLE(Bluetooth Low Energy) na minipočítač Raspberry Pi 2, na ktorý pomocou otvoreného kanála BLE telefón prenesie vygenerované parametre. Minipočítač Raspberry Pi 2 následne overí tieto parametre a v prípade správnosti buď bude pokračovať v komunikácií pomcou BLE alebo pri neúspešnej autentizácií použije GATT server ktorý zavolá metódu na odoprenie komunikácie a telefón od BLE kanálu odpojí. Ako autentizačný protokol vytvorený na báze nulovej bude implementovaný protokol **HM12**, tento protokol už bol implementovaný v jednej záverečnej práci na NFC Readery, takže spĺňa znaky pre rýchlosť, nenáročnosť a celkovú účinnosť.

2.2 Raspberry Pi 2 BLE

Vývojový počítač Raspberry Pi 2 od prvej inštalácie podporuje technológiu Bluetooth a Bluetooth Low Energy , pomocou vstavanej knižnice Bluez. Bluetooth low Energy je možné spustiť na Raspberry Pi pomocou doplnku Blueman, ktorý dokonca spustí GUI Bluetooth, avšak nemusí fungovať so všetkými Bluetooth adaptérmy, tak ako to bolo aj v prípade tejto práce. Kedže väčšina návodov na Bluetooth na Raspberry Pi 2 je vedená s adaptérom CSR ktorý si nahrá svoj firmware správne, Bluetooth s adaptérom CSR funguje normálne. V tejto práci bol k Raspberry Pi 2 priložený a napojený adaptér od firmy ASUS BT-400, ktorý v niektorých prípadoch nenačíta svoj firmware správne a teda nechce spustiť Bluetooth Adaptér. Toto sa dá vyriešiť stiahnutím presného firmware priamo od výrobcu a následne jeho manuálnym prepisom.

Firmware sa nenačíta :



Obr. 2.1: ASUS BT-400 firmware

dmesg | grep -i bluetooth

bluetooth hci0: Direct firmware load for brcm/BCM20702A1-0b05-17cb.hcd failed with error -2

následne treba súbor hex prepísať do hcd tak aby mu systém rozumel :

./hex2hcd BCM20702A1$_0$01.002.014.1315.1347.$hexBCM20702A1-0b05-17cb.hcd$

Po tomto kroku treba skopírovať nový firmware do starej zložky, avšak adaptér nemusí ísť ani potom pretože súbor sa neustále prepisuje na predošly a preto nemohol systém spustiť Bluetooth adaptér.

sudo apt-get install libdbus-1-dev libdbus-glib-1-dev libglib2.0-dev

Aktualizovanie knižnice Bluez na ďalšie využite bluetooth alebo BLE

libical-dev libreadline-dev libudev-dev libusb-dev make
mkdir -p work/bluepy
cd work/bluepy

wget https://www.kernel.org/pub/linux/bluetooth/bluez-5.45.tar.xz tar xvf bluez-5.45.tar.xz

