УДК 621.395

Канівець В.Г.,
Сомов С.В., к.т.н., доцент,
Полтавський національний технічний
університет імені Юрія Кондратюка

АВТЕНТИФІКАЦІЯ КОРИСТУВАЧІВ КОМП'ЮТЕРНИХ СИСТЕМ

У статі проведено детальний аналіз існуючих на даний час систем автентифікації: парольна, апаратна, біометрична. Виконано класифікацію систем доступу до інформації. Розглянуто загальні переваги та недоліки систем. Наведено основні характеристики систем автентифікації. Надано загальну модель роботи систем автентифікації користувачів комп'ютерної системи.

Ключові слова: *захист інформації, системи автентифікації, парольна, апаратна, біометрична автентифікація.*

Вступ

У зв'язку з загальним розповсюдженням комп'ютерних технологій все гострішою постає проблема захисту інформації в комп'ютерних системах. Тому дуже актуальним бачиться теоретичні розробки в області захисту комп'ютерної інформації та практичне їх застосування безпосередньо в певних конкретних комп'ютерних системах. 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. Створення єдиної, централізованої системи безпеки є необхідною умовою існування сучасної інформаційної інфраструктури [1].

Основна частина

Система ідентифікації і автентифікації є одним з ключових елементів інфраструктури захисту від несанкціонованого доступу (НСД) до будь-якої інформаційної системи [2].

Несанкціонований доступ до інформації – доступ до закритої для публічного доступу інформації з боку осіб, котрі не мають привілеїв, для отримання її.

Задачею систем ідентифікації і автентифікації є визначення та надання набору правил, при доступі до інформаційної системи.

Процедури ідентифікації та автентифікації нерозривно пов’язані між собою, тому що визначення повноважень проводиться так, що користувач повинен надати та яким способом, щоб отримати доступ.

Існує три найпоширеніших способів автентифікації:

1. Парольна автентифікація. Кожен суб'єкт комп'ютерної системи має пароль - секрет, який він розділяє з системою. Демонстрація знання цього секрету приймається системою як підтвердження ідентичності суб'єкта. В якості пароля зазвичай вибирається літерна і (або) цифрова послідовність, яку користувач легко може запам'ятати і при необхідності ввести за запитом системи. Різні парольні протоколи розрізняються за засобами, якими зберігається парольна інформація всередині системи, і за методами її перевірки.

Можна виділити три основні загрози протоколам парольної автентифікації:

- розголошення;
- прослуховування;
- вгадування пароля.

Загрози можуть проявитися при здійсненні трьох характерних видів атак на парольні протоколи: при повторі паролів легальних користувачів зловмисниками, повному переборі паролів та при словниковій атаці на протокол.

На практиці широко використовуються два типи протоколів парольної автентифікації: протоколи з фіксованими і з одноразовими паролями.

1.1. Фіксовані паролі. Цей тип протоколів об'єднує ті з них, в яких пароль, який пред'являється системі, не змінюється від одного сеансу виконання протоколу до іншого. Пароль повинен бути таким, що запам'ятовується для людини (зазвичай не більше 8-12 символів), час дії пароля обмежена розумними межами, паролі повинні періодично змінюватися. Для забезпечення достатньої стійкості протоколів автентифікації з фіксованими паролями використовується ряд прийомів:

- зберігання в комп'ютерній системі файлів паролів в захищеному режимі;
- зберігання в системі не самих паролів, а їх образів, отриманих як результат обчислення односпрямованої функції від пароля, взятого в якості аргументу;
- завдання правил вибору паролів (мінімальна кількість символів, недопущення використання осмислених слів, необхідність поєднання букв і цифр і т.д), що мають на меті максимізувати ентропію пароля;
- штучне уповільнення процесу введення пароля в систему з метою різкого збільшення часу на перебір паролів;
- вибір в якості пароля осмисленої пропозиції (фрази) з подальшим перетворенням за допомогою хеш-функції в коротке повідомлення, яке зазвичай має більшу ентропію, ніж пароль такої ж довжини, обраний людиною;
- додавання системою випадкової величини до паролю перед обробкою його односпрямованої функцією (метод солтінгу).

