УДК 519.711.3:343.98

В.А. Колган

ІДЕНТИФІКАЦІЯ КОРИСТУВАЧІВ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ СИСТЕМ

Вінницький національний технічний університет

Анотація

Було розглянуто та проаналізовано сучасні підходи, які використовуються для ідентифікації користувачів комп'ютерних систем, особливо важливі у зв'язку з актуальністю проблеми захисту комп'ютерної інформації та обмеженням доступу до інформаційних та технічних ресурсів комп'ютера.

Ключові слова: захист комп'ютерної інформації, ідентифікація користувачів.

Abstract

The modern approaches used to identify users of computer systems were considered and analyzed, especially important in connection with the urgency of the problem of the protection of computer information and limitation of access to computer information and technical resources.

Keywords: protection of computer information, identification of users.

Питання захисту інформації в комп'ютерних системах вирішується для того, щоб ізолювати нормально функціонуючу інформаційну систему від несанкціонованих управляючих дій і доступу сторонніх осіб або програм до комп'ютерних даних, що захищаються [1].

Щоб користувач отримав можливість працювати з програмним продуктом, його має бути авторизовано. Після цього він може запускати від свого імені процес, який інтерпретує введені ним команди і транслює їх у системні виклики, що дає йому змогу виконувати дії з файлами та користування програмним продуктом.

У захищених системах авторизація здійснюється лише після ідентифікації й аутентифікації користувача. Ідентифікація складається з двох процедур: присвоєння об'єкту (суб'єкту) ідентифікатора та розпізнавання об'єкта за наданим ідентифікатором. У програмних продуктах стосовно користувачів перша процедура полягає у створенні облікового запису користувача — цю процедуру виконує адміністратор. Друга процедура полягає у введенні користувачем свого ідентифікатора у відповідь на запит системи. Ідентифікатором може бути умовне ім'я або певне число.

Для підтвердження того, що користувач насправді є тим, за кого себе видає, проводиться автентифікація, яка вимагає від користувача введення додаткової інформації. Сьогодні існує декілька способів ідентифікації користувачів. У кожного з них є свої переваги і недоліки, завдяки чому деякі технології підходять для використання в одних системах, інші в інших.

Метою роботи є вдосконалення методу ідентифікації/аутентифікації користувача під час роботи з програмними продуктами використовуючи провідні технологій у сфері проектування програмного забезпечення.

Об'єктом дослідження є процеси створення програмного модуля для входу у програму.

Предметом дослідження є методи і засоби побудови програмного модуля ідентифікації/ аутентифікації користувача ПЗ.

Існує три найпоширеніших види ідентифікації:

1. Парольна ідентифікація. Ще не дуже давно парольна ідентифікація була ледве не єдиним способом визначення особистості користувача. І в цьому немає абсолютно нічого дивного. Справа в тому, що парольна ідентифікація найбільш проста як у реалізації, так й у використанні. Суть її зводиться до наступного. Кожен зареєстрований користувач якої-небудь системи одержує набір персональних реквізитів (звичайно використаються пари логін-пароль). Далі при кожній спробі входу він повинен вказати свою інформацію. Оскільки вона унікальна для кожного користувача, то на підставі її система й робить висновок про особистість та ідентифікує її.

Головна перевага парольної ідентифікації – це простота реалізації й використання. Крім того, введення парольної ідентифікації не вимагає зовсім ніяких витрат: даний процес реалізований у більшості програмних продуктів.

Головний недолік – величезна залежність надійності ідентифікації від самих користувачів, точніше, від обраних ними паролів. Більшість людей використовують ненадійні ключові слова, які легко підбираються. До них відносяться занадто короткі паролі, загальновідомі сполучення символів і т.д.

2. Апаратна (або електронна) ідентифікація. Цей принцип ідентифікації ґрунтується на визначенні особистості користувача по якомусь предметі, ключу, що перебуває в його ексклюзивному користуванні. Природно, мова йде не про звичні для більшості людей ключі, а про спеціальні електронні [2]. На даний момент найбільше поширення одержали два типи пристроїв: різноманітні карти (проксіміті-карти, смарт-карти, магнітні карти і т.д.) та так званні токени (token), які підключаються безпосередньо до одного з портів комп'ютера.

