GRZEGORZ BŁOŃSKI

Atak na Smart Cards

Stopień trudności

Codziennie używamy inteligentnych kart, myslimy że nasze pieniądze i dane zakodowane na kartach są bezpieczne, ale czy na pewno? Dowiedz się jakie zagrożenia na nas czekają i jak można zaatakować inteligentną kartę?

Kartę taką, o troszkę innym rozmiarze niż ten opisywany w normie ISO, posiada każdy użytkownik telefonu komórkowego. Pasjonaci telewizji satelitarnej doskonale znają karty tego rodzaju, gdyż wykorzystywane są przez komercyjne stacje nadawcze do weryfikacji opłaconego abonamentu i dekodowania programów płatnych. Podobne rozwiązania są stosowane również w kartach telefonicznych. Markowe laptopy nierzadko wyposażone są w czytniki SmartCard, więc można zabezpieczyć w ten sposób także swojego notebooka. Popularne stały się zamki w drzwiach oparte o technologię takich kart. Zapewne można znaleźć więcej zastosowań kart inteligentnych, jednak nie to jest w artykule najważniejsze. Skupimy się na tym, jak zbudowane są karty, jak działają, czy takie rozwiązania są bezpieczne i czy można im ufać.

Wymiary kart według normy ISO7816 to 85,6 mm x 53,98 mm x 0,8 mm. Najczęściej wykonane są one z plastiku z zatopionym układem elektronicznym i stykami umieszczonymi w określonym normą miejscu. Ten rodzaj kart określany jest mianem kart zintegrowanych. Istnieją jeszcze karty HMD (ang. *Hole Mounted Device*) oraz SMD (ang. *Surface Mounted Device*), jednak są one raczej stosowane jako karty testowe oraz laboratoryjne.

Złącze karty, na którym umieszczone są styki elektryczne, także posiada określone w normie wymiary i podzielone jest na osiem pól odpowiadających ośmiu stykom.

Protokół komunikacyjny APDU

Na APDU składają się dwa polecenia, które odpowiadają za komunikację pomiędzy kartą.

Command APDU (C-APDU): polecenie wykorzystywane przez aplikację na komputerze do wysyłania poleceń do karty. Korzysta z poniższych struktur danych:

- *header*, składa się z 4 bajtów:
  - klasy instrukcji (CLA),
  - kodu instrukcji (INS),
  - Parametrów: P1 oraz P2.
- *body* (opcjonalne), o zmiennej długości:
  - Lc – określa rozmiar ciała lub obszaru danych (w bajtach),
  - Le – określa rozmiar danych lub liczbę bajtów, na które oczekuje komputer w odpowiedzi na wysłaną komendę,
  - Data field (obszar danych) – zawiera dane wysyłane do karty w celu wykonania instrukcji zawartej w nagłówku.

- Response APDU (R-APDU): polecenie używane przez kartę w odpowiedzi na polecenie wysłane przez aplikację z komputera.
- *body* (opcjonalne): zawiera obszar danych określonych przez Le,
- *trailer*: zawiera dwa słowa, SW1 oraz SW2, wywołane jako status, które opisują stan przetwarzania na karcie po wykonaniu polecenia APDU.

Z ARTYKUŁU DOWIESZ SIĘ

co to jest karta inteligentna,

jak atakowana jest karta.

CO POWINIENEŚ WIEDZIEĆ

jak ważne jest bezpieczeństwo,

znać podstawy elektroniki,

umieć posługiwać się oscyloskopem.

Protokoły transmisji danych TPDU

Dwa typy protokołów *Transmission Protocol Data Units* (TPDUs) używane są do transmisji APDU oraz struktury danych, która uległa zmianie:

- T = 0: najmniejszą przetwarzaną i transmitowaną jednostką jest bajt,
- T = 1: ten protokół przetwarza sekwencje danych (bloki danych).

ATR

ATR (*Answer To Reset*) – odpowiedź na sygnał reset, używana do potwierdzania parametrów karty niezbędnych do nawiązania komunikacji z czytnikiem. Sygnał ATR wysyłany jest z karty do czytnika w momencie podania zasilania na styki karty.

Wiadomość ATR – przeważnie w rozmiarze do 33 bajtów – zawiera parametry transmisji (T=0 oraz T=1), które są obsługiwane przez kartę, a także inne konieczne dla komputera z czytnikiem informacje, takie jak:

- prędkość transmisji danych,
- parametry sprzętowe karty,
- numer seryjny karty,
- numer wersji maski.

