УДК 681.324

Маліновський В.І.

МІНІМІЗАЦІЯ ФАКТОРІВ КІБЕРЗАГРОЗ І СПЕЦІАЛІЗОВАНІ ПІДХОДИ ДО ІНФОРМАЦІЙНОГО ЗАХИСТУ МІКРОПРОЦЕСОРНИХ СИСТЕМ ІНДУСТРІАЛЬНОГО ІНТЕРНЕТУ РЕЧЕЙ

Вінницький національний технічний університет

Аннотація. Розглянуто аспекти і проведено короткий аналіз кібербезагроз у спеціалізованих мікропроцесорних системах Інтернету речей (IoT), які виникають у сучасних мікропроцесорних приладах і системах IoT. Коротко розглядяються основні чинники впливу появи інформаційних загроз в мікропроцесорних пристроях IoT, а також перспективи розвитку і прогресивні підходи до захисту даних і процесів функціонування мікропроцесорних систем, зокрема: захищене оброблення і передавання даних, криптографічне оброблення інформації у сучасних промислових системах IoT, організації безпечного зв'язку, захищене телекерування та телемоніторинг на промислових об'єктах. Дані підходи дозволять організацію захищеного режиму функціонування промислових IoT (IIoT) із вищою стабільністю та надійністю роботи. Зокрема показано основи шифрування сигналів та піходи відновлення попередніх станів обчислювального процессу із вищими інформаційної захищеності та стабільності процесів агрегації даних у мікропроцесорних системах.

Ключові слова: індустріальні пристрої, мікропроцесорні пристрої IoT, канали даних, МК система, мікроконтрролер, мікропроцесор, інформаційна загроза, кіберзагроза, Інтернет речей (IoT), промисловий Інтернет речей (IIoT).

Abstract. Aspects of cybersecurity risks and threats in specialized microprocessor systems in the Internet of Things (IoT), which occur in modern microprocessor devices and IoT systems are considered and analysis. The main factors influencing the emergence of information threats in IoT microprocessor devices, as well as prospects for development and progressive approaches to protection of data processing in microprocessor systems and devices, such as: secure data processing and transmission, cryptographic information processing in modern industrial IoT systems, organization of secure communication, secure telecontrol and telemonitoring in the industrial IoT devices. These approaches will allow the organization of a more protected mode of stabile and secure operation of industrial IoT (IIoT) with higher data processing stability and reliability. In particular, the basics of signal encryption and recovery methods of previous states of the computing process with higher information security and stability of data aggregation processes in microprocessor systems are shown.

Keywords: industrial devices, industrial IoT (IIoT), communication channels,cyberthreat, Internet of Things (IoT), microprocessor, microprocessor devices.

Сучасні технології і прилади промислового Інтернету речей є високоінтелектуальними системами із контролерами керуванням, які досить швидко впроваджуються у всі сучасні сфери нашого життя. Такі системи, як «розумний будинок», «комплексна система безпеки офісу», «системи автоматичного догляду за рослинним садом», «система автоматичного управління і моніторингу за сучасним підприємством і офісом» належать до Інтернет у речей (IoT) і відповідають концепції Індустрії 4.0- X.0 (Industry 4.0- X.0) і досить швидко розвиваються і впроваджуються в наш час. Вони є майже повністю автоматичними або автоматизованими системами і передбачають обмін даними через мережу передачі даних (МПД) на базі глобальної мережі Інтернет із функціями «смарт»-управління через кінцевий персональний пристрій (смартфон) користувача. Також сучасні інтелектуальні технології промислового Інтернету речей (Industrial Internet of Thinks, IIoT), а також останні тенденції до впровадження технологій телемоніторингу та телеуправління технологічними процесами дозволяють організовувати високоефективне, комфортне і автоматизоване керування та моніторинг промислових і інших процесів і систем через організовані канали віддаленого зв'язку на базі мережі Інтернет, що відповідає концепції розподіленого застосування сучасного індустріального Інтернету речей (Internet of Thinks або IoT).

Разом з тим, це несе значні ризики для основних обчислювальних трактів(ядра оброблення на

базі центрального мікропроцесора або мікроконтроллера) від впровадження інформаційних загроз, пов'язані із кібербезпекою та інформаційною безпекою цілісності даних у IIoT. Адже IoT використовують саме канали все «доступної» мережі Інтернет. Це потребує в свою чергу нових підходів і до вирішення задач інформаційного захисту саме у центральних обчислювальних трактах – мікропроцесорних блоках оброблення IoT, як основних критичних місць IoT, та забезпечення захисту їх функціонування від сучасних інформаційних загроз (хакерських атак, мікропрограм ШПЗ, несанкціонованого доступу, тощо).