Головним достоїнством застосування апаратної ідентифікації є досить висока надійність. І дійсно, у пам'яті токенів можуть зберігатися ключі, підібрати які досить складно. Крім того, в них реалізовано чимало різних захисних механізмів. Ну а вбудований мікропроцесор дозволяє електронному ключу не тільки брати участь у процесі ідентифікації користувача, але й виконувати деякі інші корисні функції.

Найбільш серйозною небезпекою у випадку використання апаратної ідентифікації є можливість крадіжки зловмисниками токенів або карт у зареєстрованих користувачів. Також вони можуть бути втрачені, передані іншій особі, дубльовані. Другий мінус розглянутої технології – ціна. Для введення в експлуатацію системи такої ідентифікації однаково будуть потрібні деякі вкладення. Для кожного зареєстрованого користувача потрібно забезпечити персональними токенами.

3. Біометрична ідентифікація. Біометрія – це ідентифікація людини по унікальним, властивим тільки їй біологічним ознакам. біометричні технології споконвічно розроблялися для точного встановлення особистості людини. А тому рішення використати їх в області інформаційної безпеки виглядає цілком логічним. Причому даний напрямок розвивається дуже активно. Сьогодні експлуатується вже більше десятка різних біометричних ознак [3]. Причому для найпоширеніших з них (відбитки пальців і райдужна оболонка ока) існує безліч різних за принципом дії сканерів.

Головним достоїнством біометричних технологій є найвища надійність. двох людей з однаковими відбитками пальців у природі просто не існує.

Таким чином, розглянувши технології апаратної (або електронної), парольної, біометричної ідентифікації та аутентифікації можна зробити висновок, що надалі у міру зростання обчислювальних потужностей все більш запитаним буде саме вживання біометричної ідентифікації та аутентифікації, що дозволить уникнути людських помилок, зв'язаних із застосуванням слабких паролів і посилити вимоги до парольної аутентифікації. Разом із тим, наявні ПЗ не виконують основні проблеми ідентифікації/аутентифікації користувача під час роботи з ПЗ, що зумовлює потребу у розробці нового програмного модуля.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Галатенко В.А. Основы информационной безопас- ности: учебное пособие / В. А. Галатенко; под ред. акаде- мика РАН В.Б. Бетелина, 4-е изд. – М.: Интернет- Университет Информационных технологий; БИНОМ. Лаборатория знаний, 2008. – 205 с.

2. Джхунян В.Л. Электронная идентификация / В.Л. Джхунян, В.Ф. Шаньгин. – М.: NT Press, 2004. – 695 с. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / В. П. Горбулін, О. Г. Додонов, Д. В. Ланде. – К.: Інтертехнологія, 2009. – 164 с.

3. Голубев Г.А. Современное состояние и перспекти- вы развития биометрических технологий / Г.А. Голубев, Б.А. Габриелян // Нейрокомпьютеры: разработка, приме- нение. – 2004. – № 10. – С. 39-46.Кара-Мурза, С. Г. Манипуляция сознанием. - М.: Эксмо, 2006.-832 с.

Вікторія Альбертівна Колган — студентка групи УБ-14б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: vikusha.kolgan@gmail.com.

Науковий керівник: ***Азарова Анжеліка Олексіївна —*** кандидат технічних наук, професор кафедри МБІС, заступник декана ФМІБ з наукової роботи та міжнародного співробітництва.

Kolgan Victoriia A. — student, faculty of management and information security, Vinnytsia National Technical University, Vinnytsia, email: vikusha.kolgan@gmail.com.

Supervisor: **Azarova Anzhelica O. -** candidate of technical sciences, professor of the department of MBIS, deputy of the dean of the Institute for Scientific Research and International Cooperation.