обчислювальна машина проводить аналіз створеної моделі злочинності. За результатами цього аналізу коригується початкова модель.

В статье рассмотрены подходы к созданию информационной системы, предназначенной для моделирования преступности. В работе предложена система обработки знаний, которая принимает форму системы поддержки принятия решений. При этом ЭВМ производит анализ созданной модели преступности. По результатам этого анализа вносятся корректировки в начальную модель.

In the article approaches for the creation of the informative system, intended for the design of criminality are represented. The system of treatment of knowledges, which takes a form of system of support of making a decision, is in-process offered. Thus computer is made by the analysis of the created model of criminality. On results this analysis adjustments are brought in in an initial model.

УДК 681.518

А. Л. ЄРОХІН,
д-р техн. наук, проф., ХНУВС
М. А. КУХАРЕНОК,
канд. техн. наук, доц., ХНУВС
О. П. ТУРУТА, *викл. ХНУВС*

РОЗРОБКА ФУНКЦІЇ ДОВІРИ ДЛЯ ПОКРАЩЕННЯ АЛГОРИТМУ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧА

Зростання популярності web-додатків приводить до підвищення вимог до функцій ідентифікації й автентифікації користувачів. Автентифікація – один з відповідальних етапів, на якому змінюється статус користувача, отже, цей етап може бути атакований. Нарощування захисту призведе до ускладнення процесу автентифікації й, отже, до погіршення якості роботи користувача.

Правила побудови моделей загроз і систем контролю доступу розглядали П. Н. Дев'янін [1], В. А. Галатенко [2]. Позначення етапів та функції роботи користувача визначені стандартами [3], [4], [5], але в них не вказано, як саме повинні реалізовуватись названі функції. В. Н. Томилін [6] розглядає методи автентифікації віддаленого сервера. Алгоритм автентифікації як частину моделі роботи сайту розглядає М. Ю. Биков [7]. Таким чином, актуальною є розробка засобів, що дозволяють покращити механізм ідентифікації й автентифікації користувача системою, а також механізми, що дозволяють користувачеві автентифікувати сервіс.

Мета даної статті – розробити засоби для покращення ефективності роботи алгоритму автентифікації користувача.

Користувач і комп'ютер взаємодіють із сервісом за допомогою програми – агента. Тоді завдання ідентифікації й автентифікації – дізнатися, хто управляє агентом і до якої групи користувачів належить користувач.

Для розв’язання основного завдання слід розробити функцію довіри агентові, яка буде враховувати дані, надані агентом, збирати відсутню інформацію про агента, враховувати етап, на якому обслуговується агент, а також оцінювати інформацію, отриману через неконтрольовані канали зв'язку.

Використання функції довіри спрямоване на:

– зменшення співвідношення помилок І-го й ІІ-го роду при автентифікації;

– виявлення спроб порушення режиму доступу й у той же визначення помилок користувача з позитивною історією роботи;

– зменшення кількості зайвих дій під час

збору відсутніх ознак.

Розглянемо схему механізму автентифікації (рис. 1.) і процес зміни статусів користувача.

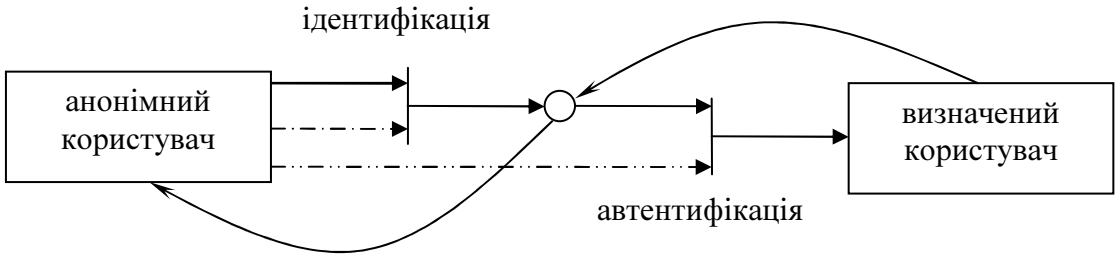

Рис. 1. Схема зміни статусу користувача

Умовні позначення

	Позначення статусу користувача	Користувач може будь-який необхідний час перебувати в такому статусі
	Проміжний статус користувача	Користувач ідентифікований, але ще не автентифікованний. Час перебування обмежений
	Контрольна точка	У цій контрольній точці перевіряються дії й відповідні параметри
	Дія	Задається користувачем або системою
	Дані ідентифікації	Задається користувачем
	Дані автентифікації	Задається користувачем

На початковому етапі користувач невідомий. Для проходження контрольної точки «ідентифікація» необхідно, щоб користувач виконав дію й указав логічне ім'я. Для підтвердження користувачеві необхідно вказати пароль. У разі успіху користувач стає впізнаним для системи.

