第8章
抗恶意软件

第8章 内容概要

- 8.1 病毒
- 8.2 蠕虫
- 8.3 病毒防御
- 8.4 特洛伊木马
- 8.5 网络骗局
- 8.6 点对点安全
- 8.7 Web安全
- 8.8 分布式拒绝服务攻击

病毒

- 病毒是一段隐藏在程序中的代码，可以自动的自我复制或者将自己嵌入其它程序
  - 不能自我传播
  - 常常需要一个主机程序寄生
  - 被感染的程序: 有病毒的主机程序
  - 非感染程序 (健康程序): 一个没有病毒的程序
  - 已消毒程序 :一个曾经感染了病毒但目前清除了的程序
- 特定于
  - 特殊类型的文件系统, 文件格式和操作系统
  - 特殊类型的体系结构, CPU, 语言, 宏, 脚本, 调试器, 和其它程序或系统环境

病毒类型

- 基于主机程序分类:
  - 引导区病毒:
    - 在引导区感染引导程序
    - 利用引导序列激活自己
    - 修改操作系统拦截磁盘访问并感染其它磁盘
    - 也可能感染PC的可写BIOS
  - 文件系统病毒:
    - 改写表项并通过文件系统传播
    - 文件系统包含一个指针表，指向一个文件的第一个簇
  - 文件格式病毒:
    - 感染单个文件
  - 宏病毒:
    - 感染包含宏病毒的文档

病毒类型(续)

- 脚本病毒:
  - 感染脚本文件
  - 在邮件附件，办公和Web文档中复制自己
- 注册表病毒:
  - 感染微软Windows的注册表
- 内存病毒:
  - 感染在内存中执行的程序

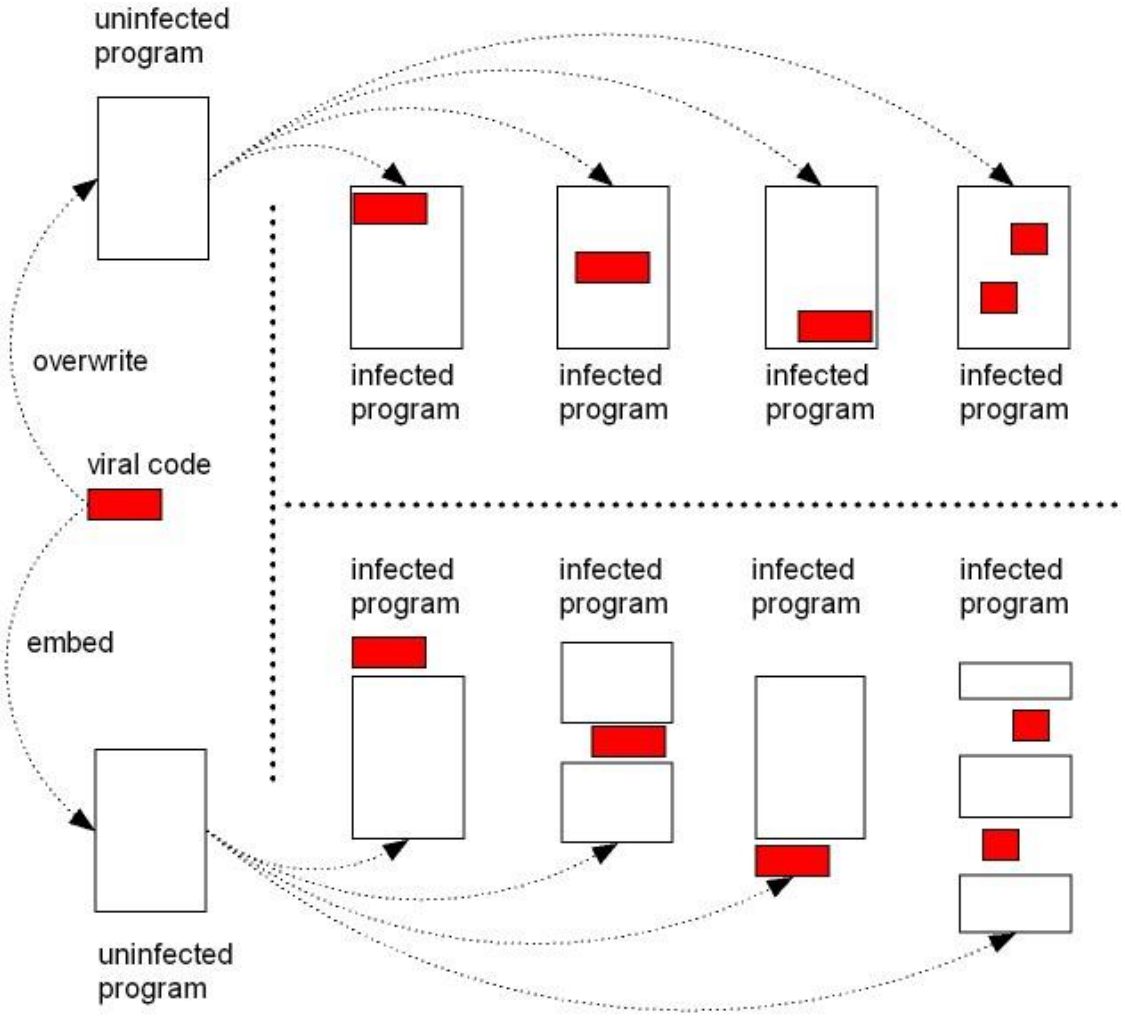
- 基于植入形式分类:
  - 隐蔽型病毒:
    - 通常用压缩来实现
  - 多态病毒:
    - 可能改变指令顺序或者讲自己加密成不同的形式
  - 变化态病毒:
    - 在传输的过程中可能被自动重写

