网络安全若干技术难点初探

国家计算机网络应急技术处理协调中心
云晓春

- 务虚：网络安全
- 网络安全的国家需求
- 网络安全形势分析
- 网络安全若干技术难点

务虚：网络安全

网络安全内涵

核心目标

- 确保系统不被非授权用户恶意使用
- 确保系统时刻能为授权用户提供基本服务

问题根源

- 设计的不完备性--现有的互联网设计缺乏完整的安全体系结构，大量安全事件的难以追踪
- 实现的不确定性--软件正确性难以证明，网络应用存在安全漏洞不可避免
- 应用的不可控性--系统配置复杂，难以保证使用者正确使用系统

网络安全的国家需求

信息安全的国家需求-美国

《Executive Order 13231—Critical Infrastructure Protection in the Information Age》（2001）

《信息时代的关键基础设施保护》

…establish the “Preside-nt’s Critical Infrastruct-ure Protection Board” …; …ensure protection of information systems for critical infrastructure …

… 建立总统的关键基础设施保护委员会…; …保护关键基础设施中的信息系统…

信息安全的国家需求-美国

《National Strategy to Secure Cyberspace》（2003）

《保护网络空间的国家战略》

Prevent cyber attacks ag -ainst America's critical infrastructures; … articul -ates five national priorit -ies including: A Nationa -l Cyberspace Security Response System …

防止关键基础设施遭受网络攻击；…明确5项国家优先计划包括：(建立)国家网络空间安全响应系统…

信息安全的国家需求-俄罗斯

《DOCTRINE OF INFORMATION SECURITY OF THE RUSSIAN FEDERATION》（2000）

《国家信息安全学说》

creation and improvement of the system of ensuring information security of the Russian Federation; … prevention and suppression of violations of law in the information sphere …

建立和完善俄联邦信息安全保障系统；…防范和抑制信息领域的犯罪活动…

信息安全的国家需求-中国

中办发[2003]27号

中共中央办公厅
国务院办公厅

《国家信息化领导小组关于信息安全保障工作的意见》

- 实行信息安全等级保护
- 建设和完善信息安全监控体系
- 重视信息安全应急处理工作

信息安全的国家需求-中国

国发[2005]44号

《国家中长期科学和技术发展规划纲要》
(2006—2020年)