System plików

Hierarchiczny system plików wykorzystywany w kartach inteligentnych wspiera trzy typy plików:

- Master file (MF) – pojedynczy plik znajdujący się w głównym katalogu systemu, zawierający w sobie pliki DF oraz EF.
- Dedicated file (DF) – katalog przechowujący inne pliki DF oraz EF.
- Elementary file (EF) – to plik, który zawiera dane. Można wyróżnić dwa typy struktur pliku:
  - Transparent structure: plik zawierający sekwencję struktur danych,
  - Record structure: pliki zawierające zapis identyfikowalnych rekordów. Dla struktury tej da się zdefiniować kolejny podział:
    - Linear fixed: plik zawiera rekordy o ustalonym rozmiarze.
    - Variable: plik zawierający rekordy o zmiennym rozmiarze,
    - Cyclic: zawiera pliki zorganizowane w strukturze koła.

Najważniejsze z obecnie wykorzystywanych standardów kart procesorowych to:

- Norma ISO 7816: *Identification cards—Integrated circuit cards with contacts*, dokument opublikowany przez International Organization for Standarization (ISO), jest najważniejszym standardem definiującym charakterystykę kart chipowych posiadających styki elektryczne.
- GSM: European Telecommunications Standards Institute (ETSI) opublikował zestaw standardów określających rodzaje kart chipowych używanych w telefonii GSM. Obecnie używanych jest kilka standardów GSM (Tabela 4)
- EMV: Standard zdefiniowany i utworzony przez Euro pay, MasterCard oraz Visa, bazuje na standardach ISO 7816 z obsługą dodatkowych funkcji spełniających potrzeby sektora finansowego.
- OCF: *OpenCard Framework*: wstępnie stworzony przez IBM, obecnie rozwijany przez OpenCard Consortium, w skład którego wchodzą najwięksi producenci kart na świecie.
- PC/SC: specyfikacja PC/SC (*Interoperability Specification for ICCs and Personal Computer* Systems), zdefiniowana przez PC/SC Workgroup – kolejne konsorcjum zrzeszające producentów kart inteligentnych. PC/SC definiuje architekturę powszechnego wykorzystania kart inteligentnych w komputerach klasy PC. Obecnie jest to na tyle popularny standard, że jego obsługa została zaimplementowana w systemach Windows XP oraz Vista. Istnieje także jego implementacja dla systemów UNIX/LINUX, nosząca nazwę MUSCLE.

Tabela 1. *Styki karty według normy ISO 7816*

Numer styku	Nazwa	Opis
1	Vcc	napięcie zasilania 5V DC
2	Reset	reset
3	Clock	zegar
4	n/c	nie podłączony
5	GND	masa
6	n/c	nie podłączony
7	I/O	wejście/wyjście
8	n/c	nie podłączony

Tabela 2. *Budowa polecenia Command-APDU*

header				body		
CLA	INS	P1	P2	Lc	Data field	Le

Bezpieczeństwo kart inteligentnych

Bezpieczeństwo kart inteligentnych można rozpatrywać w czterech głównych kategoriach.

Bezpieczeństwo komunikacji

Komunikacja – jako jeden z kluczowych elementów pozwalających na wymianę danych pomiędzy kartą a urządzeniem ją odczytującym – odbywa się przy pomocy specjalnego protokołu APDU (*Application Protocol Data Units*). Wolny, bo na poziomie 9600 bitów w trybie half

Rysunek 1. *Karta chipowa z procesorem AT90S8515*

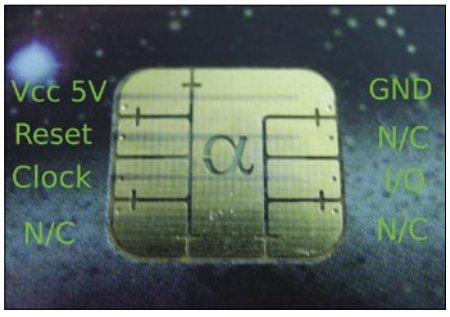
dupleks, transfer pozwala jednak na bezproblemowe wykorzystanie takich rozwiązań w wielu zastosowaniach. Niemniej każde urządzenie, z którym karta się komunikuje, jest elementem powodującym ryzyko ataku podczas przesyłania danych.

