ЭЛВИС-ПЛЮС

Эволюция подхода к построению доверенной среды

Олег Вернер,
к.т.н., начальник лаборатории доверенной среды

ЭЛВИС-ПЛЮС

ДОВЕРИЕ

В нормативных документах:

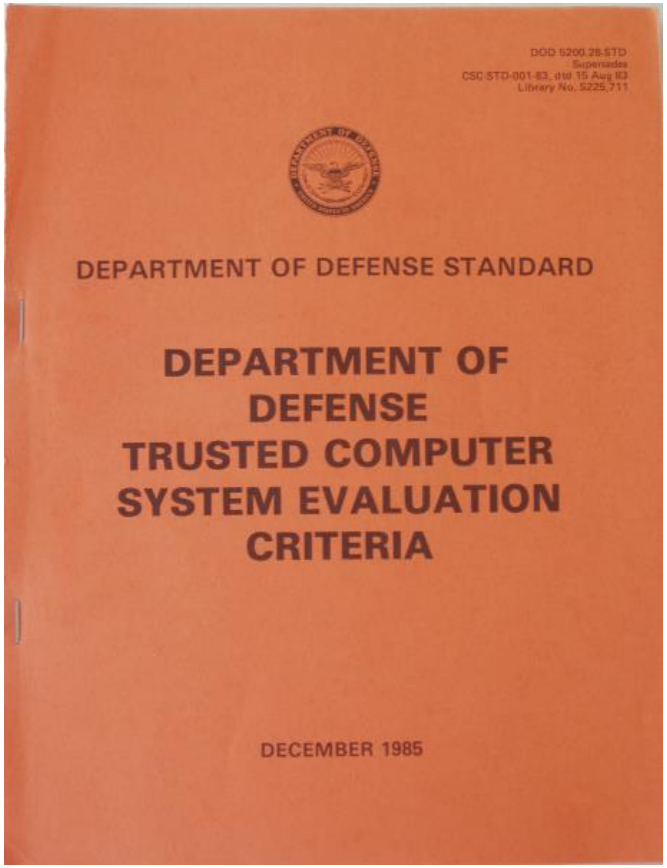
- доверенная загрузка
- доверенный канал
- доверенная связь
- модуль доверенной загрузки

На практике также:

- доверенная операционная система
- доверенная среда

Нет определения термина «доверенный»

ДОВЕРЕННАЯ СИСТЕМА



- система, использующая аппаратные и программные средства для обеспечения одновременной обработки информации разной категории секретности группой пользователей без нарушения прав доступа.

ДОВЕРЕННАЯ ЗАГРУЗКА

- функция персонального компьютера

для воспрепятствования несанкционированному запуску пользователем,

загрузке операционной системы (ОС) и получению возможности доступа к конфиденциальной

информации.

ЭЛВИС-ПЛЮС

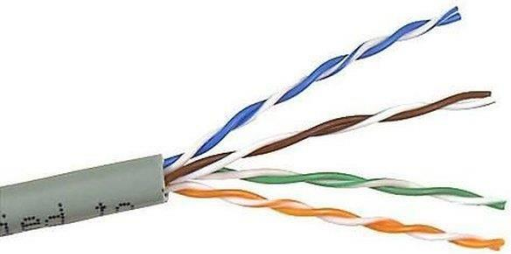
ДОВЕРЕННАЯ СРЕДА

- созданное комплексом технических и организационных мер пространство, которое обеспечивает его участникам предсказуемый результат взаимодействий,

при этом степень доверенности среды определяется надежностью контента в ней.

ВЧЕРА: ИЗОЛИРОВАННАЯ СРЕДА

- Изначально доверенная вычислительная среда понималась как

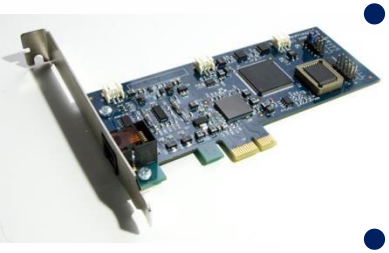


изолированная,

функционально замкнутая.

- Обеспечивает доверие к локальному компьютеру, ЛВС.
- Особое значение организационных мер (контроль физического доступа).

Резидентные компоненты безопасности ЭЗ/АПМДЗ



Проблемы:

- RAID? Шифрование диска (FDE)?
- Netbook, monoblock, ultrabook? А что с гарантией? Совместимость?
- Удаленная аутентификация платформы?

- Цена?

