ЭЛВИС-ПЛЮС

Обеспечение безопасности мобильных устройств с использованием технологии доверенной среды

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

Сценарии BYOD: предварительные вопросы

Может ли **Владелец Устройства**:

- Быть уверен, что его данные не будут доступны со стороны Компании?
- Запускать ПО и приложения по своему выбору?
- Уволится из Компании без потери своих данных?

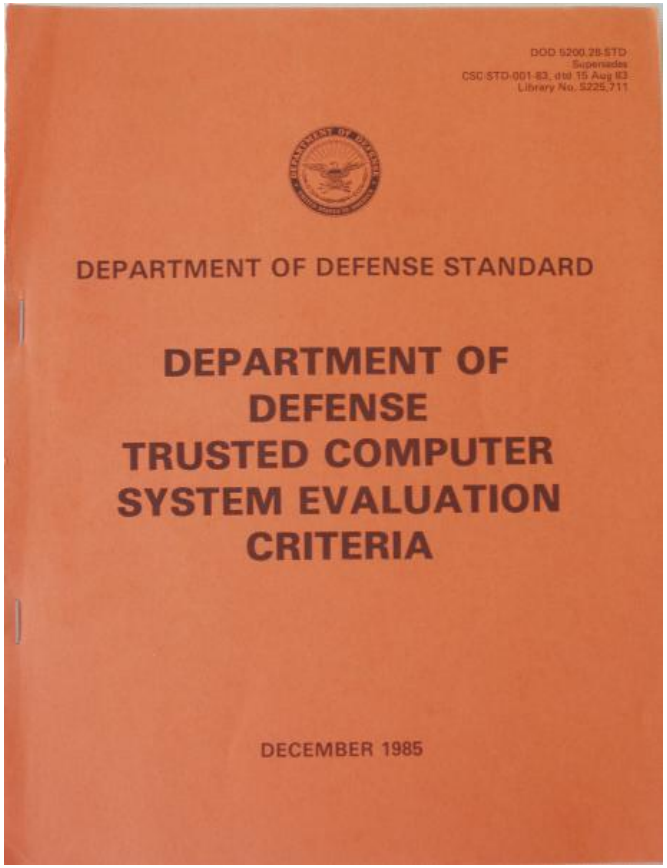
Работник – Владелец Устройства

Сервисы Компании

Может ли **Владелец Информации**:

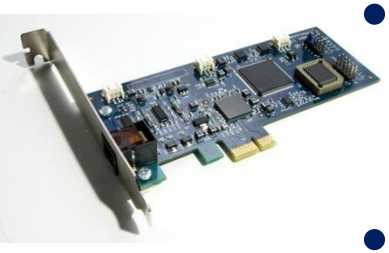
- Доверять устройству удаленный доступ к сервисам Компании?
- Доверять обрабатываемым на устройстве данным (конфиденциальность и целостность)?
- Доверять устройству обработку данных?
- Закрыть доступ к своей информации в любой момент?

ДОВЕРЕННАЯ СИСТЕМА



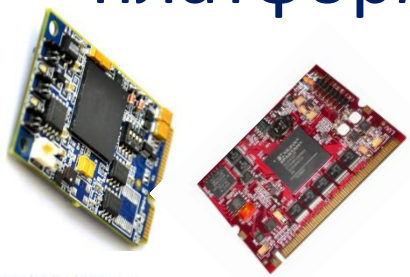
- система, использующая аппаратные и программные средства для обеспечения одновременной обработки информации разной категории секретности группой пользователей без нарушения прав доступа.

