УДК 004.8:004.056.54

ПРИМЕНЕНИЕ ИИ-АГЕНТОВ В ДОВЕРЕННОЙ ЭЛЕМЕНТНОЙ БАЗЕ ДЛЯ ПРЕДИКТИВНОГО ОБНАРУЖЕНИЯ АППАРАТНЫХ АТАК

А.О. Пилипенко, Ф.Н. Супрун

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В данной статье рассматривается вопрос о защите элементной базы с помощью встроенных ИИ-агентов. В работе анализируется, как ИИ могут находить аппаратные закладки и предотвращать атаки по внешним каналам. Данный подход позволяет сделать защиту элементной базы автоматической и более эффективно.

Ключевые слова: элементная база, защита информации, искусственный интеллект, ИИ-агент, аппаратные средства защиты, кибербезопасность, аппаратный троян, мониторинг сигналов, микросхемы, информационная безопасность.

APPLICATION OF AI AGENTS IN A TRUSTED HARDWARE COMPONENTS FOR PREDICTIVE DETECTION OF HARDWARE ATTACKS.

A.O. Pilipenka, F.N. Suprun
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. This article examines the protection of hardware components using embedded AI agents. It analyzes how AI can detect hardware bugs and prevent attacks through external channels. This approach makes hardware protection more automated and effective.
Keywords: element base, information protection, artificial intelligence, AI agent, hardware protection, cybersecurity, hardware Trojan, signal monitoring, microcircuits, information security.

Введение

Сегодня элементная база является защитой любой информационной системы, но она чаще всего используется аппаратными атаками. Обычные методы защиты, работающие по заранее прописанным правилам, не всегда могут привести к скрытым угрозам внутри системы. Решением этой проблемы может стать внедрение технологий искусственного интеллекта прямо в аппаратную часть устройства. В данной работе исследуется, как именно такие интеллектуальные компоненты помогают защитить элементные базы и повысить надежность цифровых систем.

Основная часть

Сегодня практически каждое электронное устройство, начиная от обычного смартфона и заканчивая промышленных контроллеров, работает на базе микросхем, которые мы называем элементной базой. Все время считалось, что если программное обеспечение защищено антивирусом или шифрованием, то системе никакая опасность не угрожает. Однако сейчас все чаще говорят об аппаратных атаках, когда злоумышленники пытаются взломать само «железо».

Одной из самых опасных угроз являются аппаратные трояны. Это небольшие изменения в логике работы чипа, которые могут произойти еще во время производства. Такой троян может годами «спать», а затем активироваться по специальному сигналу злоумышленника и передать секретный ключ шифрования хакеру. Главное, как раз то, что найти такую закладку обычными методами практически невозможно из-за большой сложности как раз самих микросхем [1]. Защита «железа» заметно эволюционировала: все началось с обычных проверок данных, таких как контрольные суммы, а по итогу все пришло к созданию чипов TMP. Эти чипы сегодня – отличная база для безопасности компьютера.

В наше время на помощь приходит искусственный интеллект. Если мы встроим небольшой ИИ-агент прямо в сам чип, он сможет работать как внутренний «цифровой охранник». То есть вместо того, чтобы работать по строгим правилам, ИИ-агент самообучается и действует по ситуации. В такой элементной базе выделяют три принципах: предиктивности (предсказании атак), автономности (самостоятельное принятие решений на основе конкретной ситуации) и верифицируемости (подтверждении надежности ИИ-агента).

ИИ-агент работает так: он запоминает, как ведет себя «здоровый» процессор. Например, сколько он потребляет энергии, какова скорость передачи данных и как часто процессор взаимодействует с памятью. Если параметры начинают отклоняться от нормы, например, если энергопотребление резко меняется в момент простоя, то ИИ-агент понимает, что происходит что-то подозрительное [2]. Технически это реализуется через систему сенсоров, собирающих телеметрию (температуру кристалла, тактовую частоту), и моделей ИИ, которые выделяют закономерности атаки среди обычного шума.

