УДК 004.312.466.056.5:004.415.53 **doi: 10.32620/aktt.2023.6.11**

А. Г. ТЕЦЬКИЙ

Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

ТЕСТУВАННЯ НА ПРОНИКНЕННЯ КОМПОНЕНТІВ FPGA ЯК СЕРВІСУ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Предметом *вивчення в даній статті є сучасні технології тестування на проникнення, де об'єктом тестування є платформа з доступом до FPGA-ресурсів.* ***Метою*** *роботи є вдосконалення сучасних методів тестування на проникнення сервісів, що надають послугу FPGA as a Service, для виявлення вразливостей, ліквідація яких підвищує рівень захищеності сервісів та підвищує рівень довіри користувачів до таких сервісів.* ***Завдання:*** *проаналізувати можливі загрози платформ FPGA as a Service; проаналізувати структуру платформ FPGA as a Service; проаналізувати варіанти використання стандарту проведення тестування на проникнення; запропонувати ключові складові забезпечення кібербезпеки платформ FPGA as a Service. Відповідно до поставлених завдань, були отримані наступні* ***результати****. Проведено дослідження проблем кібербезпеки платформ FPGA as a Service та пропонується комплекс складових забезпечення кібербезпеки платформ FPGA as a Service. Проведено аналіз актуальних загроз кібербезпеки платформ FPGA as a Service. Розглянуто можливість застосування стандарту проведення тестування на проникнення стосовно сервісів FPGA. Регулярне проведення аудиту та тестування на проникнення є ключовим елементом стратегії кібербезпеки та допомагає підтримувати довіру клієнтів та користувачів до FPGA сервісів. Запропоновано комплекс складових забезпечення кібербезпеки платформ FPGA as a Service, що відповідає сучасним загрозам. Комплекс містить в собі такі заходи як регулярне оновлення ПЗ, моніторинг та аналіз безпеки, аудит та тестування на проникнення, відповідність стандартам безпеки, навчання персоналу.* ***Висновки:*** *Головний внесок і наукова новизна отриманих результатів полягає в тому, що проведено дослідження можливостей тестування на проникнення, де об'єктом тестування є платформа з доступом до FPGA-ресурсів. Як і в багатьох інших сферах, забезпечення кібербезпеки платформ FPGA as a Service є комплексною задачею, де ігнорування будь-якої складової може привести до критичних наслідків. Застосування лише тестування на проникнення є недостатнім, тому надано вичерпний перелік заходів забезпечення кібербезпеки платформ FPGA as a Service.*

Ключові слова: *FPGA; FPGA як сервіс; тестування на проникнення; забезпечення кібербезпеки; заходи захисту.*

Вступ

Сучасний світ важко уявити без обчислень. Кількість переданих, збережених та оброблюваних даних постійних зростає, технології постійно вдосконалюються. Одним із способів енергоефективного та досить швидкого вирішення обчислювальних завдань є використання FPGA-ресурсів.

FPGA (Field-Programmable Gate Array) як сервіс (FaaS) є хмарною моделлю, що надає користувачам доступ до FPGA-ресурсів через Інтернет. Це дозволяє клієнтам використовувати гнучкі та потужні FPGA-ресурси для спеціалізованих обчислювальних завдань, таких як обробка даних, машинне навчання та криптографія, без необхідності фізично встановлювати та підтримувати апаратне забезпечення [1].

FPGA сервіси дають можливість космічним агентствам та приватним компаніям використовувати ресурси хмарних платформ для проектування, тестування та оптимізації апаратних систем, що значно скорочує час розробки та витрати, пов'язані із запуском космічних апаратів. Вони ідеально підходять для космічної галузі, оскільки FPGA можуть бути перепрограмовані в реальному часі для виконання різних функцій, що особливо важливо за умов динамічних завдань та невизначених умов [2].

Практично будь-який ресурс, доступний у всесвітній мережі, може бути об'єктом атак для зловмисників. Платформи, що надають FPGA as a Service, не є винятком. Тому актуальною є задача дослідження проблем кібербезпеки FPGA as a Service, виявлення можливих атак та способів захисту від них.

Метою даної роботи є вдосконалення сучасних методів тестування на проникнення сервісів, що надають послугу FPGA as a Service, для виявлення вразливостей, ліквідація яких підвищує рівень захищеності сервісів та підвищує рівень довіри корис-

ISSN 1727-7337 (print)
ISSN 2663-2217 (online)

тувачів до таких сервісів.