Резидентные компоненты безопасности ЭЗ/АПМДЗ

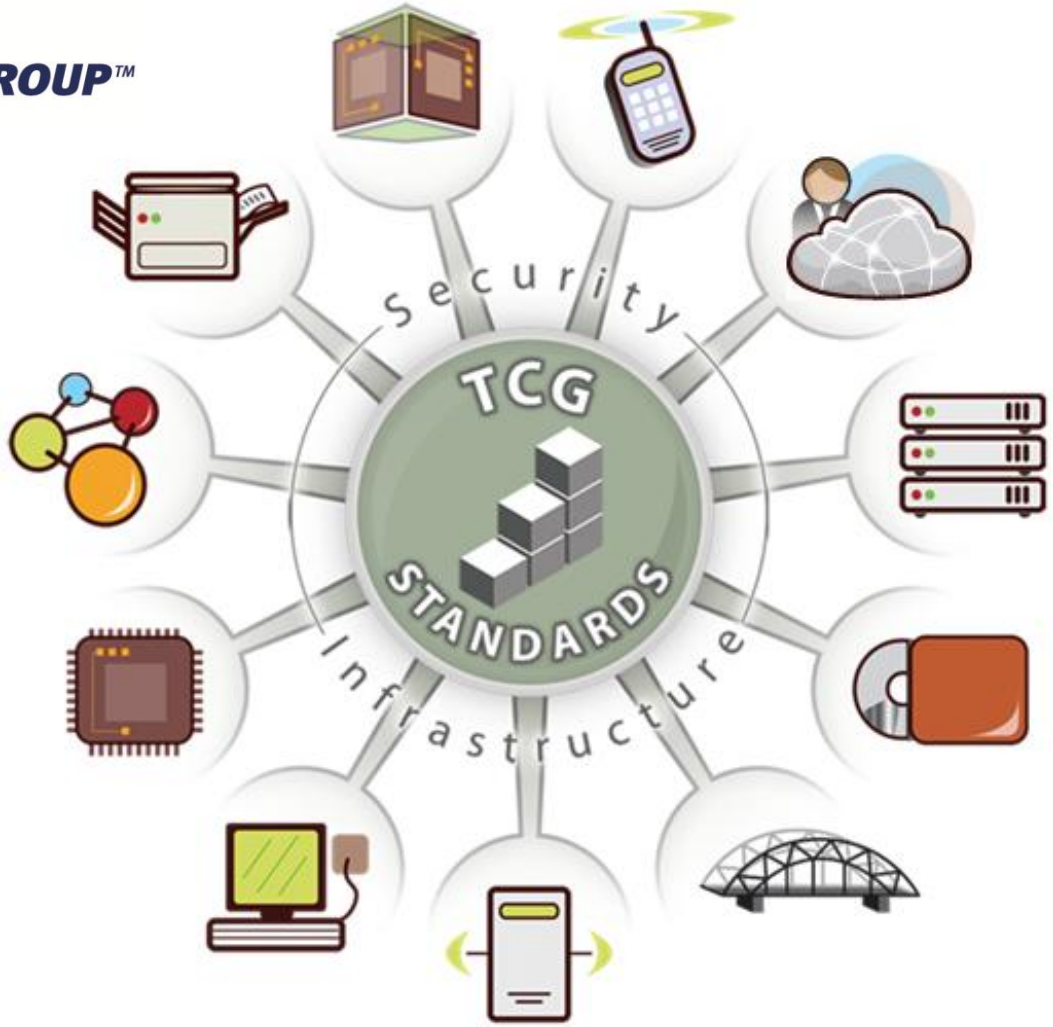


Проблемы:

- RAID? Шифрование диска (FDE)?
- Ultrabook, Tablet PC, smartphone? А что с гарантией? Совместимость?
- Удаленная аутентификация платформы?
- Цена?



