УДК 004.056.53

І. В. Хутченко
Л. М. Куперштейн

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ РОЗРОБЛЕНОЇ СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ З ВИКОРИСТАННЯМ ДВОХФАКТОРНОЇ АВТЕНТИФІКАЦІЇ НА ОСНОВІ ПЛАТФОРМИ ARDUINO

Вінницький національний технічний університет;

Анотація

Проведено дослідження вразливостей розробленої системи контролю та управління доступом з використанням двохфакторної автентифікації на основі платформи Arduino. Встановлено, що система забезпечує надійний захист від несанкціонованого доступу до приміщення.

Ключові слова: система контролю та управління доступом, платформа Arduino, вразливості RFID, RFID-зчитувач RC522, сканер відбитка пальця FPM10, ультразвуковий датчик відстані HC-SR04.

Abstract

The vulnerability studies of the developed control and access control system using two-factor authentication based on the Arduino platform were conducted. It is established that the system provides reliable protection against unauthorized access to the premises.

Keywords: access control system, Arduino platform, RFID vulnerability, RC522 RFID reader, FPM10 fingerprint scanner, ultrasonic distance sensor HC-SR04.

Вступ

За шість років обсяг світового ринку систем контролю та управління доступом (СКУД), які використовують електронні карти, виросте на 3,4 мільярди доларів - такий прогноз експертів компанії Global Industry Analysts. Джерелами зростання стануть державні і корпоративні замовники. Інтерес великих державних структур до систем контролю доступу відзначений вже давно: саме вони складають один з найбільших ринків для СКУД на основі карток. Такого роду системи використовуються в адміністративних закладах, на об'єктах енергетичного комплексу, в оборонних лабораторіях і виправних установах. Аналітики пов'язують це з тим, що зберігання кодів доступу на електронних картах при всій їх уразливості все ж являється більш надійним, ніж практика введення паролів з клавіатур. Зацікавленість в цілості бізнес-інформації сьогодні повсюдно зростає; в звіті про дослідження GIA окремо наголошує на тому, що в сучасних умовах наслідки витоку даних можуть принести величезні фінансові та моральні збитки. Разом з тим, як вважають експерти, ринок карткових СКУД відчуває і ряд складнощів: частина кінцевих користувачів все ще “не доросла” до серйозного підходу захисту своїх об'єктів [1].

Існуючі системи контролю та управління доступом (СКУД) на ринку України не вирішують проблему комплексної автентифікації, тому для вирішенням цієї проблеми, було розроблено систему, яка об’єднує застосування радіочастотної та біометричної автентифікації, а також поєднує функції охоронної сигналізації.

Отож, для дослідження вразливостей, розробленої системи контролю та управління доступом з використанням двохфакторної автентифікації на основі платформи Arduino, необхідно визначити основні вразливості складових системи та запропонувати шляхи їх вирішення.

Результати дослідження вразливостей RFID-зчитувача RC522

Радіочастотну ідентифікацію виконує RFID-зчитувач RC522. Цей зчитувач було обрано через те, що він підтримує різні типи RFID-міток (картки та брелоки), працює на, необхідній нам, відстані (до 6 см) та є найпопулярнішим серед бюджетних зчитувачів на ринку України. Але як відомо, технологія RFID є не зовсім надійною і має ряд вразливостей: клонування, подавлення, RFID-Zapper та атаки через RFID-мітки.

Давно уже не секрет, що існують пристрої які можуть клонувати RFID-мітки. Для цього достатньо наблизити спеціальний пристрій (Proxmark, BLEKey) на відстань не менше ніж 10 см

до мітки. Принцип атаки базується на тому, що RFID-зчитувачі постійно передають сигнал,а у момент виявлення RFID-карти в безпосередній близькості до зчитувача відбувається одноразова передача кадру з кодом карти від зчитувача до контролера за протоколом Weigand, ненадійність якого давно підтверджена [2]. Нині відомі типи RFID-міток неможливо захистити від клонування, адже вразливість в самому протоколі передачі даних. До організаційних заходів захисту можна віднести постійний контроль за станом цілісності корпусу зчитувача або ж унеможливити доступ до самого зчитувача.

RFID першого покоління схильні до подавлення. Деякі старі мітки використовують діапазон 902-938 МГц, розділений на канали. Зчитувач може перемикатися з одного каналу на інший, а RFID-мітка, через свою пасивність, не може змінити діапазон. Стверджується, що даний діапазон можна заглушити з відстані в 1 метр. Атака RFID-Zapper ґрунтується на знищення мітки. Дія сильного електромагнітного поля вбиває пасивні мітки. Для захисту від цих двох вразливостей слід використовувати активні RFID-мітки, які використовують для передачі енергію власного елемента живлення.

Атаки через RFID-мітки. Насправді через редагування мітки можна отримати доступ до комп'ютера і тим самим здійснювати різного роду атаки. Уразливе місця RFID-мітки – переповнення буферу (buffer overflow). Припустимо, в RFID-системі використовуються тільки мітки з об'ємом пам'яті 128 байт. Програміст, який писав додаток, обробляє вміст тегів, полінувався зробити перевірку на довжину цього самого вмісту. В результаті є можливість для переповнення буфера, адже хитрий хакер може підсунути системі мітку з великою кількістю пам'яті, ніж 128 байт, заховавши туди і shell-код. Захистись від подібного роду атак можна лише одним шляхом – обмежити максимальну пам’ять зчитування.