Для досягнення поставленої мети, в рамках даної роботи, розглядаються та вирішуються наступні **задачі**:

1) проаналізувати можливі загрози платформ FPGA as a Service;

2) проаналізувати структуру платформ FPGA as a Service;

3) проаналізувати варіанти використання стандарту проведення тестування на проникнення;

4) запропонувати ключові складові забезпечення кібербезпеки платформ FPGA as a Service.

1. Аналіз можливих загроз для платформ FPGA as a Service

У зв'язку з потребою в ефективних обчисленнях високої продуктивності, сучасні комп'ютерні архітектури часто поєднують центральні обробні пристрої (CPU), графічні обробні пристрої (GPU) і програмовані вентильні матриці (FPGA). Однак кожен із цих компонентів піддається ризикам безпеки на електричному рівні. Перехід до гетерогенних систем, включаючи можливість розрахованої на багато користувачів експлуатації, вимагає розуміння і вивчення того, як вразливості безпеки окремих компонентів можуть впливати на систему в цілому [3].

Безпека програмованих логічних інтегральних схем є ключовим питанням, оскільки будь-яка вразливість в апаратному забезпеченні може мати серйозні наслідки, якщо вони використовуються в захищених проектах. Оскільки проекти ПЛІС кодуються як бітового потоку, забезпечення безпеки цього бітового потоку має вирішальне значення. Зловмисники можуть мати безліч мотивів відновлення і маніпулювання бітовим потоком, включаючи клонування конфігурації (design cloning), крадіжку інтелектуальної власності, маніпуляцію з проектом або його компрометацію (design subversions), наприклад, через апаратні троянські програми. Враховуючи, що ПЛІС часто використовуються в кіберфізичних системах, наприклад, в авіаційній, медичній або промисловій техніці, це може призвести навіть до фізичних негативних наслідків. В результаті виробники ввели шифрування бітового потоку, що забезпечує його справжність та конфіденційність. Незважаючи на те, що в минулому було запропоновано атаки проти шифрування бітового потоку, для їх здійснення потрібне складне обладнання та значна технічна експертиза. У статті [4] представлені нові недорогі атаки проти шифрування бітового потоку Xilinx 7-Series (і Virtex-6), в результаті яких повністю втрачається справжність та конфіденційність. Така вразливість отримала назву Starbleed.

Іншою відомою вразливістю стала Thangrycat – нещодавно виявлена вразливість у маршрутизаторах Cisco, що дозволяє зловмисникам компрометувати довірений обчислювальний модуль роутера. Це призводить до можливості непомітного запуску шкідливого програмного забезпечення та робить практично неможливим видалення шкідливого програмного забезпечення після його встановлення. Thangrycat використовує можливість виконання процесів з правами системного адміністратора, і компанія Red Balloon, що розкрила вразливість, також виявила дефект, що дозволяє зловмисникам запускати код з правами адміністратора [5].

Актуальними є дослідження рішень на основі конфігурації, де є ще одна серйозна загроза безпеці FPGA – підробка бітового потоку. Втручання в бітовий потік дозволяє зловмисно модифікувати конструкції FPGA, дозволяючи зловмиснику скомпрометувати апаратний корінь довіри та обійти будь-які механізми безпеки програмного рівня. Щоб запобігти цьому, багато постачальників включають різні апаратні блоки для забезпечення довіри та автентичності файлів бітового потоку. Однак за останнє десятиліття було опубліковано все більше досліджень і експлойтів, які демонструють, як обійти ці засоби захисту та використовувати модифіковані бітові потоки для включення операцій FPGA [6]. У недавньому прикладі втручання в реальний бітовий потік маршрутизатор корпоративного рівня Cisco був включений через зловмисні модифікації бітового потоку. Ця атака на маршрутизатор Cisco на основі FPGA вплинула на ціле покоління продуктів Cisco, і її неможливо виправити без оновлення апаратного забезпечення. Показано, що цю атаку можна здійснити віддалено – без фізичного доступу до пристрою. Такі атаки, як Thangrycat, є суттєвим розвитком безпеки FPGA, оскільки вони дають можливість віддаленого використання. Оскільки FPGA дедалі частіше використовуються в мережі, як-от екземпляри Amazon EC2 F1 для хмарних обчислень FPGA, вкрай важливо, щоб методи безпеки FPGA перейшли від моделі «надійного середовища» до моделі, яка залишається чутливою після проектування та розгортання системи.

