

密码学与网络安全

二〇一二年秋季

任课教员

► 张 权

联系方式：74481-801, 13974829072

办公地点：四院综合电子科技大楼404

电子邮件：quanzhang@nudt.edu.cn
zhangquan@gfkd.mtn

教材及主要参考资料

1. W. Stallings, *Cryptography and Network Security – Principles and Practice*(5th Edition), 2011.1
2. 王育民, *通信网的安全—理论与技术*, 西安电子科技大学出版社, 2000.7
3. O. Goldreich, *Foundations of Cryptography*

课时安排

第零部分	安全的基本概念	2课时
第一部分	对称密码技术	10课时
第二部分	公钥密码技术	6课时
第三部分	数据完整性技术	6课时
第四部分	认证协议原理与实践	6课时
第五部分	信息安全技术实现	6课时

考核方式

- ▶ 课堂表现（20%）：
 - 课堂互动（5%）
 - 编程实践（10%）
 - 作业（5%*）
- ▶ 课程考试（80%）：闭卷，内容覆盖率90%，及格率?%，优秀率20%

教学目标

- ▶ 树立正确的信息安全观念
- ▶ 掌握重要的密码算法和技术
- ▶ 利用密码技术设计实现安全系统
- ▶ 明确信息系统或应用中安全的地位和作用
- ▶ 具备足够的基础知识和经验，快速掌握信息安全技术的最新进展，开展相关研究实践

安全的基本概念

张 权

二〇一二年秋季

为什么不安全-现实威胁

► Internet快速发展

- 计算机技术/通信技术/网络技术
- TCP/IP
- www/浏览器
- 分布式管理
- 商务

为什么不安全-现实威胁

► Internet快速发展

Internet的美妙之处在于

你和每个人都能建立连接

Internet的可怕之处在于

每个人都能和你建立连接

为什么不安全-现实威胁

- ▶ 1988 年 11 月 3 日 , “Morris”—— 第一个出现在Internet上, 在几小时之内, 6000台服务器被传染, Internet陷入瘫痪, 直接经济损失1亿。
 - Internet安全性研究开始

为什么不安全-现实威胁

► 1994 年 12 月 25 日, Mitink 侵入了 San Diego 级计算中心的计算机网络, 导致持续数月的网络瘫痪。

- Hacker
- Cracker
- Sneaker
- Script Kids

为什么不安全-现实威胁

- ▶ 99年4月26日，台湾人编制的CIH病毒大爆发
 - 全球超过六千万台电脑被不同程度破坏
 - 大陆受其影响的PC机总量超过 36 万台
 - 有估计经济损失近 12 亿元

为什么不安全-现实威胁

- ▶ 2000年2月份黑客攻击的浪潮，是互连网问世以来最为严重的黑客事件，三天内黑客使美国数家顶级互联网站——Yahoo、Amazon、eBay、CNN陷入瘫痪。
 - DDOS
 - 直接经济损失超过10亿美元
 - 道穷斯指数下跌了200多点
 - 纳斯达克指数下跌了80个点

为什么不安全-现实威胁

- ▶ 2000年5月4日，“爱虫（ LOVE BUG）”病毒大爆发。
 - 据美国“电脑经济”研究机构发布的统计数据，“爱虫”大爆发两天内，全球约4500万台电脑被感染，直接损失达到26亿美元。
 - 此后几天里，“爱虫”病毒所造成的损失仍以每天10亿美元左右的速度增加。

为什么不安全-现实威胁

- ▶ 2000年1月，来自亚洲的黑客群攻日本网站。
 - 日本政府11个省、厅受到黑客攻击
 - 总务厅的统计信息全部被删除
 - 外务省主页3分钟受攻击1000余次
 - 最高法院26—28日受攻击3000余次

为什么不安全-现实威胁

- ▶ 2006年11月，熊猫烧香引发病毒狂潮。
 - 传播方式囊括了漏洞攻击、感染文件、移动存储介质、局域网传播、网页浏览、社会工程学欺骗等种种可能的手法。

为什么不安全-现实威胁

- ▶ 2008年，俄攻击格鲁吉亚网络系统，使格鲁吉亚的交通、通信、媒体和金融网络瘫痪
- ▶ 2009年1月，病毒攻击法国海军计算机系统，使其计算机系统不能启动，战斗机因无法“下载飞行指令”停飞两天
- ▶ 2009年，“震网”病毒破坏伊朗核计划
- ▶ 2009年6月，美军宣布成立Cyber司令部
- ▶ 今年5月，“火焰”病毒曝光

为什么不安全-现实威胁

- ▶ 据统计，全球约20秒就有一次计算机入侵事件发生
- ▶ Internet上约1/4的防火墙 (曾)被突破
- ▶ 约70%以上的网络信息主管人员承认因机密信息泄露而遭受损失

什么是信息安全

► 什么是信息

- 信息论奠基人香农在《通信的数学理论》中提出，信息是“两次不确定性之间的差异”，是用以消除随机不确定性的东西。
- 控制论的创始人维纳认为：信息是人与外部世界相互交换的内容的名称。
- 我国信息论专家钟义信教授：事物运动的状态和方式。

什么是信息安全

► 什么是信息

- 哲学角度：信息是一切物质的属性。既非物质又非精神的第三态。
- 在本课程中：信息就是消息所携带的语义内容。
- 信息的特点：可以被传输、存储、使用

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/657055146022006134>