

RSA[®]CONFERENCE C H I N A 2012

RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑



可信计算的一些新发展

张焕国

武汉大学计算机学院



专题会议主题：

专题会议分类：

RSACONFERENCE
C H I N A 2012

目 录

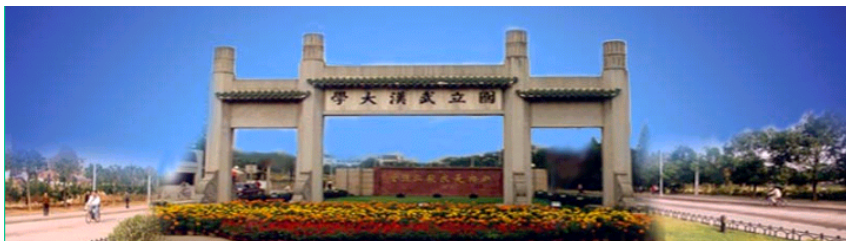
- 一、可信计算的成绩与问题
- 二、可信平台模块的发展
- 三、可信软件的发展
- 四、可信计算应用的发展
- 五、参考文献



一、可信计算的成绩与问题

1、可信计算十年的辉煌历程

- 无论是TCG的可信计算，还是中国的可信计算，都已经经历了十年的发展历程。
- 在这十年当中，可信计算已经取得了丰硕的成果，但也存在一些问题

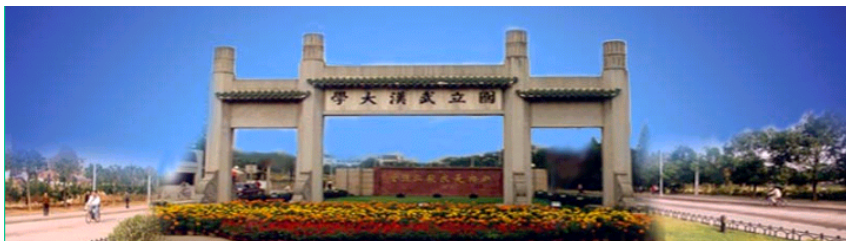


一、可信计算的成绩与问题

2、十年来可信计算的丰硕成果

① 在世界范围形成了可信计算的高潮

- 美国TCG
- 欧洲OpenTC
- 中国可信计算联盟（CTCU）
- 可信计算技术已经渗透到信息领域的各个方面



一、可信计算的成绩与问题

2、十年来可信计算的丰硕成果

② TCG制定出一系列的规范

♣ 可信PC规范

♣ 可信服务器规范

♣ 可信平台模块 (TPM) 规范

♣ 可信软件栈 (TSS) 规范

♣ 可信网络连接 (TNC) 规范



一、可信计算的成绩与问题

2、十年来可信计算的丰硕成果

③ 中国也制定出一系列的规范

- ♣ 可信计算平台密码技术方案
- ♣ 可信计算密码支撑平台功能与接口规范
- ♣ 可信PC平台主板技术规范
- ♣ 可信网络连接技术规范
- ♣ 其它



一、可信计算的成绩与问题

2、十年来可信计算的丰硕成果

④国内外推出一系列的可信计算产品

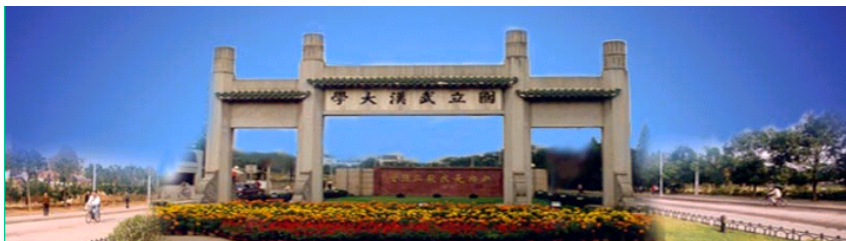
♣ 多种TPM芯片

♣ 各种可信PC机

♣ 可信服务器

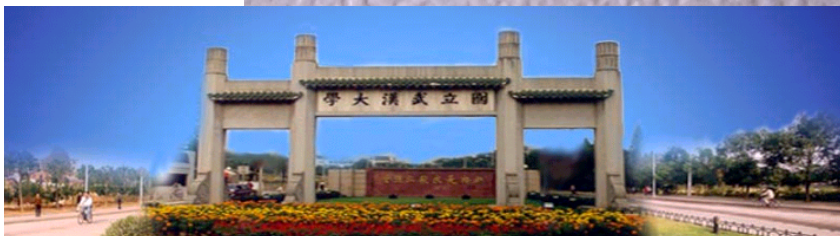
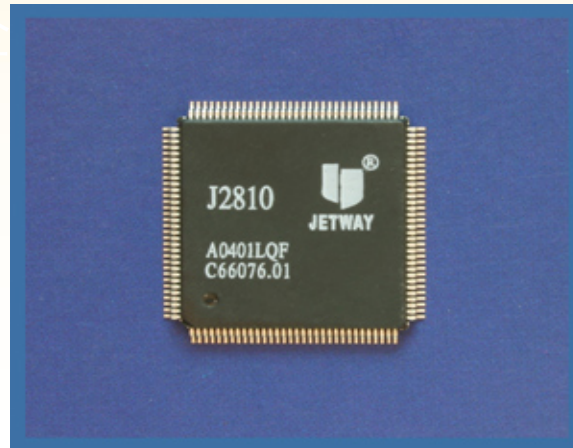
♣ 可信PDA