Результати дослідження вразливостей сканера відбитка пальця FPM10

Також в розробленій СКУД використовується оптичний сканер відбитка пальця FPM10. Вибір даного сканера обумовлений порівняною дешевизною, адже подібні сканери коштують чимало. Оптичний сканер відбитків пальців зазвичай використовують в системах безпеки. Цей сканер включає в себе DSP-чіп, який обробляє зображення, робить необхідні розрахунки для виявлення відповідності між записаними і поточними даними. Сканер дозволяє вмістити до 162 різних відбитків пальців. Найбільший недолік оптичних сканерів – слабка захищеність від муляжів та інших способів обману.

Отож, слід перевірити оптичний сканер відбитка пальця FPM10 на здатність ідентифікації муляжу. Для цього було роздруковане зображення відбитка, яке вилучене із пам’яті сканера за допомогою програми SFG Demo. В результаті двадцяти спроб (відбитки різних зареєстрованих в пам’яті пальців, а також друк на різних типах принтерів: струйний, лазерний) сканер FPM10 жодного разу не ідентифікував муляж.

Отже, як виявилось, оптичний сканер відбитка пальця FPM10 не вразливий ідентифікації муляжів. До того ж в розробленій СКУД реалізована звукова та світлова сигналізація, яка вмикається після 3 невдалих спроб автентифікації.

Результати дослідження вразливостей ультразвукового датчика відстані HC-SR04

В режимі «Охорона» активується ультразвуковий датчик відстані HC-SR04, що виконує функцію датчика руху. При потраплянні людини чи предмету в поле зору датчика відстань стає відмінною від еталонної (відстань до протилежної стіни), тому надсилається сигнал тривоги і камера робить 10 фотознімків з інтервалом в 1 секунду. Використання даного типу датчика дало змогу зменшити загальну вартість засобу. В порівнянні із інфрачервоним датчиком руху, ультразвуковий датчик відстані досить не практичний через свою лінійну діаграму спрямованості, про що сказано в технічному описі [3]. Проте для встановлення повної горизонтальної діаграми спрямованості, було проведено 25 тестів на відстані від 0 до 4 метрів та в кутових відхиленнях по 45˚в обидві сторони.

На рисунку 1 зображена експериментально встановлена горизонтальна діаграма направленості ультразвукового датчика відстані HC-SR04.

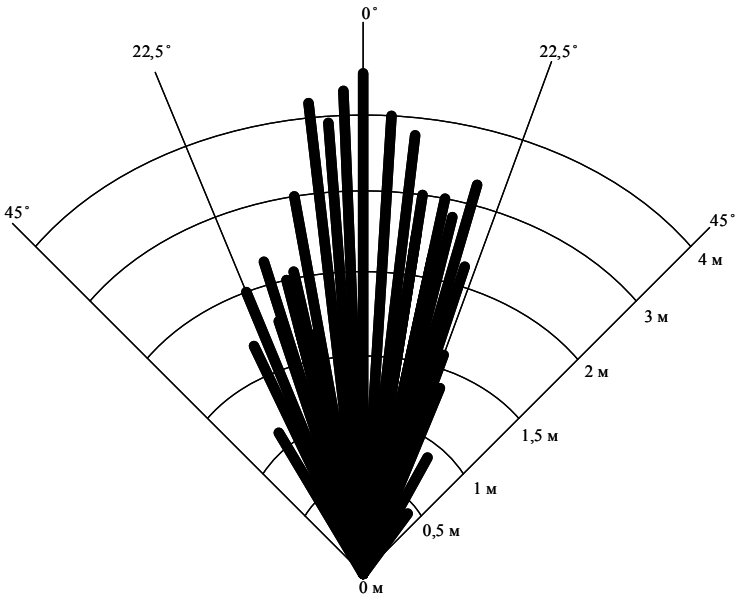

Рисунок 1 – Горизонтальна діаграма направленості ультразвукового датчика відстані HC-SR04

Проаналізувавши діаграму спрямованості можна зробити висновок, що датчик відстані HC-SR04 цілком підходить для виконання завдання детектування руху на невеликій площі.

Висновки

Отже, результати дослідження RFID-зчитувача RC522, сканера відбитка пальця FPM10 і ультразвукового датчика відстані HC-SR04 вказують на те, що розроблена система контролю та управління доступом з використанням двохфакторної автентифікації на основі платформи Arduino, гарантує надійний захист від несанкціонованого доступу до приміщення. В подальшому планується модернізація системи, шляхом наповнення функціоналу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Борсуков А. В. Інтегральний захист інформації // Системи безпеки – 2014. - №55. – с. 34-38.
2. Устройство под названием BLEKey взламывает RFID-ключи [Електронний ресурс] - Режим доступу: URL: https://threatpost.ru/blekey-device-breaks-rfid-physical-access-controls/10731/ - Назва з екрану.
3. Datasheet ultrasonic Ranging Module HC - SR04 [Електронний ресурс] – Режим доступу : URL: http://www.micropik.com/PDF/HCSR04.pdf - Назва з екрану.

Хутченко Іван Вікторович — студент, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, Україна, e-mail: chytor96@mail.ua

Науковий керівник:
Куперштейн Леонід Михайлович — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, Україна

Khutchenko Ivan — Student of Information Technologies and Computer Engineering Department, Vinnytsia National Technical University, Vinnytsia, Ukraine, e-mail: chytor96@mail.ua

Supervisor:
Kupershtein Leonid — phd. Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Vinnytsia, Ukraine