Karta do komunikacji z czytnikiem używa aktywnego protokołu autentykacji. Procesor pracujący w układzie karty generuje liczbę, która następnie jest przesyłana do czytnika – ten szyfruje ją za pomocą klucza publicznego i odsyła do karty. Procesor karty weryfikuje zwróconą liczbę przy pomocy własnego klucza i zezwala na komunikację. Kiedy połączenie zostaje ustanowione, każda wiadomość przesyłana pomiędzy czytnikiem i kartą jest weryfikowana specjalnym kodem. Kod ten to wartość wyliczona na podstawie przesyłanych danych, klucza szyfrującego oraz losowo wygenerowanej liczby. W przypadku jakiejkolwiek zmiany podczas transmisji – nawet z powodu zakłócenia – wiadomość musi zostać przesłana jeszcze raz.

Najczęściej wykorzystywane w kartach inteligentnych rodzaje szyfrowania to DES (*Data Encryption Standard*) – długość klucza 56 bitów, 3DES (potrójny DES) – długość klucza 168 bitów oraz RSA (*Rivest-Shamir-Adleman*) – długość klucza 1024 bity.

Bezpieczeństwo fizyczne.

Dane przechowywane na kartach inteligentnych znajdują się najczęściej w pamięciach EEPROM, które mogą być w łatwy sposób kasowane, a dane na nich – modyfikowane. Fizyczny dostęp do karty daje możliwość oddziaływania na nią na przykład promieniami cieplnymi czy świetlnymi w celu usunięcia zabezpieczeń zastosowanych przez część firm produkujących układy zabezpieczeń do kart inteligentnych. Bardziej destrukcyjne metody – takie, jak wycinanie układów z karty w celu ataku – są trudne do realizacji, ale w warunkach laboratoryjnych udaje się takie ataki przeprowadzać.



Rysunek 1a. *Złącze karty inteligentnej z bliska*

Bezpieczeństwo systemu operacyjnego.

Na kartach inteligentnych poszczególnych producentów zainstalowane są różne systemy operacyjne. Ich liczba stale rośnie, zatem opisywanie wszystkich obecnych na rynku nie ma sensu. Najbardziej znane i powszechne komercyjne systemy operacyjne kart chipowych to MULTOS i JavaCard. W opisanym wcześniej systemie plików wykorzystywanym w kartach inteligentnych możemy wyróżnić pięć podstawowych poziomów uprawnień.

- Always (ALW): Dostęp do pliku dla każdego bez żadnych ograniczeń.
- Card holder verification 1 (CHV1): Dostęp możliwy tylko, gdy podano właściwą wartość CHV1.
- Card holder verification 2 (CHV2): Dostęp możliwy tylko, gdy podano właściwą wartość CHV2.
- Administrative (ADM): Dostęp na poziomie administracyjnym.
- Never (NEV): Dostęp do pliku zawsze zabroniony.

Wartości CHV1 oraz CHV2 można przyrównać do znanych nam z kart SIM kodów PIN oraz PIN2. Każda z tych wartości posiada zdefiniowany

Tabela 3. *Budowa odpowiedzi Response-APDU*

body	trailer	
Data field	SW1	SW2

Tabela 4. *Standardy kart GSM*

GSM 11.11	Specyfikacja interfejsu SIM-mobile
GSM 11.14	Specyfikacja narzędzi aplikacyjnych SIM dla interfejsu SIM-mobile
GSM 03.48	mechanizmy bezpieczeństwa dla narzędzi aplikacyjnych SIM
GSM 03.19	SIM API (*Application Programming Interface*) dla platformy Java Card bazuje na standardach GSM 11.11 oraz GSM 11.14, definiuje Java API dla rozwoju aplikacji GSM, które mogą pracować na platformie Java Card.

Tabela 5. *Zestaw instrukcji wykorzystywanych w komunikacji czytnika z kartą*

Instrukcje	Funkcje
0x60	Sprawdza typ czytnika i aktywuje go
0x61	Ustawia czytnik parametrami ICC
0x62	Włącza zasilanie karty
0x63	Wyłącza zasilanie karty
0x64	Wysyła sygnał RESET do karty
0x65	Sprawdza status karty
0x66	Wysyła jeden bajt danych do czytnika
0x67	Wysyła blok danych do czytnika
0x68	Przesyła ponownie ostatni blok danych
0x69	Wyświetla możliwości czytnika
0x6A	Deaktywuje czytnik
0x6B	Aktywuje opcje dodatkowe czytnika
0x6C-0x6F	Instrukcje zapasowe do wykorzystania w przyszłości

licznik błędnie wprowadzanych kodów, poszczególni producenci stosują różne wartości.

