W drugiej części artykułu przedstawiamy dwa kolejne rodzaje ataków na zabezpieczenia stosowane w mikrokontrolerach - semi-inwazyjny oraz nieinwazyjny. Za miesiąc, w ostatniej części artykułu, pokażemy, w jaki sposób autor artykułu poradził sobie z mikrokontrolerem z rodziny PIC12.

Atak na mikrokontrolery

część 2

Atak semi-inwazyjny

Istnieje jeszcze trzeci, możliwy do przeprowadzenia atak nazywany włamaniem semi-inwazyjnym. Na czym ono polega? Tak jak atak inwazyjny, wymaga zdjęcia obudowy struktury mikrokontrolera, ponieważ konieczny jest dostęp do struktury układu. Warstwa pasywacyjna struktury pozostawiana jest nietkniętą, ponieważ metoda semi-inwazyjna nie wymaga depasywacji lub tworzenia kontaktów do wewnętrznych linii połączeniowych. Dzieje się tak dlatego, że do przeprowadzenia tego rodzaju ataku nie są konieczne mikrosondy. Atak semi-inwazyjny może być przeprowadzony za pomocą takich środków jak światło UV, promieniowanie X i innych rodzajów promieniowania jonizującego, laserów i pól elektromagnetycznych. Mogą one być używane indywidualnie lub w połączeniu, współpracując ze sobą i wzmacniając efekt.

W porównaniu do włamania nieinwazyjnego, atak semi-inwazyjny jest trudniejszy do przeprowadzenia, ponieważ wymaga zdjęcia obudowy układu. Nie jest jednak wymagany tak drogi osprzęt, jak do przeprowadzenia metody inwazyjnej. Dodatkowym atutem jest to, że może on być przeprowadzony w odpowiednio krótkim czasie.

Tab. 1. Różnice pomiędzy różnymi rodzajami pamięci i ich wpływ na bezpieczeństwo

Typ pamięci programu	Metoda programowania	Możliwość zmiany kodu programu	Czas dostępu do pamięci (szybkość rdzenia CPU)	Szybkość programowania/czas do skasowania	Czas przechowywania danych
Mask ROM	przez producenta	brak	10ns (100MHz)	2...4 tygodnie/ brak możliwości	nieograniczony
OTP ROM (do jednokrotnego programowania)	programator	brak	100ns (10MHz)	50 słów na s/ brak możliwości	10 lat
EPROM	programator lub programowanie *in-circuit*	do 100 razy	100ns (10MHz)	50 słów na s/ 10...30 minut	10 lat
EEPROM	programator lub programowanie *in-circuit*	do 10000 razy	200ns (5MHz)	100 słów na s/ 10ms	40 lat
FLASH EPROM	programator programowanie *in-circuit*	do 100000 razy	100ns (10MHz)	500 słów na s/ 5 ms	100 lat
Ferroelectric RAM	programator lub programowanie *in-circuit*	do 10^{12} razy	200ns (5MHz)	2MB na s/ nie jest konieczne	40 lat
Static RAM	programowanie *in-circuit*	nieograniczone	20ns (50MHz)	20MB na s/ nie jest konieczne	5 lat (czas zasilania bateryjnego)

Przegląd mikrokontrolerów

Podzielmy mikrokontrolery na dwie grupy: zwyczajną i „bezpieczną". Mikrokontrolery „bezpieczne" przeznaczone są do aplikacji militarnych, bankowości, zastosowań medycznych itp. i używane przeważnie w formie *smartcard* lub modułach bezpiecznych. Zapewniają różne tryby pracy, różne poziomy dostępu, szyfrowanie danych nie tylko tych używanych do komunikacji z otoczeniem, ale również do komunikacji wewnątrz struktury samego układu. Rozpoznanie takiego układu wymaga specjalistycznego i bardzo drogiego osprzętu, wysokiego poziomu umiejętności i powinno być dyskutowane na osobności.

