Tomasz Kawecki

Bezpieczeństwo kart elektronicznych

Wydawałoby się, że działanie, które mogłoby ingerować w bezpieczeństwo urządzeń i systemów bazujących na kartach elektronicznych jest niemożliwe. Pomysłowość użytkowników nie ma jednak granic, a hackerzy wymyślają kolejne metody ataków na karty elektroniczne. Najlepszym tego przykładem są systemy kodowania PAY TV, których zabezpieczenia zostały złamane. Zastosowano w nich karty elektroniczne, ale okazały się one nieskuteczne, a instrukcje dotyczące łamania zabezpieczeń szybko rozprzestrzeniły się za pośrednictwem Internetu. Nadawcy sygnałów kodowanych zostali zmuszeni do zmian systemów kodowania, a co za tym idzie ponieśli znaczne koszty. Utworzone zostały nawet specjalne wydziały do walki z piractwem, których główną rolą jest śledzenie na bieżąco informacji o błędach i niedopatrzeniach w systemach.

Karty elektroniczne mogą być zaatakowane na dwa sposoby – inwazyjnie i nieinwazyjnie. Przeprowadzenie ataku inwazyjnego polega na fizycznej ingerencji w strukturę karty elektronicznej. Ataki nieinwazyjne, nazywane również atakami podsłuchowymi, wykorzystują analogowe cechy dostarczania napięcia i połączeń interfejsowych oraz wszelkie inne cechy promieniowania elektromagnetycznego wytwarzanego podczas normalnej pracy karty.

Jednym z łatwiejszych ataków do przeprowadzenia jest zablokowanie dostępu czytnika do odpowiednich styków karty. Takie właśnie działania udały się w stosunku do systemów PAY TV, których sygnały transmisyjne były używane do sterowania kartą tak, aby blokowała kanały, za które nie wniesiono opłaty. Zaklejenie styku taśmą zapobiegało docieraniu sygnału blokującego do karty, która z kolei pozwalała użytkownikowi na bezpłatne korzystanie ze wszystkich kanałów. Podobne podejście zastosowano w systemach telefonii publicznej – jeżeli styk używany do zmniejszania wartości karty był zabrudzony lub wygięty, to liczba impulsów zapisanych na karcie pozostawała taka sama, bez względu na ich zużycie. Dzisiaj niewiele kart na rynku jest podatnych na takie proste typy ataków.

Analiza taktowania (*timing analysis*) może ujawnić czas poszczególnych operacji wykonywanych przez kartę elektroniczną. Jeżeli osoba przeprowadzająca atak ma dostęp do karty i może dokonać pomiarów czasu wymaganego dla poszczególnych operacji, to za pomocą wyników pomiarów można określić klucz kryptograficzny zapisany w karcie. Do wiadomości publicznej analiza taktowania została podana w grudniu 1995 roku, a jej wynalazcą jest Paul Kocher. Metodą pozwalającą na zapobieganie takim atakom jest nieliniowy sposób uaktualniania klucza.

Prosta analiza zasilania (*Simple Power Analysis*) oraz analiza różnicowa zasilania (*Differential Power Analysis*) mogą posłużyć ujawnieniu charakterystyk zapotrzebowania na zasilanie karty elektronicznej, a następnie charakterystyki takie mogą zostać wykorzystane do ujawnienia klucza, protokołów i algorytmów używanych w architekturze karty. Wynalazcą tego rodzaju ataków jest również Paul Kocher. Ataki bazujące na analizie zasilania zostały przedstawione dopiero kilka lat temu, więc istnieje niewiele praktycznych środków zaradczych pozwalających na zapobieganie im. Bardzo obiecującą metodę polegającą na zastosowaniu diody i sieci kondensatorów w jednostce odpowiedzialnej za zasilanie karty elektronicznej zaproponował A. Shamir.

