SKAITMENINIŲ PĖDSAKŲ PALIKIMO MASTO INTERNETE ASPEKTAI

Asta Slotkienė, Simona Ramanauskaitė
Šiaulių universitetas, Informacinių technologijų katedra

Įvadas

Nuolat tobulėjančios technologijos, jų prieinamumas ir naudojimosi nesudėtingumas leidžia vis didesnei visuomenės daliai aktyviai naudotis interneto teikiamomis paslaugomis. Internetinės technologijos pasiekiamos jau ne tik asmeniniuose kompiuteriuose, bet ir delniniuose kompiuteriuose, mobiliuosiuose išmaniuosiuose telefonuose, todėl žmonės vis daugiau laiko praleidžia naršydami internete. Tai teikia galimybių reikiamos informacijos paieškai pagreitinti, nuolat sekti naujausią informaciją, keistis duomenimis, bendrauti su kitais asmenimis, nuolat viešinti informaciją apie asmens buvimo vietą. Visa ši asmeninė ar su ja susijusi informacija, kuri paliekama internete, dažnai vadinama skaitmeniniais pėdsakais (*angl.* footprints). Šio darbo ***tikslas*** – nustatyti, kiek plačiai asmenys atskleidžia savo asmeninę informaciją internete, kuri vienaip ar kitaip gali būti panaudota prieš juos, surinkus jų skaitmeninius pėdsakus, ir įvertinti randamo informacijos kiekio ir jau turimų žinių apie tą asmenį ryšius.

Skaitmeninių pėdsakų samprata

Skaitmeniniai pėdsakai yra dažniausias asmeninės informacijos rinkimo būdas, kai suinteresuoti asmenys kaupia informaciją apie asmenis, įmones ar jose funkcionuojančias kompiuterių sistemas. Skaitmeninių pėdsakų tikslas – sužinoti kuo daugiau ir kuo tikslinės informacijos, kuri būtų tinkama prieigai prie sistemų pažeisti, konfidencialiai informacijai perimti, asmens ypatybėms ar jo veiklai atskleisti (Garfinkel, Cox, 2009). Tai duoda galimybių atakai prieš tą asmenį arba socialinę inžineriją surengti, t. y. per asmenį pasiekti atitinkamos įmonės informaciją.

Rastos informacijos internete svarba gali būti labai įvairi ir priklausanti nuo aplinkybių. Tik retais atvejais pavyksta iš karto gauti tiesioginę informaciją, kuri vienaip ar kitaip tiktų efektyvesnei atakai vykdyti. Dažniausiai atakuojantysis bando surinkti, kiek įmanoma, kuo daugiau skaitmeninių pėdsakų, juos analizuoja, interpretuoja, taiko įvairias modifikavimo (kombinacijų, pakeitimų ir kt.) procedūras. Tačiau šiems veiksmams nemažai įtakos turi informacija, kurią pavyko rasti ir kuri jau žinoma apie tą asmenį. Pavyzdžiui, slaptažodžių atrankai neretai pasitelkiamos žmogaus psichologinės savybės, kurios gali lemti slaptažodžio sudarymo techniką ar galimas kombinacijas. Tad vienareikšmiškai pasakyti, kokią informaciją pavojinga skelbti internete, ganėtinai sudėtinga.

Dažniausias atakuojančiųjų tikslas – sužinoti numatyto asmens prisijungimo prie tam tikros informacinės sistemos duomenis. Atliekama keletas pasyvių veiksmų, būtent, nekuriamos fiktyvios sistemos, nebandoma tiesiogiai išgauti informaciją, o naudojamasi tuo, kas prieinama viešai:

- Išsiaiškinti, kokiomis kitomis sistemomis naudojasi asmuo – galbūt jos turi tam tikrų spragų, leidžiančių sužinoti norimo asmens prisijungimo duomenis. Turint bent kelis asmens prisijungimo duomenis prie skirtingų sistemų, jau galima daryti aiškesnes išvadas apie vartotojo prisijungimo vardų ir slaptažodžių parinkimo idėjas.
- Surinkti apie norimą žmogų asmeninės informacijos – neretai žmonės prisijungimo vardui ar slaptažodžiui naudoja bent dalį informacijos apie save ar iš savo aplinkos, t. y. jaunos mamos mėgsta slaptažodžius parinkti savo vaikų vardus, jaunimas vartoja pravardės modifikacijas ir pan.