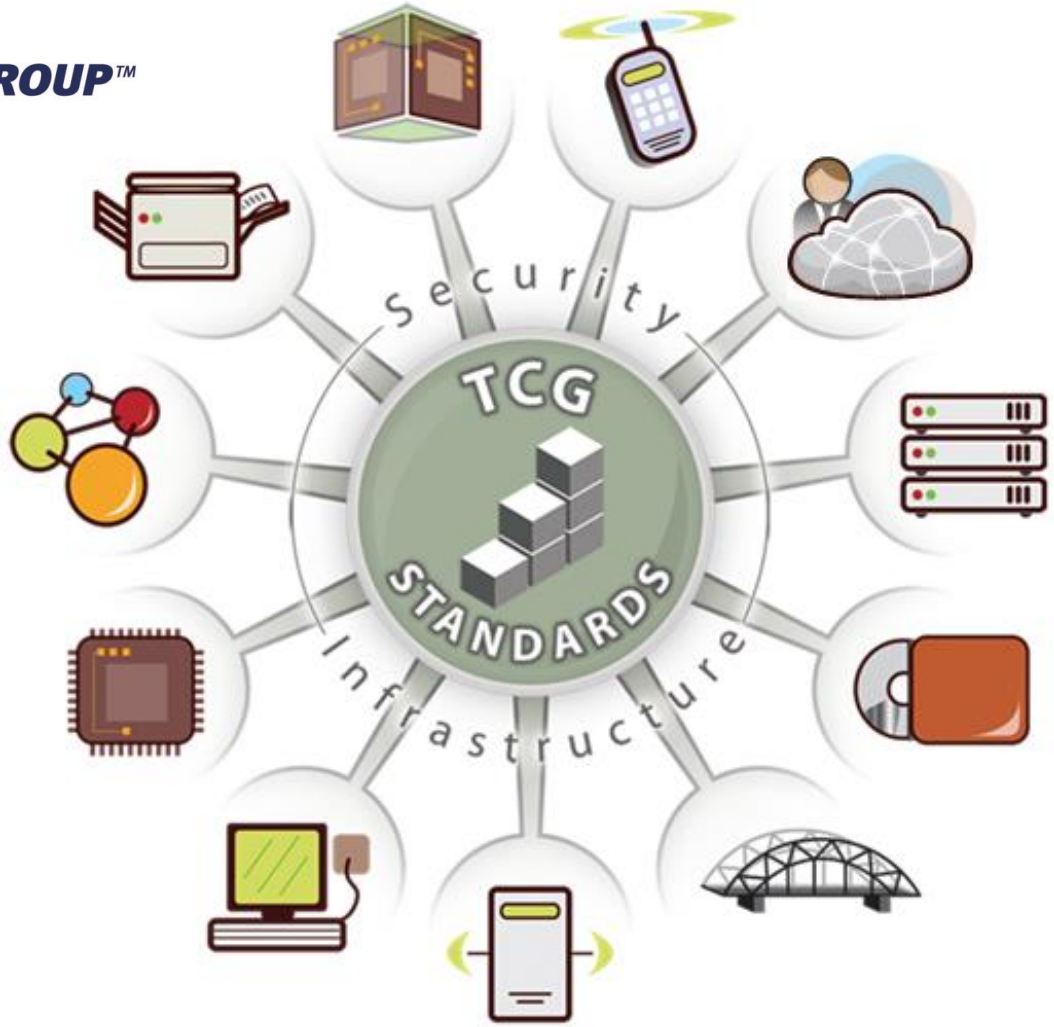
ЭЛВИС-ПЛЮС

Trusted Computer Group: ИСТОРИЯ

- 1999: Trusted Computing Platform Alliance (TCPA)
- 2001: Спецификации TCPA версии 1.0, рабочие группы TPM, ПК, спецификации TPM 1.1
- 2003: Trusted Computer Group (TCG), спецификации TPM 1.2, TNC, TSS, Mobile Platform, Storage, Infrastructure, …
- …
- 2011: Спецификации Virtualized Trusted Platform Architecture
- 2013: Спецификации TPM 2.0

