

Oponentský posudek bakalářské práce

Jana Oupického

nazvané

Kryptografické útoky na TLS protokol

Předložená práce má za cíl představit protokol TLS a některé kryptografické útoky na něj.

Je rozdělena celkem do čtyř kapitol. V prvních dvou kratičkých kapitolách jsou představeny definice a „slovníček“. Ve třetí kapitole je popsán protokol SSL 3.0, TLS 1.0 a TLS 1.1. V textu je pak už jen letmo zmíněna existence TLS verze 1.2 a 1.3, což je trochu škoda, protože obzvláště verze 1.3 obsahuje řadu vylepšení. V poslední kapitole jsou rozebrány některé staré útoky na protokol SSL/TLS.

Až na dále vzpomínané chybičky je práce celkem čtivě napsaná. Obzvláště se mi líbí použití vlastní komprimační metody v útoku CRIME, která umožnila popsat podstatu problému aniž by bylo potřeba zabředávat do detailů skutečných komprimačních algoritmů.

Trochu je škoda, že text obsahuje množství drobných chyb, které by bylo lehké odstranit, kdyby práce obsahovala i implementační část, kupříkladu:

- Ve všech zápisech HMACu chybí xor a je místo něj konkaténace.
- Hodnoty konstant *opad* a *ipad* nejsou nikde zmíněné.
- Na straně 17 ve vzorci 3.2 vypadl *ipad*.
- Na straně 34 se v POST requestu dvakrát posílá hlavička „Cookie“. To je však explicitně zakázané v RFC6265 [1].
- Útok POODLE je představován na serveru <https://sis.cuni.cz>. Ten je však podle [2] proti tomuto útoku imunní.

Otázky na studenta: Jaký význam mají konstanty *opad* a *ipad* v HMACu? Ochranu proti jaké slabině zajišťuje dvojité hashování v konstrukci HMACu?

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

Odkazy:

[1] <https://tools.ietf.org/html/rfc6265#section-5.4>

[2] <https://www.ssllabs.com/ssltest/analyze.html?d=sis.cuni.cz&s=195.113.89.1>

V Šanghaji dne 11. června 2019

Milan Boháček