Arvuti salasõna lühike ajalugu

9 aastat tagasi - 14.05.2017 Autor: AM

Salasõna ei ole midagi uut. Tegelikult on need olemas olnud sajandeid. Ammu enne seda, kui Hotmail, Skype ja Netflix soovisid, et looksite turvakoodi huvitava kasutajanime juurde, kasutasid roomlased salasõnasid selleks, et saata olulisi sõjaväeteateid oma vägedele.

Põhimõtteliselt oli tegemist lihtsa võimalusega teavet kaitsta. Paar tuhat aastat hiljem tegeleb selle teemaga Fernando Corbató.

Tegemist on mehega, keda laialt peetakse tänapäevase arvutisalasõna ristiisaks, ta tõi selle mõtte arvutiteadusse, kui töötas Massachusettsi Tehnoloogiainstituudis (MIT) 1960.aastal.

Ülikool oli välja arendanud tohutu süsteemi Computer Time Sharing System (arvuti kasutamise aja jagamise süsteem; CTSS), millele kõigil uurijatel ligipääs oli. Ometi jagati ühist põhiarvutit ja üksikut kettafaili.

Säilitamaks üksikute failide privaatsust, arendati välja salasõna kontseptsioon selleks, et kasutajad saaksid ligipääsu ainult enda spetsiifilistele failidele, mille kasutamiseks oli neil neli tundi nädalas – arvuti kasutamise aeg oli 60ndatel piiratud.

Kuigi salasõnad ei olnud veatuks lahenduseks, nii nagu Corbató ise esimesena ka tunnistaks, sai salasõnast arvutiturvalisuse tagamise peamine lahendus nii isiklikes kui ärisfäärides, sest tegemist oli niivõrd lihtsa lahendusega (kuigi hiljem nähakse seda ühena selle vigadest).

Tärkimine, sool ja krüptoloogia

Sellel varajasel arvutiajastul oli salasõnade kasutamine võrdlemisi piiratud, neid kasutasid peamiselt tüübid nagu Corbató, kes olid esimeste seas, kes hakkasid avastama arvutite võimu.

Kuid, interneti kasutuse plahvatusliku kasvu tingimustes 1990ndatel hakkas aina enam inimesi seda regulaarselt kasutama, luues tohututes kogustes tundlikke andmeid ja teavet.

Kuid isegi enne seda, kui veeb hakkas tormiliselt kasvama, töötasid varajased arvutiteadlased võimaluse kallal, kuidas salasõnasid turvalisemaks muuta. Selle jaoks rakendas arvutiteadus krüptoloogia meetodeid.

Töötades 70ndatel Bell Labsi heaks, mõtles Robert Morris välja „tärkimise“ – protsessi, mille käigus tähemärkide jada transformeeritakse arvkoodiks, mis esialgset fraasi esindab.

Tärkimist rakendati varastes UNIX operatsioonisüsteemidest, mis on tänapäeval laialt üle maailma kasutusel mobiiliseadmetes ja tööjaamades. Apple’i MacOS kasutab näiteks UNIXit, sellal kui Playstation 4 kasutab Orbis Osi, UNIXil põhinevat operatsioonisüsteemi.

Lisamaks veel üks turvalisuse kiht, kasutavad tänapäevased andmebaasid „soolamist“ selleks, et veelgi krüpteerida salasõna, lisades suvalisi andmeid tärgitud salasõnale.

See aga ei takista lihtsa salasõna ära arvamist, peamine eesmärk on takistada lekkinud salasõna/de (näiteks andmebaasilekke korral) lahti murdmist ja kasutamist.

Kuid siis, kui Corbató salasõna välja mõtles, ei olnud turvalisus niivõrd suur mure, häkkimine selle tänapäevasel moel ei tekkinud enne 80ndaid.

Nüüd on aga maailm teistsugune, pea kõik on internetis.

Pangateenuste kasutamisest ja šoppamisest teleri vaatamise ja muusika kuulamiseni hoiame me Teie andmed turvalisena tänu numbrite ja tähtede jadale. Kuid kui turvaline see on? Isegi suured ettevõtted nagu eBay ja LinkedIn on viimastel aastatel sattunud rünnaku alla.

Salasõna eelised ja puudused

Salasõnadega on seotud mõned pealtnäha olemuslikud probleemid. Üks probleem paistab olevat see, et lühemaid on kergem ära arvata, kuid ka kergem meelde jätta. Teine probleem on see, et pikemaid salasõnasid on raskem lahti murda, kuid raskem meelde jätta.

Mitme erineva salasõna meelespidamine võib samuti keeruline olla. Tuleb vaid mõelda sellele, mitu internetikontot keskmisel inimesel on: internetipank, isiklik e-postiaadress, iTunes, Skype, Amazon… see nimekiri jätkub ja jätkub.

See tähendab, et paljudel inimestel on kõigi erinevate platvormide jaoks üks või kaks salasõna. See loob muidugi suure probleemi, kui kellelgi õnnestub salasõna lahti murda, siis saadakse ligipääs kõigele.

Teiseks mureks on salasõna enda valik. On šokeeriv, kuid SplashData andmete kohaselt kasutavad paljud ikka salasõnu nagu „password“ või „123456“ oma tundlike andmete kaitsmiseks – küberkriminaalil ei kulu sellise koodi murdmiseks palju vaeva ega aega.

Salasõna on surnud … elagu salasõna

Salasõnad pakuvad muidugi turvatunnet, kuigi näiteks Bill Gates ütles juba 2004.aastal, et salasõnad on surnud, enamik ettevõtteid kasutab neid aga siiani.

Kuidas siis oma salasõnasid turvalisemaks teha? Olemas on mõned võimalused.

Inimesed, kes korraldavad World Password Day (maailma salasõna päeva), initsiatiivi, mis keskendub salasõna tugevuse parandamisele, on soovitanud, et igal kontol peaks olema unikaalne salasõna.

Oluline on aga ka see, et loodavad salasõnad ise oleksid tugevad. Tugevad on koodid, mis kombineerivad sõnu ja numbreid, vältida tuleks aga ilmselget isikliku teabe kasutamist salasõnas ning salasõna peaks olema kaheksa või enam tähemärki pikk.

Kasutajad saavad rakendada ka „pääsukoodi“ strateegiat või kaheosalist autentimist, tõstmaks oma turvalisust.

“Kolm kuldreeglit selleks, et tagada oma arvuti turvalisus on: ärge omage arvutit, ärge kasutage arvutit, ärge käivitage arvutit.”

Kui kogu see salasõnade jama on liiga palju, siis pidage meeles krüptograaf Robert Morrise veidi ebaharilikku nõu. Lisaks eelmainitule andis ta ka veidi ebaharilikumat nõu:

„Kolm kuldreeglit selleks, et tagada oma arvuti turvalisus on: ärge omage arvutit, ärge kasutage arvutit, ärge käivitage arvutit.“

Ehk veidi liiga ekstreemne…

(Avaldatud algselt Eseti blogis inglise ja eesti keeles)

- Uudised

- Tarkvara
- Turvalisus

Pilt