♣ 可信网络连接产品



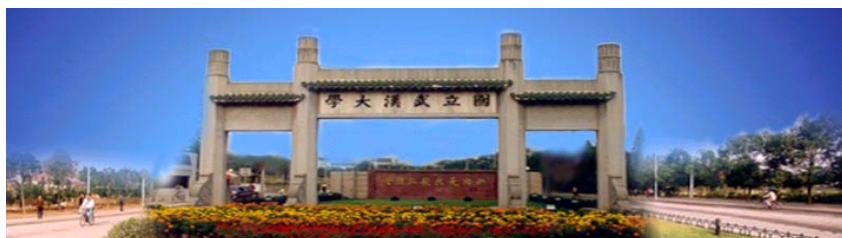
一、可信计算的成绩与问题

●中国的TPM芯片



一、可信计算的成绩与问题

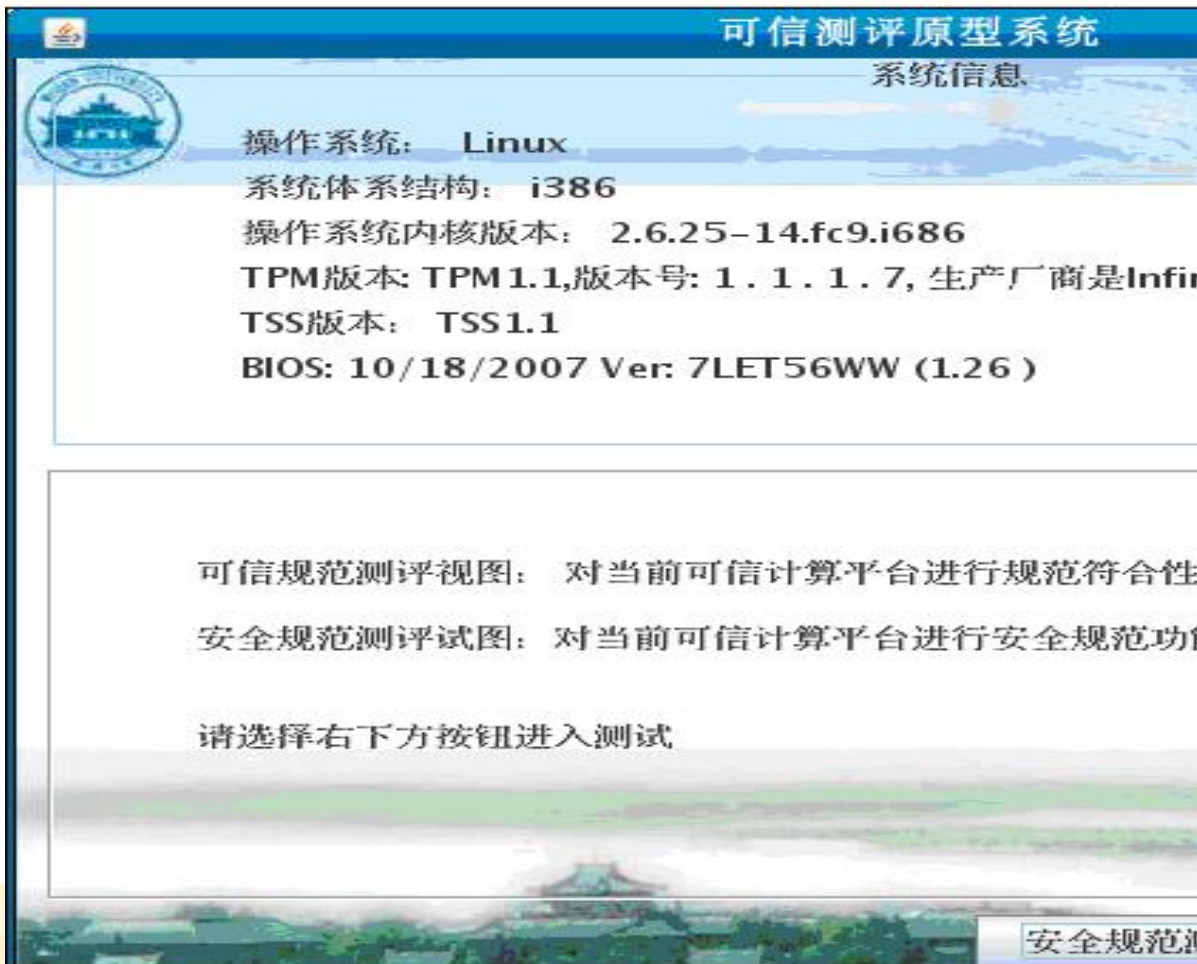
●中国的可信PC



一、可信计算的成绩与问题

●中国的可信PC测评系统

●中国的可信PDA



可信测评原型系统
系统信息

操作系统: Linux
系统体系结构: i386
操作系统内核版本: 2.6.25-14.fc9.i686
TPM版本: TPM 1.1, 版本号: 1.1.1.7, 生产厂商是Infir
TSS版本: TSS 1.1
BIOS: 10/18/2007 Ver: 7LET56WW (1.26)

可信规范测评视图: 对当前可信计算平台进行规范符合性
安全规范测评视图: 对当前可信计算平台进行安全规范功能

请选择右下方按钮进入测试

安全规范测评视图 可信规范测评视图



一、可信计算的成绩与问题

3、可信计算存在的一些问题

我们在《中国科学》2007年2期中指出，可信计算发展中还存在的5个问题：

- ① 理论研究滞后
