Opracowując programy zadawałem sobie często pytanie: na ile bezpieczny jest mój program wewnątrz mikrokontrolera? W jakim stopniu urządzenie, na którego konstrukcję i rozwój poświęciłem na przykład dwa lata, a którego (w większości przypadków) główną wartością jest program, jest trudne do skopiowania? Na ile pewne jest zabezpieczenie przez ustawienie bitów blokujących dostęp do pamięci programu? Jak skuteczna jest blokada dostępu do pamięci typu Flash przy możliwości jej wielokrotnego zapisu?

Atak na mikrokontrolery

część 1

Od redakcji

Publikując ten artykuł zamierzamy sprowokować dyskusję na temat zabezpieczenia własności intelektualnej. Zachęcamy więc do przysyłania własnych pomysłów „rozkuwania" zabezpieczeń. Nie wszystkie sposoby opisane w artykule są możliwe do natychmiastowego odtworzenia w warunkach typowego laboratorium elektronicznego, ale niektóre nie wymagają praktycznie żadnego wsparcia sprzętowego.

Pewnego razu zadałem tego rodzaju pytanie na liście dyskusyjnej programistów, znajdującej się na stronie *http://www.8052.com*. Odpowiedzi, które uzyskałem lekko mnie zaskoczyły. Była między nimi na przykład sugestia, że jeżeli program do urządzenia, które chcę skopiować, wart jest dla mnie milion dolarów, to taka kwota przesłana do firmy X - notabene producenta między innymi mikrokontrolerów - spowoduje, że udostępni mi ona technologię umożliwiającą odczyt pamięci programu, mimo jej blokady. Na poparcie tej tezy autor przysłał mi artykuł rosyjskiego stypendysty pracującego na Uniwersytecie Cambridge w Wielkiej Brytanii - Sergieja Skorobogatova. Pracuje on w laboratorium komputerowym w grupie pracowników naukowych zajmujących się zabezpieczeniami komputerów osobistych oraz mikrokontrolerów. Grupa ta bada, na ile skuteczne są wszelkiego rodzaju zabezpieczenia programów. Badania te są najczęściej wykonywane na zlecenie firm-producentów sprzętu i oprogramowania.

Jak pisze Sergiej o swojej pracy, polega ona na zrozumieniu, jak zabezpieczenie może zostać złamane i udzieleniu wskazówek producentowi, jak ono powinno być wzmocnione. Badania te, w związku z rosnącym zastosowaniem mikrokontrolerów - na przykład w kartach płatniczych - mają ogromne znaczenie.

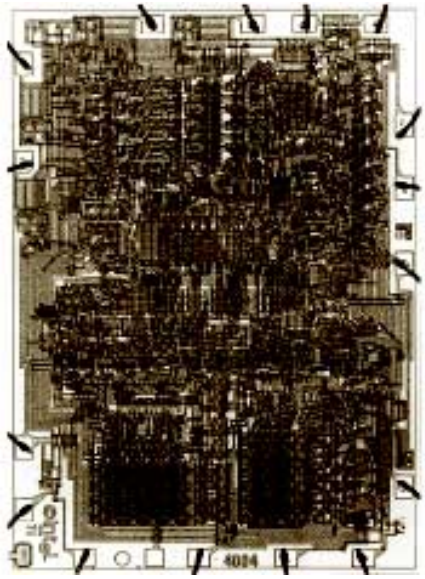
Wprowadzenie

Mikrokontrolery znajdują zastosowania praktycznie we wszystkich nowoczesnych urządzeniach. Często są także używane przez amatorów do budowania niewielkich układów „rozrywkowych", inne używane są przez firmy do budowania urządzeń służących do kontroli, pomiaru itp. Jeszcze inne stosowane są w poważnych aplikacjach przez wojsko, służby bezpieczeństwa, banki, służby medyczne.

Każdy mikrokontroler wykonuje program umieszczony w jego pamięci. Jeśli opracowujesz programy dla mikrokontrolerów, jesteś zainteresowany zabezpieczeniem wyników swojej pracy przed nieautoryzowanym dostępem czy kopiowaniem - chcesz mieć po prostu kontrolę na procesem dystrybucji swojego dzieła. Z taką intencją producenci mikrokontrolerów tworzą specjalne zabezpieczenia, które jeśli są włączone, pozwalają autorowi oprogramowania na zabezpieczenie wyników swojej pracy. To jest tak zwana opcja *copy lock*.