Bezpieczeństwo oprogramowania

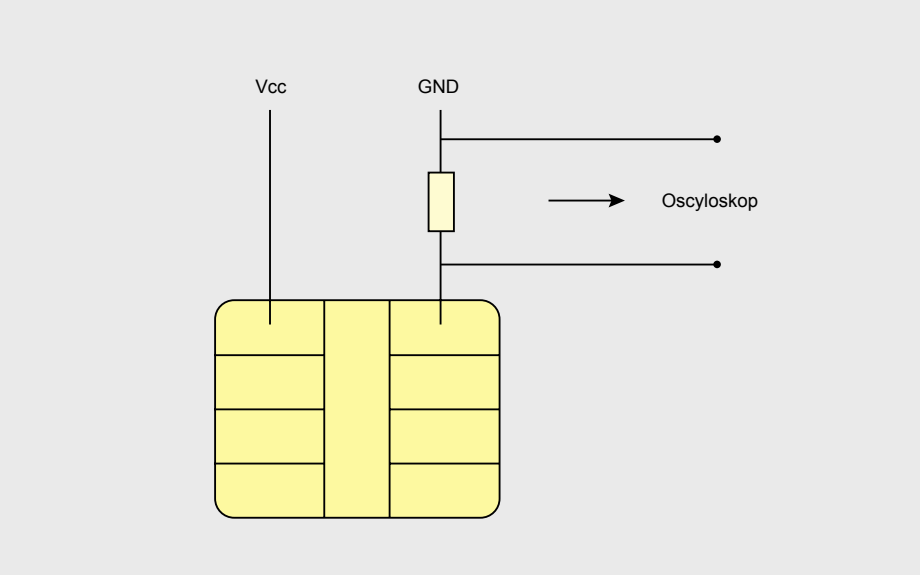
W tej materii pole do popisu mają autorzy programów współpracujących z czytnikami kart i kartami. Jeśli aplikacje przez nich wprowadzane na rynek są odpowiednio zabezpieczone i nie posiadają luk pozwalających na *przechwycenie* transmisji pomiędzy kartą a oprogramowaniem komputera, to możemy czuć się bezpieczni.

Rodzaje ataków na karty inteligentne

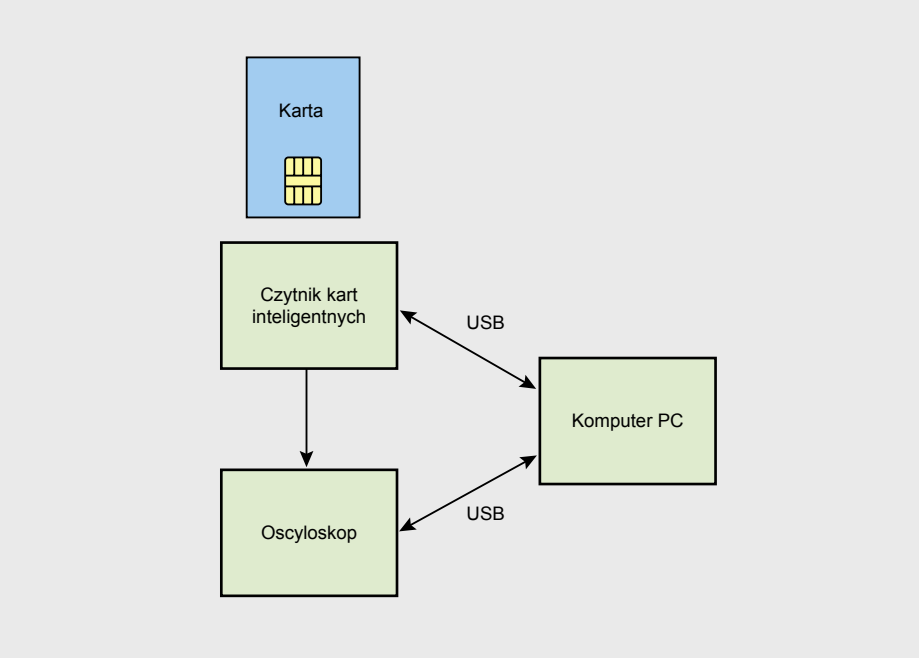
Możliwości zaatakowania kart inteligentnych nie są może ogromne, lecz istnieje kilka znanych technik, które są wykorzystywane przez crackerów.

