DROŠAS PAROLES ĪPAŠĪBAS 2020. GADĀ
SECURE PASSWORD FEATURES IN 2020

Autori: **Sandis RIMŠA**, e-pasts: sandis.rimsa@gmail.com
Aleksandrs ZELTIŅŠ, e-pasts: aleksandrs.zeltins@inbox.lv
Zinātniskā darba vadītājs: doc. Dr.sc.ing. **Sergejs KODORS**, e-pasts: sergejs.kodors@rta.lv
Rēzeknes Tehnoloģiju akadēmija
Atbrīvošanas aleja 115, Rēzekne

Abstract: *Authors completed literature analysis to actualize information about secure password in 2020 year. The paper provides description of password cracking methods to identify secure password features.*

Atslēgas vārdi*: password cracking methods, safe password.*

Ievads

Digitālā laikmetā informācija kļuva par produktu un vērtību, izveidojot sapratni par intelektuālo īpašumu, publisko un privāto informāciju un datiem. Parādījās tādas idejas un intelektuālā īpašuma lietošanas atrunas kā *Open Data*, *CC-BY* licence, *open-source* risinājumi, utt. Sabiedrība vairāk un vairāk pievērš uzmanību informācijas aizsardzības metodēm un principiem. Lai aizsargātu savu īpašumu cilvēks jau no seniem laikiem pielietoja glabātuvi un atslēgu. Līdzīga pieeja tiek pielietota arī informācijas aizsardzībai: glabātuvi veido datnes un datubāzes, bet atslēga pazīstama kā "parole". Ievērojot, ka izauga informācijas sistēmu skaits, kuras pielieto cilvēks ikdienišķajām vajadzībām, izauga un paroļu skaits kāds jāatceras. Tāpēc daudzi, lai vienkāršāk atcerētos izdomā vienkāršas paroles, kas nav droši un to pielieto ļaunprātīgas personas. Papildus paroles netiek pietiekami bieži atjauninātas, jo izvēlēties jaunu paroli cilvēkiem grūti un viņi nevēlas mainīt savus ieradumus. Var secināt, ka cilvēka atmiņa ir "ierobežota", un tāpēc lietotājs nevar atcerēties sarežģītas un drošas paroles; rezultātā tiek izvēlētas paroles, kas ir pārāk īsas vai viegli iegaumējamas. Bet katram lietotājam ir ļoti svarīgi izmantot vai sarežģītas paroles, lai novērstu neatļautu piekļuvi sistēmai vai datiem [1]. Tomēr, kas ir pietiekoši "sarežģīta" un droša parole? Autori nolēma izpildīt literatūras analīzi, lai aktualizētu informāciju un noteikt drošas paroles īpašības.

Pētījuma mērķis: noteikt drošas paroles īpašības 2020. gadā.

Pētījuma metodes: monogrāfiskā jeb aprakstošā metode.

1. Minimālās drošības prasības parolei Latvijā

MK noteikumos Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" var atrast šādus punktus, kas nosaka minimālās drošības prasības [2]:

1. katram sistēmas lietotājam parole ir obligāti jāmaina ne vēlāk kā pēc 90 dienām, taču paroli aizliegts pašrocīgi mainīt biežāk nekā divas reizes 24 stundu laikā;
2. sistēmas lietotāja parole jāizvēlas tā, lai tā nesakristu ne ar vienu no piecām iepriekšējām sistēmas lietotāja parolēm;
3. piecas secīgas reizes nepareizi ievadot sistēmas lietotāja konta paroli, šis konts (izņemot sistēmas administratora kontu) nekavējoties tiek bloķēts;
4. ar sistēmas administratora kontu piekļūt sistēmai, izmantojot iekārtas, kas atrodas ārpus iestādes telpām, kā arī iekārtas, kas neatrodas iestādes valdījumā, iespējams, tikai izmantojot daudzfaktoru autentifikāciju.