Еще один важный момент – это атаки по сторонним каналам (side-channel analysis) [3]. Хакеры научились «слушать» микросхемы, анализируя их электромагнитное излучение или шум в цепях питания. Таким образом можно буквально узнать, какой пароль или ключ обрабатывает чип в данный момент. Обычный контроллер этого не замечает, но интеллектуальный агент постоянно анализирует сигналы «аппаратных логов», поэтому может зафиксировать такого рода кражу информации.

Сложность как раз во внедрении ИИ-агента. Конечно, полноценную нейросеть в маленький чип интегрировать сложно, так как ресурсов (память и питание) просто не хватает. Поэтому в работе используются «легкие» алгоритмы машинного обучения, которые сильно не нагружают устройства. Перспективным направлением здесь является нейроморфная защита на базе спайковых нейронных сетей (Spiking Neural Networks), которые имитируют строение и работу мозга, а также позволяют работать быстро при крайне низком энергопотреблении.

Однако развитие таких систем сталкивается с новыми проблемами, такими как состязательное машинное обучение (Adversarial ML). Злоумышленники могут пытаться «обмануть» ИИ-агента. Хакеры начинают подсовывать ему искаженные данные сенсоров, чтобы скрыть наличие каких-либо неполадок.

На сегодняшний день концепция интеллектуальной защиты на аппаратном уровне уже активно внедряется лидерами ИТ-индустрии. Одним из наиболее известных примеров является технология Intel Threat Detection Technology (Intel TDT). В процессорах Intel Core (начиная с 10-го

поколения) используются блоки телеметрии, которые передают данные о работе процессора в модели машинного обучения. Это позволяет обнаруживать программы-вымогатели (ransomware) и скрытый майнинг криптовалют на уровне микроархитектуры, до того, как их заметит антивирус. В промышленном секторе такие компании, как NVIDIA (блок BlueField DPU) и NXP Semiconductors, разрабатывают специализированные блоки аппаратного ускорения ИИ, которые встроены в сетевые контроллеры.

Заключение

В ходе работы было доказано, что внедрение ИИ-агентов в элементную базу – это отличный способ защиты от скрытых аппаратных угроз. Благодаря постоянному анализу физических параметров, таких как энергопотребление и тайминги, ИИ способны находить аппаратные закладки, которые незаметны на первый взгляд и могут быть недоступны для заранее прописанного программного обеспечения. Разработка такого подхода к защите становится важным этапом в обеспечении безопасности электроники.

Список использованных источников

1. Грибунин В. Г., Васильев С. А. Цифровая стеганография и защита элементной базы. – СПб.: Солон-Пресс, 2021. – 256 с.

2. Безродный Б. Ф. Интеллектуальные системы защиты информации в микроэлектронике // Вестник кибербезопасности. – 2023. – № 2. – С. 15-22.

3. Куприянов М. С. Проектирование защищенных микропроцессорных систем. – СПб.: БХВ-Петербург, 2020. – 320 с.

References

1. Gribunin V. G., Vasiliev S. A. Digital Steganography and Protection of the Element Base. St. Petersburg: Solon-Press, 2021. 256 p.

2. Bezrodny B. F. Intelligent Information Security Systems in Microelectronics // Cybersecurity Bulletin. 2023. No. 2. pp. 15-22.

3. Kupriyanov M. S. Design of Secure Microprocessor Systems. St. Petersburg: BHV-Petersburg, 2020. 320 p.

Сведения об авторах

Пилипенко А.О., курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», pilipenkoandrej602@gmail.com.

Супрун Ф.Н., преподаватель, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», f.suprun@gmail.com

Information about the authors

Pilipenko A. O., cadet, Educational Institution "Belarusian State University of Informatics and Radioelectronics", pilipenkoandrej602@gmail.com.

Suprun, teacher, Educational Institution "Belarusian State University of Informatics and Radioelectronics", f.suprun@gmail.com