МІКРОПРОЦЕСОРНІ СИСТЕМИ ІЗ ПІДВИЩЕНИМ РІВНЕМ ЗАХИСТУ ВІД КІБЕРЗАГРОЗ НА АПАРАТНОМУ РІВНІ

доцент, к.т.н. Воргуль О.В., студент Білоцерківець О.Г.,
студент Сєріков А.О.
Харківський національний університет радіоелектроніки,
кафедра мікропроцесорних технологій і систем,
e-mail: oleksii.bilotserkivets@nure.ua

Abstract. The more powerful and comprehensive the Internet becomes, the more perfect and "smart" the components connected to it, the more areas open up for their application. However, this can lead to critical security breaches that require appropriate measures to prevent vulnerabilities. The heart and soul of the sensory technologies of the fourth industrial revolution, Industry 4.0 and the Internet of Things (IoT), are microcontrollers and their software. They offer huge potential for growth and innovation in related "smart" factories and "smart" homes. In this business boom, but at the same time they make systems vulnerable to external attacks.

Вступ. На сьогодні електронні пристрої розробляються для використання в автоматизованих системах з різними умовами експлуатації. Це можуть бути різні кліматичні фактори або тяжке електромагнітне оточення, тобто використання мікропроцесорів при досить суттєвих електромагнітних перешкодах (електростанції, підстанції), де вимоги до безпеки і надійності зростають прямо пропорційно складності системи. Тому з боку розробників систем, так і певних державних стандартів, висувається вимога до таких властивостей апаратного забезпечення, як: захист мікропроцесорної системи від випадкових програмних змін, аварійних збоїв коду, порушень пам'яті, помилок у програмі та захист системи від несанкціонованого доступу.

Основна частина. Захистом від несанкціонованих маніпуляцій та кібератак в контексті IoT, Industry 4.0 і робототехніки все частіше стають мікроконтролери. Деякі сімейства мікроконтролерів вже включають безліч функцій безпеки. Справа в тому, що мікроконтролери є основними компонентами в середовищі управління системами та мережами що створюються в галузі IoT . Їх постачальники вже використовують процеси розробки та сертифікацію згідно з відповідними стандартами безпеки. А постачальники напівпровідників також гарантують, що можуть запропонувати своїм клієнтам безпечне комплексне рішення.

З точки зору безпеки мікроконтролери можуть бути класифіковані згідно їх цільовими фінальними додатками:

– рішення в області аутентифікації і довірені платформні модулі (trusted platform module, TPM), наприклад для захисту як безпосередньо самого користувача, так і мереж IoT;

– банківські та ідентифікаційні рішення для класичних компаній-виробників і емітентів смарт-карт, що використовуються в сфері обробки платежів, як персональних ідентифікаторів, для оплати послуг транспорту і в системах доставки платного контенту для телебачення;

– мобільні рішення безпеки для рішень на базі SIM-карт в мобільних продуктах і додатках міжмашинної взаємодії - M2M (machine-tomachine);

– автомобільні рішення для комунікації ближнього поля (NFC, eSE) і систем забезпечення безпечного водіння.

Інтегровані функції захисту даних

IoT і Industry 4.0 в основному використовують стандартні мікроконтролери, створені для промислового і побутового застосування (їх загальна назва - «Мікроконтролери загального призначення»). Але також вже доступні і моделі з вбудованими функціями безпеки. Наприклад, сімейство мікроконтролерів STM32 (сімейство 32 бітних мікроконтролерів виробництва STMicroelectro nics), яке має безліч вбудованих функцій, що забезпечують їх захист, в тому числі:

– захист від крадіжки особистих даних (захист від маніпуляцій, захист цілісності, відстеження руху продукту);

– відмова в обслуговуванні даних (регулювання);

– захист від відстеження і маніпулювання даними і кодом (захист пам'яті, управління правами доступу, рівень налагодження, захист від маніпуляцій, захист цілісності, безпечні оновлення прошивки);

– захист від фізичного (механічного) втручання (захист від маніпуляцій на кристалі).

