СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТЕХНОЛОГИЙ ДОВЕРЕННЫХ СРЕД ARM TRUSTZONE И INTEL SGX

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

В современном мире большая часть приложений, обрабатывающих конфиденциальную информацию, выполняются на большой недоверенной вычислительной базе, которая включает операционные системы, гипервизоры, аппаратные средства и их встроенные микропрограммы. Эта большая вычислительная база становится сложной и неподдающейся какой-либо проверке или верификации. Эта проблема открывает злоумышленникам теоретическую возможность украсть секреты критически важного с точки зрения безопасности приложения, скомпрометировав ненадежную вычислительную базу.

Чтобы решить проблему ненадежной вычислительной базы, современные процессорные архитектуры представляют концепцию доверенных сред выполнения (англ. *TrustedExecutionEnvironments*),

которая направлена на обеспечение хранения и обработки конфиденциальных данных в изолированной среде [1].

Существующие популярные доверенные среды выполнения для изоляции сред полагаются на оборудование, как правило без использования средств операционной системы или используя их в минимальной степени.

Intel SGX и *ARM TrustZone* – наиболее популярные на сегодняшний день реализации доверенных среды выполнения. И *Intel SGX*, и *ARM TrustZone* представляют собой доверенные среды выполнения с аппаратной поддержкой, но механизм работы доверенных сред и приложений, выполняемых в них, кардинально различается.

Intel SGX создает надежную среду для доверенных приложений, которая выполняется поверх существующего ненадежного системного программного обеспечения: разработчик приложения может быть уверен, что приложение работает в доверенной среде, даже если операционная система скомпрометирована [2].

ARM TrustZone же создает новый «доверенный мир» для доверенных приложений, которые выполняются на доверенном системном программном обеспечении и оборудовании, доступном только для доверенного мира. Как правило, для выполнения какого-либо приложения в доверенном мире *ARM TrustZone*, данное приложение должно быть предустановлено на устройство его производителем, либо производителем встраиваемого программного обеспечения [3].

Таким образом, технология *Intel SGX* является наиболее подходящей для применения в программном обеспечении общего назначения, требующем обеспечения безопасной обработки данных, тогда как *ARM TrustZone* наиболее применима в мобильных устройствах и устройствах интернета вещей, в которых, как правило, отсутствует возможность установки приложений от сторонних разработчиков.

Библиографический список

1. Trusted Execution Environment: What It is, and What It is Not / M. Sabt, M. Achemlal, A. Bouabdallah. // 2015 IEEE Trustcom/BigDataSE/ISPA — 2015.

2. A survey of Intel SGX and its applications / Z. Wei [et. Al] //Frontiers of Computer Science. — 2021. — 06. — Vol. 15.

3. TrustZone Explained: Architectural Features and Use Cases / B. Ngabonziza [et al.] // 2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC). – 2016.