Різновидом фіксованих паролів є PIN-коди (від англійських слів - Personal Identification Number). Це числові паролі довжиною від 4 до 8 десяткових цифр. Найчастіше вони використовуються в поєднанні з методом «володіння чимось»: зазвичай з мікропроцесорною пластиковою карткою або картою з магнітною смугою. PIN-код забезпечує другий рівень захисту на випадок, якщо карта втрачена або вкрадена. Для захисту від повного перебору такого

маленького ключового простору необхідні додаткові заходи: організаційний і фізичний захист.

1.2. Одноразові паролі. У протоколах цього типу кожен пароль використовується тільки один раз, так як пароль є функцією деякого аргументу.

Відомі три підходи до побудови протоколів автентифікації з одноразовими паролями:

- Спільні списки одноразових паролів.
- Послідовно оновлюванні одноразові паролі
- Послідовності одноразових паролів, засновані на односпрямованих функціях[3].

2. Апаратна автентифікація. Кожен апаратний (електронний) ідентифікатор є фізичним пристроєм, зазвичай невеликих розмірів для зручності його носіння з собою. До складу електронних систем ідентифікації і автентифікації входять:

- Переносні токени:

–асинхронні – користувач вводить рядок в пристрій, отримує відповідь і вводить її в комп'ютер;

–PIN/асинхронні – асинхронний метод доповнюється введенням PIN-коду в пристрій;

–синхронні – наприклад, токен синхронізований за часом з сервером і генерує для даного користувача в дану хвилину пароль, який вже і вводиться в систему;

–PIN/синхронні.

- Різноманітні карти – це пристрої, схожі на переносні автентифікатори, але складніші по своєму складу.

Карти бувають:

- пасивні (карти з пам'яттю);
- активні (інтелектуальні карти).

За допомогою смарт-карти проводиться розрахунок одноразових паролів і здійснюється взаємодія з пристроєм через картридер. Після введення PIN-коду

картридер сам запрошує смарт-карту, і подальший процес протікає без участі людини, завдяки чому можна використовувати достатньо довгі ключі.

Поняття USB-ключ, розглянемо на прикладі eToken від компанії Aladdin Software.

eToken – персональний засіб автентифікації і зберігання даних, що апаратно підтримує роботу з цифровими сертифікатами і електронними цифровими підписами (ЕЦП). eToken може бути виконаний у вигляді USB-ключа або стандартної смарт-карти. eToken підтримує роботу і інтегрується зі всіма основними системами і додатками, що використовують технології смарт-карт або PKI (Public Key Infrastructure).

Основне призначення:

- двофакторна автентифікація користувачів при доступі до захищених ресурсів (комп'ютерів, мереж, додатків);
- безпечне зберігання закритих ключів цифрових сертифікатів, криптографічних ключів, профілів користувачів, налаштувань додатків і інше в незалежній пам'яті ключа;
- апаратне виконання криптографічних операцій в довіреному середовищі (генерація ключів шифрування, симетричне і асиметричне шифрування, розрахунок хеш-функції, формування ЕЦП).

eToken як засіб автентифікації підтримується більшістю сучасних операційних систем, бізнес додатків і продуктів з інформаційної безпеки.

Можливості застосування:

- сувора автентифікація користувачів при доступі до серверів, баз даних, розділів Web-сайтів;
- безпечне зберігання секретної інформації: паролів, ключів шифрування, закритих ключів, цифрових сертифікатів;
- захист електронної пошти (цифровий підпис і шифрування, доступ);
- системи електронної торгівлі, «клієнт-банк»;
- «домашній банк»;
- захист комп'ютерів;

•захист мереж та каналів передачі даних за рахунок побудови VPN (virtual private network – віртуальні приватні мережі);

•клієнт-банк, home-банк.

eToken забезпечує:

•автентифікацію користувачів за рахунок використання криптографічних методів;

•безпечне зберігання ключів шифрування і ЕЦП, а також закритих ключів цифрових сертифікатів для доступу до захищених корпоративних мереж і інформаційних ресурсів;

•мобільність користувача і можливість безпечної роботи з конфіденційними даними в недовіреному середовищі (наприклад, на чужому комп'ютері) за рахунок того, що ключі шифрування і ЕЦП генеруються ключем eToken апаратно і не можуть бути перехоплені;

•безпечне використання – скористатися ключем eToken може тільки його власник, що знає PIN-код ключа;

•реалізацію як західних та російських, так і вітчизняних стандартів на шифрування і ЕЦП;

•зручність роботи – ключ виконаний у вигляді брелка зі світловою індикацією режимів роботи і безпосередньо підключається до USB-портів, якими зараз оснащені 100% комп'ютерів, не вимагає спеціальних зчитувачів, блоків живлення, проводів і т.д.;

•використання одного ключа для вирішення безлічі різних завдань – входу в комп'ютер, входу в мережу, захисту каналу, шифрування інформації, ЕЦП, безпечного доступу до захищених розділів Web-сайтів, інформаційних порталів і т.д.