中华人民共和国
国务院

建立信息安全技术保障体系，具备防范各种信息安全突发事件的技术能力。

信息安全的国家需求-中国

中办发[2006]11号

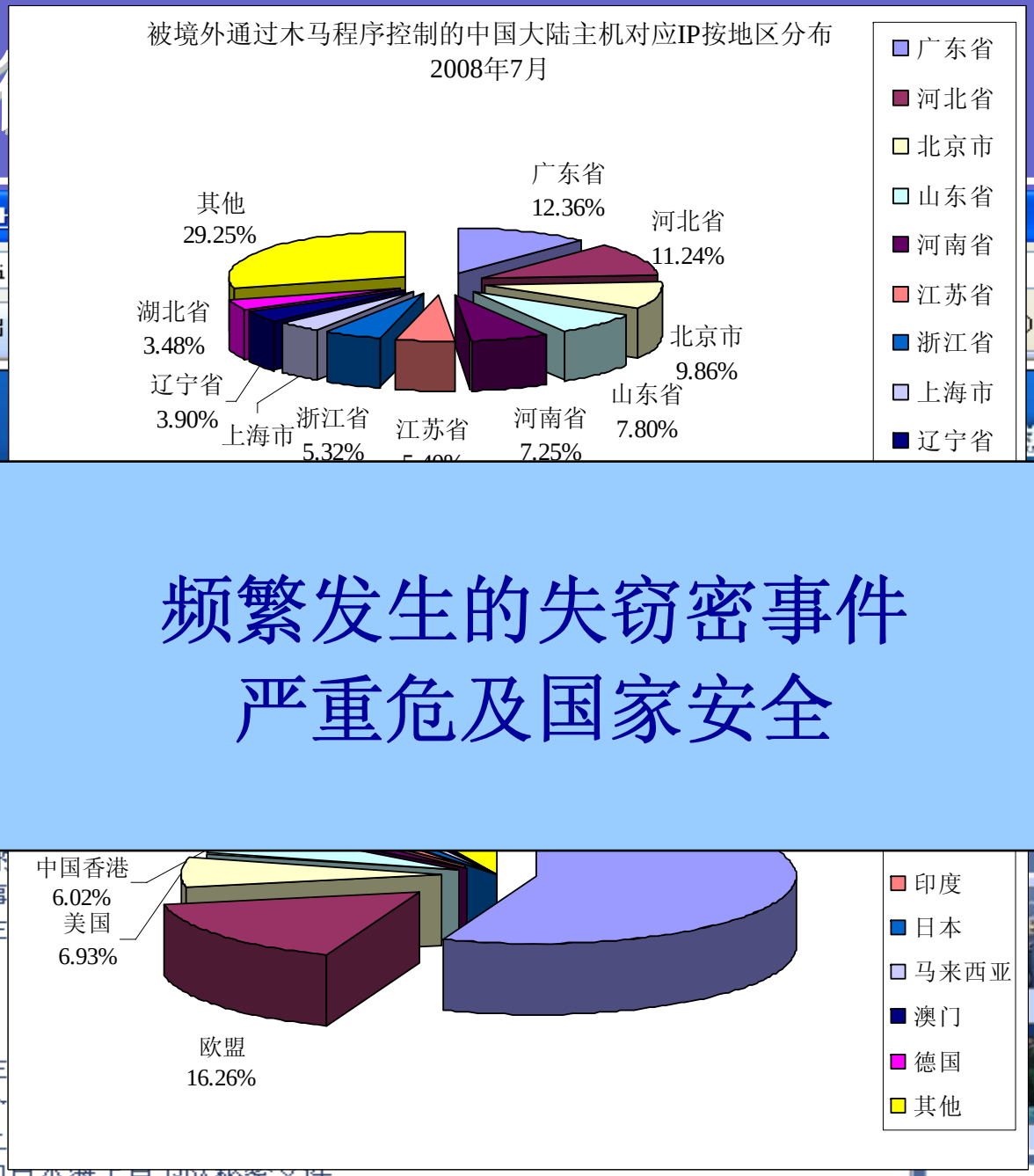
中共中央办公厅
国务院办公厅

关于印发
《2006—2020年
国家信息化发展
