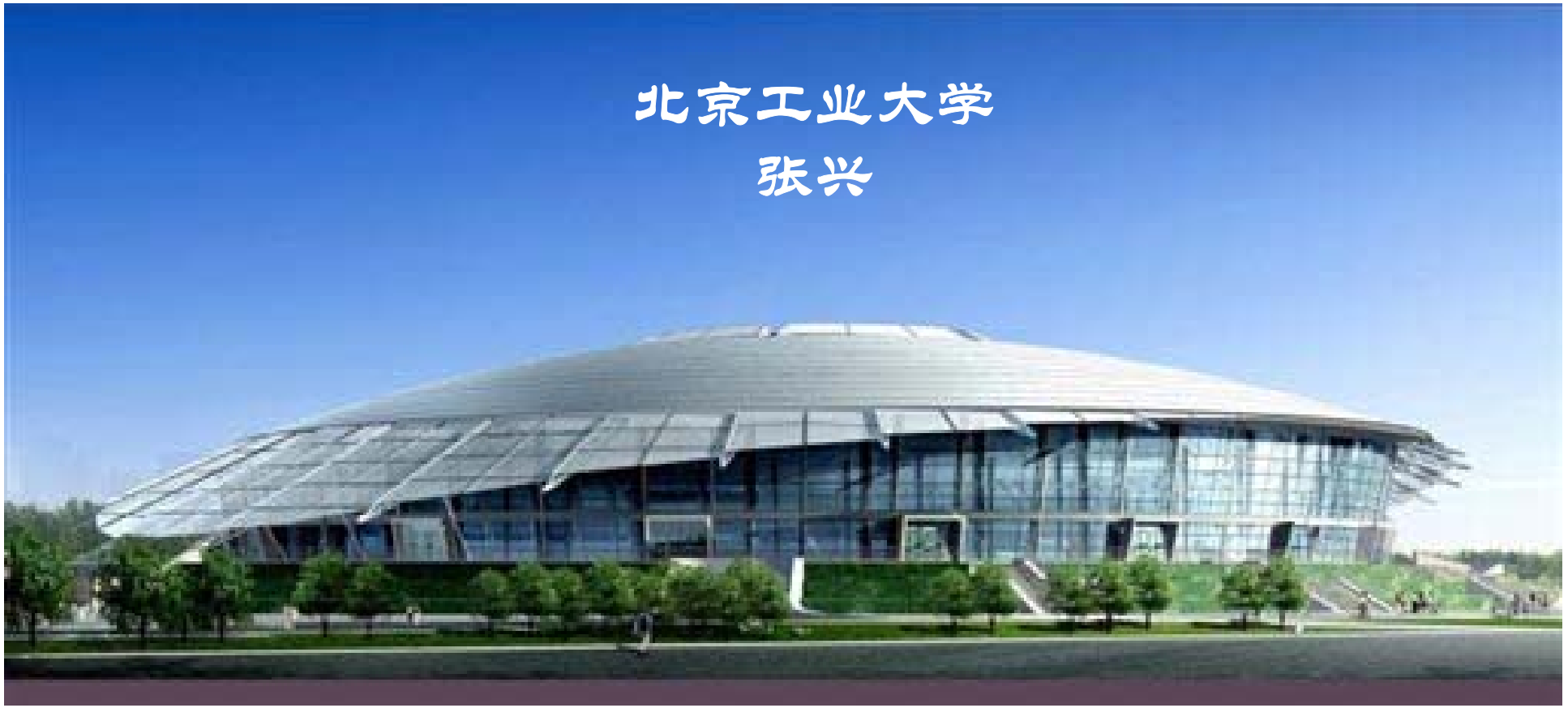
嵌入式系统联谊会
www.esbf.org.cn

可信计算技术与嵌入式系统

北京工业大学
张兴



主要内容

- 可信计算概念
  - 背景、概念、技术特点
- **PC中的可信计算**
  - 工业界做法、可信平台模块TPM、应用场景
  - 标准制定过程、技术路线、目前研究结果
- 嵌入式系统中的可信
  - 现状、需求、实现方法

一.可信计算概念

可信计算的定义

- 社会学/哲学/
  - ***To trust an entity is to give it some power to harm you***
- **TCG**
  - 如果它的行为总是以预期的方式，达到预期目标，则该实体是可信的
- **ISO/IEC15408**
  - 参与计算的组件、操作或过程在任意的条件下是可预测的，并能够抵御病毒和物理干扰
- 高可信软件
  - 可用性、可靠性、可维护性、安全性、健壮性、可测试性、可维护性等
- 微软的可信赖计算
- **IEEE总结出的可信的定义，11类20多个定义**