Mikrokontroler trzeba zaprogramować przed jego działaniem w układzie. Są różne sposoby programowania, zależne od producenta i typu mikrokontrolera. Dla przeprowadzania eksperymentów dostępne są mikrokontrolery wielokrotnie programowalne. Do produkcji niewielkiej liczby urządzeń przeznaczone są mikrokontrolery do jednokrotnego zaprogramowania (OTP), które są znacznie tańsze od tych do wielokrotnego użytku. Dla produkcji wielkonakładowej przeznaczone są mikrokontrolery programowane przez producenta w procesie jego produkcji. Tak wytwarzane układy są bardzo tanie, jednak ze względu na koszt wdrożenia tak zwanej maski, przy woluminie poniżej 1000 sztuk nie są opłacalne.

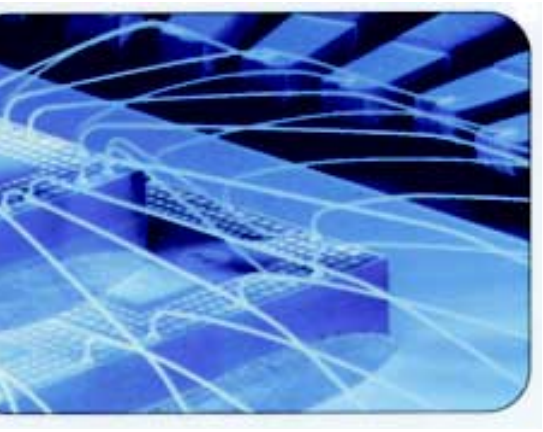
Wróćmy jednak do najczęściej stosowanych mikrokontrolerów, które wyposażone są najczęściej w pamięć EPROM,



EEPROM lub Flash. Po tym, jak program został napisany i skompilowany, powinien być zapisany w pamięci programu mikrokontrolera. Do tego celu są przeznaczone specjalne przyrządy, zwane programatorami. W przypadku większości współczesnych mikrokontrolerów są to przyrządy proste i tanie, zawierające źródło napięcia zasilania, kilka tranzystorów czy układów scalonych i nieco innych elementów elektronicznych. Dla niektórych mikrokontrolerów należy użyć specjalnego programatora rozprowadzanego wyłącznie przez producenta układu, ale te mikrokontrolery nie należą do grupy często stosowanych.

Techniki ataku

Zwiększająca się liczba urządzeń elektronicznych z mikrokontrolerami oraz wzrastająca ich powszechność i znaczenie - od płatnej TV, poprzez telefony komórkowe GSM, systemy zaliczkowych liczników energii elektrycznej i gazu, do portfeli elektronicznych i kart płatniczych - wpływa na wzrost zainteresowania zabezpieczeniem przed możliwością duplikacji funkcji mikrokontrolerów w celu ochrony przed możliwością sfałszowania na przykład kart Smartcard i innych służących dokonywaniu rozliczeń finansowych czy też bezpieczeństwu. Zabezpieczenia te nie są pewne: specjalista z dostępem do urządzeń służących do testowania układów scalonych może odtworzyć dane kluczowe poprzez bezpośrednią obserwację struktury i manipulację elementami mikrokontrolera. Faktem nie do podważenia jest, że przeznaczając na to odpowiednie środki finansowe, każde urządzenie służące zabezpieczeniu przed nieautoryzowanym dostępem do danych zawartych w strukturze mikrokontrolera może być spenetrowane i rozpoznane. Tak więc poziom zabezpieczenia oferowanego przez różnorodne produkty może być określony ilością potrzebnego czasu i pieniędzy koniecznych na spenetrowanie mechanizmów uniemożliwiających atak.



