VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
PROGRAMŲ SISTEMŲ KATEDRA

Skaitmeninės tapatybės valdymas taikant blokų grandinę

Digital Identity Management using Blockchain

Bakalauro darbas

Atliko:	Jurgis Kargaudas	(parašas)
Darbo vadovas:	asist. Aurimas Šimkus	(parašas)
Darbo recenzentas:	TO BE ADDED	(parašas)

Vilnius – 2018

Santrauka

Naudotojo autentifikavimas yra svarbus kuriant programų sistemas. Natūralus siekis įsitikinti naudotojo autentiškumu šiais laikais kelia vis didesnes problemas - tam pačiam asmeniui besinaudojant vis daugiau sistemų internete, skaitmeninių tapatybių valdymas sudėtingėja. Kiekvienas naudotojas tampa priverstas prisiminti aibę prisijungimo vardų ir slaptažodžių, neretai dėl to pradeda naudoti identiškus slaptažodžius ir paaukoja jų stiprumą, o sistemų kūrėjai turi skirti papildomų resursų identifikavimo valdymui.

Programų sistemose skaitmeninėms tapatybėms valdyti naudoti įvairūs metodai - atskiros naudotojų duomenų bazės, centralizuotos platformos kelioms sistemoms, vienkartinio prisijungimo sprendimai. Blokų grandinės yra nauja alternatyva skaitmeninių identitetų organizavimui programose. Šiame darbe nagrinėtas blokų grandinės tinkamumas skaitmeninių tapatybių valdymui, pridėti gautus dalykus.

Raktiniai žodžiai: autentifikavimas, tapatybė, skaitmeninis tapatybių valdymas, blokų grandinė

Summary

User authentication is crucial for a handful of software systems. A natural wish to ensure user's authenticity nowadays causes ever bigger problems - as the same person uses more and more internet software systems, digital identity management becomes complex. Every user is forced to remember quite a few sets of credentials, that often results in identical passwords and reduced credential strength, when software creators have to put in additional resources for identity management.

Various methods are used to manage digital identities in software applications - separate user databases, centralized credential platforms for several systems, single sign-on solutions. Blockchain is a new alternative to organize identity data in software. This thesis investigates the suitability of blockchain for digital identity management, add discovered stuff.

Keywords: authentication, identity, digital identity management, blockchain

Įvadas

Naudojimasis interneto paslaugomis šiais laikais yra neatsiejama žmonių gyvenimo dalis. Norėdami individualizuoti turinį, sustiprinti taikomosios programos saugumą ar siekdami iš anksto išvengti kenkėjiškų tikslų turinčių asmenų ar sukurtų robotų, paslaugų tiekėjai neretai prašo naudotojų prisijungti. Interneto naudotojų skaičiui perkopus 4 milijardus [Min18], o kiekvienam naudotojui vidutiniškai turint po 7 skirtingas socialines paskyras [MM17], asmenų autentifikavimas tampa vis didesniu iššūkiu.

Susidariusi situacija kelia problemų tiek paslaugų tiekėjams, tiek jų naudotojams. Kiekvienas paslaugų tiekėjas turi skirti papildomų resursų naudotojų tapatybių valdymui, jų autentifikavimui, jautrių duomenų saugumo užtikrinimui. Paslaugų naudotojams bene didžiausi atsiradę keblumai - milžiniškas įsimintinų slaptažodžių kiekis bei sunkumai kontroliuojant savo asmens duomenų sklaidą skirtingose sistemose. Prisijungimo vardui ir slaptažodžiui išliekant populiariausiais asmens atpažinimo įrankiais, naudotojai dėl per didelio įsimintinų slaptažodžių kiekio neretai paaukoja saugumą dėl patogumo ir pradeda naudoti tą patį slaptažodį sirtingoms sistemoms [PM03; Sam99]. Naudotojas, turėdamas keletą paskyrų skirtingose sistemose, taip pat praranda dalį savo asmens duomenų kontrolės. Jam tenka pasitikėti taikomosios programos naudojamomis technologijomis ir metodais ir tikėtis, kad jie bus pakankamai saugūs ir stabilūs bei suteikti asmens duomenys nepasieks nepageidaujamų adresatų. Didėjant naudojamų paslaugų kiekiui, naudotojo skaitmeninės tapatybės duomenis turi vis daugiau taikomųjų programų ir bent vienai iš jų patyrus programišių įsilaužimą ar kitokią nesėkmę, jautrūs naudotojo duomenys būna paviešinti.

