Logjam – dug koji je stigao na naplatu

Korištenje prastarih tehnologija kad tad dolazi na naplatu, bilo da je riječ o zastarjelom hardveru, operacijskom sustavu kojem je istekao životni vijek, općenitom softveru koji se više ne održava, a prema nekolicini sigurnosnih problema koji su se pojavili u zadnjih godinu ili dvije dana, to vrijedi i za korištenje zastarjelih sigurnosnih alata.

Logjam [1] je dobar primjer škole koju nismo naučili. Slično kao i FREAK napad, Logjam nastoji u komunikaciju između web klijenta (pretraživača, aplikacije...) i poslužitelja ubaciti instrukciju koja će komunikaciju između dvije točke "spustiti" na stare, tzv. "export-grade" algoritme zaštite podataka.

Sjetimo se, *export-grade* algoritmi ostatak su prošlosti, kad je američka administracija zabranila izvoz kriptografskih alata koji su svojom kompleksnošću prelazili određenu razinu. Razlog tome bila je zaštita nacionalnih interesa, ali i "neslužbeno" ostavljanje mogućnosti agencijama da presretnu i dešifriraju promet koji iz zanima.

Desetljećima kasnije, taj zaboravljeni uvjet, koji je zbog kompatibilnosti i dalje implementiran na mnogim mjestima, postaje neuralgičnom točkom jer napredak računalne snage omogućuje ne samo državama, već i zainteresiranim organizacijama, pa i pojedincima – razbijanje *export-grade* algoritama, što korisnike tehnologije ostavlja izloženima praćenju ne samo državnih agencija već i krimi-miljea.

Logjam napad zahtjeva aktivnog napadača, tj. ubacivanje u komunikacijski kanal između dvije točke (MITM). Jednom infiltriran, napadač može nagovoriti poslužitelj na spuštanje razine kriptografske zaštite na nivo 512-bitnog Diffie-Hellman [2] algoritma.

Ranjivost Diffie-Hellman algoritma poznata je već dvadeset godina, no složenost propusta smatrana je dovoljno računalno intenzivnom da u bliskoj budućnosti probijanje zaštite čini praktično neizvedivim (vidi https://www.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/discrete-logarithm-problem [3]).

Tako je bilo prije dvadeset godina. Danas je računalna infrastruktura značajno moćnija i u stanju je grubom silom razbiti 512-bitni export-grade DH algoritam. Veliku pomoć u tom procesu daje nedavno otkriveni matematički trik koji omogućava značajno kraćenje vremena razbijanja zaštite: izračunom diskretnog logaritma prim broja, vrijednosti se mogu sačuvati i ponovo koristiti za druge module, čime se potraga za pravom kombinacijom drastično ubrzava: 512-bitni DH algoritam moguće je razbiti u nekoliko minuta, nakon čega napadač može u potpunosti preuzeti kontrolu nad komunikacijskim kanalom.

Praktično, riječ je o nekoj vrsti Rainbow tablica [4] za razbijanje DH algoritma. Nešto je kompliciraniji slučaj prilikom napada na DH algoritam koji nije u klasi zastarjelih export-grade algoritama: primjerice, korištenje 1024-bitnog DH algoritma i dalje je vrlo popularno na Internetu. Kako je riječ o značajno kompleksnijem prim broju, Logjam napad nije praktično izvediv. No, poznavajući gore navedeni matematički trik, moguće je značajno ubrzati i ovaj napad: za razbijanje jednog 1024-bitnog ključa potrebno je (u mjerilima današnje tehnologije) nekoliko milijuna računala uposliti na godinu dana, ali ako već postoje tablice unaprijed izračunatih diskretnih logaritama barem dio ključeva postaje moguće razbiti, pretpostavlja se, unutar 30 dana.

Naravno, i dalje je to dugotrajna i vrlo skupa operacija, no napadač ne mora biti u strci: dovoljno je na sigurno pospremiti kopiju digitalne razmjene informacija jer u ovom slučaju napadač ne mora biti

MITM: jednom pospremljena kopija podataka uvijek je na dohvatu ruke, a napadač se samo treba strpiti da bi došao u mogućnost razbiti enkripciju i dobiti uvid u sve spremljene podatke iz komunikacijskog kanala.

Ovakve napade mogu izvesti države i odgovarajuće državne organizacije, dok je kriminalnim grupama vjerojatno još uvijek financijski neisplativo razbijati ključeve. To će se gotovo sigurno promijeniti za pet do deset godina. U međuvremenu možete biti relativno mirni što se tiče ove vrste napada: oni će biti rezervirani za osobe koje je iz nekog razloga važno prisluškivati i institucije čije bi tajne informacije mogle vrijediti vrlo velike novce. No, kao i kod *export-grade* algoritama, zanemarivanje činjenice da algoritam ima ozbiljne sigurnosne propuste mogao bi postati još jedan dug koji će u budućnosti doći na naplatu.

Zato je najbolje djelovati odmah [5]: možda je najvažniji korak zabrana *export-grade* algoritama na poslužiteljima, jer je riječ o zastarjelim tehnologijama koje danas uistinu postoje samo radi kompatibilnosti sa prastarim sustavima i prastarim softverom. Praktično, ne postoji moderni sustav niti moderni softver koji bi ukidanjem podrške za te algoritme prestao raditi.

Što se 1024-bitnog DH algoritma tiče, on je, smatraju istraživači koji su otkrili propust, preferirani algoritam na jednoj četvrtini web poslužitelja u svijetu, jednoj četvrtini SSH poslužitelja i većini VPN aplikacija. Prelazak na kompliciraniji (2048-bitni) algoritam u ovom bi slučaju mogao dovesti do problema s klijentima, pa prije prelaska valja stvar dobro ispitati.

Ukoliko je infrastruktura dovoljno mlada i fleksibilna, najbolje rješenje uz smicanje glava *export-grade* algoritmima je i prelazak na ECDHE [6] varijaciju DH algoritma koja nije osjetljiva na Logjam napad, ali traži nešto veće korištenje računalnih resursa. Ukoliko vam je sigurnost komunikacije važnija od računa za struju, neće biti teško donijeti ispravnu odluku.

pon, 2015-06-08 15:19 - Radoslav Dejanović**Vijesti:** Sigurnost [7]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1555

Links
[1] https://weakdh.org/imperfect-forward-secrecy.pdf
[2] http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/what-is-diffie-hellman.htm
[3] https://www.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/discrete-logarithm-problem
[4] http://en.wikipedia.org/wiki/Rainbow_table
[5] https://weakdh.org/sysadmin.html
[6] http://vincent.bernat.im/en/blog/2011-ssl-perfect-forward-secrecy.html
[7] https://sysportal.carnet.hr/taxonomy/term/13