Ataki wykorzystujące zakłócenia transjentowe (*glitch attacks*), ataki protokołów programowych oraz generowania wyjątków bazują na odchyleniach od normy występujących w układach scalonych. Wymagają one szczegółowych analiz oraz wykorzystania metody prób i błędów, aby zdeterminować reakcję mikroprocesora w odniesieniu do pewnych warunków środowiskowych – np. wysokich lub niskich częstotliwości zegara, wahania zasilania czy innych zakłóceń. Mogą one zostać wykorzystane do zmiany stanów przełączników logicznych.

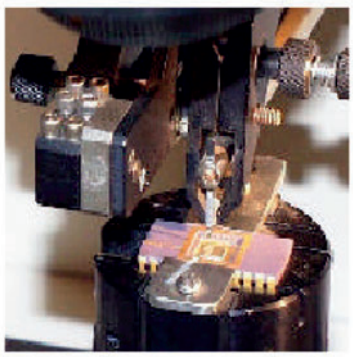
Wykorzystanie losowych sygnałów zegara czy losowej wielowątkowości operacji zapewni ochronę przed przewidywaniem czasu, w jakim wykonane zostaną pewne operacje. Wiele z produkowanych mikroprocesorów jest wyposażonych w czujniki, które powodują wyłączenie układów scalonych, jeżeli np. częstotliwość zegara, temperatura czy napięcie znajdą się poza określonym przedziałem.

Przeprowadzenie ataku inwazyjnego polegającego na ingerencji w fizyczną strukturę karty elektronicznej jest zaskakująco proste i może umożliwić odczytanie najbardziej chronionych i poufnych informacji zawartych w karcie.

Osoba przeprowadzająca atak może poddać analizie i sondowaniu chip z karty elektronicznej używając standardowego stoiska do prób (*test bed*) poprzez usunięcie procesora z karty. Tworzywo sztuczne karty można usunąć za pomocą ostrego noża. Żywica epoksydowa może zostać rozpuszczona poprzez kilka kropel dymiącego kwasu azotowego (stężenie HNO_3 powyżej 98%). Promieniowanie podczerwone przyspiesza proces rozpuszczania. Rysunek 1 przedstawia opisaną sytuację.

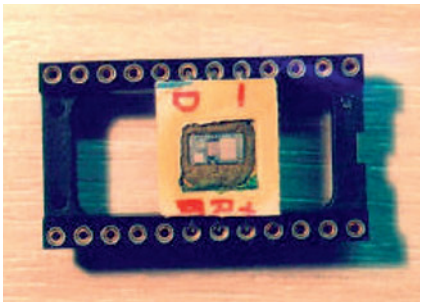
Rys. 1 *Rozpuszczanie żywicy epoksydowej przez kwas azotowy*
Źródło: M. Kuhn, O. Kömmerling, „Design Principles for Tamper-Resistant Smartcard Processors," Proceedings of the USENIX Workshop on Smartcard Technology (Smartcard '99), Chicago, Illinois, 10–11 maja 1999.

Następnie kąpiel acetonowa pozwoli na odkrycie powierzchni krzemowej. Procesor może zostać usunięty i przymocowany do obudowy testowej. Rysunek 2 przedstawia proces przymocowywania procesora do obudowy testowej. Rysunek 3 prezentuje przygotowany do mikrosondowania elektronowego procesor karty elektronicznej osadzony w obudowie testowej.



Rys. 2 *Przymocowywanie procesora do obudowy testowej*
Źródło: M. Kuhn, O. Kömmerling, „Design Principles for Tamper-Resistant Smartcard Processors," Proceedings of the USENIX Workshop on Smartcard Technology (Smartcard '99), Chicago, Illinois, 10–11 maja 1999.

Posiadając przygotowany procesor możemy odczytać jego sygnały wewnętrzne za pomocą testerów strumieni elektronowych i igieł mikrosondujących. Działanie karty elektronicznej może zostać zmienione przy użyciu laserów, strumieni ultrasonicznych lub skupionych wiązek jonowych.