Pagrindiniu skaitmeninės tapatybės valdymo keliamų problemų sprendimu išlieka vienkartinis prisijungimas (angl. *Single Sign-On*). Šis sprendimas leidžia naudotojui pasirinkti vieną tapatybės tiekėją (angl. *identity provider*) ir patikėti jam skaitmeninės tapatybės valdymą. Tuomet naudotojas prie visų paslaugų, palaikančių pasirinkto tapatybės tiekėjo (pvz. *Facebook*) prisijungimą, gali autentifikuotis naudodamas ta pačia paskyra. Tokiu būdu naudotojui pakanka prisiminti tik slaptažodžius, užregistruotus tapatybės tiekėjų sistemose, o paslaugų tiekėjai neturi patys rūpintis autentifikavimu ar autorizavimu, o jį užtikrina integruodami sistemą su tapatybės tiekėju. Tačiau šis sprendimo būdas taip pat turi aiškių trūkumų - naudotojas negali prisijungti prie paslaugų, nepalaikančių pasirinkto tapatybės tiekėjo, dėl paslaugų tiekėjų priklausomybės nuo tapatybės tiekėjo pastarojo pasiekiamumas tampa vieninteliu nesėkmės tašku (angl. *single point of failure*), naudotojas taip pat praranda dalį savo asmens duomenų kontrolės. Naršantis internete asmuo yra priverstas pasitikėti tapatybės tiekėjo gebėjimu perduoti tik naudotojo leistus asmens duomenis ir tik toms trečiosioms šalims, kurias jis patvirtina. Kaip rodo *Cambridge Analytica* neleistino duomenų perdavimo incidentas [Gra18], net didžiosios kompanijos, tokios kaip *Facebook*, ne visada sugeba tai užtikrinti.

Blokų grandinė (angl. *blockchain*) yra nauja alternatyva skaitmeninės tapatybės valdymui. Ši technologija veikia kaip paskirstytų įrašų platforma (angl. *Distributed Ledger Platform*), kurioje kiekvienas įrašas yra nekintamas (angl. *immutable*), o visi užfiksuoti įrašai atspindi tikslią transakcijų istoriją nuo pat grandinės sukūrimo [Baa16]. Saugant tapatybės duomenis šioje grandinėje ir pritaikius reikiamą blokų grandinės pasiekiamumo lygį įrašų rašymui ir skaitymui,

asmuo visada žinotų, kokia trečioji šalis gali pasiekti kokius tapatybės duomenis. Kadangi blokų grandinė yra decentralizuota, pritaikius ją skaitmeninių tapatybių valdyme taip pat būtų galima išvengti šioje srityje dažnos vienintelio nesėkmės taško problemos. Šiame darbe nagrinėjama, kada verta naudoti blokų grandinę naudotojų skaitmeniniam autentifikavimui bei autorizavimui, kokie to pranašumai, trūkumai bei priėmimo barjerai (angl. *adoption barriers*).

Darbo tikslas - ištirti blokų grandinės tinkamumą skaitmeninės tapatybės valdymui.

Darbe keliami uždaviniai:

1. Išnagrinėti esamus skaitmeninės tapatybės valdymo sprendimus ir jų keliamus iššūkius.
2. Apibūdinti blokų grandines ir jų savybes, leidžiančias išspręsti dabartines identifikavimo problemas.
3. *Apžvelgti esamas blokų grandinės sistemas, taikomas naudotojų autentifikavimui ar autorizavimui*.
4. Išskirti blokų grandinės panaudos atvejį skaitmeninės tapatybės valdymui ir įvertinti jo tinkamumą apibūdinant sprendimo privalumus, trūkumus ir pritaikymo barjerus.
5. Palyginti pristatytą sprendimą su standartiniais naudotojų autentifikavimo ir autorizavimo būdais.
6. Pademonstruoti sudaryto skaitmeninio tapatybės valdymo modelio veikimą naudojantis kažkuriuo blockchainu.

TURINYS

1. Medžiagos darbo tema dėstymo skyriai

Medžiagos darbo tema dėstymo skyriuose išsamiai pateikiamos nagrinėjamos temos detalės: pradiniai duomenys, jų analizės ir apdorojimo metodai, sprendimų įgyvendinimas, gautų rezultatų apibendrinimas.