Prześwietlanie promieniami UV lub rentgenowskimi w celu uzyskania informacji takich jak PIN czy klucz prywatny lub publiczny to metoda raczej teoretyczna i niedostępna dla każdego. Analiza EM przy użyciu mikroskopu elektronowego w celu dokładnego zbadania struktury maski to także raczej sposób dla naukowców w laboratoriach. Przykładem ataku możliwego do wykonania przez prawie przeciętnego zjadacza chleba może być klonowanie, czyli wykonanie wiernej kopii karty. Działanie takie jest nielegalne – jest ewidentnie swoistym rodzajem ataku, a jako przykład można przytoczyć kopiowanie kart kodowych nadawców płatnej telewizji satelitarnej. Znanym i dobrze opisanym jest atak DPA (*Differential Power Analysis*), polegający na analizowaniu przebiegów różnych wartości sygnałów podczas używania karty. Dogłębna analiza pozwala na odkrycie wzoru zapisu danych i późniejsze skompromitowanie karty poprzez poznanie jej PINu czy klucza prywatnego. Sprzęt potrzebny do takiego ataku to odpowiednio zmodyfikowany czytnik kart oraz oprogramowanie pozwalające dokonywać zapisu przebiegów elektrycznych. Inną, prostszą odmianą tego ataku jest SPA (*Simple Power Analysis*), polegająca na bezpośredniej analizie zapisanych danych odnoszących się do linii zasilającej kartę i zachowań poziomów napięć i prądu podczas wykonywania operacji na karcie.

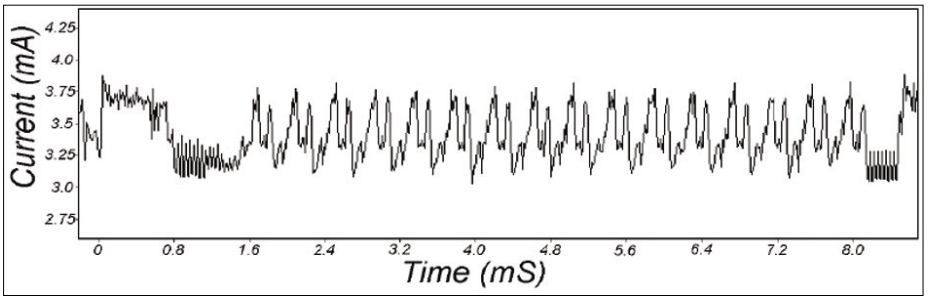
Do wykonania takiego ataku potrzeba nieco wiedzy z zakresu elektroniki, odrobiny sprzętu pomiarowego, komputera i oprogramowania do zapisu próbek oraz późniejszej analizy. Aby móc dokonywać pomiarów wartości prądu i napięcia na stykach karty, należy odpowiednio zmodyfikować czytnik w taki sposób, aby można było podłączyć do niego sondę pomiarową oscyloskopu.



Rysunek 2. *Schemat podłączenia oscyloskopu do złącza smartcard*



Rysunek 3. *Schemat blokowy zestawu do akwizycji danych w ataku SPA*



Rysunek 4. *Widoczne różnice w obciążeniu prądowym karty*

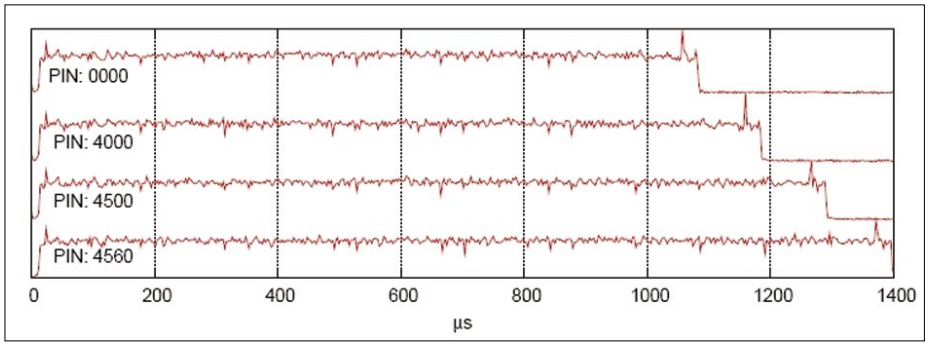
Uproszczony schemat modyfikacji, którą należy wykonać, można zobaczyć na Rysunku 2. Zastosowany rezystor powinien mieć wartość od kilku do kilkudziesięciu omów. Różne źródła podają wartości w zakresie od 5 do 50 omów.

