

FDABnet

Mikita Alchimionak

Počas tohto semestra boli implementované programy v jazyku C s CLI rozhraním pre prostredie Linux: **node-gen** (pre generáciu uzla, čiže master key mining) a **ct-man** (pre manipuláciu s **challenge-table**). Pre vývoj bolo rozhodnuté použiť open-source knižnice **monocypher** (minimalistická kryptografická knižnica) a **yespower** (Proof-of-Work knižnica) a toto je jediné externé, čo sa objaví v tomto projekte, pretože pre účely takéhoto protokolu je postačujúce použitie štandardných lib knižníc. Algoritmus **yespower** bol vybraný kvôli tomu, že je zameraný na pro-CPU a anti-GPU efektivitu výpočtu.

Program **node-gen** po spustení nastaví politiku **SCHED_IDLE** a bude zatažovať procesor niekde na 100 %, pokiaľ nie je potrebný na nejaké iné ľubovoľné účely. Začne pseudonáhodným číslom z **/dev/urandom** pre seed, ktorý sa v nekonečnom cykle inkrementuje od najvýznamnejšieho bajtu, teda v big-endian, kvôli generácii privátneho a verejného kľúča pomocou algoritmu **eddsa** implementovaného v knižnici **monocypher**, následne odvodí hash z verejného kľúča. Ak hash má prefix **FDABFDABFDAB...** aspoň minimálnej dĺžky pre zachovanie, tak ho zachová. Úspešný nález je signalizovaný znakom z 36-tkovej sústavy, pričom po každých 32 iteráciách sa pre vizuálnu kontrolu vypíše bodka. Dodatočne je možné zaplniť **challenge-response** tabuľku hashami nedostatočne „kvalitnými“, recyklujú sa na následné použitie pre verifikáciu rangu neznámeho uzla. Je to mechanizmus zamyslený proti Denial of Service útoku. Pred začiatkom v takom prípade sa rezervuje priestor na disku rozmerom s predvolenou veľkosťou 64 MiB (2^{20} defaultný rozmer tabuľky z buniek pozostávajúcich z hasha a verejného kľúča, teda $32 + 32 = 64$ bajtových buniek) a pamäť sa zobrazí pomocou **mmap** na disk. Zachovanie challenge na začiatku prevráti 8 prvých bajtov a vydelí rozmerom tabuľky a dostane index. Kvôli prevencii chýb s prerušením, kopírovanie prvých 8 bajtov verejného kľúča sa deje na konci. Algoritmus **yespower** s vybranou konfiguráciou bude potrebovať 256 MiB pre RAM: **yespower_param_n_value** (N) = 65536, **yespower_param_r_value** (r) = 32, $128 \times 65536 \times 32 = 2^{7+16+5} = 2^{28} = 256$ MiB.

Program **ct-man** realizuje podprogramy pre spracovanie **challenge table**, používajúce tiež **mmap**. Konkrétne **scan** dá vedieť rozmer a ako je plná, **poscheck** overuje, či sedí tabuľkový index s prvými 8 bajtmi, **fill** slúži na naplnenie posledného 1 % prázdnych buniek, **cannibal** - to je tragikomédia: kanibal s menom **canny** (prvá tabuľka) zožerie **dinny** (druhá tabuľka), teda svoj **dinner**.