

# 信息安全产品测评方法及发展现状

解放军信息安全测评认证中心

网络安全实验室

钟 力

66745052 zhongli123@sohu.com

# 大 纲

- ④ 测试方法
- ④ 安全产品等级划分
- ④ 安全产品发展现状

# 测试方法

- ④ 依据产品相关国家军用标准、国家标准，参考国际标准和行业标准。例如：
  - ④ GB/T 18019-1999 包过滤型防火墙安全技术要求
  - ④ GA/T 403.1-2002 信息技术 入侵检测产品技术要求 第1部分：网络型产品
- ④ 测试方法是产品技术标准与具体测试操作之间的桥梁。
  - ④ 很多标准是抽象的、高度概括的
  - ④ 可操作性不强
- ④ 测试方法对如何测试安全产品具有明确的指导，例如：
  - ④ 《防火墙产品测试评估方法》
  - ④ 《网络隔离产品测试评估方法》

# 测试方法组成

## ④ 测试内容

测试用例形式

## ④ 测试环境

拓扑结构与配置

## ④ 测试工具

每个测试用例具体的测试工具

# 测试内容

## ④ 功能测试

对产品应具备的安全功能进行测试验证。

## ④ 性能测试

对产品在执行安全功能条件下的性能进行测试。

## ④ 安全性测试

产品的自身安全性和抗攻击渗透能力测试。

## ④ 可用性测试

对产品的成熟度进行考查。

# 例：防火墙测试内容

## ④ 功能

包过滤、应用代理、NAT、日志审计、内容过滤、.....

## ④ 性能

吞吐率、延迟、TCP并发连接数、.....

## ④ 安全性

自身脆弱性、抗攻击渗透能力、.....

## ④ 可用性

人机接口、稳定性、文档、.....

# 例：IDS测试内容

## ④ 功能

TCP/IP协议栈分析、入侵检测能力、实时告警、日志审计、策略管理、.....

## ④ 性能

在不同背景流量（包长、协议类型、真实流量、流量大小）下的入侵检测能力。

## ④ 安全性

探测引擎安全、管理会话安全、.....

## ④ 可用性

人机接口、稳定性、文档、.....