Pomiar dokonywany za pomocą oscyloskopu na biegunach rezystora pozwala rejestrować wahania napięcia powodowane przez wykonywanie na karcie różnych operacji. Pojedynczy zapis operacji w postaci wykresu nazywany jest ścieżką.

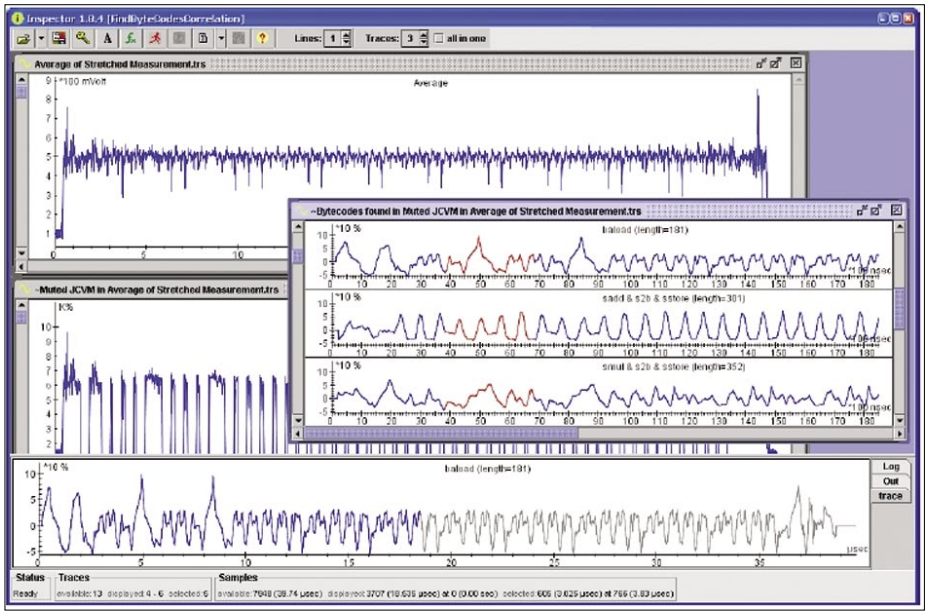
Simple Power Analysis polega na wizualnej analizie zebranych w ten sposób próbek. Odpowiednio zmodyfikowany czytnik kart w połączeniu z komputerem oraz oscyloskopem tworzy zestaw przygotowany do akwizycji danych. Przykład takiego rozwiązania z wykorzystaniem czytnika podłączanego poprzez USB oraz oscyloskopu (również podłączonego poprzez USB) pokazuje schemat blokowy na Rysunku 3.

Zapis widoczny na Rysunku 4. pokazuje, że różne operacje wykonywane przez układ elektroniczny karty powodują zmieniający się w czasie pobór prądu przez kartę. Wynika to z faktu, iż poszczególne fragmenty programu obsługi karty (a więc różne instrukcje) powodują zmienną aktywność mikroprocesora karty, czyli różne obciążenie prądowe. Dzięki takim właśnie różnicom Simple Power Analysis jest możliwa do przeprowadzenia.

W przypadku karty SIM i próby odgadnięcia numeru PIN w celu uzyskania dostępu do zaawansowanych funkcji karty, wykresy będą się różniły w zależności od cyfr, które będą wprowadzane. Podczas wprowadzania ciągu 0000 wykres pokazuje, że czas pracy procesu sprawdzającego to ponad 1000 mikrosekund. Podczas wprowadzania ciągu 4000 czas się zwiększa – co może sugerować zweryfikowanie pierwszej cyfry 4 jako poprawnej (bo tylko ona się zmieniła w stosunku do poprzednich czterech zer).



Rysunek 5. *Ścieżki wahań napięcia podczas wprowadzania kodu PIN*



Rysunek 6. *Inspector w akcji*

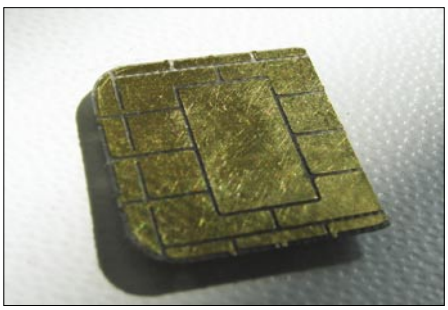
Kolejny wykres po wprowadzeniu ciągu 4500 pokazuje dalsze wydłużenie czasu pracy procesu sprawdzającego do prawie 1200 mikrosekund, co sugeruje, że cyfra 5 również jest poprawna.