Основними компонентами безконтактних пристроїв є чип і антена. Ідентифікатори можуть бути як активними (з батареями), так і пасивними (без джерела живлення). Ідентифікатори мають унікальні 32/64 розрядні серійні номери.

3. Біометрична автентифікація. Останнім часом все більшого поширення набуває біометрична автентифікація користувача, що дозволяє впевнено автентифікувати потенційного користувача шляхом вимірювання фізіологічних параметрів і характеристик людини, особливостей його поведінки. Основні переваги біометричних методів:

- високий ступінь достовірності автентифікації за біометричними ознаками (через їх унікальність);
- невіддільність біометричних ознак від дієздатної особи;
- труднощі фальсифікації біометричних ознак.

Активно використовуються такі біометричні ознаки:

- відбитки пальців;
- геометрична форма кисті руки;
- форма і розміри особи;
- особливості голосу;
- візерунок райдужної оболонки і сітківки очей.

Розглянемо типову схему функціонування біометричної підсистеми автентифікації. При реєстрації в системі користувач повинен продемонструвати один або кілька разів свої характерні біометричні ознаки. Ці ознаки реєструються системою як контрольний «образ» (біометричний підпис) законного користувача. Цей образ користувача зберігається системою в електронній формі і використовується для перевірки ідентичності кожного, хто видає себе за відповідного законного користувача. Залежно від збігу або розбіжності сукупності наданих ознак із зареєстрованими в контрольному образі, той хто надав їх визнається законним користувачем (при збігу) або незаконним (при розбіжності).

З точки зору споживача, ефективність біометричної автентифікаційної системи характеризується двома параметрами:

- коефіцієнтом помилкових відмов FRR (false-reject rate);
- коефіцієнтом помилкових підтверджень FAR (false-alarm rate).

Помилкові відмови виникають, коли система не підтверджує особистість законного користувача (типові значення FRR - близько однієї помилки на 100).

Помилкове підтвердження відбувається в разі підтвердження особи незаконного користувача (типові значення FAR - близько однієї помилки на 10000).

Ці коефіцієнти пов'язані один з одним: кожному коефіцієнту помилкових відмов відповідає певний коефіцієнт помилкових підтверджень.

У досконалої біометричної системи обидва параметри помилки повинні бути рівні нулю. На жаль, біометричні системи теж не ідеальні. Зазвичай системні параметри налаштовують так, щоб досягти необхідного коефіцієнта помилкових підтверджень, що визначає відповідний коефіцієнт помилкових відмов.

3.1. Дактилоскопічні системи автентифікації. Одна з основних причин широкого поширення таких систем - наявність великих банків даних відбитків пальців. Користувачами подібних систем головним чином є поліція, різні державні та деякі банківські організації.

У загальному випадку біометрична технологія розпізнавання відбитків пальців замінює захист доступу з використанням пароля. Більшість систем використовують відбиток одного пальця.

Основними елементами дактилоскопічної системи автентифікації є:

- сканер;
- програмне забезпечення ідентифікації, яке формує ідентифікатор користувача;
- програмне забезпечення автентифікації, яка провадить порівняння відсканованого відбитку пальця з наявними в базі даних (БД) «паспортами» користувачів.

Дактилоскопічна система автентифікації працює наступним чином. Спочатку проходить реєстрація користувача. Як правило, проводиться кілька варіантів сканування в різних положеннях пальця на сканері. Зрозуміло, що зразки будуть трохи відрізнятися, і тому потрібно сформувати певний

узагальнений зразок - «паспорт». Результати заносяться до БД автентифікації. При автентифікації проводиться порівняння відсканованого відбитку пальця з «паспортами», що зберігаються в БД.

Деякі виробники комбінують біометричні системи зі смарт-картами і картами-ключами. Наприклад, в біометричній смарт-карті Authentic реалізований наступний підхід. Зразок відбитків пальців запам'ятовується в пам'яті карти в процесі внесення в списки ідентифікаторів користувачів, встановлюючи відповідність між зразком і особистим ключем шифрування. Потім, коли користувач вводить смарт-карту в зчитувач і прикладає палець до сенсора, ключ засвідчує його особу. Комбінація біометричних пристроїв і смарт-карт є вдалим рішенням, що підвищує надійність процесів автентифікації і авторизації.

