УДК 004.35

ИССЛЕДОВАНИЕ ПРОБЛЕМЫ НЕСАКЦИОНИРОВАННОГО ДУБЛИРОВАНИЯ ОДНОРАЗОВЫХ ПРОГРАММ

Стрелец А.И.
магистр кафедры «Компьютерные системы и технологии»,
Национальный исследовательский ядерный университет «МИФИ»
Россия, г. Москва
Храпов А.С.
магистр кафедры «Компьютерные системы и технологии»,
Национальный исследовательский ядерный университет «МИФИ»
Россия, г. Москва
Иванников В.С.
магистр кафедры «Компьютерные системы и технологии»,
Национальный исследовательский ядерный университет «МИФИ»
Россия, г. Москва
Атавина А.В.
магистр кафедры «Финансовый мониторинг»,
Национальный исследовательский ядерный университет «МИФИ»
Россия, г. Москва

Аннотация: Данная статья содержит исследование проблемы несанкционированного дублирования и повторного выполнения одноразовых программ. Рассмотрена архитектура современных программно-аппаратных комплексов, организующих среду выполнения одноразовых программ.

Ключевые слова: одноразовые программы, информационная безопасность, семантическая неразличимость, компиляторы.

RESEARCH OF PROBLEM OF UNCOMPRESSED ONE-TIME PROGRAMS DUPLICATION

Strelets A.I.

master degree,

Department of Computer Systems and Technologies,

National Research Nuclear University MEPhI

Moscow, Russia

Hrapov A.S.

master degree,

Department of Computer Systems and Technologies,

National Research Nuclear University MEPhI

Moscow, Russia

Ivannikov V.S.

master degree,

Department of Computer Systems and Technologies,

National Research Nuclear University MEPhI

Moscow, Russia

Atavina A.V.

master degree,

Department of Financial Monitoring,

National Research Nuclear University MEPhI

Moscow, Russia

Annotation: This article is about research of problem of uncompressed one-time programs duplication. The article contains the structure of modern system for one-time program environment.

Key words: one-time program, information security, semantic indistinguishability, compilers.

Введение

Концепция одноразовых программ получила широкое распространение в современном мире, в особенности в области информационной безопасности и банковском секторе [1]. Защита от несанкционированного копирования и повторного воспроизведения является наиболее важным компонентом комплексной защиты программно-аппаратных комплексного подобного назначения. Новая парадигма одноразовых вычислений открывает новые возможности для концептуальных исследований [2, 3]. Одна из таких концепций - концепция «одноразовых доказательств» (one-time proof - OTP) - доказательств, которые могут быть проверены только один раз, а затем становятся бесполезными.

В рамках данной статьи рассмотрен современный подход осуществления обеспечения OTP идентификации программы, имеющей преопределённую продолжительность жизни. Данный подход включает в себя машиночитаемый носитель, содержащий машиночитаемый код для предоставления одноразовым программам. Машиночитаемый носитель включает в себя инструкции по определению программы для преобразования в новую программу, имеющую заданный срок службы. Носитель также включает в себя инструкцию по включению компиляции программы для создания новой программы, имеющей предопределенный срок службы и где новая программа, имеющая заданный срок службы, гарантированно будет иметь только определенную продолжительность жизни.

Другие варианты осуществления включают в себя компьютеризированное устройство, сконфигурированное для обработки всех способов, приведенных в этой статье в качестве вариантов осуществления изобретения [4]. В таком воплощении это компьютеризированное устройство включает в себя систему памяти, процессор, и интерфейс связи как механизм, соединяющий эти компоненты.

Структура программно-аппаратного защиты ОТР.

Для решения проблемы несанкционированного дублирования программы и повторного воспроизведения, используются программно-аппаратные комплексы, со структурой, отлично от традиционных вычислительных систем, предназначенных для программ общего вида. В частности, компьютерный программный продукт представляет собой один вариант осуществления, если он имеет машиночитаемый носитель, включающий в себя программную логику при выполнении в компьютеризированном устройстве, обеспечивающую связанные операции, обеспечивая программу, имеющую заранее определенный срок службы.

Программное обеспечение или встроенное программное обеспечение или другие подобные конфигурации могут быть установлены на компьютеризированном устройстве, чтобы один или несколько процессоров в компьютеризированном устройстве выполняли способы, поясненные в данном документе как варианты осуществления изобретения. Программные процессы, которые работают в совокупности компьютеризированных устройств, например, в группе устройств передачи данных или других объектов также могут предоставить систему по изобретению. Система по изобретению может быть распределена между многими программными процессами на несколько устройств передачи данных или все процессы могут

работать на небольшом наборе выделенных компьютеров или на одном компьютере в одиночестве.

Следует понимать, что варианты осуществления изобретения могут быть воплощены строго как программное обеспечение, как программное обеспечение и аппаратные средства, или как аппаратные средства и / или только схемы, такие как в устройстве передачи данных. Все обсуждаемые функции, методы, конфигурации и т. д. могут быть выполнены независимо скомбинированы. Соответственно, настоящее изобретение может быть воплощено и рассмотрено многими различными способами.

