УДК 004.42

Борисов И.Д.

Студент РТ-91

Гарипов А.И.

Студент РТ-91

Куцева К.В.

Студентка РТ-91

Научный руководитель: Вороной А.А., к.ф.-м.н., доц.

Поволжский государственный университет телекоммуникаций и информатики

МЕРЫ БЕЗОПАСНОСТИ И УЯЗВИМОСТИ В БЕЗОПАСНОСТИ МАССИВАХ ПОЛЕВЫХ ПРОГРАММИРУЕМЫХ ВЕНТИЛЕЙ (FPGA)

Аннотация: FPGA (field-programmable gate array)-Массив полевых программируемых вентилей, состоящий из памяти, программируемых логических вентилей и других компонентов, обычно используется при проектировании цифровых схем. Параметры FPGA обычно задаются с помощью языков описания аппаратуры (HDL), таких как VHDL и Verilog, подобно конфигурации прикладных интегральных схем (ASIC). Вы можете изменять текущие конфигурации и добавлять любые новые функциональные возможности или требования приложения, когда это необходимо.

Ключевые слова: массив полевых программируемых вентилей, Встроенные меры безопасности FPGA, Риски для безопасности FPGA, FPGA, проектирование цифровых схем.

Borisov I.D.

Student RT-91

Garipov A.I.

Student of RT-91

Kutseva K.V.

Student RT-91

SECURITY MEASURES AND VULNERABILITIES IN FIELD PROGRAMMABLE GATE ARRAY (FPGA) SECURITY

Abstract: FPGA (field-programmable gate array)-A field-programmable gate array consisting of memory, programmable logic gates and other components is commonly used in digital circuit design. The FPGA is configured using hardware description languages (HDLs) such as VHDL and Verilog, much like application specific integrated circuits (ASICs). You can modify current configurations and add any new functionality or application requirements when needed.

Keywords: field programmable gate array, Built-in FPGA safety measures, FPGA safety risks, FPGA, digital circuit design.

Встроенные меры безопасности

Некоторые встроенные средства безопасности присутствуют в хорошо спроектированной FPGA. FPGA принципиально менее прозрачна, чем обычный центральный процессор (ЦП). Чтобы создать код и программное обеспечение, которые хорошо выполняются, процессоры должны иметь хорошо документированный набор инструкций, конвейер данных и архитектуру памяти. С FPGA дело обстоит иначе.

Низкоуровневая функциональность FPGA формулируется разработчиком, что делает их недокументированными и, таким образом, создает мутную среду, затрудняющую выявление недостатков. Гора бумажной работы значительно усложняет процесс взлома и проникновения в FPGA, хотя это все еще возможно.

Риски для безопасности FPGA

Кража интеллектуальной собственности (ИС), нанесение ущерба системам на базе FPGA и значительная потеря данных - все это связано с угрозами безопасности FPGA. Для каждого нападения необходимы свои аспекты безопасности. Для разделения основных атак на FPGA можно использовать следующие категории.

Атаки клонирования

Злоумышленники копируют программы разработки FPGA в процессе клонирования. Затем они используют битовый поток в аналогичном устройстве и выдают его за свой собственный. Клонирование может

затрагивать весь проект или только его часть. Например, у продавца могут быть ограничения на приобретаемые ядра. Это самый типичный недостаток безопасности летучих FPGA.

Аппаратные трояны

Троянские программы создаются для злонамеренной модификации физических схем и изменения поведения системы. Они нарушают надежность оборудования, вызывают сбои в работе системы, предоставляют удаленный доступ к оборудованию и представляют опасность для конфиденциальных данных.

Атаки по боковому каналу

Киберпреступники не используют традиционные методы для проникновения в FPGA с помощью атак по боковым каналам. Вместо этого они используют информационные шаблоны системы против нее самой. Атаки по боковым каналам используют физические данные, которые открываются, когда в системе используется техника шифрования. Например, при шифровании битового потока, которое поддерживается большинством производителей FPGA, атаки по боковым каналам могут привести к утечке ключей, хранящихся в микросхемах FPGA, и сделать битовый поток незащищенным. Внедрение ошибок - наиболее распространенная атака по побочным каналам. Хакеры вводят ошибки для проверки реакции системы, а затем могут создать управляемые дефекты для изменения FPGA с этой точки. В таких атаках используются ошибки напряжения, синхронизации и лазерные ошибки. Чтобы найти эти шаблоны информации, хакер обычно должен находиться поблизости или физически владеть устройством.

