Zaporka od 8 znakova - relikt prošlosti

Odavno postoje sustavi zaštite, poput biometričkih sustava, koji pokušavaju nadomjestiti, poboljšati ili učiniti sigurnijima postojeće načine autentikacije. No, nijedan još nije zamijenio običnu zaporku, koju ukucavate nekoliko puta na dan (a mnogi i nekoliko desetaka puta na dan). No, ono što čini običnu zaporku opasnom je njena duljina.

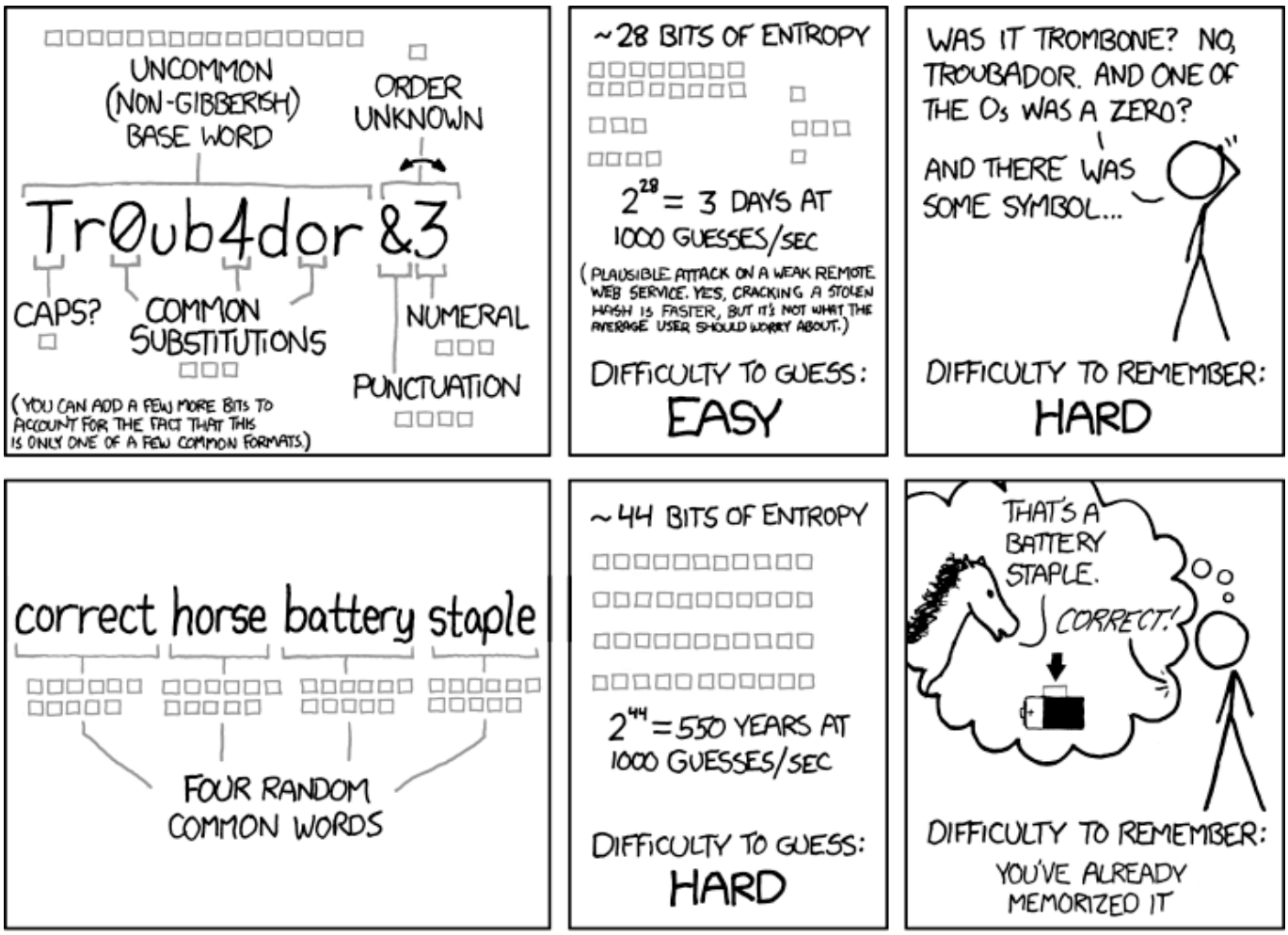
Današnji hardver je, a pri tome poglavito mislimo na procesore na grafičkim karticama, prilagođen upravo matematičkim operacijama koje se rabe u kriptografiji. Vremena procesiranja kriptografskih funkcija su se smanjila za nekoliko redova veličina, ali tu nije kraj poboljšanjima.

