4. https://cdn2.hubspot.net/hubfs/486579/Avast_Threat_Landscape_Report_2019.pdf
5. https://www.ibm.com/downloads/cas/6MLEALKV
6. https://cloud.google.com/iot/docs/concepts/device-security

УДК 651.3:518.6

ВИКОРИСТАННЯ ТРИФАКТОРНОЇ АБО ДВОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ: ПЕРЕВАГИ І НЕДОЛІКИ, ВИБІР ОПТИМАЛЬНОГО ВАРІАНТУ

М.В. Маркіна
(Україна, Дніпро, Національний ТУ «Дніпровська політехніка»)

Постановка проблеми. З розвитком технологій дедалі частіше виникають загрози, які використовують вразливості двофакторної аутентифікації для доступу до критичної інформації. Тому, необхідно зрозуміти, які нові рішення можуть бути використані для захисту від подібних загроз (у тому числі перехід до трифакторної аутентифікації) та у яких випадках яке рішення є найбільш оптимальним.

Двофакторна аутентифікація. Метод 2FA (Two-Factor authentication) був придуманий як додатковий спосіб підтвердження власника аккаунта. Він заснований на двох з трьох способах аутентифікації:

– користувач щось знає (наприклад, пароль);
– користувач володіє унікальними рисами, які можна оцифрувати і порівняти (біометрична аутентифікація, наприклад, відбиток пальця);
– користувач щось має (наприклад якийсь девайс з унікальним ідентифікатором, ключ-карту, флешку з ключовим файлом, тощо).

За думкою експертів у галузі інформаційної безпеки, двофакторна аутентифікація різко знижує можливість крадіжки особистих даних онлайн, так як знання пароля жертви недостатньо для здійснення шахрайства. Тим не менш, двофакторні підходи аутентифікації залишаються уразливими для атак типу «фішинг» та «людина посередині».

На сьогоднішній день, найпопулярнішим методом 2FA є пароль користувача (користувач щось знає) та SMS з перевірочними кодами, що генеруються за технологією OTP (one time password) та відправляється на смартфон (користувач щось має). Код приходить кожен раз різний, тому вгадати його практично неможливо.

Однак чим складніше подолати захист технічними методами, тим легше буває це зробити за допомогою соціальної інженерії. Всі настільки впевнені в надійності 2FA, що використовують її для найвідповідальніших операцій - від авторизації в Google (що дозволяє доступ до пошти, хмарного сховища, контактів і всієї інформації, що зберігається в історії) до систем клієнт-банк.

Національний Інститут стандартів і технологій США (The National Institute of Standards and Technology, NIST) оприлюднив влітку 2016 року попередню

версію майбутнього Digital Authentication Guideline (документа, який встановлює нові норми і правила щодо цифрових методів аутентифікації), у якому говориться, що механізм SMS OTP спочатку для аутентифікації не призначався і що використання SMS-повідомлень для двофакторної аутентифікації може бути «неприпустимим» і «небезпечним».

Повністю даний параграф виглядає так: «Якщо верифікація по зовнішньому каналу здійснюється за допомогою SMS-повідомлення в публічній мережі мобільного телефонного зв'язку, верифікатор повинен переконатися, що використовуваний попередньо зареєстрований телефонний номер дійсно асоціюється з бездротовою локальною мережею, а не з VoIP або іншим програмним сервісом. Після можлива відправка SMS-повідомлення на попередньо зареєстрований телефонний номер. Зміна попередньо зареєстрованого номера не повинна бути можливою без двофакторної аутентифікації в ході зміни. Використання SMS-повідомлень в аутентифікації по зовнішньому каналу неприпустимо, і не буде дозволятися в майбутніх версіях цього посібника».

Основні побоювання експертів Національного інституту стандартів і технологій зводяться до того, що номер телефону може бути прив'язаний до VoIP-сервісу, крім того, зловмисники можуть спробувати переконати постачальника послуг в тому, що номер телефону змінився, і подібні махінації потрібно зробити неможливими.

Хоча документ рекомендує виробникам використовувати в своїх додатках токени і криптографічні ідентифікатори, автори поправок також відзначають, що «смартфон або інший мобільний пристрій завжди можуть бути вкрадені, або можуть тимчасово перебувати в руках іншої людини» – йдеться в документі NIST.

Вчені з Амстердамського університету Радхеш Крішнан Конотом (Radhesh Krishnan Konoth), Віктор ван дер Вен (Victor van der Veen) і Герберт Бос (Herbert Bos) продемонстрували атаку з використанням установки уразливого додатку через Google Play. Їм вдалося успішно обійти перевірку Google Bouncer і активувати додаток для перехоплення одноразових паролів.

Трифакторна аутентифікація. При використанні трифакторної аутентифікації використовуються усі три методи аутентифікації: користувач щось знає, користувач володіє унікальними рисами та користувач щось має. Таким чином, як правило, до методів, що найчастіше використовуються у двофакторній аутентифікації, додаються технології біометричної аутентифікації.

При цьому застосовується відповідне обладнання та програмне забезпечення, а витрати на його придбання і підтримку можуть відрізнятися в рази від витрат на забезпечення двофакторної аутентифікації.

