Možemo li vjerovati SSL certifikatima?

Već znamo da je SSL "razvaljen" i nepouzdan protokol, pa kad kažemo SSL zapravo mislimo TLS. No bez SSL-a/TLS-a korištenje weba je nezamislivo, jer prave zamjene nema. Nedavno se pojavila informacija koja nas tjera da se zamislimo i nad povjerenjem koje imamo u organizacije koje izdaju SLL certifikate, čime je situacija za sigurnosno svjesnog sistemca, kao i za obične korisnike, postala još složenija, a korištenje mreže još nesigurnije.

Krajem ožujka ove godine u Googleu su otkrili nekoliko "neautoriziranih" digitalnih certifikata za domene u svom vlasništvu. Certifikate je izdala tvrtka MCS Holdings, posredni CA kojem je ovlasti dao CNNIC, *China Interent Network Information Center*. To je vijest u sažetom obliku, ogoljena do kostiju, bez komentara. Da je čujete u TV dnevniku, između dvije reklame, jedva da biste se zapitali što to zapravo znači?

Google je zatražio objašnjenje od kineskih kolega i dobio odgovor kako tvrtka MCS Holdings krši ugovor izdajući certifikate domenama kojima nije vlasnik, odnosno domenama koje nije sama registrirala. U dobro uređenom svijetu CCNIC bi povukao ovlasti koje je dao "divljoj" tvrtki. No u stvarnosti je realnost posve drugačija! Kažu da je to bio grafit na berlinskom zidu. Kinezi su se "kao" ispričali, ali nisu ništa poduzeli da isprave "pogrešku". Google je nakon toga pokrenuo mjere kojima nastoji zaštiti sebe i svoje korisnike.

CCNIC je kao nacionalni autoritet za certifikaciju zadan u svim root konfiguracijama, pa mu vjeruju svi operacijski sustavi i svi web preglednici. Googlova reakcija je odmjerena: blokirao je certifikat koji pripada MCS Holdingsu tamo gdje može, u svom pregledniku Chrome. Učinio je to koristeći CRLSet push, sigurnosnu funkciju svog preglednika, čiji je izvorni kod javan. Funkcija by default ne obavlja online provjeru certifikata, već koristi internu crnu listu čiji sadržaj, za razliku od koda funkcije, nije javan. Google je, naime, ispoštovao zahtjev neimenovanih CA tvrtki koje su tražile da crna lista bude funkcionalna, ali ne i javno objavljena. Možemo pustiti mašti na volju razmišljajući o tome čemu ova tajnovitost i netransparentnost. Čak ne treba biti ni previše paranoičan, dovoljno je zamisliti da postoji situacija u kojoj je bolje da "prevaranti" ne znaju da je njihova prijevara otkrivena. Za radoznale, pravila po kojima se kreira i održava lista nevaljanih certifikata dostupna su na adresi https://dev.chromium.org/Home/chromium-security/crisets [1].

No to nije sve što se tiče ovog konkretnog slučaja. Google tvrdi kako je tvrtka MCS Holdings postavila certifikat u ***man-in-the-middle proxy***. Neke tvrtke to rade kako bi mogle nadzirati kriptirani promet svojih zaposlenika. Da bi takva konfiguracija funkcionirala, potrebno je da korisnička računala budu konfigurirana tako da vjeruju tvrtkinom proxy serveru, koji se onda postavlja kao posrednik između korisnika i odredišnog servisa, glumeći korisniku da je ciljni server, a serveru da je korisnik. To je moguće unutar korporativne mreže, gdje admini kontroliraju konfiguraciju svakog računala. Ali kako postaviti ***World Wide Man-in-the-Middle-proxy***? Jednostavno, *proxy* je dobio pune ovlasti koje pripadaju javnom CA, što je ozbiljno narušavanje cijelog CA sustava.

Ovog puta su to napravili Kinezi, ali ako mislite da su oni u tome usamljeni, varate se. Slična stvar je 2013 izvedena s certifikatima koje izdaje ANSSI, francuski CA!

Pa se onda pitamo radi li se ovdje o nemaru, namjernoj ili nenamjernoj podršci kriminalnim organizacijama, ili o suradnji s vladinim obavještajnim agencijama? Kao, u tom slučaju bi izigravanje CA sustava bilo opravdano, zna se, radi prijetnje od globalnog terorizma, oružja masovnog uništenja i tome slično...

