МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ПОЛІТЕХНІЧНИЙ УНІВЕРСИТЕТ

ІНСТИТУТ КОМП'ЮТЕРНИХ СИСТЕМ

МАТЕРІАЛИ ДЕВ'ЯТОЇ МІЖНАРОДНОЇ НАУКОВОЇ КОНФЕРЕНЦІЇ СТУДЕНТІВ ТА МОЛОДИХ ВЧЕНИХ

присвячена 55-річчю
ІНСТИТУТУ КОМП'ЮТЕРНИХ СИСТЕМ

" Сучасні інформаційні технології 2019 "

" Modern Information Technology 2019 "

23-24 травня

Одеса
«Екологія»
2019

УДК 004.556.53

ФОРМИРОВАНИЕ ПУТИ ВНЕДРЕНИЯ КОНТРОЛЬНОГО ЦИФРОВОГО ВОДЯНОГО ЗНАКА В ПРОГРАММНЫЙ КОД FPGA-БАЗИРОВАННЫХ УСТРОЙСТВ

Защелкин К.В.
к.т.н., доцент каф. КИСС
Одесский Национальный Политехнический Университет, УКРАИНА

АННОТАЦИЯ. В работе рассмотрена проблема контроля целостности программного кода микросхем FPGA. Предлагается развитие методов контроля целостности, в рамках которых контрольная хэш-сумма внедряется в программный код в виде цифрового водяного знака. Предлагается метод, позволяющий сформировать путь внедрения цифрового водяного знака в пространстве информационного объекта программного кода микросхем FPGA.

Введение. Значительное место в номенклатуре элементной базы современных компьютерных систем занимают программно-управляемые компоненты. Ключевой особенностью таких компонентов является возможность изменения их функционирования путем внесения изменения в их программный код. Простота механизма внесения таких изменений порождает проблему обеспечения целостности программного кода. Под целостностью далее понимается свойство исключения непредусмотренных изменений системы или предоставляемых ею сервисов [1]. В данной работе рассматривается проблема контроля целостности программного кода микросхем FPGA (Field Programmable Gate Array) [2].

Цель работы состоит в формализации подхода к формированию пути внедрения цифрового водяного знака, который используется в процессе контроля целостности программного кода FPGA-базированных компонентов компьютерных систем.

Основная часть работы. Наиболее эффективным и часто применяемым подходом к контролю целостности программного кода является использование контрольных хэш-сумм [3]. Для исходного состояния программного кода вычисляется хэш-сумма, которая в дальнейшем считается эталонной. Эталонная хэш-сумма прикрепляется к программному коду или некоторым образом ассоциируется с ним. При необходимости проверки целостности для программного кода вновь вычисляется хэш-сумма. По результатам сравнения эталонной и вновь вычисленной хэш-сумм делается вывод о том, нарушена ли целостность программного кода.

В работе рассматривается подход, в рамках которого контрольная хэш-сумма внедряется в информационный объект программного кода FPGA в виде цифрового водяного знака. Такое внедрение не изменяет размер информационного объекта и не модифицирует поведение устройства, управляемого программным кодом. При этом внешний наблюдатель не может выделить цифровой водяной знак в составе информационного объекта. Более того, сам факт выполнения контроля целостности остается скрытым от внешнего наблюдателя.

Известны методы контроля целостности [4] программного кода FPGA, ориентированные на описанный выше подход. В данной работе предлагается вспомогательный для них метод, которой позволяет сформировать путь внедрения цифрового водяного знака в пространстве информационного объекта программного кода FPGA.

Пространство информационного объекта образовано совокупностью программных кодов блоков LUT (Look Up Table) [5] – наиболее массовых программируемых вычислительных блоков в структуре FPGA. Путь внедрения, формируемый предлагаемым методом, представляет собой упорядоченную последовательность блоков LUT, в программный код которых непосредственно внедряются разряды контрольного цифрового водяного знака.

