



VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

FUNDAMENTINIŲ MOKSLŲ FAKULTETAS

INFORMACINIŲ SISTEMŲ KATEDRA

Vaidas Ruškys

ĮVESTIES DUOMENŲ ANALIZĖ TAPATYBĖS VAGYSČIŲ PREVENCIJAI

KEYSTROKE ANALYSIS FOR IDENTITY THEFT PREVENTION

Baigiamasis magistro darbas

Inžinerinė informatika, valstybinis kodas 62409P111

Informacinės sistemos

Informatikos inžinerija

Vilnius, 2010

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS
FUNDAMENTINIŲ MOKSLŲ FAKULTETAS
INFORMACINIŲ SISTEMŲ KATEDRA

TVIRTINU
Katedros vedėjas

(Parašas)

Dalius Mažeika

(Vardas, pavardė)

(Data)

Vaidas Ruškys

ĮVESTIES DUOMENŲ ANALIZĖ TAPATYBĖS VAGYSČIŲ PREVENCIJAI

KEYSTROKE ANALYSIS FOR IDENTITY THEFT PREVENTION

Baigiamasis magistro darbas

Inžinerinė informatika, valstybinis kodas 62409P111

Informacinės sistemos

Informatikos inžinerija

Vadovas Prof. habil. dr. Antanas Čenys

(Moksl. laipsnis, vardas, pavardė)

(Parašas)

(Data)

Konsultantas doc. dr. Angelė Kaulakienė

(Moksl. laipsnis, vardas, pavardė)

(Parašas)

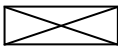
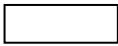
(Data)

Vilnius, 2010

Vilniaus Gedimino Technikos Universitetas
Fundamentinių mokslų fakultetas
Informacinių sistemų katedra

ISBN ISSN
Egz. sk.
Data

Magistro studijų baigiamasis darbas
Įvesties duomenų analizė tapatybės vagysčių prevencijai
Autorius: Vaidas Ruškys

Kalba
 lietuvių
 anglų

Anotacija

Šiame darbe aptariamos vartotojų internete tykančios grėsmės, susijusios su tapatybės vagystėmis. Aptariamos slaptažodžių žvejybos bei MITM atakos ir jų veikimo principai.

Problemos sprendimui siūloma naudoti vieną iš biometrijos dalių - klavišų paspaudimo analizę.

Pagrindinis darbo tikslas - atlikus tyrimą nustatyti, ar galima naudojant klavišų paspaudimo analizės metodą sėkmingai sumažinti tapatybės vagystės tikimybę.

Pateikiami tyrimo rezultatai naudojant skirtingai veikiančias programas, naudojančias klavišų paspaudimo analizės metodą. Analizuojama, kaip klavišų paspaudimo analizės panaudojimo galimybė kinta keičiant tam tikras analizės sudedamąsias dalis.

Reikšminiai žodžiai: biometrija, klavišų paspaudimo analizė, MITM, slaptažodžių žvejyba, tapatybės vagystės

Vilnius Gediminas Technical University Faculty of Fundamental Sciences Information system department		ISBN	ISSN
		Num.	
		Date	

The final project of Master's studies
Keystroke analysis for identity theft prevention
Author: Vaidas Ruškys

Language	
☐	Lithuanian
☒	English

Annotation

This paper analyzes vulnerabilities that internet users face on the internet, which are related to identity theft. Phishing and MITM attacks and their principals are described.

For solving this problem is suggested one part of biometrics-Keystroke analysis.

Goal of this paper is to analyze possibility to reduce probability of these attacks by using Keystroke analysis.

The results of using different types of programs using Keystroke analysis are presented. Analysis off how possibility of usability to use Keystroke analysis differs by changing different parts of Keystroke analysis.

Keywords: identity theft, biometrics, Keystroke analysis, MITM, phishing

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS
FUNDAMENTINIŲ MOKSLŲ FAKULTETAS
INFORMACINIŲ SISTEMŲ KATEDRA

Inžinerinės informatikos studijų kryptis

Inžinerinės informatikos studijų programa, valstybinis kodas 62409P111

Informacinių sistemų specializacija

TVIRTINU

Katedros vedėjas

(Parašas)

Dalius Mažeika

(Data)

**BAIGIAMOJO MAGISTRO DARBO
UŽDUOTIS**

.....Nr.

Vilnius

Studentui Vaidui Ruškiui

Baigiamojo darbo tema: Įvesties duomenų analizė tapatybės vagysčių prevencijai

patvirtinta 2009 m. d. dekanų potvarkiu Nr.

Baigiamojo darbo užbaigimo terminas 201...m. d.

BAIGIAMOJO DARBO UŽDUOTIS:

Išanalizuoti internetines atakas, skirtas tapatybės vagysčių įgyvendinimui.

Apžvelgti kokios šiuo metu yra naudojamos saugos priemonės.

Ištirti klavišų paspaudimo analizės galimybes padidinti sistemos saugos lygį.

Ištirti kokia klavišų paspaudimo analizės sistemos konfigūracija yra tinkamiausia naudojimui.

Vadovas
(Parašas)

Prof. habil. dr. Antanas Čenys

Užduotį gavau

.....
(Parašas)

.....
(Vardas, pavardė)

.....
(Data)

Turinys

1. Įvadas.....	12
2. Nuostoliai dėl internetinių sukčiavimų.....	13
3. Slaptažodžių žvejybos atakos	14
3.1 Sukompromituoti domenai prieš kenkimo domenų registracijas	14
3.2 Internacionalizuotų domenų (angl. IDN) naudojimas	15
3.3 Subdomenų naudojimas slaptažodžių žvejybos atakose	16
3.4 Tikslioji slaptažodžių žvejybos ataka.....	16
4. Slaptažodžių žvejybos atakų statistika	17
4.1 Slaptažodžių žvejybos atakų puslapių veikimo laikas	18
4.2 Slaptažodžių žvejybos atakos Lietuvoje.....	20
4.3 Tikrieji nuostoliai, patiriami dėl slaptažodžių žvejybos atakų	20
5. MITM ataka.....	21
6. Klientų apsaugos priemonės.....	23
6.1 PIN kodų kortelės	23
6.2 SMS arba elektroninio laiško patvirtinimas	23
6.3 Paveikslo įkėlimas	24
6.4 Virtualioji klaviatūra	25
6.5 Specializuotos saugos įrankių juostos	26
6.6 Vartotojų budrumo skatinimas	27
7. Biometrinės sistemos.....	29
7.1 Biometrinės sistemos sėkmes faktoriai	29
7.1.1 Tikslumas	30
7.1.2 Greitis	30
7.1.3 Atsparumas apgaulei	30
7.1.4 Patikimumas	30
7.1.5 Duomenų saugyklos reikalavimai	31
7.1.6 Naujo vartotojo įvesties laikas	31
7.1.7 Jaučiamas nepasitikėjimas.....	31

8 Klavišų paspaudimo analizė.....	32
8.1 Naudojamos Metrikos	32
8.2 Klavišu paspaudimo analizės tinkamumas pagal biometrinių sistemų reikalavimus.....	33
8.2.1 Tikslumas	33
8.2.2 Greitis	33
8.2.3 Atsparumas apgaulėi	33
8.2.4 Patikimumas	33
8.2.5 Duomenų saugyklos reikalavimai	33
8.2.6 Naujo vartotojo įvesties laikas	33
8.2.7 Jaučiamas nepasitikėjimas.....	34
8.3 Klavišų paspaudimo analizės sistemos variacijos	34
9. Klavišų paspaudimo analizės efektyvumo tyrimas	35
9.1 Programos veikimas	35
9.1.1 Vartotojo įvestis	35
9.1.2 Vartotojo prisijungimas	35
9.1.3 Duomenų išvedimas	36
9.1.4 Duomenų bazės struktūra	39
9.2 Variacijos.....	40
9.2.1 Vienkartinės įvesties fiksuoto ilgio variacijos:	40
9.2.2 Vienkartinės įvesties laisvai pasirenkamos eilutės variacijos:	40
9.2.3 Daugkartinės įvesties fiksuoto ilgio variacijos:.....	41
9.2.4 Daugkartinės įvesties laisvai pasirenkamos eilutės variacijos:	42
10. Rezultatai.....	43
11. Išvados.....	58
12. Literatūros sąrašas	59

Paveikslų sąrašas

1 pav. Identifikuotų slaptažodžių žvejybos atakų atvejų skaičius 2009 m. vasario mėn.	17
2 pav. Nuostoliai, susiję su slaptažodžių žvejybos atakomis	20
3 pav. MITM atakos veikimo schema	21
4 pav. PIN kodų kortelės pavyzdys	23
5 pav. Prisijungimo formos, naudojant paveiklo įkėlimą, pavyzdys	24
6 pav. Virtualiosios klaviatūros pavyzdys.....	25
7 pav. Specializuotų saugumo įrankių juostų pavyzdžiai	26
8 pav. Specializuotų saugumo įrankių juostų, skirtų konkrečioms svetainėms, pavyzdžiai	27
9 pav. Pagrindiniai metodai, leidžiantys aptikti slaptažodžių žvejybos atakų įvykdymo bandymus.....	28
10 pav. Klavišų paspaudimo analizės naudojamos metrikos	32
11 pav. Tyrime naudota prisijungimo forma.....	35
12 pav. Tyrime naudota vartotojo prisijungimo forma	36
13 pav. Tyrime naudota vartotojo prisijungimo forma su gautų rezultatų pavyzdžiu	36
14 pav. Tikrųjų vartotojų prisijungimo rezultatų išvedimo pavyzdys.....	37
15 pav. Apsimetėlių prisijungimo rezultatų išvedimo pavyzdys	38
16 pav. Duomenų bazės struktūra	39
17 pav. Rezultatų pasiskirstymas naudojant 7 simbolių iš anksto parinktą eilutę, vartotojo registracijos metu, eilutę įvedant 1 kartą	43
18 pav. Rezultatų pasiskirstymas naudojant 11 simbolių iš anksto parinktą eilutę, vartotojo registracijos metu, eilutę įvedant 1 kartą	44
19 pav. Rezultatų pasiskirstymas naudojant 15 simbolių iš anksto parinktą eilutę, vartotojo registracijos metu, eilutę įvedant 1 kartą	44
20 pav. Rezultatų pasiskirstymas naudojant 5-8 simbolių laisvai pasirenkamą eilutę, vartotojo registracijos metu, eilutę įvedant 1 kartą.....	45
21 pav. Rezultatų pasiskirstymas naudojant 8-11 simbolių laisvai pasirenkamą eilutę, vartotojo registracijos metu, eilutę įvedant 1 kartą.....	45
22 pav. Rezultatų pasiskirstymas naudojant 11-15 simbolių laisvai pasirenkamą eilutę, vartotojo registracijos metu, eilutę įvedant 1 kartą.....	46
23 pav. Rezultatų pasiskirstymas naudojant 7 simbolių iš anksto parinktą eilutę, vartotojo registracijos metu, eilutę įvedant 3 kartus.....	46

24 pav. Rezultatų pasiskirstymas naudojant 11 simbolių parinktą eilutę, vartotojo registracijos metu, eilutę įvedant 3 kartus.....	47
25 pav. Rezultatų pasiskirstymas naudojant 15 simbolių iš anksto parinktą eilutę, vartotojo registracijos metu, eilutę įvedant 3 kartus.....	47
26 pav. Rezultatų pasiskirstymas naudojant 7 simbolių iš anksto parinktą eilutę, vartotojo registracijos metu, eilutę įvedant 5 kartus.....	48
27 pav. Rezultatų pasiskirstymas naudojant 11 simbolių iš anksto parinktą eilutę, vartotojo registracijos metu, eilutę įvedant 5 kartus.....	48
28 pav. Rezultatų pasiskirstymas naudojant 15 simbolių iš anksto parinktą eilutę, vartotojo registracijos metu, eilutę įvedant 5 kartus.....	49
29 pav. Rezultatų pasiskirstymas naudojant 5-8 simbolių laisvai pasirenkamą eilutę, vartotojo registracijos metu, eilutę įvedant 5 kartus	49
30 pav. Rezultatų pasiskirstymas naudojant 5-8 simbolių laisvai pasirenkamą eilutę, vartotojo registracijos metu, eilutę įvedant 5 kartus	50
31 pav. Rezultatų pasiskirstymas naudojant 11-15 simbolių laisvai pasirenkamą eilutę, vartotojo registracijos metu, eilutę įvedant 3 kartus	50
32 pav. Rezultatų pasiskirstymas naudojant 5-8 simbolių laisvai pasirenkamą eilutę, vartotojo registracijos metu, eilutę įvedant 5 kartus	51
33 pav. Rezultatų pasiskirstymas naudojant 8-11 simbolių laisvai pasirenkamą eilutę, vartotojo registracijos metu, eilutę įvedant 5 kartus	51
34 pav. Rezultatų pasiskirstymas naudojant 11-15 simbolių laisvai pasirenkamą eilutę, vartotojo registracijos metu, eilutę įvedant 5 kartus	52

Lentelių sąrašas

1 lentelė. Slaptažodžių žvejybos atakų statistika.....	18
2 lentelė. Slaptažodžių žvejybos atakų svetainių veikimo laikas 2008 m. antrajame pusmetyje.....	19
3 lentelė. Slaptažodžių žvejybos atakų svetainių veikimo laikas 2008 m. pirmajame pusmetyje	19
4 lentelė. Rezultatų palyginimas tiriant skirtumus tarp vartotojų pasirinktų eilučių ir iš anksto parinktų eilučių, registracijos metu eilutę įvedant vieną kartą	53
5 lentelė. Rezultatų palyginimas tiriant skirtumus tarp vartotojų pasirinktų eilučių ir iš anksto parinktų eilučių, registracijos metu eilutę įvedant tris kartus	53
6 lentelė. Rezultatų palyginimas tiriant skirtumus tarp vartotojų pasirinktų eilučių ir iš anksto parinktų eilučių, registracijos metu eilutę įvedant penkis kartus.....	53
7 lentelė. Rezultatų palyginimas registracijos metu eilutę vedant 1, 3 ir 5 kartus, rezultatai pateikti naudojant iš anksto parinktas eilutes	54
8 lentelė. Rezultatų palyginimas registracijos metu eilutę vedant 1, 3 ir 5 kartus, rezultatai pateikti naudojant vartotojų laisvai pasirinktas eilutes.....	54
9 lentelė. Rezultatų palyginimas naudojant skirtingo ilgio, iš anksto parinktas eilutes	55
10 lentelė. Rezultatų palyginimas naudojant skirtingo ilgio vartotojų laisvai pasirinktas eilutes	56

Santrumpų sąrašas

ASCII - American Standard Code for Information Interchange, Amerikietiškas informacijos mainų koduotės standartas

DNR - Deoksiribonukleorūgštis- nukleorūgštis, esanti kiekvienoje gyvoje ląstelėje, daugiausia jos branduolyje. Joje (jos azotinių bazių sekoje) yra tripletiniu kodu užkoduota genetinė informacija, kuri perduodama dalijimosi metu naujoms ląstelėms, o per lytines ląsteles – individo palikuonims

FAR - False accept rate, biometrijoje vartojama sąvoka, reiškianti skaičių žmonių, kurie yra klaidingai atpažįstami kaip kiti asmenys

FRR - False reject rate, biometrijoje vartojama sąvoka, reiškianti skaičių žmonių, kurie yra klaidingai neatpažįstami

IDN - Internationalized domain name, internacionalizuoti domenų vardai – domenai, kuriose yra vienas ar daugiau ne ASCII koduotės simbolių

MITM –Man in the middle, komunikacijos ataka, kurios metu atakuotojas perima ir savo nuožiūra modifikuoja duomenis, kurie yra siunčiami, siekdamas apsimesti vienu arba keletu komunikacijoje dalyvaujančių šalių

PIN- Personal identification number, asmeninis identifikacijos numeris - slaptažodis, kuris sudarytas iš skaičių, žinomų tik vartotojui ir sistemai, kurie gali būti panaudoti vartotojo tapatumui nustatyti

SQL- Structured Query Language, struktūrizuota užklausų kalba, populiariausia iš šiuo metu vartojamų kalbų, skirtų duomenims aprašyti ir manipuliuoti jais sąryšinių duomenų bazių valdymo sistemose

SMS- Short Message Service, trumpųjų žinučių paslauga, t.y. komunikacijos paslauga, naudojanti standartizuotus komunikavimo protokolus, leidžianti mobiliesiems telefonams keistis trumpomis žinutėmis

SSL - Secure Sockets Layer, kriptografinis protokolas, skirtas informacijai, sklindančiai internete, apsaugoti šifruojant

TLD - A top-level domain –aukščiausio lygmens domenas, užimantis aukščiausią hierarchinę padėtį domenų vardų sistemoje (angl. Domain Name System(DNS))

TLS - Transport Layer Security, transportavimo sluoksnio sauga - SSL protokolo pirmtakas, skirtas informacijai, sklindančiai internete, apsaugoti šifruojant

URL – Uniform resource locator, adresai, naudojami interneto svetainėse. Nurodo adresą, kuris yra naudojamas kreipiantis į šaltinį

1. Įvadas

Augant interneto skverbčiai į kasdieninį gyvenimą, didėjant elektroninėmis paslaugomis besinaudojančių žmonių skaičiui, daugėja ir asmeninių duomenų, tapatybės praradimo atvejų. Pasak Lietuvos statistikos departamento, žmonių naudojusią elektroninės prekybos paslaugas 2009 m. išaugo 2,6%[1]. Tapatybės vagysčių skaičius JAV 2009 m. išaugo 11%, palyginti su 2008 m.[4]. Problema aktuali ne tik bankams, bet ir kiekvienai elektroninius atsiskaitymus naudojančiai įmonei.

Darbo tikslai ir uždaviniai

Darbo tikslas yra išanalizuoti pagrindines internete vartotojų laukiančias grėsmes. Apžvelgti, kokios priemonės jau yra naudojamos ir kokie jų privalumai bei trūkumai.

Išanalizuoti ir ištirti vienos iš biometrijos sričių, klavišų paspaudimo analizės, galimybes apsaugoti vartotojus nuo tapatybės vagystės ar bent jau sumažinti šią grėsmę. Klavišų paspaudimo analizės metu konkretus sistemos veikimo modelis gali būti labai įvairus, gali būti naudojamos skirtingo ilgio eilutės, eilutės gali būti iš anksto parinktos arba sugalvojamos pačių vartotojų, vartotojo registracijos metu eilutė gali būti įvedama vieną kartą arba daugiau nei vieną. Nuo šių skirtingų pasirinkčių sistemos veiksmingumas ir panaudojimo galimybės gali keistis, todėl pagrindinis uždavinys yra ištirti klavišų paspaudimo analizės metodo panaudojimo galimybes realioje sistemoje, klavišų paspaudimo analizės efektyvumą, esant įvairioms pasirenkamų dalių kombinacijoms.

Darbo metodai

Darbe buvo naudoti šie metodai: aprašomasis ir lyginamasis.

Darbe aprašomos slaptažodžių žvejybos bei MITM atakos. Aprašomos priemonės naudojamos siekiant sumažinti atakų įvykdymo galimybes.

Analizuojant gautus rezultatus, lyginamos dvi kreivės: tikrųjų vartotojų bei apsimetėlių. Taip pat lyginami ir aptariami rezultatai, kurie gauti naudojant skirtingas programos kintamųjų dalių variacijas.

Praktinė darbo vertė

Darbe tiriama, kokios yra galimybės panaudoti klavišų paspaudimo analizę internetinėse sistemose. Tiriama, kaip kinta klavišų analizės efektyvumas, keičiant programos sudedamąsias dalis. Nustatoma, kokios programos keičiamų dalių variacijos yra tinkamiausios praktiniam panaudojimui.

2. Nuostoliai dėl internetinių sukčiavimų

Įvykus tapatybės vagystei ir klientui dėl to patyrus finansiniu nuostolių, nukenčia ne tik jis bet ir finansinė institucija, kurios paslauga buvo naudojama, galimi ne tik tiesioginiai finansiniai nuostoliai, bet ir keliama grėsmė elektroninių paslaugų patikimumui . Pagal [10], 2009 m. internete įvykdytų nusikaltimų žala siekė 560 mln. JAV dolerių (1,4 mlrd. Lt), ankstesniais metais ši suma siekė 265 mln. JAV dolerių. Nuostoliai dėl sukčiavimo elektroninėje erdvėje didėja, vis daugiau kenksmingo programinio kodo yra kuriama siekiant finansinės naudos. Skundų nusikaltimais internete centras (The Internet Crime Complaint Center) Amerikoje pernai sulaukė 22% daugiau pranešimų apie sukčiavimą internete [10].

