МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
РАДІОЕЛЕКТРОНІКИ

МАТЕРІАЛИ 28-го МІЖНАРОДНОГО
МОЛОДІЖНОГО ФОРУМУ

«РАДІОЕЛЕКТРОНІКА ТА МОЛОДЬ У XXI СТОЛІТТІ»

16 – 18 квітня 2024 р.

Том 3

КОНФЕРЕНЦІЯ «ІНФОРМАЦІЙНІ РАДІОТЕХНОЛОГІЇ ТА ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ»

Харків 2024

УДК 004.31

ПРОБЛЕМАТИКА КІБЕРБЕЗПЕКИ В ПРИСТРОЯХ FPGA

Мітрофанов С. В.
Науковий керівник – асистент Білоцерківець О.Г.
Харківський національний університет радіоелектроніки, каф. МТС,
м. Харків, Україна
тел. +38057-702-0229, e-mail: d_mts@nure.ua

This article navigates the intricate terrain of FPGA cybersecurity, delineating the challenges posed by their hybrid nature and the evolving threat landscape. Exploring various attack vectors—from active disruptions to passive data extraction-it underscores the imperative for a multi-layered defense strategy. With insights into defense mechanisms, including dynamic adaptation and post-quantum preparedness, the article advocates for proactive measures to fortify FPGA-based systems against emerging cyber threats.

Програмовані логічні інтегральні схеми (FPGA) займають унікальне місце в області цифрової електроніки, пропонуючи синтез гнучкості програмного та апаратного забезпечення, який не має собі рівних у традиційних інтегральних схемах (IC). Ця гібридна природа робить їх одночасно універсальними інструментами для інновацій і привабливими цілями для кібератак. Останніми роками сфера кібербезпеки, що оточує FPGA, стає дедалі складнішим через розвиток загроз, розширення поверхонь атак і нових технологій, таких як квантові обчислення.

ПЛІС втілюють унікальне поєднання програмованої логіки та реконфігурованого апаратного забезпечення, що дозволяє розробникам пристосовувати їхню функціональність до конкретних програм. Хоча ця гнучкість сприяє інноваціям і адаптивності, вона також створює природні вразливості, якими можуть скористатися зловмисники. Динамічний характер конфігурацій FPGA створює проблеми для підтримки цілісності та безпеки цих пристроїв [1].

Оскільки FPGA інтегруються в різноманітні додатки, починаючи від аерокосмічних і оборонних систем до споживчої електроніки, складність екосистем, у яких вони працюють, зростає експоненціально. Ця складність виходить за межі самих FPGA і охоплює всю архітектуру системи, включаючи периферійні пристрої, протоколи зв’язку та програмні інтерфейси. Кожен компонент додає потенційні вектори атак, що посилює завдання захисту систем на основі FPGA від зловмисників.

Поява квантових обчислень створює фундаментальну загрозу звичайним криптографічним алгоритмам, які складають основу заходів безпеки FPGA. Схеми шифрування, які вважаються надійними проти класичних обчислень, можуть піддаватися квантовим атакам, роблячи конфіденційні дані вразливими до компрометації. У зв’язку з наближенням термінів створення життєздатних квантових обчислювальних можливостей терміновість

вирішення проблеми постквантової безпеки в пристроях FPGA стає обов'язковою.

До основних типів атак належать наступні:

- активні атаки мають на меті порушити нормальну роботу пристроїв FPGA шляхом зміни їх конфігурацій або впровадження шкідливих інструкцій;

- пасивні атаки прагнуть отримати конфіденційну інформацію з систем на основі FPGA, не змінюючи їх поведінку, використовуючи такі методи, як аналіз бічних каналів і витік інформації;

- атаки підміни включають втручання в бітовий потік FPGA, заміну законних конфігурацій шкідливими для отримання несанкціонованого контролю над пристроєм.

Основні стратегії захисту які слід застосовувати:

- багаторівневий підхід: ефективна безпека FPGA вимагає багаторівневої стратегії захисту, яка включає шифрування, автентифікацію, контроль доступу та механізми виявлення вторгнень. Розгортаючи кілька рівнів захисту, організації можуть створювати надлишкові бар'єри для запобігання кібератакам і пом'якшення їхнього впливу [2];

- динамічна адаптація: використання динамічних криптографічних схем і гнучких протоколів безпеки дозволяє пристроям FPGA адаптуватися до нових загроз у режимі реального часу. Криптошвидкість, здатність плавно переходити між криптоалгоритмами та протоколами, підвищує стійкість систем на основі FPGA до нових кіберзагроз;

- програмовані блоки безпеки: включення програмованих блоків безпеки в архітектури FPGA дозволяє організаціям швидко реагувати на виклики постквантової безпеки. Ці адаптивні модулі безпеки можна віддалено оновлювати для усунення нових вразливостей і застосування заходів протидії квантовим атакам.

Захист пристроїв FPGA від кіберзагроз вимагає цілісного підходу, який поєднує надійні заходи безпеки, динамічні стратегії адаптації та співпрацю між зацікавленими сторонами галузі. Усуваючи притаманні вразливості FPGA, передбачаючи нові загрози, такі як квантові обчислення, і застосовуючи гнучкі практики безпеки, організації можуть захистити свої цифрові активи та підтримувати довіру до систем на основі FPGA серед загроз, що розвиваються.

Список використаних джерел:

1.Xilinx.com: [Інтернет-портал]. URL: https://www.xilinx.com/products/technology/ design-security.html (дата звернення: 22.02.2024).

2. Воргуль О.В., Білоцерківець О.Г. Поліпшений захист мікроконтролера від читання // III форум «Автоматизація, електроніка та робототехніка. Стратегії розвитку та інноваційні технології» AERT-2021. Харків, ХНУРЕ, 2021. С. 34-35.