

# Politechnika Wrocławska

## Wydział Elektroniki

Kierunek: Cyberbezpieczeństwo

Ochrona Centrów Danych

Raport 5

Aneta Prządka 227164

## 1. Cel ćwiczenia

Celem piątych laboratoriów było stworzenie przykładowego projektu TPM podanych na stronie <https://github.com/tpm2-software>. Do przeprowadzenia symulacji wybrano TOTP – Time-based One-time Password, czyli algorytm generujący jednorazowe hasła, wykorzystujące czas jako niepowtarzający się składnik hasłujący.

Gdy program znajduje się w stanie „zaufania”, użytkownik generuje tajny klucz tpm2-totp, który jest stały do bieżących wartości PCR modułu TPM. Secret jest również eksportowany (np. przez kod QR), dzięki czemu można go zapisać w aplikacji TOTP (w aplikacji na telefonie).

Podczas rozruchu system operacyjny wysyła aktualny czas do modułu TPM. Moduł TPM sprawdza, czy obecne są prawidłowe wartości PCR i oblicza HMAC wejściowego czasu. Ten wynik to wartość TOTP, która zostanie wyświetlona użytkownikowi. Użytkownik może porównać tę wartość z wartością TOTP swojego urządzenia zewnętrznego (np. telefonu) i w ten sposób potwierdzić niezmiennosć i wiarygodność swojego urządzenia.

## 1. Przebieg ćwiczenia

Co ważne, trzeba pamiętać o uruchomieniu symulatora.

[illegible]

Rysunek 1. Sprawdzenie działania kontenera.

Należało pobrać poniższe repozytorium:

<https://github.com/tpm2-software/tpm2-totp>

Następnie wejść w nie i bazując na pliku `INSTALL.md` przejść przez proces instalacyjny. Po wykonaniu `make install` i komendzie `tpm2-totp init` powinien wyskoczyć kod QR lub secret. Ściągając na swój telefon aplikacje do totp (np. Authenticator) należy utworzyć konto na podstawie kodu QR lub secret.

Za pomocą komendy `tpm2-totp show` należy sprawdzić, czy kody (podane jako nazwa user) w aplikacji i na maszynie się zgadzają.

```
root@2c3e7ca1dd75:/tpm2-totp# show
bash: show: command not found
root@2c3e7ca1dd75:/tpm2-totp# tpm2-totp show
772706root@2c3e7ca1dd75:/tpm2-totp# tpm2-totp clean
root@2c3e7ca1dd75:/tpm2-totp# tpm2-totp init
```



```
otpauth://totp/TPM2-TOTP?secret=ZDRWCQ2EQGYCUZQ6KQPHT2RXH7LBYNZX
root@2c3e7ca1dd75:/tpm2-totp# tpm2-totp show
704470root@2c3e7ca1dd75:/tpm2-totp# tpm2-totp clean
root@2c3e7ca1dd75:/tpm2-totp# tpm2-totp init
```

Rysunek 2. Działający totp, wyświetlający kod QR.

Uruchamiając maszynę następnego dnia da się zauważyć, że kody nie są odpowiednio te same. Wynika to z rozjeżdżania się dat poprzez np. zapisanie stanu maszyny lub zrobienie migawki. Można to sprawdzić dopisując flagę `-t` do komend. Aby zapobiec takim problemom należy zainstalować na maszynie `ntp` (komenda `sudo apt-get install ntp`), co pozwala pokazywać aktywności maszyny w czasie rzeczywistym.