ПРИМЕНЕНИЕ БИБЛИОТЕКИ OPENENCLAVE ДЛЯ РАЗРАБОТКИ ДОВЕРЕННЫХ ПРИЛОЖЕНИЙ

Н.Н. Романович
Научный руководитель – Алексеев В.Ф.
канд. техн. наук, доцент
Белорусский государственный университет информатики и радиоэлектроники

Данные существуют в трех состояниях: данные, которые хранятся (*dataatrest*); данные, которые обрабатываются (*datainuse*) и данные, которые передаются (*dataintransit*). Даже если вы шифруете данные при хранении и передаче по сети, данные, которые обрабатываются, по-прежнему уязвимы для несанкционированного доступа и подделки во время выполнения. Защита данных при их обработке имеет решающее значение для обеспечения полной безопасности на протяжении всего жизненного цикла.

Криптография или шифрование широко используются организациями для защиты конфиденциальности (предотвращение несанкционированного просмотра) и целостности данных (предотвращение несанкционированных изменений). Существуют современные технологии обеспечения безопасности данных, которые позволяют приложениям работать в защищенных анклавах или в доверенных средах выполнения, которые предлагают шифрование данных и приложений. Примерами таких технологий являются технологии *TrustZone* (применяемая в процессорах архитектуры *ARM*, которые применяются в большинстве мобильных устройств), технология *SGX* (используется в процессорах *Intel*) [1]. И несмотря на единую цель, эти технологии имеют массу различий.

Данную проблему стремится решить библиотека *Open Enclave*. *Open Enclave SDK* – это *SDK* с открытым исходным кодом, предназначенная для создания единой унифицированной абстракции анклава для разработчиков, а также для разработки приложений на основе доверенных сред (*TEE*). По мере развития технологий доверенных сред и

появления их различных реализаций, *Open Enclave SDK* стремится поддерживать набор *API*, который позволяет разработчикам создавать и развертывать приложения на нескольких технологических платформах, в различных средах от облачных до гибридных, а также для *Linux* и *Windows* [2]. На сегодняшний день в *Open Enclave* поддерживаются технологии *TEEIntelSGX* и *ARMTrustZone* на базе доверенной среды *OP-TEE*.

Доверенное приложение делится на два компонента: ненадежный компонент (называемый хостом) и доверенный компонент (называемый анклавом). Компонент хоста работает без изменений в «ненадежной» операционной системе (такой как *Windows* или *Linux*), в то время как доверенный компонент работает в анклаве — защищенном контейнере, предоставляемом реализацией доверенной среды. Эти средства защиты позволяют анклавам выполнять безопасные вычисления с гарантией того, что секреты не будут раскрыты.

Данные технологии, в том числе с использованием библиотеки *Open Enclave*, нашли широкое применение в системах, требующих обработки конфиденциальных данных, таких как системы интернета вещей (*IoT*), системы обработки биометрических данных и др.

Библиографический список

1. Романович Н.Н. Применение технологии ARM TrustZone для обработки конфиденциальных данных в облачных сервисах // Студенческий вестник: электрон. научн. журн. 2021. № 23(168). URL: https://studvestnik.ru/journal/stud/herald/168 (дата обращения: 19.10.2021).

2. What is Open Enclave SDK? // Open Enclave URL: https://openenclave.io/sdk/ (дата обращения: 19.10.2021).