**SPRAWOZDANIE**

*Ćwiczenie 13*

*Czytnik kart chipowych*

**WYKONANIE:**

* Szymon Hutnik 252736
* Damian Mucha 252708

**TERMIN ZAJĘĆ:** środa TP, 11.15

**DATA:** 27.10.2021

**PROWADZĄCY:** dr inż. Tomasz Walkowiak

1. Treść zadania

Celem ćwiczenia było zapoznanie się z budową oraz działaniem czytników kart chipowych (telefoniczne karty SIM).

Zadaniem do zrealizowania było napisanie programu w C# pozwalającego komunikować się z kartą chipową za pomocą standardu PC/SU z wykorzystaniem komend APDU i wyświetlanie jej odpowiedzi w prostym GUI.

1. Opis urządzenia

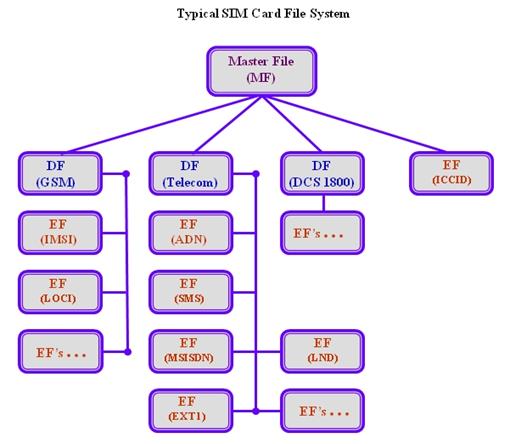
Karta chipowa – nośnik danych charakteryzujący się wielokrotnością usług oraz lepszą ochroną danych w porównaniu do jego odpowiednika z paskiem magnetycznym. Najczęściej jest zbudowana z tworzywa sztucznego, w którym jest osadzony układ scalony – chip, którego styki są pokryte złotem, standard opisuje 8 rodzajów, ale producent nie musi umieszczać wszystkich. Mikroprocesor zapewnia kontrolę odczytu i zapisu danych, może kontrolować ilość nieudanych prób odblokowania, aby móc zablokować kartę po przekroczeniu limitu. Najczęściej stosowanymi mikroprocesorami są 8-bitowe moduły z pamięcią EEPROM, którą możemy podzielić na 3 obszary:

* swobodnego odczytu – zazwyczaj przechowuje powszechne informacje o karcie i/lub użytkowniku
* poufny – dostęp do niego wymaga wprowadzenia poprawnego kodu PIN
* roboczy – przechowuje dane, które są poddawane ciągłej modyfikacji

Karty chipowe można podzielić ze względu na interfejsy komunikacyjne, czyli sposób przesyłania danych:

* stykowe – zgodne ze standardem ISO-7816. W tego rodzaju kartach wyróżniamy 2 główne protokoły komunikacyjne:
  + T=0 – jednokierunkowa transmisja bajtów
  + T=1 – jednokierunkowa transmisja bloków
* bezstykowe – zgodne ze standardem ISO14443. Komunikacja z czytnikiem polega na wykorzystaniu fal elektromagnetycznych na różnych częstotliwościach

System plików kart SIM przedstawia się następująco:



Rysunek 1: System plików karty SIM

Źródło: https://resources.infosecinstitute.com/topic/sim-card-forensics-introduction/

Działanie czytnika kart jest proste – po umieszczeniu karty w czytniku zostaje ona zasilona przez odpowiedni styk i wysyła wiadomość ATR (Answer to Reset), która informuje czytnik o rodzaju karty, sposobie kodowania bitów i wspieranych protokołach komunikacji. Po nawiązaniu połączenia można komunikować się z kartą za pomocą prokokołu APDU.

1. Fragmenty kodu
   1. Połączenie z silnikiem





W naszym programie używamy biblioteki PCSC. Połączenie polega na znalezieniu czytnika kart wśród urządzeń podpiętych do komputera, przy użyciu metody Connect() nawiązujemy połączenie, w przypadku błędu dostaniemy odpowiedni komunikat. Następnie sprawdzamy, który protokół (T=0 lub T=1) jest używany.

* 1. Odczyt wiadomości SMS



Odczyt wiadomości SMS z karty chipowej polega na wysyłaniu kolejnych zapytań i odczytywaniu otrzymywanych odpowiedzi. Zapytania to:

* SELECT TELECOM
* SELECT SMS
* READ RECORD
* GET RESPONSE

Format każdej z wiadomości jest zgodny z formatem komend APDU:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| KOMENDA APDU | | | | | | |
| CLA | INS | P1 | P2 |  | DATA FIELD |  |

* CLA to bajt określający klasę komendy, w naszym przypadku zawsze będzie on miał wartość 0xA0, która określa klasę instrukcji kart GSM
* INS to bajt określający instrukcję, którą ma wykonać karta. Użyte przez nas wartości to:

0xA4 – SELECT FILE

0xC0 – GET RESPONSE

0xB2 – READ RECORD

* długość komendy
* DATA FIELD – zapytanie APDU
* długość oczekiwanej odpowiedzi

W naszym programie najpierw dostajemy się do folderu Telecom. Następnie przechodzimy do podfolderu SMS, z którego odczytujemy i wyświetlamy dane.

1. Przedstawienie aplikacji

Graphical user interface, text, application

Description automatically generated

1. Liteatura

* ISO/IEC 7816-4 Command Set
* Smart Card API Reference
* PC/SC wrapper classes for .NET Documentation