Традиційно сучасні FPGA використовують різноманітні пасивні засоби захисту для захисту конфігурації. Сучасні ПЛІС, наприклад Xilinx 7-ї серії та сімейств пристроїв пізнішої версії, реалізують такі функції безпеки, як теги Hashed-Message-Authentication-Code (HMAC) і шифрування AES у форматі бітового потоку. Було доведено, що ці статичні засоби захисту сприйнятливі до зворотного проектування та вилучення ключів [7].

Вразливості безпеки, такі як трояни FPGA або зловмисна логіка конфігурації, впроваджена в ди-

зайн FPGA, були в центрі уваги значної кількості досліджень безпеки FPGA як в наукових колах, так і в промисловості. Популярні засоби пом'якшення загроз апаратних троянів часто включають ідентифікацію таких шкідливих схем. Проте традиційні підходи до виявлення троянів часто припускають, що зловмисник не може внести цільові зміни в базову логіку конфігурації, яка може бути використана для виявлення потенційної шкідливої діяльності. Таким чином, зловмисні зміни файлів конфігурації бітового потоку можуть залишитися непоміченими та призвести до агресивної поведінки FPGA.

У роботі [8] представлені результати порівняння комерційно доступних рішень для побудови сервісів з прискорювачами FPGA. Обговорюються переваги платформи та інструментів Xilinx для створення сервісу FPGA. Запропоновано етапи створення рішень на основі FaaS. Перераховано деякі завдання, пов'язані з FaaS, та обговорюються тенденції розвитку. Розглядається платформа SDAccel сімейства Xilinx SDx, а також можлива роль цих інструментів у створенні платформи FPGA обчислень як сервісу.

Усе вищезазначене підтверджує актуальність задачі дослідження можливостей застосування усталених підходів до тестування на проникнення, де об'єктом тестування є платформа з доступом до FPGA-ресурсів. Виявлені особливості дозволять визначити найімовірніші способи порушення конфіденційності, цілісності чи доступності.

2. Специфіка застосування FPGA

Розглянута у статті [9] архітектура FPGA as a Service складається з наступних шарів (рис. 1):

– FPGA as a Service – онлайн-ресурс із веб-інтерфейсом, куди завантажується проект;

– Dedicated Host – виділена машина (або кілька) із встановленим Ubuntu;

– FPGA Accelerator Card – модуль, що підключається до материнської плати (PCIe);

– FPGA Chip – один із чіпів на модулі.

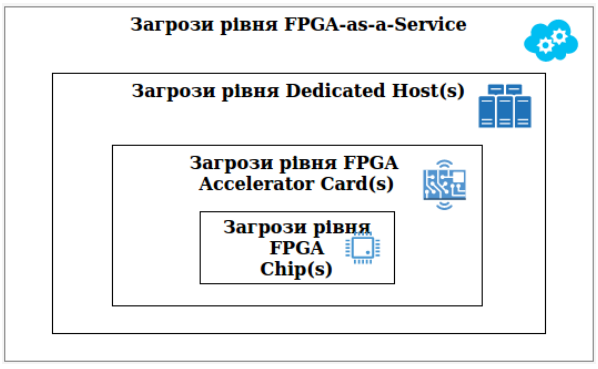

Рис. 1. Рівні загроз архітектури FPGA as a Service

Як правило, що вищий рівень системи, то легше знайти спосіб її атакувати. У системі, що розглядається, верхнім рівнем є web-сервіс, тому найбільша увага буде приділена атакам, реалізація яких можлива на цьому рівні.

Атаки на сервіс FPGA можуть бути різноманітними, враховуючи унікальні характеристики FPGA, так і загальні вразливості хмарних і мережевих сервісів. Варто виділити кілька атак та способів їх реалізації:

1. Атаки на конфіденційність. Оскільки FPGA обробляють дані клієнтів, існує ризик витоку конфіденційної інформації, особливо якщо дані не зашифровані або система не є належним чином ізольована. Зловмисник може спробувати перехопити або вкрасти конфіденційні дані на FPGA.

2. Атаки на цілісність. Зловмисники можуть спробувати змінити дані або алгоритми, запущені на FPGA, що призведе до невірних результатів або шкідливих наслідків. Також можливе отримання доступу до функцій контролю фізичного пристрою. Можливі маніпуляції з конфігурацією FPGA для досягнення несанкціонованих чи шкідливих цілей.

3. Атаки на доступність. DDoS-атаки можуть бути спрямовані на сервіс FPGA, що призведе до його навантаження та недоступності для клієнтів.