战略》的通知

建设和完善信息安全监控体系，提高对网络安全事件应对和防范能力，防止有害信息传播。

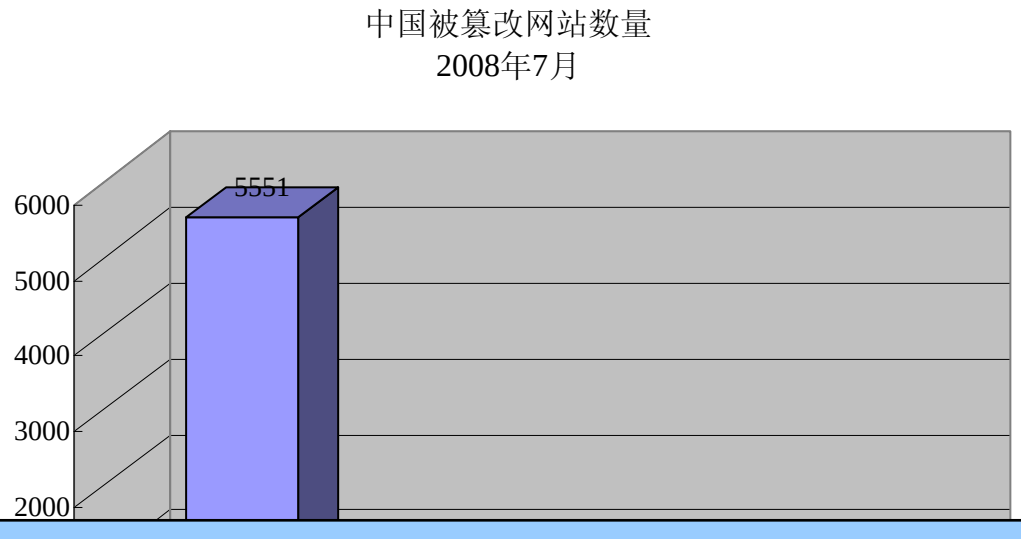
网络安全形势分析

从外显

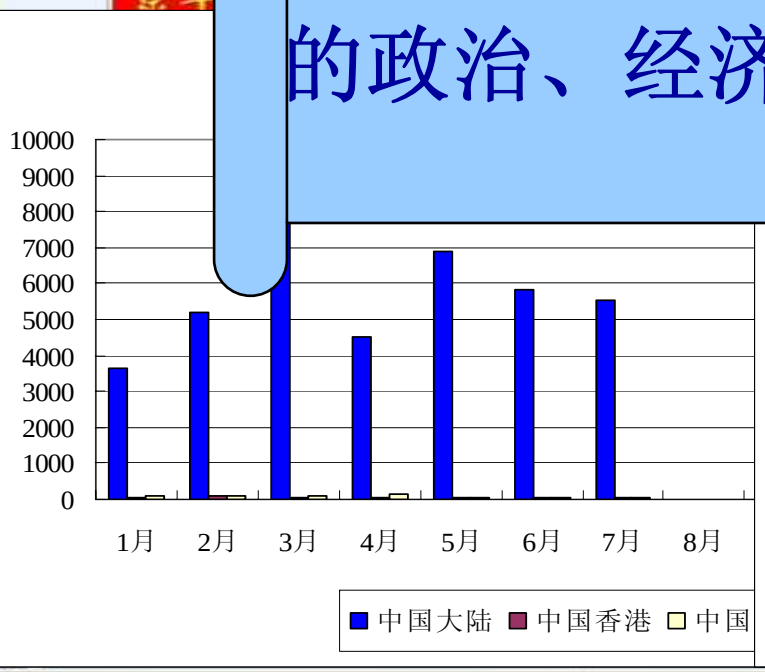