Wpisanie ciągu 4560 powoduje dalsze wydłużanie się wykresu procesu, a zatem kolejna cyfra 6 jest właściwa. Z uwagi na to, że prawdopodobnie po trzykrotnym wprowadzeniu błędnego PINu karta zostanie zablokowana, metoda może być skuteczna przy długim okresie zapisywania wprowadzanego właściwego PINu przez użytkownika i analizowaniu zapisów ścieżek oraz porównywania ich z naszymi własnymi próbami wprowadzania PINu.

Do przeprowadzenia ataku SPA nie jest potrzebny specjalistyczny oscyloskop – w zupełności wystarczy prosty, oparty na układzie ADC0820, podłączany do portu równoległego komputera PC. W przypadku bardziej zaawansowanych oscyloskopów będziemy mieli bardziej dokładne zapisy, wykonane z większą częstotliwością. Oprogramowanie do akwizycji, czyli zbierania danych, można znaleźć bez problemu w Internecie. W zupełności wystarcza ono do pierwszych testów bezpieczeństwa kart inteligentnych.

Symulowanie ataków przy użyciu nieskomplikowanych układów elektronicznych i prostych narzędzi programowych pozwala wyciągnąć wnioski na temat łatwości ich dokonania przez potencjalnego intruza.

Firma Riscure oferuje całą gamę programów przydatnych podczas badania poziomu bezpieczeństwa kart inteligentnych. Jednym z ciekawych programów do analizy podczas ataków SPA oraz DPA jest *Inspector*. Jego możliwości pozwalają na jednoczesne wyświetlanie kilku ścieżek, co ułatwia porównywanie przebiegów. Niestety,



Rysunek 7. *Wyłuskane złącze wraz z układem elektronicznym*

program nie jest darmowy, a – co gorsza – nie jest dostępna jego wersja demonstracyjna.

Bezpośredni atak na kartę – jej układ elektroniczny, strukturę danych – choć jest możliwy do przeprowadzenia, to jednak sprzęt potrzebny do jego wykonania dyskwalifikuje domorosłych crackerów. Samo obnażenie układu elektronicznego nastręcza wiele trudności. Wyjęcie układu *podczepionego* pod złącze ISO nie jest specjalnie trudne i spokojnie da się to zrobić bez specjalnych narzędzi.

Dostanie się do *wnętrza* karty poprzez podłączenie się do szyny danych z pominięciem wszelkich zabezpieczeń szyfrujących nie jest już jednak takie proste. Potrzeba do tego celu specjalnego laboratorium z odpowiednim sprzętem – przy wykorzystaniu mikroskopu można wykonać takie podłączenie, co udowodnił niedawno Chris Tarnovsky z Flylogic Engineering. Na szczęście dla bezpieczeństwa kart inteligentnych niewiele jest osób mających dostęp do takiego sprzętu i mogących dokonać tego rodzaju ataku na kartę.

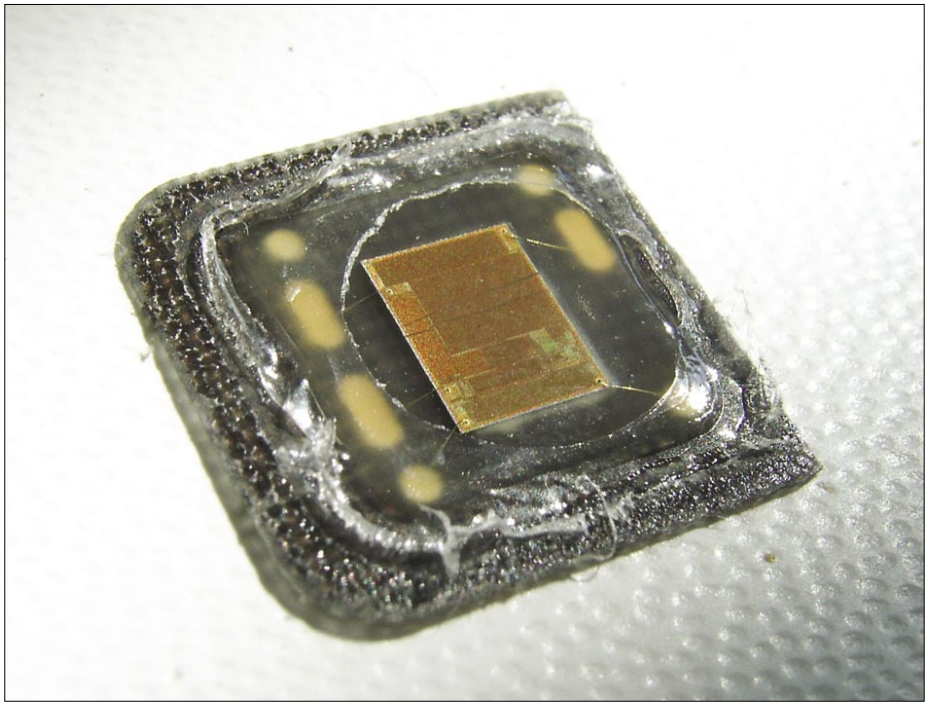
Warto w tym momencie dodać, że aby podobne ataki – naruszające fizyczną strukturę karty – były skuteczne, musiałyby odbywać się w bardzo krótkim czasie, gdyż właściciel karty zauważywszy jej brak zgłosiłby jej zaginięcie. W tym momencie odpowiednie służby mogłyby zablokować możliwość korzystania z tej właśnie karty, co byłoby kompletnym fiaskiem dla crackera.