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

病毒感染方式

- 改写一个程序的片段
- 将其插入一个未感染程序的开始，中间和结尾
- 将自己分为多片并插入主机程序的不同位置
- 病毒和主机程序具有相同的访问权限

病毒感染方案 (图示)



《计算机网络安全的理论与实践（第2版）》. 【美】王杰, 高等教育出版社, 2011年.

病毒结构

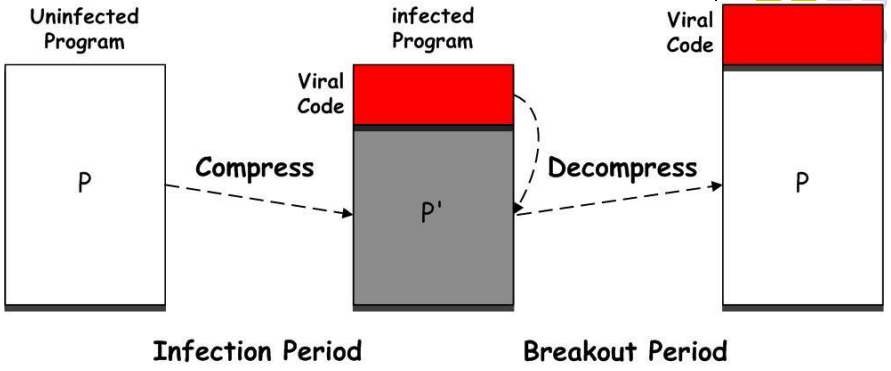
- 有四个主要的子程序构成
  - 感染
    - 搜索主机程序并检测是否被感染
  - 感染-条件
    - 检查是否具备执行感染子程序的条件
  - 发作
    - 执行具体的破坏工作
  - 发作-条件
    - 检查是否具备执行发作子程序的条件

```
1.  program V:= {
2.          12345;
3.          goto main;
4.          subroutine infect:= {
5.              loop:
6.              P:= get-random-host-program;
7.              if(the second line of P = 12345;)
8.                  then goto loop
9.                  else insert lines 1-27 in front of P;
10.         }
11.         subroutine break-out:= {
12.             modify selected files;
13.             delete selected files;
14.             ...
15.         }
16.         subroutine infection-condition:={
17.             return true if certain conditions are satisfied;
18.         }
19.         subroutine breakout-condition:= {
20.             return true if certain conditions are satisfied;
21.         }
22. main: main-program:= {
23.             if infection-condition then infect;
24.             if breakout-condition then break-out;
25.             goto next;
26.         }
27. next:
28. the original host program ...
29. }
```

《计算机网络安全的理论与实践（第2版）》. 【美】王杰，高等教育出版社，2011年.

载体压缩病毒

- 一个被感染的主机文件常常在被感染前后表现出不同的文件大小
- 载体压缩病毒试图掩盖这种变化
  - 在感染期间压缩主机文件
  - 在发作期间解压缩文件
  - 如果被压缩的主机文件加上病毒代码仍小于文件的原始大小，则需要填充




```
1.   program CV:= {
2.         012345;
3.         goto main;
4.         subroutine infect:= {
5.               loop:
6.               P:= get-random-host-program;
7.               if(the second line of P = 012345;)
8.                     then goto loop
9.                     else {
10.                          compress P to become P';
11.                          insert viral code in front of P';
12.                          }
13.        }
14.        subroutine break-out:= {
15.              modify selected files;
16.              delete selected files;
17.              ...
18.        }
19.        subroutine infection-condition:={
20.              return true if certain conditions are satisfied;
21.        }
22.        subroutine breakout-condition:= {
23.              return true if certain conditions are satisfied;
24.        }
25.  main: main-program:= {
26.              if infection-condition then infect;
27.              if breakout-condition then break-out;
28.              decompress P' back to P;
29.              Execute P;
30.        }
```

