dr inż. Piotr Bora
prof. dr hab. Jerzy Gawinecki
Wojskowa Akademia Techniczna
Wydział Cybernetyki
Instytut Matematyki i Kryptologii

Bezpieczeństwo systemów kryptograficznych wykorzystujących karty procesorowe

W konstrukcji współczesnych systemów kryptograficznych często wykorzystuje się dedykowane urządzenia wspomagające obliczenia oraz realizujące inne funkcje, jak np. bezpiecznego przechowywania newralgicznych danych takich jak klucze do algorytmów szyfrowania informacji. Problem oceny bezpieczeństwa systemu kryptograficznego sprowadza się tu nie tylko do oceny użytych w nim algorytmów czy protokołów, ale również do oceny implementacji i możliwości ataku na elementy sprzętowo-programowe systemu. W dobie coraz powszechniej dostępnego sprzętu pomiarowego o coraz lepszych parametrach, coraz powszechniejsze są możliwości ataku na implementacje sprzętowe zarówno samych algorytmów szyfrowania, jak i koprocesorów wykonujących obliczenia dla potrzeb kryptografii klucza publicznego.

W referacie przedstawiono skrótowo ataki na implementacje algorytmów blokowych szyfrowania informacji poprzez analizę ulotu elektromagnetycznego ze szczególnym uwzględnieniem ulotu przewodzonego. Przedstawiono w zarysie metody odtwarzania klucza roboczego dla elementów niezabezpieczonych na prezentowane ataki, jak i zabezpieczonych. Odniesiono się do ogólnego sformułowania modułu szyfratora z uwzględnieniem rozwiązań zarówno w oparciu o karty procesorowe, jak i specjalizowane szyfratory. Na podstawie przedstawionych ataków odniesiono się do bezpieczeństwa implementacji i metod zabezpieczeń dla rozwiązań bazujących na układach FPGA.

O stopniu zagrożenia dla systemów kryptograficznych wykorzystujących karty procesorowe (np. systemy bankowe) może świadczyć fakt, że atak wykorzystujący analizę poboru mocy, przy niezabezpieczonych kartach wymaga wykonania tylko jednej transakcji dla odtworzenia tajnych wartości klucza.