POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Název: Konkrétní bezpečnost protokolu IPSec
Autor: Marie Švarcová

Shrnutí obsahu práce

Práca si kladie za cieľ formuláciu dôkazu bezpečnostných vlastností protokolu IKE, prostredníctvom ktorého dochádza k dohode na kľúčoch v protokole IPSec. Prvú kapitolu tvorí úvod do asymptotickej a konkrétnej dokázateľnosti kryptografických protokolov. Nasleduje popis protokolu IPSec a popis modelovania protokolu a útočníkov naň. Jadrom práce kapitola 6, ktorá obsahuje dôkaz zjednodušeného protokolu $\sum_0$ v kontexte konkrétnej bezpečnosti. Dôkaz pozostáva z preukázania dvoch vlastností definície (t, q, δ, ε)-SK-bezpečnosti. Prvá vlastnosť vyjadruje hodnotu pravdepodobnosti kedy môže útočník nepozorovane narušiť výmenu tajného kľúča tak, že účastníci protokolu zdieľajú kľúč s útočníkom pričom veria, že komunikujú so svojou legitímnou protistranou. Druhá vlastnosť vyjadruje obmedzenie útočníka pri rozlíšení skutočnej hodnoty kľúča sedenia (session key) od náhodnej hodnoty pomocou testovacích sedení (test session). Práca je zakončená záverom a vysvetlením prechodu naspäť od zjednodušeného protokolu $\sum_0$ k protokolu IKE.

Celkové hodnocení práce

Téma práce. Dôkazy konkrétnej bezpečnosti protokolov sú náročné a v praxi často opomínané. Zadanie práce bolo dobre spracované a dodržané.

Vlastní příspěvek. Práca obsahuje argumenty a postup už existujúceho dôkazu konkrétnej bezpečnosti protokolu IKE, na ktorom bezpečnosť IPSec stojí. Autorka ho doplňuje originálne o explicitne vyjadrenie bezpečnosti pomocou hodnôt parametrov vety 1.

Matematická úroveň. Matematická úroveň textu je obdobná textom publikovaným v oblasti dokázateľnej bezpečnosti. Rigorózne a formálne sledovanie dôkazov je náročné vyžaduje pomerne mnoho doplňujúcich vysvetlení.

Práce se zdroji. Zdroje, z ktorých autorka čerpá, sú v práci prehľadne uvedené a postup práce s nimi je popísaný v podkapitole 1.1. Autorke sa nedá uprieť snaha o vlastné vysvetlenie termínov a postupov a v žiadnom prípade nejde o „otrocký preklad“.

Formální úprava. Úprava práce po formálnej stránke je na veľmi dobrej úrovni.

Připomínky a otázky

1. Dôkaz druhej vlastnosti v kapitole 6 je značne náročný a technický, uvedená postupnosť pomocných tvrdení je ťažko kontrolovateľná a zaslúžila by si podrobnejší popis myšlienky dôkazu. Značne rozpačito pôsobia chýbajúce dôkazy Lem 9 – 12 a Lemy 13 bez vysvetlenia alebo odkazu do literatúry. Lema 11 v dôkaze vlastnosti zdá sa vôbec nie je použitá.
2. Aké boli praktické dôvody na prechod k verzii protokolu IKEv2

Závěr

Práci považuji za velmi dobrou a doporučuji ji uznat jako diplomovou práci.

Návrh klasifikace vedoucí/oponent sdělí předsedovi zkušební (sub)komise.

Jméno oponenta: Daniel Joščák podpis
Pracoviště: NN Management Services, s.r.o.
Datum: 2. 9. 2015