УДК 621.382

МОДЕЛІ ІДЕНТИФІКАЦІЇ ТА АУТЕНТИФІКАЦІЇ В СИСТЕМАХ ХМАРНИХ ОБЧИСЛЕНЬ ДЛЯ ВЕБ-СЕРВЕРІВ ТА МОБІЛЬНИХ ДОДАТКІВ З ІНТЕЛЕКТУАЛЬНОЮ ПІДТРИМКОЮ ВИБОРУ

Пилипчук А. О.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: pylypchukangelina@gmail.com

Models of identification and authentication in cloud computing systems for web servers and mobile applications with intelligent support of choice

Six variants of mathematical models of authentication during users work with mobile applications in cloud area are represented. The intelligence approach for choice of identification and authentication system on the base of expert system knowledge base roles is proposed.

Моделі та засоби ідентифікації та аутентифікації користувачів в системах хмарних обчислень є важливим та актуальним напрямком дослідження та розробок в області захисту інформації. Ідентифікація (Identification) – процедура розпізнавання користувачів по їх ідентифікатору. Аутентифікація (Authentication) – процедура перевірки справжності заявленого користувача, процесу чи пристрою [1].

В даній доповіді розглядається інтелектуальний підхід для вибору варіантів системи ідентифікації та аутентифікації (СІА). Даний підхід базується на основі складання бази правил вибору, в якості інтелектуального інструменту застосовуються засновані на правилах експертні системи (ЕС). ЕС в базі знань включає опис класифікаційних правил СІА, відповідних профілям легальних користувачів. Експерт формує базу правил для вибору варіанта СІА. Робота такої ЕС може базуватись як на експертному підході, так і в автоматичному режимі сервера. Для першого варіанту організовується діалог, в ході якого виявляються побажання чи вимоги користувача чи адміністратора. На основі результатів опитування формується варіант. В автоматичному режимі серверу варіант СІА формується по профілям легальних користувачів.

Для реалізації даного підходу розглянемо моделі аутентифікації та ідентифікації користувачів при роботі з мобільними додатками в хмарному середовищі. Представлено шість математичних моделей аутентифікації:

Аутентифікація по паролю з сервером додатків. Ця модель заснована на тому, що користувач повинен представити серверу додатків username – U_n та password – P_s для успішної ідентифікації та аутентифікації в системі. Нехай, X – користувач, B – браузер, S – сервер додатків, A – ознака аутентифікована, n – унікальне значення, H – хеш функція, C – процес шифрування, P – k-ий додаток. Базова модель аутентифікації матиме вигляд:

$$X(U_n, P_s) \rightarrow B \rightarrow S_p;\ S_p(A) \rightarrow B \rightarrow X.$$

Аутентифікація з додатками. У цій моделі користувач повинен представити додатку username – U та password – P для успішної ідентифікації та аутентифікації в системі. Має наступний вигляд:

$$X(U_n, P_P) \rightarrow B \rightarrow P_k(S_p); P_k\left(S_p(A)\right) \rightarrow B \rightarrow X.$$

Аутентифікація по сертифікату. Нехай, CA – сервер аутентифікації, $C_a(k)$ – сертифікат користувача, K_s – секретиний ключ. Вигляд моделі:

$$X(C_a(k), K_s) \rightarrow CA; CA(C_a(k, CA) \rightarrow X;$$

$$X(C_a(k, CA) \rightarrow S_p;\ S_p \rightarrow CA;\ S_p(A) \rightarrow B \rightarrow X.$$

Модель більш надійна, однак є важкості з поширенням та реалізацією.

Аутентифікація по одноразовим паролям. Зазвичай використовується додатково до аутентифікації по паролям для реалізації двох-факторної аутентифікації (2FA). Для цього користувачу потрібно представити дані двох типів для входу в систему: щось, що він знає (наприклад, пароль), та щось, що він має (наприклад картку). Реалізація даної моделі можлива завдяки токенам, які можуть генерувати одноразові паролі на основі секретного ключа, введено в них, поточного часу – $T(K_s, t)$ та запиту одноразового паролю – R. Модель представлена в наступному вигляді:

$$X\ (U_n, P_s) \rightarrow B \rightarrow P_k\ (S_p);\ P_k\ (S_p, R) \rightarrow X;$$

$$X\ (T\ (K_s, t))) \rightarrow B \rightarrow P_k\ (S_p).$$

Аутентифікація по ключам доступу. Ця модель використовується для аутентифікації пристроїв, сервісів чи інших додатків при звернені до веб-сервісів WS, що зберігаються на хмарному сервері - S_{ws}, засобом аутентифікації є ключ доступу - K_a. Модель має вигляд:

$$X(U_n, P_s) \rightarrow B \rightarrow S_{ws};\ S_{ws}(K_a) \rightarrow X;\ X(K_a) \rightarrow P_k\ (S_{ws}).$$

