可信计算教学安排

代炜琦
华中科技大学
2024年03月26号

Email: wqdai@hust.edu.cn
QQ：511962709

个人简介

代炜琦，博士，华中科技大学副教授，博导，“武汉黄鹤英才”优秀青年人才，华中科技大学区块链安全研究中心主任，华中科技大学-智汇医疗区块链研究中心主任，趣派信息科技有限公司区块链安全首席技术顾问。在华中科技大学获得学士学位和博士学位，曾在美国德州大学圣安东尼奥分校网络空间安全实验室做访问学者。主要研究方向区块链、隐私计算、云安全、可信计算、虚拟化安全等。

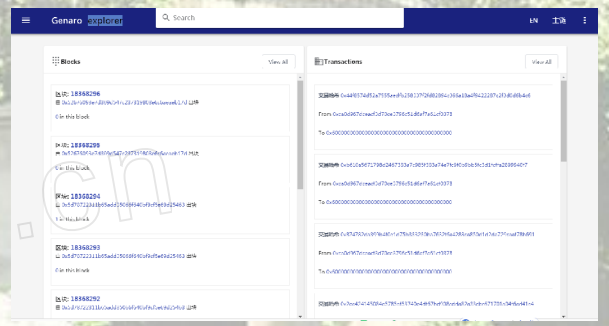
主持国家自然科学基金、广州市科技计划等多个重要项目。关注企业技术难点，积极开展校企合作，目前带领团队进行/完成多个大型区块链项目（国家重点研发计划、广州市科技计划、企业项目等）。发表区块链技术相关论文13篇，申请区块链技术相关国家发明专利31项（授权26项）、申请美国发明专利4项（授权1项），项目中的关键技术已经应用到淘通科技、农夫山泉、武汉园博园、吉罗科技等多家企业。

区块链

针对区块链分布式、多中心、合约化特性，从私钥无感认证、多方数据链上协同、智能合约热修复三个方面，解决区块链应用面临的技术挑战，构建安全可控的区块链系统。

区块链相关论文13篇，获得26项区块链技术相关国家发明专利，1项国际发明专利，建有区块链安全研究中心，医疗区块链研究中心，加速区块链技术与各行业的具体业务相结合。
相关成果/系统在Genaro Network、广州淘通科技、趣派信息科技、智汇医链等企业得到广泛应用。指导学生参加2021年微众银行FinTechathon大赛获得冠军。

针对数据的流通与共享过程中，存在全流程监管和隐私保护等需求，解决传统系统的监管和隐私无法兼顾的问题，构建安全可控的数据共享平台。



为Genaro Network开发的区块链存储公有链于2018年12月上线稳定运行至今已产生3000多万个区块

基于区块链的医院绩效考核系统

淘通面向电商联盟营销标签共享区块链平台

智汇医链系统平台

区块链，作为新一代颠覆性技术，在武汉敲响了“医工”联合的最强音，开创了链圈人在医院管理领域的破冰之旅。

2022年6月30日上午9时30分在国家网络安全人才与创新基地网安学院隆重举行了华中科技大学-智汇医疗区块链研究中心成立启动仪式暨基于区块链技术的医院管理实践研讨会。

研究中心设计并开发有智汇医链系统，一个以区块链技术为核心，AI和隐私计算为辅助的可溯源、可预警、可激励、可验证的智慧医院管理系统。研究中心的成立预示着区块链技术将首次运用到医院管理场景中，并以智慧医疗为载体惠及产业、患者、医务人员、医院等，贯通全民大健康体系，具有里程碑意义。

基于区块链的医院绩效考核系统系统针对目前医院管理工作中某些异常情况难发现、DRG支付改革要求高和国考等考核压力大三个痛点问题，结合区块链技术在医院管理方面的优势，创新性的提出了基于区块链的临床路径管理优化技术，首次利用区块链技术辅助医院院长对医院进行全维度智能化管理。

课程安排（1）

- 课程时间
  - 第6-11周，周二，周四
  - 第11-13周，周二，周四 实验

课程安排（2）

- 第1、2次
  - 可信计算概述：信息系统的安全威胁；软件固有缺陷；可信计算的发展历史；中国可信计算技术的发展；可信计算的定义等。
  - 密码学及PKI简述：Hash函数、对称密码算法、非对称密钥算法、公钥基础设施等方面的原理介绍。
- 第3、4次
  - 信息系统安全现状（与可信计算的关系）：TCG规范架构、TCG核心规范、TCG特定平台规范、TCG可信存储规范、TCG可信网络连接规范、中国可信计算联盟规范等。
  - 可信计算核心技术：安全度量和报告