Można rozróżnić cztery zasadnicze metody ataku:

- **Technika mikrosondowania** może być użyta do bezpośredniego dostępu do struktury układu. W ten sposób można obserwować, manipulować i prowadzić interakcję z układami znajdującymi się w strukturze mikrokontrolera.
- **Atak programowy** - używa się normalnego interfejsu do komunikacji z procesorem i wykorzystuje błędy zabezpieczeń odnalezione w protokole komunikacyjnym, algorytmach kryptograficznych lub ich zastosowaniach.
- **Technika „podsłuchiwania"** polega na obserwacji charakterystyk analogowych procesora z bardzo dużą rozdzielczością czasową, wszystkich połączeń zasilających i sygnałów interfejsowych oraz promieniowania elektromagnetycznego podczas normalnej pracy mikrokontrolera.
- **Generowanie stanów awaryjnych**, to technika używająca różnego rodzaju stanów zabronionych (na przykład zbyt niskie lub zbyt wysokie napięcie zasilania, bardzo wolne zmiany zboczy sygnałów zegarowych itp.) do spowodowania błędnej pracy mikrokontrolera i w ten sposób uzyskanie dostępu do danych.

Przeznaczając odpowiednie środki finansowe możemy skopiować konfigurację każdego układu PLD, oprogramowanie mikrokontrolera czy pamięć nieulotną oraz program w niej przechowywany.

Wszystkie techniki związane z mikrosondowaniem są inwazyjne. Wymagają godzin lub tygodni ciężkiej pracy w specjalistycznym laboratorium oraz zniszczenia obudowy mikrokontrolera. Pozostałe techniki są nieinwazyjne. Atakowana karta czy mikrokontroler nie są fizycznie niszczone, a oprzyrządowanie używane w czasie ataku, to czasami zwykły czytnik kart Smartcard, bądź też nieco zmodyfikowany programator.

Atak nieinwazyjny jest dla użytkownika bardzo niebezpieczny z dwóch powodów:

- po pierwsze, właściciel na przykład karty płatniczej, może nie zauważyć, że została ona skradziona, a jej zabezpieczenia złamane - od tego momentu w obiegu może się znajdować na przykład jej duplikat.
- po drugie, urządzenia potrzebne do tak przeprowadzonego złamania zabezpieczeń mogą być tanio i łatwo skopiowane przez inne osoby - może zostać rozwinięta ich funkcjonalność, na skutek czego przeprowadzenie podobnych ataków w przyszłości będzie łatwiejsze i szerzej dostępne.

Głównym problemem przy takiej metodzie ataku jest szczegółowa wiedza na temat procesora i oprogramowania. Z drugiej strony, wiedza potrzebna do przeprowadzenia ataku inwazyjnego nie jest aż tak szczegółowa, wymaga jednak orientacji w zastosowaniu różnych technik dla szerokiej gamy produktów. Atak ten zazwyczaj zaczyna się od odtworzenia struktury układu oraz schematu połączeń poszczególnych jego komponentów. Często rezultatem tak przeprowadzonego szczegółowego rozpoznania jest rozwinięcie metod ataku nieinwazyjnego.

Bezpieczeństwo mikrokontrolera lub karty Smartcard powinno być zapewnione w taki sposób, że tak mała - jak to tylko możliwe - ilość informacji (na przykład poprzez kompresję danych), powinna być możliwa do odtworzenia, gdy konieczne jest jej użycie. Drugim celem jest utrzymanie tej informacji nietkniętej podczas operacji tak, aby potencjalny włamywacz nie miał możliwości zmiany sekretnego kodu - klucza operacji do znanej sobie wartości lub w innym przypadku do interakcji oraz rozpoznania sekretnego algorytmu szyfrowania/deszyfrowania.

Obecnie większość ataków przeprowadzanych przez włamywaczy komputerowych, chcących uzyskać dostęp do danych zawartych w mikrokontrolerze czy Smartcard, można zaklasyfikować do dwóch kategorii - inwazyjne i nieinwazyjne.

