POSUDOK OPONENTA NA DIPLOMOVÚ PRÁCU:
Bc. Petra Fritzová, Bezpečnost elektronického hlasování

Predložená práca sa zaoberá bezpečnosťou elektronických volieb. V úvode študentka uvádza základné pojmy z oblasti informačnej bezpečnosti. Nasleduje stručný úvod do kryptografie a podkapitola detailnejšie popisujúca vybrané bezpečnostné hrozby. V nej je uvedených niekoľko obecnejších pojmov ako malware a man-in-the-middle útok a viacero konkrétnych techník ako ARP spoofing, ICMP redirecting a ďalšie. Popis týchto techník ale príliš nezapadá do širšieho obsahu práce, ktorá sa snaží venovať bezpečnosti elektronických volieb a nie (web) aplikačnej bezpečnosti. Uvedené technické detaily aj úvod kryptografie obsahujú viacero nepresností.

Druhá kapitola začína popisom požiadaviek na "ideálny elektronický volebný systém". Ďalej sa autorka venuje vzťahom medzi jednotlivými požiadavkami, uvádza tézy, riešenia a ich dôsledky. Predpokladám, že táto časť práce je pôvodná (nie je uvedená žiadna referencia). Text druhej kapitoly je často vágny ("zabezpečení na algebraicko-kryptografické úrovni", "požadavky ... v jistém smyslu kolidovali"). Nejasne definované požiadavky znemožňujú lepšiu analýzu. Navrhnuté riešenia sú príliš povrchné. Napríklad riešenie 2.2 na strane 44 uvádza: "Aplikace by mohla provést zašifrování hlasu a digitální podpis", ale neuvádza akými kľúčmi. Riešenie 5.2 na strane 49 tvrdí, že sa zvýši utajenie odovzdaných hlasov tým, že budú v uložené vo viacerých databázach a nie iba v jednej. Riešenie autorka uzatvára vetou "Každá databáze by byla samostatně zašifrována jiným klíčem.". Pre chýbajúce detaily ale riešenie nedáva zmysel.

Kapitoly 3 a 4 popisujú projekt elektronických volieb SERVE a systém elektronických volieb v Estónsku a obsahujú iba malé množstvo nepresností. V úvode kapitoly 5 nájdeme jednoduché porovnanie týchto dvoch projektov. V ďalších podkapitolách autorka popisuje technické útoky. Tu by som vytkol napríklad silné predpoklady (útočníkovi sa podarí podvrhnúť certifikát volebného serveru, útočník je na rovnakej sieti ako volebný server atď) a niekoľko nejasností (poznámka 37 na strane 87 - prečo by server pre každé spojenie generoval nové asymetrické kľúče?). Na niektorých miestach autorka zachádza do technických detailov, inde kde by to bolo vhodné sa im ale vyhýba.

Celkovo hodnotím prácu ako príliš popisnú, málo odbornú a na mnohých miestach bohužiaľ až vágnu. Práca sa taktiež zbytočne detailne zaoberá softwarovou a hardwarovou stránkou elektronických volieb. Vzhľadom na obor práce by bolo oveľa vhodnejšie venovať sa kryptografických protokolom pre elektronické voľby a nie ich technickému a procesnému zabezpečeniu. Podkapitola 2.3 má už s oborom práce takmer nulový prienik. Študentka v práci nepreukázala hlbšie znalosti matematiky ani kryptografie. Jazyková a formálna úroveň práce je priemerná.

Predloženú prácu doporučujem k obhajobe.

Praha, 5.5.2013 Michal Hojsík