课程安排（3）

- 第5、6次
  - 可信计算核心功能：远程证明、数据保护
  - 可信计算核心功能：TPM密钥管理
- 第7、8次
  - 可信度量技术：静态可信度量根技术、动态可信度量根技术、动态可信度量根应用等
  - 可信启动：包括可信启动技术及典型的可信启动系统，如Trusted GRUB、GRUB-IMA、OSLO、Tboot等。

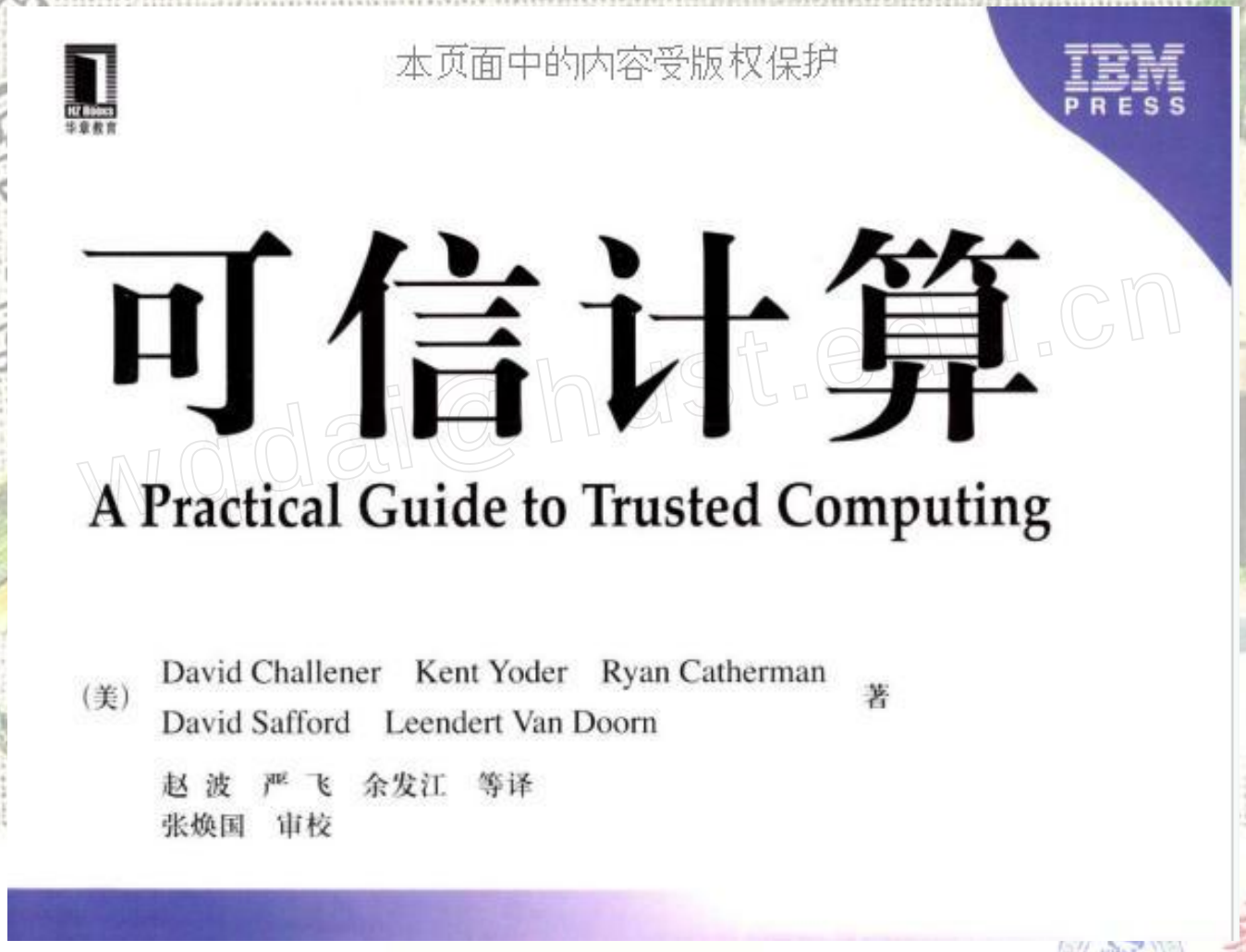
课程安排（4）

- 第9、10次
  - 可信计算软件栈：包括TCG软件栈的总体结构及功能、TCG软件栈的接口介绍、TCG软件栈的开源实现TrouSers。
  - 可信计算编程实例，Intel SGX等最新技术
- 第11、12次
  - 基于可信计算的相关技术和应用
  - 虚拟化可信计算平台，实验课安排