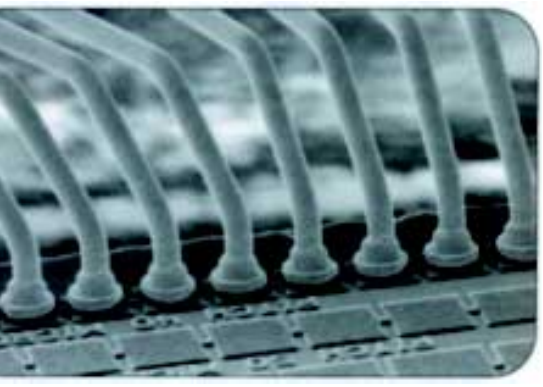
Atak nieinwazyjny

Atak nieinwazyjny odbywa się bez naruszenia struktury mikrokontrolera, czy karty Smart. Przeprowadzany jest najczęściej poprzez rozpoznanie i wszelkiego rodzaju sztuczki związane z napięciem zasilania oraz sygnałem zegarowym. Ataki w stanach, w które wprowadzany jest mikrokontroler obniżeniem lub podwyższeniem napięcia zasilania, mogą zostać użyte, aby wyłączyć obwody zabezpieczeń lub zmusić procesor do wykonania niewłaściwych operacji. Z tego powodu niektóre modele mikrokontrolerów posiadają wbudowane w strukturę układy detekcji poziomu napięcia zasilania, ale w ich działaniu jest brak reakcji na bardzo szybkie zmiany napięcia. Dlatego też szybko zmieniające się i w różny sposób napięcie zasilania jest w stanie doprowadzić do stanu wyłączenia obwodów zabezpieczeń, bez uszkodzenia chronionej informacji.

Zmiany napięcia zasilania i sygnału zegarowego mogą być również użyte w niektórych mikrokontrolerach do spowodowania przyjęcia i wykonania niektórych instrukcji. Każdy bowiem tranzystor i jego połączenie pracują tak, jak element RC z określoną charakterystyką.

Maksymalna częstotliwość zegara procesora określana jest właśnie przez opóźnienie sygnału pomiędzy jego elementami. Podobnie każdy z elementów, takich jak przerzutniki, ma swoje charakterystyczne „okienko sygnałowe" (zazwyczaj kilka pikosekund), w czasie którego „próbkuje" on napięcie wejściowe i odpowiednio zmienia stan swoich wyjść. To „okienko" może być gdzieś wewnątrz specyficznego cyklu dla danego przerzutnika, ale jest stałe dla określonego urządzenia, w określonej temperaturze i przy określonym napięciu zasilania. Tak więc, jeśli zastosujemy sygnał zegarowy krótszy niż normalnie, albo też napięcie zasilania zmieni się w sposób bardzo gwałtowny, to spowoduje zadziałanie tylko niektórych tranzystorów wewnątrz struktury układu mikrokontrolera. Poprzez różnicowanie parametrów napięcia zasilania i sygnału zegarowego, można doprowadzić do sytuacji, gdy procesor wykona szereg kompletnie różnych i błędnych instrukcji, czasami również takich, które nie są dozwolone i obsługiwane w danej strukturze CPU. Chociaż nie wiemy, która zmiana i w jaki sposób wpłynie na działanie mikrokontrolera, to całkiem łatwo można przeprowadzić systematyczne poszukiwania właściwej sekwencji sygnałów.

Inną możliwość daje analiza poboru mocy przez urządzenie. Używając rezystora o wartości 10..15 Ω włączonego szeregowo z napięciem zasilania, można zmierzyć za pomocą przetwornika A/D zmiany prądu pobieranego przez zasilany procesor. Wzmacniacze prądu sygnałów adresowych i szyny danych są często budowane z wielu połączonych ze sobą równolegle inwerterów dla każdego bitu danych czy adresów. Każda zmiana stanu takiego bitu pociąga za sobą znaczny pobór prądu zasilania. Zmiana pojedynczego bitu z 0 na 1 i odwrotnie, pociąga często za sobą wzrost poboru prądu zasilającego o około 0,5 do 1 mA dla zbocza sygnału zegarowego. Tak więc stosując przetwornik A/D o rozdzielczości 12 bitów, można stwierdzić, jaka liczba linii adresowych czy też danych, zmieniła swój stan w danym czasie. Zapis pamięci SRAM zawsze generuje bardzo duży przyrost wartości pobieranego prądu. Poprzez uśrednienie prądu mierzonego dla wielu identycznych transakcji można zidentyfikować sygnały, które nie są przesyłane poprzez szynę danych. Sygnały generowane przez takie operacje, jak ustawienie bitu przeniesienia, są szczególnie interesujące ponieważ są one używane przez wiele algorytmów kryptograficznych. Chociaż zmiany wartości bitów statusu nie mogą być bezpośrednio zmierzone, często powodują one zmiany zawartości licznika rozkazów lub wykonanie instrukcji tak zwanego mikrokodu, które z kolei pociągają za sobą bardzo wyraźne i łatwe do zauważenia zmiany poboru prądu.



