УДК 621.941-229.3:531.133

Морозова І.В., канд. техн. наук, доцент
Корчан В.М., аспірант
Національний авіаційний університет, м. Київ, korchan.vlad22@gmail.com

ІННОВАЦІЙНІ МЕТОДИ ІДЕНТИФІКАЦІЇ ЗАХИСТУ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

Інтернет речей (IoT) відноситься до простих апаратних пристроїв, підключених через Інтернет. Приклади включають камери дверного дзвінка, натільні переносні монітори здоров'я, пожежну сигналізацію та міські світлофори. За деякими оцінками, до 2025 року у світі може бути 50 мільярдів таких пристроїв, а до 2030 року – 1 трильйон. Хоча вони надають зручні послуги, пристрої IoT дуже небезпечні і їх можна легко взламати. Взломані пристрої можна змусити взламати інші пристрої. Такі ситуації загрожують репутації підприємств і можуть спричинити багато видів реальної небезпеки для людей. Уразливість виникає через те, що пам'ять і обробна здатність пристроїв занадто низькі для високої безпеки. Замінити мільярди застарілих пристроїв оновленим обладнанням неможливо. Фінансований ЄС проект INSTET розробив спосіб захисту пристроїв IoT, який дозволяє уникнути такої заміни. Нинішній проект покращив технологію ідентифікації пристроїв, розроблену в попередньому техніко-економічному обґрунтуванні фази 1 SME Instrument Phase 1 з такою ж назвою. Новий проект підтвердив комерційний потенціал концепції.

Представлений інноваційний метод спочатку призначає ідентифікатор кожному пристрою IoT на основі його унікальних фізичних характеристик. Фізичні ідентифікатори отримуються за допомогою спеціальних алгоритмів, які вимірюють випадкові варіації, що генеруються в процесі виробництва обладнання, за допомогою фізичної неклонованої функції (PUF), розробленої в рамках проекту. Це відоме як кремнієва біометрична інформація, і, по суті, відбитки пальців кожного пристрою IoT неможливо підробити.

Після того, як кожен пристрій має ідентифікатор, перш ніж стане можливим безпечний обмін даними, ідентифікатор має бути аутентифікований. Інакше не можна гарантувати, що пристрої зв'язуються з правильною стороною. Можливість перевіряти ідентичність пристрою – це те, що дозволяє захищати прості пристрої Інтернету речей.

PUF є компонентом системи безпеки INSTET. Він покращує всю систему безпеки за допомогою потужних і непідробних високоякісних служб безпеки. Головна перевага полягає в тому, що не потрібно програмувати кореневий ключ ззовні. Отже, ключ завжди залишається всередині, і тому завжди в безпеці.

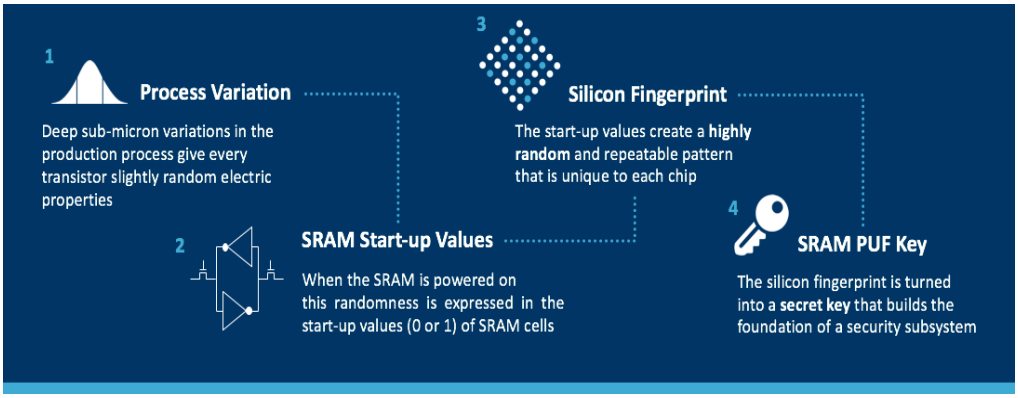

Рис.1 – Вилучення безпечного ключа з внутрішнього кремнієвого відбитка пальця

Крім того, PUF заснований на повсюдно поширених схемах статичної пам'яті з довільним доступом (SRAM). Підхід можна масштабувати до всіх пристроїв IoT — оскільки SRAM є компонентом усіх мікроконтролерів, навіть недорогих. В результаті ми можемо модернізувати ті мільйони пристроїв IoT, які встановлені в польових умовах, не вимагаючи переробки продуктів.