Як і багато інших систем, сервіси FPGA можуть включати два види вразливостей – вразливості програмного забезпечення і апаратні вразливості. Програмні вразливості – вразливості у програмному забезпеченні, що використовується для конфігурації та управління FPGA, наприклад, застарілі версії програмного забезпечення, неправильна обробка вхідних даних, вразливість у протоколах передачі даних тощо. Вразливості на апаратному рівні можуть включати проблеми з фізичною безпекою пристроїв, вразливості в процесі виробництва FPGA, такі як недоліки у схемотехніці або виробничих процесах, які можуть бути експлуатовані для несанкціонованого доступу або пошкодження пристрою.

Пошук вразливостей – обов'язковий етап тестування програм критичного призначення. З розвитком технологій розробки підвищується і якість продуктів, що розробляються. У зв'язку з цим можна припустити, що знижується можливість виявлення критичної вразливості в розробленому продукті. Тоді в парі "людина-система" слабкішою ланкою може бути людина.

Якщо використання відомих вразливостей у програмному забезпеченні або апаратних засобах, пов'язаних з FPGA, неможливе, то зловмисниками можуть бути застосовані методи соціальної інженерії. Такі методи включають обман або маніпулювання персоналом для отримання доступу або конфіденційної інформації. Можливе отримання досту-

ISSN 1727-7337 (print)
ISSN 2663-2217 (online)

пу до облікових записів через фішинг, перехоплення трафіку тощо.

Також слід згадати про те, що виділена машина із встановленим FPGA-модулем є частиною мережевої інфраструктури. Атаки мережної інфраструктури можуть проводитися для перенаправлення, зміни або блокування даних, що може призвести до порушень роботи FPGA-сервісу. Також може відбуватися експлуатація вразливостей у програмному забезпеченні, яке не має прямого відношення до FPGA, але використовується на виділеній машині.

3. Аналіз варіантів використання стандарту проведення тестування на проникнення

Тестування на проникнення FPGA сервісів – це процес ідентифікації та експлуатації вразливостей у системах, що використовують FPGA, для оцінки рівня безпеки. Це включає аналіз як апаратних, так і програмних аспектів системи. Основними етапами тестування на проникнення є [10]:

1. Попередня взаємодія. Визначення цілей тестування, планування та визначення обсягу робіт. Встановлення меж тестування, включаючи визначення тестових середовищ та компонентів системи. Можливо, замовник має бажання проводити тестування у неробочий час, коли навантаження на систему мінімальне та можливі збої не заважатимуть роботі ресурсу з обслуговування клієнтів. Також на цьому етапі фіксуються можливі проблеми під час тестування. Це питання є важливим, оскільки проведення автоматизованого тестування призводить до збільшення навантаження на ресурс, це, у свою чергу, може стати причиною відмови в обслуговуванні. Також потрібно розробити варіанти якнайшвидшого відновлення працездатного стану для мінімізації можливих втрат під час простою.

2. Збір інформації. У разі проведення тестування чорної або сірої скриньки може бути корисною будь-яка інформація, що стосується об'єкта тестування. Виконується сканування портів, визначається програмне забезпечення та їх версії, збирається інформація про відомі вразливості у виявлених версіях ПЗ. Якщо тестування на проникнення включає методи соціальної інженерії, також збирається інформація про осіб, які мають або можуть мати адміністраторські права доступу. Надалі ця інформація може бути використана для створення словників паролів. Розуміння того, як влаштована FPGA система та які вразливості можуть бути пов'язані з її конкретною архітектурою, є перевагою. Також аналізується мережа FPGA-ресурсу та які мережеві вразливості можуть бути експлуатовані.

3. Ідентифікація вразливостей. На цьому етапі необхідне використання автоматизованих інструментів та ручних методів для виявлення потенційних вразливостей. Необхідно провести перевірку налаштувань та конфігурацій FPGA щодо наявності вразливостей. На цьому етапі максимальну увагу варто приділити вразливості верхнього рівня системи – вебсервісу.

4. Експлуатація вразливостей. На цьому етапі робляться спроби експлуатації ідентифікованих вразливостей для перевірки можливості несанкціонованого доступу чи інших шкідливих дій.

5. Пост-експлуатація. Основною метою етапу пост-експлуатації є розвиток атаки і пошук нових можливостей в системі, що атакується. Можливе отримання нових даних про систему, отримання доступу до системи та мережної активності для подальшого аналізу.