考试安排

- 课程成绩=课堂考勤（10%）+课堂考核（20%）+可信计算实验（15%）+可信计算实验报告（15%）+期末考核（40%）

参考资料



华中科技大学

课外文献阅读

- http://inst.eecs.berkeley.edu/~cs61c/ UC Berkeley, “Machine Structure”
- http://ccss.usc.edu/599tc/spring07/ University of Southern California “ Trusted Computing ”
- http://inst.eecs.berkeley.edu/~cs161/sp15/ UC Berkeley “ Computer Security
- http://www-users.cselabs.umn.edu/classes/Fall-2015/csci5271/index.php?page=schedule#lec00 University of Minnesota “ Introduction to Computer Security ”
- http://www-users.cselabs.umn.edu/classes/Spring-2015/csci5471/index.php?page=schedule University of Minnesota “Modern Cryptography”
- http://www-users.cselabs.umn.edu/classes/Spring-2014/csci8271/index.php?page=schedule University of Minnesota “Security and Privacy in Computing”

教材

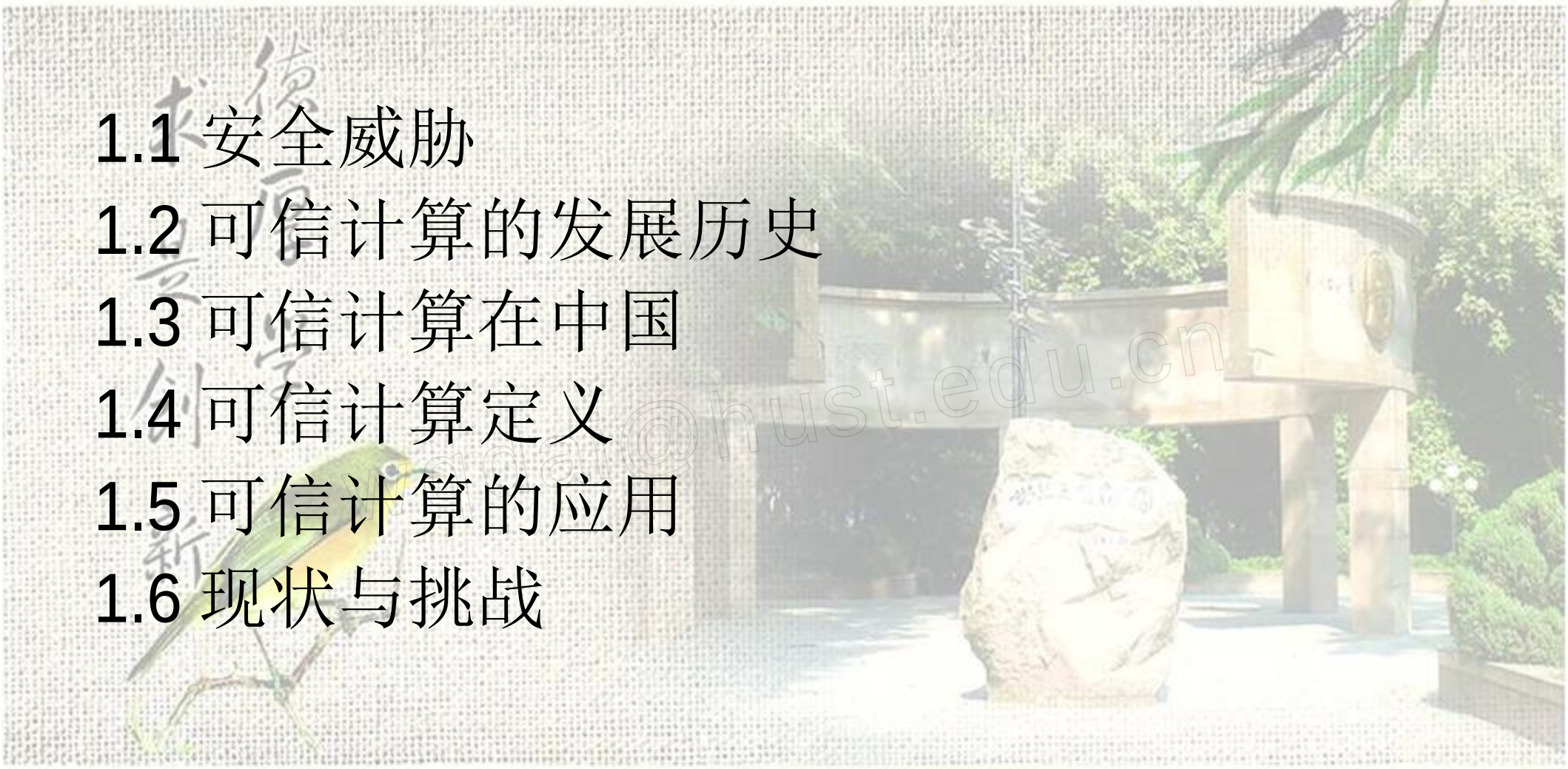
- 该教材撰写是科研工作的一部分
  - HP高校合作项目—Daolity
  - EMC高校合作项目—Daoli
- 围绕着TPM和TCM，从基础知识、技术规范、技术原理、编程和技术应用等多个角度进行阐述