- ② 一些关键技术尚待攻克
- ③ 缺少操作系统、网络、数据库和应用的可信机制配套
- ④ 缺少安全机制与容错机制的结合
- ⑤ 可信计算应用尚少



一、可信计算的成绩与问题

3、可信计算存在的一些问题

近年来这些问题有明显进展，但仍没有根本解决。

■ 国内外可信计算应用较少的原因

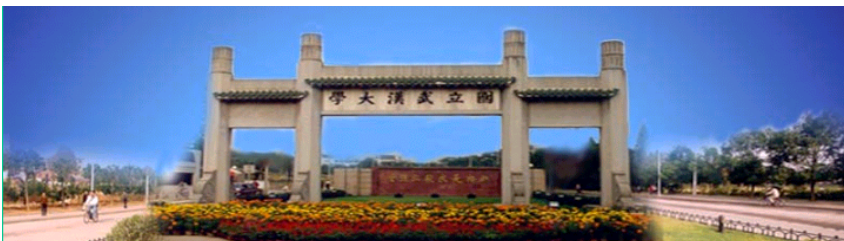
- ① TPM是可信计算的核心芯片，其规范不断升级变化，不能稳定应用
- ② 可信计算平台是硬件平台，缺少操作系统、数据库和应用软件的可信机制配套，用户使用不方便
- ③ 提供给用户的可信计算平台多，实际问题的解决方案少
- ④ 社会上对“可信”的理解不统一，影响应用



二、可信平台模块TPM的发展

1、TPM的发展历程

- 十年间, TPM从TPM 1.0 → TPM 1.1 → TPM 1.1b → TPM 1.2 → TPM2.0
- 2009年TPM 1.2 被ISO接受为国际标准
 - ◆ ISO/IEC 11889-1
 - ◆ ISO/IEC 11889-2
 - ◆ ISO/IEC 11889-3
 - ◆ ISO/IEC 11889-4