Однак, варто розуміти - біометричні аутентифікатори не є абсолютно точними даними. Відбитки одного пальця можуть мати відмінності під впливом зовнішнього середовища, фізіологічного стану організму людини і т.п. Для успішного підтвердження цього аутентифікатора достатньо неповної відповідності відбитка еталону. Методи біометричної аутентифікації містять

визначення ступеня ймовірності відповідності чинного аутентифікатора еталону, таким чином біометрія лише із заданою вірогідністю, завжди відмінної від 100%, визначає користувача, що передбачає як помилкові спрацьовування на порушника, так і можливість відмови в доступі реальному власнику. Що стосується біометричної аутентифікації і віддаленого доступу до ІС, то поки у сучасних технологій немає можливості передати по незахищених каналах достовірні дані - відбиток пальця або результат сканування сітківки ока, тобто ці технології більше підходять для використання в корпоративних мережах.

Висновки. Таким чином, можна сказати, що недолік двофакторної аутентифікації полягає в тому, шо зловмисник може підібрати пароль користувача і перехопити SMS-повідомлення зі згенерованим кодом (механізми, що зазвичай використовуються при двофакторній аутентифікації). Тобто для захисту від відповідних атак, офіцер безпеки (або відповідальна за інформаційну безпеку компанії особа) має контролювати додатки на відповідних пристроях, на які користувачі отримують SMS-повідомлення, перевіряти чи телефонний номер дійсно належить пристрою користувача і чи має доступ до пристрою тільки сам користувач. Альтернативним варіантом є уникнення зазначеного метода аутентифікації і змінення його на більш надійний (що теж треба довести). Плюси двофакторної аутентифікації полягають у більш простій реалізації (порівнюючи із трифакторною), меншою ціною реалізації та меншою ймовірністю помилки першого роду. Відповідно, трифакторна аутентифікація є більш надійною з точки зору забезпечення конфіденційності інформації, але це рішення є більш складним і дорогим; при біометричній аутентифікації можливі помилки першого і другого роду, тому є деякий ризик для доступності. Крім того, біометричну аутентифікацію можна використовувати лише для аутентифікації користувачів на локальних пристроях або в корпоративній мережі – вона не підійде для авторизації користувачів на віддалених ресурсах. Отже, загалом двофакторна аутентифікація підійде для ресурсів, на яких зберігається менш чутлива, з точки зору конфіденційності, інформація та для віддалених ресурсів, а трифакторна – для локальних ресурсів, на яких знаходиться інформація з високим ступенем конфіденційності.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Левашов А. Многофакторная (двухфакторная) аутентификация [Електронний ресурс] / Александр Левашов – Режим доступу до ресурсу: http://www.tadviser.ru/a/144161.

2. Афанасьев А. Безопасность корпоративной сети: защита изнутри [Електронний ресурс] / Алексей Афанасьев // Intelligent Enterprise. – 2003. – Режим доступу до ресурсу: https://www.aladdin-rd.ru/company/pressroom/articles/bezopasnost_korporativnoj_seti_zasita_iznutri.

3. Обходим двухфакторную аутентификацию с помощью Modlishka [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://xakep.ru/2019/05/28/ .

4. Пилипенко О. Взуття, жувальна гумка або недопалки — тепер ваш додатковий пароль [Електронний ресурс] / Олег Пилипенко. – 2017. – Режим доступу до ресурсу: https://www.imena.ua/blog/new-verification-ways/.

УДК 004.94

ПРОГРАМНА РЕАЛІЗАЦІЯ ТА ДОСЛІДЖЕННЯ ГЕНЕТИЧНОГО АЛГОРИТМУ ДЛЯ РОЗВ'ЯЗКУ ЗАДАЧІ КОМІВОЯЖЕРА

Т.В. Селівьорстова, В.М. Пеліпака
(Україна, Дніпро, Національна металургійна академія України)

Постановка проблеми. Як відомо задача комівояжера є відомою у такому формулюванні. Дано кількість міст і вказано відстані між ними. Комівояжер повинен вийти з першого міста, відвідати по одному разу в певному порядку всі міста і повернутися в перше місто. Необхідно знайти такий порядок відвідування міст, щоб довжина замкнутого маршруту комівояжера була мінімальною.

Аналіз останніх публікацій та досліджень. Для розв'язку задачі комівояжера було розроблено ряд методів, зокрема метод Літтла (точний метод) та наближений метод розв'язання задачі комівояжера (метод найближчого міста). Проте, при збільшенні кількості міст, точний алгоритм демонструє дуже великий час обчислень, а наближений надмірну похибку. Тому для розв'язання даної задачі доцільно використовувати методи обчислювального інтелекту, зокрема генетичний алгоритм.

Постановка завдання. Метою роботи є програмна реалізація та дослідження генетичного алгоритму для розв'язку задачі комівояжера. Вивчення особливостей реалізації кросовера при реалізації генетичного алгоритму для розв'язання задачі комівояжера.

Матеріали дослідження. Значення функції пристосованості повинне відповідати відстані, що проходить комівояжер відповідно до шляху, що представляє хромосома. Оскільки це значення повинне бути мінімальним, то кінцева формула функції пристосованості j-й хромосоми часто виглядає в такий спосіб:

$$f_j = d_{\max} \cdot 1{,}1 - d_j,$$

де $d_{\max}$ – довжина максимального маршруту в поточній популяції;

d_j – довжина маршруту, що представляє j-у хромосому.

Значення цієї функції чим більше, тим краще. Існує чотири основних варіанти подання маршруту комівояжера у вигляді хромосоми: сусідське, порядкове, шляхове й матричне. Оскільки класичні оператори схрещування й мутації для них, як правило, незастосовні, кожне із цих уявлень мають власні «генетичні» оператори, всі вони дуже сильно розрізняються. Що порядкове