Dėl patiriamų nuostolių bankai ar kitos finansinės institucijos, teikiančios paslaugas, susijusias su internetinėms pinigų transakcijoms, yra suinteresuotos kaip galima geriau apsaugoti vartotoją.

Panagrinėkime, kokios konkrečiai grėsmės laukia vartotojų internete.

3. Slaptažodžių žvejybos atakos

Viena iš didžiausių grėsmių, tykančių vartotojų internete, yra phishing, kurią galime vadinti slaptažodžių žvejybos ataka. Slaptažodžių žvejybos ataka tai bandymas iš vartotojų apgaulės būdu išgauti elektroninės komercijos prisijungimo vardus bei slaptažodžius. Dažniausiai ji būna nukreipta prieš didelį skaičių žmonių, tikintis kad bent iš dalies jų pavyks perimti svarbius duomenis.

Slaptažodžių žvejybos atakos schema yra gana paprasta, bet kaip rodo praktika, gana veiksminga. Dideliam skaičiui žmonių yra išsiuntinėjami elektroniniai laiškai, apsimetant banko atstovais, naudojant panašų į banko elektroninį paštą, logotipus ir t.t. Laiške yra įdedama nuoroda, kuri veda į sukčių sukurtą internetinį puslapį, kuris yra padarytas kaip galima panašesnis į tikrąjį banko puslapį, taip siekiant įtikinti, kad puslapis yra tikrasis banko puslapis. Puslapyje įvesti prisijungimo duomenys patenka į sukčių rankas ir jie gali jais pasinaudoti atlikdami bankines operacijas su aukos pinigais.

Panagrinėkime konkrečiau, kokius metodus ir priemones naudoja kenkėjai, siekdami išvilioti iš vartotojų prisijungimo vardus bei slaptažodžius.

3.1 Sukompromituoti domenai prieš kenkimo domenų registracijas

Ne visada slaptažodžių žvejybos atakai naudojamas domenas yra užregistruotas kenkėjo, kartais naudojami nekenkimo domenai, į kuriuos neteisėtai įsibraunama. Skirtingi metodai yra svarbūs imantis priemonių sumažinti atakos pasekmes.

AntiPhishing Work Group atliko tyrimą[14:9], kai puslapis buvo priskiriamas prie kenkimo domenų registravimų, jei domenas buvo užregistruotas labai trumpą laiką arba/ir domene buvo atakuojamas vardas, arba domenas buvo, kai užregistruota keletą panašių domenų vienu metu. Kai kuriuos kenkimo domenus buvo sunku priskirti vienai ar kitai grupei, todėl jie nebuvo priskirti nė vienai iš jų.

Iš 30131 slaptažodžių žvejybos atakos domenų 4382 domenai buvo identifikuoti kaip kenkėjų užregistruoti domenai. Tai sudarė 14,5% visų slaptažodžių žvejybos atakos domenų. 86% visų šių kenkėjų užregistruotų domenų buvo užregistruoti tik 5-iuose aukščiausio lygio domenuose: .COM, .EU, .NET, .BE, .ORG.

Likę 85,5% domenai, naudoti slaptažodžių žvejybos atakose, buvo domenai, kurie yra užregistruoti ne kenkėjų. Dažniausiai puslapis yra dedamas į serverį nežinant serverio administratoriams. Tokiu būdu kenkėjas ne tik gauna nemokamą svetainės talpinimo paslaugą, bet ir

žymiai apsunkina kenkimo svetainės panaikinimą, kadangi tiesiog domeno panaikinimas panaikina ir teisėtai veikiančią svetainę. Kenkimo svetainė šiuo atveju naudoja arba teisėto domeno subdomeną arba subkatalogą.

3.2 Internacionalizuotų domenų (angl. IDN) naudojimas

Vis labiau didėjant susidomėjimui internacionalizuotais domenais, didėja ir noras sužinoti kaip internacionalizuoti domenai gali būti panaudoti slaptažodžių žvejybos atakose. IDN charakteristikos nėra palankios kenkimo puslapių skaičiaus mažinimui.

IDN yra domenai, kuriuose yra vienas ar daugiau ne ASCII koduotės simbolių[14:16]. Tokie domenai gali turėti simbolių, kurie nėra lotyniški, pvz., arabiški, kiniški, kirilicos ir t.t.

Kenkėjai gali pasinaudoti tuo, kad tam tikri simboliai yra vizualiai panašūs arba netgi neatskiriami, nors jų koduotė yra skirtinga. Pavyzdžiu gali būti domenas, kuris adreso juostoje atrodo taip:

<http://www.paypal.com/>

Tačiau pirmoji raidė “a” yra pakeista taip pat atrodančia “a” raidė iš kirilicos. Vizualiai neįmanoma pastebėti skirtumo, tačiau techniniu atžvilgiu tai visiškai skirtingas domenas.

Nuo 2007 m. sausio mėn. 1d. iki 2009 m. birželio mėn. 30 d. buvo užregistruota tik 85 atvejai, kai slaptažodžių žvejybos atakom buvo naudojami internacionalizuoti domenai[14:16]. Didžioji dalis buvo kiniškų ir lotyniškų simbolių mišinys.

Dar vienas pavyzdys buvo užfiksuotas 2009 m. sausio mėn. 16 d.[14:16] Užregistruotas domenas buvo:

xn--hotmal-t9a.net

Naršyklėje toks adresas buvo rodomas:

hotmail.net

Tačiau i raidė buvo apgaulinga, paimta iš kitos koduotės.

Turint galvoje, kad IDN adresai yra prieinami jau ne vienerius metus, kyla klausimas, kodėl atakų skaičius naudojant tokio tipo slaptažodžių žvejybos adresus kol kas dar nėra grėsmingai išaugęs?

1. Kenkėjams nėra būtina naudoti tokius adresus, kaip rodo tyrimai, atakuotojams pats adresas nėra labai svarbus[14:16], atakos ir taip pasiekia rezultatą, kurio tikimasi.
2. Kai kurios naršyklės rodo ne perverstą adresą, o užkoduotą (pvz. xn--hotmal-t9a.net)

3.3 Subdomenų naudojimas slaptažodžių žvejybos atakose

Subdomenai yra labai plačiai naudojami slaptažodžių žvejybos atakose. 2009 m. pirmojoje pusėje 6441 slaptažodžių žvejybos atakos puslapiai buvo užregistruoti naudojant subdomenus. Tuo tarpu įprastiniu būdu užregistruotų kenkimo puslapių buvo 4382 [14:17]. Tai gana neįprasta tendencija, turint galvoje, kad tokių puslapių skaičių galėtų sumažinti subdomenų registravimo paslaugas teikiantys registratoriai. Deja, dalis iš tų registratorių nekovoja su šia grėsme arba kovoja neefektyviai.

Subdomenų registravimo paslauga yra tokia, kai registruojama su paslaugos tiekėjo domenu.

Pvz.:<vartotojo vardas>.<paslaugos_tiekėjo domenas>.TLD

Taip pat pastebimas vis dažnesnis naudojimas paslaugos, leidžiančios sutrumpinti URL adresą. Naudojant šią paslaugą įvedamas sutrumpintas URL adresas ir vartotojas yra nukreipimas į ilgesnį adresą. Naudojant tokią priemonę vartotoją lengviau suklaidinti.

3.4 Tikslioji slaptažodžių žvejybos ataka

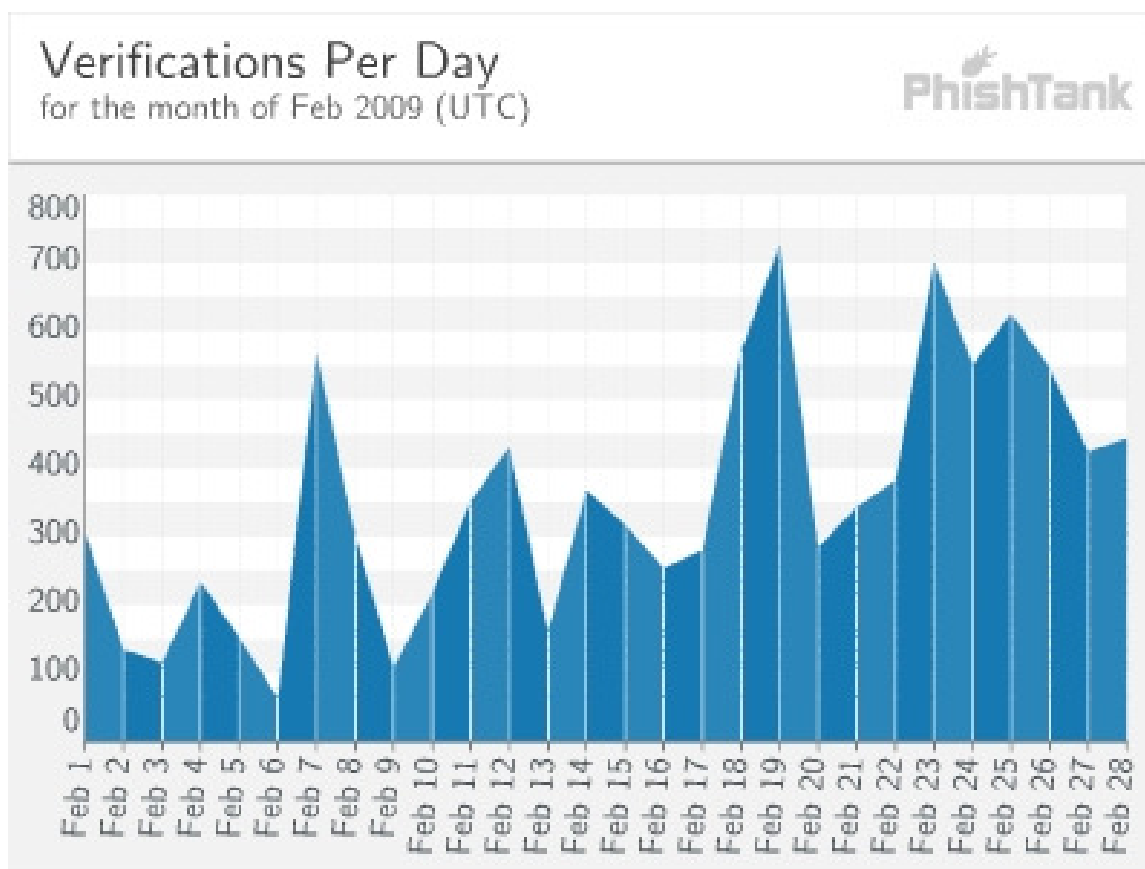
Tikslioji slaptažodžių žvejybos ataka (angl. Spear phishing) yra slaptažodžių žvejybos atakų ir socialinės inžinerijos kombinacija, nukreipta prieš vieną asmenį arba nedidelę žmonių grupę [20:6]. Tokia ataka yra labai koncentruota siekiant padidinti atakos efektyvumą.

Atakuotojai naudoja asmeninę arba viešą informaciją, kuri yra žinoma apie aukas. Tokiu būdu siunčiami elektroniniai laiškai, kurie sudaro įspūdį, jog yra atsiųsti iš patikimų šaltinių. Taip yra sumažinamas aukos budrumas ir nepasitikėjimas. Atakuotojams įgijus aukos pasitikėjimą yra daug paprasčiau išvilioti asmeninę informaciją, tokią kaip prisijungimo vardai bei slaptažodžiai.

Kaip pavyzdį galima pateikti tokį scenarijų: kontaktinė informacija apie Vardenį Pavardenį yra paskelbiama spaudoje arba kitoje viešoje erdvėje. Kenkėjai siunčia elektroninį laišką Vardeniui Pavardeniui, kuris atrodo kaip oficialus laiškas, siųstas iš patikimo elektroninės komercijos tiekėjo. Laiške siūloma aktyvuoti nemokamą paskyrą. Spausdamas nuorodą, pateiktą laiške, vartotojas suteikia galimybę į jo kompiuterį įdiegti kenkimo programą arba perimti jo prisijungimo vardus bei slaptažodžius, kurie tikėtina, jog sutaps su jo naudojamo banko prisijungimo vardais bei slaptažodžiais.

3. Slaptažodžių žvejybos atakų statistika

Kalbant apie slaptažodžių žvejybos atakos grėsmę būtina įvertinti jos mastus bei augimo tempus, kokius nuostolius patiria vartotojai bei elektroninės bankininkystės paslaugas teikiančios įmonės. www.phishtank.com [19] duomenimis, 2009 m. vasario mėn. buvo aptikta 8695 apgaulingų puslapių, bandančių perimti prisijungimo duomenis.



1 pav. Identifikuotų slaptažodžių žvejybos atakų atvejų skaičius 2009 m. vasario mėn.

Tokiu būdu perėmę duomenis internetiniai vagys arba juos panaudoja ištuštinami sąskaitas, arba tuos duomenis parduoda kitiems.

Per 2007 m. buvo gauta apie 800 tūkstančių nusiskundimų dėl tapatybės vagystės ir 23% iš jų buvo susiję su kreditinėmis kortelėmis[2]. Tačiau net 68% nusiskundimų buvo susiję su finansinėmis operacijomis. Remiantis tuo pačiu šaltiniu, per 2007 m. tokių apgaulių būdu interneto vartotojai neteko apie 3,2 milijardo dolerių.

Buvo apskaičiuota, kad vidutiniškai apgaulės metu vienas vartotojas netenka apie 900 dolerių. Nors šis rodiklis, palyginti su 2006 m., nukrito, 2006 m. jis buvo apie 1250 dolerių vienam vartotojui,

patekusiam į sukčių pinkles. Tačiau šio rodiklio sumažėjimas nedaug ką keičia, nes pačių išpuolių padaugėjo ir padaryta bendra finansinė žala tik padidėjo.

Slaptažodžių žvejybos atakų skaičiaus augimą galima matyti ir iš AntiPhishing Work Group ataskaitoje [14:5] pateiktų duomenų (1 lentelė).

1 lentelė. Slaptažodžių žvejybos atakų statistika

	2009 1-as pusmetis	2008 2-as pusmetis	2008 1-as pusmetis	2007 2-as pusmetis
Slaptažodžių žvejybos atakų svetainės	30131	30454	26678	28818
Slaptažodžių žvejybos atakos svetaines su unikaliais IP adresais	3563	2809	3389	5217
Aukščiausio lygio domenai (TLD) slaptažodžių žvejybos atakų svetainių adresuose	171	170	155	145
Atakų skaičius	55698	56969	47342	

4.1 Slaptažodžių žvejybos atakų puslapių veikimo laikas

Kalbant apie slaptažodžių žvejybos atakų keliamą grėsmę ir padaromą žalą būtina aptarti ir slaptažodžių žvejybos atakų puslapių veikimo laiką. Slaptažodžių žvejybos atakų puslapių veikimo laikas yra esminis matas, parodantis žalą, kurią daro šios atakos, taip pat šis matas parodo sėkmingą arba nesėkmingą bandymą sumažinti atakų skaičių. Kuo ilgiau veikia kenksmingas puslapis, tuo daugiau žalos jis padaro. Vidutiniais apskaičiavimais kiekviena valanda, kurią veikia slaptažodžių žvejybos atakos puslapis padaro 300\$ žalą[14:9]. Suprantama, kenkėjų tikslas, kad puslapis veiktų kaip galima ilgiau, todėl jie registruoja puslapius rinkdamiesi registratorius, kurie yra neatidūs arba netaiko jokių saugos priemonių.

Modernesni atakuotojai naudoja greitai kintančius(angl. Fast-flux) tinklus, taip siekdami padidinti puslapio gyvavimo trukmę[9:4]. (Puslapiai esantys greitai kintančiuose tinkluose gyvuoja maždaug du kartus ilgiau nei puslapiai esantys paprastuose tinkluose). Ilgai veikiantis vienas puslapis

gali labai iškreipti vidutinius tokių puslapių gyvavimo laikus, todėl vertinant atakų mastą naudojamas ir vidurkis ir mediana.

2008 m. antrajame pusmetyje vidutinis slaptažodžių žvejybos atakų puslapių gyvavimo laikas buvo 52 valandos, mediana 14 valandų ir 43 minučių.[15:11] 2008 m. pirmajame pusmetyje vidutinis slaptažodžių žvejybos atakų puslapių gyvavimo laikas buvo 49 valandos ir 30 minučių, mediana 19 valandų ir 29 minutės[13:10].

Taigi matoma, kad slaptažodžių žvejybos atakų svetainių gyvavimo laikas padidėjo net 2 valandomis ir 30 minučių.

2 lentelė. Slaptažodžių žvejybos atakų svetainių veikimo laikas 2008 m. antrajame pusmetyje[15:11]

	Vidurkis	Mediana
Liepa	53:32:30	16:17:24
Rugpjūtis	43:31:12	15:26:41
Rugsėjis	54:46:22	15:58:45
Spalis	49:11:03	14:14:54
Lapkritis	53:55:39	13:59:50
Gruodis	58:35:36	14:21:43
Visas pusmetis	52:01:58	14:43:15

3 lentelė. Slaptažodžių žvejybos atakų svetainių veikimo laikas 2008 m. pirmajame pusmetyje[13:10]

	Vidurkis	Mediana
Sausis	54:33:10	21:14:55
Vasaris	37:44:43	17:29:40
Kovas	38:45:45	14:34:03
Balandis	50:07:46	18:23:37
Gegužė	56:39:48	19:41:19
Birželis	53:55:46	22:39:09
Visas pusmetis	49:30:03	19:29:32

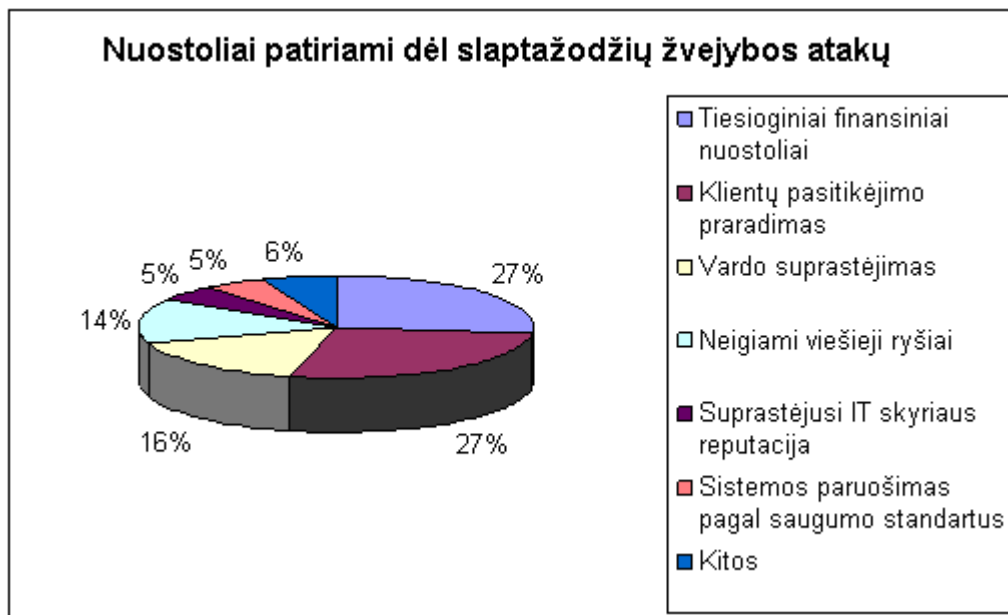
4.2 Slaptažodžių žvejybos atakos Lietuvoje

Slaptažodžių žvejybos atakų skaičius pasaulyje tendencingai auga, kartu auga ir slaptažodžių žvejybos atakų padaroma žala bei grėsmė. Dabar trumpai apžvelgsime, kokia situacija yra Lietuvoje.

