БЕЗОПАСНАЯ СРЕДА ИСПОЛНЕНИЯ В МОБИЛЬНЫХ УСТРОЙСТВАХ

Евланов М.А.

Институт информационных технологий БГУИР,
г. Минск, Республика Беларусь

Шелягович А. С. – магистр технических наук

Сегодня особенно актуален вопрос безопасности операций, совершаемых с помощью мобильных устройств. При исполнении таких операций особенно важно задействовать механизмы, предотвращающие компрометацию системы злоумышленниками. Реализацией такого механизма являются системы под общим названием «Безопасная среда исполнения» (англ. Trusted Execution Environment).

Trusted Execution Environment (TEE) – особо защищенная область процессора в мобильных устройствах и комплекс микропрограммных средств, служащие для выполнения операций требующих высокую степень информационной безопасности. Для организации TEE, системы оборудуются дополнительными компонентами, основными из которых является энергонезависимая память TEE которая используется для хранения исполняемых кодов микропрограммных компонентов, специальных кодов и значений записываемых на этапе производства мобильного устройства; энергозависимая память TEE – используется при непосредственной работе компонентов безопасной среды исполнения; криптографические механизмы – служат для верификации кодов системы.

Начало работы TEE происходит при запуске устройства: в рамках процесса аутентифицированной загрузки проверяется целостность мобильной платформы. TEE предоставляет код начала загрузочной последовательности, следуя которому процессор обязан начинать загрузку только их определенной области памяти. Загрузка прерывается, если процесс, инициированный безопасной средой исполнения, обнаруживает изменения в компонентах запускаемой платформы, при этом для поиска изменений используются специальные сертификаты загрузочного кода, подписанные самим производителем и хранящиеся в энергонезависимой памяти TEE. В процессе последующей работы устройства преимуществами TEE могут пользоваться не только производители самого устройства, но также и разработчики программных продуктов, обладающие специальными сертификатами для работы с данной областью процессора. Данной возможностью пользуются разработчики мобильных операционных систем и крупные разработчики приложений. К примерам функций, которые реализованы с использованием TEE, можно отнести:

– защита лицензионного мультимедиа-контента – устройства воспроизведения оборудуются процессорами с TEE, что позволяет производить предварительную проверку прав на обладание того или иного продукта, защищенного лицензией;

– мобильные финансовые услуги – при работе приложения происходит идентификация устройства, с помощью которого происходит платеж. Особое внимание уделяется при произведении операций с использованием технологии бесконтактных платежей (мобильное устройство устанавливает связь с платежным терминалом), в таких случаях происходит дополнительные идентификации как платежного терминала, так и самого мобильного устройства;

– авторизация пользователя – наличие обособленной энергонезависимой памяти, позволяет обеспечить безопасное хранение данных для авторизации пользователя, таких как результаты работы сканера отпечатка пальца или радужной оболочки глаза. Эти данные будут использованы в последующем при работе программы для авторизации.

Консорциум GlobalPlatform ведет активную разработку целого ряда стандартов:

– о проектировании систем с безопасной средой исполнения;

– о разработке микропрограммных компонентов TEE;

– о разработке программных продуктов для эффективной работы с такими системами.

Наличие стандарта позволит производителям устройств и разработчикам программных продуктов устранить различия в реализациях и объединить подходы при дальнейшей разработке данных систем, что приведет к еще большему росту информационной безопасности операций, совершаемых с использованием мобильных устройств.

Список использованных источников:

1. ARM TrustZone. [Электронный ресурс]. – Режим доступа: https://developer.arm.com/technologies/trustzone. – Дата доступа: 01.04.2017.

2. From Wikipedia, the free encyclopedia: Trusted execution environment. [Электронный ресурс]. – Режим доступа: https://en.wikipedia.org/wiki/Trusted_execution_environment. – Дата доступа: 01.04.2017.

3. GlobalPlatform made simple guide: Trusted Execution Environment (TEE) Guide. [Электронный ресурс]. – Режим доступа: https://www.globalplatform.org/mediaguidetee.asp. – Дата доступа: 01.04.2017.

4. Защищенные среды мобильных устройств. Ян-Эрик Экберг, Кари Костяйнен, Н. Асокан. [Электронный ресурс]. – Режим доступа: https://www.osp.ru/os/2014/08/13043488. – Дата доступа: 01.04.2017.