Ці функції в основному реалізуються їх інтеграцією безпосередньо на кристалі мікроконтролера. Вони забезпечують надійну перевірку справжності (верифікацію), цілісність платформи і постійний захист даних, включаючи захист конфіденційності кінцевих користувачів, а також комплексний захист даних, IP-адрес і брендингу та відповідають найвищим вимогам безпеки даних для стандартних продуктів. Типові цільові програми таких мікроконтролерів - це, наприклад, комп'ютери, шлюзи, кінцеві точки IoT і різні датчики.

Функції захисту на апаратній основі

На апаратній основі як мінімум використовується залишок циклічного надмірного коду (cyclic redundancy check calculation), тобто обчислюється контрольна сума, яка виявляє помилки при передачі або зберіганні даних.

Це не тільки забезпечує перевірку цілісності коду, але і означає, що сигнатура ПО може бути розрахована під час його роботи. Моніторинг живлення - ще один метод з високим ступенем захисту. Для визначення причини скидання і, таким чином, забезпечення скидання тільки за допомогою аутентичного доступу використовується система управління

статусом прапора POR (power on RESET) / PDR (power down RESET)/ BOR (brown out RESET) / PVD (programmable voltage detector). Для ефективного виявлення маніпуляцій і ведення журналу все це доповнюється функцією «Read while Write »

Функціональність CSS (Clock Security System) заснована на тому, що якщо при використанні зовнішнього генератора (в мікроконтролерах серії ST32 він позначений як HSE, external) в якості джерела тактового сигналу тактової частоти система не зависне намертво в невизначеному стані, а зможе виконати якісь дії, якщо в SYSCLK або PLL, станеться збій генерації, то CSS автоматично перемкне всю систему на роботу від вбудованого RC-генератора (в мікроконтролерах серії ST32 він позначений як HIS, internal). Таким чином, якщо щось трапиться з тактовими сигналами, то можна перевести об'єкт управління мікро контролером в безпечний стан. Крім того, резервний таймер (Watchdog) і віконний резервний таймер (Window Watchdog) також контролюють тимчасові вікна незалежно один від одного. Цілісність і достовірність вмісту пам'яті забезпечується перевіркою і справляння помилок коду (Error Correction Code, ECC) і, як вже було сказано, перевіркою парності. Тут теж забезпечується все щоб отримати додатковий захист від атак, спрямованих на недопущення зараження систем помилками коду. Крім того, датчик температури безперервно вимірює температуру середовища, що оточує мікроконтролер. Це необхідно для того, щоб переконатися, що вона залишається в зазначеному діапазоні, і таким чином уникнути ризику його пошкодження при спеціальному тривалому нагріванні.

Висновки. Аналізуючи сучасний стан та розвиток мікропроцесорних систем ми бачимо, що виробники використовують захист на апаратному рівні. Даний захист в залежності від виробника може бути реалізований як певний специфічний модуль, наприклад, у мікроконтролерів сімейства RX інтегрований модуль захисту пам'яті (MPU), який може розглядатися як апаратний брандмауер, що відокремлює, привілейований код операційної системи від програми користувача. Засоби та функції які наведенні в даній публікації дозволяють легко виявити збій і забезпечують гнучкі сценарії усунення помилок, що підвищує надійність програмного забезпечення та автоматизованої системи в цілому.

Список використаних джерел.

1. ST’s secure microcontrollers contribute to a smarter and more secure connected world https://www.st.com/en/secure-mcus/secure-hardware-platforms.html

2. STM32 Trusted platforms https://www.st.com/content/st_com/en/stm32trust.html

3. The National strategy Industry 4.0 Асоціація підприємств промислової автоматизації України (АППАУ) https://appau.org.ua/en/category/pubs/