Аналіз мікропроцесорних трактів сучасних індустріальних систем Інтернету речей свідчить про те, що основними інформаційними ризиками для них є :

- прямий доступ до пам'яті, доступ до регістрів/буфера мікроконтроллера керування IoT;
- переповнення стеку/буфера, переповнення буфера, вичитка буфера пам'яті ;
- віддалений запуск коду, та/або зовнішній доступ до ліній передачі даних у МК, вичитка із зовнішніх ліній передачі даних в МК ;
- зміна порядку адресації в МК, зміна/підміна значень адрес;
- окремі вразливості ядра та інших компонент, вразливості архітектури, вразливості і вплив на процеси роботи АЛП(арифметико-логічного пристрою) мікроконтролера/мікропроцесора;
- доступ до ресурсів МК та до окремих регістрів (в т.ч. конфігураційних із зовні), пряму втручання/пересилка команд керування і передачі даних;
- переповнення стека адреса, переповнення пам'яті, пряма вичитка значень стека, взлам та несанкціоноване втручання в ядро системи;
- несанкціоноване втручання і вичитка/пересилка команд і даних із ліній портів мікропроцесорної системи. Втручання в роботу регістрів даних та індикації стану портів вводу/виводу мікроконтроллера;
- вплив і передача даних. зміна слідування порядку команд управління та/або перехоплення їх і потоків даних у ядрі та/або області ядра мікропроцесорної системи;
- несанкціоноване зовнішнє втручання в роботу ліній передачі даних та/або вторинних ліній – зовнішніх ліній передачі інформації в мікроконтроллері. Сюди також можна віднести несанкціоноване (стороннє) пересилання/вичитку команд керування МК, зчитування інформаційних потоків (послідовностей) прийому/переді даних до/від мікроконтроллера;
- загрози нульового дня («zero day threats») і загрози запуску шкідливого коду шляхом впровадження в основну підпрограму(в т.ч. загрози запуску «сліпих/порожніх» циклів в підпрограммі, зміна і переповнення памяті МК шліхом запуску ресурсоємного програмного коду, інше)
- інші потенційні загрози фізичного і прямого електромагнітного впливу на мікропроцесорну систему.

Також проведений аналіз факторів кіберзагроз визначив основні тенденції і ризики для мікроконтролерів індустріальних IoT, зокрема:

- вплив на команди керування і підміна команд керування в мікропрограмі контролера IoT;
- зміна порядку слідування команд і зміна технологічного циклу і алгоритму мікропрограми;
- недосконаліть коду програми і потенційно наявні «слабкі» місця в машинному коді ПЗ мікроконтррлера;
- уразливості в архітектурі МК, потенційно-небезпечні і можливі комбінації в архітектурі МК, які можуть бути виконані за допомогою спеціальних послідовностей команд;
- уразливості пам'яті;
- відкритість та «не захищеність» коду у ПЗП та ОЗП мікроконтролера;
- Атаки типу stack-read та stack-overflow Пряме читання буфера і переповнення буфера;
- Вразливості Кеш-пам'яті;
- Вразливості ядра і таймерної системи, а також системи переривань мікропроцесора;
- Вразливості і генерація замкнутих пустих циклів і циклів переповнення памяті МК за рахунок регулярних повторних операцій і операцій , що викликають ірраціональне використання ресурсів і архітектури МК;
- Неправомірне і нелогічне шкідливе використання механізму зовнішніх переривань і механізму апаратного і програмного скидання мікропроцесора (функції: «reset»);

- Вразливості «0»-го дня (zerodayvulcatuanables) – не виявлені актуальні вразливості для кожної архітектури і ядра окремих мікроконтрролерних систем;
- Випадкові загрози та/або недосконалості і помилки в программному коді, наявність «не “пропрацьованих» критичних та/або проблемних місць в програмному коді, потенційно вразливих місць, недосконаліть / не врахування всіх можливих станів в алгоритмі програмютього коду та процедурах і функціях мікропрограм МК. Наявність критичних і помилкових місць у них;
- Недосконаліть і незахищеність архітектури МК, окремих периферійних пристроїв, ядра .