Jesmo li time iscrpili listu mogućnosti zloporabe SSL certifikata? Ni izdaleka! Ne treba nabrajati sve dosadne detalje, dovoljno se prisjetiti da je moguće provaliti na server neke od tvrtki koji izdaju certifikate i dočepati se podataka koji bi trebali biti tajni. Nešto tako dogodilo se tvrtki Comodo, jednom od lidera u tom poslu.

S druge strane, dosta se truda ulaže u poboljšanje vjerodostojnosti CA sustava, a veći dio tog posla odvija se na specijalističkoj i tehničkoj razini, izvan pozornosti javnosti.

Na primjer, jedna od zaštita protiv nelegalne proliferacije certifikata je tehnika nazvana "certificate pinning", ugrađena u Chrome 13. Sve konekcije na mail.google.com odnedavno moraju ići preko https protokola, čak i kad korisnik zaboravi upisati https:// na početku adrese. Uz to je ograničen broj tvrki koje mogu jamčiti za Google certifikate. Zabilježeni su slučajevi kada su korisnici pokupili lažne certifikate, dobili poruku da se radi o samo-potpisanom certifikatu i bez razmišljanja prihvatili rizik, naivno vjerujući da tvrtka poput Googlea nema novca za kupovinu legitimnih certifikata! Zapravo takvi korisnici nisu uopće razmišljali niti bilo što zamišljali, naprosto su prihvaćali sve što im se nudi, samo da što prije dođu do usluge koja ih zanima.

Na smanjivanju rizika radi i Radna skupina DANE pri IETF-u. DANE stoji za ***DNS-based Authentication of Named Entities***. Ukratko, radi se o proširenju DNS servisa koji omogućuje da se za svaku domenu definira njezin legitimni CA. Potrajat će dok to postane dio DNSSEC standarda, ali je utješno da se na tome već naveliko radi.

Radoznali i sigurnosno osviješteni sistemci mogu naći dovoljno materijala za proučavanje, treba samo guglati. Na primjer, pročitajte što piše na stranici: http://googleonlinesecurity.blogspot.com/2011/04/improving-ssl-certificate-security.html [2].

Što da u cijeloj to zbrci rade obični korisnici? Oni naprosto koriste mrežne servise, žure što prije obaviti posao, a sigurnosna upozorenja ih samo nerviraju i udaljavaju od onog što očekuju od Mreže. Preopterećene i nedovoljno cijenjene (čitaj plaćene!) sistemce također ova zbrka nervira. Pred njih se dnevno stavlja sve više zahtjeva: održavaju sve više računala, servera, servisa, sve više mrežne opreme, za sve manju plaću. Tko će sad još brinuti o tome da li je neki certifikat valjan ili ne? Jer, čini se, bio valjan ili nevaljan, u oba slučaja su nas možda nasanjkali.

Svijet u kojem živimo sve je složeniji, sve kompliciraniji, sve nepregledniji. Sve je više detalja o kojima mogu brinuti samo usko specijalizirani "fah idioti". Pa što da se radi? Da se odreknemo korištenja Mreže koja je donijela toliko dobra, ili da se izvalimo na leđa, kao pseto koje se predaje jačem od sebe? U psećem svijetu sve je jednostavnije: jači pas odmah odustaje od dokazivanja premoći čim mu se slabiji pokori. U ljudskom svijetu pohlepa i želja za moći nemaju takva ograničenja. Ako želimo preživjeti i pri tom sačuvati dostojanstvo, moramo se obrazovati i držati korak. U protivnom, izvalimo se na leđa i otkrijmo svima slabe točke, pa što bude.

Ah, da, imate na raspolaganju još jednu mogućnost: Google zapošljava pametne mlade ljude koji žele raditi na poboljšanju sigurnosti SSL certifikata.

pon, 2015-04-13 14:37 - Aco Dmitrović**Vijesti:** Sigurnost [3]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1536

Links
[1] https://dev.chromium.org/Home/chromium-security/crisets
[2] http://googleonlinesecurity.blogspot.com/2011/04/improving-ssl-certificate-security.html
[3] https://sysportal.carnet.hr/taxonomy/term/13