



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Projekt TraceXpert

Projekt *Nástroje pro verifikaci bezpečnosti kryptografických zařízení s využitím AI*
podpořený Ministerstvem vnitra České republiky (výzva IMPAKT)

ČVUT ve spolupráci s VUT a MUNI

Petr Socha, Vojtěch Miškovský
1. července 2022, Horoměřice

Cíle

- Měření postranních kanálů
- Práce s různými komunikačními rozhraními a protokoly, kryptografickými zařízeními, osciloskopy, měřícími scénáři
- Uživatelsky přívětivé grafické rozhraní
- Multiplatformní, vícejazyčné (česky, anglicky)
- Výpočetně nenáročné
- Koncoví uživatelé: Policie České republiky (PČR), Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), Certifikační laboratoře, Univerzity,...

Klíčové osoby

- Petr Socha – koordinátor prací, vývojář
- Vojtěch Miškovský – vývojář
- Tomáš Přeučil – vývojář

- David Pokorný – tester
- Martin Novotný – tester

Funkcionalita I

- Projekty
 - Uložitelné a znovu otevíratelné projekty
- Vstupně/výstupní zařízení
 - Soubory, generátory náhodných dat, sériový port, smartcard, lokální/síťový socket,...
 - Implementováno jako plug-iny se společným rozhraním
 - Plně nastavitelné a ovladatelné skrze grafické rozhraní

Log

```
in[0]: 0x00 0x01 0x02 0x03 0x04
out[0]: 0xFF 0xAB 0x00 0xFF 0x11
```

Raw String

Option	Value	Description
Port	COM3	Serial port name
Baudrate	9600	Transmission baudrate
Stop bits	1	Number of stop bits
Parity	None	Parity check type

Funkcionalita II

- Protokoly

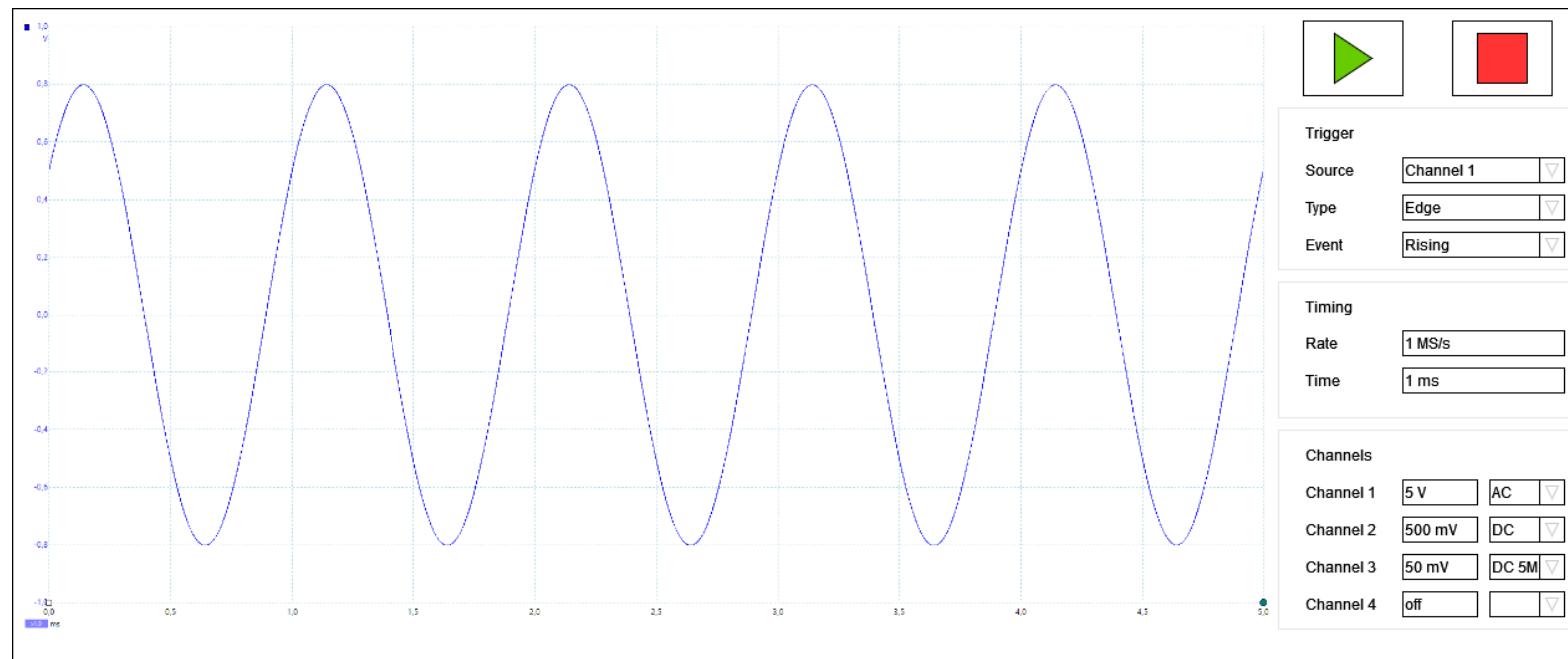
- Předdefinované parametrizovatelné zprávy
- Odesílané nebo obdržené ze vstupně/výstupního zařízení
- Konfigurovatelné skrze grafické rozhraní

