Oponentský posudek bakalářské práce

Ondřeje Meda

nazvané

Vulnerabilities and security proofs of communication protocols used by malware

Předložená práce má za cíl aplikovat automatické dokazovací systémy pro kryptografické hry na známé protokoly používané v malware.

Je rozdělena do čtyř kapitol. V prvních kapitole popisuje použitý matematický aparát. Ve druhé kapitole je představen nástroj Cryptoverif který je v následujících dvou kapitolách použit pro analýzu protokolů malware Emotet a LockCrypt. Je napsaná dobrou angličtinou.

Vytyčeného cíle bylo bezpochyby dosaženo. Nebylo to však bez ztrát, obsahuje netriviální množství chyb, které by bylo lehké odstranit jedním až dvěma přečteními navíc. Kupříkladu:

- Místo pomlčky je několikrát použit mínus.
- V definici 1 se nerozlišuje mezi množinou všech zpráv (klíčů) $\mathcal{M}$ ($\mathcal{K}$) a náhodných veličin M (K). Chybí tečka za $P[M = m]$.
- V sekci 1.3 se mluví o útočnících pracujících v čase $O(n^k)$ aniž by bylo definováno k.
- V sekci 1.4 chybí velká písmena na začátku vět, je použito slovo *cipher* místo *encrypt*.
- V sekci 1.5 se mluví o generátoru nepojmenované grupy. Tato je ke konci pojmenována G. Předpoklad, že g generuje podgrupu G řádu q není zmíněn. Je psáno $args$ ve smyslu `args`.
- V sekci 1.6 chybí *s* na konci slova *term*.
- V sekci 2.2 je psáno $<-$ místo $\leftarrow$, to samé v dalších výpisech kódu.
- V sekce 2.2.1 je v nadpisu psáno *primitiva* místo *primitives*.
- Ve výpisech kódu je navíc ~, kterou měl TEX odstranit, ale neudělal to.
- V nadpisu kapitoly 4 je psáno *inpsired* (sic!) místo *inspired*.

V rámci obhajoby bych si rád poslech detailnější vysvětlení definice 1.

Navrhuji, aby práce byla přijata jako práce bakalářská a ohodnocena známkou velmi dobře.

V Praze dne 13. června 2023 Milan Boháček