Grzegorz Wojtenko

Karta mikroprocesorowa i matematyka

gwarantami bezpieczeństwa w e-administracji

Fot. Philippe Ramakers/KOR

Karty mikroprocesorowe (vel inteligentne – od angielskiego terminu *smart cards*) stanowią zwieńczenie osiągnięć technologicznych silnie związanych z aparatem matematycznym. Karty mikroprocesorowe można oferować szerokim rzeszom potencjalnych użytkowników jako narzędzie gwarantujące bezpieczeństwo różnego rodzaju operacji, w tym bankowych i administracyjnych, które jest jednocześnie poręczne i odporne na zakłócenia zewnętrzne.

Czas potrzebny do złamania algorytmu kryptograficznego liczy się w jednostkach MIPS-year odpowiadających liczbie obliczeń wykonanych przez 1 rok z szybkością miliona instrukcji na sekundę.

Karta mikroprocesorowa, popularnie, choć nieprawidłowo zwana też kartą „chipową", jest kawałkiem tworzywa z wbudowanym układem elektronicznym i należy do kategorii układów aktywnych, tzn. mogących nie tylko przechowywać, ale i przetwarzać informacje. Obok kart mikroprocesorowych istnieją także bardzo popularne karty z paskiem magnetycznym i rzadziej karty optyczne, w których dane zapisuje się w sposób analogiczny do zapisu na dyskach CD. Wszystkie wymienione rodzaje kart mają zunifikowane rozmiary określone przez stosowną normę. Warto zaznaczyć, że karty SIM do telefonów komórkowych, choć odbiegają rozmiarami od kart bankowych, także są kartami mikroprocesorowymi. Cechami wyróżniającymi karty mikroprocesorowe od kart magnetycznych jest możliwość przechowywania znacznie więk-

szej ilości danych (prawie o 2 rzędy więcej), zdolność do przetwarzania danych i przede wszystkim nieporównywalnie skuteczniejszy poziom zabezpieczeń, o których będzie mowa dalej.

Karty mikroprocesorowe stanowią, obok kart pamięciowych (także pamięciowych z blokiem bezpieczeństwa), jeden z typów kart elektronicznych. Istnienie mikroprocesora w układzie scalonym karty decyduje o funkcjonalności, a przez to i przeznaczeniu karty. Karta z mikroprocesorem, nadal najczęściej 8-bitowym, jest *de facto* mikrokomputerem. Typowe wartości pamięci karty to: 64 KB pamięci ROM przeznaczonej na system operacyjny, 8 KB RAM i do 2-16 KB pamięci EEPROM, pełniącej rolę twardego dysku. W części rozwiązań, w których wymaga się dużej ilości obliczeń kryptograficznych, kartę wyposaża się dodatkowo w koprocesor kryptograficzny.

Ze względu na sposób komunikacji karty ze środowiskiem zewnętrznym. karty dzieli się na karty stykowe i bezstykowe. Karty bezstykowe znajdują zastosowanie przede wszystkim w transporcie miejskim i systemach kontroli dostępu. **Istnieją też karty dualne, w których w tym samym kawałku tworzywa zatapia się układ stykowy i bezstykowy lub jeden układ stykowo-bezstykowy.** Na rynku dostępne są także karty hybrydowe łączące różne technologie – najczęściej mikroprocesor z paskiem magnetycznym lub mikroprocesor z obszarem pamięci optycznej przeznaczonej do zapisywania dużych ilości danych statycznych, jak np. zdjęcia użytkownika.

Fot. Wincor Nixdorf

Należy pamiętać, iż karta zawsze musi współpracować z aplikacją zewnętrzną (bankomatu, terminala płatniczego, aplikacją na PC itd.), z którą kontaktuje się za pomocą komunikatów ustalonego formatu, poprzez tzw. jednostki APDU zdefiniowane w podstawowej dla kart normie ISO/IEC 7816. Większość kart, zwanych „natywnymi", posiada własny system operacyjny. Coraz silniej jednak obserwuje się trend w kierunku kart programowalnych, takich jak Java Cards czy MULTOS.

Bezpieczeństwo kart mikroprocesorowych tworzy szereg mechanizmów sprzętowych i logicznych. Karty odporne są na ataki typu SDA (*Side Channel Attack*) bazujące na analizie zużycia mocy czy czasu przetwarzania operacji. Karty poddawane są procesom oceny bezpieczeństwa (np. *Common Criteria* czy ITSEC) takim samym jak inne systemy teleinformatyczne i zgodne są z wymaganiami stawianymi modułom bezpieczeństwa a zdefiniowanym w normie FIPS 140-1.

Karty mikroprocesorowe poprzez zaimplementowane algorytmy kryptografii symetrycznej i asymetrycznej umożliwiają realizacje podstawowych usług ochrony informacji – uwierzytelnienie, zapewnienie poufności i integralności danych, niezaprzeczalność. Klucze kryptograficzne, numery PIN lub inne sekrety są w sposób bezpieczny przechowywane na karcie, tzn. że nie istnieje możliwość ich odczytania lub niedozwolonej przez użytkownika modyfikacji.

Siła zabezpieczeń kryptograficznych jest rzeczywiście zadziwiająca, a zrozumienie ich wymaga wyobrażenia na jak dużych liczbach operują algorytmy kryptograficzne (proszę choć jeden raz przeliczyć ile wynosi liczba 2^{160}). Kryptografia bazuje na następującym założeniu:

osoba znająca sekret potrafi wyliczyć poszukiwaną wartość w bardzo krótkim czasie, ale osoba nieznająca tego sekretu będzie musiała wykonać bardzo dużą liczbę obliczeń, aby ten sekret odkryć. Oto prosty przykład: z iloczynu jakich liczb składa się liczba 21? Na to pytanie odpowie dziecko, bo zna tabliczkę mnożenia – skoro 3 x 7 = 21, to 21 = 7 x 3. Problem zacznie się, gdy w pytaniu zamiast 21 pojawi się np. liczba 7754888484848387837737737737737882929088484848848481, nie mówiąc o dłuższych liczbach. Przedstawiony przykład dotyczy tzw. problemu faktoryzacji wykorzystanego w RSA, najbardziej popularnym obecnie algorytmie kryptografii asymetrycznej. Inne powszechnie znane problemy wykorzystywane w kryptografii asymetrycznej to problemy logarytmu dyskretnego, w tym logarytmu dyskretnego na krzywej eliptycznej. Czas potrzebny do złamania algorytmu kryptograficznego liczy się w jednostkach MIPS-year odpowiadających liczbie obliczeń wykonanych przez 1 rok z szybkością miliona instrukcji na sekundę.

e-administracja pozwala na zastąpienie dokumentów papierowych postacią elektroniczną oraz honorowanie podpisu elektronicznego na równi z podpisem składanym odręcznie. Oznacza to duże ułatwienie i przyśpieszenie procedur biurowych ze względu na ich „odmiejscowienie" i automatyzację. Nikogo nie trzeba przekonywać jak wpłynie to na oszczędność czasu (i nerwów…) czy też obniżenie kosztów administracyjnych w dłuższym horyzoncie czasowym. Powszechność rozwiązań elektronicznych uwarunkowana jest bezpieczeństwem ich realizacji, które dają właśnie omawiane karta, jako platforma i tak bliska nam, poprzez różne życiowe doświadczenia, matematyka.