软件安全—恶意代码机理与防护

C1 软件安全概论

彭国军

武汉大学国家网络安全学院

guojpeng@whu.edu.cn

提纲

1.1 信息与信息安全

1.2 软件安全威胁与来源

1.3 软件安全威胁的典型防护手段

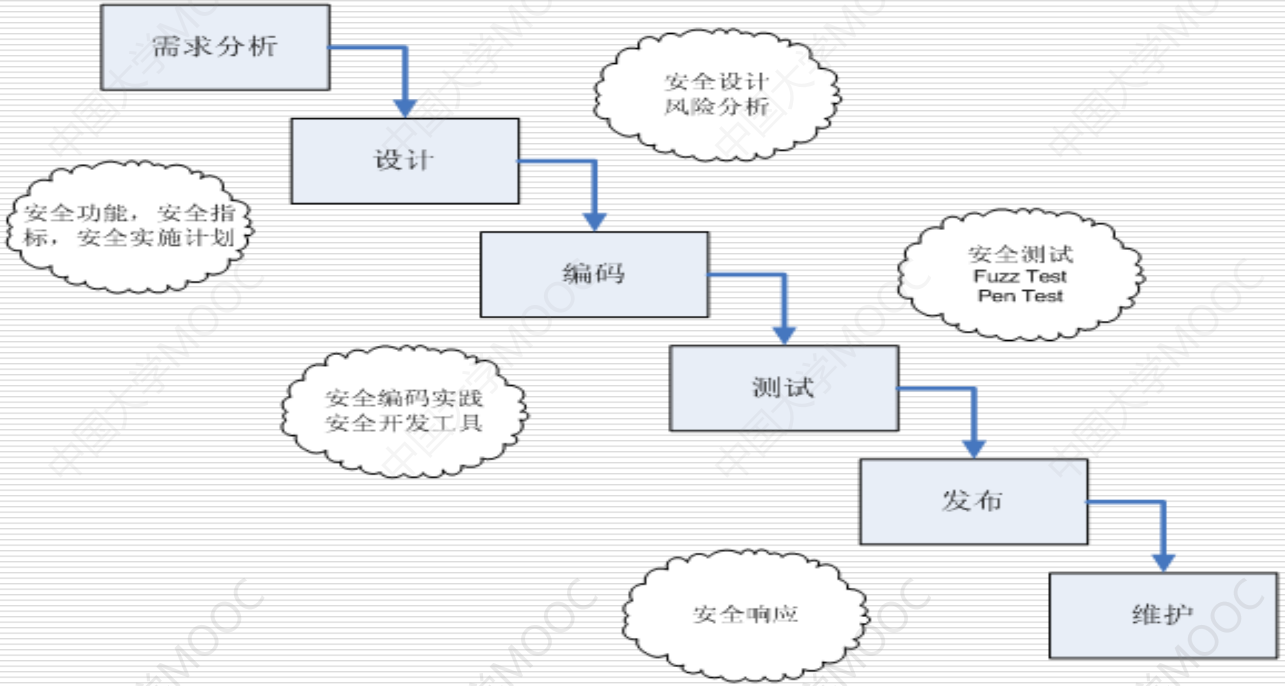
1.3 软件安全威胁的典型防护手段

- 安全设计
- 保障运行环境
- 加强软件自身行为认证
- 恶意软件检测与查杀
- 黑客攻击防护
- 系统还原
- 虚拟隔离等

1.3.1 安全设计

- 强化软件工程思想，将安全问题融入到软件的开发管理流程之中，在软件开发阶段尽量减少软件缺陷和漏洞的数量。
- 微软：信息技术安全开发生命周期流程 （Secure Development Lifecycle for Information Technology，缩写为SDL-IT）。
  - 该流程包含有一系列的最佳实践和工具，用于微软内部业务应用以及许多微软客户的开发项目中。
  - 微软的Windows 7、8系统

