Каннер Андрей
kanner@okbsapr.ru

LFCE-1700-0355-0200

TPM и IMA/EVM против программно-аппаратных средств защиты информации от НСД

Суздаль, 2018

Принцип пошагового контроля целостности

1. На раннем этапе активизации проводится **аппаратный** контроль целостности программных и технических средств СВТ:
– BIOS/UEFI, носителей данных и др.;
– критически важных компонентов ОС;
– программных средств статического и/или динамического контроля целостности (разграничения доступа и др.).

2. В дальнейшем целостность защищаемых данных контролируется **программно** (программными средствами, целостность которых уже подтверждена).

Подходы к реализации пошагового контроля целостности (1/2)

АМДЗ
(для x86)

↓

СПО для контроля целостности
(ПАК СЗИ НСД)

↓

конфиденциальная информация,
персональные данные и т.д.

Подходы к реализации пошагового контроля целостности (2/2)

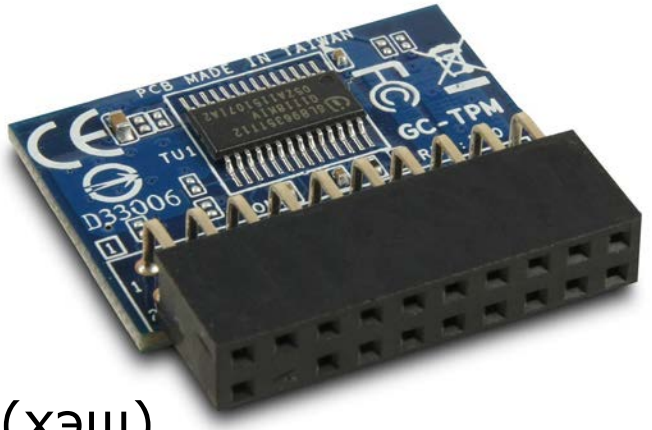
TPM
(для x86)

IMA/EVM
(Linux)

конфиденциальная информация,
персональные данные и т.д.

Trusted Platform Module (TPM)

Стандартизованный (ISO/IEC 11889) аппаратный модуль для «доверенных вычислений» с поддержкой криптографических операций.



1. Аппаратный ГСЧ.
2. Криптографический процессор.
3. Хранилище ключевой информации.
4. PCR-регистры для хранения метрик (хэш)

Функции*:

– Обеспечение целостности платформы («root of trust»).
– Шифрование/подпись, хранение ключ. информации в составе системы шифрования, DRM и др.
– …

* выполняются пассивно

Количество доступных для хранения в TPM метрик ОС/СВТ

– Доступно ограниченное число 160-битных PCR-регистров (не менее 16).

Но!

– Можно хранить намного больший объем метрик, чем общий объем памяти регистров:

$$PCR_{i\text{-}new\text{-}value} = hash(PCR_{i\text{-}old\text{-}value} \,||\, new\text{-}data)$$

Integrity Measurement Architecture (IMA) Extended Verification Module (EVM)

1. Возможности IMA:
   – вычисление значений хэш-функций загружаемых в память бинарных данных (исполняемые файлы, разделяемые библиотеки, модули ядра ОС);
   – *TPM + IMA* => возможность удаленной аттестации системы (только доверенное ПО было запущено с момента загрузки СВТ).
2. Возможности EVM:
   – хранение хэш-кодов в расширенных атрибутах файлов;
   – защита расширенных атрибутов с хэш-кодами от несанкционированного изменения;
   – блокировка доступа к несанкционированно измененным данным;
   – локальная аттестация системы и проверка целостности объектов (не только бинарных данных).

Отличия TPM и IMA/EVM от ПАК СЗИ НСД

1. Активная роль АМДЗ **vs** пассивная роль TPM (необходимо использовать адаптированные UEFI, TrustedGrub и др.).
2. TPM и IMA/EVM можно применять только на современных СВТ и ОС.
3. TPM более универсальное средство, АМДЗ – специализированное.
4. Все критически важные данные ПАК СЗИ НСД можно изменять (генерировать личную ключевую информацию).

В интересах кого реализуются функции защиты? Производителя СВТ или конечного владельца?

Владелец СВТ должен иметь возможность беспрепятственно запускать любое ПО?

Владелец должен доверять уникальным ключам/сертификатам TPM?

Вопросы?

Каннер Андрей
kanner@okbsapr.ru

LFCE-1700-0355-0200