Левиев Илья Андреевич 018 гр.
Protecting Data with the Trusted Platform Module

Интегрированная технология обеспечения безопасности компьютерных систем на основе Модуля TPM, спроектированного в соответствии со спецификацией группы Trusted Computing Group.

Сеть обеспечивает важную функциональность в любой коммерческой фирме, офисе или предприятии. В ее основные задачи входит обеспечение сотрудников необходимой информации и простата общения с клиентами, которые становится приоритетными. Т.к из-за роста компании и клиентской базы сеть будет расширятся, что повлечет за собой угрозу информации.

В основном инструменты, обеспечивающие безопасность систем, представляют собой программные средством защиты данных. Такая распространенность обусловлена тем, что сами по себе программные решение обладают невысокой стоимостью и легко устанавливаются поэтому много компаний, желающих обеспечить защиту данных в своих сетях. Если применять только программные методы для защиты информации в компьютерных сетях это может привести к тому что сети останутся по-прежнему уязвимы для нападения злобных прграмеров (хакеров) или недобросовестных сотрудников.

Материнские платы со встроенным в них модулем ТПМ дают возможность получить более высокий уровень защиты инфы. Так как этот способ совокупляет в себе аппаратные программные и микропрограммные компоненты ,что создает более надежную среду. Плата со встроенным модулем ТПМ обладает аппаратными механизмами защиты которые дополняют программные методы такие как шифрование, цифровые подписи и т.д..

Защита особо важных данных

Корпоративные данные которые участвуют в бизнес процессах могут подвергаться риску .Большинством пользователей используются программные инструменты шифрования для защиты Электронной почты файлов папок и других документов .Так как технологии применяющиеся для создания вредоносных программ усложняются то обеспечение безопасности корпоративных данных становиться все более сложной задачей .

Разработка средств которые шифруют данные может решить проблему но такие программы сохраняют ключи шифрования на жестком диске , поэтому существует вероятность того что хакеры получат доступ к этой информации. Но если хранить ключи при помощи которых шифруются файлы и папки в модуле TPM то это может сделать систему более надежной к таким атакам .

Альтернативным методом защиты электронной почты является цифровая подпись. Сообщение и вложение получают такую подпись перед отправкой такой метод дает некоторую гарантию получателю в том кто именно отправил письмо а так же в том что это письмо не было изменено после отправки. Так как алгоритм создающий цифровую подпись выполняется в самом модуле и ключи не становятся доступными при расшифровки и никогда не помещаются в оперативную память что уменьшает вероятность того что злоумышленник получит ключи.

Так же замечу что надежность ключей которые используют при шифровании документов зависит от генератора случайных чисел. Злоумышленники пользуются обычным ПК для того что бы взломать ключи которые были созданы с помощью слабого способа генерации случайных чисел что дает им возможность получить доступ к защищенным данным.Так как модуль TPM содержит надежный аппаратный генератор случайных чисел это обеспечивает возможность создания стойких криптографических ключей, поэтому атакам методом грубой силы на ключ вычислительно не осуществима.

Решение TPM Solution Stack
Решение TPM Solution Stack содержит в себе как аппаратные так и программные компоненты которые в совместно дают возможность обеспечить более надежную платформу.

Аппаратная платформа

Аппаратным компонентом решения является системная плата Intel® D865G для настольных ПК с модулем Infineon Trusted Platform Module (TPM). Модуль TPM является криптографическим микроконтроллером обеспечивающим следующие функций:

- Алгоритмы RSA создания и проверки подлинности цифровой подписи; длина ключа — до 2048 бит
- Алгоритм кэширования SHA-1
- Механизмы, обеспечивающие защиту создания и хранения криптографических ключей
- Несколько анонимных ключей идентификации (AIK)
- Аппаратная генерация случайных чисел
- Поддержка в BIOS

Интегрированный модуль TPM поднимает уровень надежности, который недосягаем для программных методов. Он увеличивает надежность криптографических методов, обеспечивает дополнительную стойкость существующих систем, а также может обеспечить встроенную защиту ключей цифровой подписи.

Технологии защиты информации приобретают большую стойкость при использовании встроенных аппаратных средств.

Платформы, использующие только программные решения обеспечения безопасности не защищают данные так как ключи хранятся на жестких дисках.

В прошлом ключи, созданные с использованием генераторов псевдослучайных чисел, приводили к возникновению уязвимостей. В модуле TPM для генерации случайных чисел используется генератор случайных чисел с нормальным распределением. Такие ключи взламываются методом грубой силы, что в данном случае является неосуществимым с вычислительной точки зрения. В Дополнении С к нормативному документу FIPS 140-1 (в настоящее время принят нормативный документ FIPS 140-2, заменяющий FIPS 140-1), принятому в США, перечислены

специфические требования, относящиеся к степени "случайности" случайных чисел.

