LIETOTĀJU AUTENTIFIKĀCIJAS DROŠĪBA
USER AUTHENTICATION SECURITY

Autors: **Andris Lastovskis,** e-pasts: lastovskis.andris@inbox.lv
Zinātniskā darba vadītājs: **Pēteris Grabusts, Dr.sc.ing., prof.,** e-pasts:peteris.grabusts@rta.lv
Rēzeknes Tehnoloģiju akadēmija, Inženieru fakultāte, Atbrīvošanas aleja 115, Rēzekne

Abstract. *Nowadays, the rapid development of technology and increased amount of data that must be processed and stored. All stakeholders are interested in security level of their system. To improve security, specific process was created, which will help identify the user, and only then give him access.*

As a result, developed process – authentication, it's purpose of this is to improve user identification process, and to let him go further. In the end, as a result, this process either allows the user to work with the system, or rejects it because incorrect data was received by system.

Often, the authentication process is based on some secret element that both the system and the user himself knows about. As an example it can be system's provided login and password, some readable element, or even fingerprints.

Keywords: *Authentication, identification, identity, security, user.*

Ievads

Mūsdienās strauji attīstoties tehnoloģijām un pieaugot apstrādājamo datu apjomiem. Bieži vien visas ieinteresētās puses nopietni izvērtē izmantojamās sistēmas un to saistītus drošības pasākumus. Tāpēc arī tika izstrādāts speciāls process, lai varētu identificēt lietotāju un tikai pēc tam ļaut tam strādāt ar sistēmas datiem.

Risinājums ir izstrādāts process – autentifikācija, kas ir virzīts uz lietotāju identitātes pārbaudi kādā no sistēmām. Rezultātā tiek noteikts, vai lietotājs atbilst tā uzrādītajiem identifikatoriem.

Autentifikācijas process parasti balstās uz kāda slepena elementa pamata, ar kuru ir iepazīts gan lietotājs, gan pati sistēma. Par piemēru sekojošiem elementiem var kalpot: lietotājam izsniegtā parole vai identifikācijas numurs, nolasāms elements, vai pat pašas personas pirkstu nospiedumi.

Pētījuma objekti un metodes

Autentifikācijas faktori

No vēstures zināms ka pat pirms datorsistēmu plašas izmantošanas, jau tika izmantotas visvisādas metodes, lai spētu noteikt kādas personas atšķirīgas īpašības, un balstoties uz dotās informācijas tiks veiktas turpmākās darbības. Tagad galvenokārt izdala 3 autentifikācijas faktorus:

- Kaut kas, ko mēs zinām – parole. Ir slepena informācija ko jāzina tikai autorizētai personai. Paroļu sistēmu ieviešana ir lēta, un vienkārša, bet tā ir izplatītākā ko cenšas uzlauzt ļaundari.
- Kaut kas, kas mums pieder – iekārta. Piemērs: bankas karte, *smart*-karte, ļaundarim tādu iekārtu iegūt ir grūtāk nekā ievadāmo paroli, jo subjekts uzreiz var ziņot par zagšanu vai kāda cita veida problēmām. Metode ir drošāka, bet izmaksas tās ieviešanai ir lielākas salīdzinājumā ar paroļu mehānismu.
- Kaut kas, kas ir subjekta elements – biometrika. Perspektīva sistēma, ar lielisku precizitāti, bet tomēr ar trūkumiem, un lielu ieviešanas cenu. [1]

Autentifikācijas līdzekļi

Izvērtējot esošās sistēmas drošības līmeni, var izmantot dažāda tipa autentifikācijas pieejas, sākot ar parastām atslēgas frāzēm vai parolēm līdz vairāku etapu risinājumiem. [2]

http://dx.doi.org/10.17770/het2017.21.3555

Autentifikācija izmantojot elektronisko parakstu

Elektroniskais paraksts jeb e-paraksts ir elektroniski dati, kas viennozīmīgi apliecina elektroniskā dokumenta (parakstāmā dokumenta) autentiskumu, apstiprina parakstītāja identitāti. Bieži vien atrodas papildus failos, kas tiek saņemt kopā ar parakstāmo dokumentu.