6. Створення звіту. Останнім та дуже важливим кроком є документування результатів. Саме цей звіт містить опис результатів кожного етапу. Він передається розробникам та включає деталі ідентифікованих вразливостей, методи їх експлуатації, а також рекомендації щодо усунення.

Наступним можливим етапом може бути повторне тестування виявлених проблем – перевірка того, що вразливості були належним чином усунені.

FPGA через специфіку апаратного забезпечення мають унікальні характеристики, які можуть вимагати спеціалізованих знань та підходів. Дослідження таких особливостей може потребувати фізичного доступу до пристрою.

4. Запропоновані ключові складові забезпечення кібербезпеки платформ FPGA as a Service

Як і в багатьох інших сферах, забезпечення кібербезпеки платформ FPGA as a Service є комплексною задачею, де ігнорування будь-якої складової може привести до критичних наслідків.

Варто виділити такі складові забезпечення кібербезпеки:

1. Важливо регулярно оновлювати програмне забезпечення та прошивки FPGA, щоб усувати відомі вразливості. Регулярне оновлення програмного забезпечення та прошивок FPGA є критично важливим для підтримки безпеки та ефективності цих пристроїв, оскільки це допомагає усувати відомі вразливості, покращувати функціональність та запобігати потенційним кібератакам. У сфері FPGA, де пристрої часто використовуються для обробки чутливих даних та виконання критично важливих завдань, застаріле програмне забезпечення або прошивки можуть стати слабкою ланкою, наражаючи

на систему ризику несанкціонованого доступу або маніпуляцій. Оновлення часто містять патчі для усунення вразливостей безпеки, які були виявлені після випуску попередніх версій, а також можуть включати поліпшення продуктивності, що робить пристрої більш надійними і ефективними. Крім того, в умовах постійного розвитку ландшафту загроз у сфері кібербезпеки, регулярні оновлення забезпечують адаптацію до нових методів атак, допомагаючи запобігти потенційним загрозам ще до того, як вони можуть завдати шкоди. Неоновлені системи не тільки схильні до вразливостей, але й можуть не відповідати сучасним стандартам безпеки та нормативним вимогам, що може призвести до юридичних та репутаційних ризиків для організацій. Таким чином, регулярне оновлення програмного забезпечення та прошивок FPGA є невід'ємною частиною стратегії забезпечення кібербезпеки та надійності критично важливих систем.

2. Безперервний моніторинг мережевого трафіку та аналіз поведінки системи можуть допомогти виявити спроби експлуатації вразливостей. Моніторинг мережевого трафіку в FPGA сервісах є критично важливим компонентом системи безпеки, що забезпечує безперервне спостереження та аналіз даних, що передаються через мережу. Він дозволяє оперативно виявляти аномалії, підозрілу активність чи спроби несанкціонованого доступу, що є ключем до запобігання та мінімізації потенційних кібератак. Ефективний моніторинг мережного трафіку включає використання спеціалізованих інструментів і програмного забезпечення, здатних аналізувати великі обсяги даних у реальному часі, виявляючи незвичайні патерни передачі даних, які можуть вказувати на компрометацію системи. Такий підхід дозволяє не лише виявляти активні атаки, а й прогнозувати потенційні загрози, спираючись на аналіз поведінкових моделей трафіку. Важливість моніторингу мережного трафіку особливо зростає в контексті FPGA сервісів, де висока продуктивність та гнучкість систем можуть бути використані зловмисниками для швидкого розповсюдження шкідливих атак або отримання цінних даних. Отже, безперервний моніторинг та аналіз мережевого трафіку є невід'ємною частиною загальної стратегії кібербезпеки, спрямованої на захист цінної інформації та підтримку стабільної роботи FPGA сервісів.

3. Регулярний аудит безпеки та тестування на проникнення можуть виявити потенційні вразливості, перш ніж вони будуть експлуатовані. Аудит безпеки та тестування на проникнення відіграють важливу роль у забезпеченні безпеки FPGA сервісів, оскільки вони дозволяють ідентифікувати та усувати потенційні вразливості до того, як вони експлуатуватимуться зловмисниками. Ці процедури включають всебічну оцінку як апаратних, так і програмних аспектів FPGA, включаючи аналіз конфігурації, перевірку коду, оцінку мережевої безпеки та фізичну безпеку пристроїв. Аудит безпеки зазвичай здійснюється досвідченими фахівцями та спрямований на виявлення слабких місць у системі, тоді як тестування на проникнення фокусується на активних спробах злому системи з метою виявлення вразливостей. Ці методи не тільки допомагають забезпечити захист від зовнішніх загроз, але також сприяють запобіганню внутрішніх загроз, таких як помилки програмного забезпечення або ненадійні конфігурації. Регулярний аудит та тестування на проникнення є ключовим елементом стратегії кібербезпеки, допомагає підтримувати довіру клієнтів та користувачів до FPGA сервісів. Крім того, ці процедури дозволяють організаціям відповідати нормативним та законодавчим вимогам, що особливо важливо у галузях із високими стандартами безпеки.