https://doi.org/10.17770/het2020.24.6756

2. Paroles sarežģītības noteikšanas algoritmi

Izpētot kādi algoritmi eksistē, lai automātiski novērtētu paroles sarežģītību, autori atrada gan sarežģītus algoritmus, kas ievēro uzbrukumu metodes un balstās uz varbūtības uzminēt paroli [3], gan vienkāršus ar iebūvētu loģiku [4] (skat. 2.1. attēlu).

```
...
var score = 0;
var r_class = 'weak-password';
...

//password length
score += password.length * 4;
score += ( $.updatePasswordMeter._checkRepetition(1,password).length - password.length ) * 1;
score += ( $.updatePasswordMeter._checkRepetition(2,password).length - password.length ) * 1;
score += ( $.updatePasswordMeter._checkRepetition(3,password).length - password.length ) * 1;
score += ( $.updatePasswordMeter._checkRepetition(4,password).length - password.length ) * 1;

//password has 3 numbers
if (password.match(/(.*[0-9].*[0-9].*[0-9])/))  score += 5;

//password has 2 symbols
if (password.match(/(.*[!,@,#,$,%,^,&,*,?,_,~].*[!,@,#,$,%,^,&,*,?,_,~])/)) score += 5;

//password has Upper and Lower chars
if (password.match(/([a-z].*[A-Z])|([A-Z].*[a-z])/))  score += 10;

//password has number and chars
if (password.match(/([a-zA-Z])/) && password.match(/([0-9])/))  score += 15;

//password has number and symbol
if (password.match(/([!,@,#,$,%,^,&,*,?,_,~])/) && password.match(/([0-9])/))  score += 15;

//password has char and symbol
if (password.match(/([!,@,#,$,%,^,&,*,?,_,~])/) && password.match(/([a-zA-Z])/))  score += 15;

//password is just a nubers or chars
if (password.match(/^\w+$/) || password.match(/^\d+$/) )  score -= 10;

//verifing 0 < score < 100
score = score * 2;
if ( score < 0 )  score = 0;
if ( score > 100 )  score = 100;

if (score > 25 ) r_class = 'okay-password';
if (score > 50  ) r_class = 'good-password';
if (score > 75 ) r_class = 'strong-password';
...
```

2.1. attēls. Vienkārša algoritma piemērs paroles sarežģītības noteikšanai [4]

3. Visizplatītākās paroļu uzlaušanas metodes

Profesionāli veidotās vietnēs neglabā paroles "tīrā formā". Datubāzē tiek glabāts tikai to jaucējkods. Eksistē dažādi jaucējkoda algoritmi (skat. 3.1. attēlu). Ieejot vietnē, parole tiek pārrēķinātā jaucējkodā, ja tas atbilst tam, kas tiek glabāts datubāzē, tad sistēma atļauj ienākt. [5]

Lai iegūtu paroles *p* jaucējkodu *h* tiek pielietota šifrēšanas funkcija $h = f(p)$. Tāpēc paroles uzlaušanas uzdevums ir, pielietojot metodi *c*, atrast paroli no jaucējkoda $c(h) = p$. Hakerim jāizdomā, kāda metode *c* izmantot, lai ar lielāko iespēju varētu atrast paroli *p*. Bieži izmantotās paroļu uzlaušanas metodes ir pārlases uzbrukums, vārdnīcas uzbrukums un dažādas variācijas no iepriekš minētajām metodēm, ņemot vērā laika un vietas kompromisu apsvērumus. [6]

Adler32	0f910374
CRC32	35c246d5
Haval	2221b19499669a2da53c49caf3c5e5be
MD2	f03881a88c6e39135f0ecc60efd609b9
MD4	8a9d093f14f8701df17732b2bb182c74
MD5	5f4dcc3b5aa765d61d8327deb882cf99
RipeMD128	c9c6d316d6dc4d952a789fd4b8858ed7
RipeMD160	2c08e8f5884750a7b99f6f2f342fc638db25ff31
SHA-1	5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8
SHA-256	5e884898da28047151d0e56f8dc6292773603d0d6aabbdd6
SHA-384	a8b64babd0aca91a59bdbb7761b421d4f2bb38280d3a75b
SHA-512	b109f3bbbc244eb82441917ed06d618b9008dd09b3befd1b
Tiger	d476a6b8b5c35ce912781497d02d09faeb8aa05a489223f5
Whirlpool	5b59c49b6dc8bcb2a554a64c42e859c6d43c5fbfe9adc41d6