Autentifikācija pēc parolēm

Par paroli saprot kādu slepenu vārdu, vārdu salikumu vai simbolu virkni, kura glabā pieeju kādai nozīmīgai informācijai, piemēram, bankas kontam, e-pastam, telefona SIM kartei un/vai telefonam, seifam, kāpņu telpas durvīm, operētājsistēmu piekļuvei, utt. Pie tam paroles var iedalīt sekojoši:

- Atkārtoti lietojamās paroles
- Vienreizējas paroles

1.attēls **Identifikatora un paroles ievada forma**

Atkārtoti lietojamās paroles – viens no autentifikācijas veidiem sistēmā, kur lietotājs papildus savam identifikatoram (*login*) ievada arī paroli (*password*) - slepenu simbolu rindu. Pie tam pareiza doto datu kombinācija jau ir zināma sistēmai, un tiek glabāta datubāzē. [3]

Vienkāršu autentifikācijas procesu izmantojot paroles var aprakstīt sekojoši:

1. Tiek veikts sistēmas pieejas pieprasījums, un ievadīts identifikators ar paroli;
2. Ievaddati tiek nosūtīti serverim, kur notiek salīdzināšana ar pareizo kombināciju;
3. Ja pārbaude ir veiksmīga, autentifikācijas procesu uzskata par veiksmīgu, pretējā gadījumā – subjektam tiek piedāvāts atkārtoti veikt datu ievadi.

Parole var būt nodota serverim divos veidos:

- Nešifrētā, atklātā veidā (*Password Authentication Protocol, PAP*)
- Izmantojot šifrēšanas protokolus (*SSL, TLS*), tādā gadījumā ievaddati tiek transformēti un droši nosūtīti līdz autentifikācijas serverim.

Savukārt runājot par drošību, drošākais variants ir tad, ja lietotāja parole tiek glabāta servera pusē jau pārveidota veidā. Bieži vien tādām situācijām izmanto kriptogrāfijas jaucējfunkcijas (*hash*), tātad lietotājs ievada savu paroli, serveris to saņem, pārveido, un tikai tad salīdzina to. Rezultātā ja uzbrucējs pat piekļūs datubāzes datiem, no pārveidotas paroles izmantojot jaucējfunkciju ir gandrīz neiespējami iegūt lietotāja ievadāmo paroles kombināciju.

Atkārtoti lietojamās paroļu lietošanā arī ir savi trūkumi. Pirmkārt bieži vien paroles datubāzēs glabājas atklātā veidā, vai ar minimālam transformācijām. Piekļūstot uzbrucējam šādai informācijai, pārējos konfidenciālos datus iegūt nesagādās problēmas. Otrkārt subjektam, vienmēr ir jāatceras vai jāpieraksta sava parole. Ļaundaris doto informāciju var iegūt pielietojot sociālo inženieriju - cilvēka psiholoģiska manipulēšana, lai panāktu noteiktu darbību veikšanu vai konfidenciālas informācijas izpaušanu. Papildus problēmas arī var rasties sistēmās tad ja lietotajam ir dota izvēle ievadīt pašam savu paroli. Tādos gadījumos bieži vien par paroli kļūst kāds vārds vai vienkārša ciparu, burtu kombinācija. Tas ļauj ļaundarim pielietojot *brute-force* kriptogrāfijas pieeju, mēģināt atlasīt paroli, vienkārši ievadot dažnedažādas kombinācijas.

Izmantojot automatizētus rīkus un jaudīgas datorsistēmas iespējams salīdzinoši ātri identificēt pareizo simbolu rindu. Piemēram, ja parole sastāv no 46 simboliem (burti un cipari), un tās garums ir 6 simboli, tā saturēs 2176782336 iespējamos variantus un īstās kombinācijas noteikšanai ar 25 gadu veco procesoru (*Pentium 100*) būs nepieciešamas tikai 6 stundas. Zinot cik strauji procesori attīstās, mūsdienās noteikti var teikt ka paroles atlase notiks vel ātrāk. [1]

Risinājumi tādām problēmām ir sekojoši:

- Automātiski ģenerēto paroļu izmantošana
- Paroļu derīguma termiņu ierobežošana (vēlāk paroli būs obligāti jāmaina)