Remiantis AntiPhishing Work Group pateiktais duomenimis, 2008 m. antrojoje pusėje Lietuvoje buvo užregistruota net 40 unikalių slaptažodžių žvejybos atakų. Jos buvo įgyvendintos užregistravus 25 unikalius domenų vardus, kurie buvo panaudoti šiose atakose[15:22]. Skaičiai nėra labai dideli, tačiau 2008 m. pirmojoje pusėje buvo užregistruota tik 24 unikalios slaptažodžių žvejybos atakos, kurios buvo įvykdytos užregistravus 18 unikalių domenų vardų[13:20]. Taigi matomas slaptažodžių žvejybos atakų skaičiaus augimas. Tuo pačiu laikotarpiu slaptažodžių žvejybos atakų puslapių gyvavimo laikas išaugo nuo 13 valandų ir 28 minučių[13:20] iki 19 valandų ir 30 minučių[15:22].

4.3 Tikrieji nuostoliai, patiriami dėl slaptažodžių žvejybos atakų

Kalbant apie slaptažodžių žvejybos atakų padaromus nuostolius, reikia pabrėžti, kad tiesioginiai finansiniai nuostoliai yra tik dalis. Taip pat nuostoliai yra ir tai, kad yra prarandamas vartotojų pasitikėjimas, nukenčia ir pats prekinis ženklas. Taigi vien tik rodikliai, parodantys, kokios tiksliai sumos buvo išviliotos iš finansinių sistemų vartotojų, dar neatspindi tikrosios finansinės žalos, padaromos įmonei. Remiantis [12], nuostoliai dėl slaptažodžių žvejybos atakų pasiskirsto taip kaip parodyta 2 paveiksle.



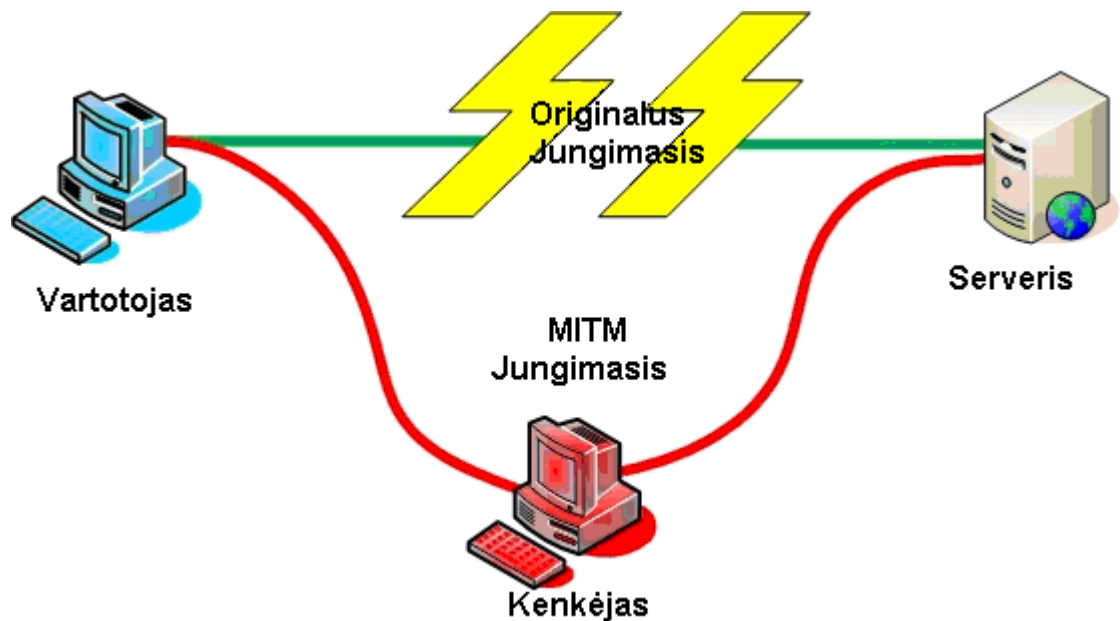
2 pav. Nuostoliai, susiję su slaptažodžių žvejybos atakomis

5. MITM ataka

Dar viena grėsmė, laukianti vartotojų internete, yra MITM (Man in a middle) ataka. Internetinio saugumo žodyne MITM ataka apibūdinama kaip komunikacijos ataka, kurios metu atakuotojas perima ir savo nuožiūra modifikuoja duomenis, kurie yra siunčiami, siekdamas apsimesti vienu arba keletu komunikacijoje dalyvaujančių šalių[17:105]. Ši ataka yra ne mažiau pavojinga nei prieš tai aptarta slaptažodžių žvejybos ataka.

Tipiškas atakos atvejis yra, kai kenkėjas įsiterpia tarp vartotojo ir serverio taip, kad galėtų vienu metu atskirai komunikuoti tiek su vartotoju, tiek su serveriu. Tokiu atveju, tiek vartotojas, tiek serveris nepastebi, kad jie komunikuoja per tarpininką. Kriptografija šiuo atveju neišsprendžia problemos, nes kenkėjas gali tiek užšifruoti, tiek iššifruoti duomenis, kurie yra siunčiami. Jei vartotojas nori prisijungti prie serverio, jis savo duomenis atskleidžia ir kenkėjui, kuris yra įsiterpęs tarp jo ir serverio. Tada kenkėjas gali duomenimis pasinaudoti neteisėtu būdu. Norint vartotojui nesukelti įtarimo, kenkimo programa vartotojui nusiunčia atsakymą iš serverio, tarsi jis būtų tiesiogiai prisijungęs prie serverio.

MITM atakos schema pavaizduota 3 paveiksle.



3 pav. MITM atakos veikimo schema[7]

Praktika rodo, kad dažniausiai įdiegti vartotojų tapatumo nustatymo mechanizmai nesugeba efektyviai apsaugoti nuo MITM atakų, net jei yra naudojami SSL/TLS protokolai.

Taip yra dėl dviejų priežasčių:

1. SSL/ TLS serverio tapatumo nustatymas dažnai yra padarytas prastai arba jo išvis nėra.
2. SSL/TLS sesijos nustatymas dažnai yra atskirtas nuo vartotojo tapatumo nustatymo.

Dėl pirmame punkte minimos priežasties yra galima situacija, kai vartotojas komunikuoja su kenkėju atskleidamas jam savo prisijungimo duomenis.

Dėl antrame punkte minimos priežasties prisijungimo duomenys, perimti iš vartotojo, gali būti panaudoti kenkėjo, tuo pačiu imituojant tikrojo serverio veikimą.

Labai dažnai MITM ataka yra vykdoma kartu su slaptažodžių žvejbos ataka.[16:4] Vartotojui bandant prisijungti prie tikrosios banko svetainės, kenkimo programa, jam to nežinant, nukreipia jį į kenkimo svetainę, kuri imituoja banko svetainę. Joje vartotojui įvesti prisijungimo vardas bei slaptažodis patenka į kenkėjų rankas[18:2].

Ataka yra vykdoma naudojant programą, kuri į vartotojo kompiuterį įdiegta prieš jo valią. Todėl yra labai sunku gauti bent apytikslę statistinę informaciją apie šią ataką.

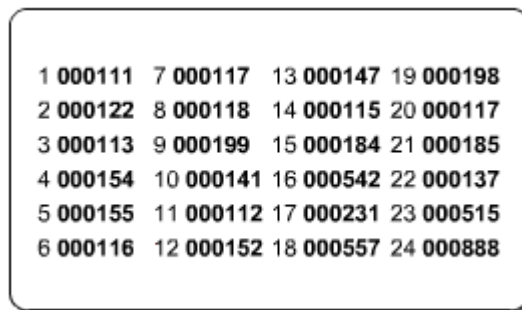
Tačiau dėl to, kad MITM ataka dažnai yra vykdoma kartu vykdam ir slaptažodžių žvejbos ataką, ir dėl slaptažodžių žvejbos atakų skaičiaus augimo pastaruoju metu, galima daryti prielaidą, kad taip pat augo ir MITM atakų skaičius.

6. Klientų apsaugos priemonės

Šiame skyriuje aptarsime, kokios šiuo metu yra naudojamos klientų apsaugos priemonės realiai veikiančiose sistemose ir pabandysim aptarti kiekvienos iš šių priemonių plusus bei minusus.

6.1 PIN kodų kortelės

Tai turbūt plačiausiai naudojamas klientų apsaugos metodas banko sistemose. Be vartotojo prisijungimo vardo ir slaptažodžio, taip pat yra naudojama kiekvienam klientui išduodama individuali kodų kortelė. Dažniausiai joje būna 24 kodai, bet skaičius gali kisti. Jungiantis prie sistemos vartotojui yra nurodoma, kurį iš tų kodų reikia įvesti. Dažniausiai ta kortelė yra naudojama ne tik prisijungimui, bet ir vykdomų operacijų patvirtinimui, tačiau kartais operacijų patvirtinimui būna išduodama atskira kortelė.



4 pav. PIN kodų kortelės pavyzdys

Nors šis apsaugos būdas apsunkina vartotojo tapatybės vagystę, jis visiškai neapsaugo nei nuo slaptažodžių žvejybos, nei nuo MITM atakų. Perėmus tik vieną iš 24 kodų, juo pasinaudoti yra gana sunku, tačiau teoriškai vis tiek įmanoma. Vartotojui nepastebėjus, kad banko svetainė yra netikra, ir įvedus daugiau kodų arba ilgą laiką jo kompiuteryje veikiant kenkimo programai, gali būti perimta ir visa kodų lentelė.

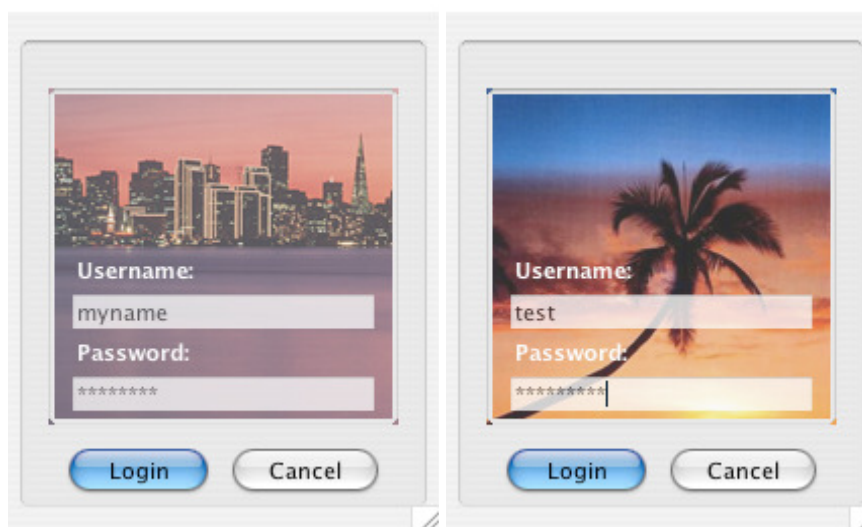
6.2 SMS arba elektroninio laiško patvirtinimas

Dažnai norint atlikti kažkokį veiksmą, susijusį su pinigų pervedimu, tenka jį patvirtinti SMS žinute gautu kodu. Esant tokiai sistemai nepakanka perimti vien tik vartotojo prisijungimą ir slaptažodį, bet reikia perimti ir SMS žinute gautą kodą, o tai apsunkina duomenų vagystę[21:4]. Jei sumos nėra labai didelės arba sistema nereikalauja tokio didelio saugomo laipsnio, vietoj SMS žinutės gali būti naudojamas elektroninis paštas. Tokiu atveju visas sistemos veikimas yra toks pat tik vietoj to, kad kodas būtų atsiunčiamas sms žinute, jis atsiunčiamas elektroniniu paštu.

Pagrindinis šio apsisaugojimo būdo minusas yra tas, kad jis tinka tik tiems vartotojams, kurie turi pastovų telefono numerį arba elektroninį paštą. Todėl tokia sistema dažniau naudojama internetinių sistemų, kuriose visa registracija atliekama internetu. Banko svetainėse tokios sistemos naudojimą apsunkina tai, kad ne visi vartotojai turi elektroninį paštą, o telefono numeris gali būti pakeistas. Galima būtų suteikti galimybę vartotojui prisijungus prie banko sistemos pačiam įsivesti naują ar pasikeitusį telefono numerį ar elektroninį paštą, tačiau taip atsirastų grėsmė, kad tokios įvesties metu duomenys bus perimti.

6.3 Paveikslo įkėlimas

Ši apsaugos priemonė yra paremta tuo, kad klientas į banko sistemą įkelia paveikslą. Vartotojui, bandančiam prisijungti prie banko sistemos, yra parodomas jo paties įkeltas paveikslas[3:4]. Jei paveikslas nesutampa su tuo, kurį įkėlė vartotojas, tai yra ženklas, kad banko svetainė yra netikra ir yra bandoma pavogti vartotojo duomenis. Tokia apsaugos priemonė yra veiksminga tik prieš slaptažodžių žvejybos atakas, tačiau yra visiškai neveiksminga prieš MITM atakas.

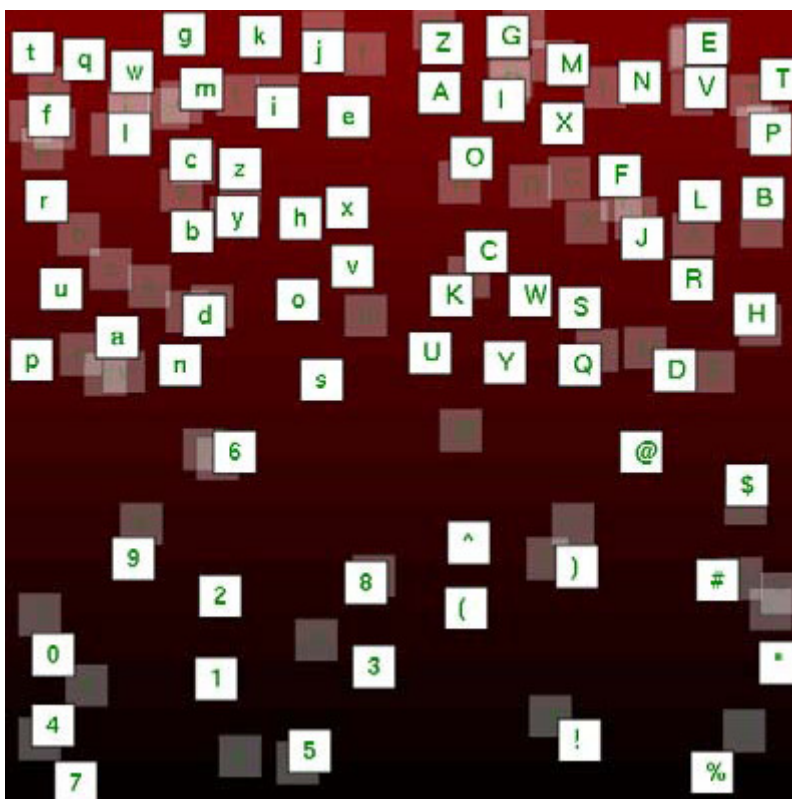


5 pav. Prisijungimo formos, naudojant paveikslo įkėlimą, pavyzdys

Kitas svarbus aspektas, susijęs su šio metodo efektyvumu, yra vartotojo budrumas: jei vartotojas nepastebės, kad paveikslas nesutapo su jo įkeltu paveikslu arba pastebės, bet vis tiek nekreips dėmesio ir įves duomenis, tai ši priemonė taps neveiksminga. Taip pat gali būti tokia situacija, kai vartotojai yra nepakankamai informuoti ir nesupranta to paveikslo paskirties bei svarbos jų pačių saugumui.

6.4 Virtualioji klaviatūra

Virtualiosios klaviatūros[21:5] klientų apsaugos metodas kol kas nėra labai dažnai aptinkamas. Pagrindinė šio metodo idėja yra ta, kad klientas prisijungimo duomenis įveda ne iš klaviatūros, bet naudodamasis pele renka tekstą virtualioje klaviatūroje, kuri atsiranda kaip paveikslas, ir paspaudus vieną simbolį sugeneruojamas vis naujas paveikslas. Toks metodas visiškai neapsaugo nuo tapatybės vagystės, bet tikrai apsunkina neteisėtą duomenų perėmimą. Nuo slaptažodžių žvejybos atakų tokia priemonė visiškai neapsaugo, nors tokią sistemą padaryti netikroje svetainėje yra sunkiau, tačiau vis tiek įmanoma

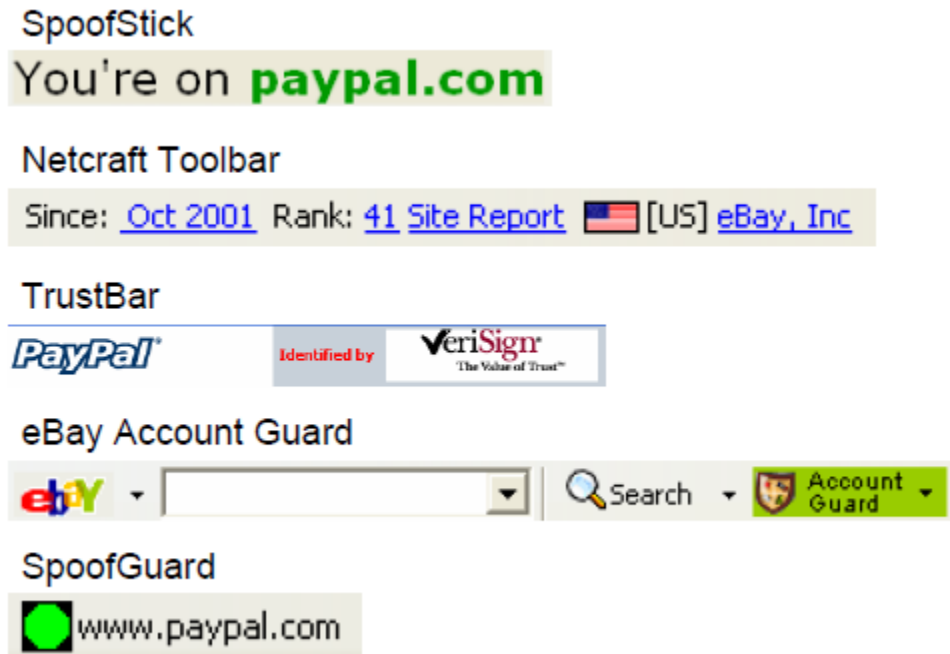


6 pav. Virtualiosios klaviatūros pavyzdys

Pagrindinis tokio metodo pliusas yra tai, kad vartotojui nereikia įsiminti papildomų kodų, taip pat nereikia nešiotis kodų kortelių.

6.5 Specializuotos saugos įrankių juostos

Saugos įrankių juostos (angl. toolbars) naršyklėje rodo puslapio informaciją, kuri yra aktuali vertinant puslapio saugą ir atpažįstant slaptažodžių žvejybos atakos galimybę. Šis įrankis yra skirtas pačiam vartotojui, galutinį sprendimą jis turi priimti pats.



7 pav. Specializuotų saugumo įrankių juostų pavyzdžiai [22:1]

Įrankių juostų yra gana įvairių, keletas pavyzdžių pateikta 7 paveiksle. Skirtingos įrankių juostos pateikia skirtingą informaciją[22:2]:

- Domeno registracijos datą: jei domenas yra užregistruotas neseniai, galima įtarti, kad bandoma įvykdyti apgaulę, nes tikrosios svetainės dažniausiai jau yra gana seniai užregistruotos.
- Šalį, kurioje yra patalpinta svetainė: žinant šalį, kurioje įmonė vykdo veiklą, įtarimą gali sukelti tai, kad svetainė yra patalpinta kitoje šalyje.
- Populiarumą tarp kitų įrankių juostos vartotojų: mažas populiarumas rodo tai, kad veikiausiai tai nėra tikroji svetainė, nes tikrosios svetainės populiarumas dažniausia būna labai didelis.
- Ar naudojamas SSL ir sertifikato autoritetą (angl. Certificate authority): svetainės, teikiančios internetinės bankininkystės paslaugą, visada naudoja kriptografinės apsaugos priemones. Tokių priemonių nebuvimas svetainėje sukelia įtarimą.

- Įrankių juosta skirta konkrečioms svetainėms (pvz., PayPal, eBay), rodančios, ar svetainė priklauso šioms įmonėms. Šios įrankių juostos dažniausiai ne tik parodo, ar konkreči svetainė priklauso tikrajai įmonei, bet ir parodo, jei puslapis jau yra įtrauktas į juodąjį sąrašą, į kurį įtraukiamos jau žinomos kenkimo svetainės.



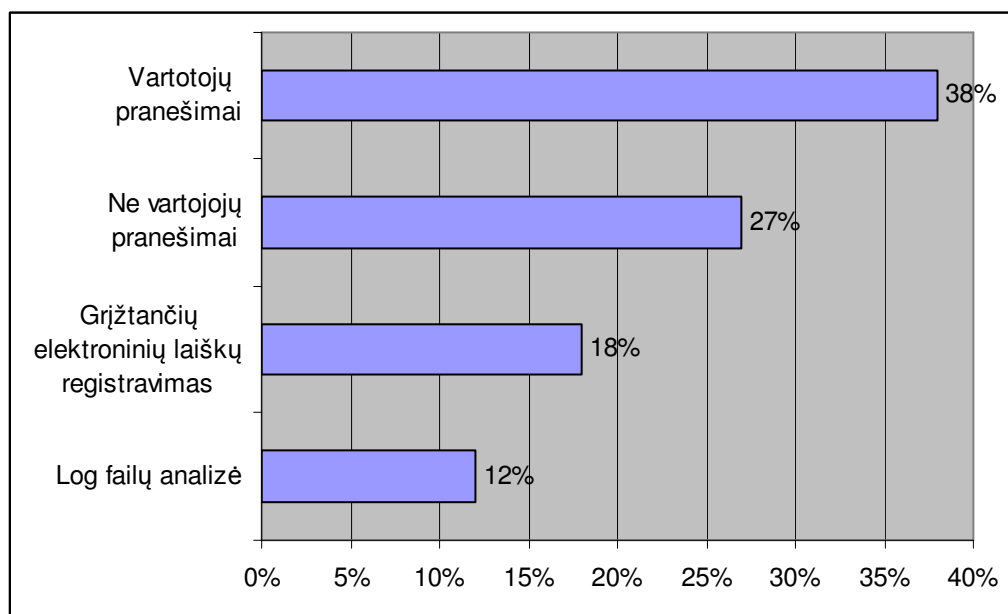
8 pav. Specializuotų saugumo įrankių juostų, skirtų konkrečioms svetainėms, pavyzdžiai[22:3]

Visa ši informacija yra labai vertinga norint atskirti tikrąją svetainę nuo kenksmingos.

Didžiausias šios priemonės minusas yra tas, kad galutinį sprendimą turi priimti pats vartotojas. Dažniausiai vartotojas, bandantis pasinaudoti internetinėmis bankininkystės paslaugomis, pirmiausia galvoja apie tai, kokius veiksmus jis planuoja atlikti, o saugos klausimai neretai pamirštami. Iš atliktų tyrimų[22:9] yra matoma, kad tokių įrankių juostų efektyvumas yra stebėtinai žemas. Nors dalis vartotojų kartais ir pastebėdavo įrankių juostos pranešimus apie tai, jog svetainė nėra saugi, nė viena iš tyrimuose naudotų įrankių juostų nesugebėjo visiškai apsaugoti vartotojų nuo apgaulės įvykdymo. Dar viena bėda yra tai, kad tam tikrus įrankių juostos pranešimus vartotojai interpretuodavo gana skirtingai, pvz.: tai kad svetainė yra gana neseniai užregistruota, vartotojai interpretuodavo kaip įmonės plėtrą internetinėje erdvėje, o tai, kad svetainė yra patalpinta ne toje šalyje, kurioje yra vykdoma pagrindinė įmonės veikla, dalis vartotojų interpretavo kaip naujo įmonės padalinio atidarymą naujoje šalyje.

6.6 Vartotojų budrumo skatinimas

Remiantis [12], aptinkant bandymus įvykdyti slaptažodžių žvejybos atakas didelę įtaką turi ne technologiniai sprendimai, o vartotojų pranešimai apie įtartino turinio laiškus ar kitokius bandymus iš jų išgauti privačią informaciją.



9 pav. Pagrindiniai metodai, leidžiantys aptikti slaptažodžių žvejybos atakų įvykdymo bandymus

Daugelis specialistų pripažįsta, kad vienas sėkmingiausių metodų kovojant su tokio tipo nusikaltimais yra vartotojų perspėjimas ir sąmoningumo ugdymas, skatinimas pranešti apie bet kokią bandymą išvilioti konfidencialius duomenis[12:3].

Tačiau nors daugiausiai informacijos apie bandymus įvykdyti atakas gaunama iš vartotojų, nederėtų užmiršti ir technologinių perspėjimo bei apsaugojimo sistemų, nes geras grįžtamasis ryšys iš vartotojų padeda tik sužinoti apie įvykį, o geros technologinės priemonės gali padėti sumažinti atakų skaičių.

7. Biometrinės sistemos

Dažnai, siekiant padidinti sistemos saugumo lygį, yra naudojamos biometrinės apsaugos sistemos.

Biometrija nagrinėja žmogaus atpažinimo metodus, remiantis būdingais jo fiziniais arba elgsenos požymiais.[2]

Biometrija skaidoma į dvi dalis:

- **Fiziologinę** - susijusi su fizinėm kūno savybėm. Tyrinėja žmogaus atpažinimą pagal: pirštų antspaudus, veido savybes, DNR, rankos ir delno geometrines savybes, akies rainelės savybes ir t.t.
- **Elgsenos** - susijusi su žmogaus elgsena. Tyrinėja žmogaus atpažinimą pagal: eisena, balsą, klaviatūros klavišų paspaudimo charakteristikas ir t.t.

Biometrijoje dažnai vartojamos tokios sąvokos kaip I-ojo ir II-ojo tipo klaidos.

I-ojo tipo klaida- tai klaida, kai žmogus yra klaidingai neatpažįstamas. Dar kartais naudojamas angliška santrumpa FRR (False reject rate), reiškiantis klaidingai neatpažįstamų žmonių skaičių.

II-ojo tipo klaida-tai klaida, kai žmogus yra klaidingai atpažįstamas kaip kitas žmogus. Naudojamas angliška santrumpa FAR (False accept rate), reiškiantis, kiek žmonių yra klaidingai atpažįstami kaip kiti asmenys.

I-ojo tipo klaida dažniausiai būna neišvengiama, tačiau jos reikšmė yra žymiai mažesnė nei II-ojo tipo klaidos, nes įvykus I-jo tipo klaidai vartotojas tiesiog gali pakartotinai atlikti atpažinimo procedūrą. Tačiau įvykus II-ojo tipo klaidai vartotojas yra klaidingai atpažįstamas kaip kitas asmuo, o tai įgalina jį naudotis jam nepriklausančiomis teisėmis, pavyzdžiui prieti prie slaptos informacijos.

7.1 Biometrinės sistemos sėkmes faktoriai

Kuriant biometrines saugos sistemas būtina susipažinti su faktoriais, lemiančiais biometrinės apsaugos sistemos efektyvumą.

Tom Olzak , turintis ilgametę patirtį informacinių technologijų saugume, savo darbe, paskelbtame 2006 metais [11:2], atkreipia dėmesį į tai, kad būtina atsižvelgti ne tik į technines biometrinės sistemos savybes, bet ir į žmogiškąsias aplinkybes, t.y. į tai, ar sistema bus patraukli ir patogi vartotojui.

Išskiriamos šios charakteristikos:

1. Tikslumas
2. Greitis
3. Atsparumas apgaulei
4. Patikimumas
5. Duomenų saugyklos reikalavimai
6. Naujo vartotojo įtraukimo laikas
7. Jaučiamas nepasitikėjimas

7.1.1 Tikslumas

Nors biometrijos algoritmai vis labiau tobulėja, 100% vis dar nepasiekiamas, todėl naudojant biometriją tenka nuspręsti, koks netikslumo procentas yra toleruojamas[11:2]. Parinkdami sutapimo ribą, mes keičiame I-ojo ir II-ojo tipo klaidų procentą. Mažindami I-ojo tipo klaidų skaičių, didiname II-ojo tipo klaidų skaičių ir atvirkščiai.

7.1.2 Greitis

Tam, kad sistema būtų sėkmingai naudojama, yra labai svarbu, kad ji būtų priimtina sistemos vartotojams. Dėl šios priežasties yra svarbus laikas, per kurį vartotojas yra priimamas arba atmetamas. Priimtinas greitis yra toks kai vienas vartotojas užtrunka maždaug 5 sekundes arba per 1 minutę spėja biometrine sistema pasinaudoti nuo 6 iki 10 žmonių[11:3]. Esant mažesniai greičiui, vartotojai pradeda jausti nepasitenkinimą.

7.1.3 Atsparumas apgaulei

Kai kurie biometriniai sprendimai gali būti jautrūs bandymui sistemą apgauti. Kai kurias pirmąsias biometrines sistemas, naudojusias pirštų antspaudų skanavimą, buvo galima apgauti nevisiškai prispaudus pirštą. Šių dienų sistemos yra gana pažengusios nuo tų dienų, tačiau vis tiek yra labai svarbu apgalvoti visus galimus sistemos apgaulės būdus ir kaip gali elgtis piktavališkai nusiteikęs vartotojas.

7.1.4 Patikimumas

Naudojant papildomą įrangą, labai svarbus yra tos įrangos dėvėjimosi laikas. Senstant įrangai, matavimai gali tapti ne tokie tikslūs ir gali padidėti klaidų skaičius.

7.1.5 Duomenų saugyklos reikalavimai

Reikalavimai duomenų saugyklai priklauso nuo to, kas iš tikro yra saugoma saugykloje. Balso atpažinimo sistemai reikalinga gana didelė saugykla, nes garso failas yra sąlyginai didelis. Kitokia situacija yra pirštų atspaudų sistemoje, nes joje saugoma informacija užima gana mažai todėl ir reikalavimai saugyklai yra mažesni.

7.1.6 Naujo vartotojo įvesties laikas

Tai laikas, per kurį yra įvedamas naujas vartotojas taip, kad biometrinė sistema jį atpažintų. Tai neturėtų užtrukti ilgiau nei 2 minutes vienam vartotojui[11:4]. Tai taip pat susiję su tuo, kad sistema būtų priimtina jos vartotojams, nes per ilgas registravimo laikas gali kelti nepasitenkinimą sistema.

7.1.7 Jaučiamas nepasitikėjimas

Šis aspektas taip pat susijęs su vartotojų noru naudoti konkrečią sistemą. Kartais vartotojams iškyla tokios baimės[11:4]:

1. Baimė, kad įmonė kaupia unikalią asmeninę informaciją
2. Baimė, kad įmonė kaupia informaciją apie darbuotojų sveikatą (pvz., akies skenavimo metu gauta informacija, gali būti panaudota nustatant tam tikras ligas)
3. Baimė, kad naudojama įranga kenkia sveikatai (pvz., lazeris skenuojantis akį)
4. Baimė, kad kontaktuojant su daugelio naudojama įranga galima užsikrėsti ligomis

Šis aspektas nėra techninis, tačiau jo pamiršti nevertėtų, nes šiuo klausimu neišspręstos problemos gali trukdyti sėkmingam sistemos naudojimui.

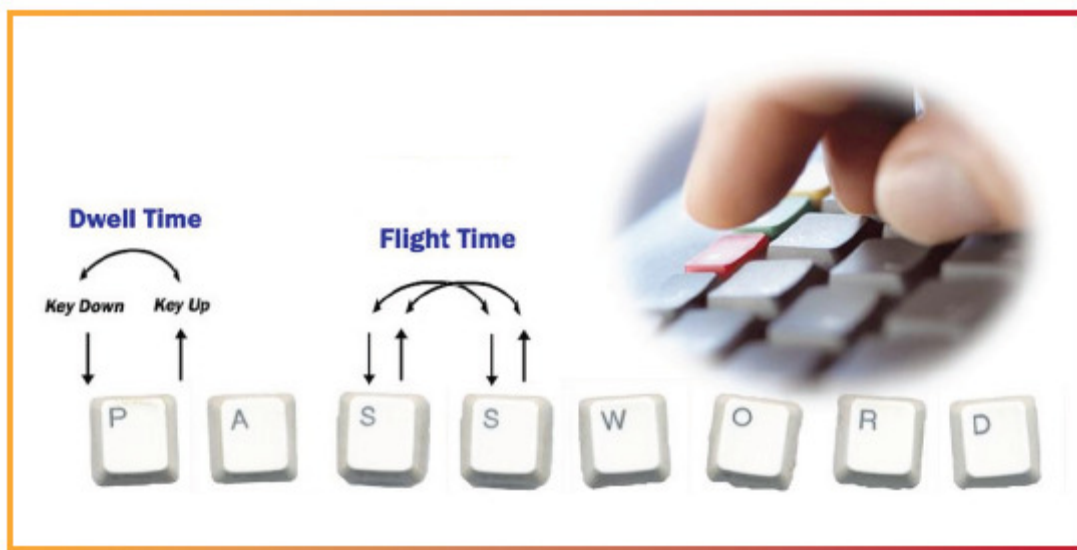
8 Klavišų paspaudimo analizė

Klavišų paspaudimo analizė (angl. Keystroke analysis) yra biometrijos dalis, naginėjanti žmogaus identifikavimą pagal tai, kaip jis renka tekstą kompiuterio klaviatūra. Kitaip tariant, yra tiriama ne tik tai, kas yra įvedama, bet ir tai, kaip yra įvedama. Bandoma ieškoti tam tikrų metodų, kaip iš gautų duomenų išgauti informaciją, kuri būtų naudinga vieno vartotojo atskyrimui nuo kito vartotojo.

Ši biometrijos sritis yra vertinama gana dviprasmiškai. Yra teigiančių, kad tokiu būdu neįmanoma užtikrinti pakankamo saugumo lygio, tačiau taip pat yra tvirtinančių, kad naudojant klavišų paspaudimo analizę galima padidinti sistemos saugą[6:9].

Galima rasti pavyzdžių, kad klavišų paspaudimo analizės pritaikymas buvo sėkmingas ir iki šiol naudojamas, tačiau kol kas šis metodas nėra labai plačiai taikomas sistemose, kurios yra viešai prieinamos ir naudojamos daugelio vartotojų[8:5].

8.1 Naudojamos Metrikos



10 pav. Klavišų paspaudimo analizės naudojamos metrikos

Dažniausiai klavišų paspaudimo analizės naudojamos metrikos[11:6](10 pav.):

- Užlaikymo laikas (angl. Dwell time) – laikas, kurį yra laikomas paspaustas klavišas
- Perėjimo laikas (angl. Flight time) – laikas, kuris sugaištamasis pereinant nuo vieno klavišo prie kito. Egzistuoja dvi metodikos šiam laikui matuoti: pirmoji - tai laikas, nuo vieno klavišo paspaudimo iki kito klavišo paspaudimo; antroji - tai laikas nuo vieno klavišo atleidimo iki kito klavišo atleidimo. Galima naudoti kurią nors vieną iš jų, tačiau galima ir abi.

8.2 Klavišu paspaudimo analizės tinkamumas pagal biometrinių sistemų reikalavimus

Apžvelkime, kaip klavišų paspaudimo analizė atitinka bendrus biometrinių sistemų reikalavimus, kuriuos prieš tai aptarėme.

8.2.1 Tikslumas

Nors dabar klavišų paspaudimų analizės algoritmai yra pakankamai tikslūs, labai svarbu tinkamai išspręsti klausimus, susijusius su reagavimu į klaidas. Labai svarbu sumažinti antrojo tipo klaidų skaičių, kaip galima mažiau mažinant vartotojų trukdžius, kurie atsiranda didėjant pirmojo tipo klaidoms.

8.2.2 Greitis

Greičio atžvilgiu klavišų paspaudimų analizės pranašumas yra tai, kad dažniausiai užtenka įvesti vartotojo vardą ir slaptažodį tam, kad sistema automatiškai atliktų analizę. Kartais vartotojams tenka įvesti ilgesnius sakinius kurie yra išvedami į ekraną (tai priklauso nuo to kaip suprojektuota sistema), tačiau tai neužima daug papildomo laiko.

8.2.3 Atsparumas apgaulei

Naudojant vien tik klavišų paspaudimo analizę negalima atsisakyti kitų priemonių, tokių kaip PIN kodų lentelės, slaptažodžiai ir vartotojo vardai. Naudojant vien tik klavišų paspaudimo analizę sistema yra gana pažeidžiama, bet jei tai yra naudojama kompleksiškai, sistema tampa labai atsparia bandymui įvykdyti apgaule.

8.2.4 Patikimumas

Naudojant įvairius skenerius ar kitą papildomą įrangą, bėgant laikui ji gali imti dėvėtis ir klaidų skaičius imti augti. Čia naudojama tik paprasta kompiuterio klaviatūra, todėl tokios problemos nėra.

8.2.5 Duomenų saugyklos reikalavimai

Reikalavimai duomenų saugyklai nesiskiria nuo reikalavimų paprasčiausiai sistemai, nes, palyginti su kitais duomenimis apie vartotoją, duomenys apie vartotojo įvestų eilučių analizę užima nedaug vietos.

8.2.6 Naujo vartotojo įvesties laikas

Nors yra sistemų, kuriose naujo vartotojo įvestis niekuo nesiskiria nuo sistemos, kurioje nėra naudojama klavišų paspaudimo analizė, norint padidinti tikslumą kartais yra naudojama tokia praktika:

eilutę, kuri bus analizuojama, vartotojas turi įvesti daugiau nei vieną kartą. Tai priklauso nuo sistemos suprojektavimo. Esant daugiau nei vienai eilutes įvesčiai, žinoma, kad ilgėja ir vartotojo įvesties laikas.

8.2.7 Jaučiamas nepasitikėjimas

Kadangi yra naudojama kompiuterio klaviatūra, kurią vartotojai ir taip naudoja, problemų dėl vartotojų nepasitikėjimo įranga neiškyla. Taip pat nėra kaupiami jokie duomenys, kurie gali būti naudojami sveikatos būsenos nustatymui, pvz., duomenys apie akies rainelę.

8.3 Klavišų paspaudimo analizės sistemos variacijos

Prieš tai paminėti reikalavimai taikomi ne tik klavišų paspaudimo analizės metodams, bet ir bendrai biometrinėms sistemoms. Yra nemažai galimų skirtingų klavišų paspaudimų analizės variacijų.

Variacija šiame darbe vadinsime konkretų sistemos kintamų dalių parinkimą.

Kevin S. Killourhy ir Roy A. Maxion [5:3] pateikia tokius galimus paspaudimo analizės pakeitimus:

- Ar įvedant nauja vartotoją jis analizuojamą tekstą įveda vieną kartą, ar keletą kartų?
- Ar bus fiksuotas įvedamo teksto ilgis, ar laisvai pasirenkamas?
- Ar naudojami užlaikymo, ar perėjimo laikai? O gal abu kartu?
- Ar tekstas bus parenkamas sistemos, ar vartotojas pats jį galės parinkti?
- Ar galima pakartotinę teksto įvestis? Jei taip, tai kiek yra galimų bandymų?

Deja, galimos klavišų paspaudimo analizės variacijos yra tik aprašytos, trūksta kokybinių įvertinimų ir palyginimų tarp vienos ir kitos pasirinkties.

9. Klavišų paspaudimo analizės efektyvumo tyrimas

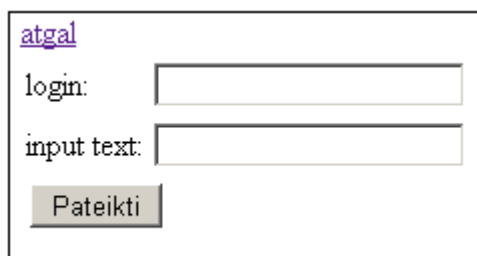
Tyrimo metu buvo tiriama, kaip klavišų paspaudimo analizės efektyvumas ir galimybės panaudoti keičiasi, keičiant tam tikras metodo dalis. Taip pat analizuojama, ar pasiektas apsaugos lygis yra pakankamas apsaugai nuo slaptažodžių žvejybos ir MITM atakų. Buvo sukurta keletas skirtingų programų, veikiančių su skirtingomis konfigūracijomis.

9.1 Programos veikimas

Buvo sukurtos skirtingos programos skirtingoms klavišų paspaudimo analizės konfigūracijoms. Konfigūracijos buvo parinktos remiantis Kevin S. Killourhy ir Roy A. Maxion pateiktais galimais paspaudimo analizės pakeitimais.

