УДК 621.391

С. П. Євсеєв, О. Г. Король
Харківський національний економічний університет імені Семена Кузнеця

ДОСЛІДЖЕННЯ ЗАГРОЗ МЕТОДІВ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

Розглянуто побудову методів двофакторної автентифікації. Оцінено ризик різних методів онлайн-атак проти системи двофакторної автентифікації PassWindow, запропоновано ефективний практичний метод моніторингу системи двофакторної автентифікації PassWindow у разі її застосування у банківських системах.

Ключові слова: методи двофакторної автентифікації, ризики онлайн-атак, система автентифікації PassWindow.

INVESTIGATION THREATS BIFACTOR AUTHENTICATION METHODS

Evaluated risk of various methods of online attacks against the system of bifactor authentication PassWindow. Propose effective practical method for monitoring bifactor authentication system PassWindow at its application in the banking systems

Key words: bifactor authentication methods, risks on-line attacks, authentication systems PassWindow.

Вступ

Сучасні системи автентифікації базуються на пред’явленні користувачем комп'ютера статичної пари ідентифікатор/пароль. Однак такі пари можуть бути скомпрометовані через халатність користувачів або можливості підбору паролів зловмисником [1–5]. Значні інтервали часу, протягом яких пароль та ідентифікатор залишаються незмінними, дають змогу застосувати різні методи їх перехоплення і підбору. Для того, щоб підвищити захищеність комп’ютерної системи, адміністратори обмежують термін дії паролів, але в типовому випадку цей термін становить тижні та місяці, що цілком достатньо для зловмисника. Радикальним рішенням є застосування двофакторної автентифікації, коли система просить користувача надати їй “те, що ти знаєш” (ім'я і, можливо, якийсь PIN-код), і “те, що у тебе є”– який-небудь апаратний ідентифікатор, що асоціюється з цим користувачем [2, 3].Останнім часом такі системи автентифікації широко використовують у банківських системах, особливе місце серед них займає некриптографічна система двофакторної автентифікації PassWindow, яку застосовують великі банки Малайзії, Чилі, Туреччини, Індонезії та Австралії.

Основна частина. Класифікація методів двофакторної автентифікації

В останнє десятиліття Інтернет перетворився на основний спосіб зв’язку нашого сучасного життя. Він, безсумнівно, буде основним інструментом для здійснення покупок та інших фінансових операцій. Поява цих технологій створила суспільний попит на методи автентифікації, основані не тільки на традиційних криптографічних способах (шифрування, гешування, цифровий підпис), а й на методи, основані на використанні декількох чинників забезпечення достовірності особи, яка здійснює фінансову операцію. Двофакторна система безпеки основана на тому, що користувач, крім того, що знає пароль доступу до певного імені користувача (“логіна”), володіє й інструментом для отримання відповідного йому ключа доступу. Останнім може слугувати збережений на комп’ютері

електронний сертифікат безпеки або код, який надходить на особистий телефон як СМС з кодом підтвердження, або ж відбиток пальця, знятий електронним пристроєм [2].

Методи строгої (двофакторної) автентифікації найчастіше використовуються у фінансовій сфері, але в принципі можуть застосовуватися практично в будь-якій області. Основні способи побудови систем двофакторної автентифікації поділяються на:

1. *Програмне забезпечення для ідентифікації конкретного ПК*. У комп'ютер інсталюється спеціальна програма, що встановлює в ньому криптографічний маркер. Тоді в процесі автентифікації задіяні два фактори: пароль і маркер, вбудований у ПК. Оскільки маркер постійно є на комп'ютері, користувачеві для входу в систему потрібно буде лише ввести логін і пароль.

2. *Біометрія*. Використання біометрії як вторинного фактора ідентифікації полягає в ідентифікації фізичних характеристик людини (відбиток пальця, райдужна оболонка ока тощо).

3. *Одноразовий електронний mail- або sms-пароль*. Використати як вторинний фактор ідентифікації такий пароль можливо, відправивши другий одноразовий пароль на зареєстровану адресу електронної пошти або на мобільний телефон.

4. *Токен з одноразовим паролем*. Користувачу видається пристрій, що генерує паролі, які постійно змінюються. Саме ці паролі і вводять користувачі на додаток до звичайних паролів під час автентифікації.

5. *Контроль ззовні*. Цей метод передбачає дзвінок з банку на попередньо зареєстрований телефонний номер. Користувач повинен ввести пароль з телефону, і лише після цього він отримає доступ до системи.

6. *Ідентифікація з використанням гаджетів*. Таку ідентифікацію здійснюють, помістивши криптографічну мітку на будь-який пристрій користувача (наприклад, на USB-накопичувач, iPad, карту пам'яті тощо). Під час реєстрації користувач повинен під'єднати цей пристрій до ПК.