Vienreizējas paroles (*OTP — One Time Password*) – ir atkārtoto paroļu risinājums, kas neļauj uzbrucējam iegūstot paroli, pastāvīgi to izmantot darbā ar sistēmu vai tās datiem. Galvenā atšķirība ir tajā ka katra parole ir derīga tikai vienai lietotāja autentifikācijai. Vienreizējo paroļu mehānisms var būt realizēts gan aparatūras, gan programatūras līmenī. [4]

Izmantojamās tehnoloģijas tādam risinājuma var iedalīt sekojoši:

- Vienotu pseidogadījuma skaitļu ģenerācija, gan subjektam, gan sistēmai
- Laikspiedolu izmantošana – ir zināmi laika periodi kad ģenerētie skaitļi tiks atjaunoti.
- Vienotas gadījuma paroļu bāzes izmantošana

Pirmajā metodē, tiek ģenerētas simbolu rindas lietotājam un sistēmai, pie tam katrā nākošā pieprasījuma tiek veikta atkārtota ģenerēšana.

Otrajā metode – sistēmā un lietotāja iekārtā glabājas slepena atslēga, ieiešanai sistēmā lietotājam tiek pieprasīts PIN kods, un ģenerētais skaitlis dotajā momentā, tad sistēma apvieno PIN kodu un slepeno atslēgu, pēc kā ģenerē gadījuma skaitli balstoties uz slepenās atslēgas parametriem un dotā momenta laiku. Rezultātā tiek pārbaudīts dota momenta ģenerētais skaitlis ko ievadīja lietotājs, un ko noģenerēja sistēma.

Trešais piemērs balstās uz sinhronizācijas un vienotas datubāzes ar parolēm, kuras tiek izmantotas sistēmas piekļuvei, kur katra parole ir vienreizēja. Pateicoties tam ja uzbrucējs iegūst lietotāja izmantoto paroli, tā jau nebūs derīga turpmākām darbībām.

2.attēls. **Vienreizējo paroļu ģenerēšanas iekārtas piemērs.**

Autentifikācija izmantojot SMS

Mūsdienās ātri attīstoties mobilajiem tālruņiem un to apjomiem cilvēku vidū, tika izstrādāta jauna metode, kas ļauj izmantot savu telefonu kā papildus iekārtu veiksmīgai autentifikācijai.

Procedūra ir sekojoša:

1. Lietotājvārda un paroles ievads
2. Lietotājs saņem vienreizēju autentifikācijas atslēgu SMS ziņojumā
3. Saņemtā atslēga tiek ievadīta sistēmā

Dotās metodes priekšrocība ir tāda ka atslēga tiek saņemta izmantojot citus sakaru kanālus, nevis to caur kuru notiek autentifikācijas process. Tas praktiski novērš draudus kurus dēvē par "cilvēks vidū" – kas nozīmē to ka veidot kādu darbību, pastāv informācijas nodošanas starpposmi, kuros ir iespējama datu noplūde. Tāda metode bieži vien tiek izmantota banku sistēmās.

Biometriska autentifikācija

Biometriska autentifikācija, balstās uz cilvēka biometrisko parametru mērīšanu, un nodrošina gandrīz simtprocentīgu identifikāciju, papildus risinot problēmas, kas var rasties pazaudējot paroles vai kādus citus identifikatorus.

Izplatītākie biometriskie risinājumi:

- Pirkstu nospiedumu atpazīšana
- Rokas ģeometrijas pārbaude, der gadījumos, kad ir pirkstu traumas kad nav iespējams izveidot korektu pirkstu nospiedumu.
- Varavīksnenes skenēšanas iekārtas, uz doto momentu viens no precīzākajiem risinājumiem
- Termisks sejas tēls, uz doto momentu ļoti atkarīgs no apkārtējā apgaismojuma, kas būtiski ietekmē precizitāti.
- Sejas formas identifikācija, ir salīdzinoši precīza sistēma, bet bieži vien pat izmantojot personas fotogrāfiju iespējams iegūt pozitīvu autentifikācijas rezultātu.
- Balss atpazīšana – nodrošina attālinātu piekļuvi, bet ierobežo lietotāju ar sakaru kvalitāti, un nav derīga ja persona ir saslimusi utt.
- Klaviatūras ievada risinājums, analizē cik ātri tiek veikts datu ievads.
- Rokraksta parasta pārbaude izmantojot digitalaizeru.