Różne instrukcje powodują również różną aktywność dekodera instrukcji i jednostki arytmetyczno - logicznej. Można w ten sposób łatwo zidentyfikować część kodu programu i zrekonstruować algorytm. Podobnie różne elementy procesora powodują charakterystyczne dla siebie zmiany przepływu prądu zasilającego w różnym czasie, odpowiednio do sygnału zegarowego, i ich stan może być rozpoznany poprzez próbkowanie sygnału zasilającego z odpowiednio dużą częstotliwością.

Inną możliwość włamania stwarzają właściwości pamięci RAM - utrzymywanie danych przez pewien czasu po wyłączeniu napięcia zasilania. Statyczna pamięć RAM potrafi nawet (wskutek istnienia pojemności) przechowywać swój stan do momentu następnego załączenia napięcia zasilającego. Możliwe jest również odtworzenia stanu statycznej pamięci RAM przez poddanie jej działaniu bardzo niskiej temperatury (około -20ºC) na czas od kilku minut do kilku godzin.

Atak inwazyjny

Na przekór pozornej złożoności ataku inwazyjnego, niektóre z jego rodzajów mogą być przeprowadzone bez drogiego osprzętu laboratoryjnego. Włamywacze dysponujący małym budżetem mogą korzystać z używanego sprzętu sprzedawanego przez producentów układów scalonych do ich testowania. Dysponując odpowiednią wiedzą oraz uzbrajając się w cierpliwość, nie jest zbyt trudno zdobyć odpowiednie narzędzia za cenę poniżej 10 tysięcy dolarów, kupując używany mikroskop i konstruując własny mikropozycjoner. Laser nie jest niezbędny do pierwszych prób, ponieważ otwory w strukturze półprzewodnikowej mogą być również wykonywane poprzez wibracje igły mikropozycjonera.

Atak inwazyjny zaczyna się najczęściej od zdjęcia obudowy struktury. Plastykowa część obudowy może być zdjęta za pomocą na przykład noża. Izolację epoksydową umieszczoną wokół struktury, można usunąć za pomocą kwasu azotowego. Opary podgrzanego kwasu azotowego mają też właściwość rozpuszczania plastikowej obudowy. Można się więc jej pozbyć bez uszkodzenia struktury układu. Cały proces należy przeprowadzić w warunkach bardzo dużej czystości, z zachowaniem szczególnej ostrożności, najlepiej pod strumieniem bieżącej wody, ponieważ opary mogą spowodować również uszkodzenie aluminiowych doprowadzeń układu. Struktura krzemowa powinna być później umyta w płuczce ultradźwiękowej za pomocą acetonu. Mycie to można poprzedzić krótką kąpielą w wodzie dejonizującej oraz w isopropanolu. Po tym struktura może być przyklejona i podłączona ręcznie do wyprowadzeń pakietu testowego. Metoda ta umożliwia usunięcie izolacji epoksydowej bez uszkodzenia połączeń struktury i jej zewnętrznych wyprowadzeń.

Gdy obudowa układu jest otwarta, możliwe jest przeprowadzenie sondowania lub atak poprzez modyfikację struktury układu. Bardzo ważnym narzędziem do przeprowadzenia ataku inwazyjnego jest tak zwana stacja do mikrosondowania. Jest to po prostu zespół mikrosond, które można podłączać do struktury układu. Jednym z jej głównych elementów jest mikroskop umożliwiający ostry obraz z odległości około 8 mm nad powierzchnią struktury układu. Na stabilnej platformie dookoła złącza pakietu testowego instaluje się kilka mikropozycjonerów, które umożliwiają przesuwanie ramienia sondy z bardzo dużą precyzją nad powierzchnią struktury układu. Na tym ramieniu instaluje się igłę sondy. Wykonana jest ona z elastycznego metalu tak, że umożliwia kontakt z elementami struktury półprzewodnikowej bez ich uszkodzenia.

Oczywiście, przed podłączeniem takiej sondy należy usunąć warstwę pasywującą. Jest to górna warstwa przykrywająca aluminiowe doprowadzenia do struktury układu (zazwyczaj jest to tlenek krzemu). Zabezpiecza ona strukturę układu przed wpływem środowiska oraz migracją jonów. Czasami dodatkowo jest ona pokryta warstwą poliamidów, której nie usuwa kwas azotowy, ale może ona być rozpuszczona przez ethylodiaminę. Inną, trudniejszą w realizacji metodą pozbycia się warstwy pasywującej jest jej usunięcie za pomocą noża laserowego.