9.1.1 Vartotojo įvestis

Įvedant vartotoją, jo duomenys ir kiti, klavišų paspaudimo analizei reikalingi, duomenys buvo išsaugomi duomenų bazėje. Vartotojo įvesties langas parodytas 11 paveiksle.



The image shows a web form with a purple link labeled 'atgal' at the top left. Below it are two input fields: the first is labeled 'login:' and the second is labeled 'input text:'. At the bottom of the form is a grey button with the text 'Pateikti'.

11 pav. Tyrime naudota prisijungimo forma

Vartotojui bandant prisijungti, duomenys, apie klavišų paspaudimo atitikimą buvo išsaugoti MySQL duomenų bazėje, kurios struktūra pateikta 16 paveiksle.

9.1.2 Vartotojo prisijungimas

Vartotojo prisijungimo langai parodyti 12 paveiksle ir 13 paveiksle. 12 paveiksle pavaizduotas pradinis langas, kuriame rodomas vartotojo vardas ir kokią būtent eilutę jis turi įvesti. Taip imituojama situacija kai kenkėjas žino ir vartotojo vardą, ir slaptažodį.

13 paveiksle pavaizduota situacija, kai vartotojas įveda įvesties tekstą ir paspaudžia “Pateikti”. Šiuo atveju, pagal eilutės įvesties charakteristiką yra apskaičiuojamos koreliacijos pagal užlaikymo charakteristikas ir pagal perėjimo charakteristikas.

[registruoti nauja](#)
[vartotoju sarasas](#)
 vartotojas: vaidas
 iveskite teksta: "obuolys"
 input text:
 Rezultatas:

12 pav. Tyrime naudota vartotojo prisijungimo forma

[registruoti nauja](#)
[vartotoju sarasas](#)
 vartotojas: vaidas
 iveskite teksta: "obuolys"
 input text:
 Rezultatas:
 dwell: 0.91426768888502
 flight: 0.96068816393617

13 pav. Tyrime naudota vartotojo prisijungimo forma su gautų rezultatų pavyzdžiu

Gautas rezultatas iš karto pavaizduojamas ekrane. Be to visi šie duomenys įrašomi į duomenų bazę.

9.1.3 Duomenų išvedimas

Galutinis sutapimo laipsnis laikomas abiejų koreliacijų sandauga

$$R = \text{corr}(\text{DwellTime}) * \text{corr}(\text{FlightTime}) \quad (1)$$

Duomenų bazėje išsaugoti rezultatai išspausdinami atskirai pagal tai, ar prisijungti bandė tikrieji vartotojai ar apsimetėliai. Rezultatų išvedimo pavyzdžiai yra pateikti 14 paveiksle ir 15 paveiksle.

Tikri vartotojai		
DwellResult	FlightResult	SandaugaResult
0.68992771047705	0.92798220576848	0.64024063858929
0.5978988897802	0.91016449351342	0.54418634018903
0.507970405518	0.92949494593699	0.47215592461454
0.46361359146998	0.91920468136534	0.4261557836238
0.49886169837844	0.88551991654836	0.44175196951725
0.49313420195176	0.80142359341335	0.3952093841632
0.83442242253482	0.50251290749206	0.41930803762454
0.82340936965394	0.97681249080313	0.8043165573223
0.67448675848482	0.95043197623292	0.64105378280966
0.78527724995026	0.94351949437631	0.74092439381829
0.67518494366239	0.86723778863398	0.58554589746073
0.67963502183434	0.89742308230779	0.6099201561389
0.69230366189077	0.80777122050235	0.55922297392375
0.68620215925043	0.83844033488509	0.5753395682008
0.60226557396109	0.83982738084315	0.50579911955174
0.7645416387207	0.97182088893951	0.74299753497282
0.65297630699183	0.88245038046334	0.57621919053849
0.59858669211823	0.96835977698071	0.57964727568323
0.76392642413546	0.96142756866008	0.73445992459174
0.79720538053509	0.95974881813713	0.76511692178111
0.64206001227428	0.80298596845072	0.51556518075954
0.6496993869952	0.87800408353813	0.57043871485401

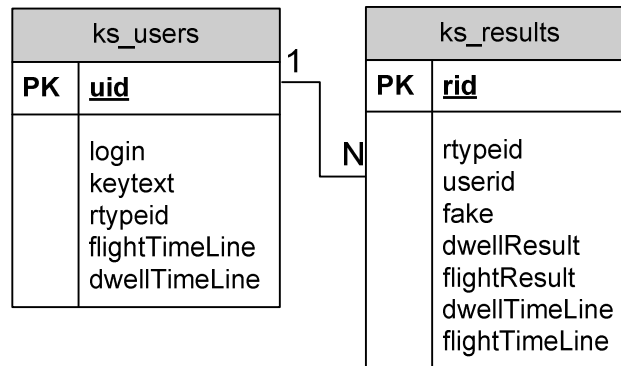
14 pav. Tikrųjų vartotojų prisijungimo rezultatų išvedimo pavyzdys

Apsimeteliai		
DwellResult	FlightResult	SandaugaResult
0.84222718538049	0.87926361903274	0.74053972306541
0.67709980817478	0.88371228632106	0.59836141954969
0.66170117237952	0.86917457783026	0.57513383715276
0.87183268955693	0.80186179054246	0.69908932150157
0.5767693087514	0.57443092543431	0.33131412778817
0.63552267756409	0.83672791635876	0.53175956579694
0.66837889383504	0.8273219935735	0.55296455891006
0.67477772898417	0.84412392249067	0.56959602339946
0.48675975033223	0.74085889200379	0.36062028930318
0.5069639347209	0.74120664842866	0.37576503892868
0.55994137488908	0.44728426298737	0.2504529651834
0.34439665901137	0.84378944786406	0.29059826675343
0.43748095557612	0.76565241517375	0.33495835022938
0.47259753758544	0.81740977571856	0.38630584720286
0.82816659250206	0.8343172504621	0.69095367438089
0.54676484271032	0.82751581982923	0.45245655706923
0.41653631201978	0.85754639234594	0.35719921165365
0.5865957345116	0.85875781609204	0.50374367189809
0.66724057267794	0.35873407592821	0.23936193026143
0.74550774676455	0.78763260049573	0.58718620527387
0.5616230997079	0.84903875144389	0.47683977535804

15 pav. Apsimetėlių prisijungimo rezultatų išvedimo pavyzdys

9.1.4 Duomenų bazės struktūra

Tyrimo naudojamos MySQL duomenų bazės struktūra pavaizduota 16 paveiksle.



16 pav. Duomenų bazės struktūra

Lentelėje **ks_users** saugoma informacija apie esamus vartotojus. Ją sudaro:

- uid - unikalus laukas, reiškiantis vartotojo ID sistemoje;
- login - vartotojo vardas;
- keytext – tekstas, kuris yra analizuojamas klavišų analizės paspaudimo metodu;
- rtypeid - variacijos ID, skirtas atskirti, kurią variaciją naudojant buvo įvestas vartotojas;
- flightTimeLine - perėjimo laiko charakteristikos, gautos įvedant analizuojamą tekstą;
- dwellTimeLine - užlaikymo charakteristikos, gautos įvedant analizuojamą tekstą;

Lentelėje **ks_results** saugoma informacija apie vartotojų bandymus prisijungti prie sistemos.

Ją sudaro:

- rid - unikalus laukas;
- userid- vartotojo ID sistemoje;
- rtypeid - variacijos ID, skirtas atskirti, kurią variaciją naudojant buvo gautas rezultatas;
- fake - parodo, kas bandė prisijungti: tikrasis vartotojas ar apsimetėlis. Galimos reikšmės 0 ir 1;
- dwellResult - koreliacijos rezultatas, gautas tarp dviejų užlaikymo charakteristikų: įvestos registravimo metu ir įvestos bandymo prisijungti metu;
- flightResult - koreliacijos rezultatas, gautas tarp dviejų perėjimo charakteristikų: įvestos registravimo metu ir įvestos bandymo prisijungti metu;
- dwellTimeLine - užlaikymo charakteristikos, gautos įvedant analizuojamą tekstą;
- flightTimeLine - perėjimo laiko charakteristikos, gautos įvedant analizuojamą tekstą;

Lentelės yra susietos laukais uid (ks_users lentelė) ir userid (ks_results lentelė), ryšys yra vienas su daugybe, lentelėje ks_users uid yra unikalus.

9.2 Variacijos

Siekiant rasti efektyviausias sistemos variacijas buvo parinktos variacijos keičiant tam tikras sistemos dalis.

9.2.1 Vienkartinės įvesties fiksuoto ilgio variacijos:

1 Variacija:

Vartotojo įvestis – įvedama, pirmą kartą įvedus eilutę;

Eilutės ilgis - 7 simboliai;

Eilutė - „abecele“;

2 Variacija:

Vartotojo įvestis – įvedama, pirmą kartą įvedus eilutę;

Eilutės ilgis - 11 simbolių;

Eilutė - „kompiuteris“;

3 Variacija:

Vartotojo įvestis – įvedama, pirmą kartą įvedus eilutę;

Eilutės ilgis - 15 simbolių;

Eilutė - „the quick brown“;

9.2.2 Vienkartinės įvesties laisvai pasirenkamos eilutės variacijos:

4 Variacija:

Vartotojo įvestis – įvedama, pirmą kartą įvedus eilutę;

Eilutės ilgis - nuo 5 iki 8 simbolių;

Eilutė - laisvai pasirenkama;

5 Variacija:

Vartotojo įvestis – įvedama, pirmą kartą įvedus eilutę;

Eilutės ilgis - nuo 8 iki 11 simbolių;

Eilutė - laisvai pasirenkama;

6 Variacija:

Vartotojo įvestis – įvedama, pirmą kartą įvedus eilutę;

Eilutės ilgis - nuo 11 iki 15 simbolių;

Eilutė - laisvai pasirenkama;

9.2.3 Daugkartinės įvesties fiksuoto ilgio variacijos:

7 Variacija:

Vartotojo įvestis - įvedama, eilutę įvedus 3 kartus;

Eilutės ilgis - 7 simboliai;

Eilutė - „abecele“;

8 Variacija:

Vartotojo įvestis - įvedama, eilutę įvedus 3 kartus;

Eilutės ilgis - 11 simbolių;

Eilutė - „kompiuteris“;

9 Variacija:

Vartotojo įvestis - įvedama, eilutę įvedus 3 kartus;

Eilutės ilgis - 15 simbolių;

Eilutė - „the quick brown“;

10 Variacija:

Vartotojo įvestis - įvedama, eilutę įvedus 5 kartus;

Eilutės ilgis - 7 simboliai;

Eilutė - „abecele“;

11 Variacija:

Vartotojo įvestis - įvedama, eilutę įvedus 5 kartus;

Eilutės ilgis - 11 simbolių;

Eilutė - „kompiuteris“;

12 Variacija:

Vartotojo įvestis - įvedama, eilutę įvedus 5 kartus;

Eilutės ilgis - 15 simbolių;

Eilutė - „the quick brown“;

9.2.4 Daugkartinės įvesties laisvai pasirenkamos eilutės variacijos:

13 Variacija:

Vartotojo įvestis - įvedama, eilutę įvedus 3 kartus;

Eilutės ilgis - nuo 5 iki 8 simbolių;

Eilutė - laisvai pasirenkama;

14 Variacija:

Vartotojo įvestis - įvedama, eilutę įvedus 3 kartus;

Eilutės ilgis - nuo 8 iki 11 simbolių;

Eilutė - laisvai pasirenkama;

15 Variacija:

Vartotojo įvestis - įvedama, eilutę įvedus 3 kartus;

Eilutės ilgis - nuo 11 iki 15 simbolių;

Eilutė - laisvai pasirenkama;

16 Variacija:

Vartotojo įvestis - įvedama, eilutę įvedus 5 kartus;

Eilutės ilgis - nuo 5 iki 8 simbolių;

Eilutė - laisvai pasirenkama;

17 Variacija:

Vartotojo įvestis - įvedama, eilutę įvedus 5 kartus;

Eilutės ilgis - nuo 8 iki 11 simbolių;

Eilutė - laisvai pasirenkama;

18 Variacija:

Vartotojo įvestis - įvedama, eilutę įvedus 5 kartus;

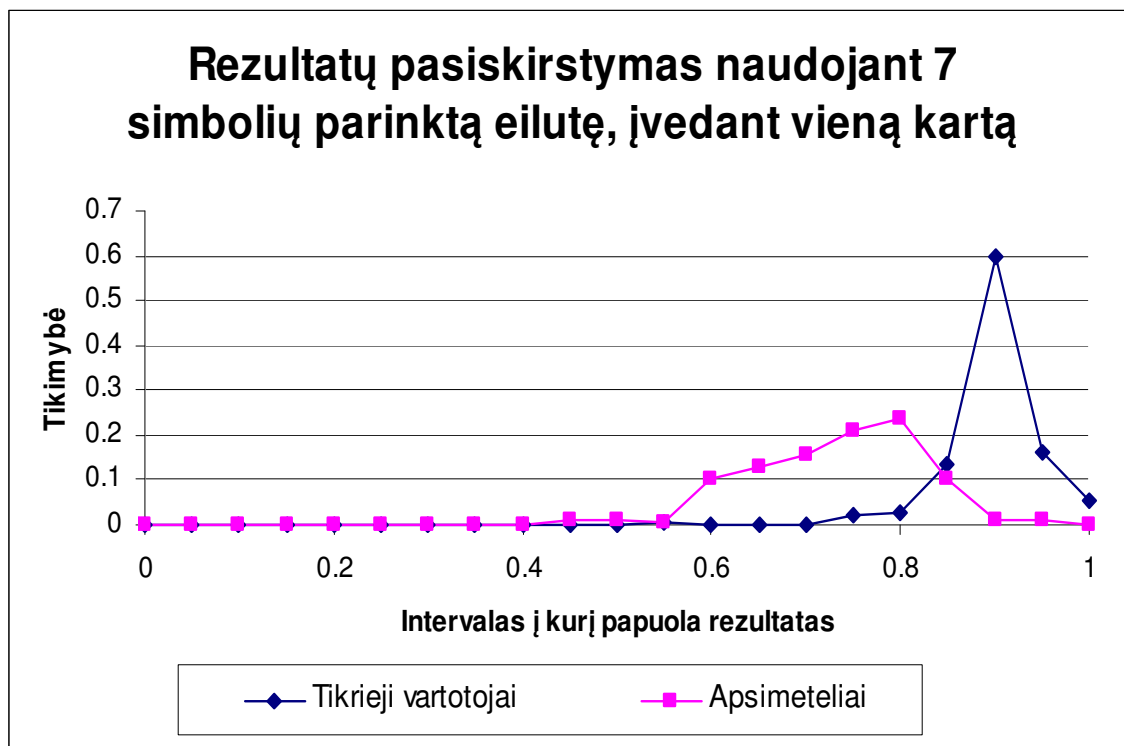
Eilutės ilgis - nuo 11 iki 15 simbolių;

Eilutė - laisvai pasirenkama;

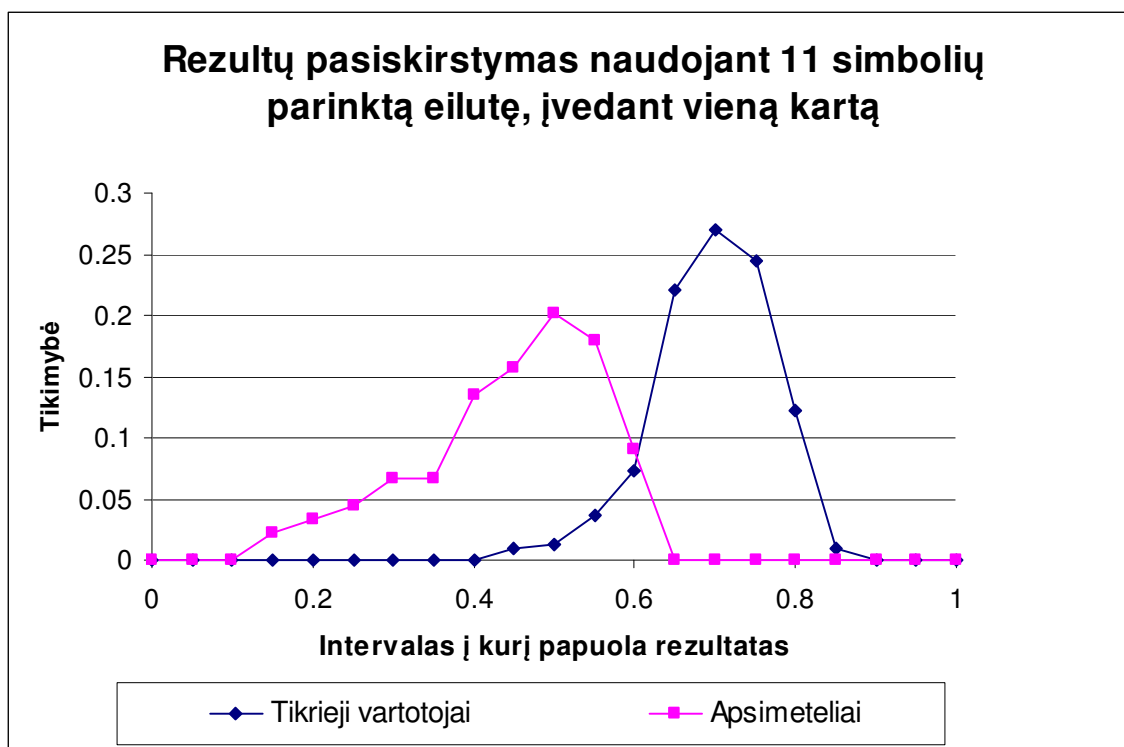
8. Rezultatai

Tyrimo metu buvo renkami duomenys ir įrašomi i duomenų bazę. Tyrime dalyvavo 10 žmonių, kurie užsiregistruodavo sistemoje, o vėliau įvesdavo analizuojamas eilutes kaip tikrieji vartotojai. Taip pat jie įvesdavo kitų įvestas eilutes, taip imituodami apsimetėlių prisijungimą.

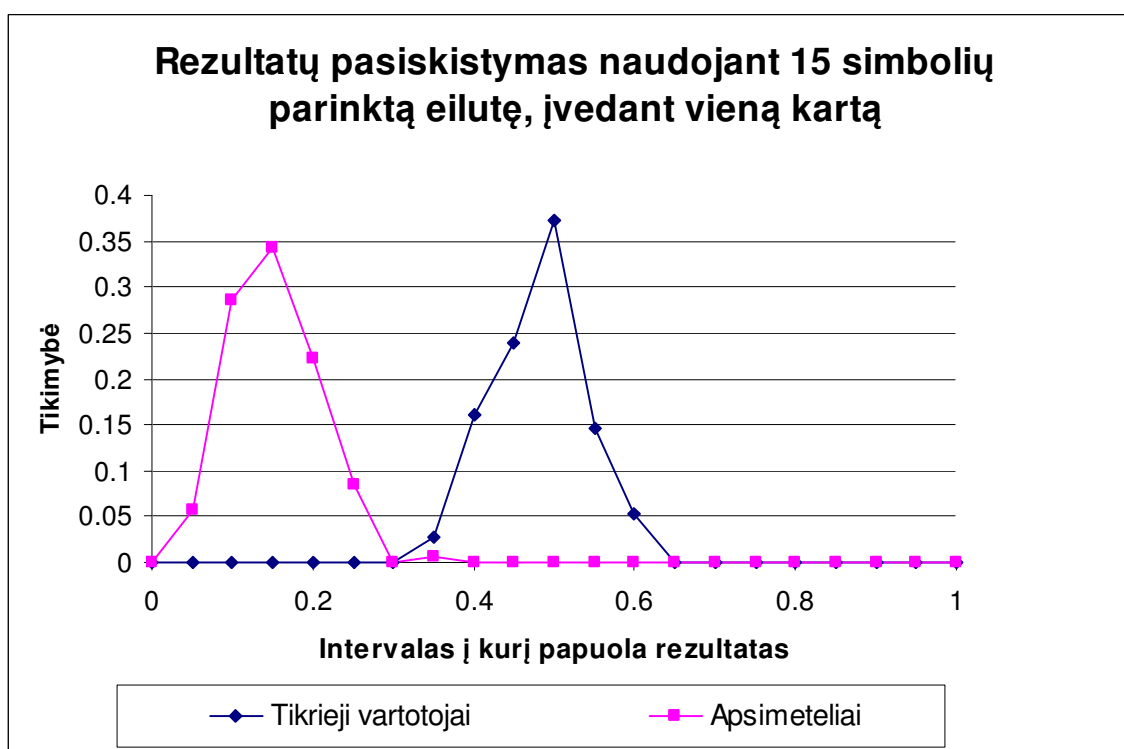
Atskirų variacijų rezultatai pateikti 17-34 paveiksluose.



