Wojskowa Akademia Techniczna

Wydział Elektroniki

Rodzaj pracy: Magisterska
Dyplomant: **mgr inż. Piotr Adamowski**
Promotor: **dr hab. inż. Adam Rosiński**

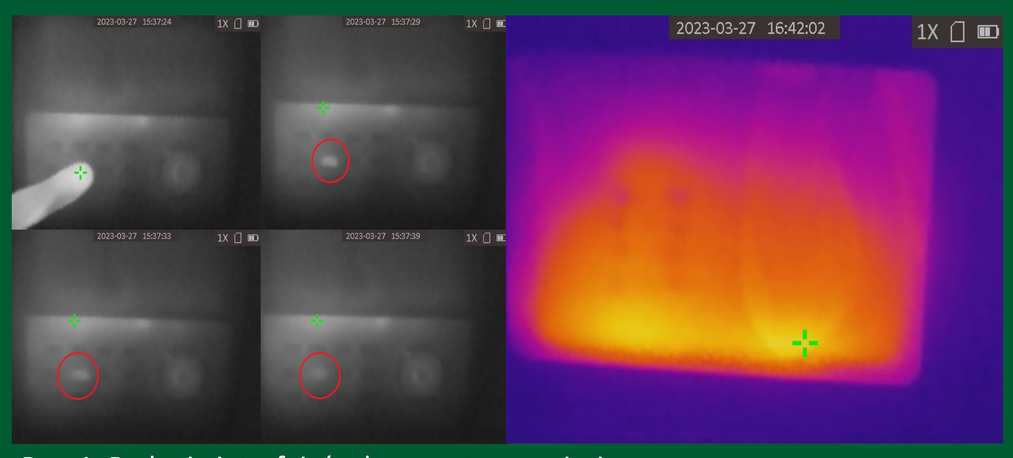
ANALIZA MOŻLIWOŚCI MODERNIZACJI INTERFEJSÓW CZŁOWIEK-SYSTEM W SYSTEMACH SYGNALIZACJI WŁAMANIA I NAPADU

Wprowadzenie

Interfejsy w SSWiN stanowią swego rodzaju translator pomiędzy akcjami podejmowanymi przez użytkownika, a wynikiem ich działania. Zapewniają one szereg różnych funkcjonalności. Pozwalają one na wizualizację stanu działania całego systemu, modyfikowanie jego parametrów, konfigurowanie wejść, a także zmianę kodu dostępu. Jedną z najistotniejszych funkcji jest proces autoryzacji użytkownika bądź operatora. Autoryzacja może przebiegać na podstawie trzech kryteriów. Coś co wiem (czyli np. kod), coś co mam (czyli np. klucz), bądź coś, czym jestem (biometria). W większości takich interfejsów proces autoryzacji następuje poprzez wpisanie odpowiedniego, najczęściej czterocyfrowego kodu dostępu. Celem tego projektu było usprawnienie tego pierwszego, jakże ważnego pod względem zabezpieczenia systemu kroku, którym jest autoryzacja.

Badania

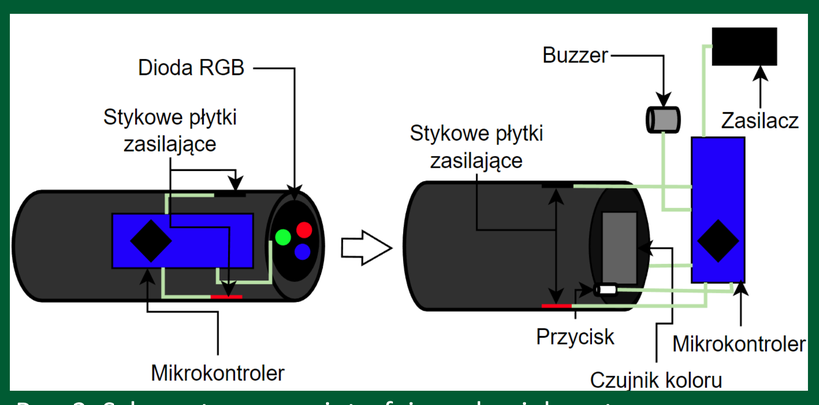
W pierwszej kolejności przeprowadzone zostały badania interfejsów. Pierwsze z nich miało na celu sprawdzenie, czy po użyciu manipulatora pozostaje widoczny ślad cieplny. Na rysunku 1 po lewej stronie pokazano wynik przyciśnięcia przycisku przez około 10 sekund oraz pozostawioną sygnaturę cieplną. Rysunek 1 z prawej strony przedstawia efekt wpisania kodu za pomocą zimnej dłoni. W obu przypadkach istnieje ryzyko, że osoba nieuprawniona mogłaby uzyskać informacje o wprowadzonych cyfrach.