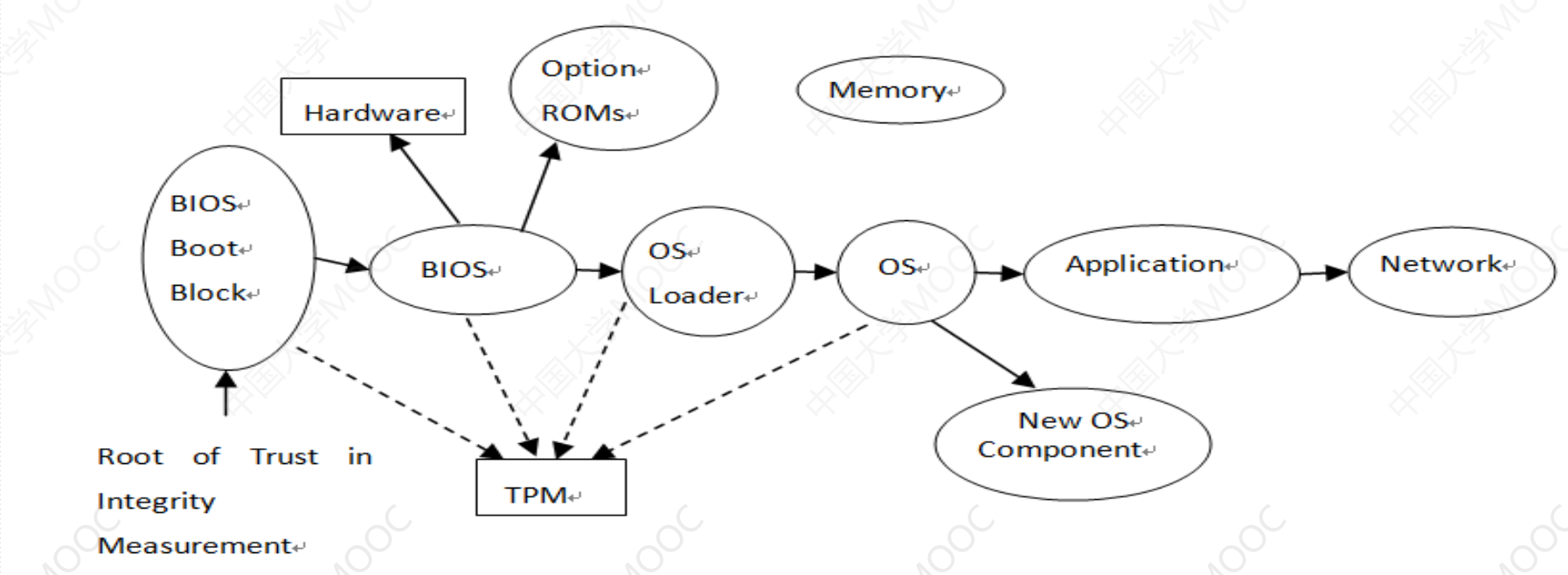
SDL开发模式


需求分析
设计
编码
测试
发布
维护
安全设计
风险分析
安全功能，安全指标，安全实施计划
安全测试
Fuzz Test
Pen Test
安全编码实践
安全开发工具
安全响应

1.3.2 保障运行环境

- 保障软件自身运行环境，加强系统自身的数据完整性校验
  - 软件完整性校验
    - 目前很多安全软件在安装之初将对系统的重要文件进行完整性校验并保存其校验值， 如卡巴斯基安全套件。
  - 系统完整性校验
    - 目前有些硬件系统从底层开始保障系统的完整性，可信计算思想是典型代表。

