RTU Liepājas akadēmija

Dabas un inženierzinātņu centrs

Viktorija Šabanova,

Studiju programmas “Informācijas tehnoloģijas”

2.kursa studente

Autentifikācijas veidi

Referāts kiberdrošībā

Zinātniskais vadītājs –

Artūrs Ausējs

Liepāja, 2024

Anotācija

Darba autors: Viktorija Šabanova

Darba tēma: Autentifikācijas veidi

Darba veids: Referāts

Studiju programma: Informācijas tehnoloģijas 2.kurss

Darba zinātniskais vadītājs: Artūrs Ausējs

Darba apjoms: 11 lappuses

Atslēgas vārdi: kiberdrošība, autentifikācija, parole, drošība, piekļuve

Pētījuma mērķis: izpētīt dažādus autentifikācijas veidus, salīdzināt tos, atrast visdrošāko

Darba saturs: anotācija, ievads, saturs, autentifikācijas jēdziens, autentifikācijas metožu veidi, secinājumi, literatūras saraksts

Darba rezultāti: tika pierādīta hipotēze, ka lietotājs, kurš labāk pārzina autentifikācijas iespējas, izdarīs labāko opciju, noteiktam gadījumam, lai pasargātu sevi no kiberuzbrukumiem.

Darba izmantojamība: mācību līdzeklis skolām, kursiem, brīvas piekļuves dokuments pašapgūšanai

Saturs

Ievads

Šajā referātā tiks apskatīti dažādi autentifikācijas veidi, drošās paroles izveides padomi. Tēma tika izvēlēta pamatojoties uz tās aktualitātes, jo aizvien biežāk lietotāji uzķeras uz noziedznieku manipulācijām, ļaunprogrammatūrām un citiem veidiem kā "ielauzties" lietotāja personīgā kibertelpā, ar mērķi dabūt sensitīvus datus, paroles, naudas līdzekļus un tā tālāk, bet droša autentifikācija novērš vismaz kādu daļu no iespējama uzbrukuma riska, pārējais ir atkarīgs no lietotāja, piemēram, ja viņš pats "uzķērās" uz piešķērēšanas vēstuli, tad viņš pats brīvprātīgi nodod savus datus .

Pētījuma objekti ir pasaulē plaši un aktīvi izmantojami autentifikācijas veidi. Pētījuma mērķis ir iegūt priekšstatu par dažādiem autentifikācijas veidiem, ar mērķi iemācīties digitāli pasargāt sevi un citus. Galvenais darba uzdevums ir apskatīt un salīdzināt autentifikācijas veidus.

Hipotēze: Lietotājam ar lielākām zināšanām par autentifikācijas un drošās paroles izveidošanas veidiem, ir lielākā iespēja pasargāt sevi no kiberuzbrukumiem un/vai datu noplūdēm.

1. Autentifikācijas jēdziens

Autentifikācija ir process, ko lietotāji izmanto, lai nodrošinātu, ka lietotāju resursus var iegūt tikai atbilstošās personas, pakalpojumi un programmas ar pareizajām atļaujām. Tā ir svarīga kiberdrošības daļa, jo ļaunprātīga faktora galvenā prioritāte ir iegūt nesankcionētu piekļuvi sistēmām. Tas var to izdarīt, nozogot to lietotāju lietotājvārdus un paroles, kuriem ir piekļuve. Autentifikācijas process ietver trīs pamatdarbības:

1) Identifikācija: Lietotāji norāda, kas tie ir, parasti izmantojot lietotājvārdu.
2) Autentifikācija: Parasti lietotāji pierāda, ka viņi ir tie, par kuriem uzdodas, ievadot paroli (kas būtu jāzina tikai konkrētajam lietotājam), bet, lai stiprinātu drošību, daudzas organizācijas arī pieprasa, lai viņi pierādītu savu identitāti ar kaut ko, kas viņiem ir (tālrunis vai marķiera ierīce), vai kaut ko, kas viņi ir (pirkstu nospiedumu vai sejas skenēšanu).
3) Autorizācija: Sistēma pārbauda, vai lietotājiem ir atļauja izmantot sistēmu, kurai viņi mēģina piekļūt.