cd bluez-5.45

./configure –disable-systemd

make

sudo make install

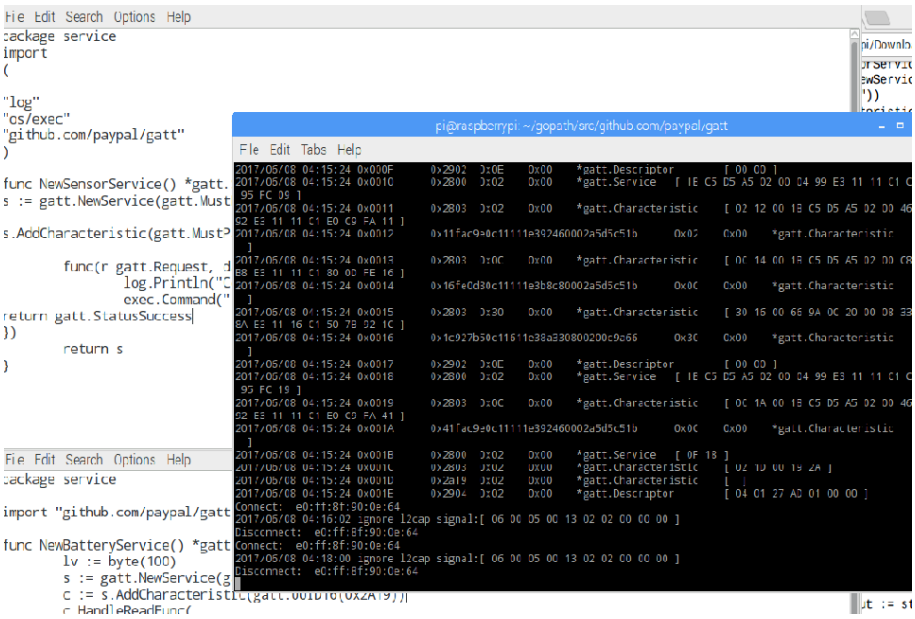
Po nefunkčnej Blueman knižnici pre použitý adaptér, bol použitý Gatt package pre jazyk Go, ktorý prináša podporu BLE do Go jazyka. Generic Attribute Profile(Gatt), umožňuje prenášať malé veľkosti dát, známe ako atribúry pomcou BLE rozhrania. Dôležitá úloha je vytvorenie servera.go a jeho následné spúšťanie pomocou sudo ./server. [16]

go get github.com/paypal/gatt

cd /home/pi/gopath/src/github.com/paypal/gatt

go build examples/server.go

sudo ./server



Obr. 2.2: Spustenie vysielania Gatt serveru

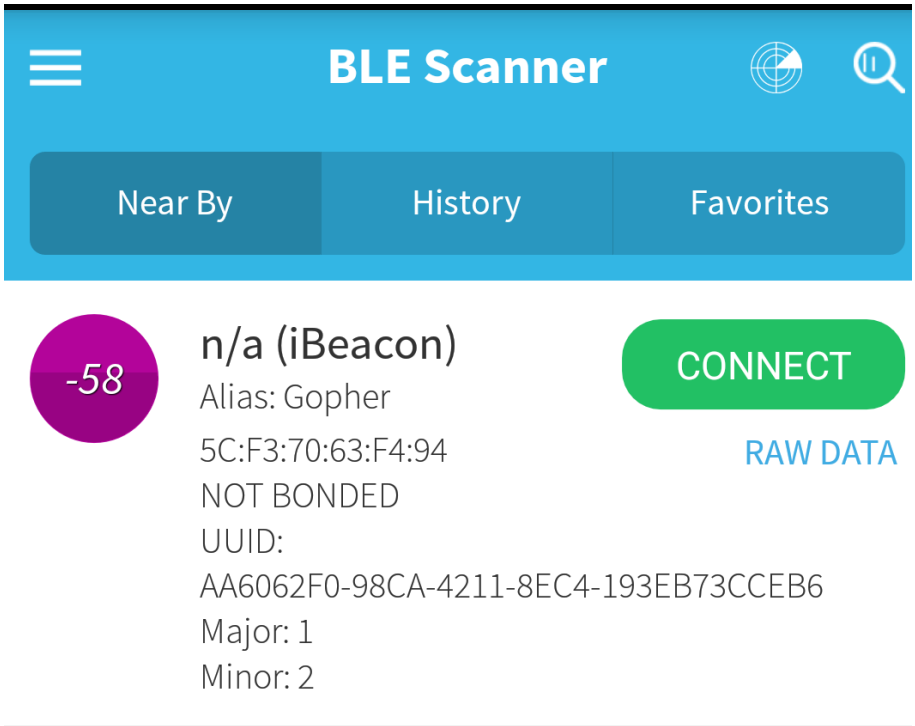
Posledný príkaz incializuje Gatt profily a spustí vysielanie

d.AdvertiseNameAndServices("Gopher", []gatt.UUIDs1.UUID(), sSensor.UUID(), s2.UUID())

Ukážka kódu implementovaného do súboru server.go, telo príkazu s ešte dodatkovými atribútmi/miernou zmenou, vie vykonávať rôzne činnosti - otváranie súborov, reštart dosky, poslanie textu :