Під час роботи користувач може втрачати ознаку «перевірений».

На рис. 2 наведені групи ознак, які сервіс одержує від агента. Частина ознак надається користувачем (клас доступу, порядок обходу сайту, виконувані дії, ім'я, пароль); інші ознаки збираються сервісом у процесі роботи.

Незважаючи на те, що ініціатива збирання ознак належить системі, користувач може модифікувати інформацію про себе. Залежно від можливості користувача впливати на значення ознак виділимо підмножини множини P_2.

Слід відзначити, що ознаки, які модифікують інформацію на рівні транспортного протоколу для глобальних мереж Web, можна вважати стабільними (на відміну від локальних мереж), тому що підмінити адресу простою заміною або підключенням до іншого сегмента, не порушуючи правил маршрутизації, складно. Для підміни адреси необхідно використати Proxy-сервер, bot-мережі, але це є підміною на прикладному рівні й санкціонованій дії агента.

Окремо необхідно виділити історію роботи агента. Інформація про неї зберігається з позитивною або негативною оцінкою. Ідентифікатором агента є IP або заявлене ім'я; додатково зберігаються заголовок, час роботи тощо.

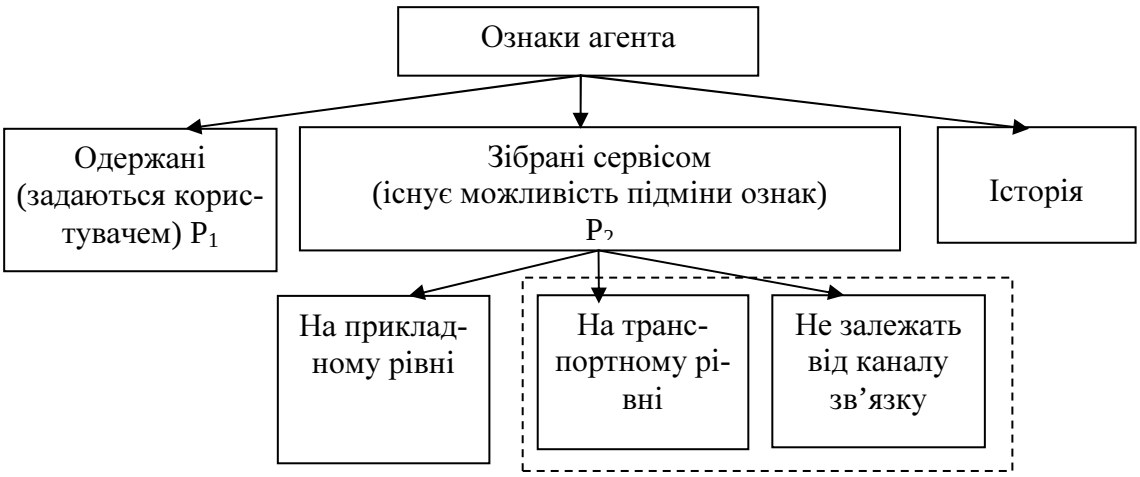

Рис. 2. Структура груп відомих ознак сервісу про агента

На основі проведеного аналізу роботи сервісу можна виділити такі проблеми, ознаки, що дозволяють їх ідентифікувати, й способи розв'язання проблем.

Проблема 1. Після успішної автентифікації агентом став управляти інший користувач (алгоритм).

Ознака: оцінка функції довіри роботи агента $< \Delta$. Змінений IP під час сесії, timeout сесії не вичерпаний; вичерпаний timeout сесії, IP, заголовок тощо залишилися незмінними; змінився консольний портрет користувача. Розв'язання: повторна автентифікація при збереженні колишньої ідентифікації (зміна статусу користувача).

Проблема 2. Дані для ідентифікації й автентифікації перехоплені, скопійовані, підроблені.

Ознака: оцінка функції довіри автентифікації $< \Delta$. Введення коректних даних ідентифікації й автентифікації, при зміні: IP; заголовку; операційної системи; браузера. Розв'язання: 1) використання механізму одноразового блокнота; 2) перевірка секретним каналом.

