УДК 004.056.523

Б.М. Резанов, С.С. Бульба, Д.В. Шокотько

Національний технічний університет «Харківський політехнічний інститут», Харків

ФАКТОРИ АУТЕНТИФІКАЦІЇ СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ

У статті розглянуті базові фактори процесу аутентифікації у системі контролю та управління доступу. Проведено порівняння факторів за позитивними та негативними показниками, що дає змогу чіткіше представити ризики які притаманні процесу аутентифікації у сучасних системах захисту різних форм власності.

Ключеві слова: *аутентифікація, СКУД, біометрика, захист.*

Вступ

Останнім часом одним з найбільш ефективних і цивілізованих підходів до вирішення завдань комплексної безпеки об'єктів різних форм власності стає використання системи контролю та управління доступом (СКУД). Інтерес до СКУД неухильно зростає, що в недалекому майбутньому призведе до їх широкого поширення.

Використання СКУД дозволяє:

– закрити несанкціонований доступ на територію, в будівлю, окремі поверхи і приміщення;

– відслідковувати тимчасове переміщення співробітників і відвідувачів по об'єкту;

– вести табельний облік робочого часу кожного співробітника;

– здійснювати тимчасової і персональний контроль відкриття внутрішніх приміщень.

Система контролю і управління доступом є сукупністю технічних і програмних засобів, призначена для автоматизованого контролю доступу в окремі зони об'єкта. Зазвичай СКУД використовуються як одна зі складових інтегрованої системи безпеки. Найбільш поширена інтеграція - з системою відеоспостереження і системою охоронної сигналізації.

Принцип дії СКУД простий: кожен співробітник отримує пластикову картку або інший пропуск, що містить індивідуальний код. Біля входу на підприємство або в інше приміщення що підлягає контролю встановлюються зчитувачі - спеціальні пристрої, що зчитують з пропусків код і передають його в систему. Кожен код містить відповідну інформацію про права власника пропуску. На основі співставлення цієї інформації та ситуації, при якій був пред'явлений пропуск, система приймає одне з таких рішень: відкриває прохід, переводить приміщення в режим охорони або включає сигнал тривоги. СКУД запам'ятовує всі факти пред'явлення пропусків і пов'язані з ними дії. Ця інформація в подальшому використовується системою для складання різноманітних звітів.

Залежно від застосовуваної СКУД на об'єкті, окремі її пристрої можуть бути об'єднані в єдиний блок (контролер зі зчитувачем) або взагалі бути відсутнім (персональний комп'ютер).

Зчитувачі СКУД є програмно-апаратними засобами системи та призначені для зчитування коду з брелків, міток, магнітних і безконтактних карт. Приклад системи СКУД представлено на рис. 1.

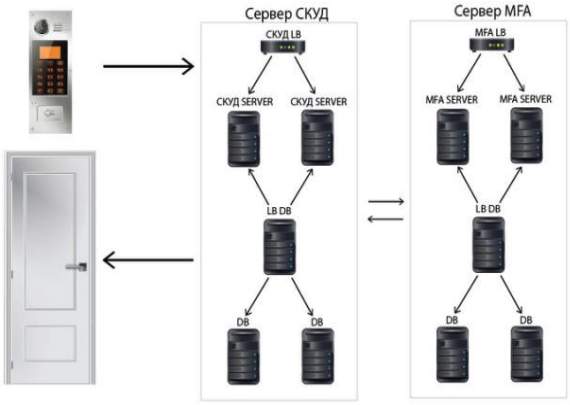

Рис. 1. Схема побудови СКУД

В процесі аутентифікації може приймати участь три фактори:

– щось, що ми знаємо – пароль;

– щось, що ми маємо – пристрій аутентифікації;

– щось, що є частиною нас – біометрика.

Пароль

Пароль – це секретна інформація, якою повинен володіти тільки авторизований суб'єкт. Паролем може бути мовне слово, текстове слово, комбінація для замка або персональний ідентифікаційний номер (PIN). Сьогодні розроблено кілька методів реалізації систем аутентифікації із застосуванням одноразових паролів.

1. Метод "запит-відповідь". На початку процедури аутентифікації користувач відправляє на сервер свій логін. У відповідь на це останній генерує випадкову послідовність символів і посилає її назад. Користувач за допомогою свого ключа зашифровує ці дані і відправляє їх серверу. Сервер у цей час за допомогою секретного ключа що належить користу-

вачу кодує вихідну послідовність. Далі проводиться порівняння обох результатів шифрування. При їх повному збігу вважається, що аутентифікація пройшла успішно.

2. Метод "тільки відповідь". Програмне або апаратне забезпечення користувача самостійно генерує вихідні дані, які будуть зашифровані та відправлені на сервер для порівняння. При цьому в процесі створення даних використовується значення попереднього запиту. Сервер теж володіє такими даними. Тобто він, використовуючи ім'я користувача, знаходить значення його попереднього запиту та генерує встановленим алгоритмом ідентичний рядок.