# 测试环境

## ① 离线仿真测试环境与实时在线测试环境

模拟环境与真实环境

## ② 功能、安全性测试环境与性能测试环境

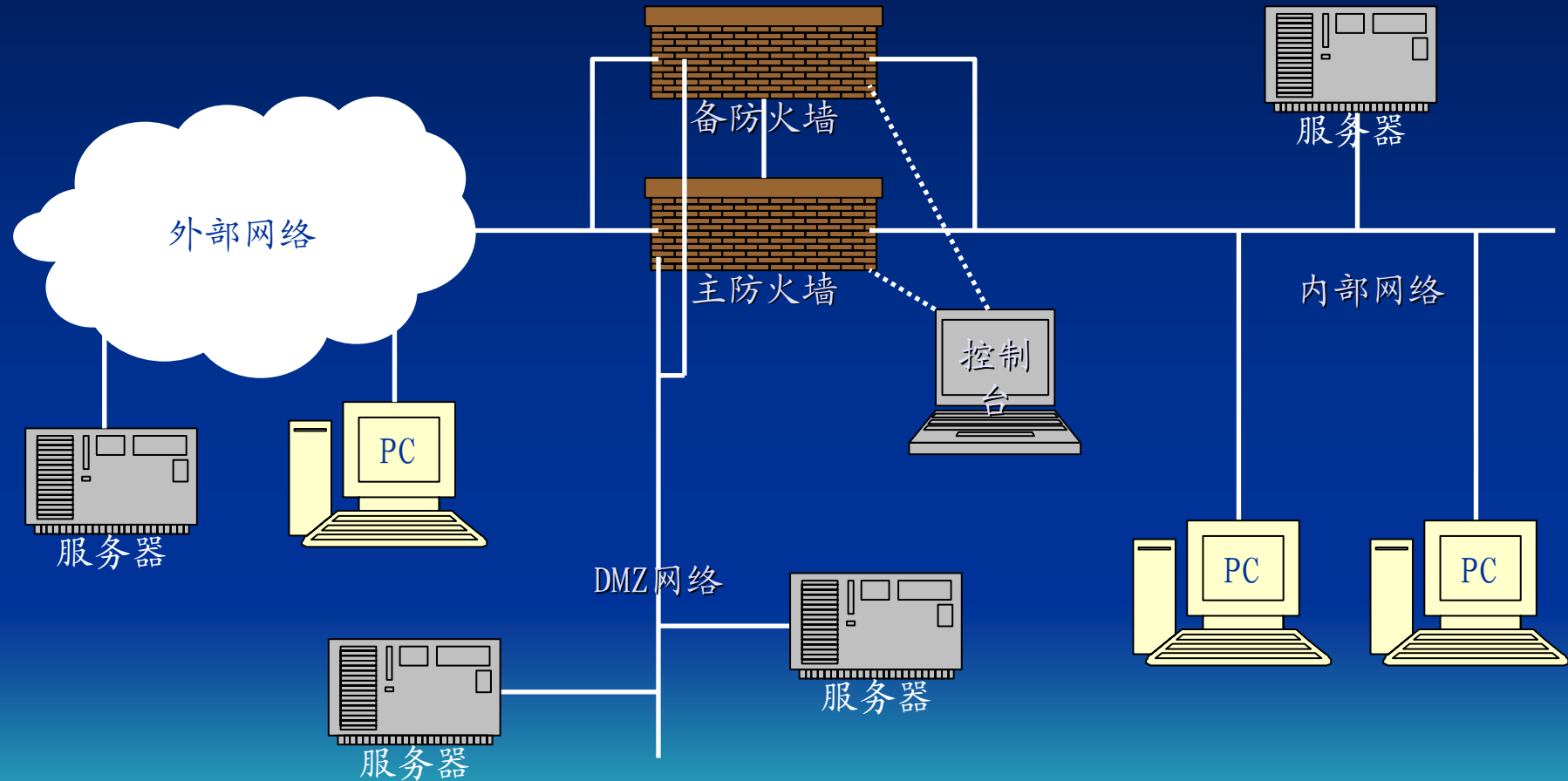
功能、安全性测试需尽可能模拟真实应用环境

性能测试重点考虑的是使产品处理能力达到临界状态

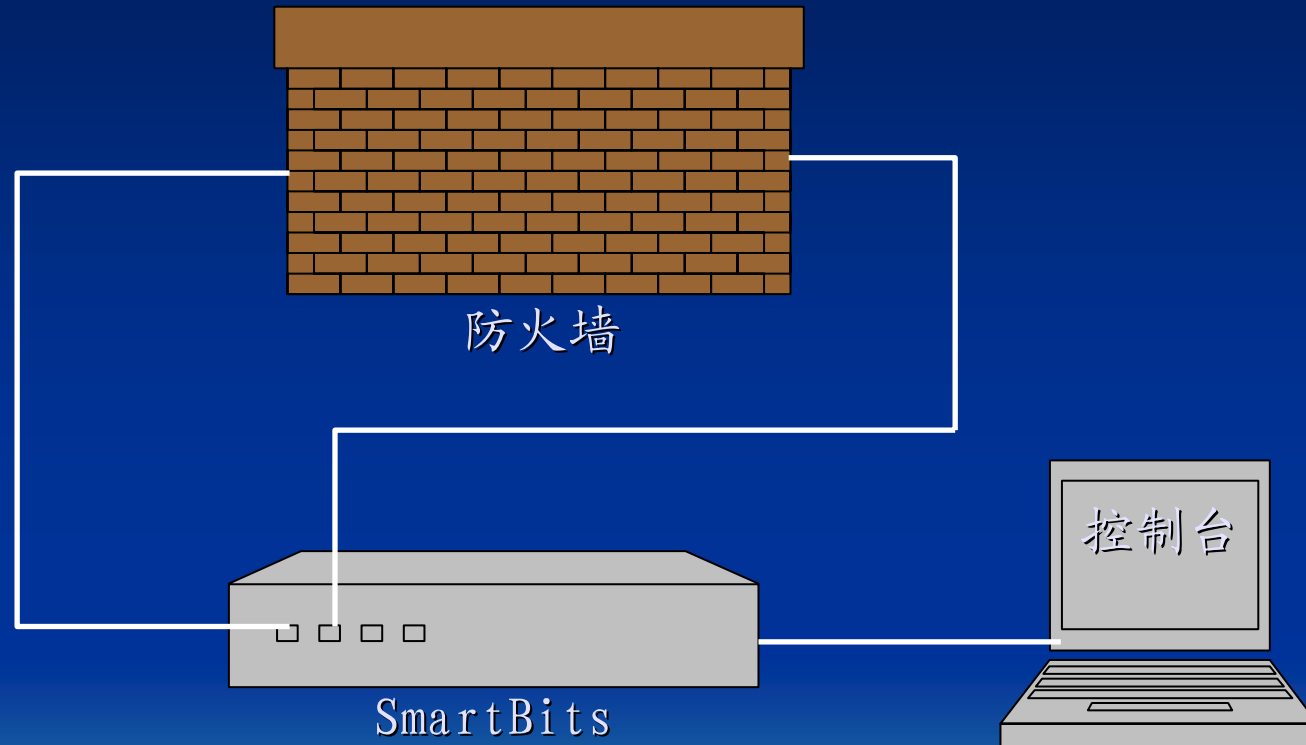
## ③ 测试环境不能影响产品效能的发挥

对网络和主机系统都提出了要求

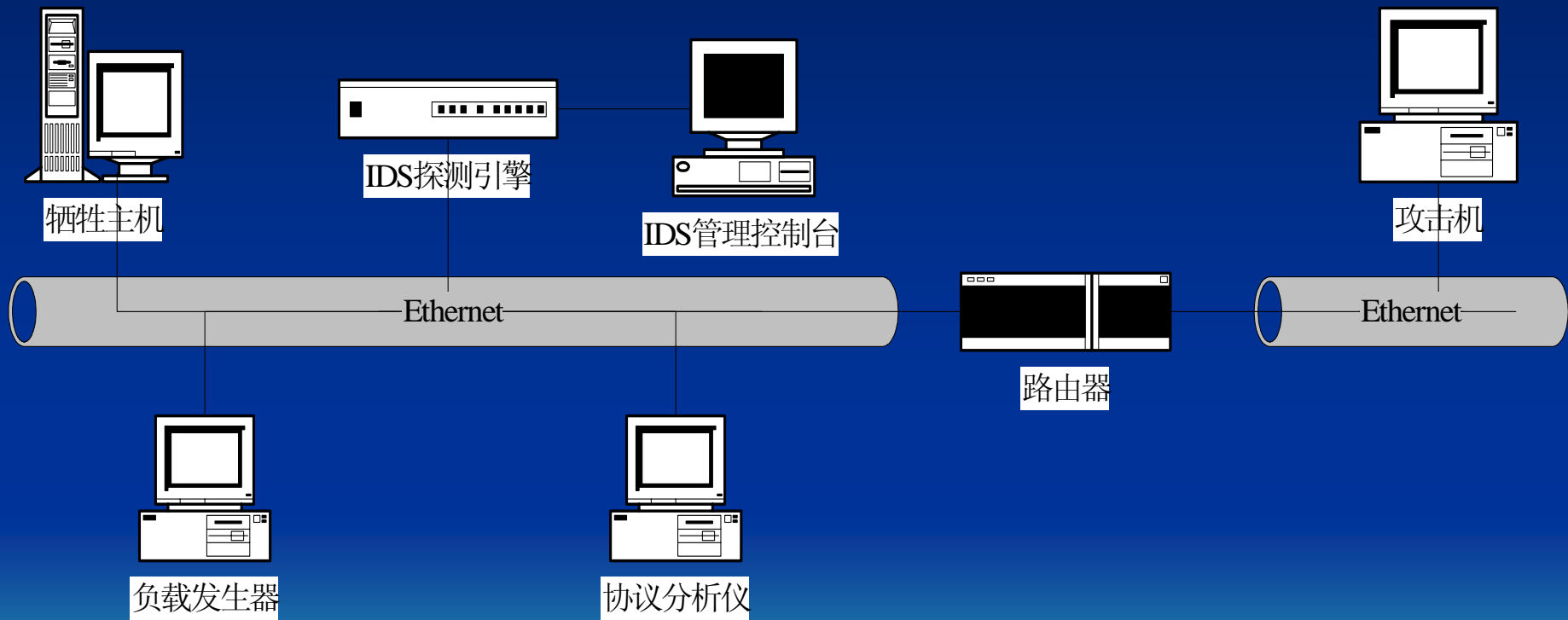
# 例：防火墙功能、安全性测试环境



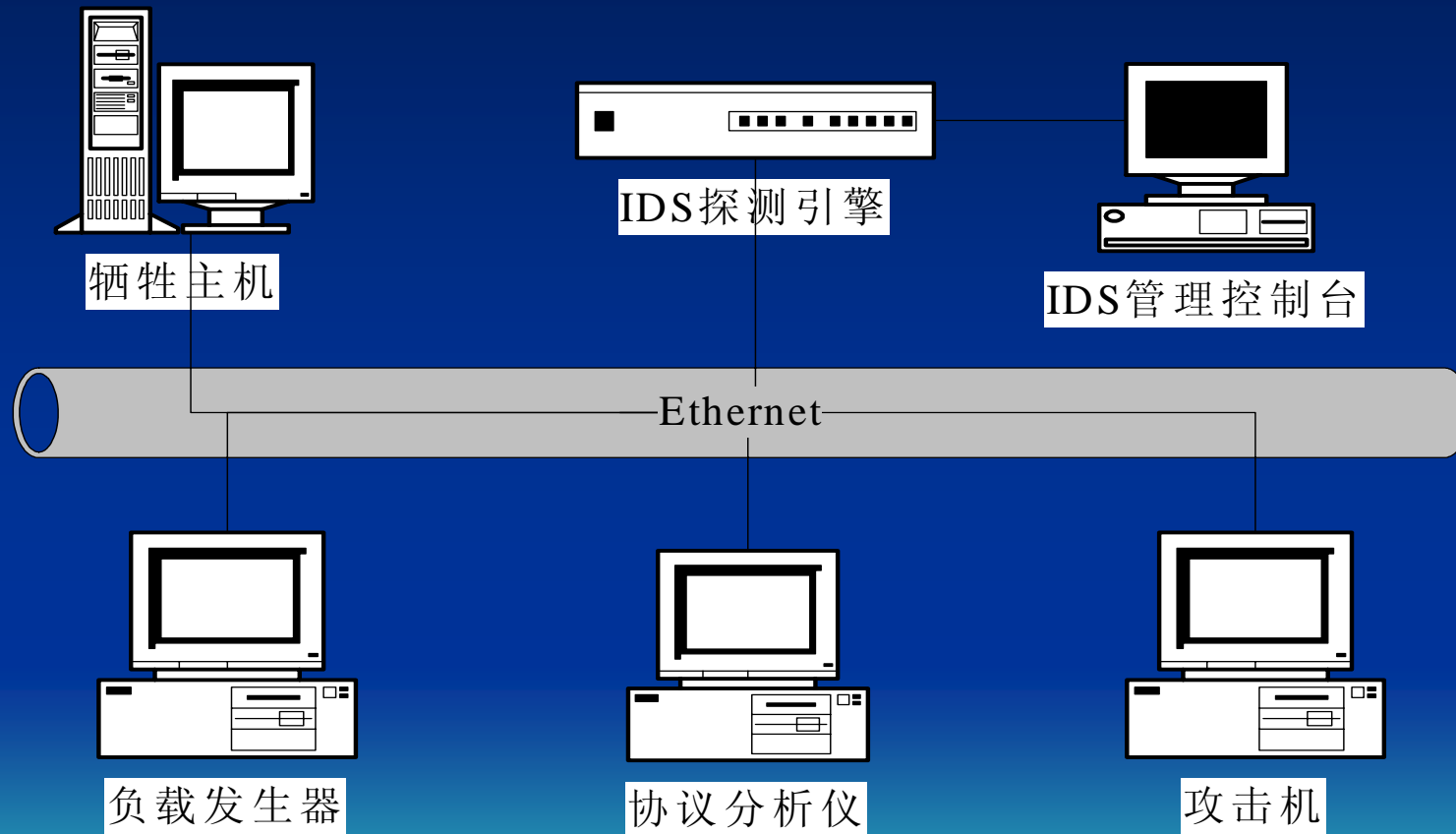
# 例：防火墙性能测试环境



# 例：IDS功能、安全性测试环境



# 例：IDS性能测试环境



# 测试工具

## ④ 自行研制工具

防火墙测试系统、IDS基准测试系统 .....