二、可信平台模块TPM的发展

2、TPM 1.2 总体是成功的，但存在一些问题

- 适合PC平台，不适合服务器平台和嵌入式平台
- 密码方面存在较多不足：
 - ◆ 只配置公钥密码，没有对称密码，不方便
 - ◆ 公钥密码和HASH函数的设置存在一些问题
 - ◆ 密码方案不支持本地化，世界各国应用困难
 - ◆ 密钥和证书种类繁多，管理困难



二、可信平台模块TPM的发展

3、TCG为解决这些问题，推出TPM2.0

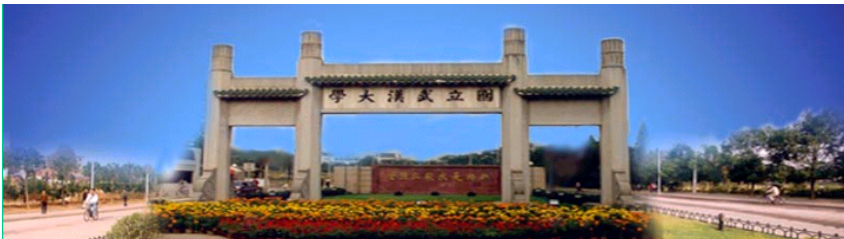
■ TPM 2.0 设计与以前版本的不同

◆ 密码算法多样化，更合理

- 公钥密码：RSA, ECC, 其它
- 对称密码：AES, 其它
- 函数：SHA-384, 其它
- 当前，每一个密码算法的强度不得低于128位

◆ 支持密码算法本地化

- 支持各国使用自己的密码，例如，中国SMS4, SM2, SM3
- 命令不依赖于具体的密码算法，统一命令结构和参数



二、可信平台模块TPM的发展

3、TCG为解决这些问题，提出TPM2.0

■ TPM 2.0 设计与以前版本的不同

◆ 支持虚拟化

- 云计算需要虚拟化
- 以前的TPM不支持虚拟化
- 芯片多核能够支持虚拟化

- 改变原密钥树结构
- 增加虚拟存储根密钥PSRK



二、可信平台模块TPM的发展

3、TCG为解决这些问题，提出TPM2.0

■ TPM 2.0 设计与以前版本的不同

◆ 统一授权框架

- TPM1.2中对应用、委托应用、迁移对象采用不同的授权方法
- TPM1.2中隐私保护模型不一致：有时是使用TPM保护隐私，而有时又假定必须有操作系统的参与
- 现在采用统一的授权框架
- 而且扩展了授权方法，允许利用对称签名和HMAC进行授权，并允许进行组合



二、可信平台模块TPM的发展

3、TCG为解决这些问题，提出TPM2.0

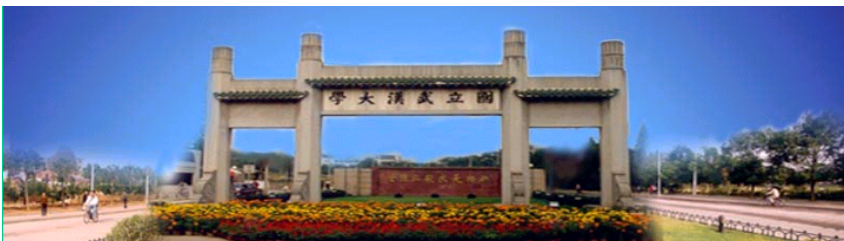
■ TPM 2.0 设计与以前版本的不同

◆ 增强了BIOS的支持

- 增加了一个由平台固件控制的存储层次，直接利用底层的密码功能

◆ 简化了控制模型

- 虽然对于一个对象TPM的操作可能有所限制，但所有命令在所有时间都是可用的，这使得基于TPM开发应用更方便



二、可信平台模块TPM的发展

3、TCG为解决这些问题，提出TPM2.0

■ TPM 2.0 设计与以前版本的不同

◆ 增强了健壮性

- TPM1.2中授权数据选择存在问题，一个低熵的授权数据可在中间人攻击中被猜测
- 密钥句柄未包含到HMAC中，导致非法的授权数据使用密钥
- 通过在授权会话HMAC中实施加盐操作来保护弱授权数据
- 将密钥名字包含至授权HMAC值中防止密钥替换攻击



