Вопрос 1. Дать определение TEE, анклава, назвать реализации TEE для как минимум двух архитектур ЦП. Что может располагаться в анклаве?

TEE (Trusted Execution Environment) безопасная среда выполнения - технология, которая позволяет размещать код и данные в специальном отдельном пространстве ОП (анклаве) с защитой шифрованием.

Анклав – хранилище данных и кода на основе TEE в специально выделенном пространстве ОП.

Аппаратные реализации TEE:

• ARM Thrust Zone;

• Intel SGX.

В анклаве может размещаться:

• Хранилище данных;

• Модуль исполняемого кода;

• ОС с «доверенными» приложениями (trustlet).

Вопрос 2. В чём заключается защита, предоставляемая TEE коду и данным. Для размещения какого кода и данных предназначен TEE?

ОП, принадлежащая анклаву, шифруется, ключами шифрования располагает только CPU.

Области применения TEE:

• Размещение, расшифровка и обработка конфиденциальных данных (биометрия и др.);

• Защита цифрового контента (DRM);

• Всё вышеперечисленное как на пользовательских устройствах (терминалы оплаты, мобильные телефоны и др) так и на облачных серверах.

Вопрос 3. Дать определение LibOS для TEE. Назвать как минимум 2 примера LibOS. Назвать отличия LibOS от обычных ОС по предоставляемому функционалу.

LibOS (One Library OS) – «Библиотечные» ОС для анклавов, как правило реализованные в одной библиотеке или облаке, имеющие ограниченный функционал, т.к. берут на себя только базовые системные функции ввод/вывод в устройства и переключение процессов, а также для уменьшения поверхности атаки.

Примеры:

• Gramine;

• OP TEE.

Вопрос 4. Назвать аппаратные средства, обеспечивающие работу TEE:

1. Каким образом CPU переключается на исполнение кода, размещённого в TEE?

Переключение потока команд/процессорного времени из Host в TEE с помощью специальных машинных команд, имеющих ещё большие привилегии, чем ядро и даже гипервизор

• ARM – EL3, S-EL0, S-EL1;

• Intel – SMM и SGX.

1. Где расположен ключ шифрования для доступа к данным или коду, расположенному в TEE?

Ключами шифрования располагает только CPU.