Ultrafioletowy lub zielony laser mocowany jest na uchwycie kamery mikroskopu. Jego światło pada na niewielki, prostokątny obszar z bardzo dużą precyzją. Właściwe dozowanie błysków lasera powoduje wypalenie warstwy pasywującej. Dodatkową zaletą tej metody jest możliwość odsłonięcia niewielkiego obszaru i odkrycie w ten sposób poje-

dynczej linii danych lub tranzystora. Zabezpiecza to resztę struktury przed przypadkowymi zwarciami do sąsiednich linii, a wykonany dodatkowo otwór stabilizuje pozycję sondy i czyni kontakt mniej wrażliwym na wibracje i zmiany temperatury. W ostateczności warstwę pasywującą można usunąć miejscowo poprzez zarysowanie, wiercenie lub nacięcie. Pamiętajmy jednak, że te operacje odbywają się w mikroskali! Jednak dopiero usunięcie warstwy pasywującej gwarantuje, że sonda będzie miała dobry kontakt ze strukturą układu.

Oczywiście nie jest praktykowane odtwarzanie wartości klucza kryptograficznego poprzez kontakt sondy do poszczególnych komórek pamięci i odczyty stanów bitu. Zapamiętane dane mogą zostać odczytane poprzez szynę danych pamięci w miejscu, w którym wszystkie dane są dostępne w pojedynczej lokalizacji. Mikrosondowanie jest używane do obserwowania stanów szyn i ich rejestracji. Jest jednak bardzo trudno obserwować szyny danych i adresową w całości. Wymaga to wykonania zazwyczaj ponad 20 połączeń do maleńkiej struktury układu, co nie jest łatwe. Stosowane są więc różne techniki obserwacji. Można na przykład wielokrotnie wykonać tę samą transakcję obserwując różne kombinacje bitów na szynie danych i adresowej, wykorzystując na przykład cztery sondy. Tak długo, jak procesor wykonuje tę samą sekwencję dostępu do danych w pamięci, mamy możliwość połączenia obserwowanych przebiegów w kompletny diagram zależności czasowych oraz informacji pojawiających się na szynach.

W przypadku gdy chcemy odczytać wszystkie komórki pamięci bez uruchamiania oprogramowania mikrokontrolera, musimy uzyskać dostęp do komponentów procesora, takich jak licznik programu. Zawartość licznika rozkazów jest automatycznie zwiększana podczas każdego cyklu rozkazowego i jest on używany do odczytu następnego adresu, co powoduje, że doskonale nadaje się do wykorzystania jako generator sekwencyjny sygnałów adresowych. Musimy tylko zabezpieczyć procesor przed wykonywaniem skoków, wywołań podprogramów oraz instrukcji powrotów, które przeszkadzają w sekwencyjnej pracy licznika programu. Niewielkie modyfikacje dekodera instrukcji lub licznika programu, które mogą być łatwo wykonane przez rozwarcie odpowiedniego połączenia za pomocą lasera zawsze przynoszą pożądany efekt.

Inną metodą poznania działania danego układu jest tak zwany *reverse engineering*, to znaczy odtworzenie schematu struktury układu na podstawie jego topografii i analizy budowy poszczególnych elementów. Pierwszym krokiem jest wówczas stworzenie mapy elementów procesora. Może to być zrobione przy użyciu mikroskopu optycznego z podłączoną kamerą CCD umożliwiającą wykonywanie zdjęć struktury procesora z dużą rozdzielczością. Proste elementy architektury, takie jak linie adresowe czy danych, mogą być rozpoznane całkiem szybko, bez studiowania mozaiki połączeń, za pomocą śledzenia przebiegu metalowych linii, które zakreślają bardzo widocznie komponenty struktury układu (ROM, RAM, EEPROM, ALU, dekoder instrukcji itd.). Wszystkie współpracujące ze sobą moduły są zazwyczaj podłączone do głównych szyn za pomocą łatwo rozpoznawalnych przerzutników typu latch oraz wzmacniaczy prądowych. Włamywacz musi dobrze znać technologię wykonania układów CMOS i architektury mikrokontrolerów, ale potrzebne do tego celu infromacje znajdują się w praktycznie każdej bibliotece akademickiej.

