网络及其内容安全
Network and Content Security

北京邮电大学
信息与通信学院
裘晓峰
qiuxiaofeng@bupt.edu.cn



Significance of network security

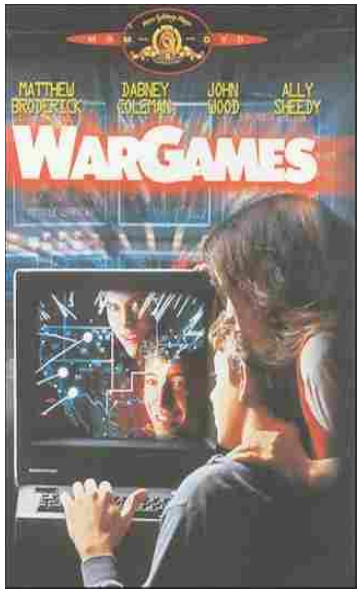
- It has been shown that complex networks including the Internet are resilient to independent random failures, but fragile to intentional attacks

Doyle, J.C., Alderson, D., Li, L., Lowet, S., et al.: The ‘Robust Yet Fragile’ Nature of the Internet. PNAS 102(41) (2005)

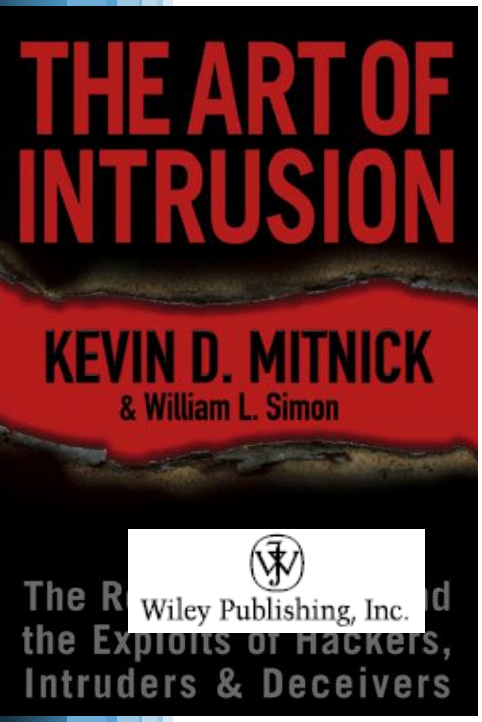
历史

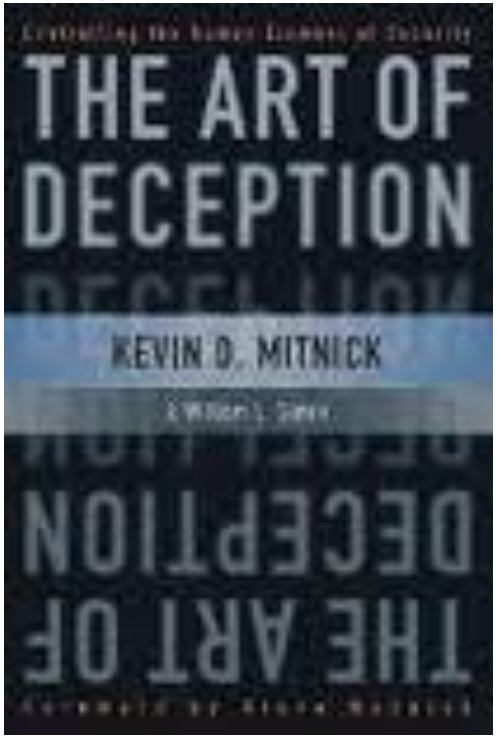
凯文.米特尼克

- 凯文•米特尼克是美国20世纪最著名的黑客之一，他是“社会工程学”的创始人
- 1979年他和他的伙伴侵入了北美空防指挥部



1983年的电影《战争游戏》演绎了同样的故事





下村勉 (Tsutomu Shimomura)
《纪实：追捕美国头号电脑通缉犯——由追捕者自述》

莫里斯蠕虫（Morris Worm）

- 时间
  - 1988年
- 肇事者
  - -Robert T. Morris ，美国康奈尔大学学生，其父是美国国家安全局安全专家
- 机理
  - -利用sendmail, finger 等服务的漏洞，消耗CPU资源，拒绝服务
- 影响
  - -Internet上大约6000台计算机感染，占当时Internet 联网主机总数的10%，造成9600万美元的损失
- CERT/CC的诞生
  - -DARPA成立CERT（Computer Emergency Response Team），以应付类似“蠕虫（Morris Worm）”事件



重要的安全事件

- 近年黑帽大会(Blackhat)&Defcon演示的攻击
  - “BadUSB”的重大USB安全漏洞，可以使USB接口控制器芯片固件被重新编程，

    移动互联网安全：

    物联网安全： 心脏起搏器(Pacemaker)和植入型心脏复律除颤器(ICD)； 胰岛素泵；汽车；飞机；武器
- OpenSSL曝出“心脏流血”(Heartbleed)安全漏洞：获得服务器私钥



安全事件

- 实例：
  - 智能家居：
    http://m.bobao.360.cn/learning/detail/648.html
  - **2015**上半年十大网络安全事件：
    http://songwl.baijia.baidu.com/article/96709
  - **2015**美黑帽大会**10**大演讲:
    http://jroclee.baijia.baidu.com/article/119520

IMPLANTABLE MEDICAL DEVICES: HACKING HUMANS

PRESEN

Barnaby

In 2006 approximately 350,000 pacemakers and 173,000 ICD's (Implantable Cardioverter Defibrillators) were implanted in the US alone. 2006 was an important year, as that's when the FDA began approving fully wireless based devices. Today there are well over 3 million pacemakers and over 1.7 million ICD's in use.