Обратный инжиниринг

Реверсивная разработка нетлиста на уровне затворов и реверсивная разработка с использованием обработки изображений - это два основных типа реверсивной разработки ИС. Злоумышленники могут извлечь функциональность более высокого уровня из нетлиста уровня затворов, используя реверсивный инжиниринг нетлиста уровня затворов, например, описание на уровне регистров (RTL) или на уровне структуры.

Перехватив битовый поток, хакеры могут использовать стратегии обратного проектирования для дальнейшего изучения FPGA. Существуют инструменты, специально разработанные для сопоставления битов битового потока, восстановления схем и других задач. Хотя технически это не

является взломом, обратное проектирование всего или части битового потока является кражей ИС у создателей.

Подделка

В процессе подмены битовый поток злоумышленника подменяется оригинальным битовым потоком FPGA (рис. 6). Этот битовый поток может содержать элементы, полученные путем обратной разработки или клонирования. В результате система может стать уязвимой, предоставляя хакерам эффективный контроль над машиной или системой. Такое поведение может привести к травмам или смертям, прямо или косвенно вызванным действиями хакера в некоторых приложениях, критичных для безопасности. Серьезный риск для безопасности существует, если битовый поток может быть просмотрен удаленно.

Перехват битового потока

Перехват битового потока - один из наиболее часто используемых злоумышленниками методов воздействия на FPGA. Эта брешь в системе безопасности имеет много документации. Что касается уязвимостей, то получение доступа к этим важнейшим конфигурационным файлам открывает целую банку червей. Хакеры могут использовать файлы для захвата управления, кражи данных битового потока и других методов.

Одним из самых важных кусочков головоломки является битовый поток. Получив его, преступники могут свободно творить хаос. Для получения битового потока хакерам обычно требуется физический доступ к устройству.

Шифрование битовых потоков

Битовые потоки FPGA должны быть правильно зашифрованы и аутентифицированы. Эффективные методы шифрования позволяют предотвратить атаки по боковым каналам, перехват данных и многое другое. В лучшем виде шифрования для FPGA используется летучий ключ. Как и битовые данные, эти ключи хранятся в ОЗУ (памяти с произвольным доступом), работающей от батарейки.

Храните свои данные в зашифрованном виде, поскольку расшифровка происходит только после их использования и удаления из SRAM. Данные надежно защищены на каждом этапе процедуры. Криптографические данные с летучим ключом теряются во время цикла питания системы.

Сеансовые ключи, используемые в этом методе шифрования, каждый раз разные. Хакеры не могут проникнуть в систему, используя атаки по боковым каналам или другие методы перехвата.

Изоляция процесса конфигурирования

FPGA используют методы изоляции на кристалле для защиты системы от атак микропроцессора. Сравнимая нагрузка ложится на FPGA, поскольку подключенные микропроцессоры особенно восприимчивы к проблемам безопасности.

Обычные маршруты передачи данных отделены от процедуры конфигурирования, чтобы предотвратить вмешательство. Это функционирует как брандмауэр и изменяет поверхность атаки. Дополнительную безопасность обеспечивает изоляция, которая также гарантирует, что схема не может измениться во время использования.

Циклические проверки избыточности и мониторинг

Циклические проверки избыточности (CRC) способны находить ошибки, непреднамеренные повреждения и другие неожиданные проблемы. Во время передачи данных можно проверить битовый поток с помощью CRC, чтобы найти ошибки или преднамеренные изменения. Во время загрузки логические анализаторы могут проверить связь между флэш-памятью и FPGA. Они также обнаружат необычные данные Joint Test Access Group (JTAG) и проблемы с другими портами отладки, что будет полезно.

Внешние устройства безопасности

FPGA могут использовать внешние устройства безопасности для хранения ключей шифрования. Для проверки FPGA использует механизм "вызов-ответ". Доступ к FPGA предоставляется после того, как внешнее устройство узнает правильный ответ.

Использованные источники:

1) Технология FPGA для тысячи применений// habr.com. URL:https://habr.com/ru/articles/505838/(дата обращения 14.03.2023)
2) FPGA Security Vulnerabilities and Countermeasures// electronicdesign.com. URL:https://www.electronicdesign.com/technologies/industrial/article/21261753/einfochips-an-arrow-company-fpga-security-vulnerabilities-and-countermeasures (дата обращения 15.03.2023)