Controller de tastatură cu criptare și decriptare la destinație

Rotaru Adrian

Rezumat

În contextul dezvoltării societății (informaționale) cresc și riscurile cu privire la accesarea neautorizată a unor sisteme restricționate. Prin urmare, realizarea de dispozitive mai sigure devine o necesitate. [1]

Se consideră o tastatură ca fiind un periferic folosit pentru a introduce text, caractere sau alte comenzi într-un sistem de calcul sau alte dispozitive similare. Aceasta poate fi externă sau incorporată în sistem. Tastatura poate fi considerată principala modalitate de comunicare cu un sistem de calcul. Informațiile transmise de utilizator prin intermediul acesteia au un caracter privat și pot reprezenta o țintă pentru entități răuvoitoare.

În lucrarea de față se prezintă o soluție care permite evitarea modificărilor neautorizate sau chiar înlocuirea tastaturii unui astfel de sistem în scopuri malicioase. Soluția este compusă dintr-o suită hardware plus software ce are ca scop sporirea securității la nivelul tastaturii.

Pentru dezvoltarea soluției s-a ținut cont și de sugestiile oferite de patentul US8566608. Lucrarea își propune, pe lângă realizarea circuitului tastaturii, baleerea acestuia, prelucrarea semnalului și inserarea unui strat de criptare între nivelul de transmitere a codului tastei și recepționarea acestuia de către aplicație.

Partea hardware a proiectului este compusă dintr-o tastatură de tip membrană matricială formată din 16 taste, circuit pentru interfațarea cu microcontroller, plăcuță de dezvoltare XMC1100 BootKit de la Infineon. Comunicarea cu sistemul de operare se va face prin protocolul UART. Placa de dezvoltare se va ocupa cu baleerea tasturii, interpretarea tastelor, criptarea și împachetarea acestora și transmiterea prin canalul de comunicație. Programarea microcontrollerului se va face în C, folosind mediul de programare DAVE, ce aparține companiei Infineon. Partea software este compusă dintr-o aplicație ce este scrisă în Python și se va ocupa cu recepționarea informațiilor primite de la microcontroller, decriptarea și afișarea acestora. Pentru comunicare se foloseste biblioteca pySerial. Pentru criptare se foloseste algoritmul AES de la NIST cu o cheie de criptare de 128 biți. Autentificarea device-ului se realizază prin transmiterea unei chei unice ce a fost generată în prealabil. Această cheie de autentificare s-a obținut aplicând algoritmul SHA3 de la NIST pe informațiile de configurare a plăcii de dezvoltare. Acest lucru încearcă sa împiedice modificări hardware ce pot fi aduse dispozitivului sau chiar înlocuirea acestuia. Cheia de autentificare a fost precalculată și scrisă pe dispozitiv.

Dispozitivul este destinat în principal utilizatorilor de rând, lucru ce a impus o funcționare simplistă. Se detaliază modul de funcționare a proiectului. Utilizatorul conectează circuitul tastaturii la microcontroller, îl alimentează la portul USB, pornește aplicația DAVE și rulează codul sursă. Se pornește aplicația Python și se așteaptă inițierea comunicării, deschiderea portului, primirea și validarea cheii de autentificare. În cazul în care cheia nu corespunde, se afișează un mesaj corespunzător iar sesiunea de lucru este terminată. Dacă validarea cheii este

confirmată, utilizatorul este anunțat că poate apăsa pe taste. Acesta introduce 16 taste, ce vor fi afișate în consolă. După întroducerea celor 16 taste, se criptează și se trimite pe serială. Aplicația recepționează acest pachet, comunică ulitizatorului acest lucru și apoi îl decriptează. Se compară dacă setul decriptat corespunde cu datele inițiale primite, iar utilizatorul este înștiințat dacă decriptarea s-a încheiat sau nu cu succes. Procesul se reia de la pasul în care utilizatorul introduce un nou set de 16 taste.

Obiectivele lucrării sunt înțelegerea și realizarea procesului de baleere a tasturii, înțelegerea algoritmilor AES și SHA3 și implimentarea lor și realizarea unui proiect funcțional ce va îmbunătăți securitatea tastaturii.

Se așteaptă ca la finalul lucrării să se obțină un prototip de produs ce va îmbunătăți securitatea la nivelul tastaturii. Se dorește o bună funcționare a acestuia.