This talk will focus on the security of wireless implantable medical devices. I will discuss how these devices operate and communicate and the security shortcomings of the current protocols. Our internal research software will be revealed that utilizes a common bedside transmitter to scan for, and interrogate individual medical implants.

I will also discuss ideas manufacturers can implement to imp
these devic

Barnaby Jack

(ID：dark spyrit)



安全事件

- 课外：
  - http://www.blackhat.com/
  - https://www.defcon.org/
  - http://www.wooyun.org/
  - 公司技术博客：
    - http://blog.nsfocus.net/
    - http://blogs.360.cn/

国家安全层面

- **Security of Critical infrastructure:**
  - 2010, StuxNet: http://en.wikipedia.org/wiki/Stuxnet
  - 2012 Flame virus

- **APT (Advanced Persistent Threat)**
  - SCADA (Supervisory Control and Data Acquisition)
  - Symantec demon: http://www.symantec.com/connect/blogs/stuxnet-breakthrough

cyberwar

- **Pentagon declared that any cyber attack by a foreign power against a U.S. asset could be interpreted as an act of war and would be answered with measured military force, even a missile strike as retaliation, 2011**



再加上：可怕的水桶原理

“没有安全的信息化是一种灾难”

[yes, this is a doctored photo, used here just to lighten a serious moment]

Source: **http://www.armscontrolwonk.com/1955/missile-palooza**



课程目的：

- 培养安全意识 （安全和我们有什么关系？）
  - 无论将来做什么，基本的安全意识都是必须的
- 掌握基本安全技术
  - 安全是几乎所有系统的一部分
- 了解最新网络发展动态及相关安全威胁和技术
  - 安全技术的发展与网络、业务发展密切相关
- 欢迎进入安全行业

安全产业和职业市场

几乎各行各业

- 政府机关
- 测评认证组织
- 院校研究机构
- 互联网公司、安全公司、网络公司、金融企业、企业 IT部门…
- 国防产业、军队、警察…

攻防、架构、管理、审计、开发、评估、运营、保障、取证….

企业需要即懂业务又具备一定安全知识的人才
安全行业需要即懂安全，又了解业务的人才

宽广的知识 ⟷ 极专业的技能

安全市场的人才竞争：职业市场的真实故事

安全产业所需知识技能

- 管理
  - 国内外相关标准和法律法规
  - 业务连续性、灾难恢复…
- 咨询
  - 漏洞挖掘、安全风险、风险评估、扫描与渗透测试技术 …
- 研发
  - 各种安全威胁，包括攻击与入侵、病毒、内部误用与滥用…
  - 安全架构、密码技术、安全编码、安全测试、安全开发环境…
- 维护
  - 各种IT设备的安全维护和安全配置
  - 安全事件紧急响应、事件重建与分析…

宽广的知识 ⟷ 极专业的技能

网安武器：信息安全大阅兵进行时！

http://mp.weixin.qq.com/s?__biz=MjM5ODM2MjQzNg==&mid=207763108&idx=1&sn=3c24511899273b7b006d4fbb9cfa30ed&scene=5&srcid=0904s6EpXdbwwaedz9NPU2Iy#rd

课程内容：

What is Cyber Security?

According to the
NATIONAL INITIATIVE for CYBERSECURITY CAREERS and STUDIES

"Cyber Security consists of strategy, policy, and standards regarding the security of and operations in cyberspace, encompassing the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure."

Kennesaw State University

Coursera: Cybersecurity and Its Ten Domains

课程内容：信息安全与网络安全

组织/人事

业务/应用

数据/信息

环境/设施

不仅仅是攻防

信息安全更广的范畴：信息对抗， 信息隐藏，数字版权…



网络与内容安全课程大纲

- 概述：安全概念、相关标准、术语等 2
- TCP/IP 基础及互联网安全威胁 8
- 密码学基础 及应用 6
  - ✓ 电子商务，PKI及证书
- ✓ 网络安全技术 4
  - ✓ 安全域，VPN，防火墙，入侵检测，抗DOS等
- ✓ 认证与授权 6
  - ✓ 认证模型，互联网认证协议
- ✓ WEB安全（代码安全） 2
- ✓ 总结，作业点评，考试 4



教学基本要求

- 要求的基础
  - TCP/IP基本原理
  - 计算机网络
- 按时到课
- 课前预习
- 课后：练习，课外资料扩展阅读



reference：

- 各章讲义中的参考资料及网站

- **Online reference:**

  http://www.freetechbooks.com/information-security-f52.html

  - **Principles of information security** fourth edition, Michael E. Whitman, Herbert J. Mattord, 2011 （books.google.com）

- 一本很有思想的书：

Security engineering Ross Anderson 2007

中文:信息安全工程（第2版）齐宁等译 清华大学出版社，2012



网络及其内容安全评分

- 平时成绩：　20％
- 作业：　30%
- 考试大作业：５０％



作业邮箱，请发送至

xxwlaq2015@126.com （信息网络安全）

Subject：学号_作业内容名称

课件下载，百度网盘账号:
buptnetwork2013@163.com

百度网盘密码: lessonbupt

Thank You!

LOGO