(Microsoft, 2024)

1.1. Kā darbojas autentifikācija?

Autentifikācija ir svarīga, jo tā palīdz organizācijām aizsargāt savas sistēmas, datus, tīklus, tīmekļa vietnes un programmas pret uzbrukumiem. Tā arī palīdz personām uzturēt savus personas datus konfidenciālus, ļaujot tām veikt tādas darbības kā bankas operācijas vai līdzekļu ieguldīšanu tiešsaistē ar mazāku risku. Ja autentifikācijas procesi ir vāji, uzbrucējam ir vieglāk apdraudēt kontu, uzminot atsevišķas paroles vai ar viltu liekot lietotājiem izpaust savus datus. Tas var novest pie šādiem riskiem:

1) Datu drošības pārkāpums.
2) Ļaunprogrammatūras, piemēram, izspiedējprogrammatūras, instalēšana.
3) Neatbilstība reģionālajiem vai nozares datu konfidencialitātes noteikumiem.

(Microsoft, 2024)

2. Autentifikācijas metožu veidi

2.1. Paroles autentifikācijas

Paroles autentifikācija ir visizplatītākais autentifikācijas veids. Daudzas programmas un pakalpojumi pieprasa, lai lietotāji izveidotu paroles, kurās tiek izmantota ciparu, burtu un simbolu kombinācija, lai mazinātu risku, ka ļaunprātīgs aktors tās uzminēs. Tomēr paroles arī rada drošības un lietojamības izaicinājumus. Lietotājiem ir grūti izdomāt un iegaumēt unikālu paroli katram savam tiešsaistes kontam, tāpēc viņi bieži izmanto paroles atkārtoti. Savukārt, uzbrucēji izmanto daudzas taktikas, lai uzminētu vai nozagtu paroles vai lai no lietotājiem tās izvilinātu pret viņu gribu. Šī iemesla dēļ organizācijas pāriet no parolēm uz citiem ievērojamāki drošākiem autentifikācijas veidiem.

2.1.1. Kas ir droša parole?

Šodien par drošu paroli tiek uzskatīta zīmju kombinācija, kas sastāv no 9 simboliem. To vidū obligāti jābūt gan mazajiem un lielajiem burtiem, gan cipariem un simboliem, piemēram, izsaukuma zīmei vai kolam. Noteikti jāizvairās no savu tuvāko radinieku vai mājdzīvnieku vārda vai dzimšanas datuma iekļaušanas parolē. Tās būs pirmās lietas, ko izmēģinās pārlieku ziņkārīgs noziedznieks. Nederēs arī citi ar Jums saistītu lietu nosaukumi, par kuriem apkārtējie labi zina, piemēram, iecienītā sporta komanda, mīļākie ziedi un tamlīdzīgi. Drošības eksperti pat saka, ka neviens ikdienā lietots vārds pats par sevi nav drošs, jo uzlaušanas programmas var īsā laikā pārbaudīt visu vārdnīcu. Vajadzētu izvairīties arī no pārāk vienkāršotas simbolu kombinācijas, piemēram, “k0ks” vai “4iekurs”, izmantošanas , visām vietnēm lietojiet citu paroli, izveidojiet savu šifra atslēgu un lietojiet to visās parolēs (SEB, 2015). Tātad, piemērs drošai parolei būtu “Q_entiO97_*p”.

2.2. Sertifikāta autentifikācija

Sertifikāta autentifikācija ir šifrēta metode, kas ļauj ierīcēm un personām sevi identificēt citās ierīcēs un sistēmās. Divi bieži sastopami piemēri ir viedkarte un ciparsertifikāts, kā arī eParaksts, ko lietotāja ierīce nosūta uz tīklu vai serveri, tas nodrošina to, ka no servera līdz klienta datoram parsūtītā informācija tiek šifrēta un to nav iespējams pārtvert, izmainīt vai viltot. (AreaIT, 2024).

(Drošo savienojumu slāņa sertifikāts) ir vietnes unikālais digitālais paraksts, kas sastāv no failu komplekta, kas ir instalēts serverī, un satur publisko atslēgu, sertifikācijas centra parakstu un sertifikāta īpašību aprakstu. Sertifikāta īpašībās tiek aprakstīti galvenie parametri: aizsargātās domēna nosaukums, domēna īpašnieks, derīguma termiņš, sertifikāta īpašnieka fiziskā atrašanās vieta, sertifikāta piegādātāja uzņēmuma rekvizīti un citi parametri. Tas palīdz

apmeklētājiem pārliecināties, ka viņi ir nonākuši uz oriģinālās vietnes un ka visi dati, ko apmeklētāji un klienti ievada vietnē, tiek pārraidīti, izmantojot šifrētu savienojumu un nevar tikt pārtraukti trešām personām. (Zomro, 2022)