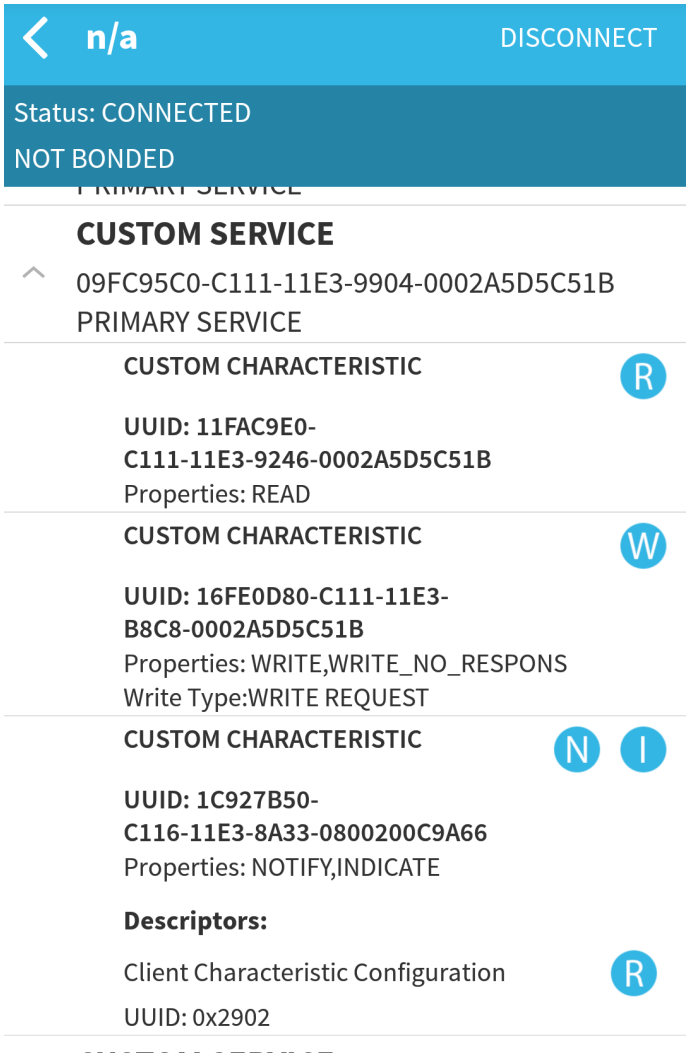
s.AddCharacteristic(gatt.MustParseUUID ("41fac9e0-c111-11e3- 92460002a5d5c51b")).
HandleWriteFunc(func(r gatt.Request, data []byte) (status byte)
log.Println("Command received")
exec.Command("sh", c", "sudo reboot").Output()
return gatt.StatusSuccess)

Pomocou komerčnej aplikácie BLE Scanner je možné overiť či Raspberry Pi vysiela BLE Advertise, Gatt Services .



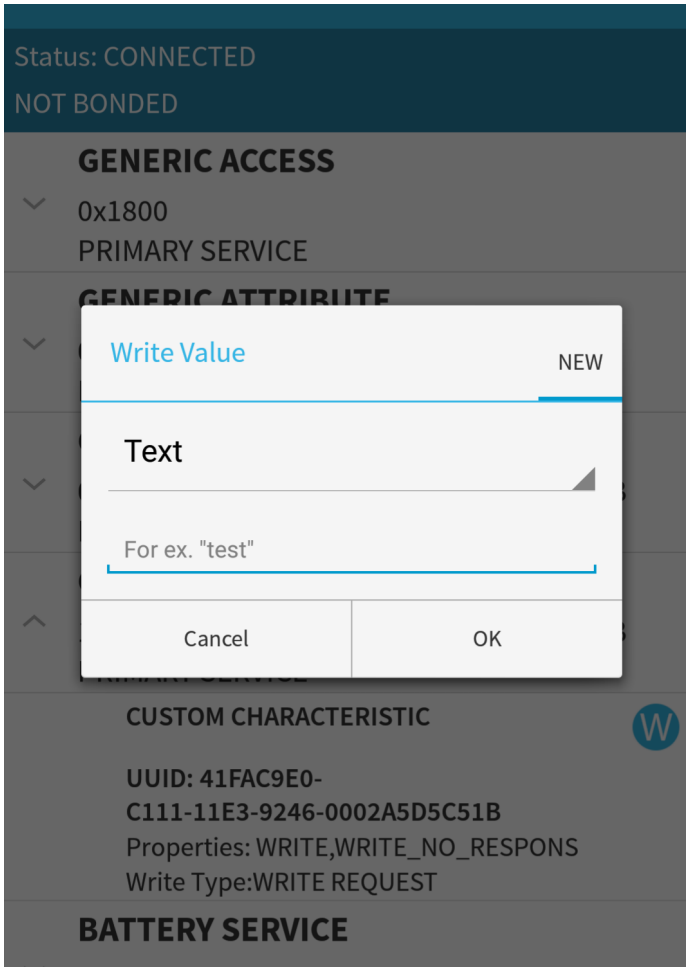
Obr. 2.3: Vysielanie BLE na Raspberry Pi

Overenie Gatt vysielaných služieb cez ktoré bude príkazy posielať aj Android aplikácia



Obr. 2.4: Gatt služby bežiace na Raspberry Pi

Manuálne zadanie textu a odoslanie na dosku



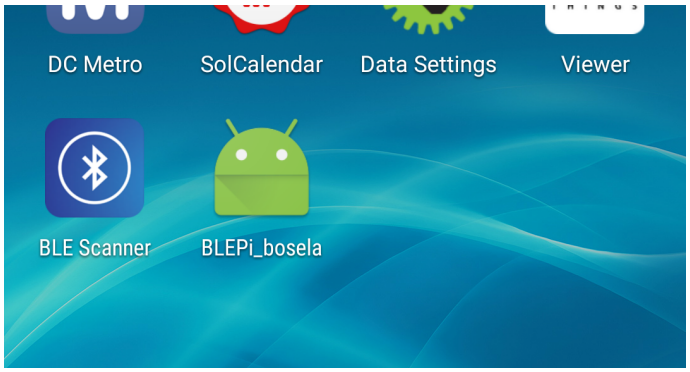
Obr. 2.5: Využie aplikácie na odoslanie textu do RPi pomocou BLE

2.3 Android Aplikácia

Aplikácia na spojenie s Raspberry Pi je programovaná v Android Studiu. Hlavný súbor je **MainActivity.java**, kde sú definované všetký triedy a premenné na inicializáciu Bluetooth, v metóde **ScanCallback scanCallback** je zadefinované skenovanie a následné spojenie s Raspberry Pi ktoré vysiela pod menom Gopher, predtým však ešte bola zadefinovaná metóda **startScan** ktorá obsahuje príkazy na zapnutie rozhrania Bluetooth v prípade, že je vypnuté a potom následne spustenie BluetoothLE(Low Energy). Po doplnení ďalších metód bol vytvorený jednoduchý layout(dve tlačidlá a potvrdzovací text o spojení) následné aplikácia testovaná na pripojenie a poslanie príkazu na reboot do minipočítača Raaspbery Pi, kde príkaz prešiel a počítač sa reštartoval, teda komunikácia na úrovní prenesenia textových príkazov/jednoduchých hodnôt bola funkčná. Aplikácia bola testovaná na mobile Honor 7

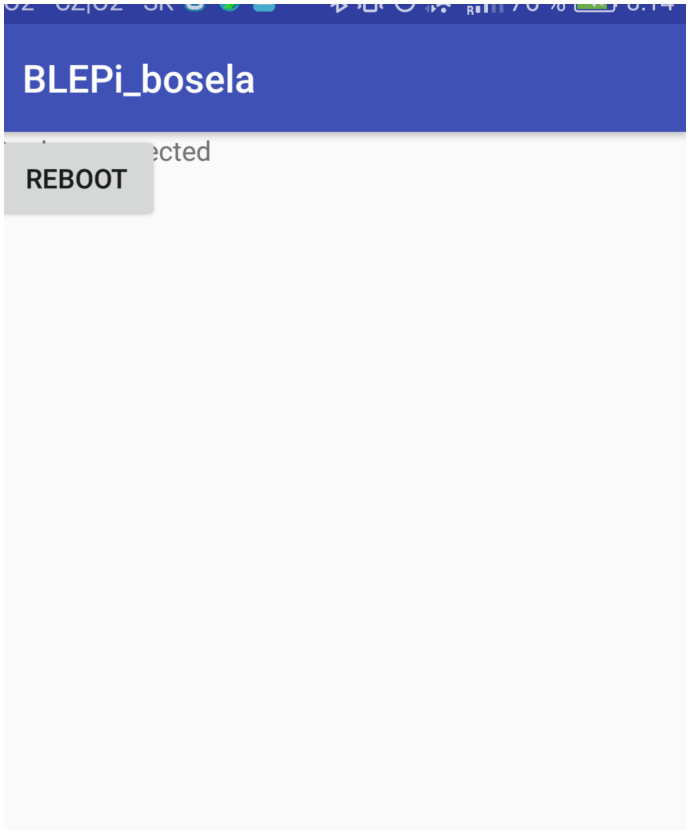
bežiaci na Andride 6.0, aplikácia bola programovaná v Android studio verzie 2.3.2.

Ukážka aplikácie



Obr. 2.6: Aplikacia Android

Layout Aplikácie



Obr. 2.7: Tlačidlo reboot

3 ZÁVER

Cieľom bakalárskej práce bolo zoznámenie sa s autentizáciou nulovou metódou, opísať princíp a konkrétne Zero knowledge protokoly. Autentizovať podľa vybraného protokolu komunikáciu medzi telefónom a minipočítačom Raspberry Pi 2. Celá komunikácia má prebiehať pomocou jednoduchých správ na rozhraní Bluetooth Low Energy.

V teoretickej časti bola rozobraná autentizácia, jej základné typy a v skratke popísaný rozdiel medzi autentizáciou nejakou znalosťou a autentizáciou nulovou znalosťou. Ďalej bol opísaný a jednoducho na príklade jaskyne ilustrovaný princíp autentizácie nulovou znalosťou a opísané tri protokoly nulovou znalosťou, cih výhody, nevýhody, rôzne vlastnosti. Ďalej boli v práci rozoberané technológie Bluetooth, Bluetooth Low Energy a ich špecifikácie, zobrazená protokolová sada a jej využite na rôzne špecifické úlohy(Gatt Server). Ďalej boli pomocou technológie BLE popísané schopnosti technológie IoT a definícia štandardov pre tento účel. V malej miere práca opísala aj mobilný operačný systém Android, jeho podporu pre BLE a vývojovú dosku Raspberry Pi 2, ktorá bola v práci použitá.

V praktickej časti práce bola implementovaná komunikácia medzi zariadeniami. Na strane Raspberry Pi 2 bežal Gatt Server s podporou BLE, na strane telefónu vyskúšaná BLE Android aplikácia, nebol však implementovaný autentizačný protokol, bol len opísaný praktický protokol HM12, ktorý je založený na overovaní nulovou znalosťou.

LITERATÚRA

[1] BURDA, Karel. *Bezpečnost informačních systémů*. 1.vydanie Brno: FEKT VUT Brno, 2005.

[2] QUISQUATER, Jean-Jacques, GUILLOU, Louis C., BERSON, Thomas A. *How to Explain Zero-Knowledge Protocols to Your Children* [online]. 1990 [cit. 10. 12. 2016]. Dostupné z URL:<`http://pages.cs.wisc.edu/~mkowalcz/628.pdf`>.

[3] SCHWARZ, Thomas. *Zero Knowledge Proofs* [online]. 2003 [cit. 10. 12. 2016]. Dostupné z URL:<`http://www.cse.scu.edu/~tschwarz/coen350/zkp.html`>.

[4] HAJNÝ, Ján. *Autentizace pomocí Zero-Knowledge protokolů* [online]. 2008 [cit. 10. 12. 2016]. Dostupné z URL:<`http://crypto-world.info/casop10/crypto09_08.pdf`>.

[5] KNAPP, Jeffrey. *Overview of Zero Knowledge Protocols* [online]. 2009 [cit. 7. 6. 2017]. Dostupné z URL:<`https://www.cs.rit.edu/~jjk8346/paper.pdf`>.

[6] CORON, Jean-Sébastien, NACCACHE, David. *Cryptanalysis of a Zero-Knowledge Identification Protocol of Eurocrypt '95* [online]. 1995 [cit. 11. 12. 2016]. Dostupné z URL:<`http://www.jscoron.fr/publications/zk20.pdf`>.

[7] Wikipedia: the free encyclopedia: *Bluetooth* [online]. San Francisco (CA): Wikimedia Foundation, 2016 [cit. 20. 11. 2016]. Dostupné z URL: <`https://sk.wikipedia.org/wiki/Bluetooth`>.

[8] TOWNSEND, Kevin, Robert DAVIDSON, AKIBA a Carles CUFI. *Getting started with Bluetooth low energy: tools and techniques for low-power networking*. Prvé vydanie. Sebastopol, CA: O'Reilly, 2014. ISBN 978-149-1949-511.

[9] TOWNSEND, Kevin. *Introduction to Bluetooth Low Energy* [online]. 2015 [cit. 29. 11. 2016]. Dostupné z URL:<`https://learn.adafruit.com/introduction-to-bluetooth-low-energy`>.

[10] OLŠAN, Jan. *Bluetooth dostal novou verzi 4.1. Je univerzálnější a chystá se na internet věcí* [online]. 2013 [cit. 29. 11. 2016]. Dostupné z URL:<`https://goo.gl/2zTPrt`>.

[11] VENEZIA, Michael. *BLE 4.1 vs. BLE 4.2 - New Features and Advantages* [online]. 2015 [cit. 03. 12. 2016]. Dostupné z URL:<http://www.semiconductorstore.com/blog/2015/BLE-4-2-vs-BLE-4-1/1548/>.

[12] IMEL, David. *Bluetooth 5 is finally here, bringing 4x the range and 2x the speed* [online]. 2016 [cit. 05. 12. 2016]. Dostupné z URL:<http://www.androidauthority.com/bluetooth-5-734667/>.

[13] ANDROIDDEVELOPER. *Bluetooth Low Energy* [online].2013 [cit. 05. 12. 2016]. Dostupné z URL:<https://developer.android.com/guide/topics/connectivity/bluetooth-le.html>.

[14] ARGENOX TECHNOLOGIES. *Android 5.0 Lollipop brings BLE Improvements* [online].2013 [cit. 05. 12. 2016]. Dostupné z URL:<http://www.argenox.com/blog/android-5-0-lollipop-brings-ble-improvements/>.

[15] KOVACZICZ, Johanna. *Android 6 je oficiálně na světě: Bude nám Marshmallow chutnat?* [online]. 2015 [cit. 07. 12. 2016].KURT, Gökhan. Raspberry Pi Android Projects. Birmingham: Packt Publishing, 2015. ISBN 978-1-78588-702-4.

Dostupné z URL:<https://www.svetandroida.cz/android-6-shrnuti-201509//>.

[16] Kurt, Gökhan, *Raspberry Pi Android Projects*. Prvé vydanie. Birmingham, UK : Packt Publishing, 2015. ISBN 978-1-78588-702-4.

[17] JAVŮREK, Karel. *Raspberry Pi 2: šestkrát vyšší výkon ve stejném balení* [online]. 2015 [cit. 07. 12. 2016]. Dostupné z URL:<http://www.zive.cz/clanky/raspberry-pi-2-sestkrat-vyssi-vykon-ve-stejnem-baleni/sc-3-a-177031/default.aspx//>.

ZOZNAM SYMBOLOV, VELIČÍN A SKRATIEK

BLE	bluetooth s nízkou spotrebou energie – Bluetooth Low Energy
PAN	osobná sieť – Personal area network
BSIG	špeciálna záujmová skupina Bluetooth – Bluetooth Special Interest Group
IoT	internt vecí - Internet of Things
GAP	generický prístupový profil – Generic Access Profile
GATT	generický profil atribútov – Generic Attribute Profile
L2CAP	logický linkový kontrolný a adaptačný protokol – Logical Link Control and Adaption Protocol
GATT–less	profily s menším GATT základom
GPS	globálny pozičný systém – Global Position System
ATT	protokol atribútov – Attribute protocol
SM	vrstva bezpečného manažmentu – Security manager
HCI	hostiteľské kontrolné rozhranie – Host Controll Interface
LL	linková vrstva – Link Layer
PHY	fyzická vrstva – Physical Layer
P	vlastník, držiteľ – Prover
V	overovateľ - Verifier