Úlohy na precvičenie – OPS 2019 – séria E

Úlohy riešte samostatne a podrobne. Celý postup zaznamenajte a komentujte. Odpovedajte podľa možnosti na všetky položené otázky v úlohe. V záhlaví uveďte svoje meno, priezvisko a zdroje, ktoré ste pri riešení použili (citácie, URL adresy internetových zdrojov a mená osôb, s ktorými ste riešenie prípadne konzultovali). Za každé správne a vyčerpávajúce riešenie (s komentovaným postupom) možno získať bod (ak nie je uvedené inak). Zlomky bodov možno získať aj za čiastočné riešenia. Riešenia odovzdajte do 2. 4. 2019, 14:25 (do začiatku prednášky). Riešenia pred termínom môžete odovzdať na sekretariáte Ústavu informatiky do môjho priečinka. Neskôr dodané a opisované riešenia nebudú opravované ani hodnotené. Problémy môžete konzultovať po prednáške alebo elektronickou poštou na adrese jirasek at upjs.sk.

1. TCP spojenie (trojfázový handshake aj s jednoduchou odpoveďou) s austrálskou webovou stránkou trvalo 20 ms. Bude server geograficky v Austrálii? Dalo by sa odhadnúť jeho umiestnenie?

2. (2 body) Odsledujte Wiresharkom priebeh TCP relácie pri otvorení stránky https://www.google.com – odfiltrujte príslušný TCP stream a vypíšte použité štartovacie sekvenčné čísla (so SYN príznakmi) klienta aj servera a ich potvrdenie. HTTPS protokol používa TLS reláciu, tak zapnite dekódovanie TLS. Vypíšte dve najpreferovanejšie sady algoritmov, ktoré podporuje klient a vybratú sadu algoritmov zo strany servera (podľa skratiek identifikujte príslušné konkrétne algoritmy a ich určenie). Bola zriadená nová relácia, obnovená relácia alebo len nové spojenie (connection) v rámci existujúcej relácie (session)? Ako sa autentifikoval server? Nájdite CCSP správy pre začiatok šifrovaného prenosu. Komentujte aj spôsob ukončenia celého TCP streamu.

3. (2 body) Odsledujte Wiresharkom priebeh TLS relácie spojenia so stránkou AISu (prihlásenie a odhlásenie). Zase odfiltrujte a dekódujte príslušný TLS stream. Vypíšte sadu algoritmov (nie len skratky), ktorú vybral pre spojenie server AIS. Nájdite náhodné čísla klienta a servera a zašifrované PreMaster Secret tajomstvo (potrebujete na to úplný začiatok relácie). Vysledujte príslušné CCSP správy na oboch smeroch komunikácie a pozorujte štruktúru RLP aplikačných fragmentov. Porovnajte ukončenie príslušnej TCP relácie s ukončením relácie pre https protokol (v úlohe 2).

5. (2 body) Vysledujte certifikáty servera AIS v spojení z úlohy 3 – ktorá certifikačná autorita podpísala certifikát pre AIS a ktorá autorita je pre ňu koreňovou? Dokedy trvá platnosť certifikátu pre AIS? Vypíšte prvé štyri bajty verejného kľúča AIS a na čo je možné tento kľúč používať. Vypíšte tiež prvé štyri bajty podpisu certifikátu - ktorý kľúč a ktorý algoritmus by ste použili na kontrolu správnosti certifikátu AIS? Sú v protokole všetky potrebné informácie na overenie certifikátu AIS (resp. čo by sme ešte potrebovali na jeho úplné overenie)?

Výsledky pozorovaní môžete zapísať ručne, alebo vytlačiť stream (resp. jeho dôležité časti – začiatok a ukončenie) a v ňom okomentovať príslušné javy, prípadne okomentovať (zvýraznene) do elektronického dokumentu a poslať e-mailom na moju adresu upjs.sk.