УДК 681.3

ІДЕНТИФІКАЦІЯ ТА АУТЕНТИФІКАЦІЯ КОРИСТУВАЧІВ КОМП'ЮТЕРНИХ СИСТЕМ В ЗАДАЧАХ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Н. І. Мазниченко
Національний університет «Юридична академія України ім. Ярослава Мудрого»
maznichenko_nata@ukr.net

Створення єдиної, централізованої системи безпеки є необхідною умовою існування сучасної інформаційної інфраструктури. Останнім часом у зв'язку зі збільшенням загроз для комп'ютерної інформації все більше уваги приділяється задачам вдосконалення існуючих та розробці нових засобів захисту інформаційних комп'ютерних систем від небажаного доступу з боку неавторизованих користувачів. Основними функціями системи захисту від несанкціонованого доступу до ресурсів комп'ютерних систем є, перш за все, ідентифікація та підтвердження достовірності користувачів при доступі до обчислювальної системи а також розмежування їх доступу до комп'ютерних ресурсів.

Система ідентифікації і аутентифікації є одним з ключових елементів інфраструктури захисту від несанкціонованого доступу будь-якої інформаційної комп'ютерної системи.

Ідентифікація - це пред'явлення користувачем якогось унікального, властивого тільки йому ідентифікатора (ознаки). Аутентифікація дозволяє переконатись, що суб'єкт дійсно той, за кого він себе видає.

Як синонім слова «аутентифікація» іноді використовують словосполучення «перевірка достовірності».

Сьогодні існує декілька способів ідентифікації та аутентифікації користувачів. У кожного з них є свої переваги і недоліки, тому як розроблювачам програмного забезпечення, так і користувачам потрібно самостійно обирати, який спосіб реалізовувати у власних інформаційних комп'ютерних системах.

Існують наступні найпоширеніші підходи до ідентифікації та аутентифікації:

1). Парольна ідентифікація та аутентифікація. Суть її зводиться до наступного. Кожен зареєстрований користувач якої-небудь комп'ютерної системи одержує набір персональних реквізитів (звичайно використаються пари логин-пароль). Далі при кожній спробі входу він повинен вказати свою інформацію. Ну а оскільки вона унікальна для кожного користувача, то на підставі її система й робить висновок про особистість та ідентифікує її. Головна перевага даного підходу - це простота реалізації і використання. Крім того, введення парольної ідентифікації не вимагає зовсім ніяких витрат: даний процес реалізований у більшості програмних продуктів. Недоліки цього підходу добре відомі, пароль може бути скомпрометований безліччю способів. Парольний захист на сьогодні є одним з найпоширеніших способів захисту інформації від несанкціонованого доступу як в окремих комп'ютерах, так і в мережах світового масштабу.

2). Апаратна (електронна) ідентифікація та аутентифікація. Цей принцип ґрунтується на визначенні особистості користувача по якомусь предметі, електронному ключу, що перебуває в його ексклюзивному користуванні. На даний момент найбільше поширення одержали два типи пристроїв: всілякі 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, у них реалізовано чимало різних захисних механізмів. Ну а наявність вбудованого мікропроцесору дозволяє електронному ключу не тільки брати участь у процесі ідентифікації користувача, але й виконувати деякі інші корисні функції. Ну а тепер розглянемо недоліки цього підходу. Мабуть, найбільш серйозною небезпекою є можливість крадіжки зловмисниками токенів або карт у зареєстрованих користувачів. Також вони можуть бути втрачені, передані іншій особі, дубльовані. Другий мінус розглянутої технології – ціна, яку на сьогоднішній день неможливо вважати загальнодоступною.

3). Біометрична ідентифікація та аутентифікація. Біометрія - це визначення людини по унікальним, властивим тільки їй біологічним ознакам. Тобто, можна сказати, що біометричні технології споконвічно розроблялися для точного встановлення особистості людини. А тому рішення використовувати їх в області інформаційної безпеки виглядає цілком логічним. Причому даний напрямок розвивається дуже активно. Сьогодні експлуатується вже більше десятка різних біометричних ознак. Для найпоширеніших з них (відбитки пальців і райдужна оболонка ока) існує безліч різних за принципом дії сканерів. Головною перевагою біометричних технологій є найвища надійність. Основним недоліком біометричної ідентифікації є вартість устаткування, адже для кожного комп'ютера, що входять до цієї системи, необхідно придбати власний сканер.

Розглянуті вище однофакторні системи ідентифікації та аутентифікації користувачів на

сьогоднішній день не можна назвати надійними. Саме тому поступово все більшого поширення одержує багатофакторна ідентифікація та аутентифікація, коли для визначення особистості користувача застосовується відразу кілька параметрів. Втім, сьогодні в переважній більшості випадків використовується тільки одна пара: парольний захист і токен. У цьому випадку користувач може не боятися підбора його пароля зловмисником (без електронного ключа пароль працювати не буде), а також крадіжки токена (він не буде працювати без пароля). Втім, у деяких системах застосовуються одночасно паролі, токени й біометричні характеристики людини і саме такі системи можна назвати максимально надійними.

На основі аналізу загроз інформаційній безпеці, та існуючих засобів ідентифікації та аутентифікації користувачів комп'ютерних систем, можна впевнено зробити висновок, що надалі у міру зростання обчислювальних потужностей все більш запитаним буде саме вживання систем багатофакторної ідентифікації та аутентифікації, що дозволить значно підвищити рівень надійності цих систем. Щодо вибору системи ідентифікації та аутентифікації безпосередньо в кожній окремій ситуації, користувач повинен: об'єктивно оцінити співвідношення цінності інформації, що захищається, і вартості програмно-апаратного забезпечення ідентифікації/аутентифікації (включаючи супровід); оцінити зручність у використанні (контактні, безконтактні) та сприйняття обраного підходу користувачами; визначити потрібний рівень захищеності («що» і від «кого» потрібно захищати). Але безперечною порадою є використання комплексної системи ідентифікації та аутентифікації, яка поєднує декілька підходів до вирішення задач доступу до інформаційних ресурсів комп'ютерних систем.