Це єдине рішення на ринку, яке забезпечує надійну апаратну безпеку, використовуючи лише програмне забезпечення, яке легко розгортається на пристроях IoT з обмеженою потужністю обробки.

Система орієнтована на три окремі сегменти IoT. INSTET Wearables забезпечує повну безпеку для переносних пристроїв. INSTET Medical підтримує зв'язування програмного забезпечення з апаратним забезпеченням медичного пристрою. Нарешті, INSTET Critical Infrastructures підтримує хмарне підключення IoT. Дослідники успішно створили різні архітектури програмного забезпечення для кожної програми. Команда також створила та керувала демонстраторами для кожного сегмента ринку. Співробітники проекту розробили детальний аналіз ринку та плани експлуатації.

Далі консорціум зосереджений на розробці ринкових стандартів і правил. Результатом стане усунення серйозної слабкості безпеки, яка впливає на пристрої IoT.

Список посилань

1. Bkheet, S. Огляд методів ідентифікації Інтернету речей (IOT). / Bkheet, S., Agbinya, J. – Досягнення в Інтернеті речей, 2021. – 153-174 с.

2. Захист Інтернету речей за допомогою унікальної технології відбитків пальців мікрочіпа [Електронний ресурс]. – Режим доступу: https://cordis.europa.eu/article/id/422611-innovative-identification-methods-secure-iot-devices

3. Sram PUF Технологія [Електронний ресурс]. – Режим доступу: https://www.intrinsic-id.com/sram-puf/

УДК 629.7.01:629.734/735:331.101.1

Козир А.Г., канд. техн. наук,
Зройчиков Д.В.,
Шабанов Д.М.,
Державний НДІ випробувань і сертифікації озброєння та військової техніки, м. Чернігів,
niv_dndi@ukr.net

ОЦІНКА АЛГОРИТМІВ ДІЯЛЬНОСТІ ЧЛЕНІВ ЕКІПАЖУ ПОВІТРЯНОГО СУДНА МЕТОДОМ ПОБУДОВИ ЦИКЛОГРАМИ

Під час проведення випробувань авіаційної техніки велике значення має оцінка алгоритмів діяльності членів екіпажу повітряного судна (операторів). Зважаючи на те, що дана оцінка є завданням великої складності, то найчастіше аналізу піддається не весь алгоритм, а його складові частини стосовно конкретних етапів, а також структура і якість діяльності оператора на цих етапах.

При оцінці алгоритму використовують показники зовнішньої і внутрішньої структури діяльності і дій, їх кількість, склад, послідовність, часові характеристики виконання дій тощо. Для підтвердження правильності вибору конструктивного рішення системи “людина-машина” для кожної гілки загального алгоритму будуються та аналізуються циклограми взаємодії оператора і “машини”.

Циклограма дає змогу наочно оцінити упорядкування елементарних операцій оператора з органами управління і приладами, і дозволяє розрахувати часові витрати на взаємодію, а також оцінити очікувану темпову напруженість діяльності в конкретному режимі функціонування системи “людина-машина”.

Резерв часу на виконання операцій, а також темпова напруженість (комфортна і гранична) дають уявлення про якість циклограми. Зрозуміло, що вказані часові витрати, рівно, як і очікувана темпова напруженість взаємодії між оператором і “машиною”, повинні бути однаково вимірюванні і пов’язані з часовими параметрами діяльності оператора у складі всієї системи “людина-машина”.