СЕГОДЯ: Доверенная среда TCG

TRUSTED COMPUTING GROUP™

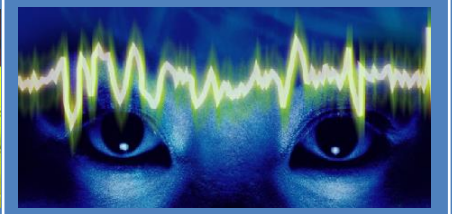


Взлом TPM

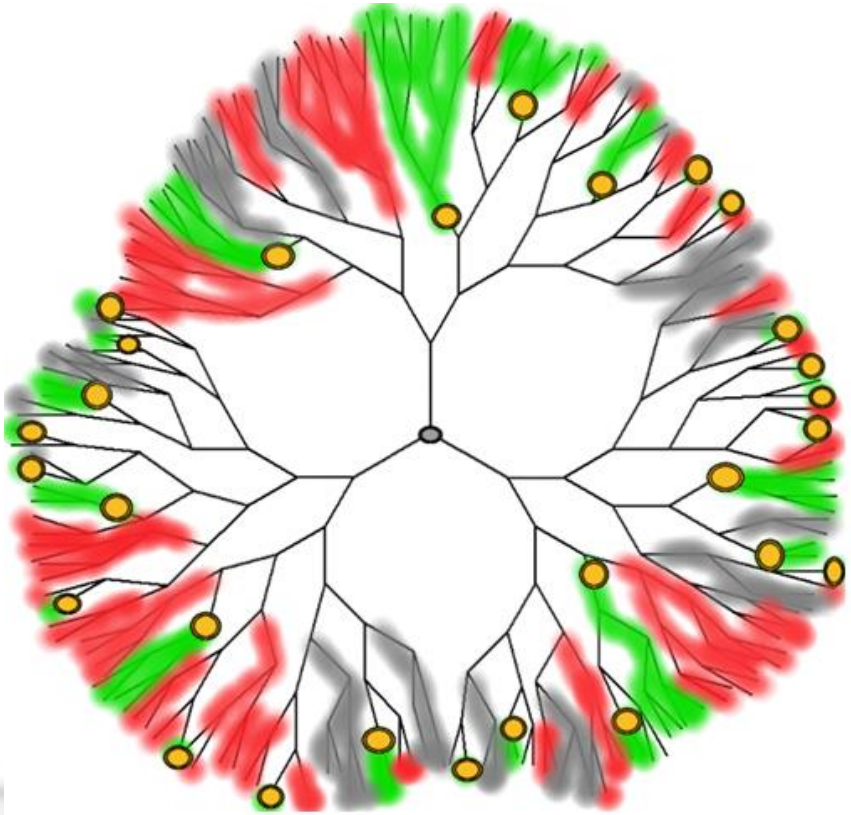
Black Hat 2010: Christopher Tarnovsky сообщил, что ему удалось взломать TPM Infineon SLE 66 CL PC

INTEGRITY GUARD

Stefan Rüping, Marcus Janke и Andreas Wenzel – номинанты Немецкой премии будущего за 2012 год

			
Класс атаки	**Manipulating**	**Observing**	**Semi-Invasive**
Время на разработку	**месяцы**	**дни**	**месяцы**
Время на реализацию	**дни**	**часы**	**минуты**
Стоимость	**> 100.000 €**	**> 10.000 €**	**> 100 €**
Пример	**Microprobing**	**Power Analysis**	**Spike Attack**