对可信的理解

- 可信就是可预期，保持原状不被篡改，可证实
  - 可信计算是安全的基础，从可信根出发，解决**PC**机结构所引起的安全。
  - 可信既有技术上的“可信”，又有社会学“可信”，双重含。因为可信最终反映的是软件、硬件产品的设计者、制造者的可信，厂商的可信，品牌的可信。用户相信软件、硬件产品的设计者、制造者们按照所声称的规格实施了生产。同时，可信也是各方的利益在产品中的一个平衡。
  - 软件、硬件产品的设计者、制造者完成的产品交付到用户（所有者/使用者）所声称的状态。如果其运行的状态一直处于原始状态，则它是可信的。一旦出现不可信的状态，系统应该感知并报告这些部件的不可信状态。易变部件的原始状态。
  - 从用户角度看，计算机系统所提供的服务是可信赖的，并且，这种可信赖是可论证的.

信息安全呼唤可信计算

- 由于计算机总是出现安全问题，系统出现病毒、木马，甚至崩溃，一再“失信”，出现了信任危机，所以才会关注可信计算
- 如果你不信任一个人，就不会交给他事情，但对计算机不管信任不信任，却不得不将文件存储，不得不将重要系统的控制权交给计算机，所以才关注可信

可信计算技术

- 根源： PC机体系结构的简化，系统不分执行“态”，内存无越界保护等等，使操作系统难以建立真正的TCB
- 导致：资源配置可以被篡改；

  恶意程序被植入执行；

  利用缓冲区（栈）溢出攻击；

  非法接管系统管理员权限等

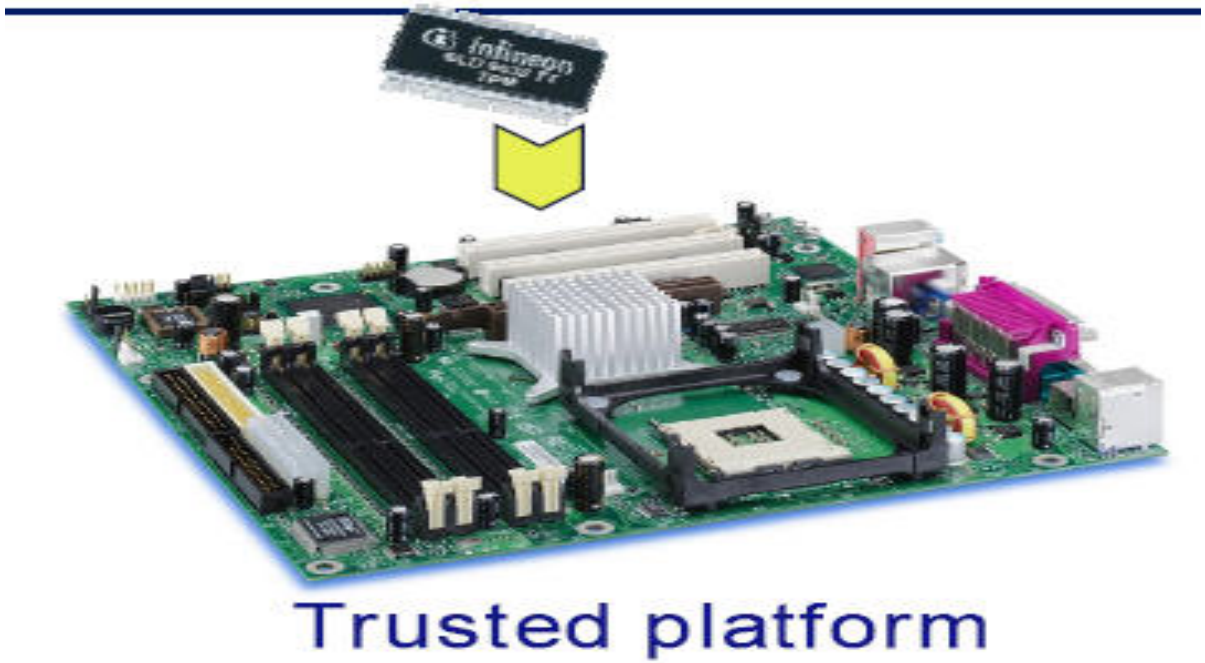
新型计算呼唤可信计算

- 互联网
- 云计算
- 物联网

二.计算机中的可信计算

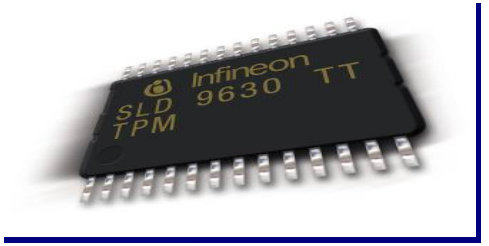
工业界的做法

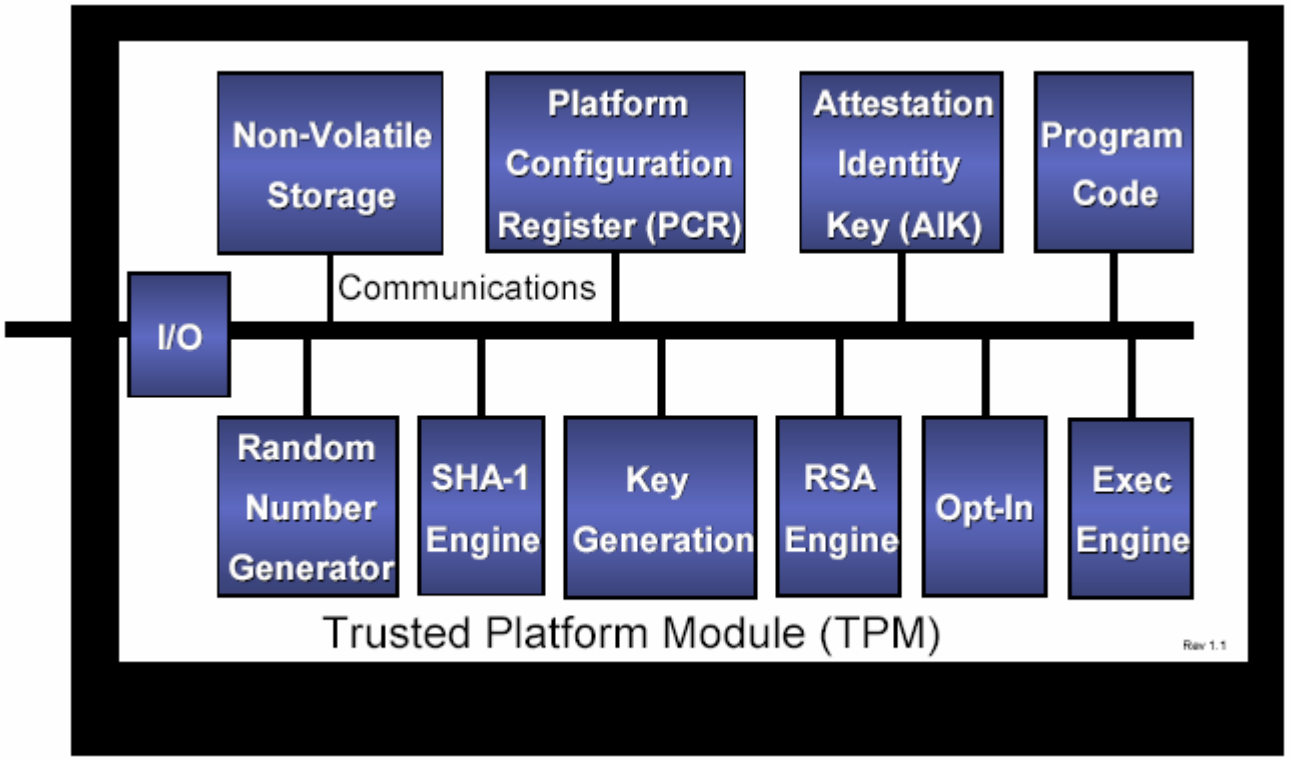