Ataki inwazyjne są skomplikowane. Wymagają wielu godzin pracy, specjalistycznego laboratorium, wysoko kwalifikowanych specjalistów oraz dużych nakładów finansowych.

Fotografie uzyskane po pierwszym etapie obserwacji strawienia powierzchni struktury ukazują górną warstwę metalu, która nie jest przeźroczysta i dlatego też zasłania widok wielu struktur znajdujących się pod nią. Strukturę układu można co prawda rozpoznać po jej wysokości, jednak nie jest to metoda zbyt dokładna. Głębsze warstwy mogą być rozpoznane tylko w drugiej serii fotografii, po zdjęciu górnej warstwy metalu, co może być wykonane na przykład przez jej wytrawienie - zanurzenie na kilka sekund w kwasie hydrofluorowym (HF) w płuczce ultradźwiękowej. HF bardzo szybko rozpuszcza tlenek krzemu dookoła metalowych połączeń i odłącza je od powierzchni układu.

Większość z aktualnie dostępnych mikrokontrolerów i procesorów Smartcard ma rozmiar pojedynczego elementu na poziomie 0,5 do 1 µm i tylko dwie warstwy. Mogą one być rozpoznane za pomocą mikroskopu i poprzednio opisywanych technik. Do podglądania układów o większej liczbie warstw, z elementami o rozmiarach mniejszych niż długość fali światła widzialnego, trzeba stosować znacznie droższe narzędzia.

Większość wyrafinowanych narzędzi używanych na przykład w laboratoriach fizyki, takich jak stacje FIB, mogą zostać użyte do wykonania nowych linii połączeń, a nawet nowych tranzystorów w strukturze układu! Stacja FIB zawiera komorę próżniową z rodzajem wyrzutni, porównywalnej z używaną w mikroskopie elektronowym. Jony są przyspieszane napięciem około 30 kV i skupiane w wiązkę o średnicy 5...10 nm i prądzie strumienia od 1 pA do 10 nA. Poprzez zwiększanie prądu strumienia jonów materiał krzemowy może zostać usunięty z rozdzielczością 5 nm. Lepszą rozdzielczość można uzyskać w otoczeniu gazu. Stosując gaz można wykonywać otwory około 12 razy głębsze niż szersze i w ten sposób uzyskiwać dostęp do znajdujących się pod spodem warstw metalu. Stosując gaz, tak zwany organometaliczny z zawartością platyny, można tworzyć nowe pola kontaktowe, natomiast stosując inne dodatki można powstały w ten sposób kontakt zabezpieczyć przed zwarciem z otaczającymi go warstwami. Wprawny operator FIB, posługując się dodatkowo przyrządami laserowymi, może nawigować po powierzchni struktury z rozdzielczością nawet 0,15 µm. Jest to dużo poniżej rozmiaru pojedynczego elementu struktury. Można również zdjąć warstwę podłoża struktury przez jej zeszlifowanie. Wówczas staje się możliwe nawet lokalizowanie pojedynczych tranzystorów i wykonywanie pomiędzy nimi połączeń. Ta „odtylna“ technika nie jest wprawdzie jeszcze stosowana przez włamywaczy, ale technologia i urządzenia stają się coraz bardziej dostępne i kto wie, co przyniesie przyszłość. Obecnie większość zastosowań stacji FIB zmierza do wykonywania dostępu do interesujących połączeń. Otwór wykonywany jest dla danej ścieżki sygnałowej, następnie jest wypełniany platyną tak, aby wyprowadzić sygnał na powierzchnię struktury, gdzie łatwy już jest dostęp do niego za pomocą sondy.

Nowoczesne stacje FIB kosztują nieco mniej niż pół miliona dolarów i są dostępne w więcej niż setce organizacji. Mogą one być wynajęte od niektórych z nich za cenę kilkuset dolarów za godzinę pracy urządzenia.

Wszystkie ataki inwazyjne są skomplikowane. Wymagają wielu godzin pracy specjalistycznego laboratorium i nie mogą się odbyć bez wiedzy właściciela badanego urządzenia - niszczą bowiem jego obudowę oraz czasami strukturę. Dodatkowo wymagają wysoko kwalifikowanych specjalistów oraz dużych nakładów finansowych. Oczywiście nie czyni to ich niemożliwymi do przeprowadzenia...

Sergiej Skorobogatov
Opracował Jacek Bogusz,
jacek.bogusz@ep.com.pl