Asmeninių duomenų viešinimo socialiniuose tinkluose aspektai

Asmeninių duomenų paviešinimo visiems vartotojams prieinamose interneto svetainėse, forumuose, socialiniuose tinklapiuose, portaluose privalumai įžvelgiami kaip savęs ar įmonės pateikimas ir reklama. Tačiau tai visada turi ir neigiamų aspektų: informacijos vagystės, psichologinis teroras ir pan. Pastaruoju metu atlikta nemažai tyrimų, atskleidžiančių viešai prieinamos informacijos (skaitmeninių pėdsakų palikimo) paplitusiuose socialiniuose tinkluose tendencijas. Kaip pastebi US CERT (McDowel, Morda, 2011), socialiniuose tinkluose ar internete randama informacija gali būti panaudojama net nusikalstamai veiklai: socialinės inžinerijos atakos, asmens vagystės ir pan. (Felt, Evans, 2008). Tuo tarpu ECAR tyrimo duomenimis (2008), daugiau nei 85 % apklaustųjų yra vieno ar kelių socialinių tinklų vartotojai. Jie bendrauja su draugais, publikuoja asmenines nuotraukas, dalijasi informacija. Šio tyrimo duomenimis, net 51 % apklaustųjų teigė ieškantys informacijos apie kitus žmones.

R. Gross ir A. Acquisti (2005) atliko tyrimus, analizuodami asmeninės informacijos pateikimo mastus *Facebook* socialiniame tinklapyje, ir pastebėjo, kad turintys asmeninius profilius asmenys pateikia palyginti daug skirtingo tipo asmeninės informacijos apie save (iki 80 % respondentų nurodo savo tikrąjį vardą, nuotraukas, gimimo datą, baigtą mokyklą ir pan.). Tuo tarpu H. Jones, J. H. Soltren

(2005) atlikti tyrimai atskleidė ne tokius didelius asmeninių duomenų paviešinimo mastus, tačiau pastebėjo, kad kiekvienais metais studentai paviešina vis daugiau asmeninės informacijos apie save. Be to, kitas svarbus šio tyrimo metu išryškėjęs faktas – *Facebook* vartotojams neaktualus jų asmeninių duomenų pateikimas ir jų saugumas: apie 80 % respondentų visiškai nesidomi arba tik retkarčiais įvertina savo pateiktų duomenų saugumą, 12 % apie tai galvoja ir tik 5 % yra labai susirūpinę pateikiama informacija. A. L. Young ir A. Quan-Haase (2009) duomenimis, daugiau nei 70 % *Facebook* sistemos vartotojų savo informaciją pateikia tik draugų ratui. Tai rodo žmonių nenorą visiškai viešai platinti savo asmeninių duomenų.

R. Goettke ir J. Christiana (2007) atliko tyrimus ir nustatė, kaip įvairių socialinių tinklapių vartotojai reaguoja į prašymus priimti į draugus nepažįstamus asmenis. Tokio tyrimo rezultatai iš dalies leistų kiekybiškai įvertinti vartotojų rūpinimosi savo pateikiamos informacijos viešumu lygtį. Deja, kaip ir patys autoriai teigia, – buvo tiriamas per mažas skirtingus socialinius tinklapius naudojančių asmenų kiekis bei nebuvo galimybių įsitikinti, ar prašymai buvo ignoruojami, ar siunčiami tuo metu sistemoje neaktyviems vartotojams. Remiantis šiais duomenimis, galima daryti preliminarias prielaidas, kurios rodytų, jog nemaža dalis *Facebook* vartotojų linkę „aklai“ priimti naujus, nepažįstamus asmenis į savo draugų sąrašą.

Remiantis mokslininkų tyrimų rezultatais apie asmeninių duomenų viešinimo socialiniuose tinkluose savybes, pastebėta, kad vartotojai, pateikdami duomenis apie save, neįvertina jų viešinimo pasekmių. Nors atlikti tyrimai su realia *Facebook* aplinka ir jos simuliacija parodė, kad vartotojų elgsena jose yra panaši (Parris, Abdesslen, Henderson, 2010), bet visi aptikti tyrimai koncentruoti į socialinius tinklapius ir juose viešinamą informaciją, bet apibendrinimų apie internete (forumai, straipsniai ir kita) skelbiamus asmeninius duomenis praktiškai nėra, neatskleista ir tai, kiek internete rasta asmeninė informacija atitinka realius duomenis ir jų patikimumą.