4. Дотримання стандартів безпеки та кращих практик може допомогти запобігти багатьом типам атак. Дотримання стандартів безпеки при створенні FPGA сервісів є критично важливим для гарантії їхньої надійності та безпеки, особливо враховуючи їх широке застосування у чутливих сферах, таких як телекомунікації, оборона та медицина. Стандарти безпеки, такі як ISO 27001, NIST SP 800-53 або стандарти Common Criteria, надають рамки та керівні принципи для розробки, які допомагають ідентифікувати, керувати та мінімізувати ризики, пов'язані з кібербезпекою. Це включає заходи захисту від зовнішніх і внутрішніх загроз, таких як несанкціонований доступ, маніпуляції з даними та апаратні атаки. Застосування цих стандартів у процесі розробки та експлуатації FPGA допомагає забезпечити конфіденційність, цілісність та доступність даних, а також підтримувати довіру користувачів до системи. Крім того, відповідність міжнародним стандартам підвищує конкурентоспроможність продукту на ринку, оскільки це є доказом високого рівня безпеки та якості. На додаток до цього, дотримання стандартів допомагає у дотриманні законодавчих та нормативних вимог, що особливо важливо у галузях, де вимоги до безпеки особливо суворі.

5. Підвищення поінформованості персоналу стосовно актуальних способів атак також є ключовим елементом захисту. Навчання персоналу про способи атак на FPGA сервіси відіграє важливу роль у забезпеченні кібербезпеки, оскільки співробітники, поінформовані про потенційні загрози та методи атак, можуть ефективно запобігати, виявляти та реагувати на інциденти. FPGA, що використовуються в різних галузях від телекомунікацій до військової промисловості, являють собою складні та гнучкі системи, схильні до унікальних загроз, включаючи

ISSN 1727-7337 (print)
ISSN 2663-2217 (online)

атаки на апаратному рівні та експлуатацію програмних вразливостей. Ретельно навчений персонал, який розуміє, як працюють ці атаки і які заходи безпеки необхідні для їх запобігання, стає важливим елементом системи захисту. Це не тільки допомагає мінімізувати ризик успішних кібератак, а й зміцнює загальну стратегію кібербезпеки організації, підвищуючи її стійкість до потенційних загроз. Крім того, навчання сприяє розвитку культури безпеки серед співробітників, що є критично важливим для підтримки високого рівня захисту від кіберзагроз, що швидко змінюються.

Висновки

Проведено дослідження проблем кібербезпеки платформ FPGA as a Service та пропонується комплекс складових забезпечення кібербезпеки платформ FPGA as a Service.

Проведено аналіз актуальних загроз кібербезпеки платформ FPGA as a Service.

Розглянуто можливість застосування стандарту проведення тестування на проникнення стосовно сервісів FPGA. Регулярне проведення аудиту та тестування на проникнення є ключовим елементом стратегії кібербезпеки та допомагає підтримувати довіру клієнтів та користувачів до FPGA сервісів.

Запропоновано комплекс складових забезпечення кібербезпеки платформ FPGA as a Service, що відповідає сучасним загрозам. Комплекс містить в собі такі заходи як регулярне оновлення ПЗ, моніторинг та аналіз безпеки, аудит та тестування на проникнення, відповідність стандартам безпеки, навчання персоналу.

Наукова новизна отриманих результатів полягає в тому, що проведено дослідження можливостей тестування на проникнення, де об'єктом тестування є платформа з доступом до FPGA-ресурсів. Як і в багатьох інших сферах, забезпечення кібербезпеки платформ FPGA as a Service є комплексною задачею, де ігнорування будь-якої складової може привести до критичних наслідків. Застосування лише тестування на проникнення є недостатнім, тому надано вичерпний перелік заходів забезпечення кібербезпеки платформ FPGA as a Service.