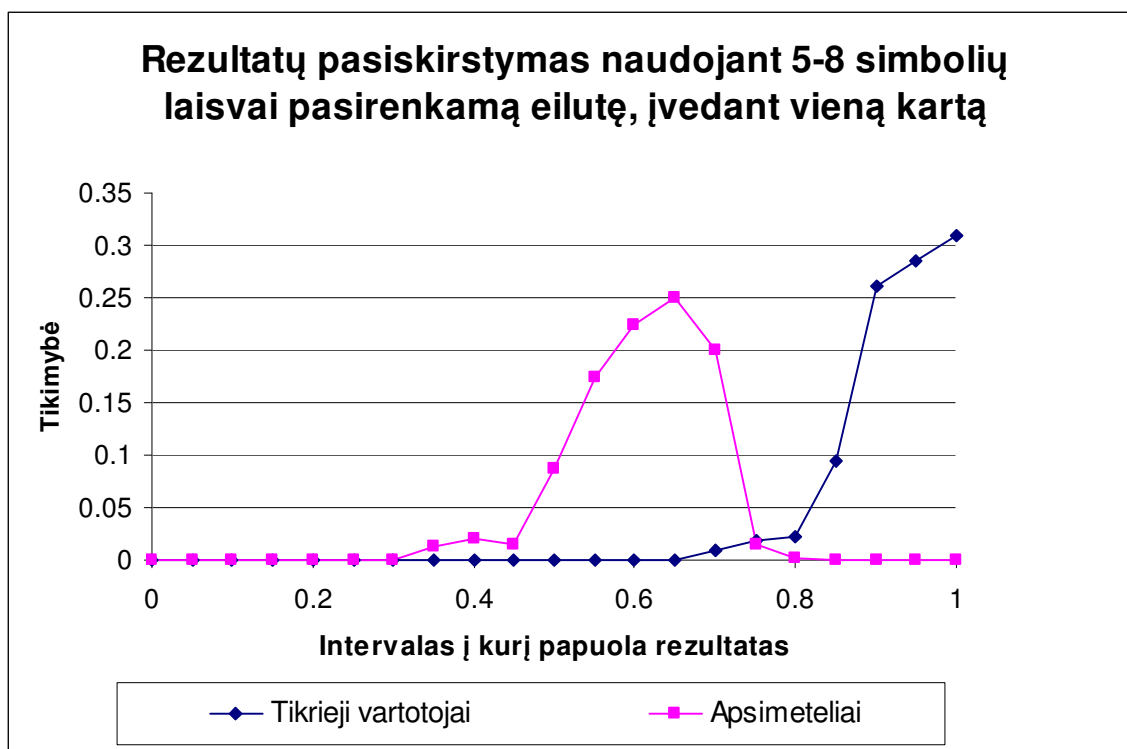
17 pav. Rezultatų pasiskirstymas naudojant 7 simbolių iš anksto parinktą eilutę, vartotojo registracijos metu, eilutę įvedant 1 kartą



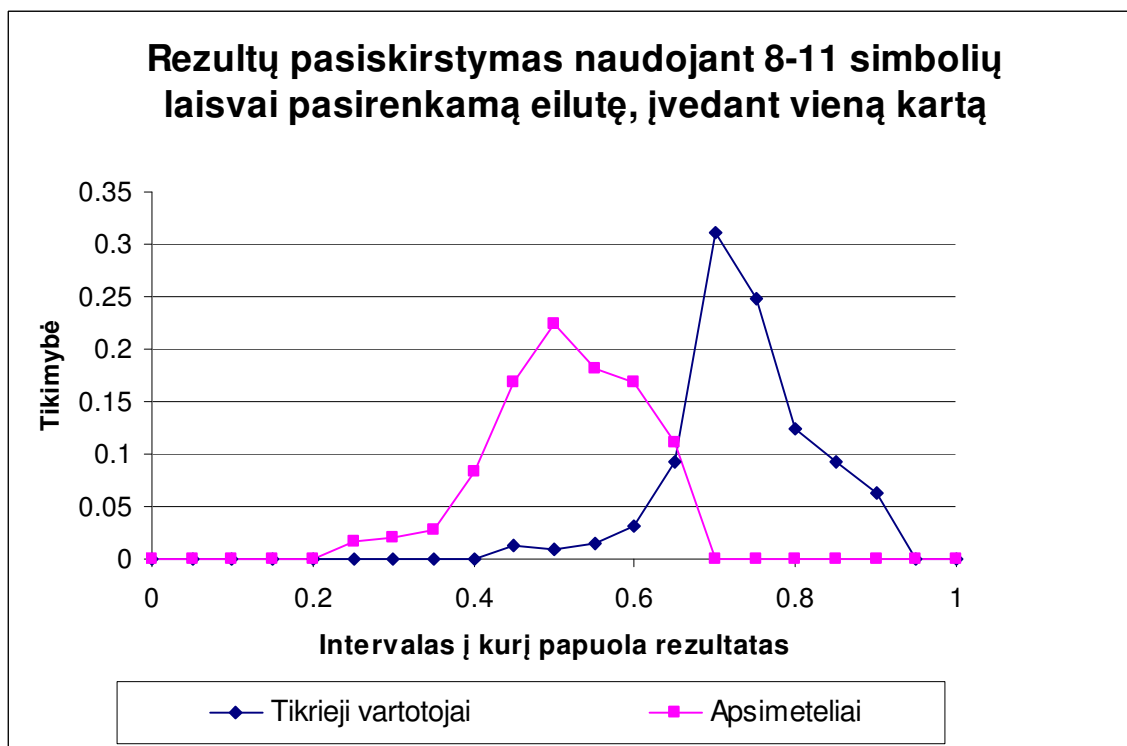
18 pav. Rezultatų pasiskirstymas naudojant 11 simbolių iš anksto parinktą eilutę, vartotojo registracijos metu, eilutę įvedant 1 kartą



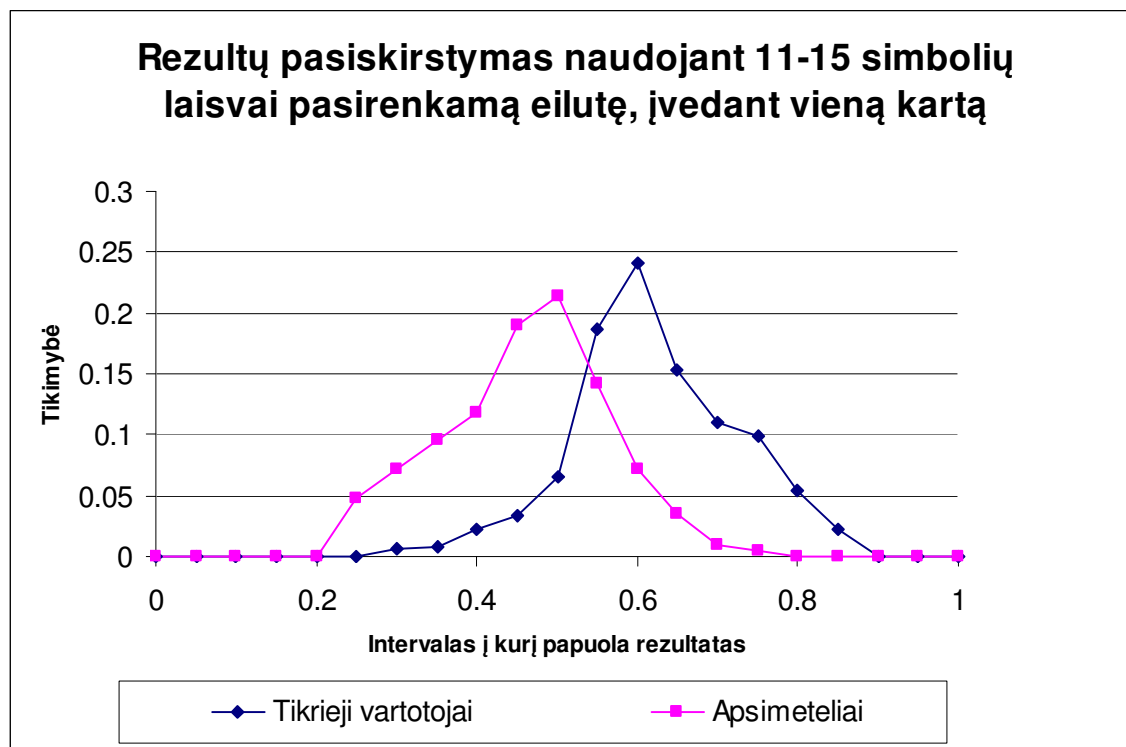
19 pav. Rezultatų pasiskirstymas naudojant 15 simbolių iš anksto parinktą eilutę, vartotojo registracijos metu, eilutę įvedant 1 kartą



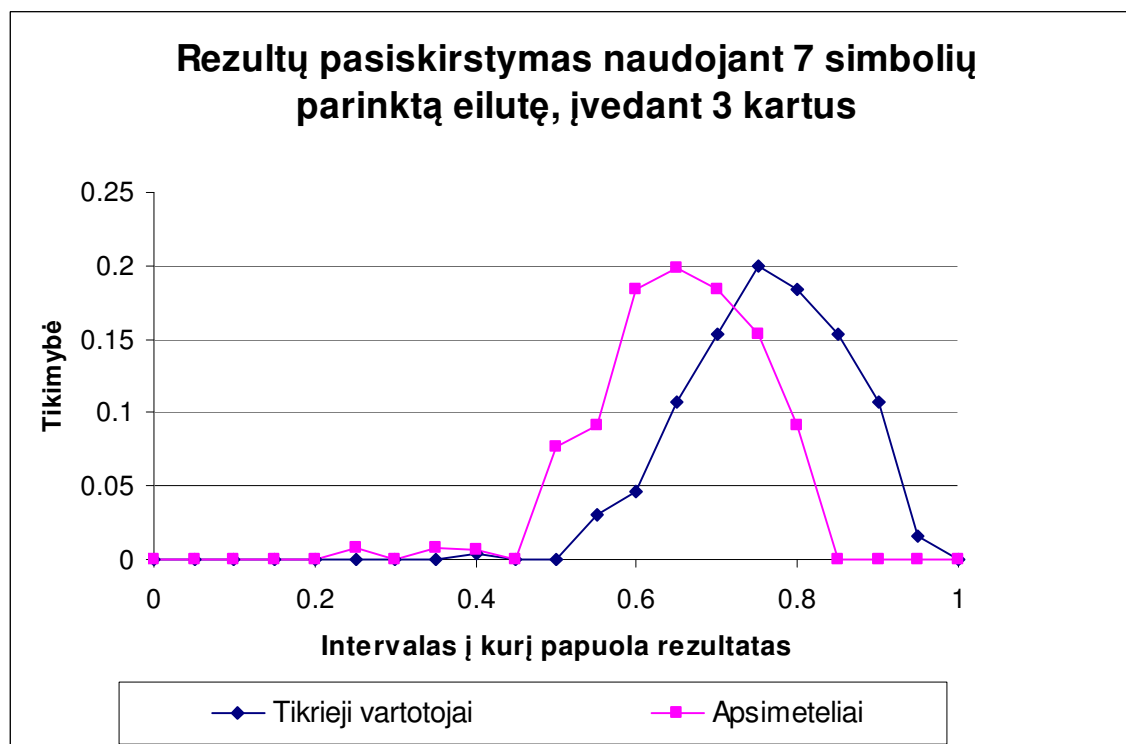
20 pav. Rezultatų pasiskirstymas naudojant 5-8 simbolių laisvai pasirenkamą eilutę, vartotojo registracijos metu, eilutę įvedant 1 kartą



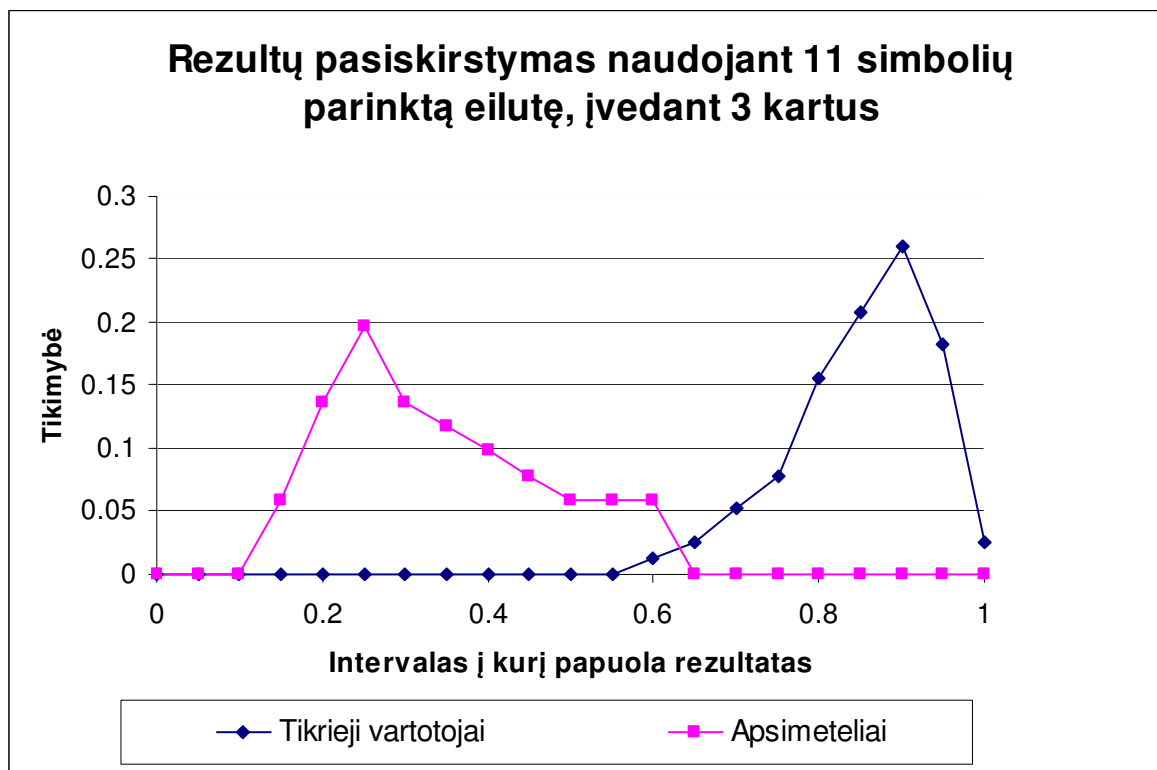
21 pav. Rezultatų pasiskirstymas naudojant 8-11 simbolių laisvai pasirenkamą eilutę, vartotojo registracijos metu, eilutę įvedant 1 kartą



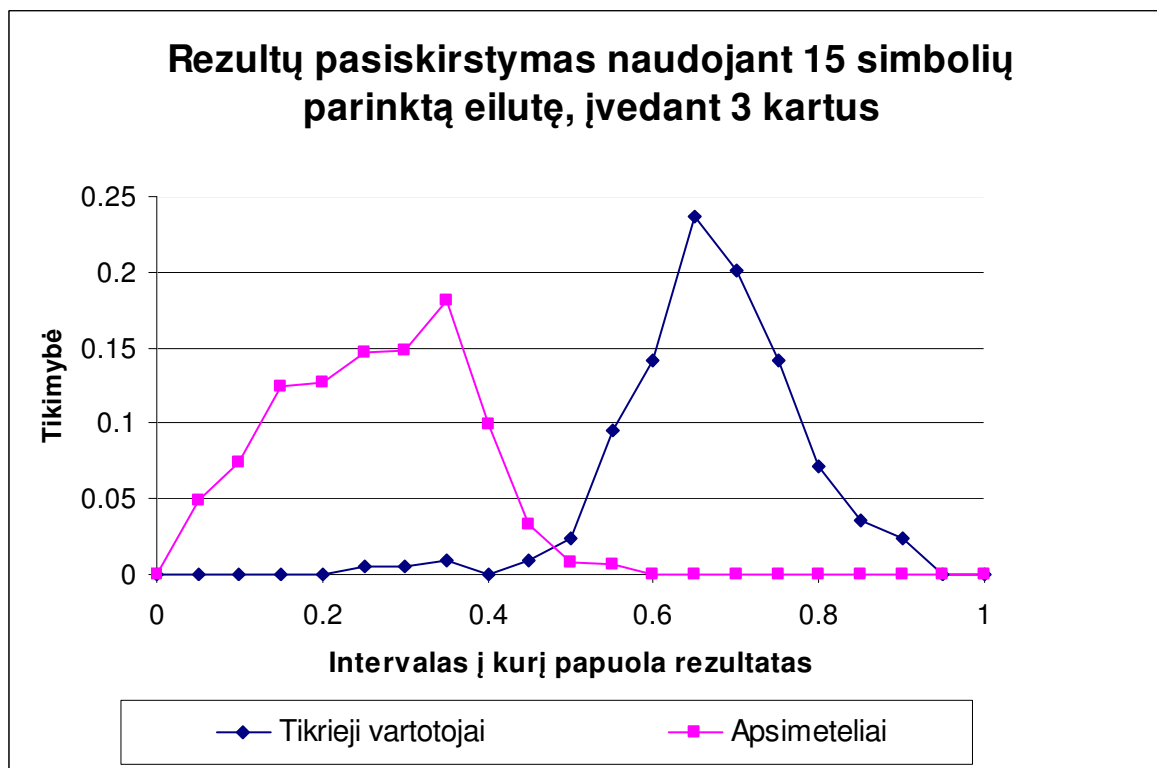
22 pav. Rezultatų pasiskirstymas naudojant 11-15 simbolių laisvai pasirenkamą eilutę, vartotojo registracijos metu, eilutę įvedant 1 kartą



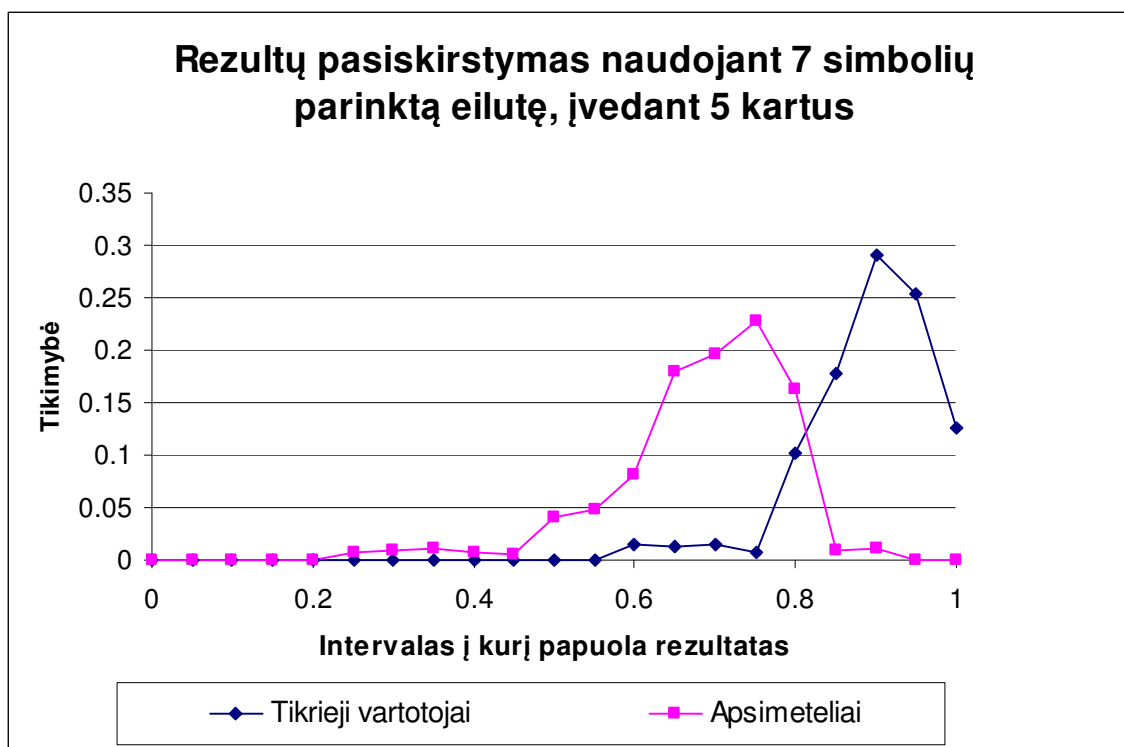
23 pav. Rezultatų pasiskirstymas naudojant 7 simbolių iš anksto parinktą eilutę, vartotojo registracijos metu, eilutę įvedant 3 kartus