二、可信平台模块TPM的发展

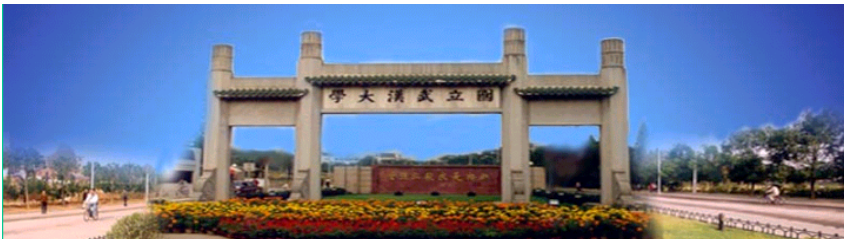
3、TCG为解决这些问题，提出TPM2.0

■ TPM 2.0 设计与以前版本的不同

◆ 管理更方便

- 用户很难理解TPM的管理，如TPM enable和active的区别
- 安全性和隐私性使用相同的保护机制
- 依赖于PCR值的密钥管理很困难

- 用于管理控制的模型更简单，比如只有开/关；
- 安全性和隐私性基于不同机制：基于SRK保护安全；基于EK保护身份隐私



二、可信平台模块TPM的发展

3、TCG为解决这些问题，提出TPM2.0

■ TPM 2.0 设计与以前版本的不同

◆ 改善了生态环境

- TPM1.2/TCM不能互操作
- TPM1.2和TCM都不能既满足国际化，又满足本地化
- SHA-1出现问题对TPM1.2的生态环境影响巨大
- 这表明不能依赖一个算法集，一旦算法出问题会导致TPM生态系统的巨大变化



二、可信平台模块TPM的发展

4、TPM2.0的密码机制

■ 设置6项密码功能

1. Hash函数

- 用于完整性校验，认证、单向函数，PCR扩展
- 使用经认可的且与非对称密码安全强度相当的Hash函数
- 例如，SHA384与ECC384匹配，安全强度都为192b