- 在主板上嵌入一个专用的芯片可信平台模块，目的是增强计算平台的安全性。



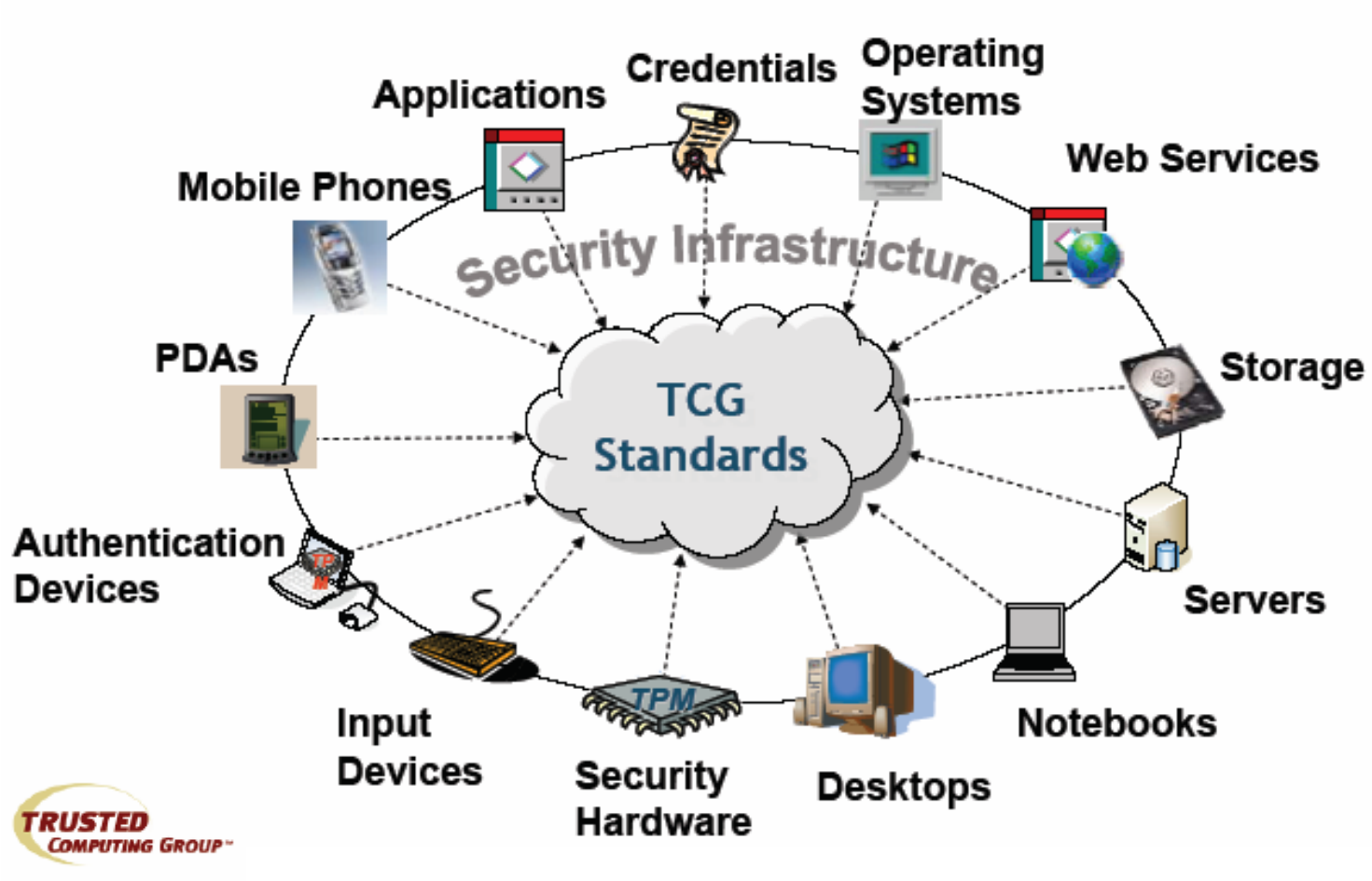
TPM（Trusted Platform Module） *可信平台模块*

可信平台模块－TPM


Infineon
SLD
TPM
9630
TT


Non-Volatile Storage
Platform Configuration Register (PCR)
Attestation Identity Key (AIK)
Program Code
Communications
I/O
Random Number Generator
SHA-1 Engine
Key Generation
RSA Engine
Opt-In
Exec Engine
Trusted Platform Module (TPM)
Rev 1.1