Проблема 3. Користувач системи кілька разів указував неправильні пари «ім'я користувача + пароль». Атака на помилку II-го роду.

Ознака: оцінка функції довіри користувачеві $> \Delta$. Зазначені логічне ім'я й пароль не відповідають образу, зазначеному в базі даних; інші ознаки відповідають попередньому підключенню. Розв'язання: внести негативний запис в історію зі зменшенням часу заборони повторного підключення $\tau() / \Delta$, де $\tau()$ – функція визначення часу заборони, а Δ – величина «пом'якшення».

Проблема 4. Сервіс експлуатує невідомий бот. Відбувається підбір параметрів. Агентом управляє алгоритм (у випадках, коли це небажано).

Ознака: оцінка функції довіри користувачеві $< \Delta$. Агентом управляє невідомий бот (алгоритм, програма); перевірка під час сесії не дозволила встановити, що агентом управляє людина або CAPTCHA-тест указав, що агентом управляє комп'ютер. Розв'язання: 1) виявляти відомі й корисні боти. Наприклад, роботи пошукових систем. Вони можуть бути ідентифіковані за заголовками і IP-адресами; 2) проводити виявлення невідомих ознак, а також провести CAPTCHA-тест.

Проблема 5. Зловмисник намагається перехопити дані автентифікації, підробити їх, замінити сервер, замінити клієнта. Можливо, були пропущені елементи послідовності.

Ознака: оцінка функції довіри web-додатку $> \Delta$. Неправильна автентифікація сервера; протягом сесії, після успішної автентифікації, виникають проблеми з обміном ключів. Розв'язання: проведення повторної ініціалізації процесу автентифікації.

Для обчислення функції довіри пропонується використати: 1) надані ознаки;

2) ознаки, отримані сервісом про агента; 3) дані з історії, зібраної за IP, логічним іменем; 4) час доступу як фактор застарівання даних історії; 5) клас доступу й послідовність обходу web-сервісу.

Нехай $AUTH$ - функція автентифікації, що обчислюється за двома аргументами D – оцінкою довіри й C – правилами політики безпеки. За умовою задачі, функція автентифікації одержує одне із двох значень: 0 – якщо ім'я агента не перевірене, 1 – якщо ім'я агента підтверджене.

Одержуємо $AUTH(D,C)=\{0,1\}$, де D – оцінка довіри, що обчислюється на основі двох груп ознак – P_1 і P_2, де P_1 – набір ознак, наданих агентом про себе, а P_2 – набір ознак, зібраних з ініціативи web-сервісу.

З урахуванням уведених вище позначень запишемо функцію автентифікації як $AUTH(D(P_1,P_2),C)$, де C – результат перевірки введених параметрів автентифікації, $D(P_1,P_2)$ – функція оцінки довіри на основі отриманих і зібраних ознак про агента. Значення функції автентифікації визначимо як:

$$AUTH(D(P_1,P_2),C)=\begin{cases}1, \text{если } C=1 \text{ и } D(P_1,P_2)>\Delta\\ 0, \text{в противном случае}\end{cases},$$

де Δ – рівень довіри для етапу автентифікації.

Функція довіри формує оцінку, що буде використана при переході на наступний етап. Процес обчислення функції може супроводжуватися збиранням необхідних ознак, отже, якщо ознаки невідомі в момент виклику функції, буде повернуто 0, а якщо ознаки стануть відомі, то може бути розглянута можливість повернення 1.

Покращений метод автентифікації за допомогою оцінки довіри агентові; по-перше, дозволяє поліпшити характеристики роботи алгоритму автентифікації й обслуговування агентів у web у цілому; по-друге, запобігає негативним впливам погроз, спрямованих на механізм автентифікації; по-третє, формує узагальнену оцінку за допомогою декількох ознак різної природи, що дозволяє виключити можливість навмисної підміни зловмисником.