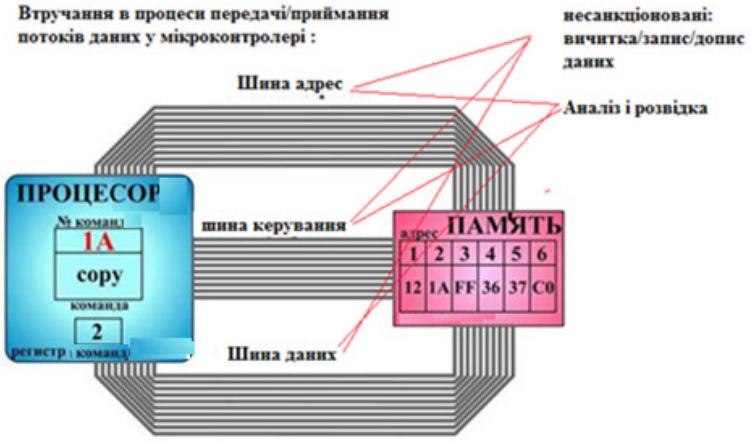

Рис.1. Основні вразливі місця в архітектурі мікропроцесора

Оскільки інформаційні загрози в мікропроцесорних трактах IoT є комплексними, то й рішення, спрямовані на захисти обчислювального процесу і алгоритмів роботи мікропрограм контролера керування також повинні мати комплексний підхід.

Вирішення проблеми безпеки мікроконтролерів IoT і мікропроцесорних трактів , а також закриття потенційно небезпечних критичних місць архітектури МК є:

- Функції захисту на апаратній основі , наприклад, підходи, використання циклічного контролю надмірності коду (cyclicredundancycheckcalculate), тобто обчислюється контрольна сума, яка виявляє помилки при передачі або зберіганні даних. Це не тільки забезпечує перевірку цілісності коду, а й означає, що сигнатура може бути розрахована під час його роботи;
- Контроль циклу обчислювального процесу і порядку слідування команд мікропрограми контрролера IoT;
- Моніторинг живлення і моніторинг обчислювальних ресурсів – ще один метод із високим ступенем захисту. Для визначення причини скидання і, таким чином, забезпечення скидання тільки за допомогою автентифікованого доступу використовується система управління статусом прапора POR (poweron RESET - включення живлення RESET) / PDR (powerdown RESET - відключення живлення RESET) / BOR (brownout RESET - "зниження живлення RESET") / PVD (programmable voltage detector - "програмований детектор напруги"). Для ефективного виявлення маніпуляцій та ведення журналу це доповнюється функцією «Readwhile Write» (буквально: «читай під час запису», тобто зчитування одного слова під час запису іншого слова);
- Підходи, що передбачають використання ізольованості і контролю функціональності CSS (Clock Security System - "система безпеки тактування") заснована на тому, що якщо при використанні зовнішнього генератора (у мікроконтролерах серії ST32-STM32, ARM він позначений як HSE) як джерело тактового сигналу тактової частоти система не зависне намертво в невизначеному стані, а зможе виконати якісь дії, SYSCLK або PLL (система ФАПЧ), відбудеться зрив генерації, то CSS автоматично переключить всю систему працювати від вбудованого RC-генератора (у мікроконтролерах серії ST32 він позначений як HSI). Таким чином, якщо щось трапиться з тактовими сигналами, можна перевести об'єкт управління мікроконтролером в безпечний стан. Крім

того, сторожовий таймер (Watchdog) та віконний сторожовий таймер (WindowWatchdog) також контролюють часові вікна незалежно один від одного.

