哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY
立足航天，服务国防，面向国民经济主战场

计算机网络之危机四伏

主讲人：李全龙

本讲主题

网络安全状况

我国互联网基本状况

-引自《2014年中国互联网网络安全报告》

- 截至2014年12月底：
  - 网站总量为364.7万
  - 独立域名为481.2万
  - ISP为1068家
  - 网民规模为6.49亿
  - 手机网民规模达5.57亿
  - 互联网普及率为47.9%

我国互联网网络安全状况

- 总体平稳，形势严峻
- 基础网络仍存在较多漏洞风险
  - 2014年，CNCERT/CC协调处理涉及电信企业漏洞事件1578起
  - CNVD(国家信息安全漏洞共享平台)收录与基础电信企业软硬件资产相关漏洞825个，66.2%与路由器、交换机等网络设备相关
- 云服务日益成为网络攻击重点目标
- 域名系统面临严峻的拒绝服务攻击
  - 2014年，针对我国域名系统，流量规模达1Gbps以上的拒绝服务攻击事件，日均约187起
- 针对重要网站的域名解析篡改攻击频发
- 网络攻击威胁逐渐向工业互联网渗透
  - 2014年9月，出现一种远程木马“Havex”，利用OPC（开放通用通信协议）工业通信技术，扫描发现工业系统联网设备，收集工控设备详细信息并回传
  - 可以接收、执行恶意代码

我国互联网网络安全状况

- 分布式反射型攻击逐渐成为拒绝服务攻击的重要形式
- 涉及重要行业和政府部门的高危漏洞事件增多
- 基础应用或通用软硬件漏洞风险凸显
  - “心脏出血”（Heartbleed）
  - “破壳”（Bash Shell Shock）
- 漏洞风险向传统领域、智能终端领域泛华演进
- 网站数据和个人信息泄露仍呈高发态势
- 移动应用程序成为数据泄露的心主体
- 移动恶意程序逐渐从主流应用商店向小型网站蔓延
- 具有短信拦截功能的移动恶意程序大爆发
- 针对金融、电信行业的网页仿冒事件大幅增加
- 钓鱼站点逐渐向云平台迁移
- 针对政府部门和重要行业单位网站的网络攻击频度、烈度和复杂度加剧

互联网网络安全一组数据（2014年）

木马和僵尸程序监测：

- 木马或僵尸程序控制服务器IP地址总数104230(↓45.0%)
- 木马或僵尸程序受控主机IP地址总数为13991480(↓25.2%)

“飞客”蠕虫监测：

- 全球互联网月均近943万台主机IP地址感染“飞客”蠕虫

移动互联网安全监测：

- CNCERT/CC捕获或通过厂商交换获得的移动互联网恶意程序样本数为951059（↑35.3%）
  - 恶意扣费类居首，为522889（55.0%），资费消耗类（15.3%）、隐私窃取类（12.9%）分列二、三位
  - 针对Android平台的占99.9%，其次是Symbian，占0.1%

互联网网络安全一组数据（2014年）

网站安全监测：

- 我国境内被篡改网站数量为36969个（↑45.0%）
  - 政府网站1763个（↓27.4%）
- 监测到仿冒、钓鱼页面99409个
- 监测到40186个境内网站被植入后门

安全漏洞：

- CNVD收集新增漏洞9163个
- 前三甲漏洞：应用程序漏洞（68.5%）、Web应用漏洞（16.1%）、网络设备漏洞（6.0%）

网络，安全？

网络安全吗？

- —不！
- —不十分安全！

❖ 目标：网络，安全！

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

立足航天，服务国防，面向国民经济主战场

谢 谢！