7. *Картка з шаром, який зіскоблюється*. Користувачу видається картка з PIN-кодом, який використовується лише один раз.

Аналіз показав, що в банківських системах, як правило, застосовуються системи двофакторної автентифікації, основані на одноразових e-mail- або sms-паролях та різних типах токенів. Сьогодні кілька компаній пропонують системи двофакторної автентифікації, основані на генерації одноразових паролів (One-Time Password – OTP), серед яких RSA Security, VASCO Data Security і ActivIdentity.

Для реалізації двофакторної автентифікації використовують різні види генераторів OTP. Генератор OTP являє собою автономний портативний електронний прилад, здатний генерувати і відображати на вбудованому ЖК-дисплеї цифрові коди. Для сім'ї пристроїв Digipass компанії VASCO механізм генерації одноразових паролів оснований на криптографічному TripleDES-перетворенні набору даних, що складається з 40 бітів поточного часу і 24-бітового вектора даних, унікальних для кожного ідентифікатора доступу. Некриптографічні алгоритми автентифікації передбачають використання для підтвердження достовірності абонента не тільки його логіна та паролю, а й додаткових засобів (мобільних телефонів, смарт-карт, токенів). Авторизація за допомогою предметів відбувається тільки за наявності спеціального пристрою, який може зчитувати інформацію з перерахованих ідентифікаторів. Робота системи має такий алгоритм:

1. Користувач надсилає запит на доступ у систему й вводить свій логін та пароль.

2. Сервіс перевіряє наявність логіна у DNS-таблиці.

3. У DNS-таблиці перевіряється відповідність введеного паролю та логіна.

4. Якщо збігаються дані, система надсилає запит користувачеві на введення ідентифікатора із додаткового засобу.

5. Абонент отримує свій унікальний ідентифікатор з пристрою.

6. Абонент надсилає ідентифікатор до системи.

7. Система перевіряє індивідуальний ідентифікатор суб'єкта.

8. У разі збігу даних із еталонним варіантом автентифікацію визнають вдалою й надають доступ до системи, якщо дані не збігаються – суб’єкт повертається до першого кроку.

Алгоритм некриптографічної автентифікації наведено на рис. 1.

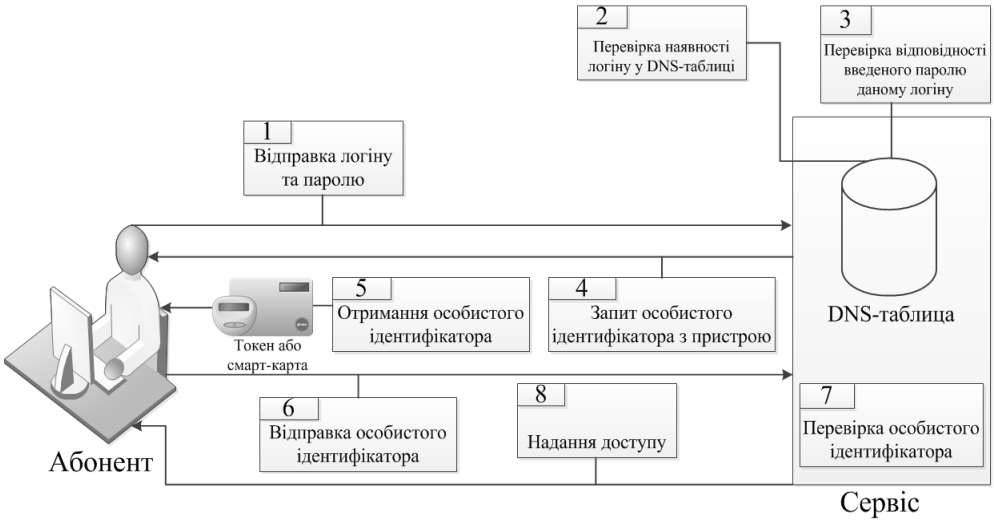

Рис. 1. Схема алгоритму некриптографічної автентифікації

Для автентифікації за допомогою біометричного алгоритму суб’єкт повинен пройти сканування однієї чи декількох фізіологічних (відбиток пальців, райдужна оболонка ока, сітківка ока, риси обличчя тощо) або поведінкових характеристик (підпис, клавіатурний почерк, тембр голосу). Цей метод, як правило, використовують на дуже важливих об’єктах та системах зі спеціальним устаткуванням. Робота системи має такий алгоритм:

1. Користувач зчитує біометричні дані за допомогою біометричного давача.

2. Зчитані дані надсилають на сервер, де порівнюють з еталонними даними, які зберігаються у базі даних.

3. У разі збігу даних із еталонним варіантом автентифікація вважається вдалою й надається доступ до системи, якщо ж ні – суб’єкт повертається до першого кроку.

Алгоритм парольної автентифікації наведено на рис. 2.