Rys. 3 *Mikroprocesor przygotowany do eksperymentów mikrosondowania elektronowego*
Źródło: M. Kuhn and R. Anderson, „Tamper Resistance – a Cautionary Note," the Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, California, 18–21 listopad 1996.

Podkładki testowe procesora można zidentyfikować za pomocą mikroskopu współogniskowego. Czasem bezpieczniki testowe zostają pozostawione niezniszczone po produkcyjnym cyklu testowania karty, a w przypadku, gdy bezpieczniki są stopione, można zastosować metodę mostkowania za pomocą dwóch igieł mikrosondujących. Tak odtworzony system testowy procesora pozwala na odczytanie zawartości pamięci procesora.
Jedną z zaproponowanych metod zabezpieczenia przed manipulacjami opisanymi powyżej jest zastosowanie czujnika pojemnościowego, aby wykryć ciągłą obecność warstwy uodparniającej na korozję. Możliwe jest również zastosowanie czujnika optycznego umieszczonego w nieprzezroczystej powłoce, który wykryłby próbę manipulacji i zniszczył procesor.
Innym rodzajem ochrony przed atakami fizycznymi jest technika przedsiębiorstwa Philips nazywana logiką kleistą (*glue logic*). Logika ta zamienia rozmieszczenie elementów procesora w losowy zbiór komponentów, uniemożliwiając jednocześnie identyfikację poszczególnych bloków procesora. Oferowana jest również ochrona pamięci, ponieważ lokalizacja danych i ich właściwe adresy są nieskorelowane. Technika ochrony pamięci ma jednak zastosowanie tylko w przypadku pamięci dynamicznych, np. RAM.
Producenci strzegą bezpieczeństwa informacji na temat stosowanych zabezpieczeń i odporności układu na manipulacje. Tabela 1 przedstawia zestawienie wybranych modeli układów scalonych oraz wykaz stosowanych zabezpieczeń, o których informują producenci.[1] Zabezpieczenia te obejmują czujniki częstotliwości zegara, czujniki optyczne, detektory anormalnego napięcia programowania Vpp, oraz komórki typu *witness*, które

1 Producenci mogą umieszczać dodatkowe zabezpieczenia bez podawania informacji o ich obecności.

pozwalają na wykrycie kasowania obszarów pamięci EEPROM[2].

Tabela 1 *Układy scalone kart elektronicznych*

Nazwa układu	Producent	RAM (B)	ROM (kB)	NVM* (kB)	Detektory	Częstotliwość zegara (MHz)
SC01	Motorola	36	1.6	1 *	–	4
SC03	Motorola	52	2	2*	-	4
SC11	Motorola	128	6	8*	F, V	4
SC21	Motorola	128	6	3	F, V	4
SC24	Motorola	128	3	1	F, V	5
SC26	Motorola	160	6	1	F, V	5
SC27	Motorola	240	16	3	F, V	5
SC28	Motorola	240	12.8	8	F, V	5
ST1821	SGS	44	2	1 *	F, T, V, L	5
ST1834	SGS	76	4	3*	F, T, V, L	5
ST16612	SGS	224	6	2	F, T, V, L	5
ST16601	SGS	128	6	1	F, T, V, L	5
ST16623	SGS	224	6	3	F, T, V, L	5
ST16F44	SGS	512	16	8	F, T, V, L	5
ST16F48	SGS	512	16	8	F, T, V, L	5
ST16301	SGS	160	3	1	F, T, V, L	5
65901	Hitachi	128	3	3	W	5
6483108	Hitachi	256	10	8	W	5
H8310	Hitachi	256	10	8	W	5
H83102	Hitachi	512	16	8	W	5
62720	Oki	128	3	2	tajne	-
62780	Oki	192	6	8	tajne	-
44C10	Infineon	128	4	1	sprzętowe	5
44C40	Infineon	256	8	4	sprzętowe	5
44C80	Infineon	256	16	4	sprzętowe	5
P8WE6004	Philips	256	32	4	V, T, F	1...8
P8WE5033	Philips	256	96	32	V, T, F	1...8
P16WX064	Philips	5k	128	64	V, T, F	1...6