Šāds sertifikāts ir obligāts, galvenokārt bankām, maksājumu sistēmām un citām organizācijām, kas strādā ar personiskiem datiem, tas ir, visur, kur jūs pieņemat maksājumus savā vietnē vai lūdzat klientiem atstāt personiskos datus. SSL sertifikāts apstiprina, ka domēns pieder reālai uzņēmumam. (Zomro, 2022)

2.3. Biometriskā autentifikācija

Biometriskās autentifikācijas laikā personas verificē savu identitāti, izmantojot bioloģiskus līdzekļus. Piemēram, daudzi lietotāji izmanto savu pirkstu vai īkšķi (skat. 1.attēls), lai pierakstītos savā tālrunī, un daži datori skenē personas seju vai acs tīkleni, lai verificētu lietotāja identitāti. Biometriskie dati ir saistīti arī ar konkrētu ierīci, tāpēc uzbrucēji nevar tos izmantot, neiegūstot piekļuvi pašai ierīcei. Šāda veida autentifikācija kļūst arvien populārāka, jo lietotājiem tā ir ērta — nekas nav jāiegaumē —, bet ļaunprātīgiem uzbrūcējiem ir grūti to nozagt, kas padara to drošāku par parolēm. (Microsoft, 2024)

1.attēls. Pirksta biometrija

Lai piekļūtu noteiktai telpai vai resursam, personai ir jāuzrāda skenerim pareizā fiziskā īpašība. Pēc tam sistēma salīdzina paraugu ar datu bāzi. Tikai pēc atbilstības iegūšanas persona var iegūt pieprasīto piekļuvi. Šāda veida biometriskās autentifikācijas spēks ir patiesi unikāla iezīme, kas jāizmanto, lai iegūtu piekļuvi. Ir ļoti grūti viltot pirkstu nospiedumus vai seju, lai apietu drošību. (TJGOnline, 2022)

Uzvedības autentifikācija balstās uz personas faktisko uzvedību. Parasti šāda veida autentifikācijas piemēri ir balss, gaita un runas ritms vai dikcija. Lai gan ir diezgan viegli atdarināt citas personas balss skaņu, viņu runas faktisko toni vai noti ir daudz grūtāk dublēt. Šis drošības veids visbiežāk tiek izmantots, lai piekļūtu datora failiem vai citai sistēmas uzturētai drošībai. (TJGOnline, 2022)

2.4. Marķiera autentifikācija

Marķiera autentifikācijā gan ierīce, gan sistēma ik pēc 30 sekundēm ģenerē jaunu unikālu numuru, ko sauc par laikatkarīgu vienreizējo PIN (time-based one-time PIN — TOTP). Ja numuri atbilst, sistēma verificē, ka lietotājam ir atbilstošā ierīce. (Microsoft, 2024)

Veicot marķiera reverso inženieriju, var identificēt vairākas iespējamās ievainojamības, kuras uzbrucēji var izmantot, lai iegūtu nesankcionētu piekļuvi vai manipulētu ar tīmekļa lietojumprogrammām. Tīmekļa lietojumprogrammu kontekstā marķieri bieži tiek izmantoti sesiju pārvaldībai, autentifikācijai un autorizācijas nolūkiem. Izmantojot reversās inženierijas pilnvaras, uzbrucēji var gūt ieskatu sistēmas iekšējā darbībā un izmantot ievainojamības ļaunprātīgām darbībām. (EIROPAS INFORMĀCIJAS TEHNOLOĢIJU SERTIFIKĀCIJAS AKADĒMIJA , 2023)

Viena no iespējamām ievainojamībām, ko var identificēt reversās inženierijas laikā, ir šifrēšanas trūkums vai vāji šifrēšanas algoritmi, ko izmanto marķieru ģenerēšanā. Tokenus parasti ģenerē serveris un nosūta klientam, kur tie tiek saglabāti un nosūtīti atpakaļ uz serveri autentifikācijai. Ja marķieris nav pareizi šifrēts vai izmanto vājus šifrēšanas algoritmus, uzbrucēji var pārtvert marķieri un manipulēt ar to, lai iegūtu nesankcionētu piekļuvi. Piemēram, ja marķieris tiek pārsūtīts pa nedrošu savienojumu vai saglabāts nešifrētā formātā klienta pusē, uzbrucējs var pārtvert marķieri un izmantot to, lai uzdotos par likumīgu lietotāju. (EIROPAS INFORMĀCIJAS TEHNOLOĢIJU SERTIFIKĀCIJAS AKADĒMIJA , 2023)

2.5. Vienreizēja parole

Vienreizējās paroles (one-time password — OTP) ir kodi, kas tiek ģenerēti konkrētam pierakstīšanās notikumam, kura derīgums beidzas īsi pēc to izdošanas. Tie tiek piegādāti, izmantojot īsziņas, e-pasta ziņojumus vai aparatūras marķierus (Microsoft, 2024). Parasti izmanto vienreizējās paroles kodu konta reģistrācijas un atjaunināšanas laikā, lai apstiprinātu jūsu kontaktinformāciju.

