Security first!

Im większa jest wydajność i dostępność Internetu, tym bardziej wydajne są również komponenty, dzięki którym połączone urządzenia stają się „inteligentne”, i tym więcej powstaje obszarów zastosowania aplikacji. Mikrokontrolery połączone z oprogramowaniem są sercem czujników w technologiach Przemysłu 4.0 oraz IoT. Całkowicie połączona fabryka i inteligentny dom tworzą ogromny potencjał rozwoju i innowacji – i to w zasięgu ręki.

Mikrokontrolery pod lupą

W ramach IoT, Przemysłu 4.0 i robotyki mikrokontrolery są coraz częściej wykorzystywane w roli tarczy ochronnej przed manipulacjami i atakami cybernetycznymi. Różne rodziny mikrokontrolerów są już wyposażone w niemały arsenał funkcji bezpieczeństwa. Jako centralne moduły sterowania i regulacji mikrokontrolery zajmują kluczową pozycję w systemach połączonych. Producenci wykorzystują już w produkcji procesy rozwojowe, certyfikowane według odpowiednich norm bezpieczeństwa. Dodatkowo producenci półprzewodników, stosując zabezpieczony łańcuch produkcyjny, starają się oferować swoim klientom bezpieczne rozwiązanie typu End-to-End.

Pod względem bezpieczeństwa wyróżnia się kilka kategorii mikrokontrolerów, zależnych od zastosowań docelowych:

- rozwiązania w dziedzinie uwierzytelniania i moduły TPM (Trusted Platform Module), na przykład do ochrony marki i sieci IoT;
- rozwiązania bankowe i identyfikacyjne do klasycznych zastosowań kart inteligentnych w obszarach płatności, identyfikacji osób, transportu i płatnej telewizji;
- rozwiązania w dziedzinie Mobile Security do rozwiązań bazujących na kartach SIM w urządzeniach przenośnych i zastosowań typu maszyna-maszyna (M2M);
- rozwiązania motoryzacyjne do komunikacji bliskiego zasięgu (NFC, eSE) i bezpiecznej jazdy.

Zintegrowane funkcje bezpieczeństwa danych

W dziedzinie IoT oraz Przemysłu 4.0 i robotyki wykorzystywane są głównie standardowe mikrokontrolery do zastosowań przemysłowych i konsumenckich (General Purpose Microcontroller). Występują jednak również modele ze zintegrowanymi funkcjami bezpieczeństwa. Na przykład seria STM32 dysponuje licznymi funkcjami, które zapewniają ochronę pod względem:

- kradzieży tożsamości (ochrona przed manipulacją, integralność, możliwość śledzenia);
- odmowy usług danych (throttling);
- szpiegowania oraz manipulowania danymi i kodem (ochrona pamięci, zarządzanie uprawnieniami, poziomy debugowania, ochrona przed manipulacją, integralność, bezpieczne aktualizacje oprogramowania sprzętowego);
- atakami fizycznymi lub mechanicznymi (ochrona przed manipulacjami przy module).

Funkcje te są realizowane głównie przez integrację „on chip” i zapewniają skuteczne uwierzytelnianie, integrację platform oraz pełne bezpieczeństwo danych i tym samym ochronę sfery prywatnej użytkownika końcowego oraz pełną ochronę danych, adresu IP i marki. W ten sposób spełniają nawet najsurowsze wymagania wobec bezpieczeństwa danych w standardowych produktach. Typowe zastosowania docelowe obejmują przykładowo: drukarki, komputery, bramy, punkty końcowe IoT i czujniki.

Funkcje sprzętowe

Integralność i niezawodność: Cykliczna kontrola nadmiarowa określa wartość kontrolną, która pozwala wykryć błędy podczas transmisji lub zapisywania danych. W ten sposób możliwe jest nie tylko

sprawdzenie ich integralności, lecz również obliczenie sygnatury oprogramowania w trakcie wykonywania. Monitorowanie sieci jest szczególnie bezpiecznym monitorowaniem zasilania: POR flagstatus (Power on RESET), PDR flagstatus (Power down RESET), BOR flagstatus (Brown out RESET) oraz PVD flagstatus (Programmable Voltage Detector) pozwalają ustalić przyczynę zresetowania i tym samym zapewnić, że odbywa się ono w ramach uprawnionego dostępu. Jest ono uzupełniane przez funkcję „Read while Write" służącą do skutecznego wykrywania manipulacji oraz protokołowania.

System Clock Security System (CSS) opiera się na tym, że zarówno zegar i system używany w celu przywrócenia, jak też zegar wewnętrzny i zewnętrzny działają niezależnie od siebie. Tak samo niezależnie od siebie moduły Watchdog i Window Watchdog monitorują odpowiednio zdefiniowane przedziały czasu.