Література

1. Девянин П. Н. Модели безопасности компьютерных систем [текст] / П. Н. Девянин : учеб. пособие для студ. высш. учеб. заведений. – М.: Издат. центр «Академия», 2005. – 144 с.
2. Галатенко В. А. Стандарты информационной безопасности [текст] / В. А. Галатенко [под ред. Бетенина В. Б.]. – М.: Интернет-университет информационных технологий, 2006. – 208 с.
3. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99.
4. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных систем. Ч.2. Функциональные требования: ГОСТ Р ИСО/МЭК 15408-2-2002. – М.: Изд-во стандартов, 2002. – 160 с.
5. ISO/IEC 27002 as ISO/IEC 17799:2005.
6. Томилин В. Н. Разработка методов аутентификации узлов распределенной ip-сети: автореф. дис. ... канд. техн. наук: 05.13.19 / Томилин Василий Николаевич. – СПб., 2002. – 18 с.
7. Быков М. Ю. Модель процесса обработки запросов системой управления web-сайтами [електронний ресурс] / М. Ю. Быков // Вычислительные методы и программирование. – С. 52-56. – Режим доступу: http://num-meth.srcc.msu.ru/.

Анотації

У роботі проводиться аналіз алгоритму автентифікації. Автори пропонують використовувати ознаки агентів, історію для визначення довіри до дій агента. Наводяться проблеми, які виникають під час роботи агента з сервісом та пропонуються методи визначення причини проблемі та шляхи подолання. Як ефективний інструмент для визначення проблемних моментів запропонована функція оцінки довіри.

В отчете рассматривается алгоритм аутентификации. Предлагается использовать различные признаки агентов, историю их работы для оценки доверия действию агента. Проводится анализ проблем, признаки и способы их решения. Предлагается метод оценки доверия для улучшения работы алгоритм аутентификации.

In the paper algorithm of authentication is determined. The analysis of problems, sign and methods of their decision are conducted. The method of estimation of trust is offered for the improvement of work algorithm of authentication

УДК 681.3

О. Ф. ЛАНОВИЙ,
канд. техн. наук, доц. ХНУВС
І. В. КОБЗЕВ, *канд. техн. наук, доц. ХНУВС*
О. С. УДОВЕНКО, *аспірант ХНУРЕ*

СИСТЕМА ПІДРАХУНКУ ТРАФІКУ МЕРЕЖІ З ВИКОРИСТАННЯМ ЗАСОБІВ ОБ'ЄКТНО-ОРІЄНТОВАНОГО ПРОГРАМУВАННЯ

Проблема обміну інформацією між комп'ютерами існує з часу виникнення обчислювальної техніки. Вона полягає в ефективній організації спільної роботи окремих комп'ютерів, що дозволяє вирішувати одну задачу за допомогою декількох комп'ютерів, спеціалізувати кожен із комп'ютерів на виконання певної функції, спільно використовувати ресурси тощо. Існує безліч засобів обміну інформацією: від простого перенесення файлів за допомогою носіїв інформації до використання глобальної комп'ютерної мережі Інтернет, яка здатна пов'язати всі існуючі комп'ютери.

Найчастіше під терміном «локальні мережі» (LAN (Local Area Network)) розуміють такі мережі, які мають невеликі, локальні розміри і з'єднують близько розташовані комп'ютери. Проте досить поглянути на характеристики деяких локальних мереж, щоб зрозуміти, що таке визначення не дуже точне. Здебільшого локальна мережа позв'язує від двох до декількох десятків комп'ютерів. Але граничні можливості деяких локальних мереж набагато вищі: максимальна кількість абонентів може досягати тисяч. Називати таку мережу малою, напевно, неправильно.

У свою чергу, більшість локальних мереж підключена до глобальної комп'ютерної мережі Інтернет. Підключення здійснюють провайдери, що надають послуги як з обслуговування локальної мережі, так і з доступу до мережі Інтернет. Провайдери повинні забезпечувати: якісний підрахунок використовуваного користувачами мережі трафіку, тарифікацію користувачів, своєчасне відключення неплатників, спрощення способів оплати і ін.

Для вирішення цих завдань були запропоновані системи обліку трафіку і системи білінгу. Звичайно ці дві системи використовуються разом і реалізуються як програмний комплекс, призначений для обліку й управління трафіком у локальних мережах.

Найбільш прості системи обліку трафіку виконують такі операції:

– збирання даних;

– підсумовування даних;

– збереження суми в базі даних або лог-файлі;

– надання даних відповідно до запитів;

– сигналізація зовнішній програмі про перевищення трафіку.

Подальшим розвитком систем обліку трафіку є створення білінгових систем, до визначальних особливостей яких можна віднести:

– розвинений інтерфейс управління, налаштування, запитів для клієнтської частини;

– перерахунок значень лічильників у грошове вираження відповідно до тарифного плану;