Невеликий розмір і невисока ціна датчиків відбитків пальців на базі інтегральних схем перетворює їх в ідеальний інтерфейс для систем захисту. Їх можна вбудувати в брелок для ключів, і користувачі отримають універсальний ключ, який забезпечить захищений доступ до всього, починаючи від комп'ютерів до вхідних дверей, дверей автомобілів і банкоматів.

3.2. Системи автентифікації по формі долоні. Вони використовують сканери форми долоні, зазвичай встановлюються на стінах. Слід зазначити, що переважна більшість користувачів вважають за краще системи цього типу.

Пристрої зчитування форми долоні створюють об'ємне зображення долоні, вимірюючи довжину пальців, товщину і площу поверхні долоні. Наприклад, продукти компанії Recognition Systems виконують більше 90 вимірів, які перетворюються в 9-розрядний зразок для подальших порівнянь. Цей зразок може бути збережений локально, на індивідуальному сканері долоні або в централізованій БД.

3.3. Системи автентифікації по обличчю і голосу найбільш доступні через їх дешевизну, оскільки більшість сучасних комп'ютерів мають відео- і аудіо засоби. Системи даного класу застосовуються при віддаленій ідентифікації суб'єкта доступу в телекомунікаційних мережах.

Технологія сканування рис обличчя підходить для тих додатків, де інші біометричні технології непридатні. В цьому випадку для ідентифікації та автентифікації особистості використовуються особливості очей, носа і губ.

Виробники пристроїв розпізнавання рис обличчя застосовують власні математичні алгоритми для ідентифікації користувачів.

Дослідження, що проводяться компанією International Biometric Group, говорять про те, що співробітники багатьох організацій не довіряють пристроям розпізнавання за рисами обличчя. Крім того, за даними цієї компанії, сканування рис обличчя - єдиний метод біометричної автентифікації, який не вимагає згоди на виконання перевірки (і може здійснюватися прихованою камерою), а тому має негативний для користувачів підтекст.

Слід зазначити, що технології розпізнавання рис обличчя вимагають подальшого вдосконалення. Велика частина алгоритмів розпізнавання рис обличчя чутлива до коливань в освітленні, викликаним зміною інтенсивності сонячного світла протягом дня. Зміна положення особи також може вплинути на впізнаваність. Різниця в положенні в 15% між запитуваним зображенням і зображенням, яке знаходиться в БД, безпосередньо позначається на ефективності: при розходженні в 45° розпізнавання стає неефективним.

Системи автентифікації по голосу під час запису зразка і в процесі подальшої ідентифікації спираються на такі особливості голосу, як висота, модуляція і частота звуку. Ці показники визначаються фізичними характеристиками голосового тракту і унікальні для кожної людини. Розпізнавання голосу застосовується замість набору номера в певних системах Sprint. Технологія розпізнавання голосу відрізняється від розпізнавання мови: остання інтерпретує те, що говорить абонент, а технологія розпізнавання голосу абонента підтверджує особистість мовця.

Оскільки голос можна просто записати на плівку або інші носії, деякі виробники вбудовують в свої продукти операцію запиту відгуку. Ця функція пропонує користувачеві при вході відповісти на попередньо підготовлений і регулярно змінюваний запит, наприклад такий: «Повторіть числа 0, 1, 3».

Технології розпізнавання мовця мають деякі обмеження. Різні люди можуть говорити схожими голосами, а голос будь-якої людини може змінюватися з часом в залежності від самопочуття, емоційного стану і віку. Більш того, різниця в модифікації телефонних апаратів і якість телефонних з'єднань можуть серйозно ускладнити розпізнавання.

3.4. Системи автентифікації по візерунку райдужної оболонки і сітківки ока можуть бути розділені на два класи:

- використовують малюнок райдужної оболонки ока;
- використовують малюнок кровоносних судин сітківки ока.

Сітківка ока являє собою унікальний об'єкт для автентифікації. Малюнок кровоносних судин внутрішньої частини ока відрізняється навіть у близнюків. Оскільки ймовірність повторення параметрів райдужної оболонки і сітківки ока має порядок 10^{-78}, такі системи є найбільш надійними серед всіх біометричних систем і застосовуються там, де потрібен високий рівень безпеки.