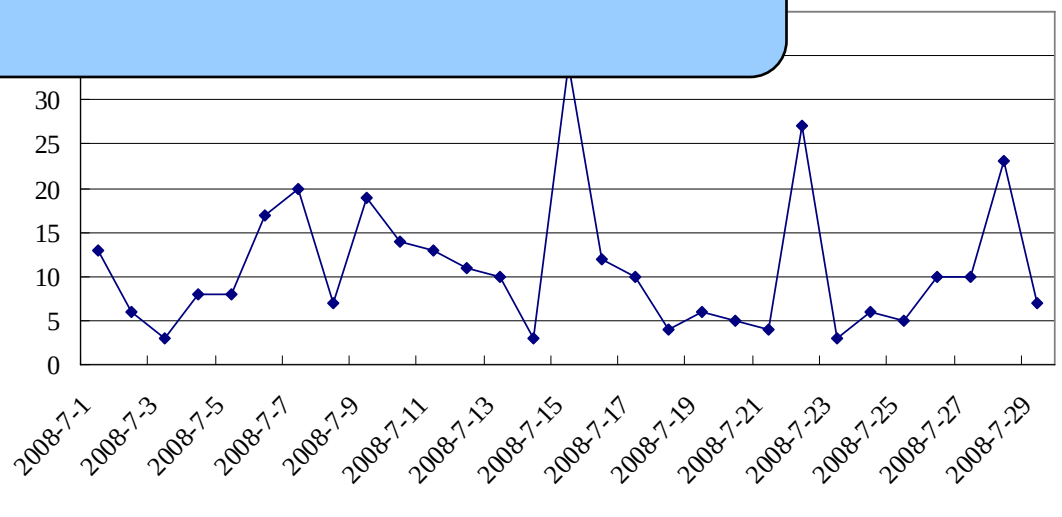
频繁发生的失窃密事件
严重危及国家安全

从外显

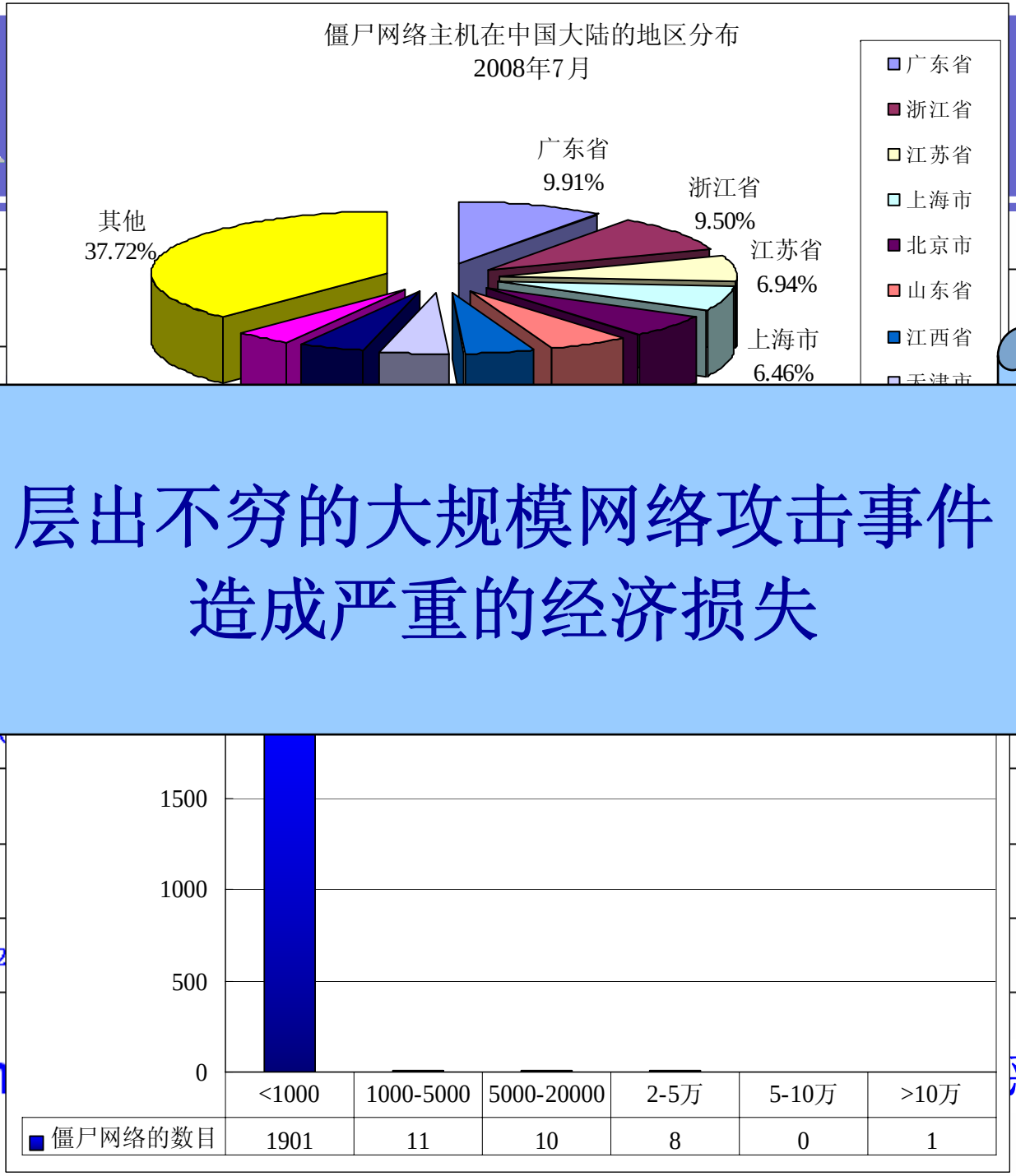


对网络资源的滥用，扰乱国家的政治、经济秩序，影响社会稳定





从外显



CIH（1998.6）

梅利莎(Melissa)