Література

1. Технології реалізації штучного інтелекту як сервісу на основі апаратних прискорювачів [Текст] / А. Є. Перепелицин, Є. В. Касапєн, Г. В. Фесенко, В. С. Харченко // Авіаційно-космічна техніка і технологія. – 2022. – № 6. – С. 57–65. DOI: 10.32620/aktt.2022.6.07.

2. Перепелицин, А. Є. Метод створення і впровадження FPGA проєктів стійких до змін вимог і середовищ розроблення для хмарних інфраструктур [Текст] / А. Є. Перепелицин, В. О. Куланов // Авіаційно-космічна техніка і технологія. – 2023. – № 5. – С. 87–97. DOI: 10.32620/aktt.2023.5.07.

3. Mahmoud, D. G. Electrical-Level Attacks on CPUs, FPGAs, and GPUs: Survey and Implications in the Heterogeneous Era [Text] / D. G. Mahmoud, V. Lenders, M. Stojilović // ACM Computing Surveys. – 2022. – Vol. 55, No. 3. – Article No. 58. – P. 1–40. DOI: 10.1145/3498337.

4. Ender, M. The unpatchable silicon: a full break of the bitstream encryption of xilinx 7-series FPGAs [Text] / M. Ender, A. Moradi, C. Paar // Proceedings of 29th USENIX Conference on Security Symposium (SEC'20). – 2020. – Article No. 102. – P. 1803–1819. DOI: 10.5555/3489212.3489314.

5. Red Balloon Security. 100 Seconds of Solitude: Defeating Cisco Trust Anchor with FPGA Bitstream Shenanigans [Online]. – Available at: https://redballoonsecurity.com/files/CycIhULVL5FS6VNM/100_seconds_of_solitude.pdf. – 22.08.2023.

6. Chakraborty, R. S. Hardware Trojan Insertion by Direct Modification of FPGA Configuration Bitstream [Text] / R. S. Chakraborty, I. Saha, A. Palchaudhuri, G. K. Naik // IEEE Design & Test. – 2013. – Vol. 30, No. 2. – P. 45-54. DOI: 10.1109/MDT.2013.2247460.

7. Lohrke, H. Key Extraction Using Thermal Laser Stimulation: A Case Study on Xilinx Ultrascale FPGAs [Text] / H. Lohrke, S. Tajik, T. Krachenfels, C. Boit, J.-P. Seifert // IACR Transactions on Cryptographic Hardware and Embedded Systems. – 2018. – Vol. 2018, No. 3. – P. 573–595. DOI: 10.13154/tches.v2018.i3.573-595.

8. Zarizenko, I. Analysis of tools and technologies of FaaS development [Text] / I. Zarizenko, A. Perepelitsyn // Radioelectronic and computer systems. – 2019. – No. 4 (92). – P. 88–93. DOI: 10.32620/reks.2019.4.10.

9. Perepelitsyn, A. Analysis of Ways of Digital Rights Management for FPGA-as-a-Service for AI-Based Solutions [Text] / A. Perepelitsyn, V. Kulanov // Proceedings 2023 IEEE 13th International Conference on Dependable Systems, Services and Technologies, DESSERT 2023. – 2023. – 5 p., accepted.

10. *The Penetration Testing Execution Standard [Online]. – Available at: http://www.pentest-standard.org/. – 22.08.2023.*

References

1. Perepelitsyn, A., Kasapien, Y., Fesenko, H., & Kharchenko, V. Tekhnolohiyi realizatsiyi shtuchnoho intelektu yak servisu na osnovi aparatnykh pryskoryuvachiv [Technologies for Implementing of Artificial Intelligence as a Service based on Hardware Accelerators]. *Aviacijno-kosmicna tehnika i tehnologia – Aerospace technic and technology*, 2022, no. 6, pp. 57–65. DOI: 10.32620/aktt.2022.6.07. (In Ukrainian).

2. Perepelitsyn, A., & Kulanov, V. Metod stvorennya i vprovadzhennya FPGA proyektiv stiykykh do zmin vymoh i seredovyshch rozroblennya dlya khmarnykh infrastruktur [Method of creation and deployment of FPGA projects resistant to change of requirements and development environments for cloud infrastructures]. *Aviacijno-kosmicna tehnika i tehnologia – Aerospace technic and technology*, 2023, no. 5, pp. 87–97. DOI: 10.32620/aktt.2023.5.07. (In Ukrainian).

3. Mahmoud, D. G., Lenders, V., & Stojilović, M. Electrical-Level Attacks on CPUs, FPGAs, and GPUs: Survey and Implications in the Heterogeneous Era. *ACM Computing Surveys*, 2022, vol. 55, no. 3, article no. 58, pp. 1–40. DOI: 10.1145/3498337.

