Politechnika Wrocławska
Wydział Elektroniki

Kierunek: Cyberbezpieczeństwo

Ochrona centrów danych

TPM - TOTP

Politechnika Wrocławska

Krzysztof Bocian

Wrocław, 2021

1.Wstęp

Celem tego laboratorium było stworzenie i zaprezentowanie projektu opartego o TPM. TPM czyli Trusted Platform Module to standard układu scalonego. Stworzone zostały by mogły wykonywać operacje obliczeniowe związane z kryptografią, np. generowanie liczb pseudolosowych, podpisów cyfrowych. Często za ich pomocą zabezpiecza się produkty, w których ingerencja użytkownika mogłaby narazić produkt na uszkodzenie.

Do przeprowadzenia projektu wybrałem TOTP. TOTP (Time-based One-time Password) to algorytm generujący jednorazowe hasło wykorzystujący czas jako nie powtarzający się składnik szyfrujący. W trakcie projektu korzystałem z https://github.com/tpm2-software/tpm2-totp.

2.Realizacja projektu

Podczas projektu skorzystałem z kontenera w Dockerze do utworzenia środowiska wraz z symulatorami TPM. To rozwiązanie pozwala na ingerowanie w TPM, co nie jest możliwe w rozwiązaniu hardware'owym. Instalacja projektu githuba została zrealizowana zgodnie z zamieszczoną w nim instrukcją, czyli:

1. Pobranie projektu za pomocą komendy "git clone".
2. Pobranie i instalacja wymaganych pakietów.
3. Wykonanie komendy ./bootstrap
4. Wykonanie komendy ./configure
5. Wykonanie komendy make & make install

Ważne aby po instalacji upewnić się, że uruchomiony jest symulator TPM, w innym wypadku wystąpi błąd krytyczny. W moim przypadku zrobiłem to za pomocą poniższych komend:

dbus-daemon –system

tpm2-simulator 2325 -m &

tpm2-abrmd –allow-root -t mssim:port=2325 &

Po wykonaniu tych kroków projekt tpm2-totp powinien być gotowy do uruchomienia. Najprostszym sposobem sprawdzenia tego jest wykonanie komendy “tpm2-totp init”, co spowoduje wygenerowanie “secret” z domyślnymi wartościami, czyli PCR (Platform Configuration Register) 0, 2, 4 oraz SHA1 i SHA256. Można zmieniać te wartości stosując argumenty odpowiednio -P dla PCR oraz -b dla szyfrowania.

Aby sprawdzić poprawność działania projektu pobrałem oprogramowanie TOTP Authenticator na telefon i sprawdziłem, czy wygenerowany wynik będzie taki sam jak w kontenerze. Od strony urządzenia mobilnego zeskanowałem kod QR wygenerowany przez projekt i na jego podstawie stworzyłem użytkownika. Wykonując komendę “tpm2-totp show” generowane było hasło na podstawie secret oraz czasu. Ważne jest, aby na maszynie była aktualna data z dokładnością do sekund, ponieważ to na tej podstawie generowane są hasła. W moim przypadku zainstalowałem usługę NTP aktualizującą czas za pomocą serwera zewnętrznego. Po wykonaniu komendy hasło zgadzało się z tym, co wygenerowała aplikacja TOTP Authenticator.

3.Troubleshooting

Podczas realizacji projektu napotkałem się na dwa błędy. Pierwszym z nich był błąd krytyczny podczas uruchamiania tpm2-totp. W moim przypadku było to spowodowane wyłączonym symulatorem TPM. Warto wspomnieć że taki sam komunikat generowany jest, gdy tpm2-totp nie ma dostępu do symulatora. Jednym z powodów, może być nieodpowiedni użytkownik, dlatego nie mając dostępu do roota, należy korzystać z konta “tss”, które tworzone jest podczas instalacji TSS.

Drugim problemem była synchronizacja czasu w aplikacji mobilnej i projekcie. Ważne jest to, że generowane hasło korzysta z okienka 20s, dlatego każda różnica w czasie obu urządzeń może spowodować rozbieżność w czasie. Najlepiej, aby oba urządzenia korzystały z jednego serwera czasu, a przynajmniej z serwerów zbliżonych do siebie