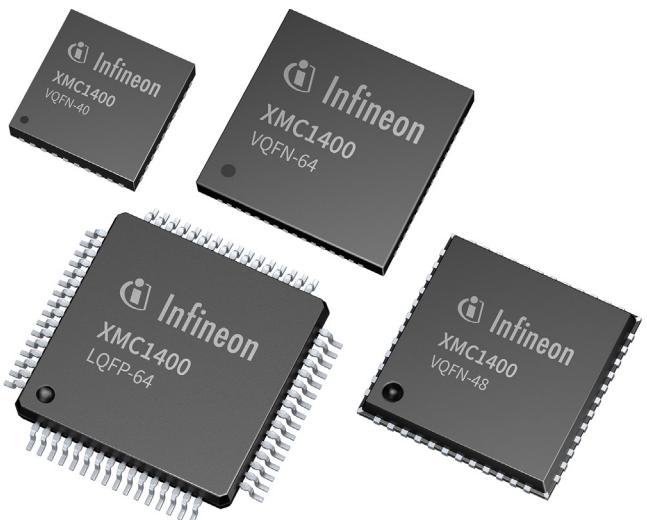
Integralność i wiarygodność zawartości pamięci są zapewnione przez Error Correction Code (ECC) i kontrolę parzystości. Dodatkowo zapewniają one rozszerzoną ochronę przed atakami w celu przemycenia błędów. Czujnik temperatury mierzy na bieżąco temperaturę otoczenia IC, aby nie mógł on opuścić wyznaczonego zakresu przez ukierunkowane nagrzewanie i w ten sposób nie uległ uszkodzeniu.

Szyfrowanie – ale właściwe

Szyfrowanie chroni tekst wyjściowy przed nieupoważnionym dostępem przez zaszyfrowanie pierwotnego tekstu jawnego za pomocą kodu. Kto złamie kod jest w stanie rozszyfrować również zabezpieczony tekst. Zaawansowane metody kryptologiczne wykorzystują szyfrowanie symetryczne lub asymetryczne. W przypadku wariantu symetrycznego do szyfrowania i rozszyfrowania służy jeden klucz, czyli nadawca i odbiorca używają tego samego klucza. W przypadku metod asymetrycznych każdy partner komunikacji wykorzystuje własny klucz, tworzony przy użyciu pary kluczy, składającej się z klucza publicznego służącego do zaszyfrowania danych oraz klucza prywatnego do ich rozszyfrowania.

W niektórych seriach STM32 do szyfrowania służy generator liczb losowych zintegrowany całkowicie w układzie. Szyfrowanie jest wykonywane symetryczną metodą Advanced Encryption Standard (AES). Serie STM32 F2, F4, F7, L4 mają przy tym długość klucza, do wyboru, 128 lub 256 bitów w różnych metodach (ECB, CBC, CTR, GCM, GMAC, CMAC), natomiast w seriach STM32 L0/L1 wdrożono 128-bitowe szyfrowanie AES.

Zaletą metody symetrycznej jest to, że w stosuje się jeden klucz, a więc zarządzanie nim jest łatwiejsze niż w przypadku metod asymetrycznych. Ponadto szyfrowanie i rozszyfrowanie przebiegają znacznie szybciej. Niektóre modele STM32 zawierają dodatkowo całkowicie zintegrowaną funkcję skrótu. Dane są rozdrabniane i rozpraszane, a funkcja przekształca dużą ilość wprowadzonych danych do mniejszej ilości docelowej. Dodatkowo stosowany jest kod Keyed-Hash Message Authentication Code (HMAC). Ta struktura kodu Message Authentication Code (MAC) opiera się na kryptograficznej funkcji skrótu. Kody HMAC są zdefiniowane w standardzie RFC (Request for Comments) 2104 oraz NIST (National Institute of Standards and Technology) FIPS 198.



Zapobieganie manipulacjom

Zabezpieczenie przed manipulacjami służy do obrony przed świadomie lub nieświadomie wywołanymi atakami fizycznymi w systemie sprzętowym na zewnątrz mikrokontrolera. Domena zapasowa, odnosząca się do różnych źródeł wybudzania, zapewnia utrzymanie ochrony również w trybie niskiej mocy. Zegar czasu rzeczywistego (RTC) przypisuje znacznik czasu do każdego zdarzenia związanego z manipulacją. Niektóre serie STM32 zawierają dodatkowo ochronę rejestru RTC. Blokuje ona niedozwolone procesy zapisu i działa niezależnie od resetowania systemu. Nie obejmuje ona jednak ochrony przy zapisywaniu sekwencji przycisków. Po wykryciu manipulacji rejestr zabezpieczenia pilnuje, aby zapisane przy tym treści były automatycznie usuwane. Dodatkowo możliwe jest ukierunkowane zamknięcie kanałów komunikacji za pomocą blokady konfiguracji GPIO. Blokuje ona wybrane wejścia/wyjścia ogólnego przeznaczenia (GPIO), a jej zniesienie jest możliwe przy kolejnym resetowaniu.

Więcej broni przed atakami

Blokada debugowania zapobiega nieautoryzowanemu dostępowi do mikrokontrolera przez interfejs debugowania. Poziom bezpieczeństwa można wybrać w zależności od zastosowania lub zapotrzebowania, lecz jego późniejsze obniżenie nie jest możliwe.