我爱你(IL

红色代码(

SQL Slamm

冲击波(Bl

霸王虫(So

MyDoom(2004.1)

Bagle（2004.1）

震荡波(Sasser)(2

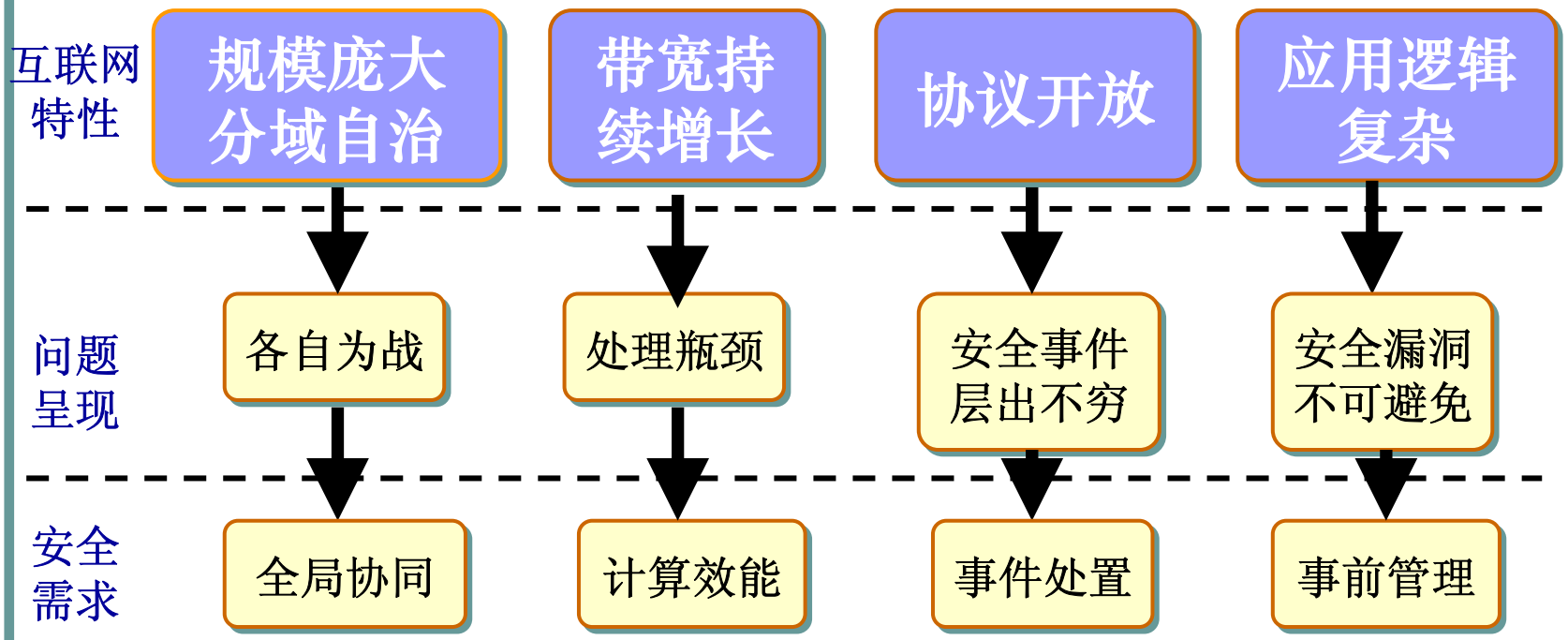
层出不穷的大规模网络攻击事件
造成严重的经济损失

摘自《Inform

恶意代码

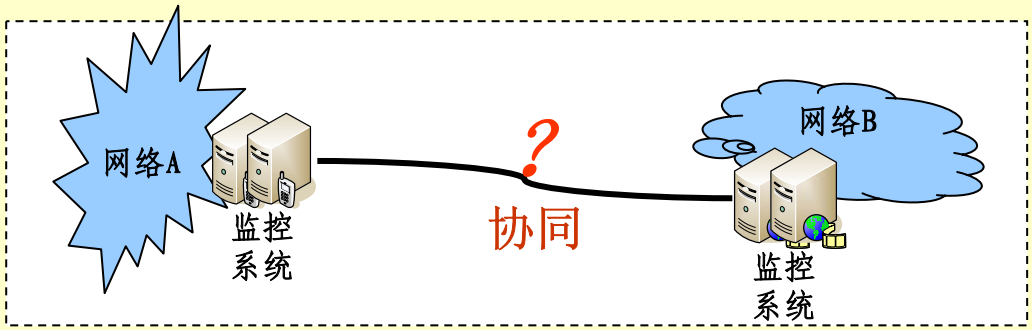
网络安全若干技术难点

挑战性问题


互联网特性
规模庞大 分域自治
带宽持续增长
协议开放
应用逻辑复杂
问题呈现
各自为战
处理瓶颈
安全事件层出不穷
安全漏洞不可避免
安全需求
全局协同
计算效能
事件处置
事前管理