Программное обеспечение
С системной платой поставляется ПО Wave Systems EMBASSY Trust Suite, в состав которого входят:

- Document Manager: Программа шифрования файлов и папок, использующая функции модуля TPM.
- Private Information Manager: Защищенное хранилище для персональной информации: учетных записей, номеров кредитных карт и так далее. Эта программа помогает указывать необходимую информацию при заполнении онлайновых форм.
- SmartSignature: Расширение для программы Adobe Acrobat, использующее функции модуля TPM для создания цифровых подписей документов в формате PDF.

ОС и драйверы
Данное решение совместимо с операционными системами Windows XP Professional и Windows 2000.

Вывод

В наше время, когда множество домашних и корпоративных компьютеров подключено к сетям, особую важность приобретает роль безопасности данных, проходящих через эти компьютеры. Все серьезней становится необходимость разработки методов и технологий защиты, которые не нарушали бы доступности данных для тех, кто имеет право к ним обращаться, но предотвращали несанкционированный доступ.

Приложение
Основные компоненты в спецификации:

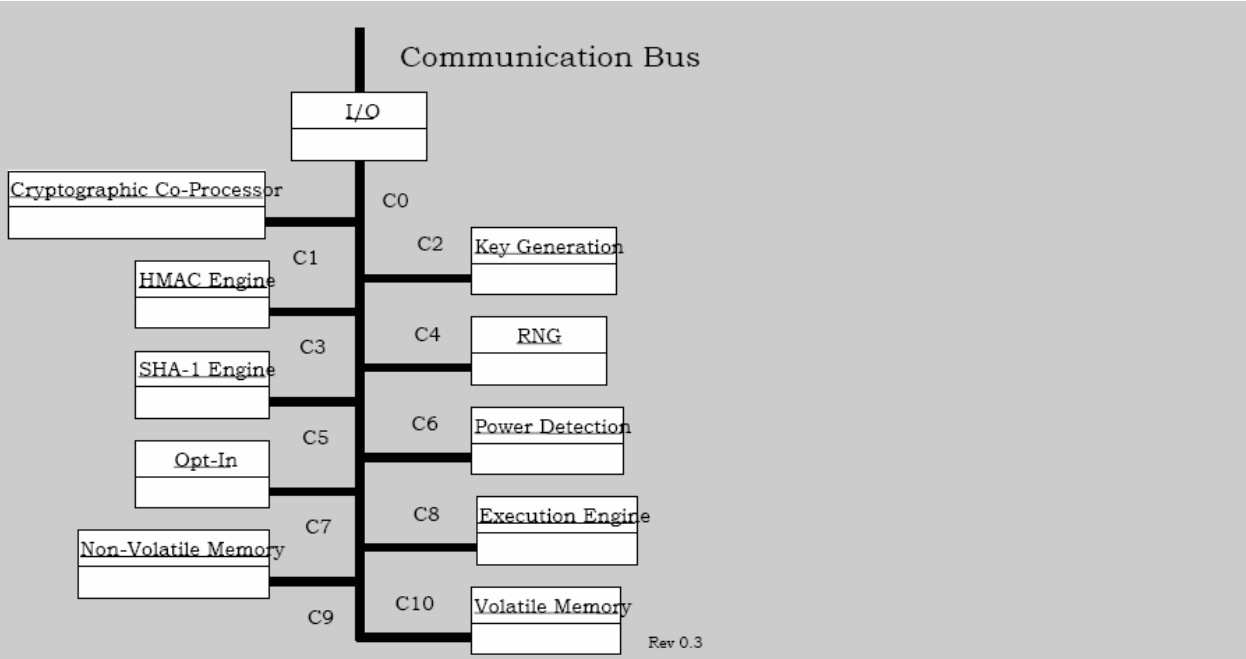

Figure 2:a - TPM Component Architecture

Components :
Input and Output
Cryptographic Co-Processor
Key Generation
HMAC Engine
Random Number Generator
SHA-1 Engine
Power Detection
Opt-In
Execution Engine
Non-Volatile Memory

Параметры модуля Infineon Trusted Platform Module:

Infineon Technologies Platform Module Solution Provides the Following Features

Infineon Technologies TPM Hardware Overview:

- 64 kBytes of ROM & 8 kBytes of RAM
- 16 kBytes of EEPROM with 500 write-erase cycles
- 48 kBytes of EEPROM for firmware secure updates
- RSA hardware accelerator for signature calcution and verification as well as 2048 bit key generation when using CRT
- World-leading security protection against SPA and DPA
- Low Pin Count (LPC) bus optimized
- Low power consumption

Ссылки:

http://www.infineon.com/

http://www.wave.com/

https://www.trustedcomputinggroup.org

http://www.intel.com