Neskatoties uz doto risinājumu plašu pielietošanu, tam ir savi trūkumi:

- Pārbaudes šabloni noveco, nepieciešama pastāvīga atjaunošana
- Šablonu bāzes datus uzbrucēji var izmainīt
- Personas datus iespējams viltot (fotogrāfija, maska, …)
- Ja personas dati bija nozagti (kompromitēti), tos nav iespējams mainīt īsos terminos
- Biometriskā informācija ir unikāla, bet ir grūti atstāt pilnīgā slepenībā

Autentifikācija, izmantojot ģeogrāfisko atrašanās vietu

Dotajā grupā iespējams izdalīt sekojošus punktus:

- Autentifikācija izmantojot globālās pozicionēšanas iekārtu (*GPS - Global Positioning System*) – process tiek uzskatīts par veiksmīgu, ja subjekts autentificējas no konkrēta zemeslodes reģiona. *GPS* aparatūra ir vienkārša un droša, un salīdzinoši lēta. Tas ļauj izmantot tādu risinājumu kad ir nepieciešams nodrošināt attālinātu piekļuvi no vajadzīgas vietas.
- Autentifikācija, kas balstās uz vietas no kuras notiek piekļuve internetam. Galvenokārt balstās uz serveru atrašanas vietas, vai bezvadu tīkla piekļuves punkta (*AP – access point*), no kurienes arī notiek pieslēgums internetam. Bet tāda metode nav tā drošākā, jo mūsdienās ir salīdzinoši viegli mainīt savu atrašanas vietu izmantojot tā saucamos proksi (*proxy*) serverus, vai sistēmas ar anonīmu piekļuvi (*Tor - anonymity network*).

Daudzfaktoru autentifikācija

Pēdējā laikā kļūst populāra pieeja kad veiksmīgai lietotāja autentifikācijai ir nepieciešami vairāku nosacījumu izpilde. Bieži vien tiek vienkārši kombinēti iepriekš aprakstīti risinājumi. Izvēloties priekš sistēmas vienu vai otru faktoru, pirmkārt ir nepieciešams noskaidrot kādu aizsardzības līmeni ir jāsasniedz, kādi ir pieejami resursi, un kā notiks subjektu mijiedarbība ar to. [4]

Zemāk tabulā ir attēlota salīdzināšanas tabula:

1.tabula

Autentifikācijas risinājumi dažāda drošības līmeņa sistēmām

Riska līmenis	Prasības pret sistēmu	Autentifikācijas tehnoloģija	Pielietojuma piemēri
Zems	Nepieciešams nodrošināt autentifikāciju sistēmas pieklušanai, pie tam datu noplūdei, nebūs būtiskas ietekmes.	Minimālās prasības - atkārtoti lietojamās paroles	Reģistrācija interneta portālā
Vidējs	Nepieciešams nodrošināt autentifikāciju sistēmas pieklušanai, pie tam sistēmas uzlaušana un konfidenciālo datu izpaušana radīs nelielus zaudējumus.	Rekomendējams izmantot vienreizējās paroles	Persona veic naudas operācijas bankas mājaslapā
Augsts	Jānodrošina autentifikācija sistēmas izmantošanai. Papildus tam datu nopludināšana radīs nopietnus zaudējumus.	Kā minimums ir jānodrošina daudzfaktoru autentifikāciju.	Lielu starpbanku operācijas vai transakcijas izmantojot vadošo ierīci

Visas iepriekš aprakstītās metodes ir pielietojamas sekojošiem servisiem:

1) Ē-pasts, sociālie tīkli, maksājuma sistēmas, maksājumi internetā, interneta veikali, forumi, u.c. [5]

Izplatītākie autentifikācijas jeb personas identitātes apliecināšanas veidi Latvijā ir:

- Iestāžu uzturētās autentifikācijas sistēmas
- Internetbanku autentifikācija lietotājvārds, parole, kodu no kodu kartes
- Mobilais ID - jāievada mobilā tālruņa numurs, drošības kods, speciāls PIN kods
- e-Me viedkartes e-paraksts - Izmanto e-paraksta viedkartē iekļauto autentifikācijas sertifikātu.
- eID kartes - kurās ir iekļauts e-paraksts. [6]

Rezultāti un to izvērtējums

Apskatot izplatītākos risinājumus noskaidrojām ka uz doto momentu ir pietiekoši daudz variantu, kas spēj nodrošināt autentifikācijas pārbaudi. Papildus tam kad ir zināmas katras sistēmas "šaurās" vietas, var mēģināt apvienot dažādu tipu metodes. Tas rezultātā palielinās kopējo drošību, un mazinās iespējamās nepilnības kurus uzbrucēji var izmantot, lai piekļūtu lietotāju datiem.

Secinājumi

Attīstoties datoru tehnoloģijām un programmatūrai, rodas gadījumi, kad ir vērts izveidot datu aizsardzības sistēmu, kas būs gan ērta, gan pietiekoši droša. Viens no svarīgākajiem posmiem drošai lietotāju identifikācijai ir autentifikācija.

Mūsdienās, noteikti katrai datu apstrādes sistēmai, būs iespējams piemeklēt optimālu variantu, kas nodrošinās papildus drošības etapus ieviešot autentifikāciju. Un tomēr, katrām no apskatītajām sistēmām ir savas nepilnības, kas rada potenciālo risku ka sistēmā tiks ļaundari. Galvenais ir arī tas ka, pirms izdarīt izvēli vienmēr ir jāizvērtē nepieciešamais drošības līmenis, un vai to būs iespējams sasniegt ar konkrētiem risinājumiem.

Papildus tam nav jāaizmirst par to ka, vairākums problēmu rodas vienkāršas cilvēku neuzmanības dēļ, piemēram nozaudējot kodu karti, vai glabājot paroli vienuviet ar lietotājvārdu. Ja cita persona doto informāciju ir redzējusi un piefiksējusi, tas neradīs grūtības izmantojot tos piekļūt sistēmai, pie nosacījuma ja tie tiek izmantoti parastā autentifikācijas sistēmā ar atkārtoti lietojamām parolēs bez citiem papildus pārbaudes elementiem.

Viens no izplatītākajiem un drošākajiem risinājumiem mūsdienās, ir izmantot sarežģītu kombināciju garas paroles, kuras tiek atjaunotas pēc kāda laika, kopā ar vienreizējo atslēgu ģenerēšanu, ko lietotājs saņem SMS veidā. Iepriekš aprakstītu uzdevumu spēj nodrošināt divpakāpju autentifikācija.

Summary

With the development of computer technologies and software, there are situations when it is necessary to create a data protection system that is both convenient and sufficiently safe. One of the most important steps for the safe identification of users is authentication.

Currently, for each system that works with data, it is possible to choose the best option that will provide additional security measures by implementing authentication. And yet, each of the solutions discussed has its own drawbacks, creating the potential risk that the data in the system can be obtained using the disadvantages of a particular authentication solution. The key is the fact that, before making a choice, it is always necessary to assess the level of security, and whether this can be achieved through specific solutions.

In addition, we should not forget that most of the problems arise from simple human negligence, for example, the loss of a code card or the storage of passwords in one place with a username. If someone has seen this information, it will not cause any difficulties in using them to access the system, if the authentication system is simple enough and works with reusable passwords and without any other additional security elements.

One of the most common and safe solutions at the moment is the use of a complex combination of long passwords that are recovered after some time, along with the generation of a one-time key, the user receives in the form of SMS. Two-step authentication will be the best solution of such a system.

Literatūra

1. https://lv.wikipedia.org/wiki/Autentifikācija
2. http://ru.wikipedia.org/wiki/Аутентификация
3. https://en.wikipedia.org/wiki/Authentication
4. https://www.esidross.lv/2013/02/19/divpakapju-autentifikacija/
5. https://cert.lv/uploads/Pasākumi/1-Informacijas_sistemu_drosiba.pdf
6. http://odo.lv/Training/EServicesSecurityConcepts