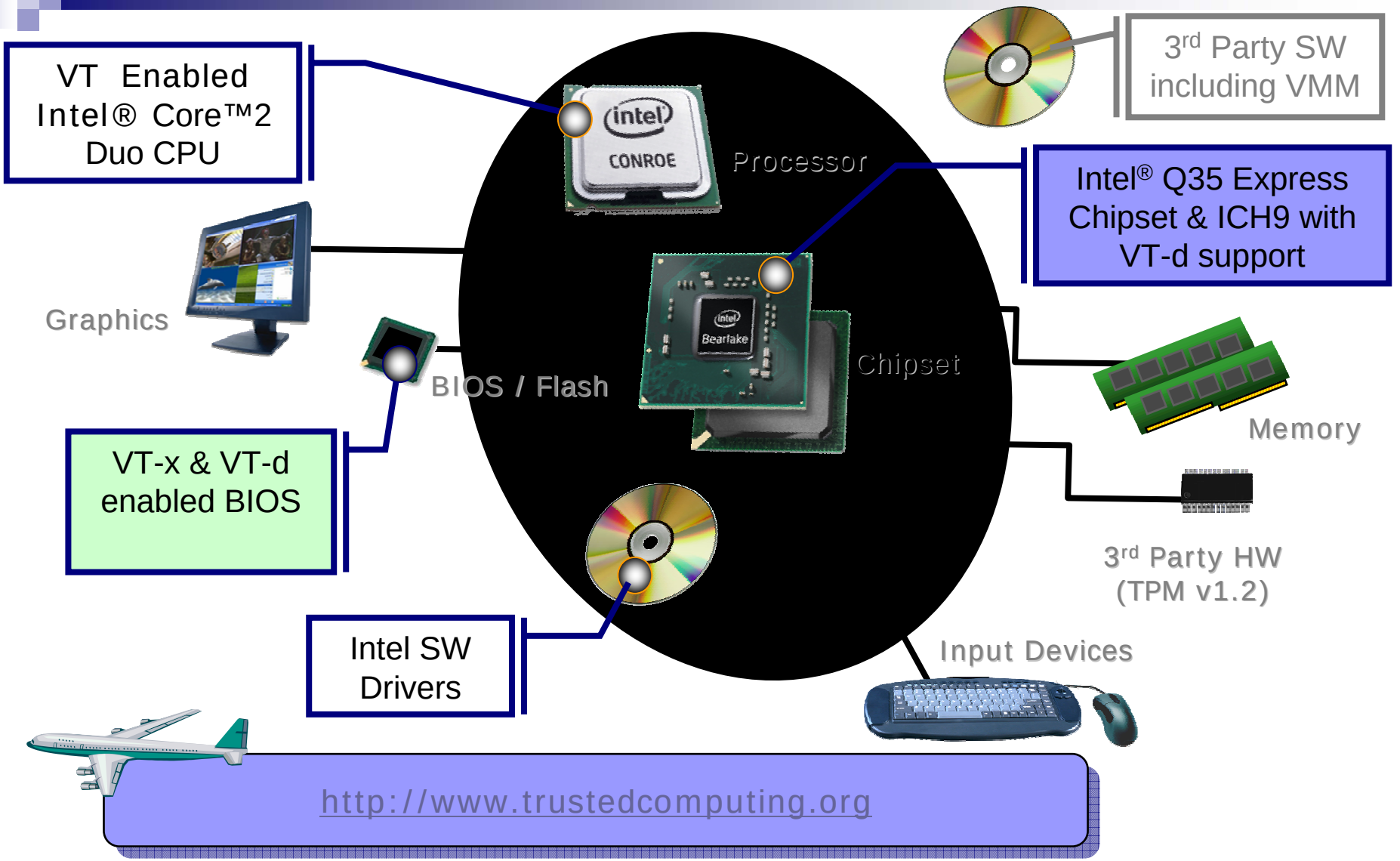
可信计算涉及产品


Applications
Credentials
Operating Systems
Web Services
Mobile Phones
Security Infrastructure
PDAs
TCG Standards
Storage
Authentication Devices
Servers
Input Devices
TPM
Security Hardware
Desktops
Notebooks
TRUSTED COMPUTING GROUP

可信计算产品前景

- 2010年，基本上所有的笔记本电脑和大多数台式机都将配置有TPM 芯片。
- TPM模块价格下降和软件应用成熟；
- PC中的大多数TPM将被集成到其它组件中；
- 最终将会在CPU芯片组中集成TPM。