3. Метод "синхронізація за часом". У ньому в якості початкових даних виступають поточні показання годинника спеціального пристрою або комп'ютера, на якому працює людина. Ці дані зашифровуються за допомогою таємного ключа що у відкритому вигляді відправляються на сервер разом з ім'ям користувача. При отриманні запиту, сервер отримує поточний час від свого таймера, зашифровує його та порівнює два значення.

4. Метод "синхронізація по події". Цей метод майже ідентичний попередній технології. Тільки в якості ключа в ньому використовується не час, а кількість успішних процедур аутентифікації, проведених до поточної процедури. Це значення підраховується обома сторонами окремо один від одного.

У деяких системах реалізуються змішані методи, де в якості початкового значення використовується два або навіть більше типів інформації.

Технологія одноразових паролів вважається досить надійною. Але вони також мають недоліки діляться на дві групи. До першої належать потенційно небезпечні вузькі місця, притаманні всім методам реалізації. Найбільш серйозною з них є можливість підміни сервера аутентифікації. При цьому користувач буде відправляти свої дані прямо зловмисникові. Інша вразливість властива тільки синхронним методам реалізації одноразових паролів, оскільки існує ризик розсинхронізації інформації на сервері і в програмному або апаратному забезпеченні користувача.

Усе це робить парольний механізм слабо захищеним.

Пристрій аутентифікації

Тут важливий факт володіння суб'єктом – унікальним предметом. Це може бути особиста печатка, ключ від замку, для комп'ютера це файл даних, що містять характеристику.

Аутентифікаційні пристрої поділяють на дві категорії: пасивні та активні. В обох випадках пристрої несуть в собі базовий секрет і для того, щоб виготовити копію пристрою необхідно мати копію базового секрету. Пасивні аутентифікаційні пристрої зберігають базовий секрет, наприклад ключі від механічних замків, карточки банкомату, більшість типів електронних перепусток, тощо. Проблемою таких пристроїв є те, що дані, які в них записані, можуть бути легко відтворені за допомогою копії. Активні аутентифікаційні пристрої можуть в різних обставинах генерувати різні вихідні дані. Наприклад, пристрій може бути задіяний в протоколі аутентифікації по методу питання-відповідь або забезпечувати іншу функцію шифрування, в якій використовується базовий секрет цього пристрою. Значною перевагою активних пристроїв є те, що вони не передають свого базового секрету, а використовують його. Дізнатись секрет у такому випадку теоретично можливо, але практично досить маловірогідно.

Аутентифікація із застосуванням активних аутентифікаційних пристроїв передбачає генерацію різного типу повідомлень при кожній спробі власника аутентифікувати себе, це значить, що атакуючому не має змісту перехоплювати згенеровану послідовність і відтворювати попередній набір повідомлень.

Біометрика

Характеристикою є фізична особливість суб'єкта. До групи фізіологічних показників належать такі джерела біометричних даних:

– відбитки пальців – технологія перейнята від систем, які використовувалися правоохоронними органами для співставлення відбитків;

– геометрія руки – зчитувальні пристрої сприймають розмір пальців користувача, товщину та геометрію руки;

– характеристика ока: сітківка – в таких системах використовується ретинальна камера, розміщена позаду спеціального окуляра, користувач розміщує око напроти окуляра і камера записує картину кровоносних судин сітківки ока людини;

– характеристики ока: райдужна оболонка – в цих системах використовується спеціальна камера, яка досліджує райдужну оболонку ока і фіксує її характерний образ;

– обличчя. Камера сканує обличчя і порівнює зображення із зображенням, що зберігається в запису користувача.

На відміну від фізіологічних показників, поведінкові не завжди мають вимірювати одне і те ж саме: людині може бути запропоновано сказати, написати чи пройтись певним чином, аби зменшити ризик відтворення. До поведінкових показників належать наступні.

1 Голос – система просить користувача сказати кілька слів, на їх основі будується кілька голосових шаблонів. Такий підхід має ряд недоліків: велика вірогідність помилок в шумному середовищі, легко обманути записом голосу користувача.

2 Підпис – система порівнює представлений підпис з оригіналом. Для зниження ризику підробки

надійні системи також вимірюють динаміку руху руки, силу натиску, нахил пера.

3 Динаміка роботи на клавіатурі – системи відстежують поведінку користувача під час роботи на клавіатурі, а потім використовують унікальні особливості цієї поведінки для аутентифікації.

