

Швець М.В., магістрант, Вербицький В.Г., професор, науковий керівник,
Безверхий А.І., доцент, консультант

ДОСЛІДЖЕННЯ ТА РОЗРОБКА МЕТОДІВ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА ІНТЕРНЕТУ ЗА ПАТЕРНОМ ПОВЕДІНКИ

Запорізька державна інженерна академія, кафедра ПЗАС

У сучасному світі, що центрований в Інтернеті, задача автентифікації та ідентифікації користувачів стала важливішою ніж коли-небудь раніше.

Проблеми ідентифікації і автентифікації є основними при побудові систем розмежування доступу, які, в свою чергу, грають ключову роль в системах забезпечення інформаційної безпеки. В сучасних інформаційних системах, як правило, застосовуються способи ідентифікації, засновані на інформації про IP-адреси комп'ютерів відвідувачів і зберігання на комп'ютері користувача даних Cookie [1,2]. Істотним недоліком цих методів є ототожнення користувача і його комп'ютера або браузера, що не завжди коректно. За результатами останніх досліджень, частка багатокористувацьких комп'ютерів варіюється від 20 до 40 відсотків [3].

Метою даної роботи є розробка методу, який дозволяє ідентифікувати користувачів, які здійснюють доступ в мережу Інтернет за але не являються ідентифікованими чи авторизованими у веб застосунку. Для вирішення даного завдання в роботі використані дані користувача, які будуть унікальними для кожної людини і не залежатимуть від обчислювальної платформи. Біометрична ідентифікація перевіряє користувача на основі властивих йому унікальних характеристиках. На додаток до фізіологічної біометрії, поведінкова біометрія є дуже корисною для ідентифікації користувача. Динаміка миші, та її унікальна закономірність рухів миші є однією з таких поведінкових біометрій. У цій роботі я перевірю ідентифікацію користувача системи, що використовує динаміку миші та клавіатури що є одночасно точним і достатньо ефективним методом для майбутнього використання. Щоб можна було використовувати даний метод на практиці, він повинен мати такі особливості:

Точність. Необхідно точно ідентифікувати людину серед інших користувачів. Також даний метод повинен використовувати дані, які будуть унікальними для кожної людини, щоб легше було ідентифікувати різних користувачів навіть на одному комп'ютері.

Швидка відповідь. Система повинна зробити швидку перевірку користувача. Іншими словами, це повинно бути в змозі відрізнити користувача своєчасно.

Основний принцип автентифікації чи ідентифікації користувачів на основі біометричних засобів зосереджений на "хто ти". Це відрізняється від звичайних підходів до автентифікації та ідентифікації користувачів, які є в основному, на основі "те, що у вас є" або "що ви знаєте". На жаль, фізичний об'єкт, такий як ключ або ідентифікаційна картка можуть бути втрачені або вкрадені. Точно так само як пароль. [5, 6] І навпаки, біометричний підхід спирається на притаманний і унікальний характеристики автентифікації чи ідентифікації користувача. Біометрика ніколи не може бути втрачена чи забута. Це робить біометрику дуже підходящою для автентифікації та ідентифікації користувача. Біометрія класифікується на фізіологічну та поведінкову. Фізіологічна біометрія, як відбиток пальців і розпізнавання обличчя, привернули до себе значну увагу. Недоліком цієї біометрії є те, що вони потребують спеціалізованого устаткування, що може бути проблематичним для широкого використання. Для автентифікації та ідентифікації користувача через Інтернет, не завжди можна покладатися на існування апаратного забезпечення на стороні клієнта. На відміну від поведінкових біометричних методів. Людина-комп'ютерна взаємодія (HCI) може записувати дані зі звичайних пристроїв вводу, таких як клавіатура чи миша, забезпечуючи автентифікацію та

ідентифікацію користувача доступною і зручною. Найважливіший вид поведінкової біометрії - манера друкувати на клавіатурі. При її визначенні фіксується швидкість друку, тиск на клавіші, тривалість натискання на клавішу, проміжки часу між натисканнями. Відмінним біометричним фактором може служити манер використання миші.

Висновки:

2. Однак багато питань автентифікації та ідентифікації користувачів на основі їх клавіатурного почерку не достатньо вивчені. Існуючі програмні реалізації подібних систем характеризуються недостатньою достовірністю автентифікації та ідентифікації. Актуальна розробка нових методів, алгоритмів і їх програмно-апаратних реалізацій, що підвищують ефективність систем ідентифікації і автентифікації.

3. Підвищення достовірності автентифікації та ідентифікації користувачів може досягатися за рахунок розробки нового алгоритму автентифікації та ідентифікації в системах і мережах телекомунікації - полігауссового алгоритму, що дозволяє досліджувати нові параметри клавіатурного почерку при одночасному збільшенні реєстрованої інформації користувачів. Однак застосування даного алгоритму стримується недостатнім розвитком методик його реалізації.

Література

1. Understanding IP Addressing: Everything You Ever Wanted To Know
http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf
2. McKinkley, K.: Cleaning Up After Cookies. iSec Partners White Paper
http://www.isecpartners.com/storage/white-papers/iSEC_Cleaning_Up_After_Cookies.pdf
3. Gian Fulgoni. When the Cookie Crumbles
http://www.comscore.com/Insights/Blog/When_the_Cookie_Crumbles.
4. Брюхоміцкій Ю.А., Казарін М.Н. Програма аутентифікації особистості по динаміці клавіатурного почерку / Програма для ЕОМ. Реєстр. № 2003610944 (17.04.2003). ПРО «Програми для ЕОМ, бази даних, топології інтегральних мікросхем», № 2, 2003.
5. Б. Росс, К. Джексон, Н. Міяке, Д. Бонех та В. І., Дж. Мітчелл. Більш надійна автентифікація пароля за допомогою розширення браузера. У симпозиумі безпеки USENIX 2005 р
6. Ю. Чжан, Ф. Монрос та М. К. Рейтер. Безпека сучасного закінчення пароля: алгоритмічний рамки та емпіричний аналіз. На конференції ACM на комп'ютері та зв'язку безпеки (CCS), 2010 рік.