POSUDEK VEDOUCÍHO BAKALÁŘSKÉ PRÁCE

Název: Kryptografické útoky na TLS protokol
Autor: Jan Oupický

Shrnutí obsahu práce

Práce pojednává o komunikačním protokolu TLS/SSL a několika vybraných útocích na tento protokol. Po dvou úvodních kapitolkách týkajících se značení a základních definic přichází jádro práce ve třetí a čtvrté kapitle. Třetí kapitola obsahuje podrobný popis TLS/SSL protokolu a historii modifikací protokolu. Čtvrtá kapitola pak ukazuje čtyři dříve publikované útoky na tento protokol. Práce je tedy převážně kompilační, pouze poslední kapitla přináší drobné vlastní příspěvky autora v podobě matematických tvrzení doplňujících některé nejasně popsané části útoků v původních zdrojích, případně výpočty ukazující efektivitu útoků a jejich praktickou použitelnost.

Celkové hodnocení práce

Téma práce. Téma práce je přiměřené bakalářské práci. Náročnost tématu spočívá spíš v nutnosti probrat se informatickou literaturou. Zadání práce bylo splněné, trochu mi schází praktická implementace některého z útoků, nicméně tato implementace nebyla v zadání práce.

Vlastní příspěvek. Vlastní příspěvek autora spočívá v matematických formulacích časové náročnosti útoků v poslední části práce.

Matematická úroveň. Práce obsahuje rigorózně zformulovaný matematický text v posledních dvou kapitolách. Matematická úroveň práce odpovídá tématu na pomezí matematiky a informatiky. Nelze zde očekávat obecná matematická tvrzení, jde spíš o pracné zkoumání jednotlivých bytů v otevřených a šifrovaných zprávách a „hackerské“ využití drobných pochybení v protokolu.

Práce se zdroji. Práce neobsahuje žádné zkopírované nebo otrocky přeložené pasáže z jiných zdrojů. Uvítal bych uvedení použitých zdrojů přímo v částech, které z těchto zdrojl vycházejí, nikoliv pouze v seznamu literatury. Jde zejména o zdrje použité v poslední kapitole o útocích.

Formální úprava. Formální úprava práce je na výborné úrovni. Je napsána kvalitní češtinou, drobné výhrady lze mít spíš k některým formátovacím pochybením, které ale nijak neovlivňují čitelnost práce..

Připomínky a otázky

1. Při obhajobě uveďte prosím originální zdroje pro jednotlivé útoky ve čtvrté části.
2. V případě útoku POODLE uvádíte na začátku ilustraci pomocí komunikace se SISem. Jak daleko se lze s tímto útokem na současnou verzi SISu dostat?

Závěr

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

Doc. RNDr. Jiří Tůma, DrSc

Katedra algebry MFF UK

3.6.2019