Rys. 1. Badanie interfejsów kamerą termowizyjną

Następnie przeprowadzono badanie manipulatora graficznego. Miało ono na celu sprawdzenie, czy po wprowadzeniu kodu pozostaje widoczny ślad. Niestety, odciski palców są nadal widoczne po wprowadzeniu kodu. Producentom udało się to częściowo zniwelować, umieszczając klawiaturę numeryczną w różnych miejscach manipulatora, ale nadal kształt pozostawionych odcisków jest widoczny na ekranie.

Aby zapobiec nieautoryzowanemu uzyskaniu dostępu do kodu oraz zapewnić bardzo dużą liczbę kombinacji kodu, zaproponowano nowy interfejs oparty na nadajniku i odbiorniku. Nadajnik zawiera diodę RGB i mikrokontroler do generowania kodu dostępu w postaci sekwencji kolorów. Odbiornik zawiera czujnik koloru i mikrokontroler do autoryzacji na podstawie danych z czujnika. Nadajnik jest zasilany przez odbiornik poprzez dedykowane płytki stykowe, aktywowane przyciskiem, zapewniając responsywność interfejsu. Schemat ideowy interfejsu przedstawia rysunek 2.



Rys. 2. Schemat nowego interfejsu człowiek-system

Fizyczną realizację interfejsu wykonano przy użyciu obudów zaprojektowanych w programie FreeCAD i wydrukowanych na drukarce 3D. Interfejs widoczny jest na rysunku 3. W obudowie nadajnika znajdują się mikrokontroler Arduino Pro Mini i dioda RGB z dyfuzorem. Obudowa odbiornika ma kształt D, który pozwala na umieszczenie nadajnika tylko w jednej płaszczyźnie, zapewniając poprawną polaryzację napięcia zasilania nadajnika. Istotny jest również otwór w obudowie, który umożliwia dostęp światła generowanego przez nadajnik.

Ważnym aspektem tego interfejsu jest również opracowany model rozpoznawania kolorów. Model ten obejmuje 6 poziomów mocy świecenia dla każdej składowej RGB, wykluczając zerową moc (czarny) i maksymalną moc (biały). Kolor biały jest zarezerwowany jako sygnalizacja rozpoczęcia podawania sekwencji kolorów. To rozwiązanie zapewnia 214 rozróżnialnych kolorów, które służą jako słownik do generowanego hasła. Na przykład, dla hasła o długości 5 kolorów, istnieje około 4,5·10^11 możliwych kombinacji. Co ważne, osoby postronne nie mają możliwości podejrzenia wprowadzanego hasła dostępu.

Rys.3 . Fizyczna realizacja nowego interfejsu człowiek-system bazującego na czujniku koloru

Wnioski

Przeprowadzona analiza oraz badania wskazują na istotne braki w zabezpieczeniach systemów SSWiN wynikające z zastosowania przestarzałych interfejsów człowiek-system oraz metod autoryzacji.

Zaproponowany interfejs zapewniający nową metodę autoryzacji w poprawny sposób jest w stanie zapewnić większe bezpieczeństwo tego procesu, a także może umożliwić zastosowanie uwierzytelniania dwuskładnikowego podczas podejmowania działań przez użytkownika.