3.1. attēls. Jaucējkodu piemēri

1. uzbrukumu variants: izmantojot vārdnīcas

Izmanto vienkāršu failu, kurā glabājas vārdi, kurus var atrast vārdnīcā. Šāda veida uzbrukumi izmēģina visus vārdus, kurus daudzi cilvēki izmanto kā paroli. Vienkārši sagrupējot vārdus, kā "simsimatveries" vai "essuperadministrator", neglābs paroli no uzlaušanas – tas tikai nebūtiski aizkavēs procesu. [7]

2. uzbrukuma variants: pārlases uzbrukums

Šī metode ir līdzīga vārdnīcas uzbrukumam, bet ar papildīpašību - hakeris, kurš var atklāt vārdus, kuru nav vārdnīcā, sakārtojot visas iespējamās burtciparu kombinācijas . Tā ir lēna metode, it īpaši, ja parole sastāv no vairākiem simboliem, bet parole tiks uzlauzta. Tādu metodi var vienkāršot, izmantojot papildu datora skaitļošanas jaudu, tostarp izmantojot videokartes iespējas, un, piemēram, izmantojot izplatītus skaitļošanas modeļus un zombiju robottīklus. [8]

3. uzbrukuma variants: makšķerēšana

Visizplatītākais veids, kā "zog" populāro e-pasta pakalpojumu un sociālo tīklu paroles, ir makšķerēšana. Metodes būtība ir tāda, ka lietotājs nokļūst šķietami pazīstamā vietnē (piemēram, tajā pašā *gmail, draugiem.lv, odnoklassniki, utt.*), un viņam pieprasa ievadīt savu lietotājvārdu un paroli, lai apstiprinātu kādu procesu; pēc ievadīšanas parole kļūst zināma hakerim.

Kā tas notiek: parasti lietotājs saņem vēstuli, kurā tiek informēts par nepieciešamību pieteikties savā kontā un tiek dota adrese uz vietni, kura vizuāli ir ļoti līdzīga oriģinālajai. Cita metode, kad pēc nejaušas nevēlamas programmatūras instalēšanas datorā, sistēmas iestatījumi tiek mainīti tā, ka pārlūkprogrammas adreses joslā ievadot vajadzīgās vietnes adresi, lietotājs faktiski nokļūst makšķerēšanas vietnē. [9]

4. uzbrukuma variants: spiegprogrammatūra

Spiegprogrammatūra (*spyware*) - plašs ļaunprātīgas programmatūras klāsts, kas slepeni tiek instalēts lietotāja datorā, lai sekotu ievadāmajai informācijai. Spiegprogrammatūras funkcijas var tikt iekļautas citā programmatūrā, šādi paslēpjot to īsto nolūku. Spiegprogrammatūra var sekot taustiņu uzspiešanai vai veikt slēpto trafika analīzi, lai iegūtu lietotāja paroli. [10]

Diskusija un rezultāti

Nedrīkst lietot paroles sastādītas tikai no cipariem vai pielietot vārdus, kurus var atrast vārdnīcā. Vārdu kombinācijas tikai nebūtiski aizkavēs uzbrukuma metodes. Visizplatītākais cipars parolēs ir 1. Vispopulārākā parole ir 12345. Burtu aizvietošana ar līdzīgiem pēc izskata cipariem (piem., "*passw0rd"*) arī nepalīdzēs aizsargāt paroli.

Sastādot paroli, neizmantojiet klasiskās kombinācijas un šablonus: nekādu personisko datu, informācijas, vārdu, dzimšanas datumu vai citu simbolisku faktu, vienkāršu vārdi savienojumu, vārdnīcas vārdu, standarta frāzes.

Nekad nelietot vienu paroli visām sistēmām un vietnēm. Ja tiks uzlauzta kāda sistēma, tad hakeris varēs piekļūt visām pārējām.

Nekad neglabājiet paroli tīklā, pārlūkprogrammās un citās automātiskās saglabāšanas sistēmās. Atcerieties, ka neviens serviss jums neprasīs nosaukt savu paroli. Pat ja vietnēs esat aizmirsis paroli, vienmēr ir iespēja atgūt paroli ar identitātes apstiprinājumu, izmantojot SMS, e-pastu vai citu veidu.

Visbiežāk paroles sastāv no 6 simboliem. Drošībai labāk ir izmantot paroles, kuru garums ir vismaz 8 simboli. Izmantojiet garas paroles un atsakieties no īsām.