全局协同

- 异构网络安全资源的整合问题

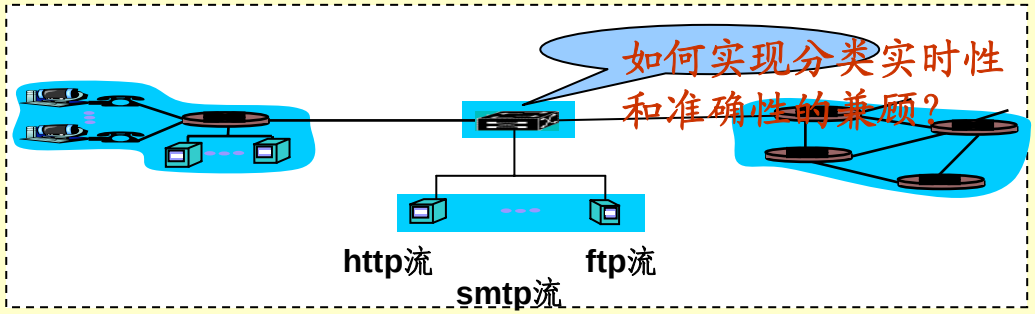


促进安全系统建设由自发向自觉转化

- 开放的安全管理体系框架和标准
- 包容已有的安全系统，适应未来的安全系统

计算效能

- 高效的数据业务流分类问题

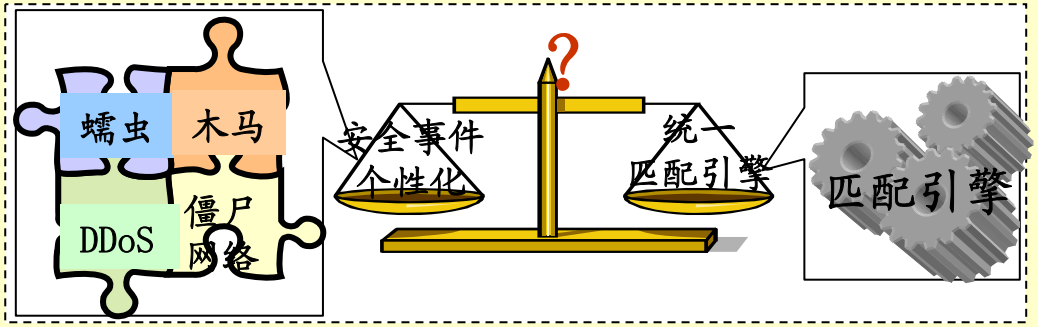


实现无关协议数据的精简

- 基于行为特征的流识别：学习模型
- 基于内容特征的流识别：特征提取

计算效能

➢安全事件的多样化和统一匹配引擎之间的矛盾消除问题

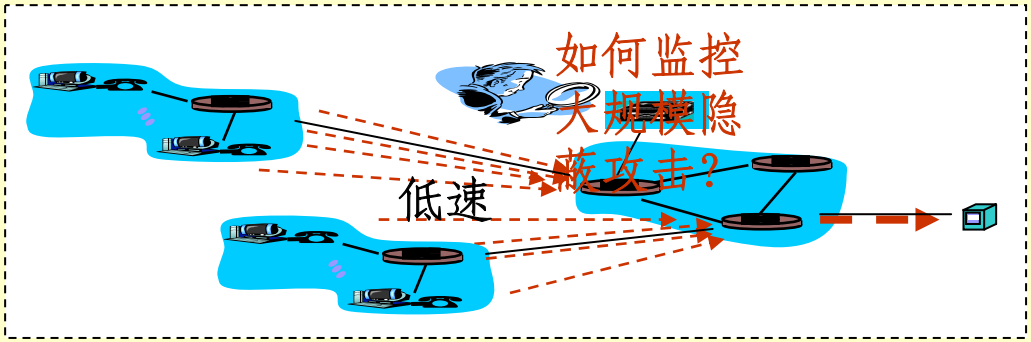


实现安全事件特征的高效匹配

- 大规则集串匹配算法
- 大规则集正则表达式匹配算法

事件处置

➢隐藏特征（低速率、源欺骗）分布式攻击的监控问题

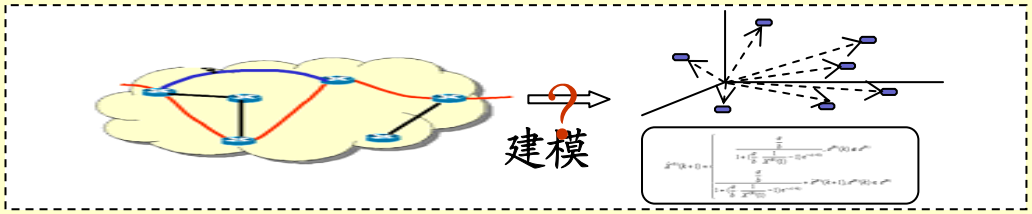


