Istraživači otkrili slabost TLS protokola

Kenneth Paterson, profesor informacijske sigurnosti i njegov student Nadhem AlFardan, oba s Londonskog Royal Holloway Collegea otkrili su tehnike pomoću kojih se može dešifrirati promet kriptiran protokolima TLS/DTLS. Napad su nazvali **Lucky Thirteen**. Ne radi se o pogrešci u implementaciji, već o slabosti samog protokola.

Rezultate svog istraživanja objavili su 4. veljače na webu fakulteta, ali i kao znanstveni rad. Napad nije jednostavno izvesti, oslanja se na mjerenje vremena pa ga je moguće izvesti samo ako su napadačevo i napadnuto računalo u istoj lokalnoj mreži, kako bi se smanjila greška koju unosi latencija.

Kako Paterson i AlFardan nisu hackeri *black hat* tipa, već etički istraživači, prije objavljivanja rada obavijestili su proizvođače ranjivog softvera, među kojima su Microsoft, Oracle (OpenJDK) i OpenSSL. Uskoro možemo očekivati izlazak novih verzija softvera u kojima su ranjivosti onemogućene.

Ako vas zanimaju detalji, možete pročitati objavu na webu [1] i znanststveni rad [2].

čet, 2013-02-07 07:44 - Aco Dmitrović**Vijesti:** Sigurnost [3]
Vote: 4

Vaša ocjena: Nema Average: 4 (3 votes)

Source URL: https://sysportal.carnet.hr/node/1200

Links
[1] http://www.isg.rhul.ac.uk/tls/
[2] http://www.isg.rhul.ac.uk/tls/TLStiming.pdf
[3] https://sysportal.carnet.hr/taxonomy/term/13