Доверенная среда TCG



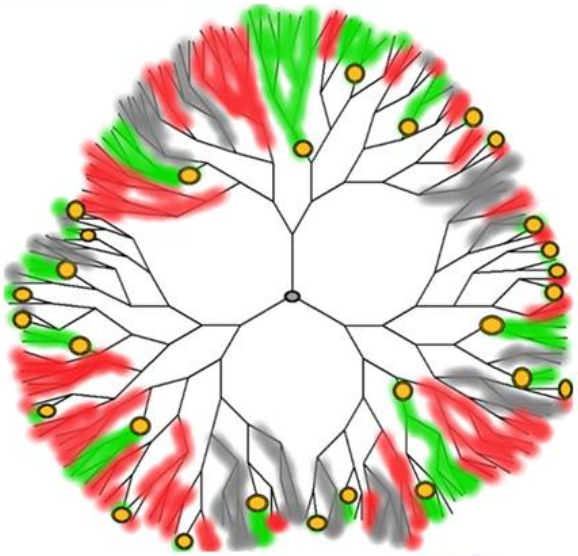
Взлом TPM

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

От традиционного подхода к Integrity Guard

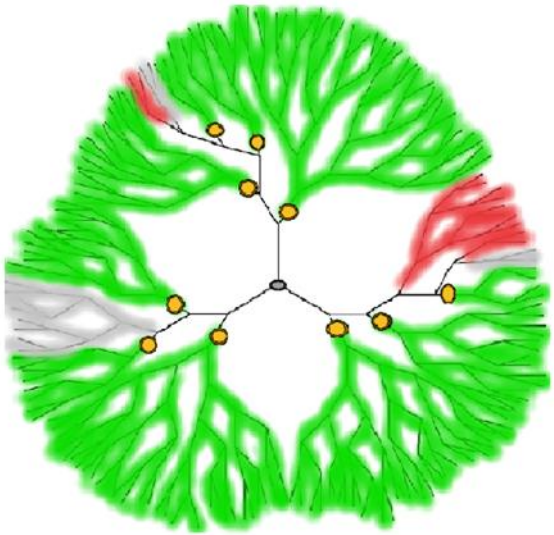


Контрмера

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

Сценарии BYOD: разделение данных

Личные Данные
данные Владельца Устройства – IO_1

Данные Компании

Корпоративная электронная почта

Сторонние приложения, социальные сети, мультимедиа

Владелец Устройства

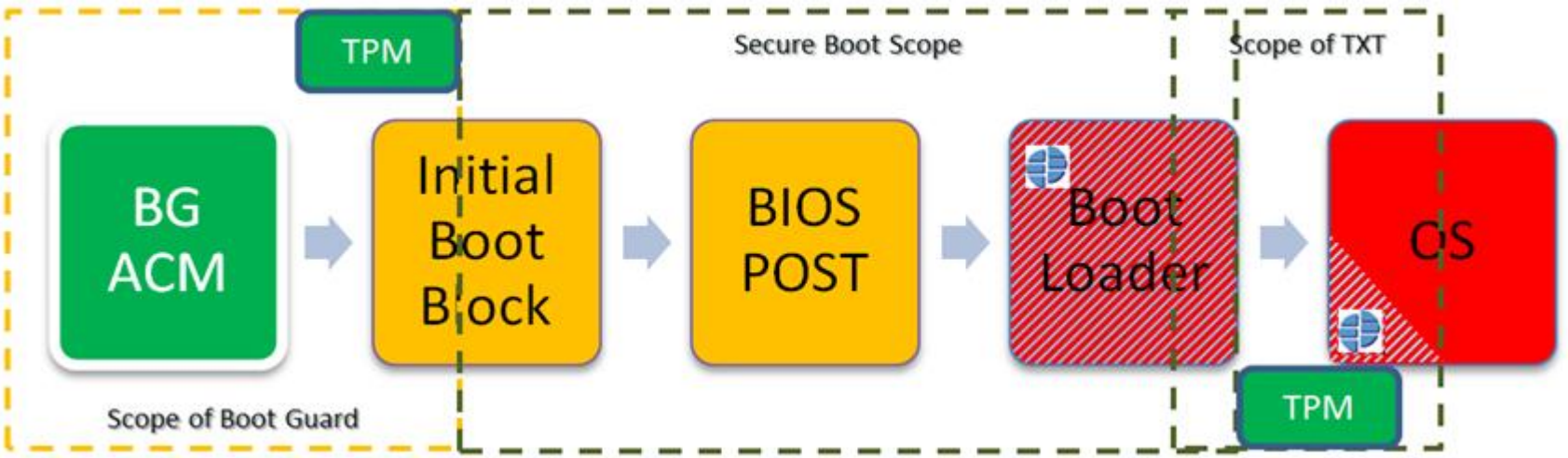
Аппаратный Корень Доверия
База для защиты на устройстве

- Корпоративных данных от неавторизованного доступа
- Личных данных от неавторизованного доступа владельцев информации

