



Сергій ТУРАНСЬКИЙ,
вчитель інформатики Кам'янець-Подільського ліцею №7,
вчитель-методист

Розробка апаратного менеджера паролів

Анотація

У статті описано досвід розробки та програмної реалізації апаратного пристрою для автоматизації ідентифікації користувачів в інформаційних системах. Розглянуто переваги використання мікроконтролерів із підтримкою HID-режиму для підвищення рівня кібербезпеки. Стаття підготовлена на основі науково-дослідницького проекту Лісевича Андрія, учня 8-го класу Кам'янець-Подільського ліцею №7. Дослідницький проект "Розробка програмного забезпечення для апаратного менеджера паролів" був представлений на конкурсі-захисті дослідницьких проєктів здобувачів освіти 6-8 класів «Перший крок у науку» в 2024/2025 навчальному році в м. Хмельницькому. Проєкт посів I місце. Матеріал може бути використаний учителями інформатики для факультативних занять та гурткової роботи в сфері STEM-освіти.

Ключові слова: DigiSpark, HID-пристрій, ідентифікація користувача, інформаційна безпека, Arduino IDE.

Інформаційна безпека стає критично важливою складовою цифрового життя. Керування доступом до даних здійснюється через ідентифікацію користувача. Система ідентифікації є одним із ключових елементів системи захисту даних від несанкціонованого доступу. Її завданням є визначення і верифікація набору повноважень суб'єкта при доступі до інформаційної системи.

Існує три найпоширеніші способи ідентифікації користувачів:

1. Парольна ідентифікація. Це найпростіший у реалізації та використанні метод ідентифікації користувача. Логін і пароль повинні бути унікальними для кожного зареєстрованого користувача. Щоразу при вході в систему користувач вказує зазначені дані.

Однак цей метод має серйозний недолік. Ступінь надійності залежить від самих користувачів, а точніше від паролів, які вони створюють. Справа в тому, що більшість людей використовують ненадійні паролі, які можна легко підібрати. До них відносяться занадто короткі паролі, загальновідомі комбінації поширених символів і т.д. Це зумовлено тим, що користувачі лінуються запам'ятовувати та вводити складні, надійні паролі. Фахівці в галузі інформаційної безпеки радять використовувати довгі паролі, що складаються з випадкового сполучення букв, цифр і різних символів.

Незважаючи на свої недоліки, цей метод ідентифікації реалізований у більшості програмних продуктів.

2. Апаратна (або електронна) ідентифікація. Цей принцип ідентифікації базується на використанні різних електронних ключів. Найпоширенішими є електронні магнітні

картки і так звані токени, які підключаються безпосередньо до одного з портів комп'ютера.

Апаратна ідентифікація має високий рівень надійності. Електронні ключі можуть зберігати досить складні паролі. Крім того, у них реалізовано чимало різних захисних механізмів. Такі електронні ключі належать конкретній особі, що дає можливість відстежувати поведінку конкретного користувача.

Основним недоліком цієї технології ідентифікації є її вартість.

3. Біометрична ідентифікація. Біометрія – це ідентифікація особи за унікальним, властивим тільки їй біологічним ознакам. Біометрія дозволяє встановити особистість людини. Найпоширенішим методом біометричної ідентифікації є визначення особи за відбитком пальця. Біометрична ідентифікація є найнадійнішою, але впровадження таких систем коштує дуже дорого.

В інформаційних системах, які потребують високого ступеня захисту запроваджують комплексну (або багатофакторну) систему ідентифікації. У таких системах для ідентифікації особи використовується відразу кілька методів ідентифікації, тим самим підвищуючи рівень безпеки. При цьому методи ідентифікації можуть комбінуватись у будь-якому порядку.

Зазначені вище методи ідентифікації забезпечують високий рівень безпеки. Однак їх реалізація потребує значних фінансових витрат, тому більшість додатків використовують класичні методи ідентифікації за допомогою логінів та паролів.

Якщо дотримуватись певних правил, то системи ідентифікації за допомогою паролів також можуть забезпечити належний рівень захисту. Ось кілька порад щодо створення паролів:

- використовувати паролі довжиною не менше 12-16 символів;
- доцільно поєднувати великі і малі літери, цифри і спеціальні символи, це значно ускладнює підбір пароля;
- уникати очевидних комбінацій, таких як "123456", "password" або дата народження – це перше, що перевіряють хакери;
- створювати окремі паролі для кожного облікового запису, використання одного пароля для всіх сервісів – це поширена помилка користувачів;
- використовувати «Менеджери паролів» для збереження унікальних та складних паролів;
- використовувати програмні генератори, вони дозволяють створювати складні та надійні паролі;
- часто змінювати паролі, це ще один важливий аспект кібербезпеки;

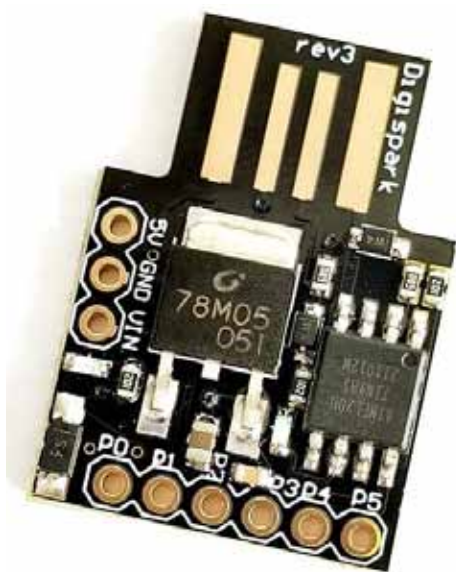
- для особистих акаунтів – рекомендується змінювати пароль раз на пів року;

- для корпоративних і фінансових сервісів – бажано оновлювати паролі кожні 3 місяці;

- у разі підозри на компрометацію – зміна пароля має відбутися негайно.

Щоб спонукати користувачів використовувати складні та надійні паролі пропонуємо реалізацію апаратного менеджера паролів, який допоможе генерувати, зберігати та автоматично вводити логін та пароль при вході в інформаційну систему.

Проект реалізовано на базі компактного мікроконтролера із вбудованим USB роз'ємом - DigiSpark.



Плата розробки DigiSpark

DigiSpark – це мінімалістичний мікроконтролер, побудований на базі мікросхеми ATtiny85. Процесор ATtiny85 має вбудований контролер USB-порту, тому плата DigiSpark може працювати напряму з USB портом без додаткових адаптерів. Ця особливість робить плату DigiSpark унікальною і дозволяє використовувати її як HID пристрій, тобто пристрій введення, такий як клавіатура або миша.

Використання DigiSpark у режимі HID пристрою надає широкі можливості застосування цієї плати:

- емуляція клавіатури. DigiSpark може імітувати натискання клавіш, тобто надсилати код потрібної клавіші до комп'ютера. Будь-яка програма буде сприймати ці дані як введення з клавіатури.

- емуляція миші. DigiSpark може керувати переміщенням курсору миші на екрані монітора та імітувати натискання кнопок миші.

- автоматизація виконання завдань. DigiSpark можна використовувати для швидкого виконання команд або макросів.

- тестування інформаційної безпеки. DigiSpark можна запрограмувати на імітацію дій зловмисника, який намагається зламати пароль. Це дозволить перевірити стійкість системи до злому та виявити слабкі місця у системі безпеки.

Обчислювальних потужностей DigiSpark достатньо, щоб реалізувати апаратний менеджер паролів.

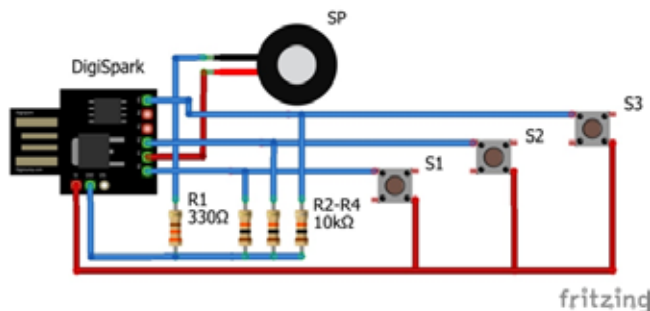
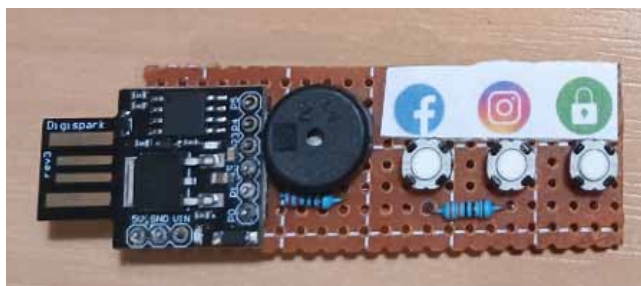


Схема пристрою

Запропонований пристрій зможе реалізовувати декілька функцій:

- генерація та збереження складних і надійних паролів;
- автоматичне введення паролів та забезпечення автоматичного входу в інформаційну систему;
- захист від шпигунських програм-кейлогерів, оскільки введення пароля відбувається без використання фізичної клавіатури.