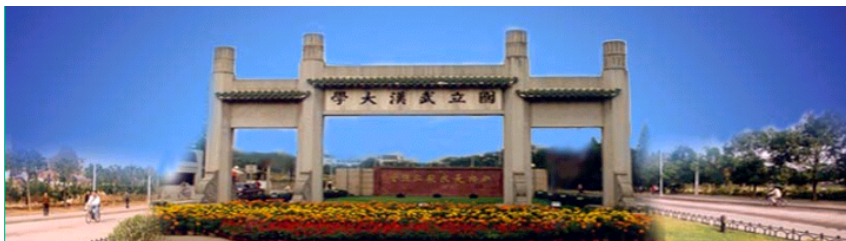
二、可信平台模块TPM的发展

4、TPM2.0的密码机制

■ 设置6项密码功能

2. 非对称签名与签名验证

- 非对称密码算法主要用于认证、证明、秘密共享
- TPM2.0至少应支持一种非对称密码算法, TCG采用RSA和ECC



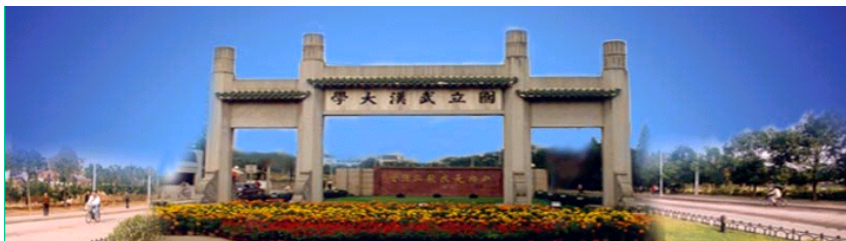
二、可信平台模块TPM的发展

4、TPM2.0的密码机制

■ 设置6项密码功能

3. 非对称加解密

- 非对称加解密主要用于少量重要数据的加解密，如利用数字信封形式加解密对称密钥
- 非对称密码加解密的速度是比较慢的



二、可信平台模块TPM的发展

4、TPM2.0的密码机制

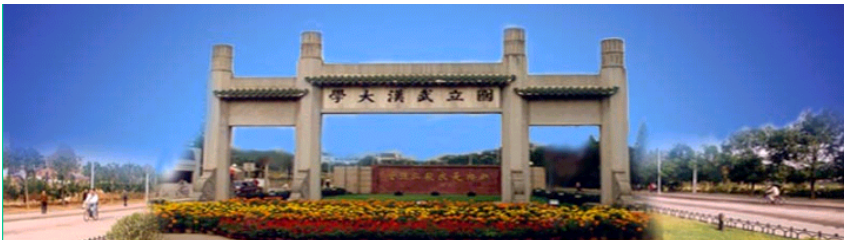
■ 设置6项密码功能

4. 对称签名 (HMAC) 与签名验证

- 由于基于Hash函数的消息认证码HMAC，具有良好的消息认证功能，TPM2.0充分发挥了它的作用。

- HMAC 采用FIPS 198a

$$\text{HMAC}(K, \text{text}) = \text{H}((K0 \oplus \text{opad}) \parallel \text{H}((K0 \oplus \text{ipad}) \parallel \text{text}))$$



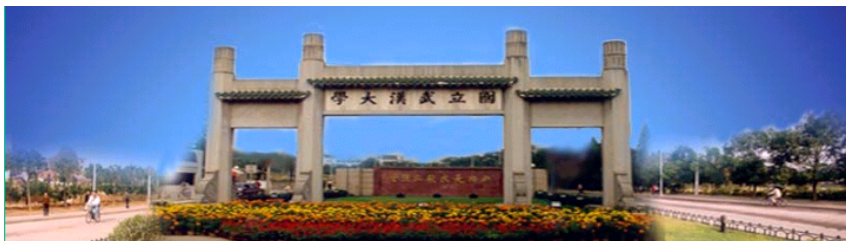
二、可信平台模块TPM的发展

4、TPM2.0的密码机制

■ 设置6项密码功能

5. 对称加解密

- 增加对称加解密是TPM2.0的一个进步
- 主要用于TPM命令参数加解密和存储在TPM外面的数据加解密
- 对于分组密码，采用CFB工作模式
- 对于基于Hash函数的掩码方式，进行异或加解密



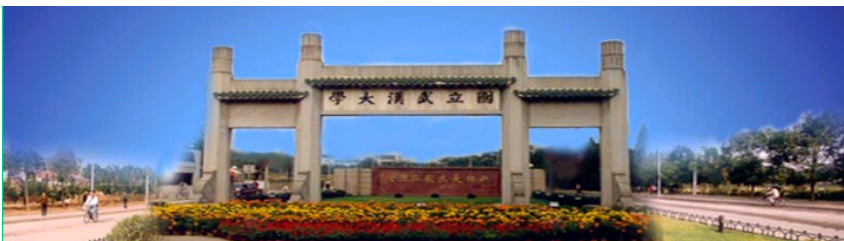
二、可信平台模块TPM的发展

4、TPM2.0的密码机制

■ 设置6项密码功能

6. 密钥产生

- 产生两种不同的密钥：普通密钥和主密钥
- 普通密钥用随机数产生器（RNG）产生
- 主密钥的产生：用RNG在TPM内部产生一个种子，利用密钥派生函数KDF基于这个种子产生出主密钥
- TPM2.0采用两种KDF：基于椭圆曲线的ECDH SP800-56A，基于HMAC的KDF SP800-108