IO = Владелец Информации

Логическая архитектура мобильного устройства NIST

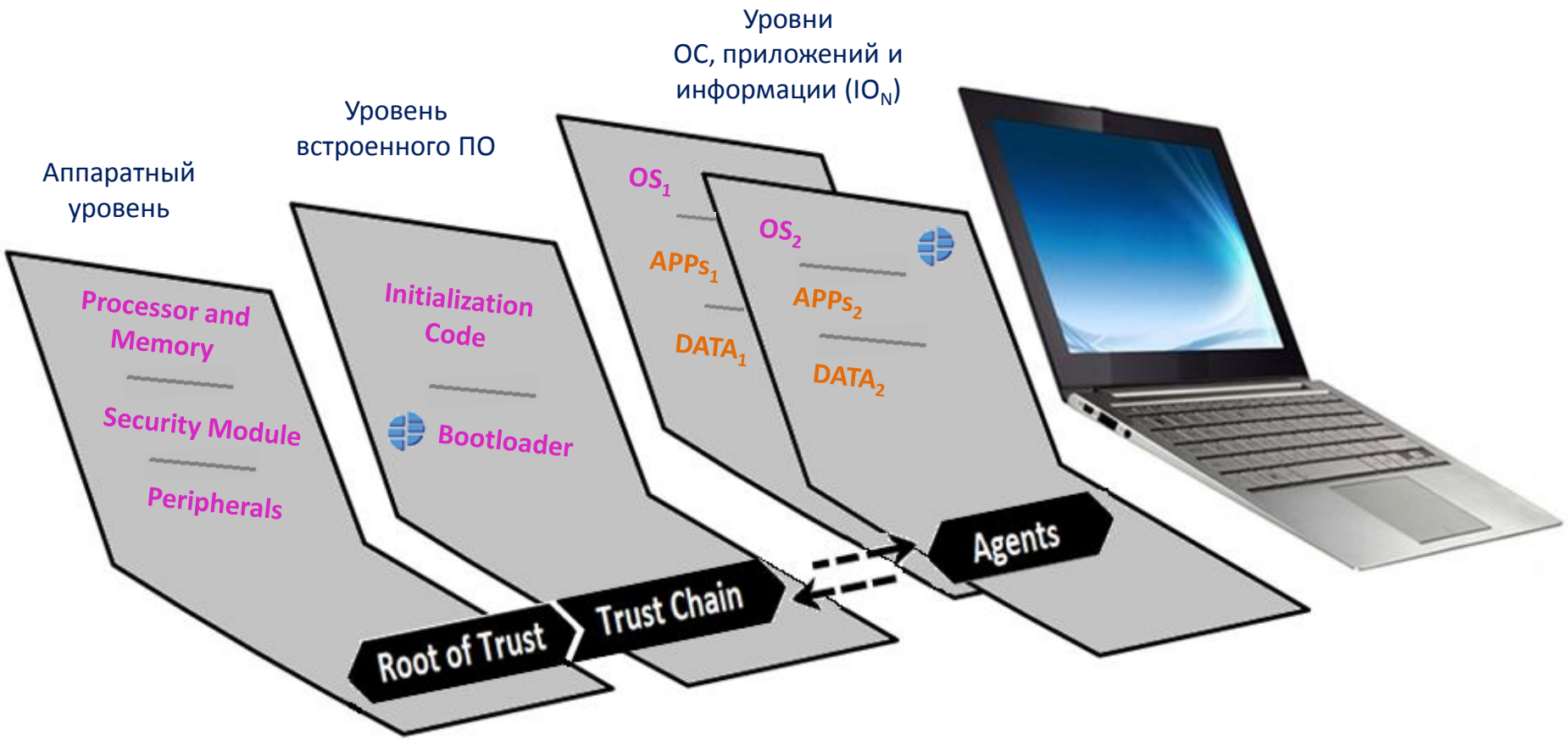
Мобильное ЗАРМ - Модуль ДСК



СПО ЭЛВИС+, разработанное в соответствии с требованиями регуляторов, предназначено для:

- доверенной начальной загрузки компьютера с контролем целостности его конфигурации, BIOS, начального сектора диска, СПО ЭЛВИС+ и критичных файлов и настроек ОС;
- обеспечения конфиденциальности хранимых данных при утере или краже компьютера за счет шифрования жесткого диска алгоритмами, соответствующими Российскому законодательству.

Модуль ДСК: Логическая архитектура



Модуль ДСК Roadmap

Модуль ДСК

Thin Client

Ultrabook

chromebook

СПО МОДУЛЬ-Z

TNC support

Tablet

Windows 8 Phone

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;
- Репутация ведущих производителей «железа» и ПО, использующих TPM;
- Технология является сегодня единственным практическим методом обеспечения доверия к мобильным устройствам.

Благодарю за внимание