## ④ 专用性能测试设备

SmartBits、协议分析仪、包仿真器

## ④ 网络小程序

黑客程序 .....

# 例：防火墙测试工具

- ④ 专用防火墙测试系统
- ④ SmartBits性能测试工具
- ④ 协议分析仪
- ④ 黑客程序
- ④ ....

# 例：IDS测试工具

④ AQX-621迅捷NIDS基准测试系统

④ Blade IDS

④ 协议分析仪或其它负载发生工具

④ Fragrouter、NIDSBench

④ 黑客程序

④ .....

# 安全产品等级划分的意义

④ 信息系统安全等级保护已成为国家信息安全的基本国策

GB17859 27号文件 分三步推进等级保护

④ 安全产品等级划分与信息系统等级保护相呼应

不同等级信息系统需要不同等级的安全产品。

# 如何进行安全产品等级划分？

❶ 能否套用信息系统等级保护方法？

❶ 信息系统等级保护以数据保护为核心内容。

❶ 信息系统安全是一个面，而安全产品是一个点，信息系统等级保护更为复杂。

❶ 不同的安全产品解决信息系统中不同的安全问题。

# 如何进行安全产品等级划分？

- ④ 某一种类安全产品的等级划分应该在该种安全产品的范围内进行（小尺度）
  - ④ 安全产品等级划分是产品质量（主要是安全方面的质量）的划分。
  - ④ 质量高低体现在产品的功能、性能、安全性和可用性四个方面。
- ④ 安全产品等级划分同时也应考虑该产品在信息系统安全中的地位和作用（大尺度）

# 产品等级划分的具体实施

④ 产品安全等级分为C、C+、B、B+和A五个等级

④ 最开始是三级五档模式，即C、B、A渐进提高的三级，C+、B+级分别是C级和B级产品在附加功能上的增强。

④ 现发展到C、C+、B、B+、A五个渐进提高的级别，更能反映某些较大型复杂安全产品的区别。

# 产品等级划分的具体实施

- ④ 不同安全产品的最低安全等级与最高安全等级存在不同
  - ④ 充分考虑每一类型安全产品在信息系统安全中的地位和作用，并非所有类型的安全产品都跨越全部五个安全等级。
  - ④ 例如，防火墙（C→A）、安全操作系统（C+→A）、网络隔离卡（C→C+）、非法外联监控系统（C→B）

# 产品等级划分的具体实施

④ 产品等级划分直接与测试方法相结合

④ 测试方法中的测试内容，由功能、性能、安全性和可用性四个方面的测试用例组成。

④ 每一个测试用例均有等级标记，同样分为C、C+、B、B+、A五个等级，与产品等级对应。

④ 测试用例还有类型的差别，分为基本型、增强型和附加型三种。

# 产品等级划分的具体实施

- ④ 产品要达到某个安全等级，应通过等级标记为该等级和该等级以下级测试用例的测试。

例如，产品要达到B级，应通过等级标记为C、C+、B级测试用例的测试。其它等级类推。

- ④ 基本型测试用例必须通过（100%通过率）
- ④ 增强型测试用例要达到一定比率（60%通过率）
- ④ 附加型测试用例针对产品自身独特的特性，原则上必须通过（100%通过率）