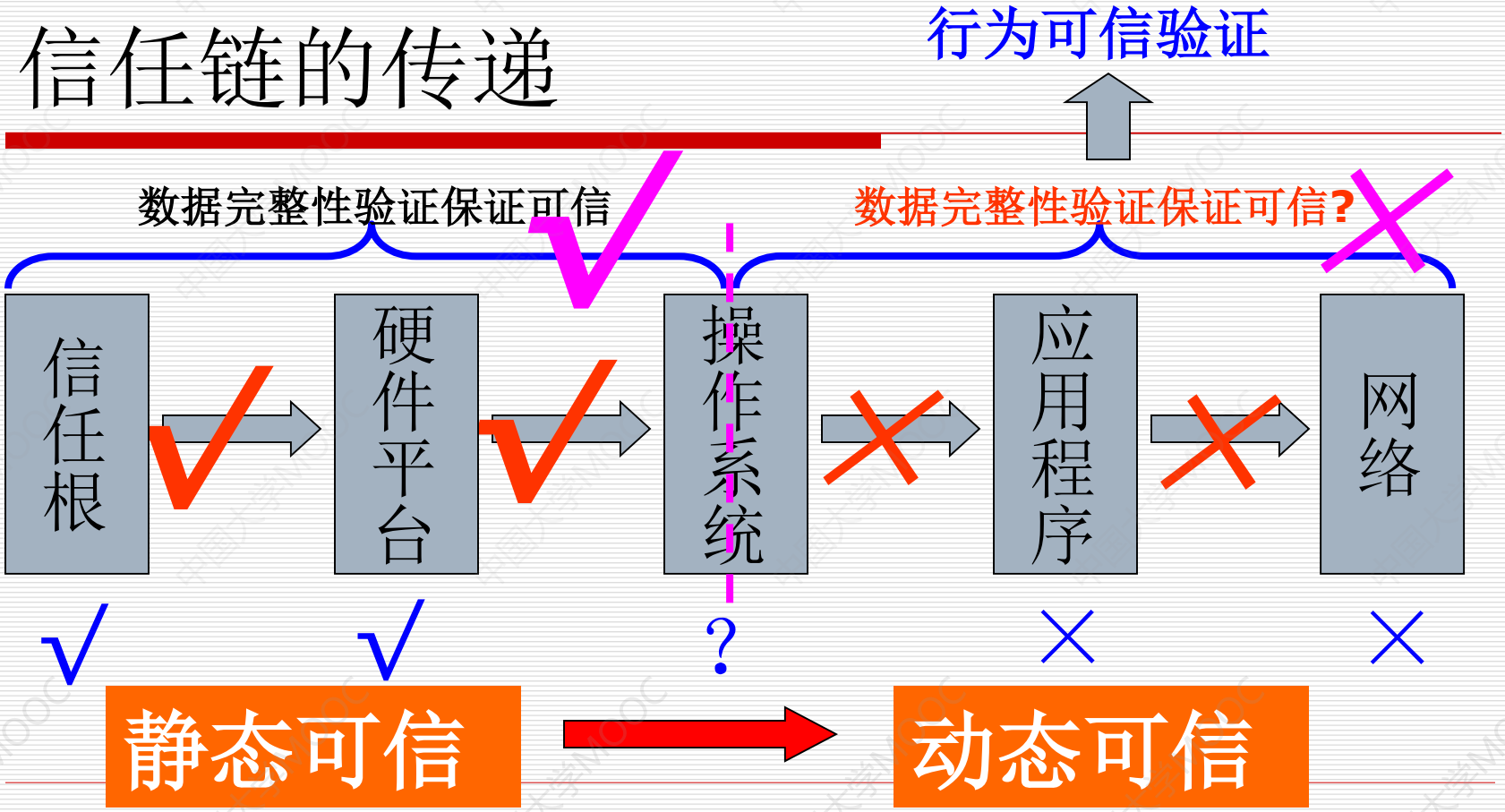
TCG的可信计算信任链的传递



1.3.3 加强软件自身行为认证

- 软件动态可信认证
  - 在确保软件数据完整性的前提下，如何确保软件的行为总是以预期的方式，朝着预期的目标运行。

信任链的传递


行为可信验证
数据完整性验证保证可信
数据完整性验证保证可信?
信任根
硬件平台
操作系统
应用程序
网络
√
√
?
×
×
静态可信
动态可信

高可信软件技术研究

- **美国计算研究协会:**把高可信软件系统看作是目前计算机研究领域必须应对的五大挑战之一。
- **美国国家科技委员会:**在其总统财政预算报告中指出，高可信软件技术是需要优先开展的研究工作，包括构造更加安全、可靠和健壮的可信软硬件平台，提供更高效的可信软件开发技术，以及建立新的保证复杂软件系统高可信的科学和工程体系等。
- **美国国防部高级研究计划署（Defense Advanced Research Projects Agency，DARPA）:**将高可信系统和软件列为目前需要面对的四大挑战之一。
- **美国国家科学基金会、美国宇航局和美国安全局（National Security Agency，NSA）等:**高可信软件技术研究的重要投资方。
- **微软：**可信赖计算(Trustworthy computing,TWC)

- 我国政府十分重视软件系统的可信性问题。
  - 国家自然科学基金委从2007年启动了“可信软件基础研究”重大研究计划；
  - 国家高技术发展（863）计划中设立了专门的重大项目，研究高可信软件生产工具及集成环境；
  - 国家重点基础研究发展（973）计划将可信软件的研究确定为重点发展方向，研究基于网络的复杂软件可信度和服务质量。

- 为了集中技术力量进行专项研究，我国还设置了可信软件的专项实验室
  - **华东师范大学：**高可信软件技术教育部重点实验室和上海市高可信计算重点实验室等。
  - **武汉大学：**“空天信息安全与可信计算”教育部重点实验室。

1.3.4 恶意软件检测与查杀

- 反病毒软件主要用来对外来的恶意软件进行检测。
  - 通常采用病毒特征值检测、虚拟机、启发式扫描、主动防御、云查杀等等几种方法来对病毒进行检测。

- 恶意软件是软件安全的一个主要安全威胁来源，针对系统的外来入侵通常都离不开外来恶意软件的支撑。

1.3.5 黑客攻击防护

- 防火墙
  - 网络、主机防火墙
- 入侵检测系统IDS
- 入侵防护系统IPS
  - 基于网络、基于主机（HIPS）
- 基于主机的漏洞攻击阻断技术
  - EMET：Microsoft's Enhanced Mitigation Experience Toolkit

1.3.6 系统还原

- 将关键系统文件或指定磁盘分区还原为之前的备份状态，从而将已有系统中的恶意程序全部清除，以保护系统安全。
  - Windows自带的“系统还原”功能
  - Ghost还原软件
  - 还原卡、影子系统（PowerShadow）等

1.3.7 虚拟隔离等

- 虚拟机（如VmWare）
  - 隔离风险
    - 用户可以通过在不同的虚拟机中分别进行相关活动（如上网浏览、游戏或网银等重要系统登陆），从而可以将危险行为隔离在不同的系统范围之内，保障敏感行为操作的安全性。
- 沙箱，也叫沙盘或沙盒（如SandBoxIE）
  - 隔离风险
  - 通常用于运行一些疑似危险样本，从而可以隔离安全威胁，也可以用于恶意软件分析。