В.А. Іванюк, студ., V курс, гр. СІ-66м, ФІКТ
П.М. Повідайко, к.т.н., доц.
Житомирський державний технологічний університет

ДОСЛІДЖЕННЯ МЕТОДІВ ІДЕНТИФІКАЦІЇ ОСОБИ В СИСТЕМАХ КОНТРОЛЮ ДОСТУПУ НА ОБ'ЄКТ

З появою і розвитком нових інформаційних технологій стала актуальна проблема інформаційної безпеки, пов'язана із забезпеченням збереження і конфіденційності інформації, що оброблюється та зберігається в комп'ютерних системах. Важливим елементом забезпечення цілісності конфіденційної інформації є захист від несанкціонованого доступу до ресурсів інформаційних систем, що викликає необхідність створення надійних і зручних систем контролю доступу. Система ідентифікації є одним з ключових елементів інфраструктури захисту від несанкціонованого доступу будь-якої інформаційної комп'ютерної системи. Доступ користувачів до різних класів інформації визначається ідентифікацією, тобто процесом розпізнавання параметрів, що однозначно визначають особу користувача.

Сьогодні існують наступні найпоширеніші підходи до ідентифікації користувачів.

Парольна ідентифікація.

Суть її зводиться до наступного. Кожен зареєстрований користувач будь-якої комп'ютерної системи одержує набір персональних реквізитів. Далі при кожній спробі входу він повинен вказати свою інформацію. Оскільки вона унікальна для кожного користувача, то на її підставі система робить висновок про особу 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. Таким чином, система захисту інформації виявляється простою і доступною.

На жаль, даний метод має багато недоліків. І самий головний - повна залежність надійності ідентифікації від самих користувачів, точніше, від обраних ними паролів. Справа в тому, що більшість людей використовують ненадійні ключові слова, які легко підбираються. Крім того, пароль можна легко підгледіти або користувач навмисно передасть пароль іншій особі.

Апаратна (електронна) ідентифікація.

Цей принцип ідентифікації ґрунтується на визначенні особи користувача по якомусь предметі, ключу, що перебуває в його ексклюзивному користуванні. 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.

Головною перевагою 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.

Говорячи про недоліки апаратної ідентифікації, то 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 такої системи ідентифікації будуть потрібні чималі вкладення. Все-таки кожного зареєстрованого користувача потрібно забезпечити персональними токенами. Крім того, згодом деякі типи ключів можуть зношуватися, можуть бути загублені і т.д.

Біометрична ідентифікація.

Біометрія – це ідентифікація людини за унікальними, властивими тільки їй біологічними ознаками. Тобто, можна сказати, що біометричні технології розроблялися для точного встановлення особи людини, 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.

Серед біометричних механізмів ідентифікації можна виділити такі:

- по статичних ознаках — те, що практично не міняється з часом, починаючи з народження людини (фізіологічні характеристики);
- по динамічних ознаках — поведінкові характеристики, тобто ті, які побудовані на особливостях, характерних для підсвідомих рухів в процесі відтворення якої-небудь дії. Динамічні ознаки можуть змінюватися з часом, але не різко, а поступово.

Серед статичних методів ідентифікації користувача на сьогодні використовуються наступні: ідентифікація по відбитку пальця, по розташуванню вен на долоні, по сітківці ока, по веселковій оболонці ока, за формою грона руки, за формою обличчя.

Серед динамічних методів можна назвати наступні: ідентифікація по голосу, по почерку, по клавіатурному почерку.

При всьому теоретичному різноманітті біометричних методів, на практиці серед них застосовуються небагато. Основних методів три – розпізнавання по відбитку пальця, по зображенню особи (двомірному або тривимірному) і по веселковій оболонці або сітківці ока.

Головною перевагою біометричних технологій є найвища надійність. І дійсно, усі знають, що двох людей з однаковими відбитками пальців у природі просто не існує.

Основним недоліком біометричної ідентифікації є вартість устаткування. Адже для кожного комп'ютера, що входять до системи, необхідно придбати власний сканер. Але слід відзначити, що останнім часом ціни на біометричні пристрої постійно знижуються.

Багатофакторна ідентифікація.

В цьому випадку для визначення особи застосовується відразу кілька параметрів. Причому комбінуватися ці фактори можуть у довільному порядку. Втім, сьогодні найчастіше використовується тільки одна пара: парольний захист і токен. У цьому випадку користувач може не боятися, що його пароль буде підібраний зловмисником (без електронного ключа пароль працювати не буде), а також крадіжки токена (він не буде працювати без пароля). У деяких системах застосовуються максимально надійні процедури ідентифікації: у них одночасно використовуються паролі, токени й біометричні характеристики людини.

Впровадження комбінованих систем суттєво збільшує кількість ідентифікаційних ознак і тим самим підвищує безпеку.

Детальніше розглянувши вищевказані методи, можна впевнено сказати, що найперспективнішим нині методом є біометрична ідентифікація. У разі ідентифікації за індивідуальними біометричними ознаками визначається особа як носій цих ознак, а не виданий їй документ (картка, код, ключ тощо). Це і є основною відмінністю цих систем від будь-яких інших пристроїв ідентифікації, оскільки унеможливлює втрату, крадіжку ідентифікатора, а також ускладнює чи й взагалі унеможливлює його підробку. Але не існує єдиної біометричної технології, яка підійшла б для всіх потреб. Всі мають переваги і недоліки.

На українському ринку біометричні пристрої з‘явилися для унеможливлення доступу до комп’ютерних систем і мережевих ресурсів. З часом їх кількість і області застосування значно зросли. Ці системи основані на методах ідентифікації за відбитками пальців. Вони невеликих розмірів, зручні і прості в користуванні. Крім того, технологія розпізнавання за відбитками пальців може бути інтегрована без особливих затрат в уже наявні системи безпеки. Використання даного методу біометричної ідентифікації забезпечує унікальні можливості. Швидкість операції розпізнавання або ідентифікації у сучасних системах навіть за наявності великої кількості користувачів вимірюється секундами, тобто відповідає запитам виробничого режиму.

Як приклад, термінал Ridge Reader, запропонований американською фірмою Fingermatrix, який завдяки процедурі компенсації різних відхилень, що виникають при знятті відбитка пальця в реальних умовах, а також завдяки способу «очищення» зображення і відновлення папілярного візерунка (який може бути «затуманений» через наявність на пальці бруду , масла або поту) допускає коефіцієнт помилок 1-го роду не більше 0,1%, 2-го роду - не більше 0,0001%. Час обробки зображення становить 5 с, реєстрації користувача становить 2-3 хв. Для зберігання одного цифрового способу відбитка (еталона) витрачається 256 байт пам'яті.

Сказане дає підстави для висновку: біометрика й основані на її принципах системи стали ефективним засобом убезпечення всіх видів власності, захисту від шахрайства та фальсифікації. Подальше їх впровадження в різні галузі є актуальним завданням, адже забезпечить створення зручних і надійних інструментів як для державного сектору, індустріальних і комерційних структур, так і для окремих громадян.