Vienreizējo paroli var ģenerēt, izmantojot dažādus līdzekļus, piemēram, mobilo lietojumprogrammu, fiziskās drošības marķieri, SMS un citus (Miscellanea, 2021). Tas padara autentifikāciju drošāku pret pikšķerēšanu.

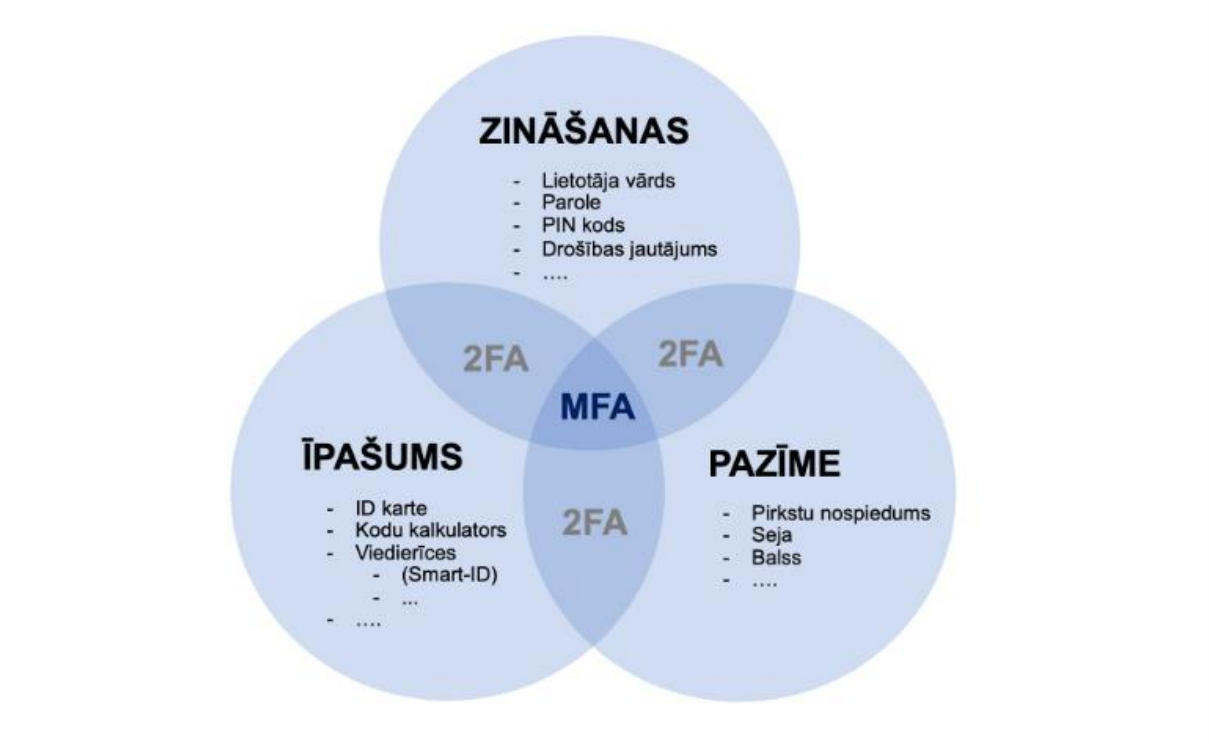
2.6.Daudzfaktoru autentifikācija

Divfaktoru autentifikācija (2FA) ir autentifikācijas process, kad papildus lietotājvārdam un parolei tiek pieprasīts papildu apstiprinājums, ka tiešām esat šī konta īpašnieks. Tā aizsargā lietotāja datus, ja lietotāja paroli ir ieguvusi cita persona. (Latvijas Universitāte, 2024)

Viens no vislabākajiem veidiem, kā samazināt konta apdraudējumu, ir pieprasīt izmantot vismaz divas autentifikācijas metodes, kuras var ietvert jebkuru no iepriekš norādītajām metodēm. Efektīva paraugprakse ir pieprasīt jebkuras divas no šīm metodēm:

1) Kaut kas, ko lietotājs zina. Parasti tā ir parole.
2) Kaut kas, kas tam ir, piemēram, uzticama ierīce, kuru nav viegli dublēt, piemēram, tālrunis vai aparatūras marķieris.
3) Kaut kas, kas ir lietotājs, piemēram, pirksta nospiedums vai skenēts sejas attēls.