Asmeninių duomenų viešinimo internete tyrimas

Tyrimo metodika

Siekiant išsiaiškinti, kokiu mastu viešinama asmeninė informacija internete, buvo atliktas tyrimas, kuriame dalyvavo informatikos inžinerijos IV kurso studentai (tarp jų 6, studijuojantys pagal Erasmus programą ir atvykę iš Latvijos bei Turkijos). Tyrimas atliktas 2011 m. pavasarį. Jo metu buvo tiriama jautriausia asmeninė informacija, kuri gali būti panaudojama skaitmeninių atspaudų rinkimui (Tuunainen, Pitkanen, Hovi, 2009).

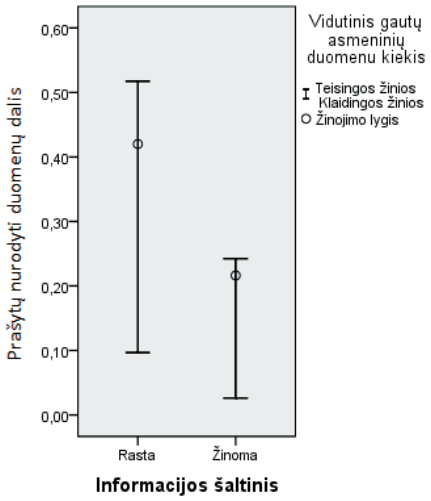
Pirmame tyrimo etape respondentams buvo pateikta anketa, kurioje jie nurodė savo asmeninę informaciją ir nusakė dažniausiai vykdomą veiklą internete (ši informacija tyrime įvardyta kaip „tikra“). Antrame etape, priskyrus tyrėjui nagrinėjamą asmenį, buvo surinkta pradinė informaciją apie jį, siekiant įvertinti, kiek tyrėjas žino apie asmenį, prieš ieškodamas skaitmeninių jo pėdsakų internete (ši informacija tyrime įvardyta kaip „žinoma“). Tai sudarė prielaidas nusakyti, ar pradinė informacija palengvina tyrėjui pėdsakų paiešką. Trečiajame etape tyrėjas anketoje nurodė, kokią informaciją t. y. skaitmeninius pėdsakus, rado apie nagrinėjamą asmenį internete (ši informacija įvardyta kaip „rasta“).

Asmeninių duomenų viešumo tyrimu siekta šių tikslų: nustatyti, kurią dalį galimai jautrios asmeninės informacijos tyrėjas gali gauti nejučia, tiesiog bendraudamas su atitinkamu asmeniu; nustatyti, kiek internete pateikiamos informacijos apie asmenį iš dalies ar visiškai neatitinka realybės ir kokia dalis galimai jautrių asmeninių duomenų gali būti aptikta viešai internete; įvertinti, kaip pradinės informacijos apie asmenį kiekis turi įtakos skaitmeniniams pėdsakams rasti internete.

Tyrimo rezultatų analizė

Vertinant internete viešinamos informacijos apie asmenį teisingumą, nustatyta, kad netikslios informacijos apie asmenį pateikiama mažiau nei tikslių duomenų, t. y. dažniausiai internete informacija apie asmenį yra skelbiama arba ne, o klaidinančios informacijos apie konkretų asmenį yra palyginti nedaug. Be to, dažniausiai klaidingi duomenys atsiranda dėl sutampančių asmens vardų ir pavardžių, bet ne dėl to, jog siekiama specialiai klaidinti interneto vartotojus.

Palyginus tarpasmeninio bendravimo metu gautus ir internete rastus duomenis, pastebėta, kad žmonės negeba tinkamai įvertinti internete rastos informacijos teisingumo (bendravimo būdu surinktose žiniose pasitaikė 3 % klaidinančios informacijos, o iš internete rastų duomenų net 10 % netikslūs ar klaidingi).

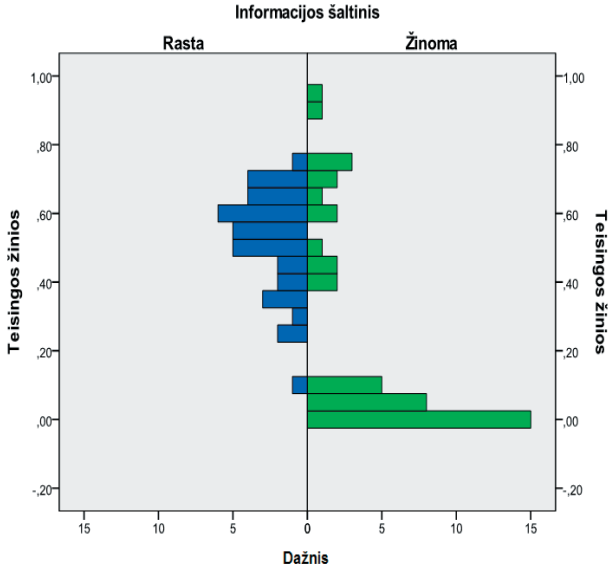


1 pav. Teisingi, klaidingi ir vidutiniškai žinomi bei rasti internete duomenys apie asmenį, procentais