В качестве входных данных предлагаемый метод получает:

– информационный объект программного кода FPGA;

– цифровой водяной знак, содержащий контрольную хэш-сумму;

– стеганографический ключ – набор правил, в соответствии с которыми выполняется внедрение и извлечение цифрового водяного знака.

Выходными данными метода является путь внедрения цифрового водяного знака – упорядоченное множество элементов, каждый из которых описывает отдельный блок LUT, а также содержит информацию, необходимую для внедрения одного разряда цифрового водяного знака в программный код этого блока.

В работе определены основные теоретические положения предлагаемого метода. Первое положение заключается в способе введения отношения порядка на множестве блоков LUT информационного объекта программного кода. Второе и третье положение метода заключаются в способе учета при формировании пути внедрения естественных и искусственных ограничений, накладываемых структурой информационного объекта и стеганографическим ключом соответственно. Четвертое положение метода определяет возможность включения в путь внедрения блоков LUT, связанных с ранее уже включенными в путь внедрения блоками.

На основе представленных основных теоретических положений в работе предлагается последовательность действий, образующих предлагаемый метод. Последовательность состоит из пяти циклически выполняющихся действий, привядших к получению элементов пути внедрения.

Предложенный в работе метод реализован программно с использованием языка C# в рамках программной платформы .Net. При помощи разработанного программного обеспечения произведено тестирование метода. В ходе тестирования были использованы целевые микросхемы FPGA Intel (Altera) Cyclone II – IV [6]. Для получения информационного объекта программного кода исследуемых в ходе тестирования проектов была задействована САПР Intel Quartus Prime. Результаты тестирования показали эффективность использования предложенного метода и его реализации в составе системы контроля целостности программного кода FPGA.

Выводы. Предложен метод формирования пути внедрения цифрового водяного знака в информационный объект программного кода микросхем FPGA. Метод является вспомогательным в процессе контроля целостности программного кода FPGA-базированных устройств. Выполнена программная реализация метода. В среде полученного программного обеспечения произведен экспериментальный анализ предложенного метода. Традиционные подходы к внедрению цифрового водяного знака в пространство информационного объекта программного кода FPGA используют неформализованный, основанный на случайном выборе процесс построения пути внедрения. Предлагаемый в данной работе метод формализует этот процесс и позволяет получать путь внедрения оптимальный по параметру возможного количества задействованных блоков LUT.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Отказобезопасные информационно-управляющие системы на программируемой логике [Текст] / Е. С. Бохмач, А. Д. Герасименко, В. А. Головир, В. А. Сиора, В. В. Скляр, В. И. Токарев, В. С. Харченко; под ред. В. С. Харченко, В. В. Скляра. – Х. : НАУ «ХАИ», НПП «Радий», 2008. – 380 с.

2. Andina, J. FPGAs: Fundamentals, Advanced Features, and Applications in Industrial Electronics [Text] / J. Andina. – CRC Press, 2017. –450 p.

3. Stallings, W. Cryptography and Network Security: Principles and Practice, 7th Edition [Text] / W. Stallings. – United Kingdom, Harlow: Pearson Education Limited, 2017. – 768 p.

4. Zashcholkin, K. LUT-object integrity monitoring methods based on low impact embedding of digital watermark [Text] / K. Zashcholkin, O. Ivanova // Proceedings of the 14th International Conference “Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET-2018)”. – Lviv-Slavske, 2018. – P. 519-523.

5. Drozd, A. Use of natural LUT redundancy to improve trustworthiness of FPGA design [Text] / A. Drozd, M. Drozd, M. Kuznietsov // CEUR Workshop Proceedings. – 2016. – Vol. 1614. – P. 322-331.

6. Vanderbauwhede, W. High-performance computing using FPGAs [Text] / W. Vanderbauwhede, K. Benkrid. – New-York: Springer, 2016. – 525 p.