目录结构（1）

总体上划分为三大部分，包括背景知识、可信计算架构及功能，以及可信计算平台

目录结构（2）

第1章 可信计算概述



1.1 安全威胁
1.2 可信计算的发展历史
1.3 可信计算在中国
1.4 可信计算定义
1.5 可信计算的应用
1.6 现状与挑战

华中科技大学

Part I: 背景材料

- 是什么推动了可信计算的出现
- 它试图解决什么问题
- TPM提供了哪些功能

1.1 安全威胁

- 计算机安全问题
  - 主要针对系统中软件的攻击
  - 软件安全漏洞产生的根源在于现代软件系统惊人的复杂性
    - 软件系统设计的致命问题（仅利用了0环和3环）
    - 软件安全漏洞与软件规模成正比的关系
      - 典型的产品级软件每千行代码就会有一个与安全相关的漏洞
      - 一个主流应用系统有可能隐藏了１０万个以上的安全漏洞

1.1 安全威胁

- 软件漏洞引起的攻击
  - 跨站脚本攻击（XSS）
  - SQL注入
  - 缓冲区溢出
  - 恶意文件执行
  - 不安全的对象引用
  - 不安全的身份鉴别和加密存储
  - ……

1.1 安全威胁

- 软件漏洞状况
  - 呈现了两年翻一番的发展趋势
  - 需要做频繁的补丁更新
  - 客户端系统更易受到攻击
  - 当今世界平均每20s就有一起黑客事件发生
  - 仅在美国每年造成的经济损失就超过100亿美元

1.1 安全威胁

- 数据泄漏
  - 软件攻击
    - 身份和鉴别信息的电子盗窃
  - 移动电子设备或其它数据存储媒介失窃

1.1 安全威胁

- 计算机安全威胁日益增多
  - 安全防护方式的被动性
    - 防火墙、入侵监测和病毒防范是构成传统信息安全系统的主要技术手段
  - 现有平台架构的开放性
    - 导致恶意程序很容易植入软件系统中
  - 软件的固有缺陷不足
    - 仅依靠软件本身无法完全检测出恶意代码
    - 检测软件自身的安全性无法证明

1.1 安全威胁

- 基于硬件的嵌入式安全解决手段
  - 为计算平台增加具有安全保护功能的硬件
  - 再通过软硬件结合的方式构建可信计算环境
  - 使用可信计算环境保证其中运行程序和数据的真实性、机密性、可控性等
- 结合硬件弥补软件安全防护方式带来的不足
  - USB Key（加密锁、U盾、友key）
  - 可信计算芯片

1.2 可信计算的发展历史

- 美国国防部国家计算机安全中心于上个世纪80年代中期提出“可信计算机安全评价标准”(TCSEC)
  - 第一次提出可信计算机和可信计算基 TCB (Trusted Computing Base) 的概念
  - 针对网络、系统和数据库的三个解释性文件（1987年）
    - 可信网络解释TNI (Trusted Network Interpretation)
    - 计算机安全系统解释 (Computer Security Subsystem Interpretation)
    - 可信数据库解释TDI (Trusted Database Interpretation)
- 1993年1月，美国公布了融合欧洲ITSEC 的可信计算机安全评价准则之联邦准则