可信计算平台－ Intel® Weybridge VT平台元器件



注: VT-x 是指 Intel® VT， VT-d 是指 Intel® I/O定向VT

基于TCM的样机－瑞达

平台身份可信

- 平台身份可信：设备证书**EK**，隐匿性需要，引入**PIK**

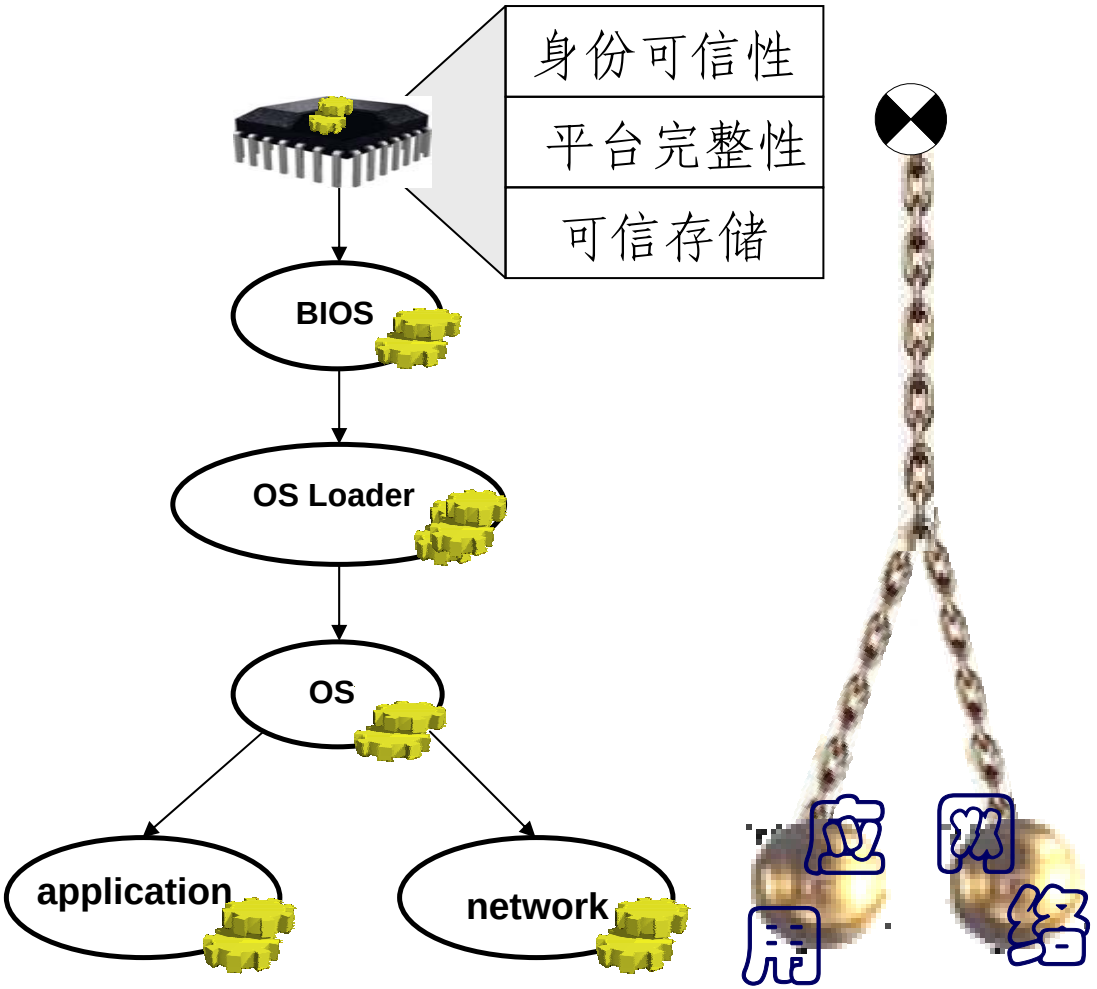
平台完整性

- 用杂凑密码算法，对所有度量对象进行校验

存储可信

- 基于物理保护和密钥树的保护机制
- 密钥树管理，结合授权数据

可信计算的核心思想

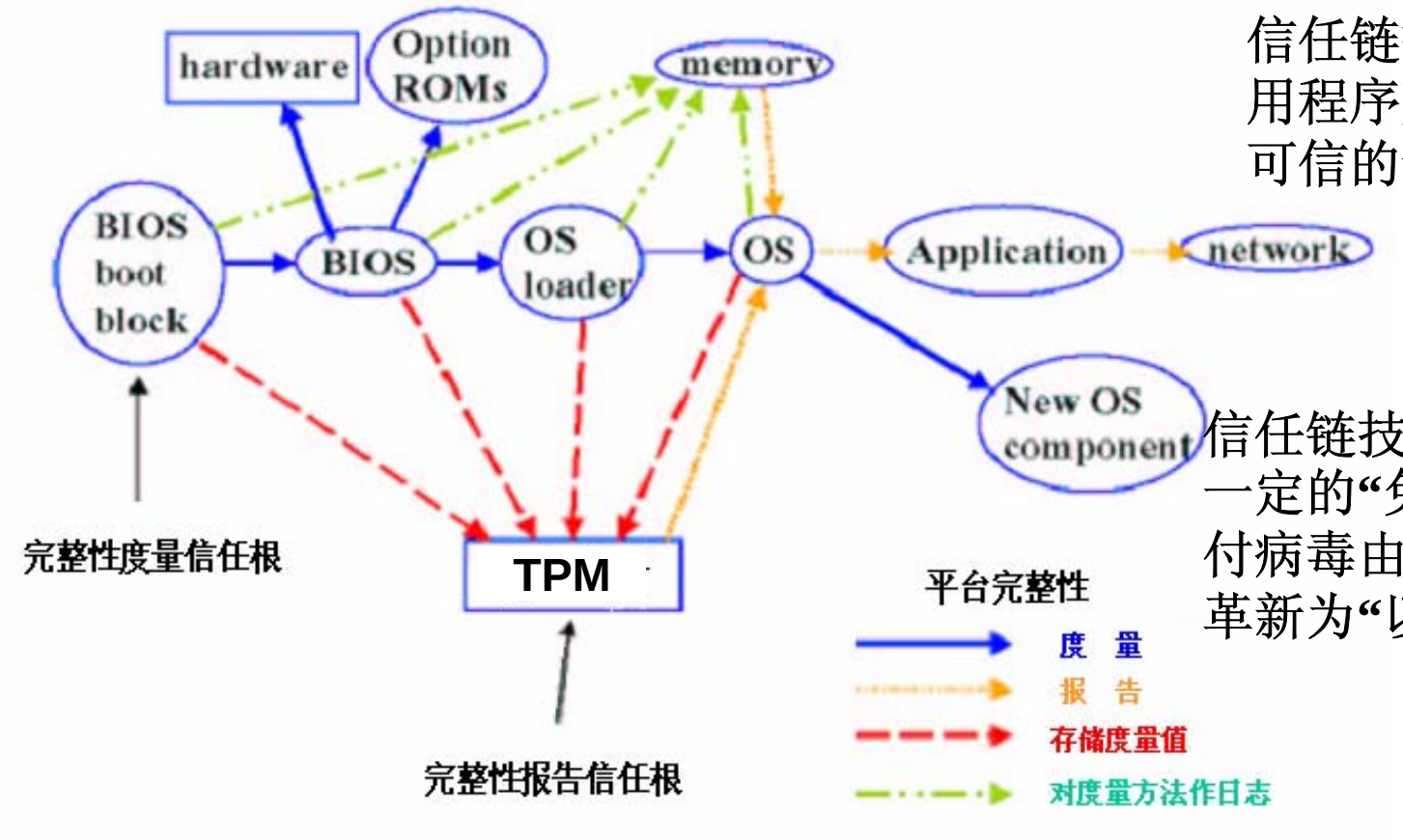


可信根：硬件模块，嵌入到主板，保证系统完整性、身份可信性、安全存储和可信存储根。

信任链：从信任根开始，一级验证一级，一级信任一级，使源头信任得以传递到整个网络，实现系统可信。

信任链技术

举PC中一个例子：信任链技术在计算机启动中的应用。



信任链技术为应用程序建立一个可信的计算环境

信任链技术为系统建立一定的“免疫”能力；对付病毒由“敌变我变”，革新为“以不变应万变”

工业界可信计算平台

- 标识平台唯一性和可信性身份（发一张身份证）
  - 提供不可否认的可靠的平台身份验证
  - 电子交易中信息和数据传递得到可靠的安全保障
- 平台完整性度量与报告（派一位监管员）
  - 保证用户每次启动的是一台“干净”的系统
  - 建立系统一定的“免疫”机制
- 硬件芯片级数据安全保护（安一个保险箱）
  - 提供密钥安全生成和保护的机制

三.可信计算标准制定

我国标准制定面临的问题

- 要在不可知、不可控的基础上做到可信
  - 我们国家面临着严峻的挑战。目前，**CPU**、**BIOS**、主板、操作系统等关键部件大多被国外公司所垄断。在某种程度上，这些关键部件对我们而言，是不可知、不可控的，并且在短时间内也不会有大的改观，这也是我国研究可信计算与国际**TCG**等研究可信计算面临的不同问题。
  - 微软黑屏警示盗版（点击）

可信计算标准制定过程－研究跟踪

- **2005**年**10**月沈昌祥院士在北京工业大学启动“可信计算密码支撑平台联合工作组”筹组和预研工作