着眼于非预设条件的大规模安全攻击趋势

- 异常行为建模
- 控制策略优化选择

事件处置

- 高性能大规模网络行为模拟的抽象建模问题

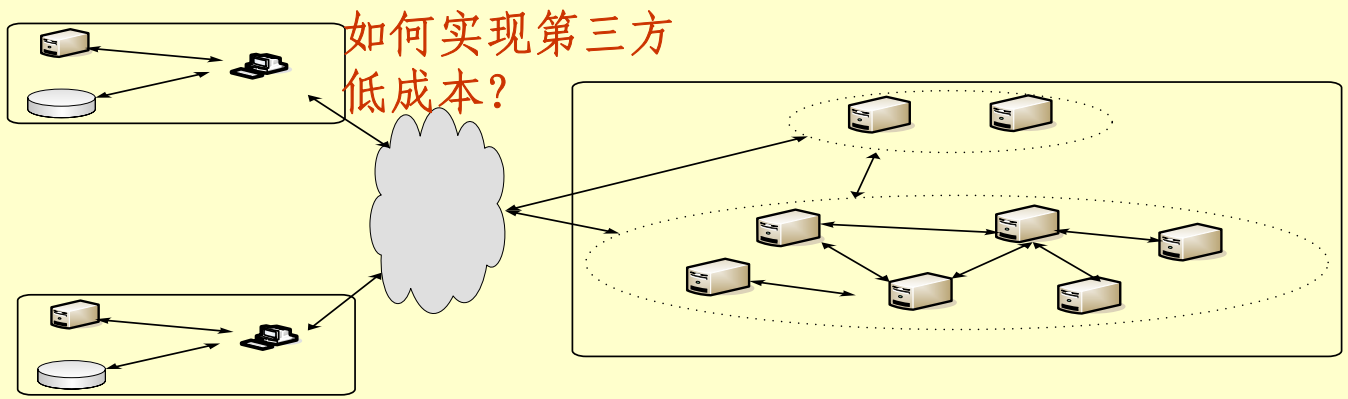


应用于安全态势预测

- 高可信、低复杂度的大规模网络行为模拟
- 多模式（模拟、模型、知识推理）结合的网络安全行为建模

事件处置

- 结构无关的数据灾备问题



数据流实时备份

致力于实现IBC

- 应用无关的快照技术
- CDP数据保护
- 降低数据存储冗余量，保证数据可靠性

灾备客户端

磁盘级增量备份

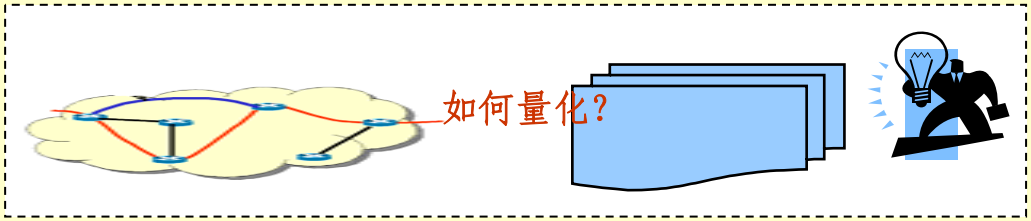
客户系统

Internet

数据流实时备份

事前管理

➢等级保护与风险评估问题



实现对于网络安全性的真实、客观分析

- 信息系统等级保护技术实现体系结构