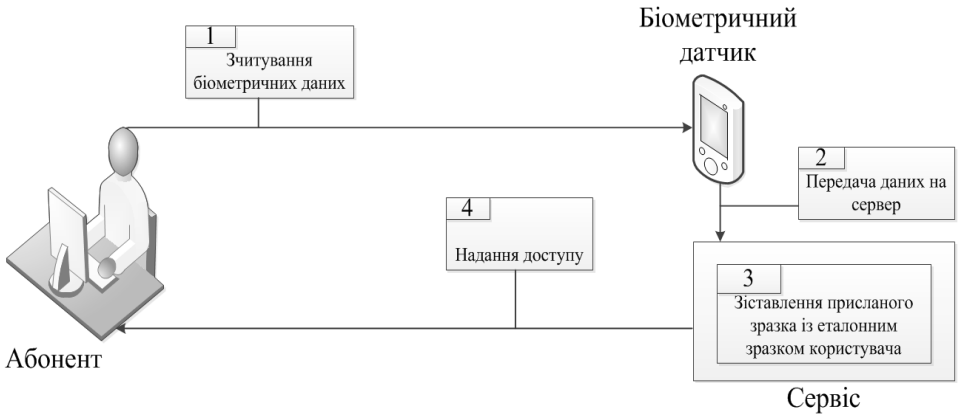

Рис. 2. Схема алгоритму біометричної автентифікації

Алгоритм двофакторної автентифікації повідомлень у банківських системах PassWindow – розробка австралійського фахівця Метта Уокера. Його концепція вперше презентована у 2009 р. у статті видавництва The Australian IT. Цей алгоритм автентифікації є переможцем у міжнародному конкурсі Asian Innovation Awards у 2010 р. [8]. PassWindow –

алгоритм двофакторної автентифікації, побудований на формуванні унікального ключа, частина якого надрукована на прозорій частині стандартного посвідчення особи у вигляді штрихкоду, який складається із рисок [1]. Щоб скласти унікальний ключ доступу, треба притиснути свою картку до екрана монітора, термінала, мобільного телефона чи планшета у відповідну область, де формується друга частина коду, що також має вигляд штрихкоду з рисками, які змінюються.

Шаблони штрихкоду PassWindow можуть існувати у вигляді унікальних статичних зображень послідовності символів або у вигляді більш розширеної анімаційної версії всього шаблону. Ці анімовані штрихкоди складаються з послідовності статичних шаблонів, кожний з яких містить закодовані символи або ж нічого не означають і просто динамічно додають ентропію у весь шаблон. Послідовності шаблонів штрихкоду генерує динамічно сервер автентифікації так, що кожен є унікальним (і, отже, є сенс) тільки у разі використання разом з ключем, до якого вони підходять. Будь-яке втручання або підробка шаблону штрихкоду будуть пасивно представлені користувачу у вигляді появи комбінацій в шаблоні, які не відповідають очікуванням, наприклад, випадково розміщені сегменти, які не містять ніяких символів, випадкові цифри, яких бракує, або надлишкові цифри, що з'являються в межах одного шаблону, або проведення перевірки інформації, яка не стосується активної транзакції. Будь-який буквено-цифровий код можна надійно передати за допомогою методу PassWindow, проте поточна реалізація методу спрямована на передавання коротких рядків випадкових цифр, щоб використати їх як одноразовий пароль у поєднанні з цифрами, які ідентифікують унікальність транзакції перевірки справжності користувача. Як тільки користувач підтверджує, що унікальна інформація в межах транзакції – закодована в штрихкодах – відповідає бажаній, він може завершити транзакцію, ввівши відповідний одноразовий пароль. Основні етапи системи PassWindow подано на рис. 3. Принцип роботи методу автентифікації має такий алгоритм:

1. Абонент ідентифікується у системі.

2. Сервіс перевіряє наявність логіна у DNS-таблиці.

3. У DNS-таблиці перевіряється відповідність введеного паролю та логіна.

4. Якщо ідентифікація пройшла успішно – абоненту надсилають запит фіксації точок картки.

5. Абонент прикладає картку до екрана, після чого відбувається фіксація відповідності точок штрихкоду картки.

6. Зафіксовані точки відправляються до сервісу, де надалі зберігаються.

7. У сервісі відкривається доступ до бази карток.

8. Здійснюється генерація штрихкоду для частини ключа, що надалі дасть змогу формувати код.

9. Сформований штрихкод частини ключа надсилається абоненту.

10. Абонент, прикладаючи персональну картку до екрана свого пристрою, формує код (код йде після літери Р).

11. Зіставлений код надсилається до сервісу.

12. Надісланий код перевіряється на правильність.

13. Якщо перевірку успішно пройдено – автентифікація успішна. Абоненту надається доступ до сервісу.