- **2005**年**12**月，提出以密码技术为基础的思路，选择了“密码”为突破口，首先制定可信计算平台密码规范，密码体系采用我国自己的标准，确保信任根密码的自主可控

可信计算标准制定过程－打基础

- **06**年**3**月国密局下达以“两个规范”为主的可信计算平台密码方案研究任务
  - 可信计算平台密码规范
  - 可信计算平台密码检测规范
  - 承担单位
    - 北京工业大学
  - 参加单位
    - 联想、兆日、瑞达、华大、中兴、兴唐、卫士通

可信计算标准制定过程－打基础

- **06**年**8**月商密办组织验收，验收意见：“在算法使用、密钥管理、授权协议、证书管理等方面有创新，体现了以我为主、自主创新的研究目的，为形成我国可信计算平台相关标准和专利奠定了良好基础，为推动我国可信计算产业发展提供了有力的密码技术支撑。”

可信计算标准制定过程－打基础

- **2007**年，国家密码管理成立独立的工程验证组，冯登国专家组组长，参与企业包括联想、兆日、瑞达、同方、方正等。经过一年时间的验证，结果表明“可信计算平台密码方案”科学可行，并由“两个规范”形成了“可信计算密码支撑平台功能与接口规范”。
- **2007**年**12**月国密局发布“可信计算密码支撑平台功能与接口规范”。同时，国内十二家企业举行可信计算平台产品发布会。

可信计算标准制定过程－构主体

- **2007**年**2**月，全国信息安全标准委员会将“可信计算关键标准研究”课题下达给北京工业大学，课题负责人沈昌祥院士，由沈院士牵头，联合有积极性的相关企业和部门共同研究，组织成立了以企业为主体的“产学研用”结合的“可信计算标准工作组”，研究制定可信计算标准方案

可信计算标准技术路线

- 先研究方案：学习借鉴**TCG**，结合国内用户需求，研究解决什么问题，创新是什么，并且验证是否可行。
- 方案基础上制订标准，同时研究专利

可信计算标准组织路线

- 企业为主体，产学研用结合
- 集中攻关与分散研究相结合
  - 集中时的任务：确定方案、讨论问题、整合文档、明确下一步计划。
  - 分散时的任务：分工编写，随时沟通，每周提交一个版本，组长整合，工大汇总

