Tor i anonimnost

Uobičajena je praksa nadzora Interneta pomoću "analize prometa". Kada znate koji se siteovi posjećuju s kojih adresa, otkrivate interese i obrasce ponašanja korisnika. Gost u stranoj zemlji koji posjećuje stranice organizacije za koju radi može tako otkriti razloge radi kojih je došao. Potrošačke navike usmjerit će oglašivače koje robe i usluge da nam ponude. Čak i kad je sadržaj, *payload* paketa kriptiran, u zaglavlju je dovoljno podataka za jednostavnije analize. Ako je sadržaj otvoren, mogu se raditi složene korelacije.

Omiljeni servis zagovornika privatnosti na Internetu je Tor - mreža servera koju uspostavljaju dobrovoljci širom svijeta koji su odlučili podijeliti svoj *bandwidth* sa svima koji žele biti na Mreži anonimno. Servis funkcionira ovako: umjesto uspostavljanja izravne veze između dva računala promet putuje "krivudavo", kriptiranim tunelima, od jednog Tor servera do drugog. Korisnik kome treba privatnost na svoje računalo instalira klijenta, koji onda na mreži uz pomoć imeničkog servisa potraži neko od računala koja služe kao relej i koje postaje ulazno čvorište. Promet se kriptira i dalje putuje po različitim "srednjim" čvorovima dok ne dođe na cilj preko izlaznog čvora. Uspostavljena veza naziva se krug, *circuit*. Ključevi se razmjenjuju sa svakim čvorem iznova, a ni jedan ne zna cijelu putanju paketa od polazišta do odredišta, već samo dva najbliža čvora. Odredišno računalo vidi samo zadnji relej. Na prvi pogled, čini se da je sve savršeno sigurno.

Tor skriva svoje korisnike unutar velike zajednice korisnika, stvarajući anonimizacijsku mrežu unutar javne mreže. Što je ta mreža veća, što više dobrovoljaca svoja računala zaposli kao relej, veća je sigurnost i anonimnost. Korist od toga može biti raznolika i neočekivana: na primjer, neki web dućani cijenu određuju prema zemlji iz koje dolaze kupci. Poznavanje polazne i završne točke Internetskog prometa omogućava raznolike analize i projekcije ponašanja korisnika. Tor sve to zamrači i omogućuje korisniku da se sakrije od neželjenih očiju koje vrebaju.

Servis je razvila američka vojska i koriste ga vojnici da bi sigurno komunicirali preko javne mreže. Intenzivno ga koriste novinari, za komunikaciju s informatorima i redakcijama. U zemljama koje nemaju demokratske tradicije, gdje su građani podvrgnuti nadzoru i progonu ako razmišljaju drugačije od vlade, Tor pruža mogućnost anonimne komunikacije i objavljivanja sadržaja koji podliježu cenzuri, pa tako postaje i alat za izigravanje cenzure. *Electronic Frontier Foundation* (EFF) preporučuje Tor kao sredstvo za održavanje građanskih sloboda na Mreži. Tor koriste i vladini agenti kada posjećuju sumnjive siteove i ne žele da se zna kako dolaze s adresa koje pripadaju vladi.

Moram priznati da sam razgovarajući s oduševljenim pobornicima Tora uvijek bio suzdržan i pomalo skeptičan. Pitao bi ih kako mogu biti sigurni da node na koji su se spojili nije pod kontrolom neke agencije? Ili hakera? Iz medija sam znao za slučajeve kada su vlade uspjele ishoditi sudsku zabranu i ukloniti s Mreže servere koji su obavljali uslugu anonimizacije prometa. Od toga pa do situacije da vladine agencije aktiviraju svoje Tor servere nije dalek put. A onda se postavlja pitanje koliko je takav promet anoniman? Pobornici Tora uvjeravali su me da je promet i dalje kriptiran i nečitljiv, čak i ako netko zna polaznu IP adresu. Zapravo, čini se da je Tor najjači baš u skrivanju sadržaja prometa, ali mu je istovremeno cilj i skrivanje polazišta i odredišta.

Nedavno se počelo intenzivnije pisati o ranjivosti Tora koja ugrožava ananimnost, o takozvanom "timing attacku". Kada netko preuzme kontrolu nad ulaznim i izlaznim čvorištem jednostavnom statistikom mogu se upariti paketi, pa je u značajnom broju slučajeva dovoljno nekoliko minuta da se otkrije identitet pošiljatelja. Tako bar pokazuje istraživanje američkih i izraelskih akademika, koji tvrde da je 58% čvorišta ranjivo na ovaj napad, a u Kini čak 85,7%! Ovome ne treba komentar.

Zanimljivo je da se za ranjivost zna već preko deset godina. Kao odgovor na taj problem razvijen je novi Tor klijent, nazvan ***Astoria***, za kojeg se tvrdi da smanjuje ranjivost čvora sa 58% na 5,8%. Nije moguće posve eliminirati "timing attack", ali zasad je dovoljno podići letvicu i time napad učiniti "skupljim".

Kad bismo živjeli u savršenom društvu, ne bi nam bila potrebna anonimnost na Internetu. Obična građanska pristojnost i etički kodeksi različitih profesija bili bi dovoljni da nam osiguraju zaštitu od zavirivanja u naše privatne stvari. No, niti su ljudi savršeni, niti institucije i organizacije koje stvaraju. To s jedne strane znači da su nam anonimnost i privatnost prijeko potrebne, a s druge strane da će ih za svoje mračne ciljeve koristiti "zločesti" dečki. Kako uspostaviti ravnotežu? Kako ljudima ostaviti slobodu istovremeno im osiguravajući sigurnost? Današnji trend u razvoju legislative i tehnologije vodi k smanjivanju prostora privatnosti uz obećanje iluzije sigurnosti. Tu se otvaraju nove teme za raspravu, pa ćemo ponešto o tome reći u nastavku.

sub, 2015-06-13 12:55 - Aco Dmitrović**Vijesti:** Sigurnost [1]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1556

Links
[1] https://sysportal.carnet.hr/taxonomy/term/13