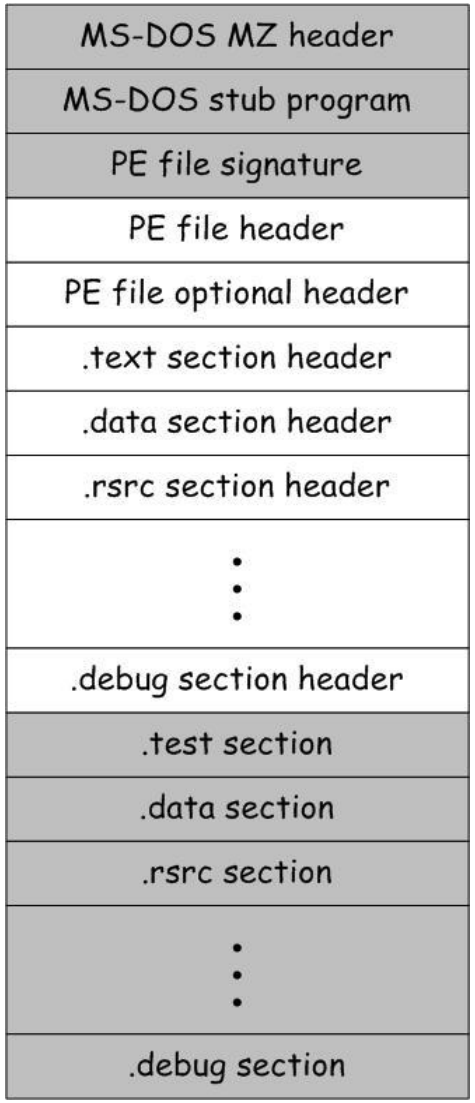
《计算机网络安全的理论与实践（第2版）》.

病毒的传播

- 通过便携存储设备传播 (传统的传播方式):
  - 软盘, CDs, 闪存
- 通过电子邮件附件和下载的程序传播 (目前的传播方式):
  - Email是重要的传播途径，因为许多电子邮件程序和用户通常会不加防备的盲目打开附件

Win32 病毒感染剖析

- Win32 病毒为了感染利用了微软的便携可执行(PE)的文件格式
- 一个PE文件包含:
  - PE分段:
    - 代码模块, 数据, 资源, 输入表和输出表
  - PE 头部:
    - 提供可执行镜像的重要信息
    - Win32病毒的首要目标

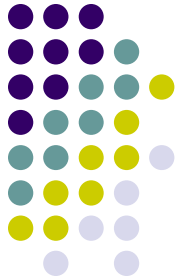


《计算机网络安全的理论与实践（第2版）》. 【美】王杰, 高等教育出版社, 2011年.

第8章 内容概要

- 8.1 病毒
- 8.2 蠕虫
- 8.3 病毒防御
- 8.4 特洛伊木马
- 8.5 网络骗局
- 8.6 点对点安全
- 8.7 Web安全
- 8.8 分布式拒绝服务攻击

蠕虫



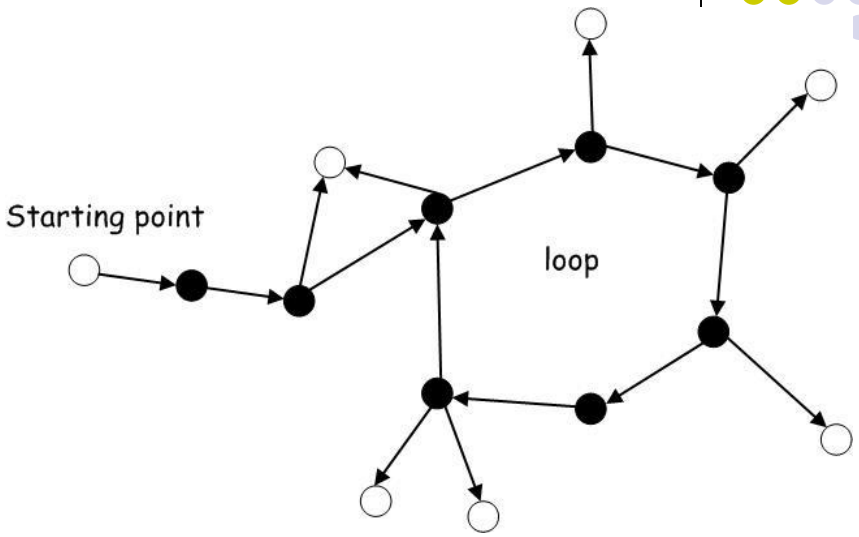
- 一个蠕虫是一个独立的程序，可以自我复制且通过网络传播
  - 可能会被看作网络病毒
- 可以在一个远程主机上自动的执行
  - 可能仍需要一个主机文件来传播
- 大多数蠕虫由下列组成
  - 目标定位器子程序: 找到新的目标
  - 感染传播器子程序: 将自己传输给一个信的计算机

常见蠕虫类型

- 批量邮件蠕虫
  - 通常在蠕虫的名字后面会加上“@mm”
  - 通过电子邮件附件而自我繁殖
- 兔子蠕虫
  - 迅速自我复制直到系统因为资源过载而奔溃
  - 通常隐藏在一个文件目录里或者以正常的文件名来伪装自己

蠕虫实例

- Morris蠕虫
  - 利用*sendmail, finger 和 rsh/rexec*实现的缺陷
  - 尽可能快的感染其它计算机
- Melissa蠕虫
  - 一种针对微软产品的宏病毒
  - 通过电子邮件附件传播
  - 传播迅速，造成了大量的Email流量



From: <the infected sender>
Subject: Important message from <the infected sender>
To: <The 50 chosen recipients>
Attachment: LIST>DOC
Body:
Here is that document you asked for ...
Don't show anyone else :-)

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

电子邮件附件

- 电子邮件附件（大致）可以分为三类
  - 安全
    - 不可执行, 不是宏
  - 须多加小心
    - 包含宏或者可执行代码，依赖于发送者
  - 危险
    - 不能打开

红色代码蠕虫

- 于2001年7月出现, 在24小时内感染了大约30万计算机
- 利用了微软IIS的一个缓冲区溢出漏洞
- 发送如下的 GET /default.ida 请求(包含224 N's)

```
GET /default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801
%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3
%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=aHTTP/1.0 ...
```

- 这个请求触发了蠕虫代码的执行

《计算机网络安全的理论与实践（第2版）》. 【美】王杰, 高等教育出版社, 2011年.