企业为主体的产学研创新团队

- 中国电子技术标准化研究所
- 西安电子科技大学
- 深圳华为技术有限公司
- 西安西电捷通无线网络通信有限公司
- 上海中标软件有限公司
- 中安科技集团有限公司
- 瑞达信息安全产业股份有限公司
- 中国长城计算机深圳股份有限公司
- 北京工业大学
- 南京百敖
- 中软华泰信息技术有限责任公司
- 武汉大学
- 信大捷安
- 北京理工大学
- 信大捷安
- 浪潮集团有限公司

JSM

S²C 中标软件

Great Wall 长城

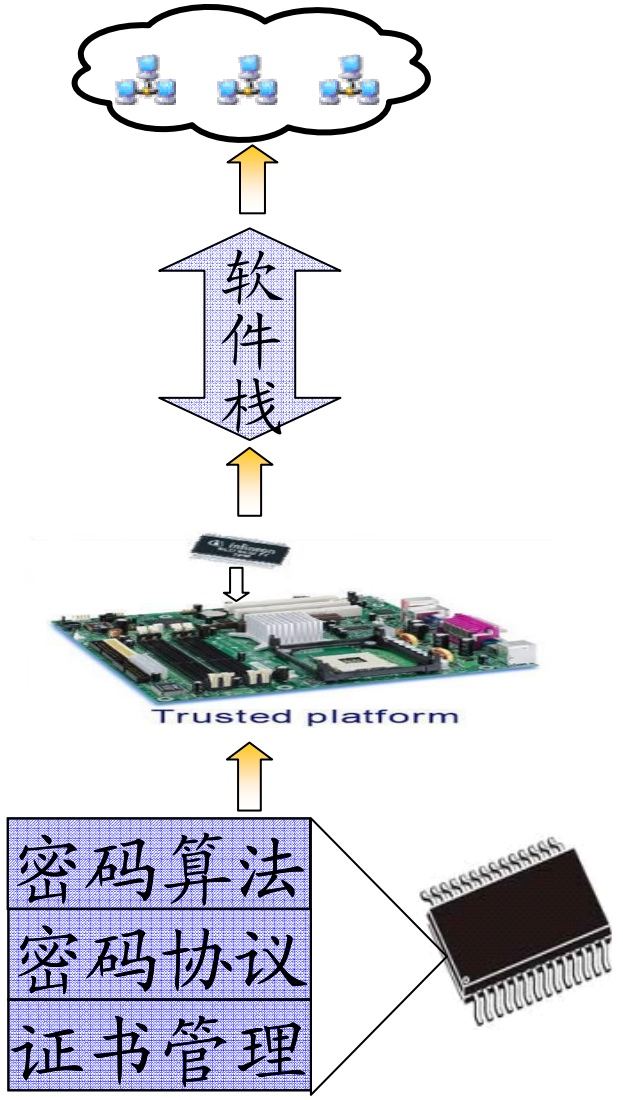
西电捷通 IWNCOMM

CIIG

HUAWEI

可信计算标准主体框架

- 以密码技术为基础
- 以芯片为信任根
- 主板为平台
- 软件栈为核心
- 网络为纽带



可信计算平台的四个主体技术标准

- 芯片-可信平台控制模块规范
- 主板-可信平台主板功能接口规范
- 软件-可信基础支撑软件规范
- 网络-可信网络连接架构规范

- 有了这四个标准，才能构建我国可信计算的基本框架，能使各厂商按我国的可信密码规范来实现可信计算芯片、可信计算平台及基本的可信应用。

可信计算平台的四个配套标准

- 在“可信平台控制模块”等四个面向主机的主体标准基础上，研究制定基础配套标准，解决服务器和存储应用等基本应用的框架性问题，满足局域网应用需求，逐步完善我国可信计算体系标准。
- 基础配套标准包括：
  - “可信计算规范体系结构”
  - “可信服务器平台规范”
  - “可信存储规范”
  - “可信计算机可信性测评规范”

四.嵌入式系统中的可信计算

嵌入式系统中的可信更重要

- 由于嵌入式系统的资源和实时性要求，软硬件结构有可能进一步简化，可信问题实质上更加严重，只是嵌入的专用性使得可信问题并不突出

嵌入式系统中的可信应用

- 打印机中的盒
- **ATM**机
- 税控机
- 汽车电子中的控制失灵

国家税控服务器

- 商业典型应用示范系统一个，利用税控服务器，的可信计算模块建立了一套安全机制，由**TPM**模块的可信根开始，逐层，逐设备，对整个系统的安全性提供了可信链保护。

北京工業大學
BEIJING UNIVERSITY OF TECHNOLOGY

谢谢大家！

Q & A