Основною проблемою підходів у біометричній аутентифікації є співставлення біометричних показників. Якщо біометричні показники змінились чи були пошкоджені, представлені не звичним чином, то співставлення може бути невдалим, що веде до відмови аутентифікації законному користувачеві. З'являється ризик помилкового прийняття однієї людини за іншу. Іншою проблемою є загроза атак відтворення. Атакуючий може отримати біометричні показники жертви або за допомогою зовнішнього записуючого пристрою, або шляхом копіювання показників у двійковому коді. Опис схеми взаємодії користувача та СКУД зчитувача, з позитивним результатом представлено на рис 2.

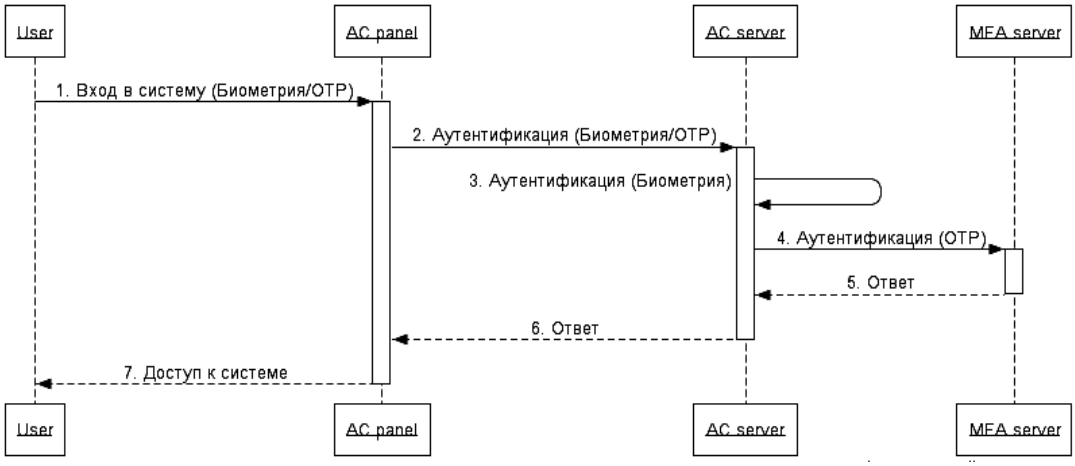

Рис. 2. Принцип взаємодії користувача та СКУД зчитувача

На рис. 2 користувач входить в систему використовуючи біометрію і токен. Access Control панель відправляє дані біометрії і токена на Access Control сервер. Виконується аутентифікація біометрії на Access Control сервері. Access Control сервер аутентифікує токен на MFA сервері.MFA сервер відправляє відповідь Access Control серверу.Access Control сервер відправляє відповідь Access Control панелі. Access Control панель дає доступ до системи.

Висновок

Усі фактори аутентифікації мають свою недоліки і кожен окремо взятий фактор не завжди може забезпечити належний рівень захисту.

Якщо виникає необхідність організувати сильний захист, стає очевидно, що потрібно комбінувати кілька факторів і використовувати їх разом. Зазвичай комбінують фактор знання з фактом наявності чи фактором, який є частиною користувача.

Список літератури

1. Rigney C., Willens S., Rubens A., Simpson W. Remote Authentication Dial In User Service (RADIUS). // RFC 2865, 2000.

2. Выбор поставщика решения двухфакторной аутентификации [Електронний ресурс] // Habrahabr.ru – Режим доступу: https://habrahabr.ru/post/238589/

3. Белкин П.Ю., Михайлский О.О., Першаков А.С. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учеб. пос. для вузов. – М.: Радио и связь. – 1999. – 168 с.

4. Маквитти Л. Федеративное управление идентификацией пользователей // Сети и системы связи, 2013. No 13.. URL : http://www.ccc.ru.

***5.** Agarwal S., Sprick B., Wortmann S. Credential Based Access Control for Semantic Web Services. // AAAI Spring Symposium, 2004.*

Надійшла до редколегії 15.03.2017

Рецензент: д-р техн. наук, проф. С.Г. Семенов, Національний технічний університет «ХПІ», Харків.

ФАКТОРЫ АУТЕНТИФИКАЦИИ СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Б.М. Резанов, С.С. Бульба, Д.В. Шокотько

В статье рассмотрены базовые факторы процесса аутентификации в системе контроля и управления доступа. Проведено сравнение факторов по положительным и отрицательными показателями, что позволяет более четко представить риски присущие процессу аутентификации в современных системах защиты различных форм собственности.

***Ключевые слова:** аутентификация, СКУД, биометрика, защита.*

FACTORS OF AUTHENTICATION ACCESS CONTROL

B.M. Rezanov, S.S. Bulba, D.V/ Shokotko

In the article the basic factors in the authentication process control system access. The comparison factor for positive and negative indicators that allows to present clearly the risks inherent authentication process in modern security systems of different ownership.

***Keywords:** authentication, access control, biometrics, protection.*