1.2 可信计算的发展历史

- 安全启动的体系结构（1997年，AEGIS项目）
  - 提出信任传递概念
    - 计算机从启动的过程开始，由前一个程序度量后一个程序的完整性，只有在完整性通过验证后，才把控制权交给后一个程序，如此反复直到操作系统的启动
- LaGrande硬件技术→NGSCB (next gen-eration secure computing base)→VISTA支持可信计算机制

1.2 可信计算的发展历史

- 可信计算平台联盟 TCPA (Trusted Computing Platform Alliance)
  - Compaq、HP、IBM、Intel和Microsoft于1999年10月牵头组织
    - 提出可信计算的初衷？
  - TCPA定义了具有安全存储和加密功能的可信平台模块(TPM)
  - 2001年1月发布了基于硬件系统的“可信计算平台规范(v1.0)”

1.2 可信计算的发展历史

- TCG(Trusted Computing Group)
  - 2003年3月TCPA改组
  - 目的：在计算和通信系统中广泛使用基于硬件安全模块支持下的可信计算平台，以提高整体的安全性
  - 涵盖范围：PC，PDA，手机，以及其他的一些平台
  - 一些国际芯片厂商依照TCG规范实现了TPM芯片

1.3 可信计算在中国

- 紧跟美国的步伐
  - 上世纪九十年代——PC机安全防护系统
  - 2004 年具有自主知识产权的可信计算机产品面世
  - 2005年联想“恒智”芯片和北京兆日公司TPM芯片
- 2002年中国信息产业商会信息安全产业分会提出了可信网络世界体系结构框架(Trusted Cyber Architecture Framework，TCAF)
- 2005年1月，成立国家安全标准委员会WG1可信计算工作小组专门规划可信计算相关标准
  - 2006年颁布了《可信计算平台密码技术方案》和《可信计算密码支撑平台功能与接口规范》
- 2007年，由沈昌祥院士主导并确定研制“可信计算平台密码规范”、“可信计算基础支撑软件”、“可信平台主机规范”、“可信网络连接规范”等草案
  - 预计今年发布

1.3 可信计算在中国

- 可信计算密码模块TCM
  - 采用国产密码算法
  - 国内可信计算机均只支持TCM
- 2008年4月底，中国可信计算联盟(CTCU)在国家信息中心成立
  - 参与单位包含计算机厂商、信息安全厂商和一些应用厂商，以及国家的科研院所
  - 北京工业大学、瑞达信息安全产业股份有限公司、国家信息中心信息安全研究与服务中心等

1.4 可信计算定义

- 可信计算组织TCG
  - 如果一个实体的行为是以预期的方式，符合预期的目标，则该实体是可信的
- ISO/IEC 15408标准
  - 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
- 沈昌祥院士可信定义
  - 可信要做到一个实体在实现给定目标时其行为总是如同预期一样的结果，强调行为结果的可预测和可控制
- 其他解释
  - 可信是指计算机系统所提供的服务可以被证明是可信赖的
  - 如果一个系统按照预期的设计和政策运行，这个系统是可信的
  - 当第二个实体符合第一个实体的期望行为时，第一个实体可假设第二个实体是可信的
  - 可信≈安全+可靠，可信计算系统是能够提供系统的可靠性、可用性、信息和行为安全性的计算机系统

1.4 可信计算定义

- 信任定义的复杂性
  - 按照TCG的定义，一个恶意软件在预期时间内做出了期望的危害行为，那么它是可信的，而依照ISO/IEC 15408 标准定义却是不可信的
  - 信任定义的多样化
    - 有些侧重信任的形式化描述，有些着重信任的特征研究，有些着重信任在实际系统中应用