Oznaczenia: * pamięć nieulotna: gwiazdka oznacza pamięć EPROM, pozostałe pamięci to pamięci EEPROM; F – detektory częstotliwości zegara, L – czujniki ekspozycji na światło, V – detektory anormalnego napięcia Vpp, T – czujniki anormalnej temperatury pracy, W – komórki typu „witness" umożliwiające wykrycie nielegalnego kasowania pamięci EEPROM

Źródło: Naccache D., M'Raihi D., „Cryptographic Smart Cards", „IEEE Micro"

Czujniki bezpieczeństwa umożliwiają zapobieganie próbom monitorowania przez kasowanie pamięci RAM lub EEPROM, a detektory zegara wykrywają manipulacje częstotliwościami zegara. Czujniki optyczne wskazują czy procesor był usuwany z karty. Jeżeli częstotliwość zegara została zmieniona na wysoką, to pamięć EEPROM nie może być zapisana we właściwy sposób, a zbyt niska częstotliwość może świadczyć o próbie wymuszenia pracy krokowej. Napięcia niezgodne z normami pracy procesora mogą wpływać na pamięć EEPROM (poprzez skasowanie lub zablokowanie operacji kasowania) lub na generator liczb losowych, który generuje stałe wielkości liczb.

Na straży zwartości kart inteligentnych zazwyczaj stoi pewna liczba tajnych kodów, których klasyfikacji dokonać można według posiadacza informacji. Typowa karta elektroniczna pozwala na przechowywanie od 8 do 16 kluczy, wśród których wyróżniamy klucze dostawcy, producenta i użytkownika.[3] Na czas transportu nowy układ scalony zabezpieczony zostaje, przed użyciem przez niepowołane osoby, poprzez kod transportowy, który pozostaje zakodowany w pamięci układu, a ujawniony jest tylko producentowi i dostawcy. Dostęp do pamięci zostaje przyznany dopiero po wprowadzeniu odpowiedniej kombinacji znaków, a każda nieudana próba jest rejestrowana. Jeżeli liczba błędnych prób przekroczy pewną normę to układ jest nieodwracalnie blokowany.[4] Personalizacja karty możliwa jest dopiero po podaniu prawidłowego kodu, który zeruje licznik prób nieprawidłowych.

Personalizacja karty oznacza dla dostawcy usługi wprowadzenie danych dotyczących producenta karty, danych dostawcy lub dostawców oraz bezpośredniego właściciela. Wprowadzane zatem zostają odpowiednie klucze: klucz główny systemu (*master*), klucz dostawcy,[5] kod PIN, klucz karty.[6]

Karty elektroniczne posiadają wiele zastosowań oferując jednocześnie wygodę. Niestety podatne są na różnego typu ataki. Aby karty inteligentne stały się bardziej rozprzestrzenionymi urządzeniami należy poprawić ich bezpieczeństwo. Zdaniem Adiego Shamira ogólne rozwiązanie zabezpieczające przez sondowaniem i atakami mikrochirurgicznymi jest obecnie niemożliwe. Zalecane są projekty wdrożeniowe dla systemów bazujących na kartach zanim wprowadzona zostanie masowa produkcja, aby uniknąć błędów umożliwiających skompromitowanie bezpieczeństwa tych systemów.

2 *Electrically-Erasable Programmable Read-Only Memory*

3 Zastosowane w mikroukładzie aplikacje mogą wymagać przechowywania większej ilości kluczy.

4 Np. układ Eurochip SLE 443x zostaje zablokowany po 5. nieudanych próbach. Porównanie kodu z wprowadzanym ciągiem znaków odbywa się wewnątrz procesora.

5 W układzie Eurochip SLE 443x dopuszczalne są dwa klucze dostawcy.

6 Klucz karty zostaje wyliczony w zależności od numeru seryjnego karty i jej danych identyfikacyjnych.