第8章 内容概要

- 8.1 病毒
- 8.2 蠕虫
- 8.3 病毒防御
- 8.4 特洛伊木马
- 8.5 网络骗局
- 8.6 点对点安全
- 8.7 Web安全
- 8.8 分布式拒绝服务攻击

病毒防御

- 预防: 阻止病毒进入健康系统
  - 及时安装软件补丁
  - 不要从不可信的Wed站点下载软件
  - 不要打开来自于位置发送方的“To-Be-Cautious” 邮件附件
  - 不要打开危险的邮件附件
- 恢复: 修复受感染系统
  - 用一个病毒扫描器扫描文件
  - 保持系统和用户文件的备份

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

标准扫描方法

- 基本扫描
  - 在主机文件中搜索知名病毒的特征
  - 检查系统文件的大小
- 启发式扫描
  - 在可执行文件中搜索可以代码片段
- 完整性校验值检查（ICV）
  - 对每个可执行文件计算ICV，附在文件后以备随后校验
- 行为监控
  - 评估可执行程序的行为

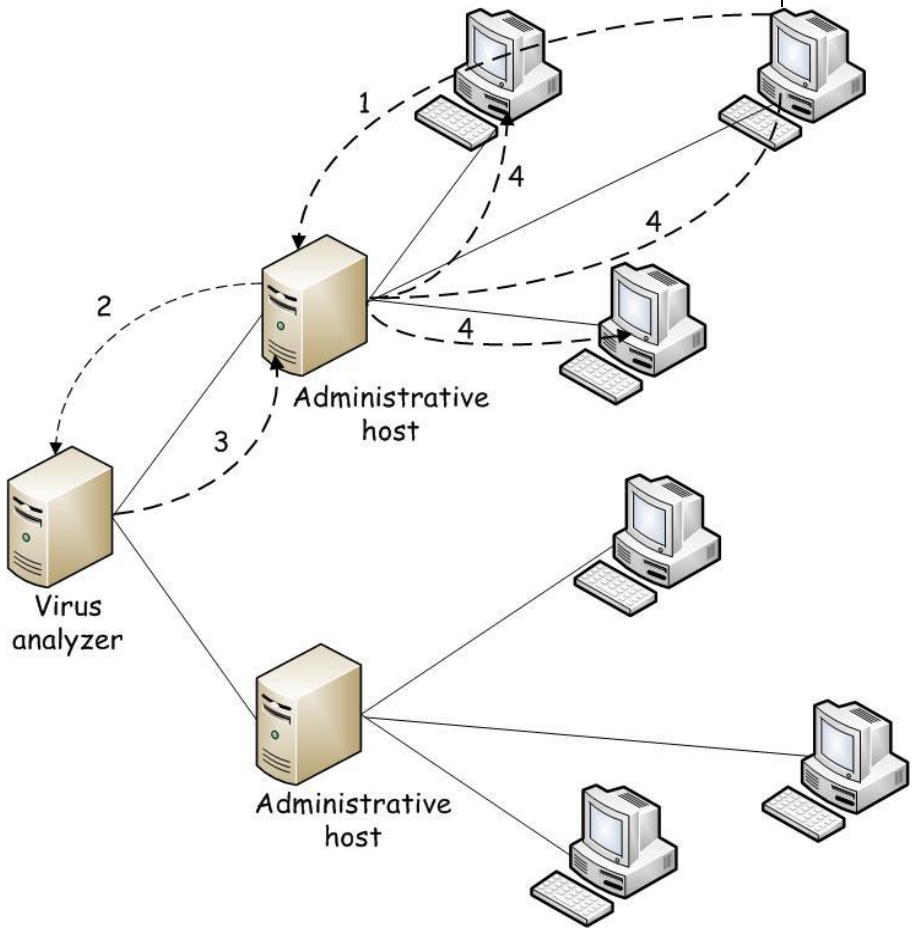
《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

一些常见的反病毒软件产品

- McAfee VirusScan
  - http://www.mcafee.com
- Norton AntiVirus
  - http://www.symantec.com
- Avast! AntiVirus
  - http://www.avast.com
- AVG
  - http://www.grisoft.com
- …

仿真杀毒

- 隔离硬件和软件来评估可以程序
  - 可能回来带来大量的计算负载
  - 有助于阻止恶意软件损害关键系统



《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

第8章 内容概要

- 8.1 病毒
- 8.2 蠕虫
- 8.3 病毒防御
- 8.4 特洛伊木马
- 8.5 网络骗局
- 8.6 点对点安全
- 8.7 Web安全
- 8.8 分布式拒绝服务攻击

特洛伊木马

- 一种看似有用的程序但包含一个恶意的负载 (也称为武士码)
  - 不能自动的自我复制
  - 需要引导用户去执行
- 可能造成如下危害:
  - 为DDoS攻击安装后门或僵尸软件
  - 安装间谍软件
  - 搜集用户的银行帐号和隐私信息
  - 给其它主机安装病毒或其它恶意代码
  - 修改或删除用户文件

第8章 内容概要

- 8.1 病毒
- 8.2 蠕虫
- 8.3 病毒防御
- 8.4 特洛伊木马
- 8.5 网络骗局
- 8.6 点对点安全
- 8.7 Web安全
- 8.8 分布式拒绝服务攻击

网络骗局

- 欺骗用户去做一些他们通常不会去做的事情
- 通常以电子邮件形式出现
- 例: “你中病毒了!”
- 针对网络骗局的对策是置之不理
  - 天下没有免费的午餐 !!

