Autors: **Labi** Raksta ID= **268**

Par un ap MD5

Ik pa laikam forumos un citur, kā datu drošības garants tiek minēts MD5, bet vai tā ir vienīgā MD5 izmantošanas iespēja? Un kas tas tāds īsti ir? Tad nu "*ņēmu rokā*" vikipēdiju un sāku lasīt, izrādījās, ka MD5 ir daudz interesantāka un noderīgāka padarīšana nekā es sākumā domāju.

Lai varētu kaut ko spriest sākumā jāiepazīstas par ko būs runa. MD5 ir plaši lietots datu kodēšanas algoritms, kas neatkarībā no kodējamās informācijas apjoma, datus interpretē kā 32 heksadecimālu simbolu virkni. Piemēram 0 simbolu gara simbolu virkne, kas ir kodēta ar MD5 izskatās šādi - **d41d8cd98f00b204e9800998ecf8427e** MD5 tika ieviests 1991. gadā, lai aizstātu novecojušo MD4 kodēšanas algoritmu. Sākot ar 2004. pētniekiem izdevies vairākas reizes pierādīt, ka MD5 kodēšanai ir dažas nepilnības, tāpēc ASV datoru drošības komanda (US-CERT - United States Computer Emergency Readiness Team) iesaka labāk izmantot citu kodēšanas algoritmu - **SHA-2**. MD5 nedrošs ir tikai priekš ļoti slīpētiem hakeriem, bet priekš parastajiem mirstīgajiem šis kodēšanas algoritms vismaz šobrīd tiek uzskatīts par neatkožamu cieto riekstu. Ja ir vēlēšanās sīkāk palsīt par MD5 algoritmu, tad to var izdarīt vikipēdijā - (WEB) http://en.wikipedia.org/wiki/MD5

Kur var atrast MD5? Unix bāzētās sistēmās MD5 ir iekļauts standartaprīkojumā, taču Windows OS jāizmanto atsevišķas kodēšanas aplikācijas, kuru ir ļoti daudz, tāpēc *Gūglē* nebūs problēmu kādu no tām atrast. Šādas aplikācijas ir pieejamas arī Android ierīcēm, piemēram, **Hash Droid** vai **Easy MD5**. Programmētājiem viss ir daudz vienkāršāk, jo gandrīz visās programmēšanas valodās ir iestrādāts MD5 algoritms, kuru var palaist ar atbilstošu funkciju, piemēram, PHP valodā tas izskatās šādi: <?php echo md5('wapblogs.eu'); ?> rezultāts ir *6a7b12660662d99eb1f12be673976eb7*

Tagad jānoskaidro, kur tad izmanto šo kodēšanas algoritmu? Sākumā es domāju, ka MD5 izmanto tikai lietotāju paroles kodēšanai, jo pat ja hakerim izdodas piekļūt lietotāja datiem, viņam neizdosies atšifrēt ar MD5 kodēto paroli, līdz ar to viņš nevarēs ielogoties ar svešiem datiem un sadarīt visādas blēņas. Laikam daudzi ir pamanījuši ka dažām programmām arhīvā līdzi nāk MD5 checksum simbolu virkne, bet vai kāds zina kam tas ir vajadzīgs? Izrādās, ka tas ir darīts, lai lietotājs varētu pārbaudīt vai kāds ļaunprātīgs hakeris nav ielicis lejuplādētajā programmā kaut kādu vīrusu un nav slepeni sakonfigurējis jūsu programmu pēc saviem ieskatiem. Lai to noskaidrotu, jāuztaisa šīs aplikācijas MD5 checksum ar jebkuru tam paradzēto aplikāciju, un tad iegūtā simbolu virkne jāsalīdzina ar arhīvā iekļauto (vai arī ar to, kas ir publicēta izstrādātāja oficiālajā mājaslapā), ja šie MD5 hash'i nesakrīt, tad kārtīgi jāapdomā vai ir vērts instalēt kāroto programmu savā datorā. MD5 ir arī daudzi citi pielietošanas veidi.

Lai arī nav dzirdēts par MD5 paroļu atšifrēšanas gadījumiem, tomēr izrādās, ka tas nav tik neiespējami, kā dažs labs stāsta. Vikipēdijā (WEB) http://en.wikipedia.org/wiki/Rainbow_table ir sīki aprakstīta tā saucamā *Varavīksnes tabula* (Rainbow table), ar kuras palīdzību it kā varot atšifrēt zināma

garuma *ne*binārus datus. Tomēr Rainbow table nedod nekādas garantijas, ka MD5 hash tiks atšifrēts, tāpēc es joprojām uzskatu MD5 par drošu kodēšanas algoritmu. Ja ir interese, tad vari palasīt sīkāk par v*aravīksnes tabulu* un pamēģināt atšifrēt kaut ko.:D

Uzrakstīts:18:56 05-08-11