mgr inż. Łukasz Dzieł
Wojskowa Akademia Techniczna, Wydział Cybernetyki
Instytut Matematyki i Kryptologii

Atak poboru mocy na niektóre implementacje sprzętowe pewnej klasy algorytmów kryptograficznych

Referat dotyczy możliwości wykonania ataku poboru mocy na implementacje sprzętowe algorytmów, które posiadają pewną szczególną budowę. Wadliwa konstrukcja implementacji sprzętowej algorytmu, pomimo bezpieczeństwa samego algorytmu, umożliwia odzyskanie pewnych informacji o tajnym kluczu za pomocą ataku poboru mocy. Przykładem takiego algorytmu jest obowiązujący standard szyfrowania — AES.

W trakcie referatu omówione zostaną najistotniejsze elementy budowy algorytmu AES w zakresie koniecznym do wykonania ataku. Przedstawiona zostanie koncepcja budowy i sposobu działania układu sprzętowego realizującego szyfrowanie wspomnianym algorytmem. Omówiona zostanie budowa uproszczonej implementacji sprzętowej algorytmu AES, która jest podatna na opracowany przez autora atak poboru mocy. Następnie podane zostaną przyjęte założenia, które umożliwiają realizację ataku poboru mocy. Przedstawiona zostanie idea opracowanego ataku. Następnie opisana zostanie procedurą postępowania, która umożliwia odzyskanie całego tajnego klucza z urządzenia, w którym używana jest implementacja sprzętowa podobna do przedstawionej. Wykazane zostanie, że przedstawiony błąd w implementacji sprzętowej występuje także w innych, powstałych niezależnie i obecnie dostępnych publicznie implementacjach sprzętowych algorytmu AES. Jako pierwsza przedstawiona zostanie analiza implementacji wykonanej przez specjalistów z NSA na potrzeby NIST podczas konkursu AES. Drugą z analizowanych implementacji jest losowo wybrany koprocesor kryptograficzny dostępny na stronie `opencores.org`. Na zakończenie referatu przedstawiony zostanie sposób modyfikacji przedstawionej implementacji, tak aby zapewnić odporność na opracowany atak poboru mocy. Porównana zostanie efektywności działania poprawionej implementacji w stosunku do implementacji nieodpornej na opracowany atak.

Praca naukowa finansowana ze środków na naukę w latach 2008–2010 jako projekt rozwojowy Nr R00 0031 06.