The image shows a configuration window with three main sections: Protocols, Command, and Content. The Protocols list includes SmartCardAES, SerialAES (highlighted), and SerialAESMasked. The Command list includes SetKey, SendData (highlighted), and ReceiveData. The Content list includes command (highlighted) and data. To the right of these lists are radio buttons for 'Static value' (selected) and 'Dynamic value'. Below these are radio buttons for 'Signed', 'Unsigned' (selected), 'Float', 'String', and 'Raw'. There are two input fields: one containing '0x03' and another labeled 'Size' containing '1'.

Protocols	Command	Content	Value Type	Value	Size
SmartCardAES	SetKey	command	<input checked="" type="radio"/> Static value	0x03	1
SerialAES	SendData	data	<input type="radio"/> Dynamic value		
SerialAESMasked	ReceiveData		<input type="radio"/> Signed		
			<input checked="" type="radio"/> Unsigned		
			<input type="radio"/> Float		
			<input type="radio"/> String		
			<input type="radio"/> Raw		

Funcionalita III

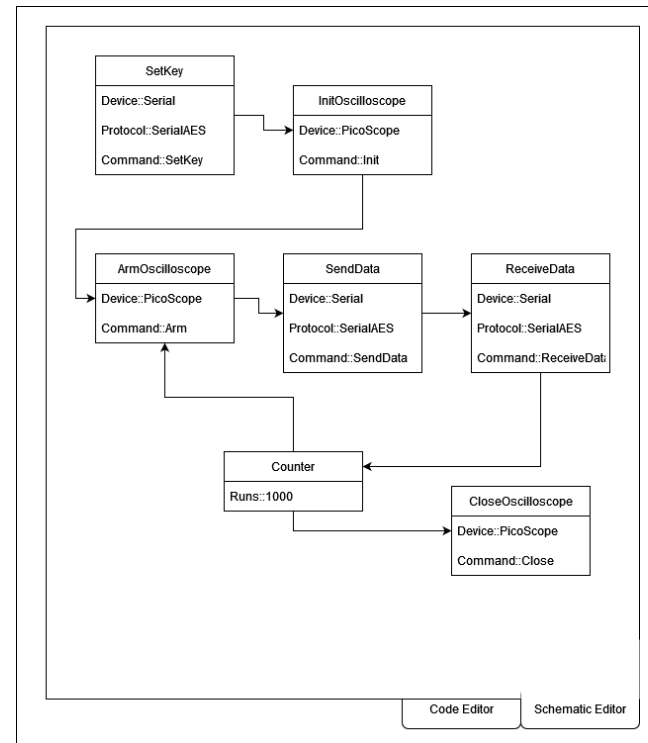
- Osciloskopy
 - Implementovány jako plug-iny se společným API
 - Plně konfiguratelné a ovladatelné skrze grafické rozhraní
 - Výstupní data (traces) snadno vizualizovatelné



Funkcionalita IV

- Měřicí scénáře
 - Automatizace ovládání vstupně/výstupních zařízení a osciloskopů
 - Plně konfigurovatelné a ovladatelné skrze grafické rozhraní

- Průvodci a vyčerpávající dokumentace



Task type

IO Oscilloscope Condition Custom

Option	Value	Description
Device	Serial	
Protocol		
Command		
Port	COM3	Serial port name
Baudrate	9600	Transmission baudrate
Stop bits	1	Number of stop bits
Parity	None	Parity check type
...

Task type

IO Oscilloscope Condition Custom

Code Editor

To je vše.

Otázky?

Děkuji za Vaši pozornost.