U nekim su se popularnim algoritmima pronašle slabosti koje značajno oslabljuju njihovu snagu u realnoj primjeni, a time i njihovu vrijednost u pogledu sigurnosti. Neki algoritmi su se, pak, pokazali kao jednostavno preslabim za današnje uvjete, pa se polako izbacuju iz upotrebe. Čak se i za PGP/GnuPG ključeve sada preporučuje uporaba samo najjačih ključeva, onih od 2048 bitova.

Nadalje, nije sve ni u sirovoj snazi procesora. Postoje već izračunate tablice s riječima iz rječnika, pa se ovaj tip napada (a to je vid klasičnog rječničkog napada - *dictionary attack*) može obaviti vrlo brzo. Umjesto da se izračunava kriptografski *hash* za svaku moguću inačicu zaporke, dovoljno ju je usporediti s onom iz tablice. Tablice su nazvane vrlo zanimljivo - *rainbow tables*.

Ni to nije sve. Svako toliko se može pročitati kako su hackeri provali u bazu podataka korisnika nekog servisa te pokupili njihove zaporke. To je odlična prilika za analizu zaporki koje ljudi najčešće rabe. Kada se kombiniraju tablice *rainbow*, milijuni proanaliziranih korisničkih zaporki i slabosti untar uobičajenih enkripcijskih rutina, nije teško zaključiti da je odzvonilo klasičnim zaporkama tipa "ma dosta ti je 8 znakova".

Nećemo ulaziti u daljnje analize kvalitete kriptogtafskih algoritama ili kvalitete zaštite on-line servisa, ali ćemo se upitati što možemo učiniti da povećamo vlastitu sigurnost? Odgovor je: povećati duljinu zaporke! Pogledajmo strip sa čuvene stranice xkcd.com:



Ovaj kratki strip jako dobro ilustrira ono što želimo reći. Godinama su nas učili, a mi dalje prenosili, da je potpuno siguran onaj password, koji ima 8 znakova, s time da se rabe i interpunkcijski znakovi, zamjenjuju neka slova brojkama i slične manipulacije. Ovo više nije dobar savjet, jer će svaki program za probijanje zaporki uzeti ovakve manipulacije u obzir. Dakle, zamjena slova brojevima i drugim znakovima (u stilu "L337 $P34|< - *leet speak*") više ne prolazi. Dodavanje brojeva na kraju zaporke također više ne prolazi. Ono što još prolazi je jednostavno povećati duljinu zaporke, što će broj kombinacija povećati na vrijednosti koje je teško sustići s današnjim, ali i sutrašnjim hardverom.

Postoje web stranice nakojima možete izračunati "snagu" svoje zaporke, ali teško je reći koliko su ti podaci precizni. Uz to, ukoliko koristite neki drugi kalkulator, dobit ćete drugačije podatke. Svejedno, navest ćemo jedan, pa provjerite svoju zaporku:

https://www.grc.com/haystack.htm [1]

Nećemo vas zamarati s brojnim linkovima, ali ćemo navesti link gdje možete naći podatak da se s klasterom od (samo) 25 Radeon grafičkih procesora svaki NTLM hash (mreža u Windowsu) može razbiti u manje od 6 sati. Taj sustav može napraviti **180 milijardi** MD5 hasheva u **sekundi**. Ili, 63 milijarde SHA1 hasheva u sekundi. Složeniji algoritmima treba više vremena, ali i tu se radi o milijunima izračuna u sekundi. Originalni članak potražite na adresi:

http://www.net-security.org/secworld.php?id=14077 [2]

Da završimo misao... ukoliko koristite zaporku tipa pero1205 (gdje je 12.05. datum vaseg rođenja), ne možete računati na sigurnost zaporke (i bez činjenice da ne treba koristiti nikakve lako dostupne podatke o vama u zaporci). Jasno da ne možete narediti svojim korisnicima da prijeđu na duljine

zaporki od 10 ili 12 znakova, ali napravite tu promjenu za kritične korisničke račune, one s povišenim privilegijama. Način na koji ćete ih složiti nije toliko bitan.

Nemojte koristiti iste zaporke na više mjesta, pogotovo ako se radi o nekim on-line servisima, društvenim mrežama i slično. Ubacite koji interpunkcijski znak i nemojte koristiti manje od 10 (ili bolje, 12) znakova, pa ćete moći "preživjeti" još koju godinu.

čet, 2013-01-31 23:58 - Marko Jukić**Vijesti:** Sigurnost [3]
Kategorije: Informacijska sigurnost [4]
Vote: 5

Vaša ocjena: Nema Average: 5 (2 votes)

Source URL: https://sysportal.carnet.hr/node/1194

Links
[1] https://www.grc.com/haystack.htm
[2] http://www.net-security.org/secworld.php?id=14077
[3] https://sysportal.carnet.hr/taxonomy/term/13
[4] https://sysportal.carnet.hr/taxonomy/term/32