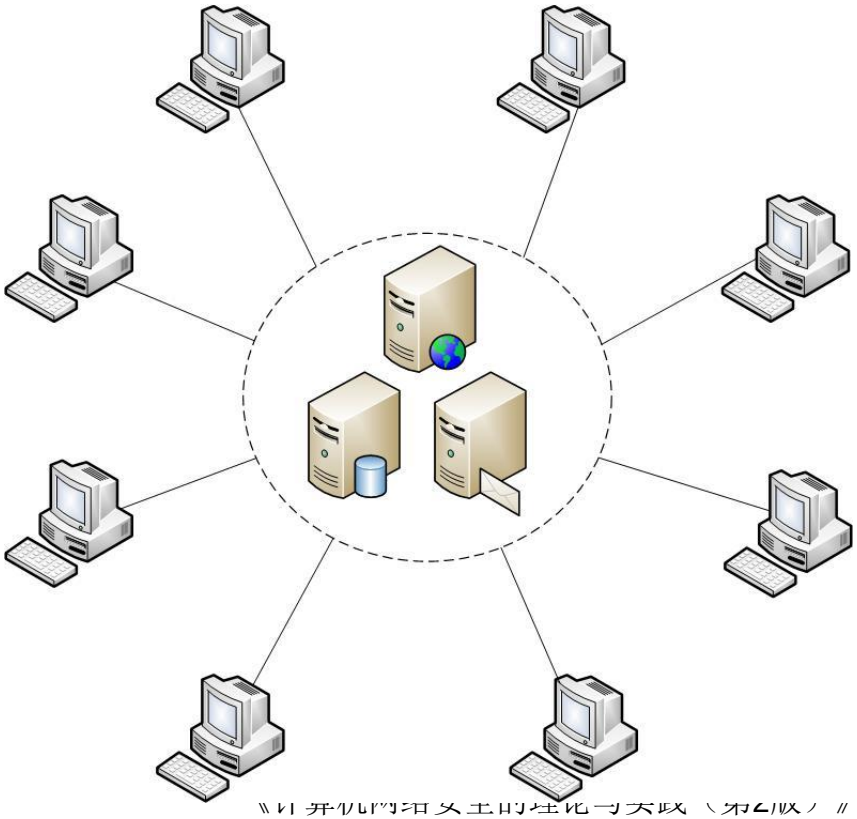
第8章 内容概要

- 8.1 病毒
- 8.2 蠕虫
- 8.3 病毒防御
- 8.4 特洛伊木马
- 8.5 网络骗局
- 8.6 点对点安全
- 8.7 Web安全
- 8.8 分布式拒绝服务攻击

点对点安全

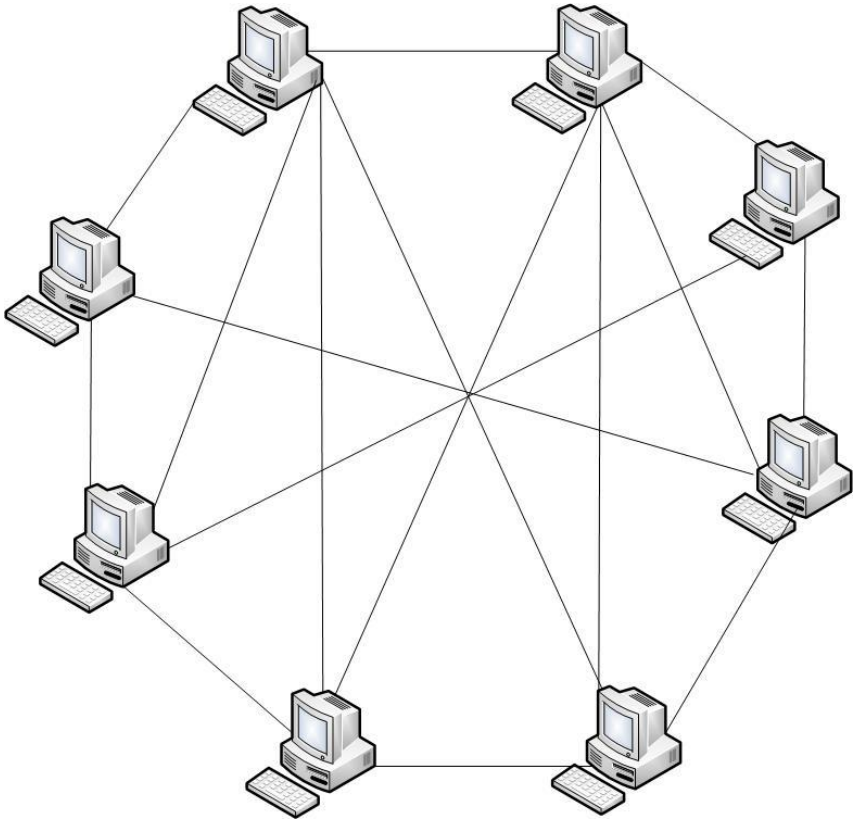
客户-服务器拓扑:

少数的服务器为大量客户提供服务



P2P 拓扑:

自组织网络, 每个计算机既扮演是客户端又是服务器



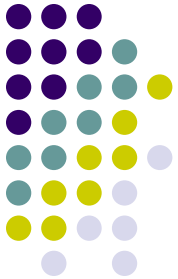
点对点安全

- 安全弱点:
  - 版权侵害
  - 消费太多的带宽和本地存储资源 → 拒绝服务攻击
  - 点对点应用程序打开一个特定的端口来与未知用户分享文件，该用户可能会为特洛伊木马，病毒，恶意软件打开一个后门
- 安全度量:
  - 仅安装官方点对点软件
  - 在打开下载的软件之前先进行扫描
  - 在公司内部不允许点对点软件运行

第8章 内容概要

- 8.1 病毒
- 8.2 蠕虫
- 8.3 病毒防御
- 8.4 特洛伊木马
- 8.5 网络骗局
- 8.6 点对点安全
- 8.7 Web安全
- 8.8 分布式拒绝服务攻击

Web安全



Web文档的基本类型:

- 静态文档:
  - 一个没有可执行代码的Web文档
  - 下载是安全的
- 动态文档:
  - 包含可执行代码的Web文档
  - 在服务器上执行CGI
  - 下载执行结果给客户端
- 主动文档:
  - 也包含可执行代码，但运行在客户端主机
  - 下载完整的代码运行

Web文档的安全

- 服务端:
  - 可能会因为动态文档和Web服务程序存在漏洞而受到攻击
  - 安全测量:
    - 升级到最新的Web服务程序
    - 严格管理CGI程序
    - 仅特定的人可提交CGI申请到Web服务器
- 客户端:
  - 可能会因为活动文档和Web浏览器程序存在漏洞而受到攻击
  - 安全测量:
    - 安装浏览器补丁
    - 禁用浏览器的JavaScript
    - 禁用浏览器的Java applets

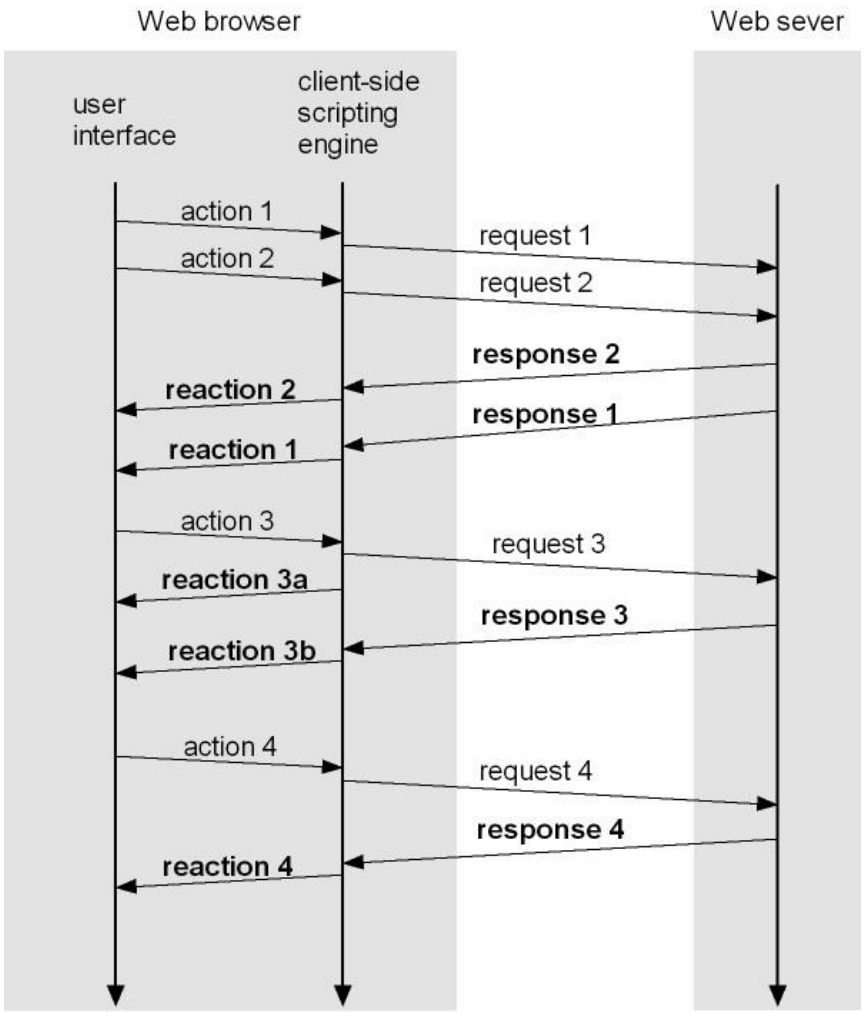
Cookies

- Web浏览器是无状态的
  - 每个URL请求，服务器都会建立一个新的连接
  - 对于并发的页面，需要建立不同的不相关的TCP连接
- Cookie存储用户的信息且传给用户的浏览器
- 浏览器为访问并发的页面沿着用户的请求发送cookie
- 服务器: 必须确保cookies不被恶意使用
- 客户机: 定期清除缓存的cookies