- 不同级别信息系统之间的访问策略的冲突消解与可信互联模型
- 信息系统等级保护安全功能符合性检验技术
- 宏观网络安全态势指标体系
- 隐藏网络脆弱性推断技术
- 无损伤匿名漏洞探测技术
- 基于弱点关联的安全性分析技术

事前管理

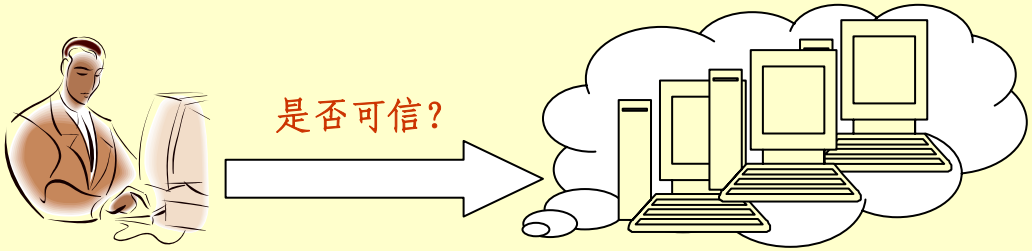
➢未知漏洞挖掘问题

致力于漏洞挖掘由技巧化向理论化的转变

- 基于漏洞分类特征的未知漏洞挖掘技术（变打哪指哪为指哪打哪）
- 无系统样本条件下，目标系统运行时未知漏洞检测技术
- 未知漏洞预测模型，推断目标系统可能存在的未知漏洞

事前管理

- 可信计算问题



致力于信息系统安全可信的源头解决

- 可信计算平台体系结构
- 可信计算平台安全测评技术

结论

- 大规模网络的客观属性决定了网络安全问题将在一段时间内长期存在
- 网络安全技术将随攻守双方的对抗不断向前演进

谢　　谢

云晓春