Аутентифікація по токенам. Дана модель аутентифікації застосовується при побудові розподілених систем Single Sing-On (SSO), де один додаток – SP (service provider) делегує функцію аутентифікації користувачів другому додатку IP (identity provider). Наприклад, вхід в додаток через обліковий запис в соціальних мережах. Токен $T(P_i)$ генерується $IP(P_i)$, де P_i – параметр токена. Модель має вигляд:

$$X(K_a) \rightarrow B \rightarrow IP;\ IP\ (n) \rightarrow B \rightarrow X;$$

$$X(H(n, K_s) \rightarrow B \rightarrow IP(T\ (P_i)) \rightarrow X;\ X(T\ (P_i)) \rightarrow SP.$$

Моделі ідентифікації базуються на трирівневому семифакторному підході класифікації ідентифікаторів [3]: (1) як характеристики приналежності – універсальний (U), корпоративний (C), особистий (P); (2) для розпізнання особистості власника – анонімний (N), персональний (I); (3) доступ власника до ресурсів – одноразовий (O) та багаторазовий (M). Отже в електронному просторі маємо різновид ідентифікацій представленої сімки: MCI = (UNM, UPO, UPM, CNO, CNM, CPM, IPM), де використані наступні

ідентифікатори: UNM - універсальний анонімний багаторазовий (користувач інтернету), UPO - універсальний персональний одноразовий (генератор одноразових паролей), UPM - універсальний персональний, що міститься в реєстрі (електронний паспорт), CNO - корпоративний анонімний одноразовий (банківська карта), CNM - корпоративний анонімний багаторазовий, CPM - корпоративний персональний багаторазовий (пропуск - смарт-карта), IPM - особистий персональний багаторазовий (біометрія на карті чи сервері). Виникає завдання вибору моделі аутентифікації та моделі ідентифікації з інтелектуальною підтримкою [2].

Розглянемо підхід для підтримки прийняття рішень по вибору моделей аутентифікації та моделей ідентифікації. Пропонується класифікація системи аутентифікації по ознакам виконання цілей та завдань [3]. Процес аутентифікації складається з послідовно виконуючих процедур двох класів: до першого відносяться процедури реєстрації нового користувача та зберігання інформації аутентифікації, до другого - процедури представлення інформації аутентифікації, протоколи обміну, валідація та прийняття рішення про результат проходження перевертючою стороною процесу аутентифікації. Модель класифікації аутентифікації - *MCA* – представимо трійкою :

$$MCA = \{A, W, C\},$$

де *A* - доступність (accessibility), *T* - цілістність (wholeness), *C* - конфіденційність (confidelity). Деталізації цілей та завдань виразимо таким чином:

$$A = \{GA, DA, CA, PA\};\ W = \{WS, WRR, WAP, WPC\};\ C = \{CPP, CAP, CPC\},$$

де *GA* - гарантія обробки запитів користувачів на аутентифікацію, *DA* - поділ доступу користувачів, *CA* - контроль доступу, *PA* - персоніфікація доступу; *WS* - цілісність ПО, *WRR* - цілісність облікових записів, *WAP* - цілісність аутентифікаційної інформації користувачів; *WSC* - цілісність аутентифікаційної інформації користувачів в хмарному середовищі; *CPP* - конфіденційність облікових записів, *CAP* - конфіденційність аутентифікаційної інформації користувачів, *CPC* - конфіденційність аутентифікаційної інформації користувачів в хмарному середовищі.

Висновок. Експертна система методом складання бази правил вибору допоможе підібрати найбільш безпечніший варіант системи ідентифікації та аутентифікації для мобільних додатків.

Література

1. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам / А.А. Афанасьев, М.: Горячая линия - Телеком, 2012. 550 с.
2. Вишняков В.А. Информационная безопасность в корпоративных системах, электронной коммерции и облачных вычислениях: методы, модели, программно-аппаратные решения / В.А. Вишняко, Минск: Бестпринт, 2016. - 276 с.
3. Сабанов А.Г. Принципы классификации систем идентификации и аутентификации по признакам соответствия требованиям информационной безопасности // Электросвязь, 2014, № 2. С. 6-9.