Medžiaga turi būti dėstoma aiškiai, pateikiant argumentus. Tekste dėstomas trečiuoju asmeniu, t.y. rašoma ne „aš manau“, bet „autorius mano“, „autoriaus nuomone“. Reikėtų vengti informacijos nesuteikiančių frazių, pvz., „...kaip jau buvo minėta...“, „...kaip visiems žinoma...“ ir pan., vengti grožinės literatūros ar publicistinio stiliaus, gausių metaforų ar panašių meninės išraiškos priemonių.

Skyriai gali turėti poskyrius ir smulkesnes sudėtines dalis, kaip punktus ir papunkčius.

1.1. Poskyris

Citavimo pavyzdžiai: cituojamas vienas šaltinis [**PvzStraipsnLt**]; cituojami keli šaltiniai [**PvzStraipsnEn**; **PvzKonfLt**; **PvzKonfEn**; **PvzKnygLt**; **PvzKnygEn**; **PvzElPubLt**; **PvzElPubEn**; **PvzMagistrLt**; **PvzPhdEn**].

1.1.1. Skirsnis

1.1.1.1. Straipsnis

1.1.2. Skirsnis

2. Skyrius

2.1. Poskyris

2.2. Poskyris

Rezultatai ir išvados

Rezultatų ir išvadų dalyje išdėstomi pagrindiniai darbo rezultatai (kažkas išanalizuota, kažkas sukurta, kažkas įdiegta), toliau pateikiamos išvados (daromi nagrinėtų problemų sprendimo metodų palyginimai, siūlomos rekomendacijos, akcentuojamos naujovės). Rezultatai ir išvados pateikiami sunumeruotų (gali būti hierarchiniai) sąrašų pavidalu. Darbo rezultatai turi atitikti darbo tikslą.

Literatūra

[Baa16] Djuri Baars. Towards Self-Sovereign Identity using Blockchain Technology. Disertacija, University of Twente, 2016. URL: http://essay.utwente.nl/71274/1/Baars_MA_BMS.pdf.

[Gra18] Kevin Granville. Facebook and Cambridge Analytica, 2018. URL: https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html (tikrinta 2018-03-28).

[Min18] Miniwatts Marketing Group. World Internet Users Statistics, 2018. URL: https://www.internetworldstats.com/stats.htm (tikrinta 2018-03-28).

[MM17] Jason Mander ir Felim McGrath. Global Web Index Social. Tech. atask., 2017. URL: https://cdn2.hubspot.net/hubfs/304927/Downloads/GWI%20Social%20Summary%20Q3%202017.pdf.

[PM03] Andreas Pashalidis ir Chris J. Mitchell. A taxonomy of single sign-on systems. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2727 LNCS:249–264, 2003. ISSN: 03029743.

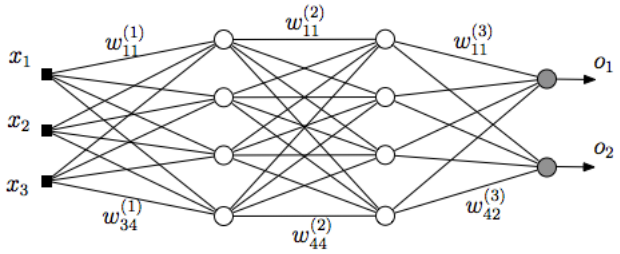
[Sam99] V Samar. Single sign-on using cookies for Web applications. Proceedings IEEE 8th International Workshops on Enabling Technologies Infrastructure for Collaborative Enterprises WET ICE99:158–163, 1999. ISSN: 10801383.

Santrumpos

Sąvokų apibrėžimai ir santrumpų sąrašas sudaromas tada, kai darbo tekste vartojami specialūs paaiškinimo reikalaujantys terminai ir rečiau sutinkamos santrumpos.

Priedas nr. 1

Niauroninio tinklo struktūra



1 pav. Paveikslėlio pavyzdys

Priedas nr. 2
Eksperimentinio palyginimo rezultatai

1 lentelė. Lentelės pavyzdys

Algoritmas	$\bar{x}$	σ^2
Algoritmas A	1.6335	0.5584
Algoritmas B	1.7395	0.5647