Как уже упоминалось выше, в нашем случае требование защиты от чтения предназначено только для тех областей памяти, к которым устройство никогда не обращается. Эти предположения кажутся минимальными, если необходимо использовать какое-либо нетривиальное использование защищенного устройства. Кроме того, устройство очень недорогое, с низким энергопотреблением и одноразовое, что очень похоже на RFID-метки, используемые в одежде. Таким образом, одноразовая программа может быть реализована с помощью комбинации стандартного программного обеспечения и таких минимально защищенных запоминающих устройств.

Понятие одноразовых программ естественным образом распространяется на k-разовые программы, которые могут быть доказуемо выполнены максимально k раз на входных значениях в любое время. Для простоты изложения в настоящем документе используются примеры с одноразовым случаем, хотя следует понимать, что те же или аналогичные понятия применимы к программам, имеющим ограниченное время (k) использования.

Одноразовая программа не может быть основана исключительно на программном обеспечении, а защищенные аппаратные устройства используются в качестве строительных блоков в конструкциях. Обычно защищенные аппаратные устройства моделируются как черные ящики с внутренней памятью, доступ к которой возможен только через интерфейс ввода-вывода.

Более того, неразличимость сохраняется даже для различающего, который принимает T в качестве входных данных. Обратите внимание, что крайне важно, чтобы симулятор S обращался к своему оракулу только один раз. Также обратите внимание, что симулятор не может получить доступ ни к какой части реальной одноразовой программы, включая аппаратное обеспечение, даже в режиме черного ящика.

Это гарантирует, что одноразовая программа не может быть продублирована и запущена более одного раза. Симулятор, конечно, не может дублировать, и, таким образом, противник, который может получить два результата программы, не может быть смоделирован. Существует много возможных безопасных аппаратных устройств, которые можно себе представить, и априори не ясно, является ли одно устройство лучше или хуже другого. Это центральный вопрос при изучении одноразовых программ и безопасного оборудования в целом.

Тривиальным решением было бы создать для каждой функции f специальное защищенное аппаратное устройство для конкретных задач, которое вычисляет f для одного входа x, а затем отказывается работать больше. Это решение крайне неудовлетворительно по нескольким причинам. Во-первых, этот подход требует создания другого аппаратного устройства для каждой отдельной функции f. Это может стоить времени для некоторых задач,

но слишком дорого для большинства задач и, следовательно, на практике невозможно. Вместо этого рекомендуется, чтобы выбранное безопасное аппаратное устройство было универсальным. В случае защищенного оборудования (а не обычного оборудования) универсальность особенно важна, поскольку необходимо тщательно изучить каждый тип аппаратного устройства, чтобы гарантировать, что оно не подвержено атакам по побочным каналам. Это кажется невозможным для каждой функции.

Во-вторых, возможно, наиболее важным для безопасного аппаратного устройства является его простота, и предложенное выше тривиальное решение является потенциально сложным, поскольку требует создания сложного оборудования для сложных функций. Наш поиск простых аппаратных устройств, которые легко создавать, анализировать и понимать, мотивирован несколькими проблемами.

Предположение о том, что аппаратное устройство является безопасным и / или защищенным от взлома, является очень сильным предположением, поскольку необходимо учитывать все возможные физические атаки. Чем проще аппаратное устройство, тем легче его проанализировать и проанализировать его безопасность, и тем более разумным становится предположение о его безопасности. Атаки по побочным каналам стали существенной угрозой целостности криптографических алгоритмов и устройств. Кажется интуитивно понятным, что чем меньше вычислений выполняет оборудование, тем менее оно восприимчиво к потенциально разрушительным атакам по побочным каналам. Действительно, это является руководящим принципом теоретического подхода к определению физически безопасных устройств. Наконец, и, возможно, наиболее очевидно, чем проще аппаратное устройство, тем проще и дешевле его будет создавать.

Результаты

Концепция одноразовых программ на данный момент является одной из наиболее важных концепция в области защиты информации. В данном исследовании проанализирована структура современных средств, осуществляющих поддержку и защищенность среды выполнения. На основе проведенного исследования, можно сделать вывод о необходимости комплексного подхода к решению проблемы несанкционированного копирования одноразовых программ. При этом решения, построенные только на программной подходе, не удовлетворяют требованиям, предъявляемым к безопасности подобных систем. Полноценное решение данной проблемы возможно только при комплексном подходе к её решению, включающем как разработку аппаратной составляющей системы, так и программной.

Заключение

Рассмотренные в статье свойства структуры одноразовых программных комплексов, позволяют прийти к выводу о необходимости комплексного подхода к решению проблемы безопасности одноразовых программ, включающем в себя как аппаратные, так и программные компоненты.

Библиографический список

1. Gagliardoni T., Hülsing A., Schaffner C. Semantic security and indistinguishability in the quantum world //Annual Cryptology Conference. – Springer, Berlin, Heidelberg, 2016. – С. 60-89.
2. Beame P. Cryptography: курс лекций. URL: https://courses.cs.washington.edu/courses/cse599b/06wi/ (Дата обращения: 15.05.2019)

3. Bagherzandi A. et al. Relations between semantic security and indistinguishability against cpa, non-adaptive cca and adaptive cca in comparison based framework //arXiv preprint cs/0508110. – 2005.
4. Bagherzandi A., Mohajeri J., Salmasizadeh M. Comparison Based Semantic Security is Probabilistic Polynomial Time Equivalent to Indistinguishability //IJ Network Security. – 2008. – Т. 6. – №. 3. – С. 354-360.

Оригинальность 95%