间谍软件

- 恶意软件未经用户许可的情况下，以一个插件模块安装在Web浏览器上
- 间谍软件可能会
  - 手机用户的信息并发送给攻击者
  - 监控用户的Web访问情况并弹出广告
  - 修改浏览器的缺省配置并且重定向到特定的网页
- 对策:
  - 配置防火墙来阻止攻击者植入间谍软件
  - 及时安装软件补丁
  - 安装反间谍软件程序

AJAX 安全



- 异步JavaScript 和XML (AJAX)
- AJAX实现异步交互使得用户的网页的访问更平滑
- 例: Google Maps
- 与传统的Web应用一样面临着相同的安全问题
- 跨站脚本攻击
- Silent calls和cookies

《计算机网络安全的理论与实践（第2版）》. 【美】王杰，高等教育出版社，2011年.

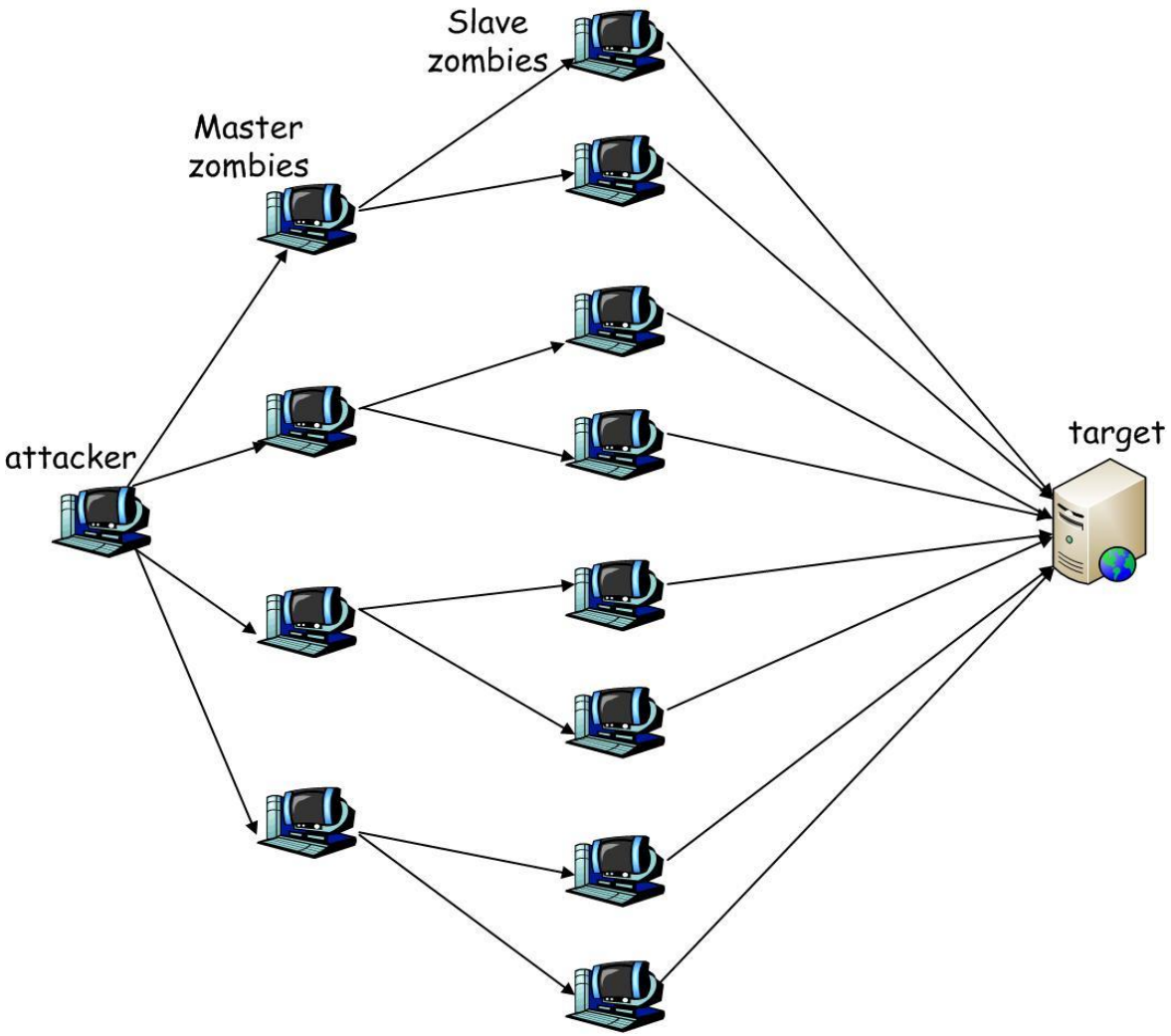
安全上网

- 只从可信的Web站点下载软件
- 不要点击弹出窗口的任何按钮
- 在安装和运行软件志强，阅读隐私说明，授权说明和安全警告，找出可能存在的风险
- 不要从受密码保护的站点内访问其他不同地址的站点
- 不要访问可疑的Web站点