Біометричний підхід дозволяє спростити процес з'ясування «хто є хто». При використанні дактилоскопічних сканерів і пристроїв розпізнавання голосу для входу в мережі співробітники позбавляються від необхідності запам'ятовувати складні паролі. Ряд компаній інтегрують біометричні можливості в системи одноразової автентифікації SSO (Single Sign-On). Подібна консолідація дозволяє мережевим адміністраторам замінити служби одноразової автентифікації паролів біометричними технологіями.

Біометрична автентифікація користувача може бути використана при шифруванні у вигляді модулів блокування доступу до секретного ключа, який дозволяє скористатися цією інформацією тільки істинному власнику приватного ключа. Власник може потім застосовувати свій секретний ключ для шифрування інформації, що передається приватними мережами або по інтернету. Ахіллесовою п'ятою багатьох систем шифрування є проблема безпечного зберігання самого криптографічного секретного ключа. Найчастіше доступ до ключа довжиною 128 розрядів (або навіть більше) захищений лише паролем з 6 символів, тобто 48 розрядів. Відбитки пальців забезпечують

набагато більш високий рівень захисту і, на відміну від пароля, їх неможливо забути[4].

Висновок

На основі аналізу загроз від несанкціонованого доступу до приватної інформації в системах інформаційної діяльності, можна впевнено сказати, що на сьогоднішній день найрозповсюдженішими системами автентифікації являються парольні. Це обумовлено тим, що побудова такої системи не вимагає великих вкладень в її апаратну та програмну реалізацію. Вона підходить для об'єктів з порівняно незначною інформаційною цінністю. Проте варто додати, що сама по собі парольна ідентифікація користувача не є досить надійною. Часто на зміну цій моделі, приходить апаратна, яка є значно надійнішою, але в той же час потребує значно більших апаратних, програмних та фінансових ресурсів. Апаратна автентифікація також має свої недоліки, такі як залежність від захищеності каналу зв'язку, за яким відбувається доступ до системи.

Найбільш досконалою системою вважається біометрична автентифікація, тому що спирається на фізичні властивості окремого індивіда чи групи людей. Біометрична автентифікація, загалом, є покращеною версією парольної, тільки замість паролю чи PIN-коду користувач «вводить» свої фізичні параметри. Вона є досить легкою в використанні, але складною в побудові та затрат на неї.

Взагалі не існує ідеальної системи автентифікації, бувають тільки симбіоз декількох рішень, для отримання бажаного результату. Тому кожен об'єкт інформаційної діяльності повинен сам для себе вирішувати яку комбінацію з методів автентифікації слід використовувати.

Посилання

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

2. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа [Текст] / А.Ю. Щеглов. – СПб.: Наука и техника, 2004. – 384 с.

3. Запечников С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности: учебное пособие / С.В. Запечников. – М.Горячая линия-Телеком, 2007, - 320с..2007.

4. Біометрична автентифікація користувача. [Електронний ресурс]. – Режим доступу до ресурсу: https://studopedia.su/3_28399_biometrichna-autentifikatsiya-koristuvacha.html.

Рецензент: Гроза Петро Миколайович, доцент кафедри комп'ютерної інженерії, с.н.с., к.т.н.

Authors: Kanivets V., Somov S.V.

AUTHENTICATION USERS OF COMPUTER SYSTEMS

Abstract. The article provides a detailed analysis of the currently existing authentication systems: password, hardware, biometric. The classification of access systems for information is carried out. The general advantages and disadvantages of systems are considered. The basic characteristics of authentication systems are presented. The general model of work of systems of authentication of users of information-computer system is provided.

Keywords: Protection of information, authentication system, password, hardware, biometric authentication.

Авторы: Канивец В.Г., Сомов С.В.

АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ КОМПЬЮТЕРНЫХ СИСТЕМ

Аннотация. В статье проведен детальный анализ существующих в настоящее время систем аутентификации: парольная, аппаратная, биометрическая. Выполнена классификация систем доступа к информации. Рассмотрены общие преимущества и недостатки систем. Приведены основные характеристики систем аутентификации. Предоставлено общую модель работы систем аутентификации пользователей информационно-компьютерной системы.

Ключевые слова: защита информации, системы аутентификации, парольная, аппаратная, биометрическая аутентификация.