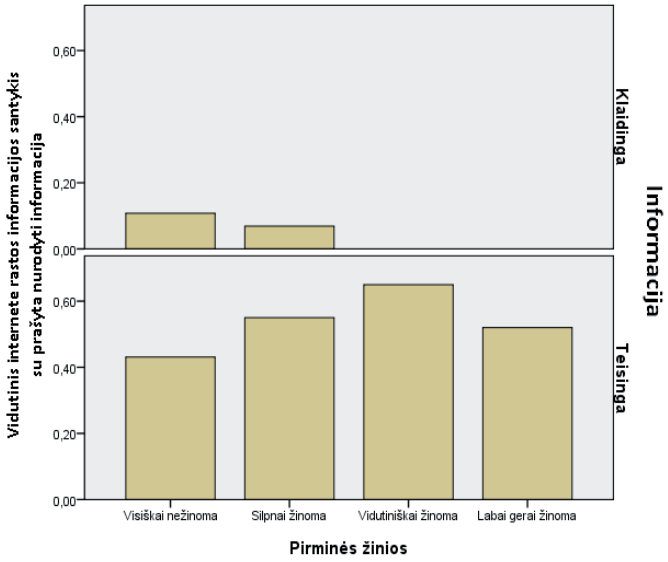
Tyrimo metu pastebėta, kad internetas gali pateikti daugiau duomenų apie asmenį nei pasyvus (gaunamas kasdieninio bendravimo, o ne specialių paieškų metu) tarpasmeninis bendravimas. Vidutinė internete rasta informacija buvo beveik du kartus didesnė už respondentų žinomos informacijos kiekį (buvo rasta 42 % reikalautų duomenų apie asmenį, o žinomi tik 23 %).

Analizuojant atskirus tyrimo anketų atvejus pastebėta, kad beveik 5 % respondentų pateikė labai gerų žinių apie analizuojamą asmenį (daugiau nei 80 % reikalautos informacijos buvo teisinga). Tuo tarpu didžiausias internete rastos informacijos kiekis apie konkretų asmenį siekė tik 80 %. Tačiau tarp respondentų žinias apie konkretų asmenį nusakančių anketų daugiau nei pusė atskleidė labai mažai žinių (nurodyta mažiau nei 20 % prašytų duomenų apie asmenį). Tuo tarpu internete rasta informacija 97 % anketų viršijo 20 % reikalautų nurodyti žinių lygį.

Vertinant pradinės informacijos apie asmenį kiekio įtaką internete randamiems duomenims, pastebėta, kad, gausėjant pradinių žinių kiekiui, padaugėja internete rastos *teisingos informacijos* ir mažėja internete randamos *klaidingos informacijos* kiekiai. Ši priklausomybė gali būti paaiškinta tuo, kad pakankamai pradinės informacijos turintys asmenys geba identifikuoti netikslius faktus internete ir jų net nemini anketoje, o turimos bazinės žinios leidžia vykdyti platesnę informacijos paiešką internete. Tuo tarpu pradinių žinių apie ieškomą asmenį neturintys respondentai, radę kelis asmenis vienodais vardais ir pavarde, nėra tikri, kurie duomenys yra teisingi, o kurie ne.



2 pav. Tyrimo anketose pateiktų teisingų duomenų apie nurodytą asmenį dažnių pasiskirstymas tarp internete rastos informacijos ir jau turimų žinių apie tą asmenį



3 pav. Klaidingos ir teisingos informacijos priklausomybė nuo žinių apie asmenį pirminio lygio

Lyginant žinomus ir rastus asmeninių duomenų kiekius apie Lietuvos ir Lietuvoje pagal Erasmus programą studijuojančius užsienio studentus, nepastebėta didelių pokyčių. Galima tvirtinti, kad panašaus amžiaus ir užsiėmimo asmenys pasižymi panašiu požiūriu į savo asmeninės informacijos viešinimą internete. Kadangi tyrime dalyvavo palyginti mažai Erasmus studentų ir nebuvo analizuojamos kitos socialinės grupės, šis teiginys nėra patikimas.

