Panuje powszechne przekonanie, że atak inwazyjny jest bardzo skomplikowany i wymaga specjalistycznych przyrządów. Oczywiście - włamanie metodą inwazyjną jest kosztowne, wymaga wyposażenia na przykład w różnego rodzaju odczynniki chemiczne, jednak czasami może być zrobione stosunkowo łatwo.

Atak na mikrokontrolery

część 3

Niektóre z modeli mikrokontrolerów są bardzo odporne na próby włamania nieinwazyjnego, jednak zupełnie bezbronne wobec metod inwazyjnych. Podany przykład zrywa z mitem, że włamanie metodą inwazyjną musi kosztować tysiące dolarów. Przytaczam go w celu ostrzeżenia konstruktorów urządzeń elektronicznych i pokazania, co może się zdarzyć. Oto przykład złamania zabezpieczeń mikrokontrolera PIC12C508 właśnie metodą inwazyjną, po lekturze którego każdy sam będzie mógł wyliczyć sobie spodziewany koszt przeprowadzenia włamania i wysnuć wnioski.

Po pierwsze trzeba zdjąć obudowę struktury. Może to być zrobione dwoma metodami: rozpuszczenie wszystkiego wokoło struktury (np. w oparach kwasu azotowego), albo poprzez usunięcie plastyku tylko znad struktury przy pomocy narzędzi mechanicznych (**fot. 1**). W tym drugim przypadku trzeba to zrobić bardzo ostrożnie. Drugi sposób ma też tę zaletę, że struktura układu pozostaje zamocowana i przytwierdzona do podłoża - nie wymaga przeniesienia na płytkę adaptera i wykonania połączeń struktury do doprowadzeń.

Jednak prawdopodobnie łatwiejsze do wykonania, będzie rozpuszczenie plastyku wokoło struktury. Przyjrzyjmy się więc temu sposobowi.

Jak już wcześniej wspomniano, można to zrobić przy pomocy oparów podgrzanego kwasu azotowego. Opary te rozpuszczą plastyk obudowy, nie naruszając połączeń struktury i wyprowadzeń. Nalot powstały w czasie rozpuszczania obudowy, jak również resztki oparów, można usunąć zanurzając strukturę np. w acetonie. Czystą strukturę przemywamy wodą i suszymy.

Jeśli z jakiś powodów nie jesteśmy w stanie tego zrobić, można tę czynność pominąć. Co prawda na strukturze pozostanie nalot, jednak przepuszcza on promieniowanie UV, które użyte będzie w tym przykładzie.

Następnie ostrożnie przenosimy strukturę na płytkę adaptera (**fot. 2**), mocujemy ją za pomocą np. kropelki kleju, odcinamy oryginalne doprowadzenia i łączymy strukturę z naszą płytką testową.

Kolejnym krokiem będzie wystawienie tak zwanych bezpieczników na działanie światła UV. Aby to zrobić, należy odnaleźć miejsce w strukturze, gdzie są one umieszczone. Jeśli dysponujemy mikroskopem o powiększeniu 100x lub więcej, nie będzie z tym większego problemu. Trzeba po prostu prześledzić drogę ścieżki, od wyprowadzenia układu, na które podawane jest napięcie programujące. Po ich odnalezieniu, osłaniamy pamięć programu, na przykład za pomocą kawałka papieru pakowego, a resztę struktury oświetlamy światłem UV przez okres około 5 minut. Bezpieczniki zostają „naprawione“, pamięć programu można odczytać przy pomocy zwykłego programatora...

Jeśli nie mamy mikroskopu, możemy również osłaniać część struktury, oświetlać światłem UV i obserwować rezultat. Oczywiście w ten sposób, można doprowadzić do utraty zawartości pamięci programu.

Groźby ataku i metody obrony

Teraz, mając informacje na temat różnych metod ataku, możemy domniemywać jakie są potencjalne zagrożenia dla urządzeń budowanych przy użyciu mikrokontrolera:

- Atak nieinwazyjny jest bardzo dużym zagrożeniem i jeśli mikrokontroler podatny jest na takie metody ataku ma on minimalny poziom zabezpieczeń. Jedynym wyposażeniem, które będzie potrzebne potencjalnemu piratowi, jest specjalny programator. Można go kupić na przykład za pośrednictwem Internetu.
- Tanie ataki inwazyjne to naprawdę duży problem dla konstruktorów. Taki atak może być przeprowadzony praktycznie przez każdą osobę

Fot. 1

Przykład ataku inwazyjnego na mikrokontroler PIC12C508

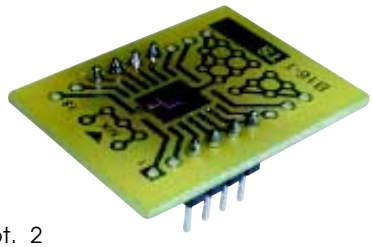
z podstawową wiedzą z zakresu chemii. Cały potrzebny osprzęt można kupić za 100 do 300 dolarów. Mikrokontrolery podatne na ten rodzaj ataku nie są wystarczająco bezpieczne.