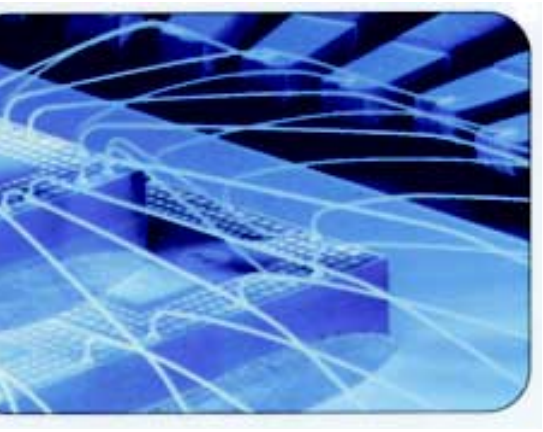
Popularne mikrokontrolery jako zasadę również mają zabezpieczenie przed odczytem programu i/lub danych, ale programiści powinni być ostrożni, ponieważ czasami te zabezpieczenia są

bardzo słabe. Przed dyskusją na temat możliwości włamań do popularnego mikrokontrolera lepiej będzie podzielić je na różne klasy w zależności od typu pamięci programu. W **tab. 1** pokazano różnice pomiędzy różnymi rodzajami pamięci, jak również zalety i słabości każdego z nich.

Jak już poprzednio wspomniano, są dwie główne metody włamań: inwazyjna i nieinwazyjna. Pierwsza z nich polega na wyjęciu struktury z obudowy, wystawieniu jej części na działania promieni lasera lub wiązki jonów. Wymaga również zastosowania specjalnych sond oraz mikroskopu. Atak nieinwazyjny to najczęściej manipulowanie sygnałami zegarowymi oraz napięciem zasilania w celu pozyskania określonej informacji.

Jeśli mikrokontroler ma pamięć typu *Mask ROM*, wówczas z zasady jakikolwiek dostęp do pamięci programu jest zabroniony już na etapie wytwarzania układu. Jednak istnieje pewna metoda dostępu do pamięci, ponieważ do kodu programu często dołączany jest program monitora, umożliwiający dostęp do pamięci programu tak, aby była możliwa weryfikacja poprawności jej zapisu. Generalnie bardzo trudno jest znaleźć ten program i metodę jego uruchomienia, toteż najszybszą drogą okazuje się otwarcie układu i odczyt pamięci programu optycznie. Czasami, aby zwiększyć bezpieczeństwo, producenci używają w obrębie tej samej struktury tranzystorów o różnym progu załączenia zamiast obecności lub nieobecności tranzystora w komórce pamięci, w celu utworzenia bitu o stanie „0“ lub „1“. Taki rodzaj pamięci ROM nie może być odczytany optycznie. W tym przypadku zawartość pamięci może być odtworzona przy pomocy techniki mikrosondowania lub przy użyciu selektywnych rozpuszczalników chemicznych.

Jeśli mikrokontroler wyposażony jest w pamięć OTP ROM, użytkownik końcowy może wybrać ustawienie zabezpieczenia programu podczas procesu programowania. Jednak nawet pomimo włączenia zabezpieczeń, nadal możliwe jest użycie zarówno techniki inwazyjnej, jak i nieinwazyjnej. Przy ataku inwazyjnym z zasady stosuje się światło UV, wystawiając niektóre obszary struktury układu na jego działanie. Inną metodą jest odcięcie linii zabezpieczających przy pomocy lasera albo też odtworzenie stanu bezpieczników (*security fuses*) na stacji do testowania struktur mikrokontrolerów, bądź też proste doprowadzenie sygnałów poza bezpiecznikiem. Atak nieinwazyjny przebiega w klasyczny sposób (manipulowanie napięciem zasilającym i sygnałami zegarowymi) do momentu aż wewnętrzne obwody zabezpieczeń „zapomną“ o zabezpieczeniu. Podobnie jest w przypadku mikrokontrolerów z pamięcią EPROM, ponieważ ma ona tę samą budowę - różnica polega tylko i wyłącznie na umieszczeniu okienka przepuszczającego światło UV w obudowie układu scalonego, bezpośrednio nad strukturą półprzewodnikową.