1.4 可信计算定义

- 可信赖计算(Dependable Computiong)
  - 源于容错计算
  - 针对元器件、系统和网络，对包括设计、制造、运行和维修在内的全过程中出现的各种非恶意故障进行故障检测、故障诊断、故障避免、故障容许，使系统达到高可靠与高可用
- 安全计算(Security Computing)
  - 针对系统和网络运行过程中的恶意攻击
- 信任计算(Trusted Computing)
  - 假定真实性可以用于度量并且不考虑度量中的损失，给出了一个信任在实体间传递的方法——在计算机系统中首先建立一个信任根，再建立一条信任链，一级度量认证一级，一级信任一级，把信任关系扩大到整个计算机系统，从而确保计算机系统的可信
- 广义上的可信计算应该包括可信赖计算、安全计算和信任计算，而本文的可信计算侧重于TCG及沈昌祥院士给出的定义，即：Trusted Computing

1.5 可信计算的应用

- 可信计算平台将加密、解密、认证等基本的安全功能交由硬件芯片来完成，并确保芯片中的信息不能在外部通过软件随意获取
  - 应用领域：信息加密保护
  - 应用领域：操作系统安全
  - 应用领域：网络保护
  - 应用领域：安全管理

应用领域：信息加密保护

- IBM嵌入式安全子系统
- 内嵌在计算机中的安全芯片
  - 不获得安全子系统口令的情况下是无法获取系统中任何信息的
  - 应用于登录密码、加密密钥和数字证书的保护
  - 对文件系统（利用IBM的文件和文件夹加密功能）和网络传输进行加密
  - 安全芯片内部的信息存储和传送也经过了高强度的加密，采用了特殊的芯片封装方法，使得安全芯片的破解极其困难
- 专用的客户端安全软件

应用领域：信息加密保护

- 瑞达的可信计算机产品
  - 插入特别的电子钥匙或IC卡才能开启计算机、为计算机提供惟一的标识、控制所有文件的输入输出等
- 联想的“恒智”安全芯片
  - 标识计算机身份以防止假冒，将所有密钥信息都存储在芯片当中

应用领域：操作系统安全

- 微软加密文件系统（EFS）
  - Windows 2000及之后出现的Windows XP等系统都支持该特性
- 微软操作系统Vista支持基于硬件的安全启动
  - 硬件设备将对每个Windows系统开机时需要用到的文件进行标记
  - 一旦在开机的过程中检验出标记状态的不吻合将很可能意味着系统受到了非授权的篡改或破坏

应用领域：网络保护

- 3Com公司的嵌入式防火墙（EFW）的网卡产品
  - 向安装了该产品的计算机提供可定制的防火墙保护
  - 提供硬件VPN功能
  - 支持基于TPM规范的认证，使得只有合法的网卡才能用于访问企业网络
  - 与软件防火墙相比
    - 性能更好
    - 可配置能力和可扩展能力相对差些

应用领域：安全管理

- Intel主动管理技术（AMT）
  - 为远程计算机管理而设计的
  - 在软件系统崩溃、BIOS损坏甚至是没有开机的状态下管理员仍然能在远程对计算机完成很多操作
  - 在系统因病毒而瘫痪的情况下管理员可以利用AMT技术远程进行病毒清除、补丁更新乃至操作系统安装等工作
  - 极大地提高安全事件的响应速度并降低管理成本，但执行更加复杂的管理工作有赖于软件环境的支持
  - 在支持AMT的网卡中写入一些服务功能，这样在计算机系统失效的情况下这些服务仍将能够执行

1.6 现状与挑战

- 可信计算并不等同于绝对安全，不能解决所有的安全问题
  - 只是提供了一种加强系统安全的方式，能够结合传统的安全技术来增强系统的安全性
  - 无法解决软件漏洞问题
  - 目前的可信计算通常需要与相应的软件结合起来工作，不正确的软件使用或管理不善的密码都可能为可信计算平台带来“短板”

1.6 现状与挑战

- 需要将可信计算延展到更深更广的层面以建立起更具安全性的计算设施
  - 仅在终端层次取得了突破
  - 网络架构的可信
- 在未来的很长时间里，可信计算平台与非可信计算平台将互相融合并朝着更加安全的系统形式发展

1.6 现状与挑战

- 当前可信计算存在的问题
  - 理论研究相对滞后
  - 存有一些尚待攻克的关键技术
  - 无论是国外还是国内的可信计算机都没能完全实现TCG的技术规范，如：动态可信度量、存储、报告机制，安全I/O等
  - 操作系统、网络、数据库和应用的可信机制配套的缺乏也影响着可信计算的发展
  - 没有关于可信操作系统、可信数据库、可信应用软件的技术规范
    - 只有硬件平台的可信，没有操作系统、网络、数据库和应用的可信，整个系统还是不安全的