Prawo dostępu nadaje użytkownikom lub grupom użytkowników prawa do wykonywania określonych działań. W tym celu zintegrowana jednostka ochrony pamięci (Memory Protection Unit, MPU) dzieli pamięć na obszary o różnych uprawnieniach i regułach dostępu.

Podczas transferu danych zapora chroni część kodu i część danych pamięci Flash lub SRAM przed resztą kodu, wykonywaną poza obszarem chronionym. Zapora działa bardziej restrykcyjnie niż jednostka ochrony pamięci (MPU), jest ona zintegrowana jedynie w modelu STM32L0 i L4.

Ochrona przed odczytem służy do zarządzania kontrolą dostępu do pamięci. W określonych warunkach zrzuty lub kopie zapasowe pamięci z poziomu adresów IP użytkowników nie są przy tym dozwolone. Ochrona przed zapisem umożliwia zabezpieczenie każdego sektora przed niechcianymi operacjami zapisu. Zamknięta ochrona kodu umożliwia skonfigurowanie każdego obszaru pamięci jako „execute only", tzn., że dozwolone jest tylko wykonanie kodu, a nie jego zapisanie.

Funkcja Mass Erase lub Secure Erase umożliwia bezpieczne usuwanie adresów IP i poufnych danych, proces całkowicie przywraca fabryczne ustawienia pamięci.

Na potrzeby śledzenia urządzenia końcowego wiele serii STM32 dysponuje specyficznym, unikatowym 96-bitowym identyfikatorem. Można wykorzystać go również do dywersyfikacji kluczy bezpieczeństwa.

Wiele serii zawiera ponadto funkcje zapewniające bezpieczną aktualizację oprogramowania sprzętowego. Funkcje bezpieczeństwa realizowane w elementach sprzętowych można rozszerzyć za pomocą rozwiązań programowych.

Bezpieczeństwo urządzenia końcowego w odniesieniu do manipulacji ze strony osób trzecich definiuje się na podstawie

zrealizowanych rozwiązań programowych, jak również wykorzystanych elektronicznych komponentów sprzętowych. Mikrokontrolery i komponenty pamięci, w razie potrzeby w połączeniu z czujnikami i obwodami IC specyficznymi dla aplikacji, odgrywają równie ważną, centralną rolę dla zastosowań IoT i Przemysłu 4.0. Firma Rutronik przygotowała w postaci białej księgi zestawienie istotnych dla bezpieczeństwa, zintegrowanych cech rodzin mikrokontrolerów: ochrona przed manipulacją, moduły szyfrowania, Permission Management, Debug Lock Level i środki ochrony pamięci (Memory Protection).Również integralność i bezpieczeństwo funkcjonalne są w nim wyszczególnione w formie tabeli (link do pobrania w bibliografii na końcu tekstu).

Firma Infineon oferuje w seriach XMC-1xxx oraz XMC-4xxx równie zaawansowaną, zintegrowaną ochronę danych bezpieczeństwa, jaką przedstawiono w tabeli na stronie 74/75 broszury poświęconej aspektom bezpieczeństwa (patrz bibliografia). W związku ze szczególnymi wymogami dotyczącymi szyfrowania symetrycznego lub niesymetrycznego producent odsyła przy tym do pakietu oprogramowania kryptograficznego. Własna ocena zagrożeń bezpieczeństwa urządzenia końcowego lub jego elementów zakłada, że projektant może na pierwszy rzut oka stwierdzić, które mikrokontrolery pozwalają zapewnić zgodność z przepisami wynikającymi z rozporządzenia RODO w ramach budowy płyty.

Jeżeli projektant zdefiniuje wymagania dotyczące bezpieczeństwa urządzenia końcowego, w ofercie produktów Rutronik znajdzie najróżniejsze rodziny mikrokontrolerów od producentów półprzewodników, które dzięki zintegrowaniu funkcji istotnych dla bezpieczeństwa spełniają wymagania wynikające z RODO.

W związku z zagadnieniami Przemysłu 4.0 można wywnioskować, że działalność związana z danymi nie jest działalnością produktową, lecz platformową. W przyszłości nie będzie liczyć się sprzedaż pojedynczych lub kilku maszyn bądź instalacji z dużym obrotem. W miejsca użytkowania będą raczej rozstawiane rozmaite maszyny wytwarzające dane, a operator platformy będzie w pierwszej linii zarabiać dzięki związanym z tym usługom danych oferowanych klientom. Wprowadzi to rewolucyjną zmianę w modelach biznesowych klasycznej budowy maszyn i usług świadczonych przez dostawców.

Inż. dypl. Martin Motz
Product Manager Digital
Rutronik Elektronische Bauelemente GmbH

Bibliografia:
Rutronik: Security Aspects: White Paper on How to Make State of the Art Electronic Designs. Dostępna pod adresem ***http://bit.ly/2YGJRm0***