Pamięć EEPROM jest bardziej odporna na atak inwazyjny. Znacznie trudniej jest postępować z ładunkami elektrycznymi niż z tranzystorami. Jednak te same rodzaje ataku, co dla mikrokontrolera z pamięcią OTP, nadal mogą być zastosowane. Nadal jest możliwe próbkowanie linii danych i adresowych wewnątrz układu, chociaż wymaga to bardzo wysokich umiejętności. Niestety - do tego samego rodzaju pamięci atak nieinwazyjny może być zastosowany bardzo łatwo. Dzieje się tak dlatego, ponieważ komórki pamięci EEPROM zachowują się w bardzo specyficzny sposób i są bardzo czułe na sygnały sterujące oraz zależności czasowe pomiędzy tymi sygnałami. To pozwala włamywaczowi łatwo znaleźć sposób obejścia systemu zabezpieczeń na przykład przez wyzerowanie bitów blokujących dostęp lub spowodowanie, że obwód kontroli zabezpieczeń otrzyma błędne dane na temat stanu bezpieczników. Sytuacja ta powtarza się również w przypadku użycia pamięci typu Flash. Czasami zabezpieczenia tego typu mikrokontrolerów mogą być bardzo łatwo złamane, czasami jest to trudniejsze, ale sytuacja jest nadal zła. Tak więc są sposoby na złamanie zabezpieczenia układu mikrokontrolera używającego pamięci EEPROM lub Flash.

W przypadku mikrokontrolera z pamięcią FRAM wydaje się być nieco lepiej, jednak nadal można użyć metody inwazyjnej i mikrosond, aby odczytać zawartość pamięci.

Najbardziej odporne na ataki są mikrokontrolery używające pamięci RAM jako pamięci programu. Dzieje się tak dlatego, ponieważ jakakolwiek próba włamania kończy się odłączeniem napięcia zasilania i utratą danych. Podobnie jest w przypadku stosowania typowych metod nieinwazyjnych - zawartość pamięci programu ulega najczęściej uszkodzeniu. Ale z powodu błędów w konstrukcji mikrokontrolerów oraz ich oprogramowaniu, również i tu możliwy jest odczyt danych. Jako przykład posłużyć może obejście zabezpieczenia produkowanego przez firmę Dallas Semiconductor mikrokontrolera z grupy „bezpiecznej“ DS5002FP.

Najważniejsze jednak jest zabezpieczenie danych przed metodą nieinwazyjną, ponieważ generalnie jest ona tańsza i łatwiejsza do wykonania niż inwazyjna. Jeśli możesz napisać program lub kupić legalnie zaprogramowany mikrokontroler, będzie to tańsze niż wszelkie metody inwazyjne. Jednak niektóre metody ataku inwazyjnego mogą być bardzo tanie. Dzieje się tak dla przykładu wówczas, gdy bity bezpieczeństwa mogą być skasowane za pomocą światła UV. Tak więc konstruując urządzenie z zastosowaniem mikrokontrolera, powinieneś wybrać ten, który we właściwy sposób zabezpieczy twoją pracę. Nie jest możliwe wytworzenie idealnego zabezpieczenia, ale możesz uczynić odczyt programu w twoim urządzeniu na tyle trudny, że nieopłacalny finansowo.

Nieinwazyjne metody ataku dla mikrokontrolerów popularnych

Kilka słów o sprzęcie używanym do testowania zabezpieczeń mikrokontrolerów. Najważniejszą jego częścią jest specjalny programator, którego konstrukcja i elementy umożliwiają gwałtowne zmiany napięcia zasilania oraz napięć sygnałów wejściowych w szerokim zakresie. Blok sygnałowy programatora generuje 32 sygnały cyfrowe o zmiennych poziomach logicznych - niektóre z nich są typu *open drain*. Blok wejściowy posiada 16 wejść cyfrowych o właściwych, stałych poziomach logicznych. To jest całkowicie wystarczające dla większości mikrokontrolerów. Innymi elementami są płytki adapterów z gniazdami dla różnych typów mikrokontrolerów.

Przykład budowy takiego programatora przedstawiony jest na **fot. 1**. Osobną kwestią jest program służący do kontrolowania jego funkcji. Dla przedstawionego na fotografii urządzenia był to program napisany w języku C dla komputera PC.

W **tab. 2** zestawiono wyniki prób przeprowadzone dla różnych modeli mikrokontrolerów. Nazwa mikrokontrolera umieszczona w nawiasie oznacza, że nie był on testowany, jednak spodziewane jest podobne zachowanie, jak w przypadku pozostałych modeli z tej

Tab. 2.

