Zbogom SSL

 Kad bismo razmišljali o događajima koji su obilježili prošlu godinu sa stanovišta informacijske sigurnosti, morali bismo se osvrnuti na SSL protokol i njegovu najkorišteniju izvedbu OpenSSL. SSL protokol je duže vrijeme bio odgovoran za kriptiranje većine prometa na Internetu, osiguravajući privatnost mnogih poslova koje obavljamo na mreži, od e-maila do Internet bankarstva. Naslijedio ga je TLS, koji je, uz male razlike zapravo isti protokol. O SSL-u se govori kao o nečem prevladanom, koristi se njegov nasljednik TLS. No SSL je često još uključen kao rezerva, u slučaju da se ne uspije uspostaviti veza TLS-om.

Ova su dva protokola u glavama korisnika, pa i informatičara, zamjenjiva; često se govoreći o SSL-u zapravo misli na TLS. Tako OpenSSL donosi oba protokola, a sistemci govore o "SSL-u za Apache", previđajući činjenicu da zapravo koriste TLS.

Već smo pisali o dvama najvećim propustima, nazvanim Hartbleed i Poodle, čije je otkriće odjeknulo prošle godine, i o reviziji koda koja je nakon toga uslijedila. Otkriveno je da je kod bremenit funkcijama koje više nisu potrebne, a kad ih se izbaci kod se više ne da kompilirati.

SSL je bio jedna od najčešćih tema na lanskoj konferenciji FSEC, u Varaždinu, koju smatram najboljom konferencijom o informacijskoj sigurnosti u Hrvatskoj. To nije konferencija kojom dominiraju bogati spoznori, već je mješavina sveučilišnog znanja, nastupa zanesenjaka i malih tvrtki koje se nastoje izboriti za svoje mjesto na tržištu.

No vratimo se SSL-u. Da se tu radi samo o pogreškama u kodiranju, to bi se dalo popraviti. No nađene su slabosti u algoritmu koji koristi protokol, slabosti pomoću kojih ga je moguće izigrati i pratiti kriptiran promet. Više o tome možete pronaći u prezentaciji [1] Miroslava Božićevića s FSEC-a

FSEC je završio zanimljivim izlaganjem Davida Kaloper Meršnjaka, programera koji radi u Velikoj Britaniji, gdje nanovo piše programski kod za implementaciju TLS-a. Radi se o zanimljivom projektu nazvanom Mirage, koji u sklopu XEN-a nastoji optimizirati virtualke. Većina virtualki služi samo pokretanju jedne aplikacije, pa nema potrebe za korištenjem cijelog operacijskog sustava sa svim bibliotekama. Ako smo dobro shvatili, cilj je projekta da se izbaci sve suvišno. Za to se koristi engleska riječ ***cruft***, koja označava sve što je nepotrebno, zaboravljeno i predstavlja smetnju. Doslovno, to mogu biti grude prašine ispod kreveta. OpenSSL ima 40.000 redaka koda, kaže Kaloper, a tu se krije mnoštvo nepotrebnih redaka, koji su nekad davno uneseni da riješe, na pr. sigurnosne probleme, koji su zatim negdje drugdje riješeni, ali se pri tom zaboravilo počistiti privremene, sada već nepotrebne zakrpe. Sa sigurnosnog stanovišta zdravo je nanovo napisati kod i tako očistiti softver od povijesnih naplavina, a to se jednako odnosi na operacijski sustav, biblioteke ali i programske jezike. Kaloper piše TLS iznova u programskom jeziku OCaml, koji je dizajniran tako da spriječi mnoge programerske pogreške, koje čine loši C programeri. Njegovom je TLS-u bilo dovoljno 10.000 radaka koda. Doduše, implementacija još nije posve gotova, nedostaju još neke funkcije, ali je uspješno izdržala napade koji pokušavaju iskoristiti Hartbleed ranjivost. Više o Kaloperovom radu i projektu Mirage naći ćete u njegovoj prezentaciji ***TLS redone***, koju možete preuzeti ovdje [2].

Sve u svemu, potrebna nam je sigurnost na Internetu, potrebna nam je privatnost i kada ne činimo ništa nezakonito i nismo teroristi. Pomisao da nas netko može nadzirati užasava većinu normalnih ljudi, jer to nekim ljudima u crnom daje moć nad nama. U agrarno doba bogatstvo i moć je donosilo vlasništvo nad zemljom, u industrijskoj eri su vlasnici tvornica zamijenili feudalce, a u informacijsko doba moć i bogatstvo daje posjedovanje informacija. Zato svatko treba načelno čuvati svoju privatnost, jer ne želimo nekome samo tako prepustiti moć da te informacije koristi protiv nas, a u svoju korist. Zato će nam još dugo trebati kriptografski protokoli, da zaštite naše osobne i poslovne

informacije. Zapravo, bez kripto protokola Internet bi nekako izgubio na vrijednosti, zar ne? Postao bi obična platforma za masovni nadzor.

Pristalice teorija zavjere podsjetiti će nas kako je američka vlada početkom ere World Wide Weba nastojala ograničiti veličinu SSL ključeva na 48 bitova. Prepirka je trajala neko vrijeme, a onda su iznenada i bez pravog objašnjenja dopušteni 128-bitni ključevi. Paranoici su odmah zaključili kako vlada ima tehnologiju za probijanje 128 bitnih ključeva. Dokument koji je nedavno procurio na Wikileaksu donosi popis kripto protokola koje NSA može probiti, a tu je ponovo dovoljno materijala za zabrinutost. Na listi je naime i SSH protokol, kojeg sistemci koriste svakodnevno za administriranje servera. Trebalo bi nanovo izgenerirati ključeve, a minimalna dužina ključa trebala bi biti barem 4K.

Zanimljiva je pouka koju nam je prenio Kaloper: softver nije savršen, pun je povijesnih, naplavljenih slojeva, bilo bi ga zdravo napisati iznova na nekom modernom programskom jeziku. U primjeru SSL-a radi se o slobodnom softveru, ali to ne oslobađa sumnje vlasnički kod. Tko zna što se sve tamo krije! No da nije sve u softveru podsjetio nas je njemački haker koji se predstavlja pseudonimom Aluz, koji je svojom prezentacijom otvorio konferenciju FSEC. On je demonstrirao probijanje SSL protokola uz pomoć zavidnog matematičkog znanja. Dočepao se zaporki mnogih korisnika, ali nakon što je ranjiv softver zamijenjen novim, zakrpanim inačicama, ponovo je imao pristup istim računalima jer se korisnici nisu zamarali smišljanjem novih zaporki. Očigledno, i sami korisnici moraju usvojiti neke "higijenske" sigurnosne navike, ako im je stalo do privatnosti.

Utrka se nastavlja, letvica se podiže sve više. Nije dovoljno biti puki promatrač i prepuštati aktivistima da se bore za naša prava. Svatko mora odraditi svoj dio, biti informiran i svakako često mijenjati zaporke. I zapamtite: informacije su moć, čuvajte svoju privatnost, ne prepuštajte olako moć nad sobom!

sub, 2015-01-31 07:10 - Aco Dmitrović**Vijesti:** Sigurnost [3]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1505

Links
[1] https://drive.google.com/folderview?id=0B8KFaORM_nPNcUJLRGw4RXptTG8&usp=sharing&tid=0B9U4zJ68G79DdWJqZEpOMlY1TGc
[2] https://drive.google.com/folderview?id=0B9U4zJ68G79DdWJqZEpOMlY1TGc&usp=sharing
[3] https://sysportal.carnet.hr/taxonomy/term/13