Традиционный подход к безопасности



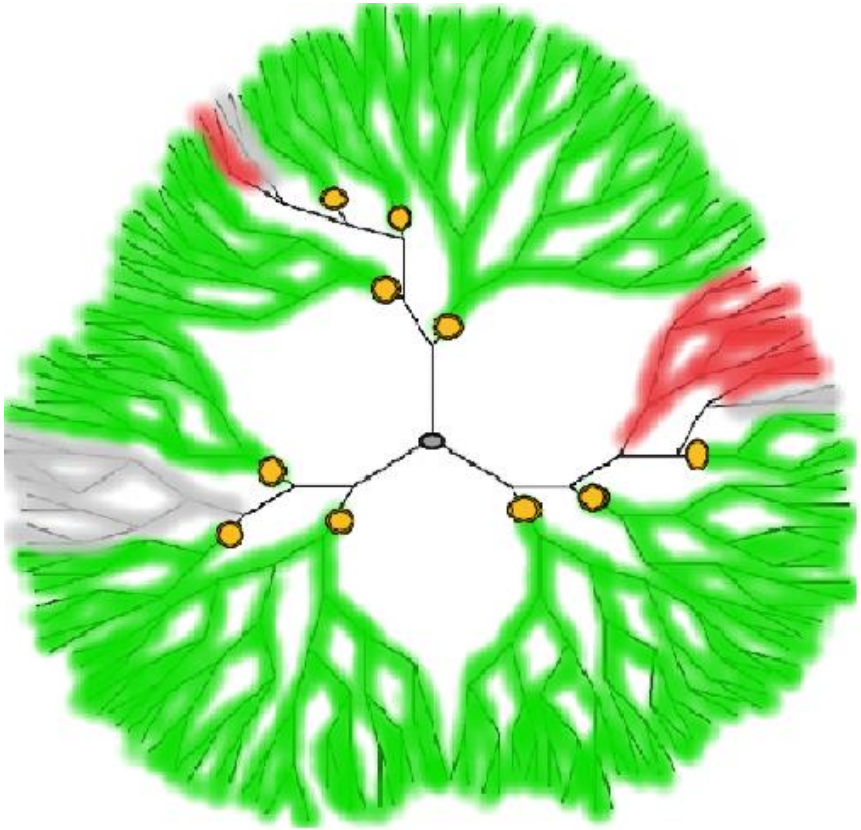
Контрмера

Защищенная

Незащищенная

Непроверенная,
Неизвестная

Новый подход – INTEGRITY GUARD



Контрмера

Защищенная

Незащищенная

Непроверенная,
Неизвестная

Базовые механизмы INTEGRITY GUARD

- Полное шифрование в чипе (Full On-Chip Encryption)
- Полный контроль целостности (Comprehensive Error Detection)
- Специальная внутренняя топология (Active I^2-shield)

SESAMES AWARDS

DEUTSCHER ZUKUNFTSPREIS
Preis des Bundespräsidenten
für Technik und Innovation

СЕГОДЯ

TRUSTED COMPUTING GROUP™

TPM 2.0

infineon

INTEGRITY GUARD

intel®

intel
Haswell

BOOT GUARD

Доверенная среда TCG

- ☑ Доверенная загрузка
- ❑ Доверенная ОС
- ❑ Доверенное ПО

Как определять доверие с учетом:

- возможной компрометацией сертификата ПО?
- уязвимости нулевого дня?
- проактивной защиты (эвристические методы)?

ЗАВТРА: Доверенное исчисление

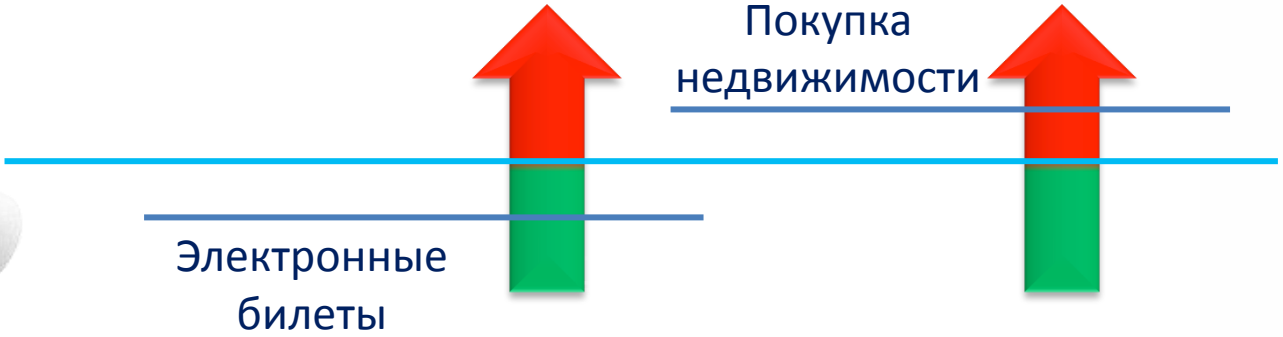
David Grawrock

Principal Engineer and Security Architect
for the Initiatives, Technology, Pathfinding,
and Planning group, Intel

Подобно тому, как алгебра смогла решить большие проблемы, а добавление исчислений изменило математику, добавление доверенного исчисления изменит то, как мы пользуемся доверием.

Уровень доверия

Уровень доверия к online операциям - граница перехода от «да» к «нет»

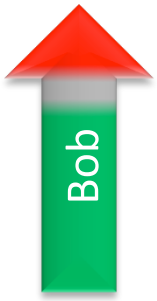


Описание доверия

Он – инженер, прекрасно разбирающийся в электронике

Она – домохозяйка, не доверяющая новым технологиям

Bob



Alice

- Как описать друг другу свои уровни доверия (которые могут не совпадать)?
- Чей уровень доверия они будут использовать, если Bob готов, например, покупать акции online, а Alice – нет?
- Как будет приниматься решение в «серой зоне» Alice?

Trust Calculus

Необходим язык, который должен быть:

- достаточно выразительным, чтобы описывать уровень доверия в «серой зоне»;
- математическим, чтобы осуществлять вычисления и проводить сравнения.

Должны быть определены:

- элементы языка;
- грамматика;
- правила вычисления и законы.

Эволюция подхода к построению доверенной среды

Можно ли доверять технологии доверенной среды TCG?

- В TCG входят практически все ведущие компьютерные фирмы;
- Спецификации открыты, изучаются учеными и хакерами;
- Чипы TPM производятся в разных странах;
- Технология является сегодня единственным методом обеспечения доверия к виртуализации;
- Репутация ведущих производителей «железа» и ПО, использующих TPM.

Благодарю за внимание