4. Ender, M., Moradi, A., & Paar, C. The unpatchable silicon: a full break of the bitstream encryption of xilinx 7-series FPGAs. *Proceedings of 29th USENIX Conference on Security Symposium (SEC'20)*, 2020, article no. 102, pp. 1803–1819. DOI: 10.5555/3489212.3489314.

5. Red Balloon Security. *100 Seconds of Solitude: Defeating Cisco Trust Anchor With FPGA Bitstream Shenanigans*. Available at: https://redballoonsecurity.com/files/CycIhULVL5FS6VNM/100_seconds_of_solitude.pdf (accessed August 22, 2023).

6. Chakraborty, R. S., Saha, I., Palchaudhuri, A., & Naik, G. K. Hardware Trojan Insertion by Direct Modification of FPGA Configuration Bitstream. *IEEE Design & Test*, 2013, vol. 30, no. 2, pp. 45–54. DOI: 10.1109/MDT.2013.2247460.

7. Lohrke, H., Tajik, S., Krachenfels, T., Boit, C., & Seifert, J.-P. Key Extraction Using Thermal Laser Stimulation: A Case Study on Xilinx Ultrascale FPGAs. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018, vol. 2018, no. 3, pp. 573–595. DOI: 10.13154/tches.v2018.i3.573-595.

8. Zarizenko, I., & Perepelitsyn, A. Analysis of tools and technologies of FaaS development. *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2019, no. 4 (92), pp. 88–93. DOI: 10.32620/reks.2019.4.10.

9. Perepelitsyn, A., & Kulanov, V. Analysis of Ways of Digital Rights Management for FPGA-as-a-Service for AI-Based Solutions. *Proceedings 2023 IEEE 13th International Conference on Dependable Systems, Services and Technologies, DESSERT 2023*, 2023. 5 p. Accepted.

10. *The Penetration Testing Execution Standard*. Available at: http://www.pentest-standard.org/ (accessed August 22, 2023).

Надійшла до редакції 22.08.2023, розглянута на редколегії 20.11.2023

PENETRATION TESTING OF FPGA AS A SERVICE COMPONENTS FOR ENSURING CYBERSECURITY

Artem Tetskyi

The subject of study in this article is modern penetration testing technologies, in which the test object is a platform with access to FPGA resources. **The goal** of this work is to improve modern methods of penetration testing of services that provide FPGA as a Service, to identify vulnerabilities, the elimination of which increases the level of security of services and increases the level of user trust in such services. **Task:** to analyze possible threats of FPGA as a Service platforms; analyze the structure of FPGA as a Service platforms; analyze options for using the penetration testing standard; and offer key components for ensuring cyber security of FPGA as a Service platforms. According to the tasks, the following **results** were obtained. A study of the cyber security problems of FPGA as a Service platforms was conducted, and a set of components for ensuring the cybersecurity of FPGA as a Service platforms was proposed. An analysis of modern cybersecurity threats of FPGA as a Service platforms was carried out. The possibility of applying the penetration testing standard to FPGA services is considered. Regular audits and penetration testing are key elements of a cybersecurity strategy and help maintain customer and user trust in FPGA services. A set of components for ensuring cybersecurity of FPGA as a Service platforms is proposed, which corresponds to modern threats. The complex includes activities such as regular software updates, security monitoring and analysis, audit and penetration testing, compliance with security standards, and staff training. **Conclusions.** The main contribution and scientific novelty of the obtained results is that a study of the possibilities of penetration testing was conducted, where the test object is a platform with access to FPGA resources. As in many other areas, ensuring the cybersecurity of FPGA as a Service platforms is a complex task, where ignoring any component can lead to critical consequences. Applying only penetration testing is not enough; therefore, a comprehensive list of cybersecurity measures for FPGA as a Service platforms is provided.

Keywords: FPGA; FPGA as a Service; penetration testing; cybersecurity ensuring; protection measures.

Тецький Артем Григорович – канд. техн. наук, доц. каф. комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Artem Tetskyi – PhD, Associate Professor at the Computer Systems, Networks and Cybersecurity Department, National Aerospace University «Kharkiv Aviation Institute», Kharkiv, Ukraine,
e-mail: a.tetskiy@csn.khai.edu, ORCID: 0000-0003-1745-2452, Scopus Author ID: 57202894656.