УДК 004.04

Станько А.А.[1], Козак Р.О.[1], Федорів І.П.[2]
[1]Тернопільський національний технічний університет ім. І.Пулюя, Україна
[2]Технічний коледж ТНТУ ім. І. Пулюя

АНАЛІЗ ВПЛИВУ ВРАЗЛИВОСТЕЙ MELTDOWN І SPECTRE НА РОБОТУ МІКРОПРОЦЕСОРІВ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ

Stanko A.A., Kozak R.O., Fedoriv I.P.

ANALYSIS OF MELTDOWN AND SPECTRE EFFECTS ON MICROPROCESSORS WORKING OF AUTOMATED SYSTEMS OF MANAGEMENT BY TECHNOLOGICAL PROCESSES

Нині чимало уваги приділяється питанням безпеки автоматизованих систем управління (АСУ). Причиною цього стала низка успішних атак на АСУ ТП, що призвели до серйозних наслідків [1]. У сучасному світі АСУ є ключовим елементом критичної інфраструктури, що забезпечує нормальну роботу вкрай важливих для розвитку держави служб і систем: урядові органи, водопостачання, фінансові і податкові системи, енергетика, космос, атомні електростанції і транспортні системи, великі виробничі підприємства тощо. Усе це об'єкти, мережі, служби та системи, збій в роботі яких у будь-якому випадку позначиться на здоров'я, безпеку і добробут громадян країни.

За поширеністю компонентів АСУ ТП на ринку лідирують компанії Honeywell, SMA Solar Technology, Beck IPC, Schneider Electric, Siemens і Bosch Security Systems, ABB, Abbott [2], в системах яких використовуються CPU виробництва Intel, і практично всі процесори з сучасною логікою, що націлено на мінімальні простої в роботі ЦП. В їх число входять процесори AMD і ядра з ARM-архітектурою, яким також властиві сучасні вразливості.

Найбільш уразливими і, разом з тим, поширеними компонентами АСУ ТП є SCADA-системи. Крім того, багато прогалин в безпеці було виявлено в архітектурах процесорів, мережевих пристроях промислового призначення і інженерному програмному забезпеченні [3].

Для надійного захисту АСУ ТП необхідно спершу проаналізувати та класифікувати притаманні їй вразливості з метою розробки ефективних заходів захисту АСУ ТП та їх реалізації в складі комплексної системи захисту інформації підприємства.

Класифікація вразливостей

SP 800-82 - комплексне керівництво з безпеки АСУ ТП, в якому подано рекомендації, що забезпечують повний цикл розробки системи захисту АСУ ТП від постановки завдання до реалізації та експлуатації. Згідно документу вразливості в АСУ ТП можна класифікувати наступним чином [1]:

– уразливості в політиці безпеки заходів по її реалізації;
– уразливості в розробці та архітектури системи;
– уразливості в налаштуванні і обслуговуванні;
– фізичні уразливості, уразливості в розробці програмного забезпечення;
– уразливості в комунікації та налаштування мережі.

Найгучнішою вразливістю останнього десятиліття стали Meltdown («Крах») і Spectre («Привид») [4]. Meltdown дозволяє порушити бар’єр між додатками і внутрішньою пам’яттю операційної системи, що відкриває доступ до даних, які зберігаються в пам'яті ОС. Незважаючи на те, що у програм немає прямого доступу на читання з кешу, вони мають повне право звертатися до збережених в ньому адрес. При повторному зверненні до помилкової адреси за швидкістю відповіді процесора можна визначити, чи зберігається в швидкій пам’яті потрібне значення. Особливості доступу програм до кешу дозволили визначити алгоритм, який змушує ЦП пройтися по всіх ділянках пам'яті, що використані в «відкинутій» раніше гілці і таким чином відкрити всю розташовану в них інформацію незалежно від привілеїв процесу.

Найбільшою небезпекою уразливості є її практично повна незалежність від операційної системи: через це антивіруси не можуть виявити подібний шкідливий код. Також Meltdown не залишає ніяких слідів в системі, що ускладнює завдання пошуку «шкідника», який вже встиг завдати шкоди.

Spectre за своєю суттю дуже схожа з Meltdown – також опирається на кеш і механізм передбачення переходів [5]. Вразливість Spectre складніша в реалізації та ширша у використанні. Ця технологія злому може змусити будь-який процес самостійно видати вміст власної пам’яті. Spectre проникає в пам’ять іншого процесу зі схожим набором повторюваних інструкцій, таким чином стираючи грань між ізольованими додатками. Виявлений механізм характеризується цілим спектром варіантів використання, що значно ускладнює випуск відповідного програмного «патча».

Аналізуючи алгоритми роботи Spectre і Meltdown, у більшості АСУ ТП відсутня низка характеристик, необхідних для успішної експлуатації Meltdown і Spectre, попри те що апаратна частина підпадає під перелік вразливостей. Компанія Intel зауважує, що для успішної атаки необхідно виконати шкідливий код в локальній пам'яті системи. У свою чергу, в більшості АСУ ТП відсутній ряд характеристик, необхідних для експлуатації Meltdown і Spectre.

Зокрема, в АСУ ТП в принципі неможливо передати шкідливий код в локальну пам'ять і виконати його. Крім цього, в системах, як правило, відсутня мережеве з'єднання і функція запуску будь-якого ПЗ, відмінного від вбудованої програми управління. Крім того, в АСУ ТП не передбачена можливість одночасного запуску декількох програм.

Запобігання атакам

Незважаючи на те, що в ряді АСУ присутній з’єднання з мережею, що забезпечує двосторонню передачу даних для полегшення віддаленої конфігурації, діагностики та обслуговування, а також для взаємодії з іншими частинами підприємства, дані типи з’єднань зазвичай не дозволяють встановлювати нове або ненадійне програмне забезпечення і, отже, ризик експлуатації Meltdown і Spectre, чи подібних, на них також невисокий.

Однак для запобігання експлуатації цих та інших вразливостей доцільно впроваджувати низку заходів [6]:

1. Перевірка систем на уразливості, особливо тих систем, на яких вже були зафіксовані інциденти інформаційної безпеки.
2. Адекватний моніторинг мереж, що застосовуються для контролю таких об'єктів критичної інфраструктури, і при необхідності їх повна ізоляція від зовнішніх з’єднань, що дозволить виявляти зовнішні атаки і запобігати доступ до систем, керованим з внутрішньої мережі.
3. Контроль над змінними пристроями.
4. Моніторинг комп’ютерів, до яких підключені програмовані логічні контролери. Ці пристрої можуть надати несанкціонований доступ до критично важливих систем управління.
5. Вчасне оновлення програмного забезпечення та заміна критично вразливих та застарілих елементів системи

Література

1. Каменских А.Н., Бортник Д.А. Анализ рекомендаций по защите автоматизированных систем управления с целью выявления типичных уязвимостей. [Электронный ресурс] / Каменских А.Н., Бортник Д.А. // Вестник Пермского национального исследовательского политехнического универ-ситета №17, 2016, Пермь
2. Positive Technologies ICS SECURITY:2017 IN REVIEW [Електронний ресурс] – Режим доступу: www.ptsecurity.com
3. Защита АСУ ТП [Електронний ресурс] - Режим доступу: www.tadviser.ru
4. УРАЗЛИВІСТЬ MELTDOWN/SPECTRE [Електронний ресурс] - Режим доступу: https://coi.com.ua
5. «Чипокалипсис»: обзор масштабной уязвимости современных процессоров [Електронний ресурс] - Режим доступу: https://tproger.ru
6. Найгучніші кібер-атаки на критичні інфраструктури http://it-ua.info