

Review of Bachelor's Thesis

Student: Kamenský Timotej
Title: Prototype of Intrusion Solution for Mobile Networks (id 24557)
Reviewer: Letavay Viliam, Ing., DIFS FIT BUT

- 1. Assignment complexity** **more demanding assignment**
Študent v práci teoreticky popísal útoky na WiFi a mobilné siete GSM a LTE. Následne navrhol a implementoval prototyp nástroja na zvolené útoky na LTE za pomoci SDR. Z dôvodu komplexity LTE sietí a práce s nimi, hodnotím zadanie ako náročnejšie.
- 2. Completeness of assignment requirements** **assignment fulfilled**
- 3. Length of technical report** **in usual extent**
- 4. Presentation level of technical report** **62 p. (D)**
Logická štruktúra a obsah vybraných častí práce má niekoľko nedostatkov:
 - Na kapitolu o útokoch na WiFi siete sa v práci ďalej nijako nenadväzuje - téma ide do stratená.
 - Pred popisom útokov na mobilné siete GSM a LTE chýba architektonický popis týchto sietí. Takto sa v texte odkazuje na protokoly, procesy a správy ktoré nie sú pred tým vysvetlené. Tento problém je zvýraznený v sekciách obsahujúcich výňatky z LTE štandardu.
 - V kapitole 5 (Design) chýba popis návrhu softwarovej časti riešenia.
- 5. Formal aspects of technical report** **70 p. (C)**
Práca bola vysádzaná za použitia fakultnej šablóny pre systém LaTeX. Jazykovo je na dobrej úrovni. Po formálnej stránke avšak obsahuje niekoľko nedostatkov:
 - Obsahuje obrázky a tabuľky na ktoré sa v texte neodkazuje.
 - Nevhodné použitie tabuliek miesto sekvenčných diagramov.
 - Miestami použité neformalizmy pôsobia rušivo.
- 6. Literature usage** **80 p. (B)**
Viacere tvrdenia nie sú podložené referenciou na literatúru. Okrem toho ale študent pracoval s dostatočne širokou a rôznorodou množinou zdrojov. Veľké zastúpenie mali online zdroje, čo je ale pre praktický charakter práce pochopiteľné.
- 7. Implementation results** **90 p. (A)**
Študentovi sa podarilo prísť na elegantný spôsob realizácie LTE útokov za využitia modulárneho charakteru nástroja srsRAN. Vďaka tomu je možné implementovať vybrané útoky na úrovni S1AP protokolu, abstrahujúc tak implementáciu samotnej rádiovkej časti LTE BTS.
Výslednej implementácií avšak chýba test s ďalšou (simulovanou) BTS v blízkosti, aby sa testovacie podmienky o niečo viac blížili testovaniu mimo Faradayovej kľetky.
- 8. Utilizability of results**
Výsledky práce môžu byť využité ďalej pri analýze bezpečnosti LTE sietí za pomoci srsRAN stacku a SDR.
- 9. Questions for defence**
 - BladeRF SDR má dva kanály, pričom v práci pracuje len s jedným. Možnosti rozšírenia prototypu o využitie druhého kanálu ?
 - Možnosti využitia SDR pri útokoch na WiFi ?
 - Čím by bolo možné vysvetliť rozdielne chovanie testovacích zariadení oproti očakávanému chovaniu zo zdrojovej literatúry ?
- 10. Total assessment** **75 p. good (C)**

Implementovaný prototyp je funkčný, no jeho testovanie by mohlo byť dôslednejšie. Text práce zároveň obsahuje svoje nedostatky. Navrhujem preto hodnotenie C.

In Brno 1 June 2022

Letavay Viliam, Ing.
reviewer