二、可信平台模块TPM的发展

5、TPM2.0带来的一些新问题

■ 目前尚没有TPM2.0芯片和系统

- 企业推出TPM2.0芯片需要一定的时间

■ TPM2.0与TPM1.2不兼容

- 从TPM1.2过渡到TPM2.0需要一个较长的过渡时间

■ 多密码环境下的兼容性、安全性、可用性验证

- TPM2.0支持多密码算法，支持密码本地化
- 实际的兼容性、安全性和可用性需要验证



三、可信软件的发展

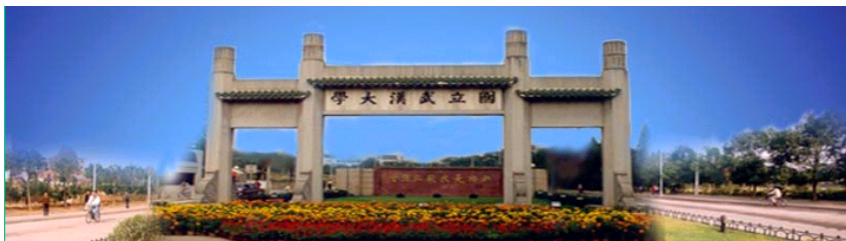
1、操作系统对可信计算的支持

■ 仅有可信计算平台，没有可信操作系统是不行的

- 长期以来，仅有TSS，缺少操作系统对可信计算的支持
- 这是可信计算缺少广泛应用的主要原因之一

■ 可信操作系统的发展

- 微软公司长期致力于操作系统对可信计算的支持
- 经历了从VISTA到WINGOWS 8 的发展历程



三、可信软件的发展

1、操作系统对可信计算的支持

■ Windows 8对可信计算的支持

- NEAT安全技术原则

- ◆ Necessary
- ◆ Explainable
- ◆ Actionable
- ◆ Testable

- 硬件要求

- ◆ UEFI BIOS
- ◆ TPM 2.0

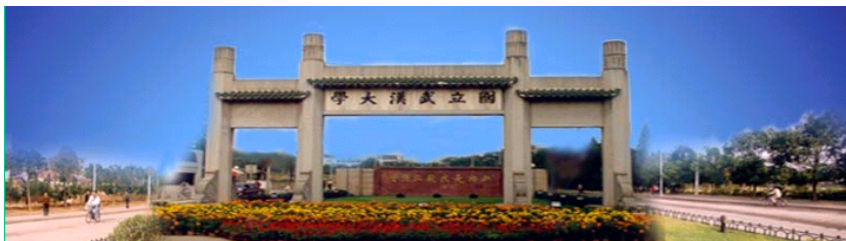


三、可信软件的发展

1、操作系统对可信计算的支持

■ Windows 8对可信计算的支持

- 可信启动 (TBoot)
 - ◆ 信任度量、存储、报告机制
 - ◆ 信任链
 - ◆ 基于TPM2.0
 - ◆ 基于UEFI BIOS 的安全启动功能



三、可信软件的发展

1、操作系统对可信计算的支持

■ Windows 8对可信计算的支持

- Bitlock磁盘加密系统
 - ◆ TPM2.0硬件支持
- 基于信誉的访问控制
 - ◆ 用户的信誉参与到访问控制中
- 应用保护系统AppLocker
 - ◆ 保护应用更安全



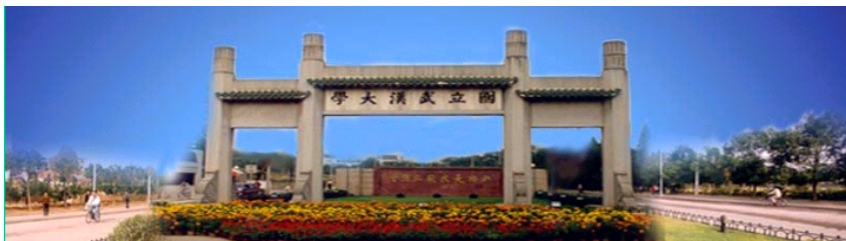
三、可信软件的发展

2、中国可信软件的研究

■ 国家自然科学基金委支持可信软件研究

● 可信软件重大研究计划

- ◆ 1.5亿RMB
- ◆ 历时5年
- ◆ 支持了上百个项目
- ◆ 重点研究了软件的正确性、可靠性和安全性
- ◆ 取得了一批成果



四、可信计算应用的发展

1、TPM已经得到实际应用

- TPM芯片已销售3亿片
- 大多数的笔记本电脑都装有TPM芯片
- 大多数的品牌PC机都装有TPM芯片

2、可信计算系统已经得到实际应用

- 增强系统的安全性
- 数据的安全存储
- 软件的安全保护



四、可信计算应用的发展

3、可信计算的新应用

- 云计算、物联网为可信计算开拓了新的应用领域
- 可信移动终端成为一个新的应用热点
- 把可信计算融进其它信息系统，将产生更广泛的应用



五、参考文献

1. SHEN Changxiang, Zhang Huanguo, Feng Dengguo, et,al. Survey of Information Security, Science in Chian Series F,Vol.50,No.3,Jun.2007, pp : 273-298.
2. SHEN Changxiang, ZHANG Huanguo, WANG Huaimin,wang et,al.,Researches on trusted computing and its developments, SCIENCE CHINA :Information Sciences,Vol.53,No.3, March 2010,pp: 405-433.
3. 张焕国, 赵波, 等著, 可信计算, 武汉大学出版社, 2010.



谢谢！



RSACONFERENCE
C H I N A 2012