Overview of the Contemporary Hardware Design Weaknesses

M. Yu. Krichanov <krichanov@ispras.ru>
Ivannikov Institute for System Programming
Moscow, Russia

Abstract. This research gives an overview of hardware design weaknesses relevant to the industry leaders (Intel, AMD, ARM). Based on the analyzes of the Common Weakness Enumeration List, this paper consistently outlines the main ideas of various attacks and appropriate design countermeasures.

Keywords: hardware design weaknesses; CWE; Intel; AMD; ARM.

Обзор актуальных аппаратных уязвимостей

М. Ю. Кричанов <krichanov@ispras.ru>
Институт системного программирования РАН
Москва, Россия

Аннотация. Цель данного исследования – это обзор аппаратных уязвимостей актуальных для флагманов индустрии (Intel, AMD, ARM). В данной работе последовательно изложены основные идеи разнообразных атак и конструктивных методов противодействия им, список которых был сформирован в результате анализа базы данных аппаратных уязвимостей (CWE).

Ключевые слова: аппаратные уязвимости; CWE; Intel; AMD; ARM.

Введение

В 1999 году под эгидой некоммерческой организации MITRE началась работа по созданию базы данных угроз компьютерной безопасности под названием CVE (Common Vulnerabilities and Exposures List) [1]. По мере наполнения базы данных и систематизации уязвимостей была выработана их классификация, получившая название CWE (Common Weakness Enumeration List). С момента своего создания и вплоть до 2020 года эта классификация описывала только программные уязвимости. Уязвимости аппаратного обеспечения находились на периферии внимания отраслевого сообщества вплоть до 2018 года, когда было обнаружено, что спекулятивное исполнение кода позволяет обойти аппаратные гарантии изоляции процессов с разными уровнями привилегий. Поскольку спекулятивное исполнение является одним из основных способов увеличения быстродействия современных высокопроизводительных процессоров, эта проблема сразу стала глобальной. Масштаб угрозы привлёк внимание отрасли к проблемам безопасности аппаратного обеспечения, что выразилось в создании баз данных аппаратных уязвимостей крупнейшими разработчиками процессоров для своих продуктов [2, 3]. Закономерным следствием возросшего интереса к проблематике стало расширение CWE классификации и на аппаратные уязвимости в 2020 году. Поскольку классификация CWE стремится описать все известные уязвимости аппаратуры, она содержит в том числе и уязвимости, давно потерявшие актуальность для современных высокопроизводительных процессоров, такие как: недостаточная надёжность аппаратуры (CWE-1248), отсутствие документации (CWE-1059), отсутствие защиты от отката к предыдущей версии (CWE-1328), отсутствие аппаратного корня доверия (CWE-1326), отсутствие криптографических примитивов (CWE-1318) или их неполная реализация (CWE-325), использование недостаточно стойких криптографических алгоритмов (CWE-1240) и недостаточно случайных источников энтропии (CWE-1241), отсутствие механизма защитной блокировки настроек безопасности (CWE-1233). Данные архитектурные недоработки, будучи неактуальными для лидеров индустрии, остаются на повестке дня встраиваемой электроники, заточенной под узко специальные задачи и жёстко ограниченной в ресурсах.

Цель данного исследования – это обзор аппаратных уязвимостей актуальных для флагманов индустрии (Intel, AMD, ARM). В рамках данной работы была проанализирована база данных аппаратных уязвимостей [4] и на основании ссылочного аппарата этой базы данных был сформирован набор первоисточников. В результате анализа оригинальных статей удалось разделить всё множество аппаратных уязвимостей на следующие укрупнённые категории, исходя из специфики физического взаимодействия злоумышленника с аппаратурой и атакуемых компонентов:

- Побочные эффекты на микроуровне.
- Электромагнитное излучение (VGA, HDMI, DisplayPort).
- Акустические колебания.
- Анализ энергопотребления.
- Периферийные устройства.
- Оперативная память.
- DMA.

- Аппаратное шифрование.
- Разделяемые ресурсы как сторонние каналы.
- Спекулятивное исполнение.
- TPM.
- BIOS.
- TEE.
- Внедрение ошибок.

В докладе будут представлены основные идеи перечисленных категорий атак, а также рекомендации для разработчиков ОС по противодействию этим атакам на конструктивном уровне. Работа выполнена в рамках совместных исследований ИСП РАН и Лаборатории Касперского.

Список литературы

[1] Common Weakness Enumeration [Электронный ресурс]. URL: https://cwe.mitre.org/about/history.html (дата обращения: 4.05.2025).

[2] Software Security Guidance [Электронный ресурс]. URL: https://www.intel.com/content/www/us/en/developer/topic-technology/software-security-guidance/advisory-guidance.html (дата обращения: 4.05.2025).

[3] Arm Security Center [Электронный ресурс]. URL: https://developer.arm.com/Arm%20Security%20Center (дата обращения: 4.05.2025).

[4] CWE VIEW: Hardware Design [Электронный ресурс]. URL: https://cwe.mitre.org/data/definitions/1194.html (дата обращения: 4.05.2025).