Оцінка безпеки систем двофакторної автентифікації. Аналіз сучасних систем автентифікації показав, що їх безпеку вимірюють, поділивши різницю між вартістю атак і вигодою для того, хто атакує, на вартість захисту від них. Тому дорогі, хоча й безпечніші методи, такі як криптографічні PKI-пристрої з власними захищеними каналами зв'язку, екранів і клавіатур, оцінюються так низько за шкалою безпеки, тоді як банківські системи все ще переважно спираються на найдешевший і, здавалося б, найменш захищений спосіб використання PIN-кодів і паролів. Через загальну вартість і складність розгортання таких пристроїв часто надають перевагу їх використанню, а не криптографічним системам безпеки.

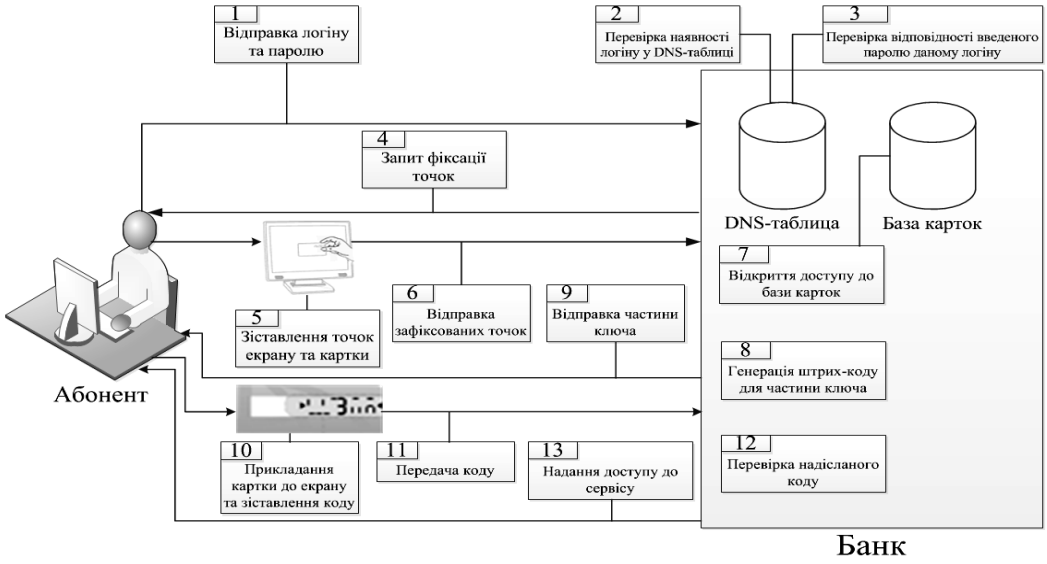

Рис. 3. Схема алгоритму подвійної автентифікації PassWindow

Загрози безпеки в мережі можна поділити на мережеві атаки (інформація, яка надходить з віддаленого агента) і локальні атаки, які походять від шкідливих програм, вже встановлених на системі клієнта, наприклад, троянів, руткітів тощо. Часто оцінки безпеки автентифікації зосереджені переважно на мережевих атаках, припускають, що користувальницький термінал (тобто настільний комп'ютер, ноутбук або мобільний пристрій) є захищеною платформою [1–5]. Проте нерідко зловмисник отримує повний доступ до ПК жертви через приховані процеси зв'язку, які залишилися від шкідливих програм, що використовують невиправлені діри в безпеці ліцензійного програмного забезпечення.

Типовими методами атак є:

• *виламування онлайнових баз даних* – викрадення інформації, що зберігається в торгових базах даних.

• *"Людина посередині"/фішинг* – третя сторона втручається і уособлює клієнта і сервер, змушуючи записувати та/або змінювати повідомлення один одного.

• *Атаки в області соцінженерії* – клієнтів обманюють, щоб вивідати їхні особисті дані й передати хакеру.

• *"Людина в браузері"* – шкідлива програма, яка встановлена на комп'ютері жертви, для повідомлення про мережеву активність, натискання клавіш, а також дані, захоплені з екрана хакером, що дає йому змогу перехоплювати дані про переказ коштів, в яких кошти можуть бути мимоволі спотворені шляхом зміни інформації, що відображається в браузері користувача.

• *Атака повним перебором паролів користувачів* – сервер опитується з усіма можливими комбінаціями паролів.

• *Проста крадіжка* – подробиці про автентифікацію записані або на картці можуть бути фізично прийняті та скопійовані.

• *Спостереження зі спини* – зловмисник може непомітно спостерігати, як користувач вводить деталі своєї угоди.

Проаналізуємо методи двофакторної автентифікації порівняно з системою PassWindow і їх протистояння різним типам атак.

Позначення *SMS-систем або систем двофакторної автентифікації на основі мобільних телефонів* є помилковим, точніший термін – це "позасмугова" автентифікація. Але з поширенням GSM, смартфонів і планшетів, підключених до мережі, навіть ця перевага безпеки може бути втрачена, якщо автентифікація транзакції користувача здійснюється на самому мобільному пристрої. Крім того, зростання небажаного програмного забезпечення для мобільних пристроїв

тепер дозволяє зловмиснику отримати доступ до кодів автентифікації, відправлених через SMS не тільки за допомогою традиційного перехоплення за допомогою шкідливого ПО, але і перехопленням і дешифруванням даних через мережу GSM-телекомунікацій. Атаки автентифікації мобільних пристроїв успішно проводяться і без таких технологій. Замість цього зловмисник просто видає себе за користувача пристрою і дає запит, щоб всі SMS-повідомлення спрямовувалися на другий номер телефону протягом всієї атаки. Інший метод перевірки автентичності використовує камеру мобільного пристрою для зчитування зображення штрихкоду на робочій станції користувача, який закодований з OTP-інформацією про транзакції. Цей метод містить помилку, припускаючи, що операційна система на мобільному пристрої користувача не схильна до подібної уразливості до шкідливого ПО, як і всі інші форми програмного забезпечення, що працює з мережею.

У разі використання *біометричної автентифікації* дані про користувача пропонуються для онлайн-автентифікації. Однак біометричні пристрої автентифікації не можуть взаємодіяти з локальними пристроями або мережею, не зазнаючи атак шкідливих програм та/або атак "посередника". Цей метод так само неможливо повторно змінити після того, як зловмисник видав себе за користувача, використовуючи біометричну автентифікацію.

Біометрична автентифікація надає користувачу зручний спосіб генерації онлайн-імені користувача, однак якщо мережа прослуховується або мобільний пристрій заражений, загальна продуктивність безпеки таких методів не вища, ніж з використанням звичайного імені та пароля користувача.

Електронні апаратні маркери бувають декількох видів і забезпечують різні функції безпеки автентифікації. Найчастіше апаратні маркери генерують одноразові паролі (OTP), використовуючи криптографічні алгоритми з внутрішнім секретним ключем, або, частіше, секретний ключ генерується на основі загального, синхронізованого значення системного часу. Користувач читає відображені пристроєм цифри і вручну вводить їх в свої термінали для перехресного посилання з сервером перевірки автентичності. Цей простий метод електронної генерації OTP залишається уразливим до атак "посередника", оскільки користувачі зобов'язані розголошувати OTP без засобів перевірки контексту автентифікації.

У відповідь на це багато виробників маркерів додали невелику цифрову клавіатуру, помітно збільшивши розмір маркера, але дозволяючи користувачу вводити інформацію про конкретні транзакції, зашифровані за допомогою секретного ключа, перш ніж користувач вводить результат у своєму терміналі. Це є одним з типів перевірки або підписання транзакції, і справді забезпечує деякий захист від атаки "посередника".

Проте цей метод, як і раніше, уразливий для атак через використання трудомісткого процесу ручного підписання транзакції. Час і увага, які необхідні для виконання ручної операції, успішно використовуються для відволікання користувача від контексту інформації про угоди, які користувач приймає, і, отже, атаки можуть бути успішно здійснені в масовому масштабі [1].

Друковані списки OTP/сітки чисел. Старіший метод надання одноразових паролів – друковані списки випадково згенерованих кодів зв'язку або кодів авторизації транзакцій на аркуші паперу або скетч-картці. Кожен код доступу запитується у послідовності та використовується для перевірки справжності однієї транзакції.

Як альтернатива може використовуватися друкована таблиця символів, і сервер автентифікації видає штрихкод, запитуючи символи, розташовані в певних координатах.

Обидва методи використовують ключі й сигнали, які можна повідомити вербально. Це дає змогу зловмиснику запитати користувача про наступний дійсний код через шкідливі програми, використовуючи соціальну інженерію або фішинг-атаки. Крім того, порівняно низька ентропія списків або сіток вимагає частої зміни ключів, щоб запобігти повторенню запиту коду зловмисником.

Ці методи залишаються вразливими для повного спектра атак "посередника" з тих самих причин, що і всі методи автентифікації з невідомим контекстом.

Гіпотетичні атаки на засіб аутентифікації PassWindow. Атаки “посередника” і фішинг (MITM) відбуваються, коли зловмисник між клієнтом і сервером і видає себе за обидві сторони, здійснює перехоплення, запис або зміну взаємодії між ними [1]. PassWindow вирішує цю проблему, надаючи пасивну перевірку на рівні транзакцій, щоб переконатися, що користувач знає про справжність транзакції, яку він виконує до введення OTP після завершення цієї транзакції. Отже, PassWindow захищає від шахрайських атак MITM транзакцій і забезпечує автентифікацію в обох напрямах – від користувача до сервера і від сервера до користувача.

Атаки в області соцінженерії.

В “атаках соціальної інженерії” користувача переконують розголосити його особисті дані, і в разі апаратних маркерів – його одноразові паролі.

Комбінації клавіш PassWindow не так легко передаються в усній формі або через друковані символи, тим самим запобігаючи найзручнішим телефонним атакам соціальної інженерії, які використовуються проти електронних апаратних маркерів. Цей метод отримав назву “вішинг”. Ці атаки використовують людину, яка дзвонить користувачу і видає себе за уповноваженого представника обслуговування. Усний запит здійснюється для читання дійсного коду авторизації з пристрою автентифікації жертви, що нібито дає змогу людині, яка дзвонить, виявити, наприклад, “важливу конфіденційну інформацію”. Малоймовірно, що зловмисник спробує дізнатись комбінацію клавіш PassWindow від клієнта цим способом, тому що важко на словах пояснити візуальні характеристики сегмента PassWindow матриці.

“Людина в браузері”, або хакерське проникнення. Зловмисник одержує звіти від шкідливих програм, встановлених на комп’ютері жертви, і виявляє, що жертва звертається до сайта фінансової організації, програмне забезпечення змінює дані форми в браузері на такі, щоб інший обсяг коштів передавався на чужий рахунок – зазвичай гібридний. Власник такого рахунка потім передає ці гроші зловмиснику. Перевірка інформації, пов’язаної з операцією, може бути закодована в штрих-коді шаблону PassWindow. Це може запевнити користувача, наприклад, що кошти переводяться на правильний рахунок.

Проста крадіжка. Єдиним способом для відкриття і копіювання ключового шаблону PassWindow є пряме копіювання карти відразу після її отримання. Цю можливість знижують, вводячи відтінок, який можна роздрукувати поверх шаблону, що ускладнить спроби фотографування і ксерокопіювання. Однак, оскільки PassWindow використовується в стратегії двофакторної автентифікації, простого знання ключового шаблону недостатньо для шахрайської автентифікації без знання логіна або пароля жертви.

Підглядання зі спини. PassWindow захищений проти “підглядання зі спини”– непомітного спостереження за тим, як користувач вводить свої дані. Оскільки ключ/штрихкод являє собою одноразовий пароль, ті, що підглядають, не можуть скористатись ним.

Знову ж, відтінок, надрукований поверх ключового шаблону на картці, робить шаблон невидимим ні для кого, окрім користувача.

Пряма атака на сервер автентифікації PassWindow. Зловмисник може спробувати безпосередньо атакувати сервер автентифікації PassWindow, щоб порушити цілісність всієї процедури автентифікації PassWindow. Сервер автентифікації PassWindow використовує дуже простий і обмежений протокол зв’язку, і вся обробка автентифікації здійснюється на самому сервері. Його функціональність обмежена створенням даних зображення штрихкоду, отриманням коротких кодів доступу і значення ідентифікаторів користувачів, і, зрештою, видаванням відповіді (так/ні) на запит перевірки автентичності. Крім цього, різні стратегії автентифікації управляють задовільною швидкістю запитів і термінів відповіді. Цей базовий цифровий зв’язок з сервером автентифікації дає невелику можливість зловмиснику безпосередньо зайняти сервер будь-яким ефективним способом, що може привести до успішного доступу.

Аналітична атака на секретний ключ

Зловмисник може спробувати вивести друковану комбінацію клавіш користувача через аналітичну (наприклад, статистичну або алгебраїчну) атаку. Це можна зробити з використанням склад-

ної програми “атака посередника” або шкідливих встановлених локально програм на основі моніторингу, що дасть змогу перехоплювати і штрихкоди PassWindow, і відповідні відповіді користувача. З часом, коли у зловмисника накопичуються ці пари запит/відповідь, він може потенційно отримати деяке уявлення про ключові шаблони PassWindow через аналіз перехоплених даних.

З метою тестування уразливості PassWindow до такого нападу розроблено алгоритм злому, який намагається використовувати ці принципи для виконання зазначеного аналізу.

Сам алгоритм використовує техніку “грубої сили”. Він починається з генерації всіх комбінацій, в результаті чого цифри, які є результатом, можуть бути поміщені в шаблоні.

Наприклад, шестизначний результат у шаблоні з 14 колонок дає такі можливі варіанти (серед інших):

2 - 5 - 7 - 2 - 4 - 3 - - -

2 - 5 - 7 - 2 - 4 - - 3 - -

2 - 5 - 7 - 2 - 4 - - - 3 -

2- - 5- - 7 - 2 - 4 - - 3

Кожна комбінація оцінюється за відомим штрихкодом, щоб розрахувати, може він становити цифру в запиті чи ні. Сегменти можуть або бути присутні, якщо вони необхідні для побудови рішення, або ні, якщо вони мають бути відсутні для нього, або можуть бути невідомими, якщо сегмент далеко від цифри чи накладається на біт штрихкоду.

Після окремого набору комбінацій для кожного перехоплення алгоритм шукає несумісності між комбінаціями. Він бере першу комбінацію першого набору, порівнюючи його, своєю чергою, з кожною комбінацією другого комплекту. Якщо вона несумісна з кожною комбінацією в другій групі, комбінація відкидається.

Перевірка сумісності триває так, що кожна комбінація в кожному наборі порівнюється з комбінаціями кожного іншого набору. Якщо комбінація відкидається, тоді кожний наступний набір необхідно переглянути. Здійснюючи перебір і аналіз достатньої кількості перехоплень, алгоритм здатний вивести ключовий шаблон з достатнім ступенем достовірності.

Однак ця атака потребує значної кількості перехоплень зломником: від 20 –30 в разі малих шаблонів (до 4–5 цифр), сотень для великих шаблонів (до 10 цифр), декількох тисяч (до 40 цифр) в разі використання методу в анімаційному режимі підвищеної безпеки.

Отже, безпека PassWindow полягає не стільки в складності алгоритму, необхідного для її вирішення, скільки в системній складності вилучення достатньої кількості інформації залежно від цілі атаки. Якщо PassWindow використовується правильно, то висока ймовірність того, що необхідна інформація може бути недоступна навіть для найдосвідченіших хакерів.

Підроблені (ослаблені) штрихкоди. Зловмисник може спробувати послабити захист PassWindow, змінюючи частоту кадрів зі справжнього (перехопленого) штрихкоду, перш ніж доставити ослаблений (спрощений) штрихкод користувачеві. Цей метод зменшує ентропію штрихкоду, щоб змінити деталі, які могли б спростити аналіз перехоплення запитів / відповідей. Однак явно пошкоджений штрихкод пасивно попереджає користувача про спробу нападу, викликаючи його підозри щодо використання обчислювальної техніки та комунікаційних каналів.

Ефективний практичний спосіб моніторингу системи PassWindow. Проведений аналіз загроз системи PassWindow показав, що найефективнішою загрозою є аналітична атака на секретний ключ (штрихкод картки). Для успішної роботи алгоритму потрібно від трьох до п’яти сесій моніторингу (передачі клієнтом ОТР банку).

Алгоритм моніторингу пластикових карток складається з таких кроків:

1. Моніторинг каналу зв’язку та отримання даних за сесіями.

2. Переведення даних у клас індикатора (у вигляді бінарного коду), яким можна оперувати як об’єктом (клас індикатора являє собою масив із семи одиниць/нулів).

3. Перевірка можливості формування “цифр” в кожній позиції картки (цикл за всіма сесіями). Всередині циклу починається цикл за кожною послідовністю – по черзі кожен індикатор представляється “правильним” (вважаємо, що в ньому була цифра).

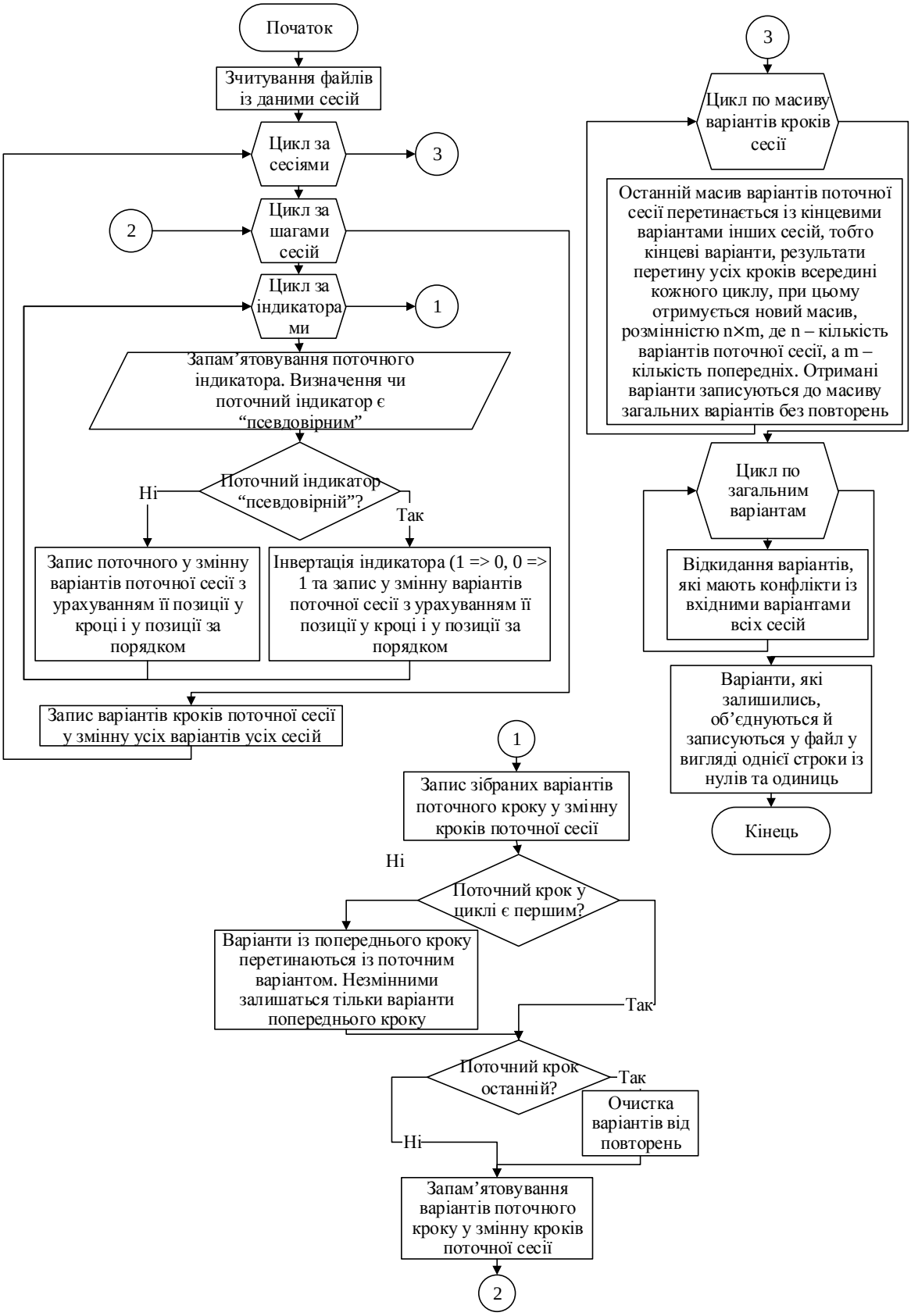

Рис. 4. Алгоритм моніторингу пластикових карток PASSWINDOW

Всередині циклу проводиться перевірка – якщо поточна позиція є “правильною”, тоді створюється варіант, в який записується інвертований індикатор генератора; якщо це “неправильна” позиція, то записується індикатор. Після кожного циклу усередині однієї послідовності йде перетин з варіантами минулої послідовності, тобто N · N (Ni & Nj), якщо всі послідовності в поточній сесії перетнуті – звільняємо їх, тобто кінцеві листи (варіанти) проглядаються і викидаються копії.

4. Перегляд всіх послідовностей у всіх сесіях. Перетин всіх листів між сесіями по черзі (перша сесія з другою, результат їх перетину з третьою сесією і т.д.). Після кожного перетину листа із суміжною сесією – листи “чистяться” від копій.

5. Перетин листів всіх сесій між собою. Цикл за всіма листами – кожен варіант (або лист) перевіряється на вхідних даних – на даних генератора. Якщо він має конфлікт з якимось з індикаторів, то такий лист (варіант) відкидається. У результаті залишиться тільки один варіант, який не має конфліктів ні з однією з послідовностей всіх сесій.

6. Виведення кінцевого варіанта в файл output.txt у форматі бінарного рядка.

Алгоритм моніторингу пластикових карток PASSWINDOW наведено на рис. 4.

Висновки

Проведений аналіз методів двофакторної автентифікації показав, що практично всі системи як основу використовують криптографічні алгоритми (таблиці) і схильні як до традиційних атак на криптографічні процедури, так і до атак на основі соціальної інженерії, і не в повному обсязі забезпечують безпеку їх використання в банківських системах. Особливе місце серед них займає система двофакторної автентифікації PassWindow, основана на використанні штрихкодів для формування автентифікатора, що ефективніше від інших протистоїть сучасним онлайн-атакам. Запропонований алгоритм моніторингу системи PassWindow дає змогу за 3–5 сесій передачі OTP паролів отримати унікальний штрихкод картки користувача, що практично призводить до руйнування безпеки банківської системи.

1. Евсеев С. П. Исследование методов двухфакторной аутентификации / С. П. Евсеев, О. Г. Король // Системи обробки інформації. – 2014. – № 2(118). – С. 81– 87. 2. Двухфакторная аутентификация [Электронный ресурс]. – Режим доступа: http://www.aladdin-rd.ru/solutions/authentication/. 3. Настройка двухфакторной аутентификации [Электронный ресурс]. – Режим доступа: http://support.citrix.com/proddocs/topic/web-interface-impington/nl/ru/wi-configure-two-factor-authentication-gransden.html?locale=ru. 4. Семь методов двухфакторной аутентификации [Электронный ресурс]. – Режим доступа: http://www.infosecurityrussia.ru/news/29947. 5. Двухфакторная аутентификация при удаленном доступе [Электронный ресурс]. – Режим доступа: http://itc.ua/articles/dvuhfaktornaya_autentifikaciya_pri_udalennom_dostupe_23166/.