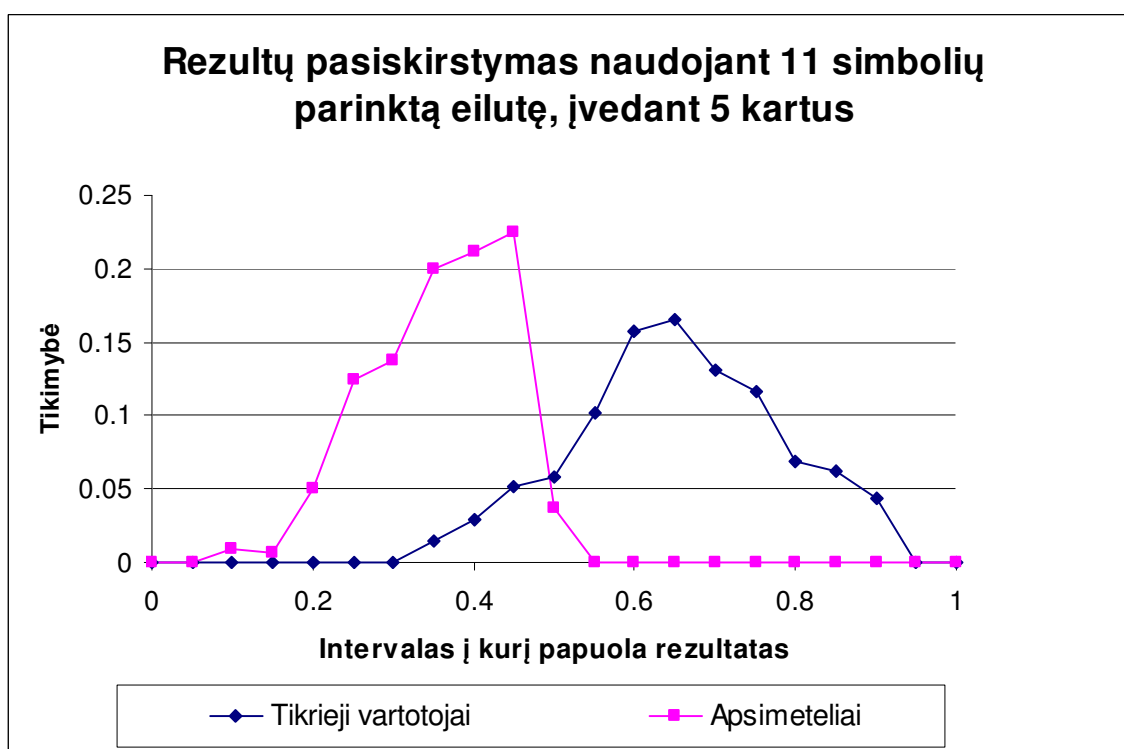
24 pav. Rezultatų pasiskirstymas naudojant 11 simbolių parinktą eilutę, vartotojo registracijos metu, eilutę įvedant 3 kartus



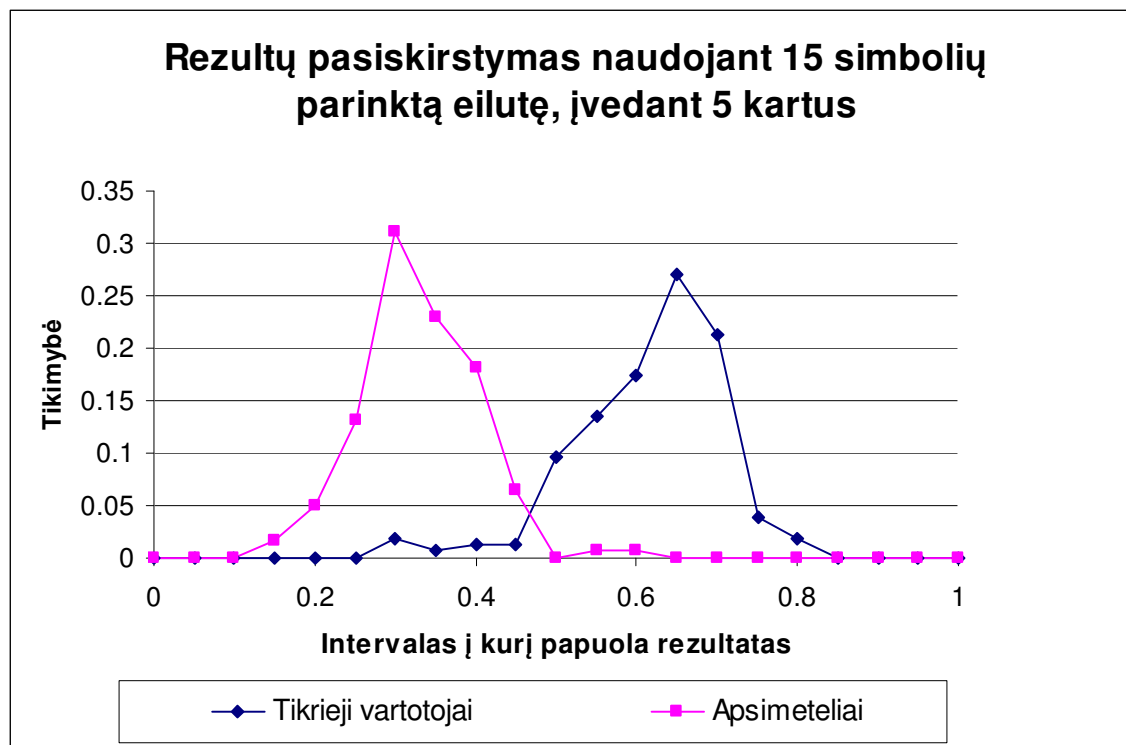
25 pav. Rezultatų pasiskirstymas naudojant 15 simbolių iš anksto parinktą eilutę, vartotojo registracijos metu, eilutę įvedant 3 kartus



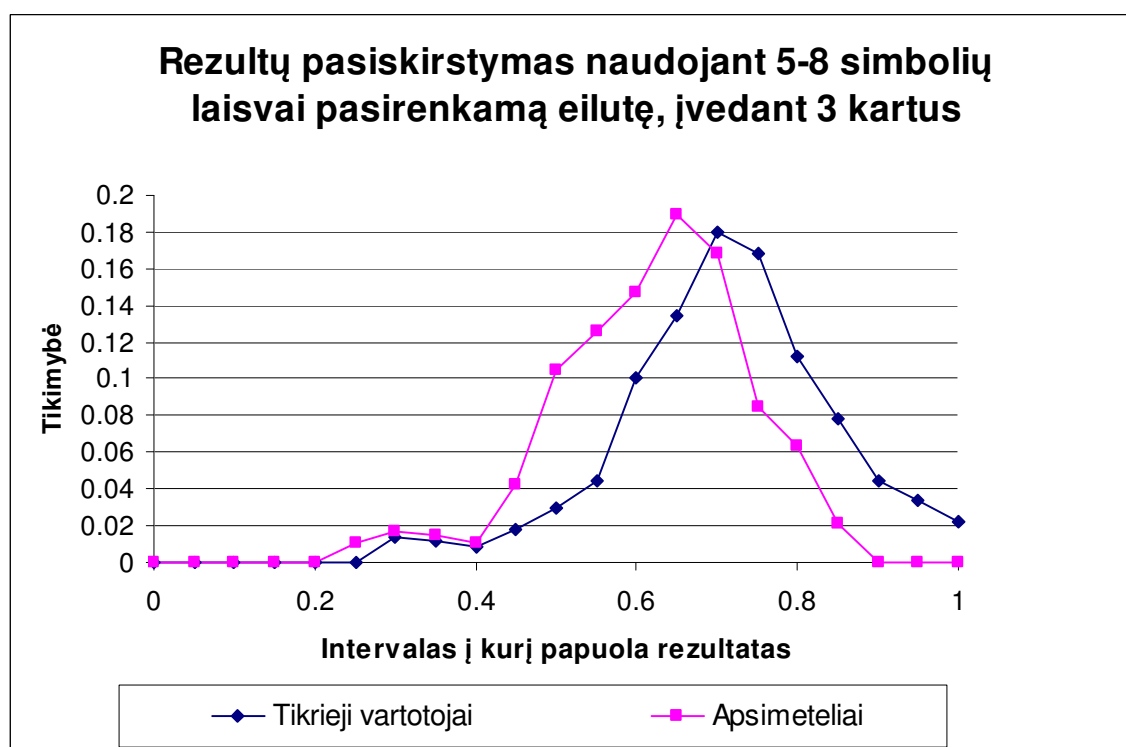
26 pav. Rezultatų pasiskirstymas naudojant 7 simbolių iš anksto parinktą eilutę, vartotojo registracijos metu, eilutę įvedant 5 kartus



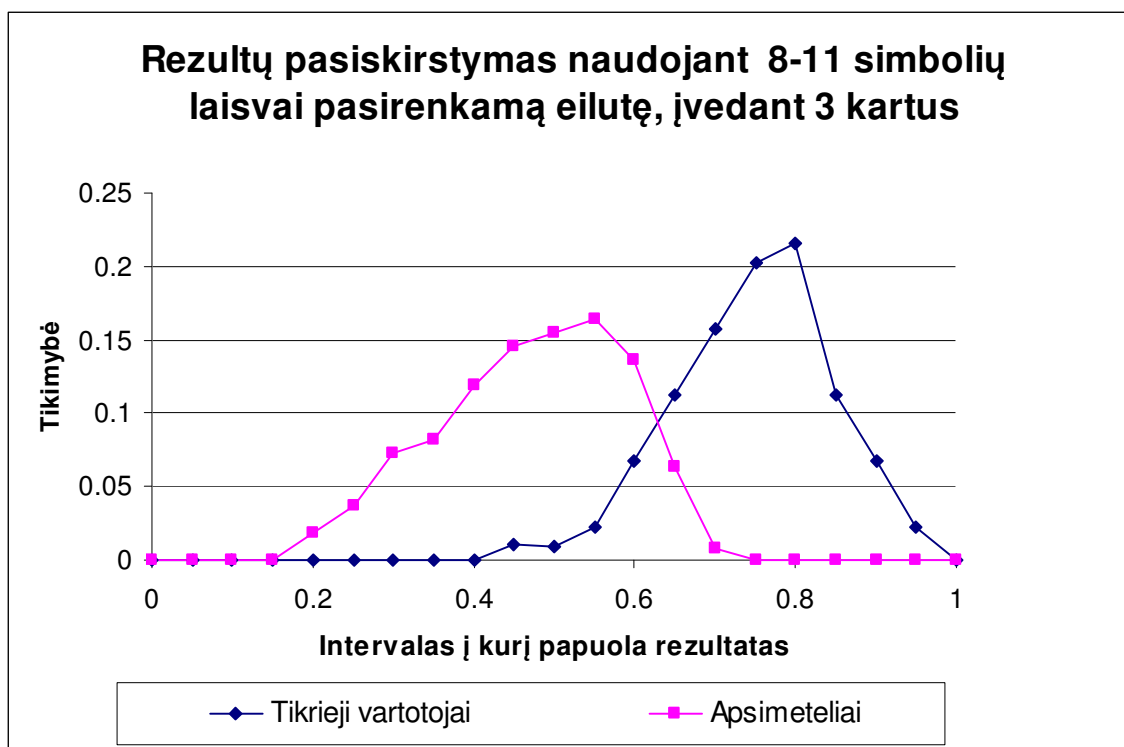
27 pav. Rezultatų pasiskirstymas naudojant 11 simbolių iš anksto parinktą eilutę, vartotojo registracijos metu, eilutę įvedant 5 kartus



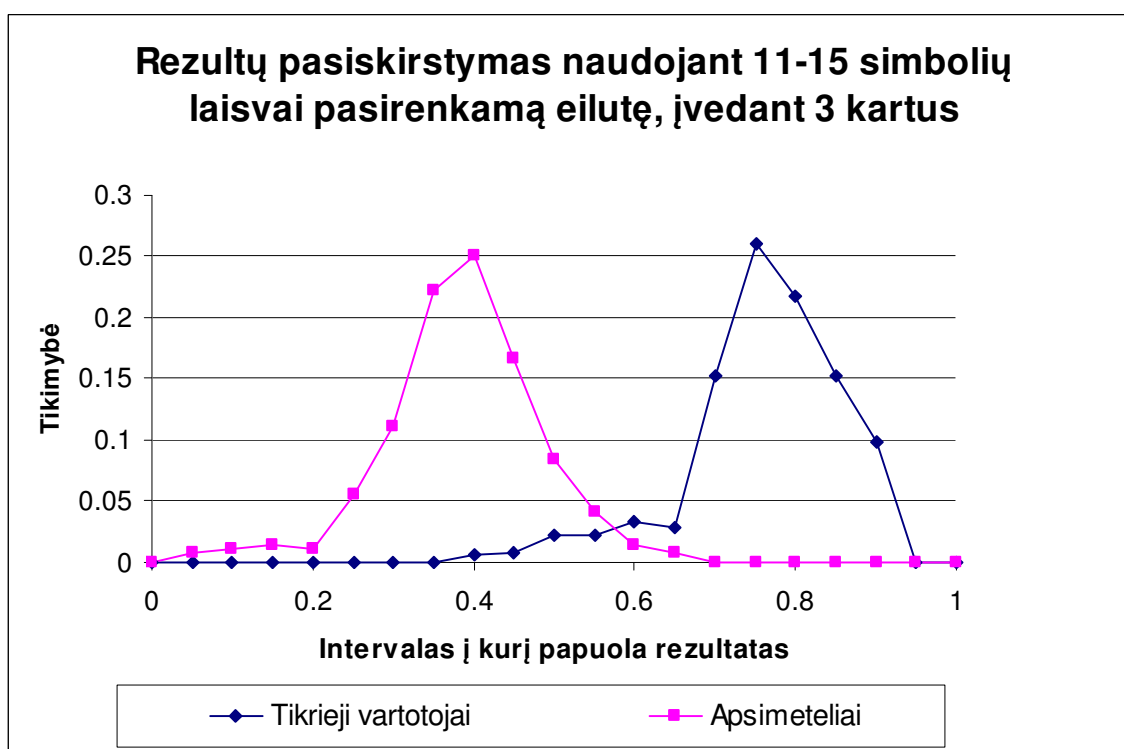
28 pav. Rezultatų pasiskirstymas naudojant 15 simbolių iš anksto parinktą eilutę, vartotojo registracijos metu, eilutę įvedant 5 kartus



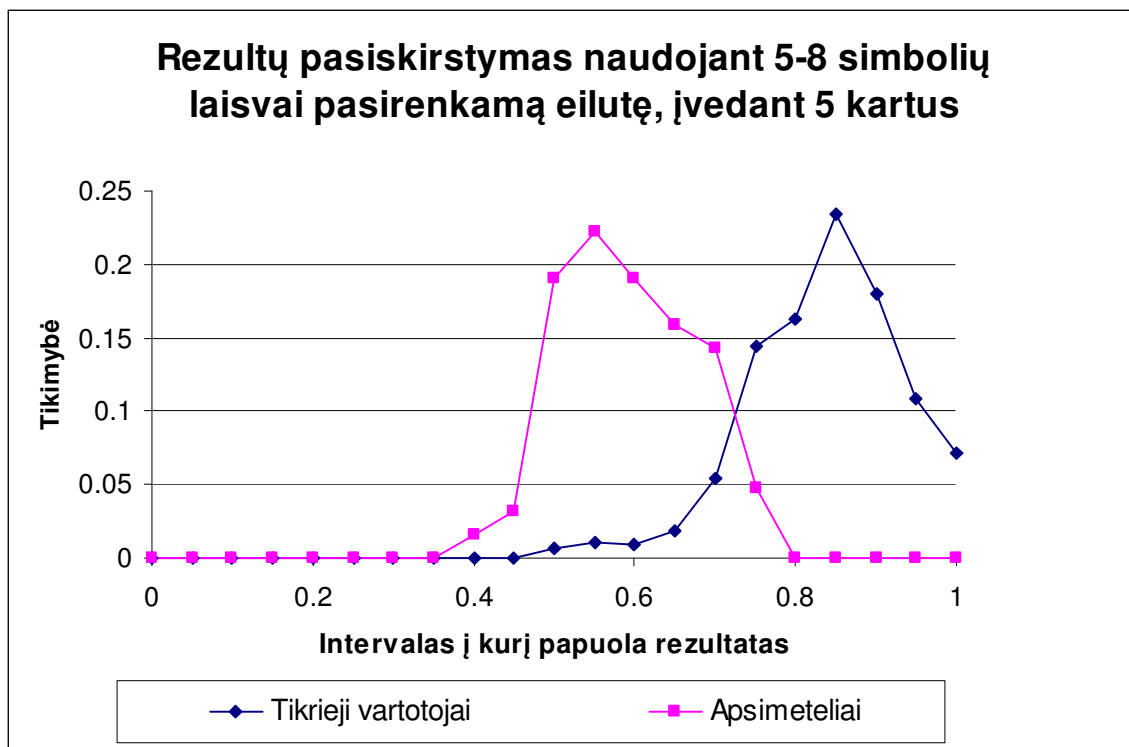
29 pav. Rezultatų pasiskirstymas naudojant 5-8 simbolių laisvai pasirenkamą eilutę, vartotojo registracijos metu, eilutę įvedant 5 kartus



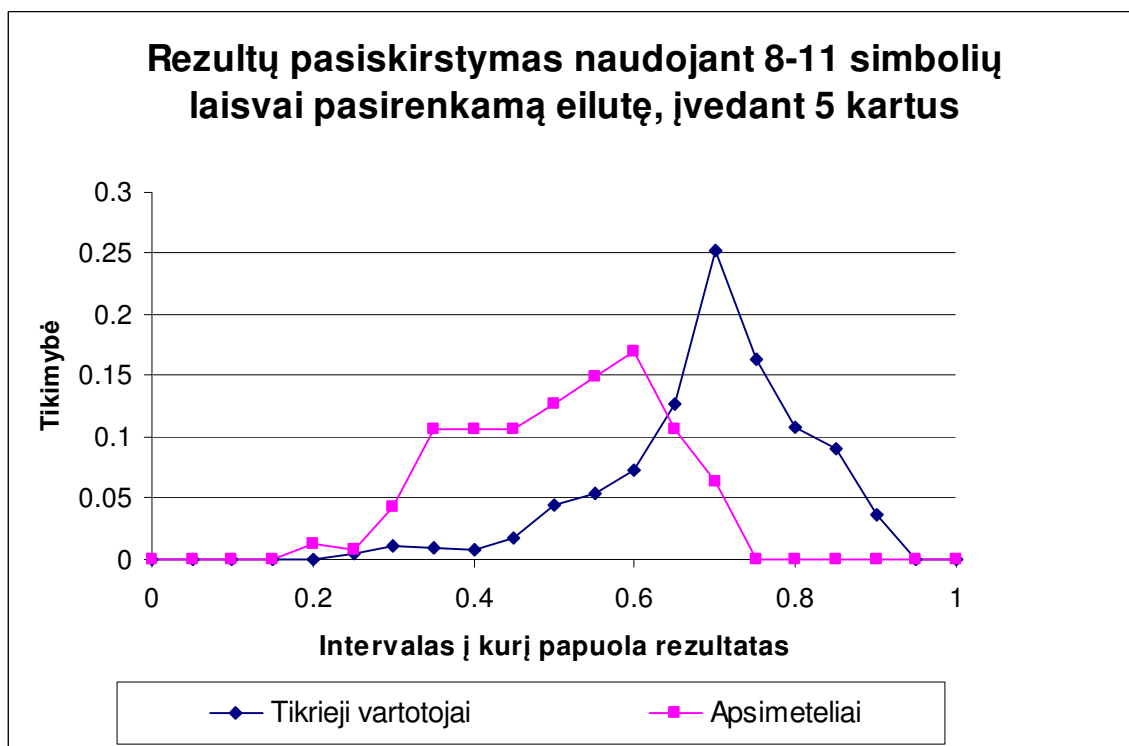
30 pav. Rezultatų pasiskirstymas naudojant 5-8 simbolių laisvai pasirenkamą eilutę, vartotojo registracijos metu, eilutę įvedant 5 kartus