Mikrokontroler	Wyposażenie	Metoda ataku	Uwagi
Motorola HC05 MC68HC05B6 MC68HC05B8 MC68HC05B16 (MC68HC05B32) (MC68HC05X4) MC68HC05X16 MC68HC05X32	Mask ROM, EEPROM, ustawiany bit bezpieczeństwa typu EEPROM	Zmiany napięcia zasilania lub zmiany sygnału zegarowego	Ma zabezpieczenie przed zapisem przeciwko przypadkowemu skasowaniu pamięci danych
Motorola HC11 MC68HC11A8 MC68HC11E9 (MC68HC11E20) MC68HC11L6 (MC68HC11KA2) (MC68HC11KA4) (MC68HC11KG2) (MC68HC11KG4)	Mask ROM, EEPROM, ustawiany bit bezpieczeństwa typu EEPROM	Zmiana napięcia zasilania	Bootloader z autokasowaniem pamięci danych, jeśli bit bezpieczeństwa jest ustawiony
Microchip PIC PIC16C84	Pamięć programu w EEPROM, EEPROM do zapisu danych, bit bezpieczeństwa typu EEPROM	Przekroczenie napięcia zasilania lub jego zmiany	Tryb Chip Erase kasuje jednocześnie bit zabezpieczenia wraz z programem i pamięcią danych
Microchip PIC PIC16F83 PIC16F84 HCS512	Pamięć programu w FLASH EPROM, EEPROM do zapisu danych, bit bezpieczeństwa typu EEPROM	Zmiany napięcia zasilania	Tryb Chip Erase kasuje jednocześnie bit zabezpieczenia wraz z programem i pamięcią danych
Microchip PIC PIC16F84A PIC16F627 PIC16F628 (PIC16F870) (PIC16F871) (PIC16F872) PIC16F873 PIC16F874 PIC16F876 PIC16F877	Pamięć programu w FLASH EPROM, EEPROM do zapisu danych, bit bezpieczeństwa typu EEPROM	Zmiany napięcia zasilania	Tryb Chip Erase kasuje jednocześnie bit zabezpieczenia wraz z programem i pamięcią danych. Ma wzmocniony mechanizm ochrony
Atmel 8051 AT89C51 AT89C52 AT89C55 AT89C1051 AT89C2051 (AT89C4051)	Pamięć programu w FLASH EPROM, bit bezpieczeństwa typu EEPROM	Zmiany napięcia zasilania	Tryb Chip Erase kasuje jednocześnie bit zabezpieczenia wraz z programem
Atmel AVR AT90S1200 AT90S2313 AT90S2323 (AT90S2343) AT90S8515	Pamięć programu w FLASH EPROM, EEPROM do zapisu danych, bit bezpieczeństwa typu EEPROM	Zmiany napięcia zasilania	Tryb Chip Erase kasuje jednocześnie bit zabezpieczenia wraz z programem i pamięcią danych
NEC 78K/0S (µPD78F9026) (µPD78F9046) µPD78F9116 (µPD78F9136)	Pamięć programu typu FLASH EPROM, brak funkcji odczytu pamięci	Zmiany napięcia zasilania	Tryb Chip Erase kasuje pamięć programu
Texas Instruments MSP430 MSP430F110 MSP430F112 MSP430F1101 MSP430F1121 MSP430F122 MSP430F123 MSP430F133 MSP430F135 MSP430F147 MSP430F148 MSP430F149 MSP430F412 MSP430F413	Pamięć programu w FLASH EPROM, EEPROM do zapisu danych, programowalne hasło dostępu do pamięci (typu EEPROM)	Zmiany sygnału zegarowego	Tryb Mass Erase kasuje hasło wraz z pamięcią programu i danych

Nazwa mikrokontrolera umieszczona w nawiasie oznacza, że nie był on testowany, jednak spodziewane jest podobne zachowanie, jak w przypadku pozostałych modeli z tej grupy.

grupy. Oczywiście obecność mikrokontrolera w tabeli nie oznacza, że nowe wersje tego produktu nie mają usuniętej wady systemu zabezpieczeń.

Dla niektórych z modeli mikrokontrolerów możliwe jest użycie kilku metod ominięcia zabezpieczeń. Dla niektórych z nich wyniki są powtarzalne, dla innych mniej niż 20% testów zakończyło się powodzeniem. Użycie większości z metod publikowanych w Internecie kończyło się zazwyczaj spaleniem nie tylko samego układu mikrokontrolera, ale również uszkodzeniem programatora.

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