Išvados

1. Atliktas asmeninių pėdsakų palikimo masto internete tyrimas patvirtina bendruosius informacijos viešinimo aspektus, kurie atsispindi straipsnyje analizuotų kitų tyrimų rezultatuose ir atskleidžia naujų tendencijų.
2. Tyrimo rezultatai parodė, kad žinomos informacijos kiekis turi labai didelės įtakos teisingos asmeninės informacijos paieškos rezultatams internete. Bent dalies informacijos žinojimas lemia internete randamos informacijos gylį ir plotį. Tai leidžia surinkti daugiau asmeninių pėdsakų apie tiriamąjį asmenį internete ir panaudoti ją prieš jį patį ar jo vykdomas veiklas.
3. Naudojantis paieškos sistemos galimybėmis, internete galima rasti pakankamai jautrių asmeniui duomenų ir pakenkti jo privatumui. Nekontroliuojamas duomenų viešinimas gali kelti grėsmę asmens privatumui ir saugumui, t. y. asmenys, naršydami internete, palieka daug informacijos apie save ir savo aplinką, neįvertindami tų asmeninių pėdsakų panaudojimo prieš juos pačius ar jų aplinką pasekmių.
4. Nepakanka informacijos apie saugų naršymą ir privatumo užtikrinimo technologijas.

Literatūra

1. Felt A., Evans D., 2008, *Privacy Protection for Social Networking APIs*. University of Virginia.
2. Young A. L., Quan-Haase A., 2009, Information Revelation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook. *Proceedings of the fourth international conference on Communities and technologies*. P. 265–273.
3. ECAR Research Study, 2008. Social Networking Sites. *Students and Information Technology*. P. 81–98.
4. Jones H., Soltren J. H., 2005, *Facebook: Threats to Privacy*.
5. Parris I., Abdesslen F. B., Henderson T., 2010, Facebook or Fakebook?: The effect of simulation on location privacy user studies. *Proceedings of Privacy and Usability Methods Pow-Wow.* Dundie. UK. P. 1–2.
6. McDowell M., Morda D., 2011, Social Securely: Using Social Networking Services. *United States Computer Emergency Readiness Team.* P. 1–5.
7. Goettke R., Christiana J., 2007, Privacy and Online Social Networking Websites. Computer Science 199r: *Special Topics in Computer Science Computation and Society: Privacy and Technology.* P. 1–12.
8. Gross R., Acquisti A., 2005, *Information Relevation and Privacy in Online Social Networks (The Facebook case)*. ACM Workshop on Privacy in the Electronic Society (WPES),.
9. Garfinkel S., Cox D., 2009, Finding and Archiving the Internet Footprint. *Personal Digital Archives for the 21st Century*.
10. Tuunainen V. K., Pitkanen O., Hovi M., 2009, Users' Awareness of Privacy on Online Social Networking Sites – Case Facebook. *22 Bled eConference eEnablement: Facilitating an Open, Effective and Representative eSociety.* P. 1–16.

ASPECTS OF EXTENT OF FOOTPRINTS MAKING ON THE INTERNET

Asta Slotkienė, Simona Ramanauskaitė

Summary

The rapid development of and accessibility to information and communication technology fuels the application of online services. Active personal online activity when a person is a participant at social sites and forums, a writer of articles, or an e-mail user affects the amount of personal data (footprints) made available online. These data can be used for malicious purposes (identity theft, social engineering, etc.) that must be taken into account before publishing data online. The article examines the extent of personal footprints making on the internet and the influence of that on a person's privacy vulnerability.

Keywords: internet, search for information, digital footprints, confidential information, vulnerability.

SKAITMENINIŲ PĖDSAKŲ PALIKIMO MASTO INTERNETE ASPEKTAI

Asta Slotkienė, Simona Ramanauskaitė

Santrauka

Sparti informacinių ir telekomunikacinių technologijų plėtra ir prieinamumas skatina interneto paslaugų vystymąsi. Aktyvus asmens, kaip socialinių tinklapių ir forumų dalyvio, straipsnių autoriaus, elektroninio pašto vartotojo, dalyvavimas internete, lemia asmeninės informacijos (pėdsakų) palikimą internete, neįvertinant duomenų paviešinimo aspektų. Straipsnyje nagrinėjami ir tiriami asmeninių pėdsakų palikimo mastai internete ir pasekmės asmens privatumo pažeidžiamumui.

Prasminiai žodžiai: internetas, informacijos paieška, skaitmeniniai pėdsakai, konfidenciali informacija, pažeidžiamumas.

Įteikta 2011-11-19