Posudek vedoucího bakalářské práce

Název: Vulnerabilities and security proofs of communication protocols used by malware
Autor: Ondřej Med

Shrnutí obsahu práce

Práce se zabývá dokazováním vlastností kryptografických schémat a protokolů. V první kapitole jsou představeny základní definice, tvrzení a prostředky pro analýzu a dokazování vlastností vybraných protokolů. Tyto jsou následně využity v následující kapitole, kde je zároveň představen Cryptoverif a na syntakticky přímočařejším příkladě na šifrování používaném variantou Miraie (rodina/kmen malwaru) je ilustrováno použití představených technik a nástrojů. V následujících dvou kapitolách jsou představena další schémata používaná rodinami malwaru Emotet a LockCrypt. Vlastní příspěvek autora se nachází především v druhé půlce práce, ať už na úrovni formalizace problémů nebo konstrukce samotných důkazů a zranitelností.

Celkové hodnocení práce

Téma práce. Téma práce bylo na bakalářskou práci zvoleno spíše náročné. Požadovaná literatura a materiály měly tématicky široký záběr, navíc mnohé zdroje obsahovaly nepřesnosti nebo používaly méně formální popisné prostředky. Zadání práce bylo jednoznačně naplněno.

Vlastní příspěvek Vlastní příspěvek studenta je na několika úrovních. Práce si vyžádala formalizaci a případné upřesnění faktů z některých zdrojů. Ačkoliv některé důkazy (přesněji z posledních dvou kapitol) byly přímočaře formulovatelné v jazyce Cryptoverifu, ilustrativní příklad šifrování Miraie vyžadoval kreativní obejití omezení tohoto nástroje.

Matematická úroveň Práce obsahuje rigorózně zformulovaný matematický text v průběhu většiny kapitol. Matematická úroveň práce odpovídá tématu z oblasti aplikované matematiky (kryptografie). Od práce nelze očekávat obecná matematická tvrzení, ale spíše formalistický přístup k obvykle ryze aplikovaným tématům. Nicméně v některých momentech by si práce zasloužila podrobnější vysvětlení nebo diskusi.

Práce se zdroji Práce si ze zdrojů vypůjčuje některé definice, především v kompilační části práce, kde je občas výhodné mít více pohledů k témuž pojmu. Kromě knižních zdrojů taktéž konzultoval některé přístupy k problémům s autorem Cryptoverifu.

Formální úprava Formální úprava je na velmi dobré úrovni, je napsaná kvalitní angličtinou, byť bohužel se nepodařilo vyhnout některým překlepům. Menší připomínky by byly k formátování, především u bloků kódu.

Závěr

Práce Ondřeje Meda „Vulnerabilities and security proofs of communication protocols used by malware"splňuje zadání a dosahuje požadované úrovně. Proto práci doporučuji k přijetí s hodnocením *velmi dobře*.

Adolf Středa
Katedra algebry
13.6.2023