Piemēram, daudzas organizācijas pieprasa paroli (kaut ko, ko lietotājs zina), kā arī nosūta OTP, izmantojot SMS, uz uzticamu ierīci (kaut kas, kas ir lietotājam), pirms atļauj piekļuvi (Microsoft, 2024).



2.attēls. Daudzfaktoru autentifikācijas princips *(ESIDROŠS, 2021)*

Secinājumi

1) Ir daudz un dažādi veidi kā sevi pasargāt izmantojot vienu vai vairākus autentifikācijas veidus. Katrs no tiem ir paredzēts saviem mērķiem. Piemēram, ikdienā, izmantojot mobilās ierīces, visērtākais un visdrošakais veids ir biometriskā autentifikācija. Izmantojot valsts pakalpojumu vietnes, ieteicama sertifikāta autentifikācija (eParaksts). Sociāliem tīkliem, e-pastiem un citiem der vairāki veidi, kā piemēram, paroles, marķiera vai daudzfaktoru autentifikācija.
2) Zinot kādu veidu izmantot katrā situācijā, lietotājs var sevi pasargāt no kiberincidentiem un/vai datu noplūdes, kas pierāda hipotēzi.

Literatūras saraksts

1) AreaIT. (2024). *SSL sertifikāts. area.lv*. Ielādēts no area.lv: https://area.lv/lv/ssl-sertifikats/
2) EIROPAS INFORMĀCIJAS TEHNOLOĢIJU SERTIFIKĀCIJAS AKADĒMIJA . (2023. gada 5. augusts). *EITCA*. Ielādēts no lv.eitca.org: https://lv.eitca.org/kiberdro%C5%A1%C4%ABba/eitc-ir-wapt-t%C4%ABmek%C4%BCa-lietojumprogrammu-iespie%C5%A1an%C4%81s-p%C4%81rbaude/t%C4%ABmek%C4%BCa-uzbrukumu-prakse/s%C4%ABkfailu-v%C4%81k%C5%A1ana-un-revers%C4%81-in%C5%BEenierija/p%C4%81rbaudes-p%C4%81rska
3) ESIDROŠS. (2021. gada 25. marts). *esidross.lv*. Ielādēts no esidross.lv: https://www.esidross.lv/2021/03/25/papildu-drosiba-vairaku-faktoru-autentifikacija/
4) Latvijas Universitāte. (2024). *itserviss.lu.lv*. Ielādēts no itserviss.lu.lv: https://itserviss.lu.lv/it-serviss/divfaktoru-autentifikacija/#:~:text=Kas%20ir%202FA%20un%20k%C4%81d%C4%93%C4%BC%20t%C4%81%20ir%20nepiecie%C5%A1ama%3F,datus%2C%20ja%20lietot%C4%81ja%20paroli%20ir%20ieguvusi%20cita%20persona.
5) Microsoft. (2024). *Microsoft*. Ielādēts no microsoft.com: https://www.microsoft.com/lv-lv/security/business/security-101/what-is-authentication?msockid=11be9fce597961752fce8ad65851609c
6) Miscellanea. (2021. gada 19. decembris). *ReviensMedia*. Ielādēts no ReviensMedia: https://reviensmedia.com/lv/advices/3758-what-is-one-time-password-definition--meaning
7) SEB. (2015. gada 17. jūnijs). *Drošība. SEB banka*. Ielādēts no seb.lv: https://www.seb.lv/info/drosiba/kas-ir-drosa-parole-un-ka-izveidot
8) TJGOnline. (2022. gada 6. marts). *TJGOnline*. Ielādēts no TJGOnline: https://tjgonline.com/kas-ir-biometriska-autentifikacija/
9) Zomro. (2022. gada 27. marts). *Noderīgi raksti. zomro.com*. Ielādēts no zomro.com: https://zomro.com/lv/blog/articles/104-chto-nuzhno-znat-o-ssl-sertifikate