Firmy produkujące karty chipowe stosują różne zabezpieczenia w swoich produktach, aby minimalizować podatność ich kart na atak.

Miniaturyzacja struktury układu elektronicznego powoduje, że bez odpowiedniego sprzętu laboratoryjnego dostęp do elektroniki jest utrudniony. Niektóre firmy stosują specjalne oprogramowanie, które podczas wykrycia działań mogących sugerować atak powodują blokadę dostępu do danych na karcie, z kasowaniem zawartości pamięci włącznie (STMicroelectronics). Wydaje się , że jednym z bardziej skutecznych ataków (i stosunkowo prostych do zorganizowania) są ataki *man-in-the-middle*, w których atakujący lokuje się na drodze komunikacji pomiędzy kartą a aplikacją w komputerze. Dla każdej ze stron – zarówno dla karty, jak i dla aplikacji – atakujący widoczny jest jako uwierzytelniony element komunikacji, co pozwala na przechwytywanie transmisji i modyfikowanie wysyłanych komend. Najbardziej narażone na tego rodzaju ataki są obecnie czytniki wyposażone w interfejsy szeregowe, równoległe czy USB.

W Sieci

- *http://www.weethet.nl/english/smartcards_types.php,*
- *http://www.devshed.com/c/a/Practices/Smart-Cards-An-Introduction/8,*
- *http://hackedgadgets.com/2008/06/03/smart-card-hacking,*
- *http://www.axalto.com,*
- *http://www.smartcard.ust.hk/security/content.htm,*
- *http://www.cl.cam.ac.uk/~rja14/tamper.html.*



Rysunek 8. *Złącze po odwróceniu kryje pod sobą układ elektroniczny z widocznymi połączeniami układu do styków karty*

Podsumowanie

Zagadnienie bezpieczeństwa kart inteligentnych nie jest łatwe do rozpatrywania, ponieważ bardzo często same karty są składnikiem systemu mającego zapewniać bezpieczeństwo. Użytkownicy bardzo często traktują zabezpieczenie poprzez kartę jako bardzo bezpieczne rozwiązanie, zapewniające stuprocentowe bezpieczeństwo – nie biorąc pod uwagę możliwości ewentualnych ataków na dane znajdujące się na karcie. W przypadku kart GSM ochrona to dwa kody PIN, a jednak bez większego problemu możliwe jest klonowanie takich kart bez posiadania specjalistycznego przygotowania. Niewiele osób zdaje sobie sprawę z faktu, iż nawet najbardziej nowoczesna technologicznie karta, z bardzo szybkim procesorem, zaawansowanymi metodami szyfrowania danych może stać się celem ataku – i całkiem możliwe, że ataku udanego. Rynek kart inteligentnych rozwija się bardzo dynamicznie – coraz więcej producentów stosuje produkty oparte właśnie o tę technologię, często w połączeniu z innymi rozwiązaniami zabezpieczającymi. Jednak nawet do tego typu zabezpieczeń należy podchodzić z odpowiednim dystansem.

Grzegorz Błoński
Grzegorz Błoński, z wykształcenia jest informatykiem, certyfikowanym specjalistą IBM. Pracuje w dużej firmie o zasięgu światowym. Zajmuje się administracją i bezpieczeństwem sieciowym. Jest członkiem organizacji International Information Systems Forensics Association (IISFA), ISACA, ISSA oraz Internet Society.
Kontakt z autorem: *mancymonek@mancymonek.pl*