第8章 内容概要

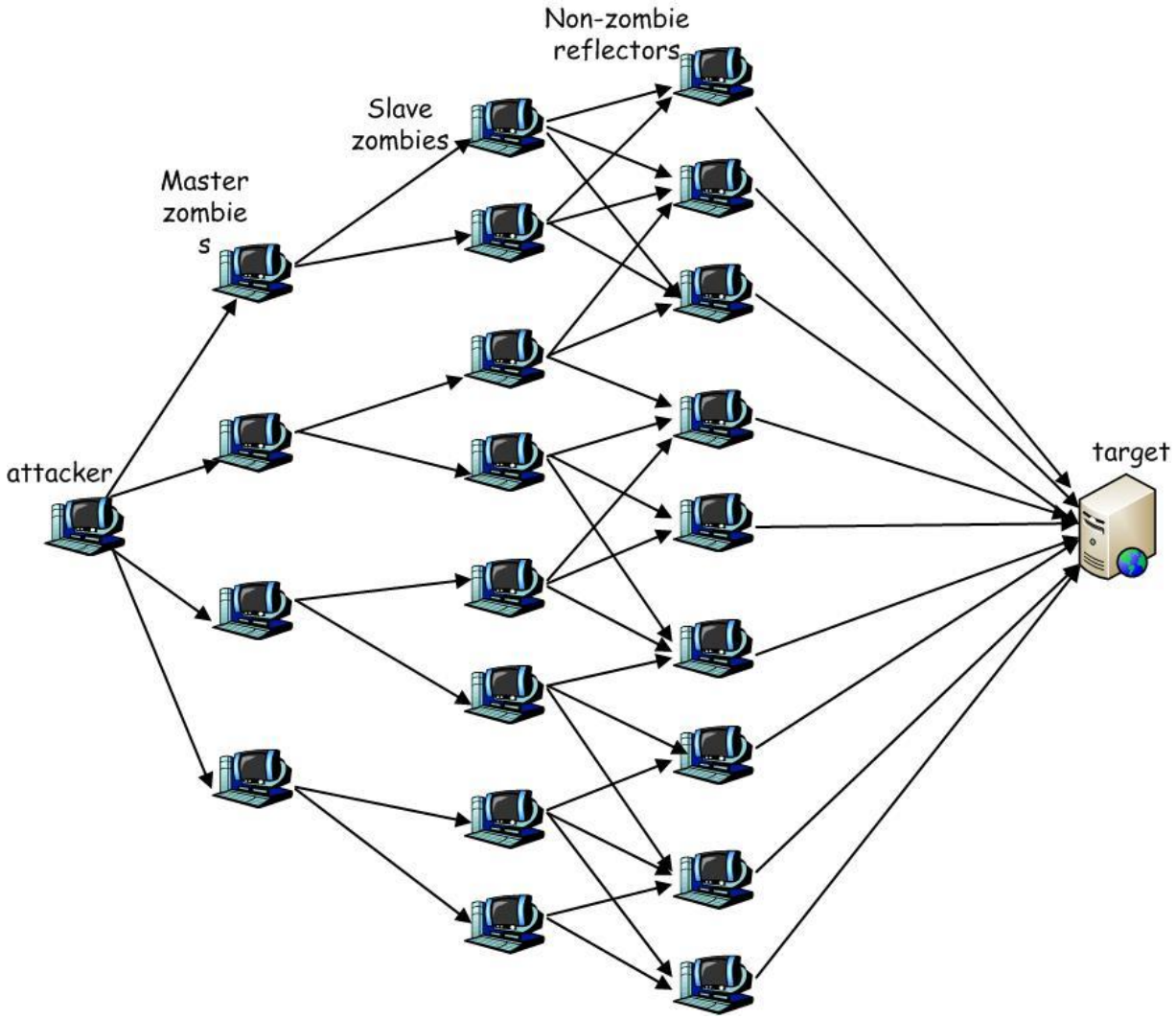
- 8.1 病毒
- 8.2 蠕虫
- 8.3 病毒防御
- 8.4 特洛伊木马
- 8.5 网络骗局
- 8.6 点对点安全
- 8.7 Web安全
- 8.8 分布式拒绝服务攻击

主-从式DDoS攻击



《计算机网络安全的理论与实践（第2版）》. 【美】王杰，高等教育出版社，2011年.

主-从-反射式DDoS攻击



《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

DDoS攻击的对策

- 减少有弱点主机的数量
  - 改进联网计算机的安全管理
  - 假设备份系统
  - 合理的分配资源
  - 构造一个DDoS 监控和响应系统
  - 保留完整的系统日志便于追踪资源
- 让攻击者们难于发现有漏洞的计算机
  - 关闭所有不必要的端口来对抗IP扫描
  - 当用户的计算机不在使用时，断开网络连接
  - 检测和移除僵尸软件

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.