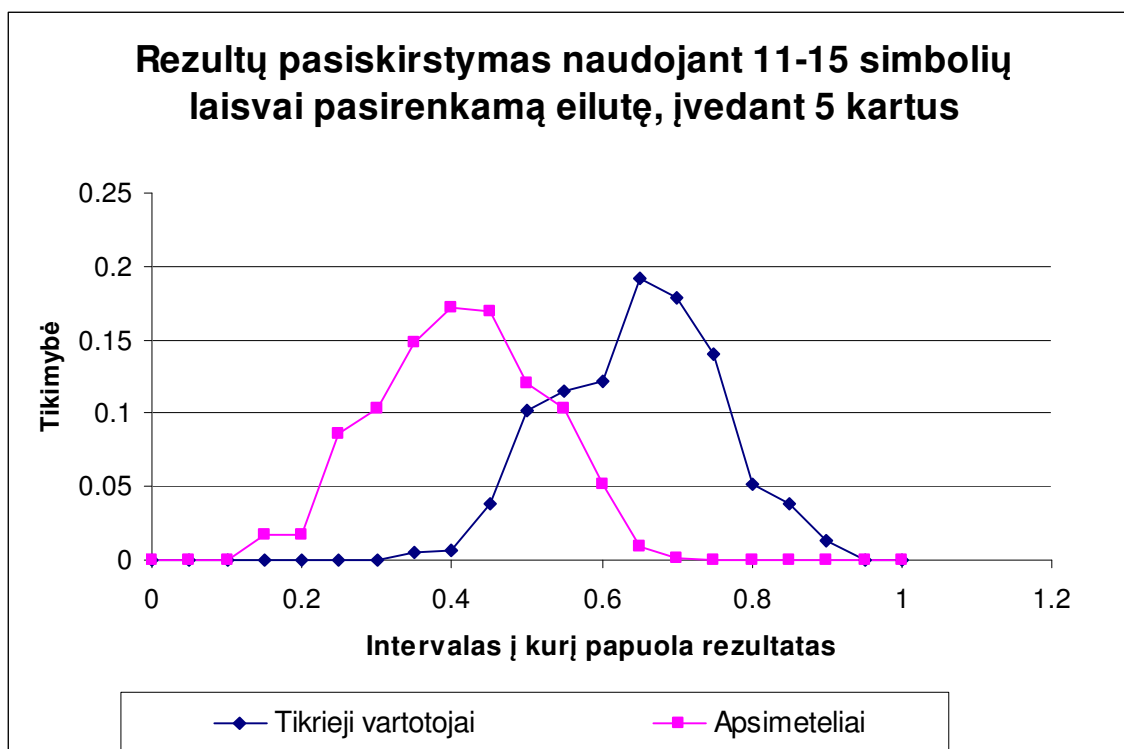
31 pav. Rezultatų pasiskirstymas naudojant 11-15 simbolių laisvai pasirenkamą eilutę, vartotojo registracijos metu, eilutę įvedant 3 kartus



32 pav. Rezultatų pasiskirstymas naudojant 5-8 simbolių laisvai pasirenkamą eilutę, vartotojo registracijos metu, eilutę įvedant 5 kartus



33 pav. Rezultatų pasiskirstymas naudojant 8-11 simbolių laisvai pasirenkamą eilutę, vartotojo registracijos metu, eilutę įvedant 5 kartus



34 pav. Rezultatų pasiskirstymas naudojant 11-15 simbolių laisvai pasirenkamą eilutę, vartotojo registracijos metu, eilutę įvedant 5 kartus

Tiriant skirtingas klavišų paspaudimo analizės dalis, lyginami skirtingi grafikai. Priimant sprendimą, kuriuo atveju buvo gautas geresnis rezultatas, kreipiamas dėmesys į tai, kaip tikrųjų vartotojų kreivė skiriasi nuo apsimetėlių kreivės. Tuo atveju, kai kreivės persikloja, buvo lyginama, kuriuo atveju didesnė tikimybė įvykti II-ojo tipo klaidai. Kuo staigiau leidžiasi žemyn apsimetėlių kreivės dešinysis kraštas, tuo ši tikimybė yra mažesnė. Kadangi I-ojo tipo klaida yra toleruojama ir dauguma atvejų neišvengiama, į ją buvo atsižvelgta tik esant panašiai tikimybei įvykti II-ojo tipo klaidai.

Tiriant, kas geriau: vartotojui leisti pačiam pasirinkti įvedamą eilutę ar iš anksto parinkti eilutę, buvo lyginami rezultatai, gauti iš anksto parinktos eilutės atveju, su rezultatais, gautais naudojant panašaus ilgio pačių vartotojų pasirinktą eilutę. Apibendrinti rezultatai yra pateikti 4-oje lentelėje.

4 lentelė. Rezultatų palyginimas tiriant skirtumus tarp vartotojų pasirinktų eilučių ir iš anksto parinktų eilučių, registracijos metu eilutę įvedant vieną kartą

Iš anksto parinktos eilutės ilgis	Pasirenkamos eilutės ilgio kitimo intervalas	Geriausias rezultatas
7	5-8	5-8 intervalas
11	8-11	Nėra didelio skirtumo
15	11-15	15 simbolių parinkta eilutė

Galima pastebėti, kad esant trumpai eilutei geresni rezultatai yra leidžiant vartotojams patiems pasirinkti eilutes, tačiau, padidinus eilutės ilgį, geresni rezultatai buvo gauti naudojant iš anksto parinktą eilutę. Tai galima paaiškinti tuo, kad vartotojams pavykdavo sugalvoti trumpas eilutes, nes jie stengėsi sugalvoti eilutes su žodžiais, kurie yra jiems įprasti. Tačiau ilgesnes eilutes sugalvoti sekėsi blogiau, nes ilgesni žodžiai yra rečiau naudojami (Ši pastaba buvo išsakyta ir daugelio tyrimo dalyvių).

Panašūs rezultatai gaunami vartotojo registracijos metu eilutę įvedant 1 kartą (4 lentelė), 3 kartus (5 lentelė) ir 5 kartus (6 lentelė).

5 lentelė. Rezultatų palyginimas tiriant skirtumus tarp vartotojų pasirinktų eilučių ir iš anksto parinktų eilučių, registracijos metu eilutę įvedant tris kartus

Iš anksto parinktos eilutės ilgis	Pasirenkamos eilutės ilgio kitimo intervalas	Geriausias rezultatas
7	5-8	Naudojant abu variantus gauti labai prasti rezultatai
11	8-11	11 simbolių parinkta eilutė
15	11-15	15 simbolių parinkta eilutė

6 lentelė. Rezultatų palyginimas tiriant skirtumus tarp vartotojų pasirinktų eilučių ir iš anksto parinktų eilučių, registracijos metu eilutę įvedant penkis kartus

Iš anksto parinktos eilutės ilgis	Pasirenkamos eilutės ilgio kitimo intervalas	Geriausias rezultatas
7	5-8	5-8 intervalas
11	8-11	11 simbolių parinkta eilutė
15	11-15	15 simbolių parinkta eilutė

Tiriant, kiek kartų įvedus eilutę vartotojo registracijos metu gaunamas geriausias rezultatas, buvo lyginami rezultatai, gauti naudojant tokio pat ilgio eilutę įvedant skirtingą skaičių kartų. Rezultatai iš anksto parinktos eilutės atveju pateikti 7 lentelėje.

7 lentelė. Rezultatų palyginimas registracijos metu eilutę vedant 1, 3 ir 5 kartus, rezultatai pateikti naudojant iš anksto parinktas eilutes

Naudotas eilutės ilgis	Kiek kartų vedama eilutė registruojant vartotoją			Komentaras
	1	3	5	
7 simbolių	+			
11 simbolių	+	+		Blogiausia įvedant 5 kartus
15 simbolių	+			

Naudojant iš anksto parinktą eilutę, geriausi rezultatai gaunami įvedant vieną kartą. Naudojant 11 simbolių eilutę, registracijos metu įvedus vieną kartą ir įvedus tris kartus gauti rezultatai buvo gana panašūs. Analogiški rezultatai gaunami ir naudojant pačių vartotojų pasirinktas eilutes. Jie pateikti 8-oje lentelėje.

8 lentelė. Rezultatų palyginimas registracijos metu eilutę vedant 1, 3 ir 5 kartus, rezultatai pateikti naudojant vartotojų laisvai pasirinktas eilutes

Naudotas eilutės ilgio intervalas	Kiek kartų vedama eilutė registruojant vartotoją			Komentaras
	1	3	5	
5-8 simbolių		+		
8-11 simbolių	+	+	+	Visi rezultatai gana panašūs
11-15 simbolių		+		

Naudojant vartotojų laisvai pasirinktas eilutes situacija truputį pasikeitė. Daugeliu atvejų geriausi rezultatai buvo gauti registracijos metu įvedant tris kartus. Naudojant 8-11 ilgio eilutes gauti rezultatai įvedant vieną, tris ir penkis kartus yra gana panašūs. Kadangi daugeliu atvejų parinkta eilutė vartotojams nebuvo dažnai naudojama, įvedus ją tris kartus įvesties charakteristikos būdavo labiau charakterizuojančios konkretų vartotoją. Galima teigti, kad įvedant 5 kartus rezultatai ne tik nepagerėjo,

bet ir pablogėjo. Panašią nuomonę išsakė ir tyrimo dalyviai. Jų teigimu, daug kartų įvedant eilutę, jos vedimo charakteristikos pasikeičia, todėl vedant prisijungimo metu, gaunami rezultatai buvo blogesni.

Tiriant, kokio ilgio įvedamą eilutę naudojant gaunami geriausi rezultatai, buvo lyginami rezultatai, gauti naudojant skirtingų ilgių eilutes. Rezultatai naudojant iš anksto parinktas eilutes pateikti 9 lentelėje.

9 lentelė. Rezultatų palyginimas naudojant skirtingo ilgio, iš anksto parinktas eilutes

Kiek kartų vedama eilutė registruojant vartotoją	Naudotas eilutės ilgis			Komentaras
	7	11	15	
1			+	
3		+	+	Šiek tiek geresnis rezultatas naudojant 11 simbolių ilgio eilutę
5		+	+	Šiek tiek geresnis rezultatas naudojant 15 simbolių ilgio eilutę

Rezultatai yra geresni naudojant ilgesnes eilutes. Taip pat matoma, kad daugiau kartų įvedant eilutę registracijos metu, geresnis rezultatas gaunamas naudojant ilgesnes eilutes.

Visiškai skirtingi rezultatai, naudojant pačių vartotojų sugalvotas eilutes. Rezultatai pateikti 10-oje lentelėje.

10 lentelė. Rezultatų palyginimas naudojant skirtingo ilgio vartotojų laisvai pasirinktas eilutes

Kiek kartų vedama eilutė registruojant vartotoją	Naudotas eilutės ilgio intervalas			Komentaras
	5-8	8-11	11-15	
1	+			
3			+	
5	+			Kuo ilgesnė eilutė tuo prastesnis rezultatas

Matoma, kad registracijos metu įvedant eilutę tik vieną arba penkis kartus, geriausias rezultatas gaunamas naudojant trumpesnes eilutes. Tačiau registracijos metu įvedant tris kartus, gaunami visiškai priešingi rezultatai. Rezultatai geriausi naudojant ilgesnes eilutes. Tokius rezultatus galima paaiškinti tuo, kad sugalvojus savo eilutę yra sunku iš pirmo karto ją įvesti taip, kad po to lengvai būtų galima pakartoti ir gauti pakankamai gerus rezultatus, todėl registracijos metu vedant tik vieną kartą geresni rezultatai buvo gauti vedant nesudėtingas eilutes. Ilgos eilutės dažnai būdavo nepakankamai įprastos vartotojams.

Registracijos metu vedant eilutę penkis kartus dažnai paskutinių vedimų charakteristikos pasikeisdavo taip, kad rezultatai vedant eilutę prisijungimo metu būdavo gaunamas gana mažas koreliacijos rezultatas.

Kadangi jau anksčiau buvo nustatyta, kad geriausi rezultatai gaunami registracijos metu eilutę įvedant tris kartus, tai nenuostabu, kad, įvedant būtent tris kartus, geriausias rezultatas gaunamas įvedant ilgas eilutes. Įvedant tris kartus įvesties charakteristikos yra geriausiai apibūdinančios vartotojo klavišų paspaudimo ypatybės. Negana to, naudojant ilgesnę eilutę apsimetėliui daug sunkiau apsimesti kitu asmeniu, nes ilgesnėje eilutėje yra daugiau biometrinės informacijos nei trumpoje.

Matoma, kad gaunami rezultatai labai ryškiai pasikeičia, pakeitus tik vieną iš sudedamųjų sistemos dalių. Taigi nustatyti, koks yra optimaliausias naudojamos eilutės ilgis negalima, nes tai labai priklauso nuo kitų sistemos sudedamųjų dalių.

Žiūrėdami ne į atskiras klavišų paspaudimo analizės sistemos dalis, o į konkrečias variacijas, galime iš visų 18 variacijų atrinkti tas, kurios yra labiausiai tinkamos naudoti realioje sistemoje (tikintis teigiamų rezultatų).

Tinkamos tokios variacijos:

- Registracijos metu naudojama vartotojo sugalvota eilutė, kurios ilgis yra nuo 5 iki 8 simbolių, registracijos metu eilutė įvedama vieną kartą.
- Registracijos metu naudojama vartotojo sugalvota eilutė, kurios ilgis yra nuo 11 iki 15 simbolių, registracijos metu eilutė įvedama tris kartus.
- Registracijos metu naudojama iš anksto parinkta 11 simbolių ilgio eilutė, kuri registracijos metu įvedama 3 kartus.
- Registracijos metu naudojama iš anksto parinkta 15 simbolių ilgio eilutė, kuri registracijos metu įvedama 1 kartą.
- Registracijos metu naudojama iš anksto parinkta 15 simbolių ilgio eilutė, kuri registracijos metu įvedama 3 kartus.
- Registracijos metu naudojama iš anksto parinkta 15 simbolių ilgio eilutė, kuri registracijos metu įvedama 5 kartus.

9. Išvados

Darbe aptartos pagrindinės kliento pusės pažaidos: slaptažodžių žvejybos bei MITM atakos. Apžvelgti metodai, naudojami vykdant slaptažodžių žvejybos atakas, ir MITM atakos specifi­ka. Taip pat analizuojant slaptažodžių žvejybos atakų statistinius duomenis įsitikinta, kad atakų apimtis bei daromi nuostoliai vis didėja.

Aptartos daugumos elektroninių komercijos sistemų naudojamos klientų apsaugos priemonės.

Aprašyta pasirinkta klientų apsaugos priemonė - klavišų paspaudimo analizė.

Atlikus tyrimą, nustatyta, kaip keičiasi klavišų analizės panaudojimo realioje sistemoje galimybės, keičiant tam tikras sudedamąsias sistemos dalis. Nustatyta, kad:

- didinant įvesčių skaičių vartotojo registracijos metu, efektyvumas kyla tik iki tam tikros ribos, vėliau jis ima kristi;
- naudojant vartotojų pasirinktas eilutes, geriausi rezultatai gaunami registracijos metu eilutę įvedant tirs kartus;
- naudojant iš anksto parinktas eilutes, geriausi rezultatai gaunami registracijos metu eilutę įvedant vieną kartą;
- naudojant iš anksto parinktas eilutes, sistema yra stabilesnė ir ne tokia jautri tam tikrų dalių pakeitimui;
- naudojant iš anksto parinktas eilutes, geresni rezultatai gaunami naudojant ilgesnes eilutes;
- vieno iš elementų įtaka rezultatui labai priklauso nuo to, kokie kiti elementai kartu naudojami;

Naudojant klavišų paspaudimo analizę, tinkamai parinkus sistemos sudedamąsias dalis, galima padidinti sistemos saugą. Tačiau tai gali būti naudojama tik kaip pagalbinė apsaugos priemonė, visiško saugumo ji užtikrinti negali.

Taip pat rekomenduojama ją naudoti tik tokiose sistemose, kur būtinas labai aukštas saugos lygis, nes dažna eilutės įvestis gali padaryti sistemą nepatrauklią vartotojui.

10.Literatūros sąrašas

1. 16–74 m. amžiaus asmenys, kurie naudojami e. prekyba asmeniniais tikslais.[interaktyvus] Statistikos Departamentas Prie Lietuvos Respublikos Vyriausybės [žiureta 2010-03-04]. Prieiga per internetą: <http://db1.stat.gov.lt/statbank/SelectVarVal/Define.asp?Maintable=M9020205&PLanguage=0>
2. Biometrics.[interaktyvus] Vikipedija laisvoji enciklopedija [žiureta 2010-04-17]. Prieiga per internetą: <http://en.wikipedia.org/wiki/Biometrics>
3. Dhamija, R., Tygar, J.D. The Battle Against Phishing: Dynamic Security Skins, 12 p.
4. Identity Theft Statistics 2010 .[interaktyvus] Identity Theft Labs [žiureta 2010-04-10]. Prieiga per internetą: <http://www.identitytheftlabs.com/identity-theft/identity-theft-statistics-2010/>
5. Killourhy, K., Maxion, R. Comparing Anomaly-Detection algorithms for keystroke dynamics, 10 p.
6. Luman, R. Dynamic Keystroke Analysis via Genetic Algorithms. 10 p.
7. Man-in-the-middle attack [interaktyvus] The Open Web Application Security Project[žiureta 2010-02-10]. Prieiga per internetą: http://www.owasp.org/index.php/Man-in-the-middle_attack
8. Monroe, F., Rubin A. D. Keystroke Dynamics as a Biometric for Authentication, 15 p.
9. Moore, T., Clayton R. Examining the Impact of Website Take-down on Phishing, 13 p.
10. Nuostoliai dėl nusikaltimų elektroninėje erdve sparčiai auga, [interaktyvus] Verslo naujienos [žiureta 2010-03-17]. Prieiga per internetą: http://vz.lt/rss/straipsnis/2010/03/16/Nuostoliai_dėl_nusikaltimų_elektroninėje_erdveje_sparci
11. Olzak, T. Keystroke Dynamics: Low Impact Biometric Verification , 2006 m. rugsejis. 10 p.
12. Protecting consumers against phishing attacks. Gatepoint research. 5 p.
13. Rasmussen, R., Aaron, G. Global Phishing Survey: Trends and Domain Name Use in 1H2008, 23 p.
14. Rasmussen, R., Aaron, G. Global Phishing Survey: Trends and Domain Name Use in 1H2009, 30 p.
15. Rasmussen, R., Aaron, G. Global Phishing Survey: Trends and Domain Name Use in 2H2008, 26 p.
16. Saltzman, R., Sharabani, A. Active Man in the Middle Attacks, A whitepaper from IBM Rational Application Security Group, 2009 m. Vasaris, 18 p.
17. Shirey, R. Internet Security Glossary, 212 p.

18. Spyware Resistant Web Authentication Using Virtual Machines 19 p.
19. Statistics about phishing activity and PhishTank usage, [interaktyvus] Phishtank.com [žiureta 2009-05-24]. Prieiga per internetą: <http://www.phishtank.com/stats/2009/02/>
20. The Evolving Threat: Combat training for the new era of malicious code, IBM Internet Security Systems 17 p.
21. Wells, J., Hutchinson, D., Pierce, J. Enhanced Security for Preventing Man-in-the-Middle Attacks in Authentication, Data Entry and Transaction Verification, 13 p.
22. Wu, M., Miller, R., Simson, L. Do Security Toolbars Actually Prevent Phishing Attacks? 10 p.