Криптографическая защита локальных данных игровых приложений

Филатов А.И.
Магистр, Московский Технологический Университет
E-mail: Luckibarry@gmail.com

Введение.

В наше время одним из наиболее перспективных сегментов индустрии развлечений является игровая индустрия. Целью статьи является предложение по внедрению в игровую индустрию достижений в области защиты информации, а именно: разработка системы защиты локальных данных игрового приложения.

Основные угрозы и методы противодействия.

Чаще всего при взломе игровых приложений прибегают к специально разработанным программам:

· Программы для сканирования памяти

· Отладчики (дебаггеры) уровня ассемблера

На рисунке 1.1 продемонстрирован процесс работы игрового приложения с оперативной памятью устройства до ввода дополнительных средств защиты. Как можно заметить переменные игровых атрибутов, обрабатывающиеся в оперативной памяти, никак не защищаются.

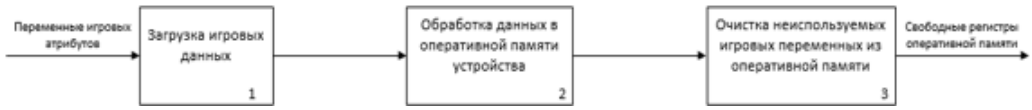

Рисунок 1. — Существующий процесс работы игрового приложения с оперативной памятью

Главным предлагаемым отличием от уже существующего процесса обработки игровых данных в оперативной памяти, является внедрение криптографической защиты т.е шифрования переменных игровых атрибутов с помощью псевдослучайно генерируемого ключа. Данный процесс представлен на рисунке 1.2.

Рисунок 2. — Описание разрабатываемой системы защиты, в части защиты данных обрабатывающихся в оперативной памяти

Помимо защиты данных в оперативной памяти, были предложены меры противодействия изменению локальных файлов игрового клиента, посредством высчитывания и последующей сверки значения хэш-суммы. Процесс представлен на рисунке 1.3.

Рисунок 3. — Описание разрабатываемой системы защиты, в части защиты от внесения изменений в локальные файлы игрового клиента

В рамках защиты от сканирования оперативной памяти устройства, было принято решение шифровать данные симметричным алгоритмом на основе побитовой операции сложения по модулю 2, с постоянно изменяющимся ключом, для того, что бы исключить возможность отслеживания действующего значение переменной игрового атрибута. Шифрование данных производится раз в 100 мс, псевдослучайно генерируемым ключом. Методом противодействия против программ- отладчиков является сравнения вычисленного на основе игрового приложения значения хэш-суммы с эталонным значением, хранящимся на сервере. Вычисление хэш-суммы выполняется с помощью 256-битного алгоритма хэширования ГОСТ Р 34.11-2012.

Заключение.

Внедрение разработанных мер защиты поможет защитить игровые данные, обрабатывающиеся на локальном устройстве пользователя, что позволяет предотвратить ущерб разработчикам игрового приложения и честным игрокам. Данная система защиты существенно не замедляет работу устройства и игрового приложения тем самым не причиняет дискомфорта игроку.

Библиографический список.

1. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 13.07.2015) «Об информации, информационных технологиях и о защите информации» [Текст]. — М.: Собрание законодательства РФ", 31.07.2006, N 31 (1 ч.), ст. 3448.
2. ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования [Текст].
3. Введ. 01.01.2013. Взамен ГОСТ Р 34.11-94. — М.: Стандартинформ 2013 г.— I, 24 с.
4. ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования [Текст]. Введ. 30.06.1990. — М.: ИПК Издательство стандартов, 1989 г. — I, 28 с.
5. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи [Текст]. Введ. 01.01.2013. Взамен ГОСТ Р 34.10-2001 — М.: Стандартинформ 2013 г.— I, 24 с.