Зовнішній вигляд апаратного менеджера паролів

Для програмування плати DigiSpark використовується мова програмування C++. Плата DigiSpark повністю сумісна з платформою Arduino та середовищем програмування Arduino IDE.

Оскільки всі сучасні операційні системи мають вбудовану підтримку HID пристроїв, то відпадає потреба у розробці власного драйвера для взаємодії операційної системи з даним пристроєм. Щоб комп'ютер ідентифікував пристрій як звичайну клавіатуру, використовується бібліотека DigiKeyboard.h.

Перші дві кнопки пристрою забезпечують автоматичний вхід до Facebook та Instagram. Третя кнопка використовується для генерування та введення пароля користувача.

Проаналізувавши головну сторінку Facebook та процедуру входу, створено алгоритм для автоматичної ідентифікації користувача:

1. За допомогою командного рядка потрібно запустити браузер Google Chrome та перейти на сторінку Facebook.

2. Коли завантажується головна сторінка Facebook, курсор автоматично встановлюється в поле для введення логіна користувача. Програма імітує роботу клавіатури та вводить необхідний логін й імітує натискання кнопки «Tab» для переходу до поля введення пароля.

3. Програма імітує введення пароля та імітує натискання кнопки «Enter». У такий спосіб відбувається автоматичний вхід до Facebook.

Програмний код, що реалізує цей алгоритм, наведено на рисунку:

```
if (btns[0]) {
    DigiKeyboard.sendKeyStroke(KEY_R, MOD_GUI_LEFT); // Windows + R
    DigiKeyboard.delay(100);
    doSimpleAction(1);
}
...
Action simpleActions[][10] = {
{
    // Facebook
    { 'p', 0, "explorer \"https://www.facebook.com/\"", 20 },
    { 'k', KEY_ENTER, NULL, 3000 },
    { 'p', 0, "YOUR_FACEBOOK_LOGIN", 10 },
    { 'k', 43, NULL, 10 },
    { 'p', 0, "YOUR_FACEBOOK_PASSWORD", 10 },
    { 'k', KEY_ENTER, NULL, 300 } // done
}
}
```

Схожий алгоритм розроблено для автоматичного входу до Instagram.
Третя кнопка може використовуватись для автоматич-

ного введення пароля при вході в будь-яку інформаційну систему. Одне натискання на кнопку імітує роботу клавіатури та вводить збережений пароль.

```
char pass[passLen]; // змінна пароля
char chars[][27] = {"qwertyuiopasdfghjklzxcvbnm",
                   "QWERTYUIOPASDFGHJKLZXCVBNM",
                   "0123456789",
                   "-_+/( )[]{}.,\""; // усі доступні символи
char charsSize[] = {27, 27, 11, 13}; // розміри усіх підрядків у chars

void passGen() { // функція для генерації пароля
    for (int i = 0; i < passLen; i++) {
        randBucket = random(5);
        pass[i] = chars[randBucket][random(charsSize[randBucket])];
    }
    eeprom_write_block(&pass, 0, passLen);
}
```

Довжина згенерованого пароля становить 16 символів, при цьому використовуються великі та малі букви латинського алфавіту, цифри та спеціальні символи.

Запропонований апаратний менеджер паролів дозволяє автоматично входити в Facebook та Instagram. Вбудований генератор паролів дає можливість використовувати надійний пароль для входу в інформаційну систему, не потребує запам'ятовування такого пароля користувачем та дозволяє легко змінювати його. Згенерований пароль зберігається в енергонезалежній пам'яті плати DigiSpark.

Розроблений апаратний менеджер паролів працює ізольовано від інформаційної системи, що робить його недоступним для враження вірусами, троянами та кейлогерами.

Повний текст програми можна завантажити за покликанням: <https://lnk.ua/QqBjBJl1>.

Використані джерела

1. Бібліотека DigiKeyboard. URL: <https://github.com/cipherswami/DigiKeyboard>
2. Гапак О. М. Захист інформації в комп'ютерних системах. Ужгород: Видавництво УжНУ, 2021. 184 с.
3. Документація для плати Digispark. URL: <https://lnk.ua/kL40MSf7z>
4. Лехан С. А., ARDUINO для школярів. Програмування. Методичний посібник. 2018. 72 с.