# 测试用例

序号	FUNC-002-010-C+	名称	后门程序攻击
等级	<input type="checkbox"/> A <input type="checkbox"/> B+ <input type="checkbox"/> B <input checked="" type="checkbox"/> C+ <input type="checkbox"/> C	类型	<input checked="" type="checkbox"/> 基本型 <input type="checkbox"/> 增强型
内容	测试IDS能否检测到后门程序攻击，例如冰河、黑洞、 <i>Subseven</i> 、 <i>B0</i> 和 <i>DeepThroat</i> 等。		
特殊要求或配置	牺牲主机已被植入了后门程序。		
测试步骤	①使用DeepThroat、B0等国际流行的后门程序对牺牲主机进行各种控制操作； ②使用冰河、黑洞等国内典型的后门程序对牺牲主机进行各种控制操作。		
预期结果	正确对各种后门操作行为报警。		
测试结果			
结论	<input type="checkbox"/> 通过 <input type="checkbox"/> 部分通过 <input type="checkbox"/> 不通过 <input type="checkbox"/> 未测试		
备注			

# 2004年安全产品测评认证情况

- ④ 边界防护产品、桌面（终端）安全产品和网络安全管理产品三足鼎立。
- ④ 产品主要有防火墙、网络隔离、入侵检测、数据保护和安全管理等类型。
- ④ 由于采取互认证方式，防病毒产品较少。

# 安全产品等级分布

- ④ 2004年认证产品的安全等级，C级为13%，C+级为33%，B级为42%，B+级为5%，A级为0，不通过或复测为7%。
- ④ 高等级的产品偏少，国家和军队缺乏相关的产品标准是一大原因。同时，测试方法、测试手段也需要进一步提高。

# 安全产品现状及热点

## ④ 边界安全

④ 防火墙、网络隔离等网关类产品占总认证产品数的40%。

④ 防火墙仍是信息安全产品的主力军。

据报道，2004年上半年防火墙的市场容量达到5.5亿元，在整个安全市场中的比重为41.7%。

④ 防火墙：千兆产品成为主流，内容过滤成为核心功能，基于NP或ASIC。

# 安全产品现状及热点

## ④ 桌面（终端）安全

④ 数据安全保护类产品所占的比例是26%

④ 数据安全存储与访问

④ 基于生物特征识别的数据存储与访问

④ 病毒、恶意代码防护

# 安全产品现状及热点

## ④ 网络安全管理

- ④ 网络安全管理、身份认证、审计、监测类产品的比例达到33%;
- ④ 据报道，2004年上半年入侵检测与防护产品的销售额达到1.6亿元，占整个安全市场的12.1%。

# 安全产品发展趋势

## ④ 内容安全

- ④ 病毒、蠕虫、恶意代码、垃圾邮件仍将对网络 and 用户产生持续的、极大的威胁。
- ④ IDC公司预测，从2004年到2008年，安全内容管理（Security Content Management, SCM）市场将以54.4%的年复合增长率递增。
- ④ 恶意代码检测：基于特征代码、启发式扫描、数据挖掘、人工免疫、行为判断等技术将得到发展和应用。
- ④ 促进边界防护和桌面防护产品的发展。

# 安全产品发展趋势

## 可信计算

- 身份识别、数字签名、数据安全、BIOS安全、.....
- Intel、微软、IBM、HP和Compaq早在1999年10月共同发起成立了TCPA（可信计算平台联盟）。
- 2002年底，IBM发布了一款带有嵌入式安全子系统ESS的笔记本电脑。
- 2003年4月8日，TCPA中的AMD、HP、IBM、Intel和微软对外宣布，将TCPA重新改组，更名为TCG（可信计算集团）。
- 2003年9月17日，Intel正式推出了支持Palladium的LaGrande技术。
- 国内近一两年，联想集团、武汉瑞达等公司开始了可信计算的产业化工作。

# 安全产品发展趋势

## ④ 无线网络安全

- ④ 美国2004年9月面世的Surfcontrol Mobile Filter，是专门针对企业日益增长的无线应用所带来的安全威胁。
- ④ 根据Jupiter Research发布的调查数据，已经有57%的企业用户支持无线应用，此外还有22%的企业计划在2004年底之前部署无线技术。
- ④ 国内已有单位开始对无线网络安全技术进行研究。



谢 谢

2005年3月