- Atak inwazyjny za pomocą mikrosond, może być przeprowadzony tylko przez bardzo zasobnego finansowo fachowca. Powoduje to, że mikrokontrolery podatne tylko na tego typu ataki, są bezpieczne. Zawsze jednak powinieneś skalkulować pieniądze potrzebne na wynajęcie, czy też zakup sprzętu, dodać do tego czas potrzebny na rozpoznanie zagadnienia i złamanie zabezpieczeń. Z całą pewnością nie otrzymasz w ten sposób kwoty tysiąca dolarów, jednak musisz brać to pod uwagę i nie możesz używać mikrokontrolerów podatnych na tego rodzaju atak w bardzo drogich projektach, gdy bezpieczeństwo danych jest niezbędne.
- Odtwarzanie mapy połączeń struktury układu scalonego (*reverse engineering*)jest najdroższą z możliwych metod ataku. Daje ono jednak wszystkie potrzebne informacje na temat schematu układu scalonego oraz struktury i metod zabezpieczeń. Zajmuje jednak bardzo dużo czasu i wymaga dużych nakładów finansowych. Łatwo stać się jednak może przyczynkiem do opracowania metod ataku nieinwazyjnego.

Tak więc jeśli zabezpieczeń mikrokontrolera nie da się obejść w żaden z powyższych sposobów, jest on dobrze zabezpieczony. Aczkolwiek może to być tylko błąd jednego z włamywaczy, z który dostrzeże ktoś następny i poradzi sobie ze złamaniem zabezpieczeń bez większego problemu.

Teraz mamy już chyba świadomość, że praktycznie każdy z popularnie używanych mikrokontrolerów można odbezpieczyć używając którejś z powyższych metod. Zazwyczaj nie jest możliwe ponowne zaprojektowanie struktury układu mikrokontrolera z powodu tylko jego zabezpieczeń. Wiąże się to bowiem z bardzo dużymi kosztami wdrożenia nowego układu do produkcji oraz z tym, że nie będzie zachowana kompatybilność z wcześniejszymi jego wersjami.

Zazwyczaj mikrokontrolery „bezpieczne“ konstruowane są dla potrzeb kart *Smartcard*, gdzie dostępne są tylko dwa wyprowadzenia interfejsu szeregowego. Oczywiście, możesz użyć „bezpiecznego“ mikrokontrolera aby chronić swój projekt, jednak jeśli włamywacz zainteresowany będzie tylko tą częścią algorytmu zaimplementowanego w typowym mikrokontrolerze, może go zdobyć bez kłopotu.



Fot. 2

Innym rozwiązaniem jest używanie zabezpieczeń sprzętowych zbudowanych na bazie programowanych układów logicznych (PAL, CPLD, EPLD itp.), które zazwyczaj oferują lepszy stopień ochrony niż standardowe mikrokontrolery. Nawet jeśli uda się włamać i odtworzyć ich kod, sporo czasu spędzi potencjalny włamywacz, zanim zrozumie jak to zabezpieczenie działa. Można również użyć pewnych nieudokumentowanych cech mikrokontrolerów. Jeśli używasz mikrokontrolerów z pamięcią OTP, EPROM, EEPROM czy Flash, możliwe jest użycie szeregu komórek pamięci dla zabezpieczenia. Na czym polega idea? Wszystkie te rodzaje pamięci są pamięciami analogowymi, to oznacza, że każda komórka wewnątrz obszaru przechowuje ładunek zamiast stanu logicznego. Gdy dokonywany jest odczyt pamięci, ładunek elektryczny z odpowiedniej komórki zamieniany jest na wartość 0 lub 1 poprzez komparator. Jeśli zmienisz wartość ładunku komórki pamięci do poziomu będącego na progu zadziałania komparatora, ze względu na obecność zakłóceń wewnątrz struktury mikrokontrolera, za każdym razem otrzymasz inną wartość odczytując daną komórkę pamięci. Ta właściwość może zostać użyta jako dodatkowe zabezpieczenie wraz z normalnymi mechanizmami zabezpieczenia mikrokontrolera.

Inną możliwym sposobem zwiększenia poziomu bezpieczeństwa danych jest zniszczenie możliwości ponownego programowania. Może to być zrobione poprzez mechaniczne odcięcie określonych wyprowadzeń albo też poprzez przyłożenie do jednego z nich wysokiego napięcia tak, aby wewnętrzne połączenie uległo przepaleniu. Jednak takie działanie nie zapewnia ochrony przed atakiem inwazyjnym. Znacznie mądrzejszą i skuteczniejszą metodą jest uszkodzenie części struktury mikrokontrolera odpowiedzialnej za programowanie pamięci. Jednak w takim przypadku wymagana jest bardzo dobra znajomość struktury układu - konieczny wręcz staje się reverse engineering , co jednak czasami jest znacznie bardziej kosztowne aniżeli cały projekt.

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