УДК 004.056

А. В. Щербатюк
В. В. Карпінець

ОСОБЛИВОСТІ ПІДВИЩЕННЯ СТІЙКОСТІ ЕЛЕКТРОННИХ КЛЮЧІВ СИСТЕМ КОНТРОЛЮ ДОСТУПУ

Вінницький національний технічний університет

Анотація

В ході дослідження було здійснено огляд існуючих можливостей підвищення рівня захищеності ключів систем контролю управління доступу (СКУД). Виявлені особливості та перспективи для підвищення рівня захищеності існуючих протоколів.

Ключові слова: системи контролю управління доступу, електронні ключі, протокол взаємодії.

Abstract

In the course of the study, an overview of the existing security enhancements to the keys of access control systems (ACS) was made. Features and perspectives for increasing the security of existing protocols have been identified.

Key words: access control systems, electronic keys, communication protocol.

Вступ

Система контролю і управління доступом (СКУД) - сукупність програмних та апаратних засобів для забезпечення контролю входу, виходу та перебування людей та транспортних засобів на підконтрольній території. Система контролю доступу дозволяє надавати доступ, контролювати час перебування на об'єкті, та зберігати інформацію про відвідування протягом довгого часу.

В роботі особливу увагу приділено унікальним ідентифікаторам відвідувачів (електронним ключам), та розглянуто особливості їх захисту.

Результати досліджень

На сьогоднішній день існує велика кількість ідентифікаторів для систем контролю управління доступу, а саме:

– Proximity - картки;
– RFID - мітки;
– магнітні картки;
– штрих-кодові мітки;
–ключі iButton;
– контактні електронні ключі.

Найкритичнішими недоліками вищеназваних ідентифікаторів є:

– малий термін придатності;
– можливість легкого копіювання ідентифікатора;
– можливість дистанційного виведення з ладу;
– відсутність захисту унікальності.

При цьому, відносно безпечними ідентифікаторами можна вважати: ключі iButton, RFID – мітки та контактні електронні ключі. Їх переваги полягають у тому, що їх протокол захищений від несанкціонованого зчитування з допомогою пароля. Тобто, зчитування мітки можливо лише з допомогою зчитувача, що зберігає в своїй пам'яті пароль. Також вони підтримують можливість зміни паролю при переводі СКУД на інший стек паролів. Перехід рекомендовано здійснювати періодично, через невеликі проміжки часу (припустимо раз на місяць). Крім просто дозволу або заборони проходу, користувач системи має, як правило, наступні

можливості:

- отримання звіту про наявність чи відсутність співробітників на роботі;
- практично миттєво дізнатися, де конкретно знаходиться співробітник;

- вести автоматичний табель обліку робочого часу;
- отримати звіт про те, хто і куди ходив практично за будь-який період часу;
- сформувати часовий графік проходу співробітників, тобто хто, куди і в який час може ходити;
- ведення бази даних співробітників (електронної картотеки), в яку користувач додає всю необхідну інформацію про співробітників, включаючи їхні фотографії.

Враховуючи усі особливості функціонування електронних ключів та їх захист, постає проблема несанкціонованого доступу до контрольованої території та приміщень з боку осіб, котрі не мають дозволу на доступ, та осіб, що мають право на доступ до цієї інформації в обсязі, що перевищує необхідний для виконання службових обов'язків.

Було визначено, що одним із найбільш перспективних методів захисту електронних ключів є використання динамічних кодів та пропрієтарних протоколів. Це дозволяє забезпечити унікальність переданих даних при кожній автентифікації користувача. Завдяки цьому, зчитавши дані при обміні (ці дії мають назву сніфінг), да передавши ідентичні дані до зчитувача СКУД, зловмисник не отримує результату у вигляді дозволу на прохід.

Висновки

Отже, в ході роботи було розглянуто особливості підвищення захисту унікальних ідентифікаторів та визначено потенційні можливості розвитку ідентифікаторів для систем контролю управління доступу. Також було виявлено основні переваги та недоліки існуючих міток різних стандартів. Описано основи практичної розробки підвищення стійкості електронних ключів систем контролю доступу на основі пропрієтарного протоколу з динамічним кодом.

Результати дослідження дозволяють розробити потенційно нові протоколи обміну даними між зчитувачем та унікальним ідентифікатором відвідувача.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Комп’ютерні технології криптографічного захисту інформації на спеціальних цифровихносіях: – К.; Тернопіль, 2007. – 272 с.
2. Боровиков А.М., Тимошенко А.А. Системы защиты информационного обмена «Клиент – Банк» // Безопасность информации.– 1995.– №1. – 53–60 с.
3. Гайкович В., Першин А. Безопасность электронных банковских систем. – М.: Единая Европа, Изд. 8, 2014. – 364 с.
4. Кісь Я.П., В.М. Теслюк Методи і засоби автентифікації в інформаційних системах // Захист даних: Збірник. –Л., 2012. – С. 231 – 267 с.
5. RFID или не RFID? Вот в чем вопрос [Електроний ресурс] / Режим доступу: http://tdplus.com.ua/razdel40/text-14.html
6. Бабенко Л.К., Ищуков С.С. Макаревич О.Б. Защита информации с использованием смарт-карт и электронных брелоков. – М.: Гелиос АРВ, 2013. – 352 с.

Щербатюк Артем Володимирович– студент групи УБ-18м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: artemmaitek@gmail.com

Карпінець Василь Васильович - к.т.н., доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: karpinets@vntu.edu.ua

Shcherbatyuk Artem - student of UB-18m group, faculty of Management and Information Security, Vinnitsa National Technical University, Vinnitsa, e-mail: artemmaitek@gmail.com

Vasyl Karpinets – Candidate of Technical Sciences, Associate Professor, Department of Management and Security of Information Systems, Vinnitsa National Technical University, Vinnytsia, e-mail: karpinets@vntu.edu.ua