Secinājumi

Sakarā ar to, ka mūsdienās ļoti daudz informācijas un datu glabājas internetā, tad paroļu drošība ir ļoti aktuāla tēma. Darba gaitā tikai izpētītas populārākās paroļu uzlaušanas metodes, kā arī apskatīti ieteikumi kā izveidot drošu paroli. Tika izsecināts, ka, ja priekš paroles izveidošanas izmanto savus datus (dzimšanas diena, vārds, uzvārds, telefona numurus), tad tādas paroles tiek uzlauztas pāris sekunžu laikā. Tātad ir jāatsakās no visiem vārdiem, kas ir saistīti ar personu, jāmēģina izdomāt pēc iespējas grūtākas frāzes. Neizmantojiet vienu paroli priekš vairākiem interneta vietnēm, pat ja tiek mainīti daži simboli, jo, ja viena parole tiek uzlauzta, tad līdzīgas paroles uzlauzt nesagādās grūtības. Tika konstatēts, ka lielākā daļa no interneta lietotājiem sāk mēģināt domāt par drošu paroli tikai tad, kad parole jau tika uzlauzta.

Summary

Due to the fact that a lot of information and data are stored on the Internet nowadays, password security is a very important issue. The most popular password cracking methods have been discussed as well as recommendations how to create a secure password. It was concluded that if user apply his data (like birthday, name, surname, telephone numbers) to create a password, then such passwords are cracked within a few seconds. So, user must refuse to use all the words that are related with his personal data, the difficult phrases must be used. Do not use one password for several websites, even if few characters are changed, because if one password is cracked, it will not be difficult to crack similar passwords.

Izmantotās literatūras un avotu saraksts

1. Study On Information Security And Passwords [Tiešsaiste] Pieejams: https://www.ukessays.com/essays/information-technology/study-on-information-security-and-passwords-information-technology-essay.php [Piekļuve 15.04.2020]

2. Prasības paaugstinātas drošības sistēmām [Tiešsaiste]
   Pieejams: https://likumi.lv/ta/id/275671-kartiba-kada-tiek-nodrosinata-informacijas-un-komunikacijas-tehnologiju-sistemu-atbilstiba-minimalajam-drosibas-prasibam [Piekļuve 15.04.2020]
3. Galbally, Javier & Coisel, Iwen & Sanchez, Ignacio. (2016). A New Multimodal Approach for Password Strength Estimation. Part I: Theory and Algorithms. IEEE Transactions on Information Forensics and Security. PP. 1-1. 10.1109/TIFS.2016.2636092.
4. How do I measure the strength of a password? [Tiešsaiste]
   Pieejams: https://stackoverflow.com/questions/1614811/how-do-i-measure-the-strength-of-a-password [Piekļuve 15.04.2020]
5. "Взлом «посоленных» хешей" [Tiešsaiste]
   Pieejams: https://www.securitylab.ru/analytics/406636.php?R=1 [Piekļuve 15.04.2020]
6. On Password Strength: A Survey and Analysis [Tiešsaiste]
   Pieejams: https://www.researchgate.net/publication/318154948_On_Password_Strength_A_Survey_and_Analysis [Piekļuve 15.04.2020]
7. ЛУЧШИЕ ПРОГРАММЫ ДЛЯ ВЗЛОМА ПАРОЛЕЙ [Tiešsaiste]
   Pieejams: https://losst.ru/luchshie-programmy-dlya-vzloma-parolej [Piekļuve 15.04.2020]
8. "Как хакеры взламывают пароли? Максимально просто!" [Tiešsaiste]
   Pieejams: https://zen.yandex.ru/media/ger/kak-hakery-vzlamyvaiut-paroli-maksimalno-prosto-5d666e6e0ef8e700adde3d10 [Piekļuve 15.04.2020]
9. "Методы взлома" [Tiešsaiste]
   Pieejams: https://hetmanrecovery.com/ru/recovery_news/methods-of-hacking-a-gmail-account-and-ways-to-protect-against-them.htm [Piekļuve 15.04.2020]
10. Spyware [Tiešsaiste]
    Pieejams: https://dic.academic.ru/dic.nsf/ruwiki/69097 [Piekļuve 15.04.2020]