- Контролюють цілісність та достовірність вмісту пам'яті, що забезпечуються перевіркою та виправленням помилок коду (ErrorCorrectionCode, ECC) та, як уже було сказано, перевіркою парності. Тут також забезпечується додатковий захист від атак, спрямованих на недопущення зараження систем помилками коду;
- Контроль зовнішніх фізичних і електричних параметрів МК. Наприклад, 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 пошкодження при спеціальному тривалому нагріванні.
- Використання «***багаторівневої програмно-апаратна ізоляції***» станів мікропроцесора та/або ділянки мікропроцесорної системи, в т.ч. важливої обласні мікропрограми, де він розміщений на різних рівнях.(До числа такої ізоляції відноситься: а.) ізоляція програмного коду і методів доступу до потоків даних і потоків програмного коду команд і даних; б.) фізична ізоляція електричної системи; в.) електрична ізоляція і в т.ч. електромагнітна ізоляція мікропроцесорної системи, г.)фільтрація вторинних шумів до/від МК, електрична ізоляція і фільтрація ліній живлення і ліній передачі даних від/до зовнішніх кіл, такі як датчики та/або кола управління, інше; д.) перевірка і ретельна кореляція програмного коду перед програмуванням/оновленням на предмет виявлення вразливостей в мікропроцесорній системі; е.) перевірка та моніторинг стану МК, перевірка ; е.) використання шифрування і кодування даних для МК із підвищеним рівнем захисту (використовується в захищених і кіберстійких мікропроцесорних системах).
- Використання криптографічних систем і алгоритмів обробки даних в мікропроцесорних системах IoT (контролера керуваннгя IoT) із надійним криптографічним захистом. Даний підхід потребує зокрема спеціалізованої архітектури МК із криптографічною периферією (коден/енкодер) і відноситься до числа спеціалізованих надійних МК систем;
- Використання резервування обчислювального процесу і основної мікропрограми (в т.ч. алгоритмічних частин і блоків), що дозволяє відновлювати дані із попередніх проміжних станів у випадку настання критичної ситуації;
- Використання сучасних інноваційних підходів до захисту мікропроцесорних систем – використання алгоритмів віртуалізації основного обчислювального процесу, його багаторівневе резервування і резервним копіюванням/фіксуванням і відновленням попередніх Ti-1, Ti-2 ...Ti-n станів обч. процесу. У випадку настання кіберзагрози вектор параметрів і стану обчислювального процесу відновлюється із попередніх значень в часових проміжках t-1; t-2; t-i. t-m тобто:

$$\varphi(\mathrm{ti},\ \mathrm{f}(\mathrm{x}, y, z, t, n, d)_{\mathrm{ti}},) = \varphi'(\mathrm{ti}, \mathrm{f}(\mathrm{x}, y, z, t, n, d)\mathrm{ti} - \mathrm{m})$$

$$\varphi'(\mathrm{ti}, \mathrm{f}(\mathrm{x}, y, z, t, n, d)\mathrm{ti},) = \sum_{ti=0}^{n} \binom{n}{t} \mathrm{F}(\varphi'(\mathrm{f}(\mathrm{ti}, \mathrm{f}(\mathrm{x}, y, z, t, n, d)\mathrm{ti},,))\mathrm{i} - \mathrm{m},)$$

де, $\varphi'(\mathrm{ti}, \mathrm{f}(\mathrm{x}, y, z, t, n, d)\mathrm{ti},,)$ - поточний вектору функції обчислювального процесу групи параметрів даних в момент часу t_i, тобто після події при настанні кіберзагрози; $\varphi'(\mathrm{f}(\mathrm{ti}, \mathrm{f}(\mathrm{x}, y, z, t, n, d)\mathrm{ti},,))\mathrm{i} - \mathrm{m}$ - попередній вектор стану попередньої функції обчислювального процесу групи параметрів даних в момент часу t_{i-1}, тобто до події настання кіберзагроз (вектор стабільних параметрів).

Таким чином відбувається відновлення попередніх значень обчислювальних параметрів до моменту настання кіберзагрози в МК системі. Недоліком даного підходу є потреба у значній мірі додаткових ресурсів мікроконтролера і в т.ч. пам’яті для резервування попередніх станів обчислювального процесу.

Використання методів захисту даних на основі поєднання функціоналу віртуалізації в контейнерах для окремих потоків інформації із підмішуванням додаткових неінформативних або псевдоінформативних потоків із надійним вдосконаленим шифруванням із зміщенням та у поєднанні із розпаралелюванням обчислювального процесу на різних розмежованих у правах доступу до обчислень віртуальних обчислювальних середовищах(оболонок) для різних процесів.

Враховуючи це, необхідним є використання комплексних підходів до забезпечення захисту мікропроцесорів і контролерів IoT, на базі нових комплексних методів, що ґрунтуються на вищезазначених підходах. В т.ч. це може бути використано і для побудови моделі комплексного захисту даних мікропроцесорних трактів для критичної інфраструктури IoT промислового (індустріального) спрямування (IIoT). Це б могло забезпечити максимальну безпеку функціоналу і захист критичних даних в основних трактах промислових IoT. Нові підходи та надійна модель захисту даних для індустріальних систем Інтернету речей повинні базуватись тільки на комплексному поєднані алгоритмів і способів захисту даних на різних рівнях організації мікропроцесорної системи для реалізації практичного і надійного захисту даних у них.

Маліновский Вадим Ігоревич – к.т.н.**,** доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінница, Україна.

Malinovskyi Vadym — PhD (Eng), Associated Professor of Data Protection Department in Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine.