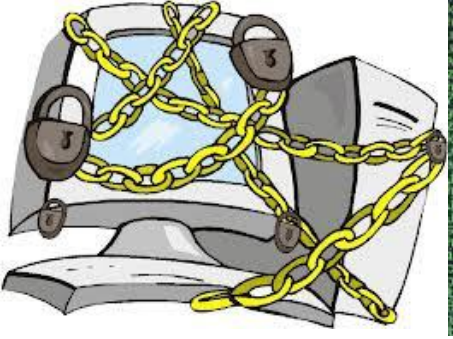



信息系统安全

概念与内涵

陈春华 博士
chunhuachen@scut.edu.cn

2018 春季
华南理工大学 软件学院

大纲

- 信息系统的威胁
  - 风险=脆弱性+威胁
- 信息系统安全的概念
  - 通信安全角度
  - 信息防御角度
  - 信息保障角度
- 信息系统安全体系
  - 安全服务、安全机制、安全策略与安全管理

系统的脆弱性

- 信息系统
  - 一种开发信息资源的工具，是信息以及用于信息的采集、传输、存储、管理、检索和利用等工具的有机整体。
- 脆弱性指从自身分析系统被威胁而出现异常的各种根源和因素
- 脆弱性导致系统呈现一些薄弱环节和漏洞
- 任何威胁都是因为系统本身具有薄弱环节和漏洞才形成或者出现的

系统的脆弱性

- 脆弱性的根源：
  - 基于信息属性的本源性脆弱
    - 信息的易复制性和易伪性等
  - 基于系统结构复杂性的结构性脆弱
    - 系统功能庞大，结构复杂；安全~系统最薄弱环节
  - 基于攻防不对称性的普通性脆弱
    - 比如，攻击薄弱的~全线防御
  - 基于网络的开放和数据库共享的应用脆弱性
- 是否存在绝对安全的系统？

系统的脆弱性

- 脆弱性的主要方面
  - 芯片的脆弱性
  - 操作系统安全漏洞
  - 数据库的安全脆弱性
  - 计算机网络的安全脆弱性
    - 网络协议
    - 网络应用

安全威胁与攻击

- 安全威胁
  - 指对于信息系统的组成要素及其功能造成某种损害的潜在可能。
  - 比如，对信息（比如用户密码）**机密性**的威胁
- 攻击可看作一种安全威胁的具体实现
  - 比如，窃听网络中传输的用户密码，造成其机密性的损失

安全威胁的分类

- 按照威胁的来源
  - 内部和外部威胁，或者进一步细分为：
  1. 自然灾害威胁
     - 不以人的意志为转移
  2. 滥用性威胁
     - 内部人员操作不当
  3. 有意人为威胁
     - 敌意性攻击
- 按照作用对象：针对信息、针对系统

攻击的主要形式

- 恶意代码攻击，包括病毒、特洛伊木马、蠕虫、陷门和逻辑炸弹等
- 窃听攻击，包括声波窃听、电磁波窃听、光缆窃听、手机窃听和网络窃听等
- 黑客攻击，信息系统敏感数据获取、网络欺骗漏洞攻击、数据驱动漏洞攻击、拒绝服务攻击攻击和陷门攻击等

恶意代码

- 恶意代码是在未授权的情况下，以破坏软硬件设备、窃取用户信息、扰乱用户心理、干扰用户正常使用为目的而编制的软件或者代码片段。
- 重要特征：
  - 目的性
  - 传播性
  - 破坏性
- 主要类型：
  - 病毒
  - 木马
  - 蠕虫
  - 或者复合型

病毒

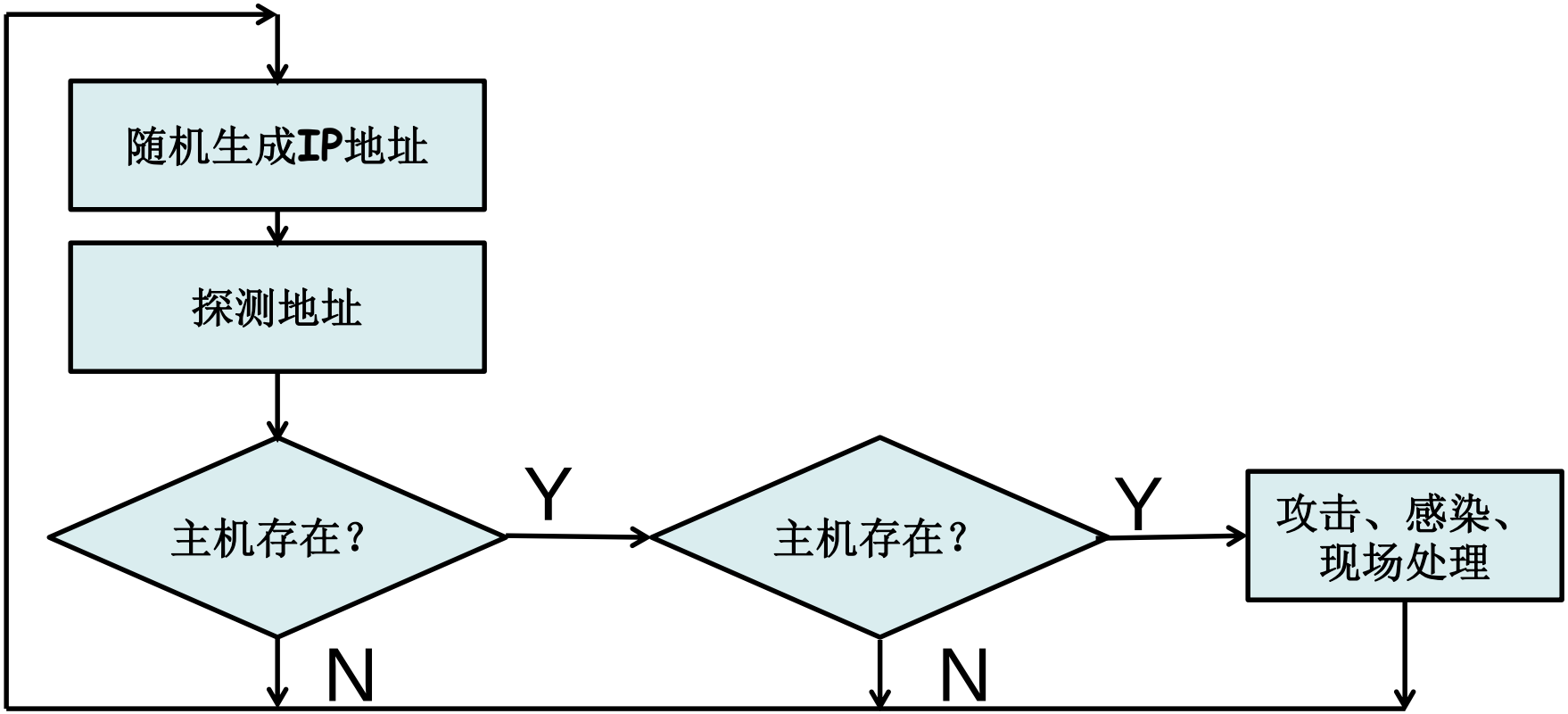
- 病毒：能够引起计算机故障，破坏计算机数据的程序代码。
- 病毒的特征：
  - 传染性，从一个程序、部件或系统传播到另外的一个程序、部件或者系统，不如通过U盘共享数据等方式。
  - 潜伏性和隐藏性，通常比较小，并等待时机再进行破坏
  - 寄生性，寄生在磁盘引导区或者可执行文件（如exe文件等）

病毒

- 病毒的特征：
  - 非授权性执行
  - 可触发性，包括日期或者时间触发等
  - 破坏性，包括占用或消耗CPU资源，攻击系统数据区或者文件系统（主流）等等
- 病毒的分类
  - 按攻击的操作系统、按寄生的位置、按是驻留内存等进行划分

病毒与蠕虫

- 蠕虫的传播过程



案例1 Morris 蠕虫病毒

- 作者：Robert Morris
- 1988，通过互联网传播的第一种蠕虫病毒
  - 起因并不是想造成破坏，而是想测量互联网的规模？
  - 莫里斯蠕虫利用了Unix系统中send mail、Finger、rsh/rexec等程序的已知漏洞（**缓存区溢出**）以及薄弱的密码
  - 康奈尔大学的学生，在MIT释放程序
  - “有人估计约有60,000台计算机连上了互联网，而蠕虫大概感染了其中的1/10。”

病毒与蠕虫

- 蠕虫与病毒都是具有恶意的程序代码

比较项目	蠕虫	病毒
存在形式	独立存在	寄生在宿主程序中
运行机制	自主运行	条件触发
攻击对象	计算机、网络、进程	文件
繁殖方式	自我复制	感染宿主程序
传播途径	系统漏洞	文件感染

特洛伊木马

- 木马是一种恶意程序，通常在提供一些有用或者令人感兴趣的功能情况下，还具有用户不知道的恶意性功能，比如窃取密码等。
- 重要特征
  - 目的性与功能特殊性，具有特定的目标
  - 非授权性与受控性，接受远程指令控制
  - 非自我繁殖性、非自传播性和预入性
  - 欺骗性

病毒、蠕虫与木马

比较项目	木马	病毒	蠕虫
自我繁殖	几乎没有	强	强
攻击对象	网络	文件	计算机、网络、进程
传播途径	植入	文件感染	漏洞
欺骗性	强	一般	一般
攻击方式	窃取信息	破坏数据	消耗资源
远程控制	可	否	否
存在形式	隐藏	寄生在宿主程序中	独立存在
运行规则	自主运行	条件触发	自主运行

案例2 10086积分陷阱木马

- 2014年，新型电信诈骗案件。
  - 攻击者将积分兑奖短信通过“伪基站”伪装成10086群发诈骗短信；并建立虚假积分兑换网站，附带在短信中，以此来诱惑用户下载安装一款伪装成木马的APP。
  - 受骗用户为兑奖，在虚假网站中输入银行卡账号等信息后，账号被冒用进行大额消费或转账。与此同时，安装在用户手机上的虚假客户端能够拦截并转发用户手机收到的支付验证信息。

通信窃听

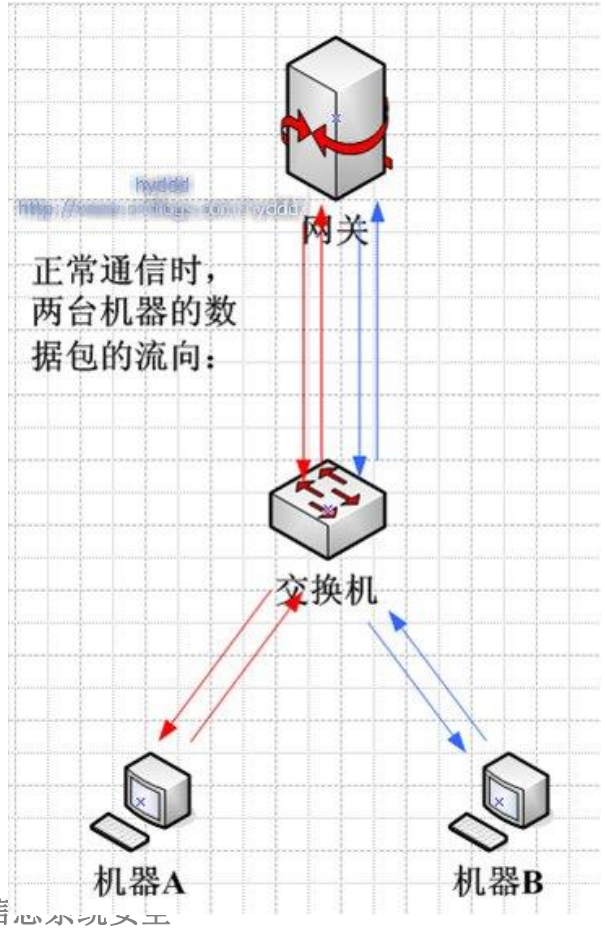
- 窃听指使用专用技术设备直接秘密窃取侦查目标的语音、图像等信息。
  - 美国“棱镜门”，爱德华．斯诺登
- 声波监听
  - 通过隐藏精巧的窃听器；激光窃听器（！！）
- 电磁波窃听
- 光缆窃取
- 手机窃听、共享网络的窃听等等

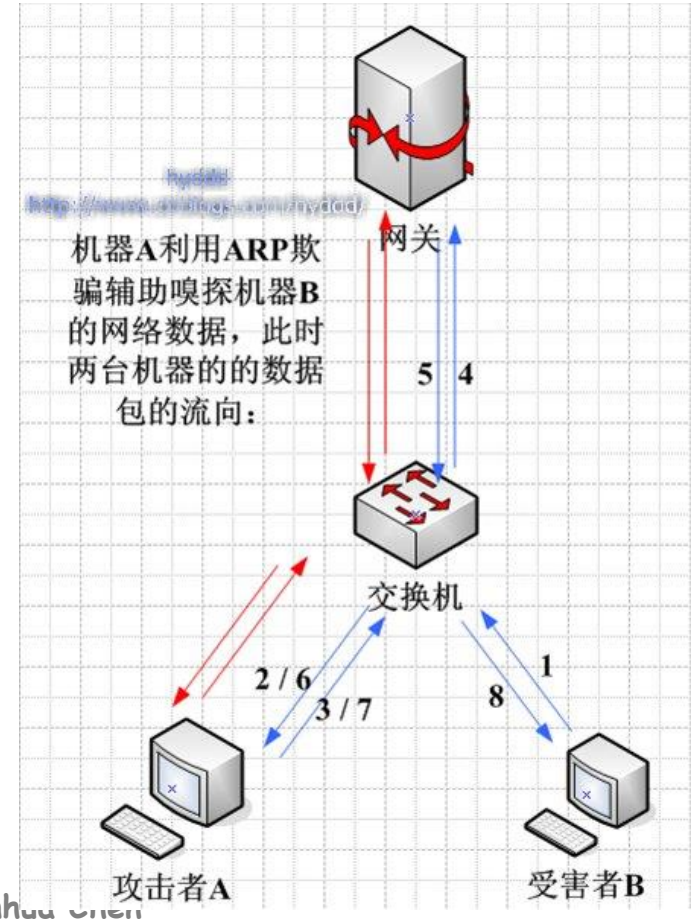
网络欺骗漏洞攻击

- ARP欺骗-交换网络监听
- IP源地址欺骗
- TCP会话劫持
- DNS欺骗
- Web欺骗和钓鱼网站

案例3 ARP欺骗-交换网络监听

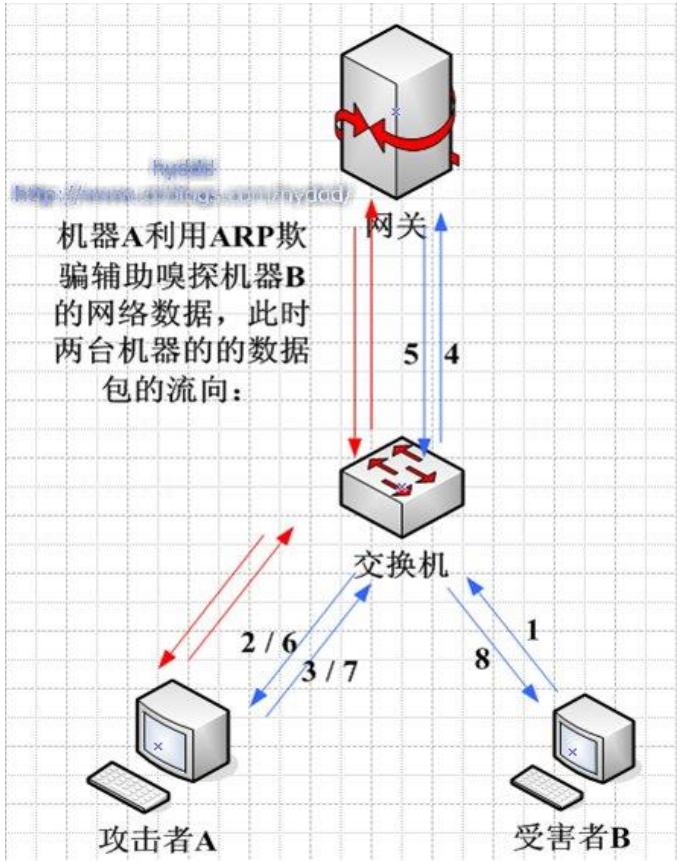
- 针对以太网地址解析协议（ARP）的一种攻击技术





案例3 ARP欺骗-交换网络监听

- 利用该方案，可以获取同网段中用户提交的密码（？！）



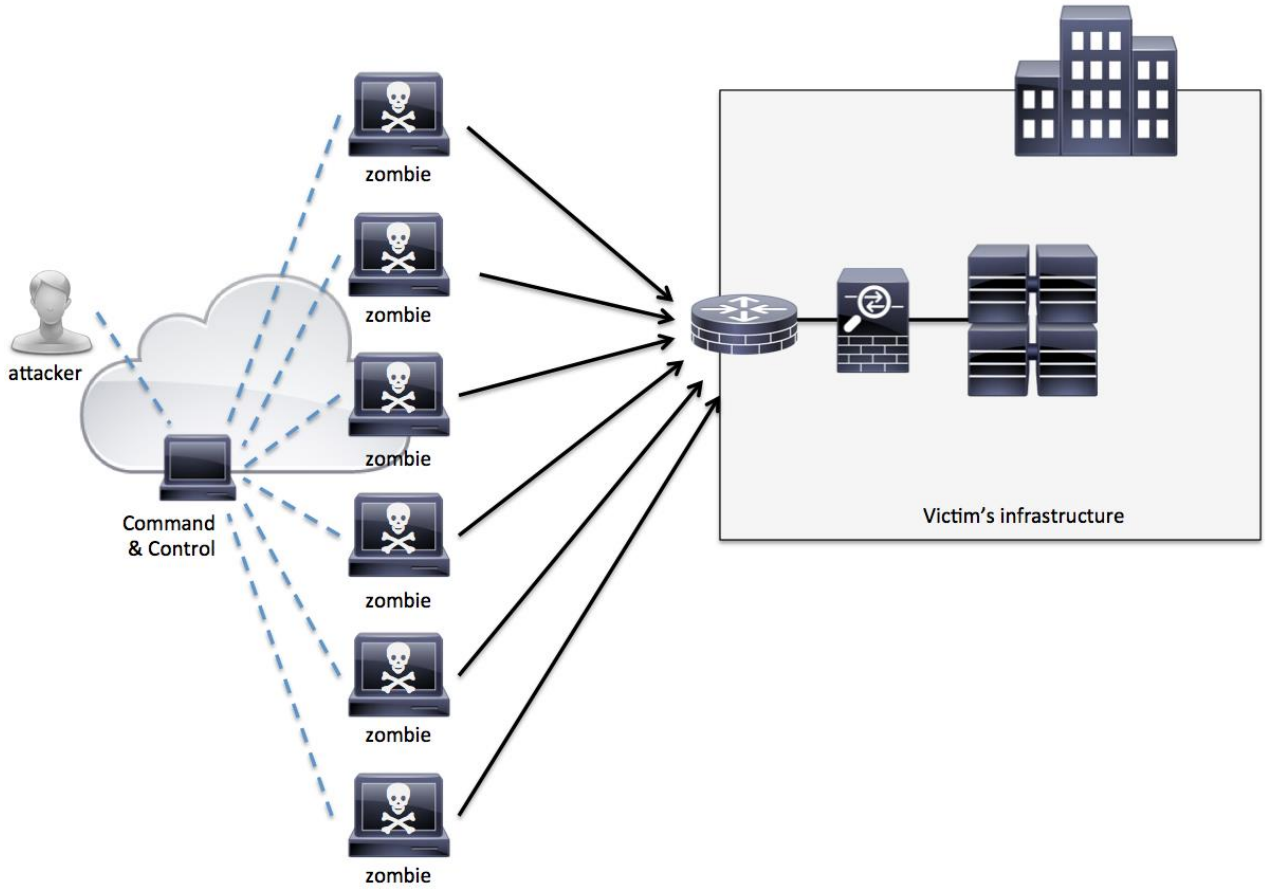
拒绝服务攻击

- 该类攻击造成目标系统遭受某种程度的破坏而不能继续提供正常的服务，甚至导致物理上的瘫痪或奔溃。
- 典型攻击：
  - IP碎片与IP碎片漏洞
  - 死亡之ping攻击
  - UDP泛洪攻击
  - **SYN泛洪攻击**
  - MAC泛洪攻击

案例4 SYN “洪水”

- 利用TCP建立连接(三次握手协议)的缺陷，是当前最流行的拒绝服务攻击方式之一。
- 攻击者发送TCP SYN，SYN是TCP三次握手中的第一个数据包，而当服务器返回ACK后，该攻击者就不对其进行再确认，那这个TCP连接就处于挂起状态，也就是所谓的半连接状态，服务器收不到再确认的话，还会重复发送ACK给攻击者。

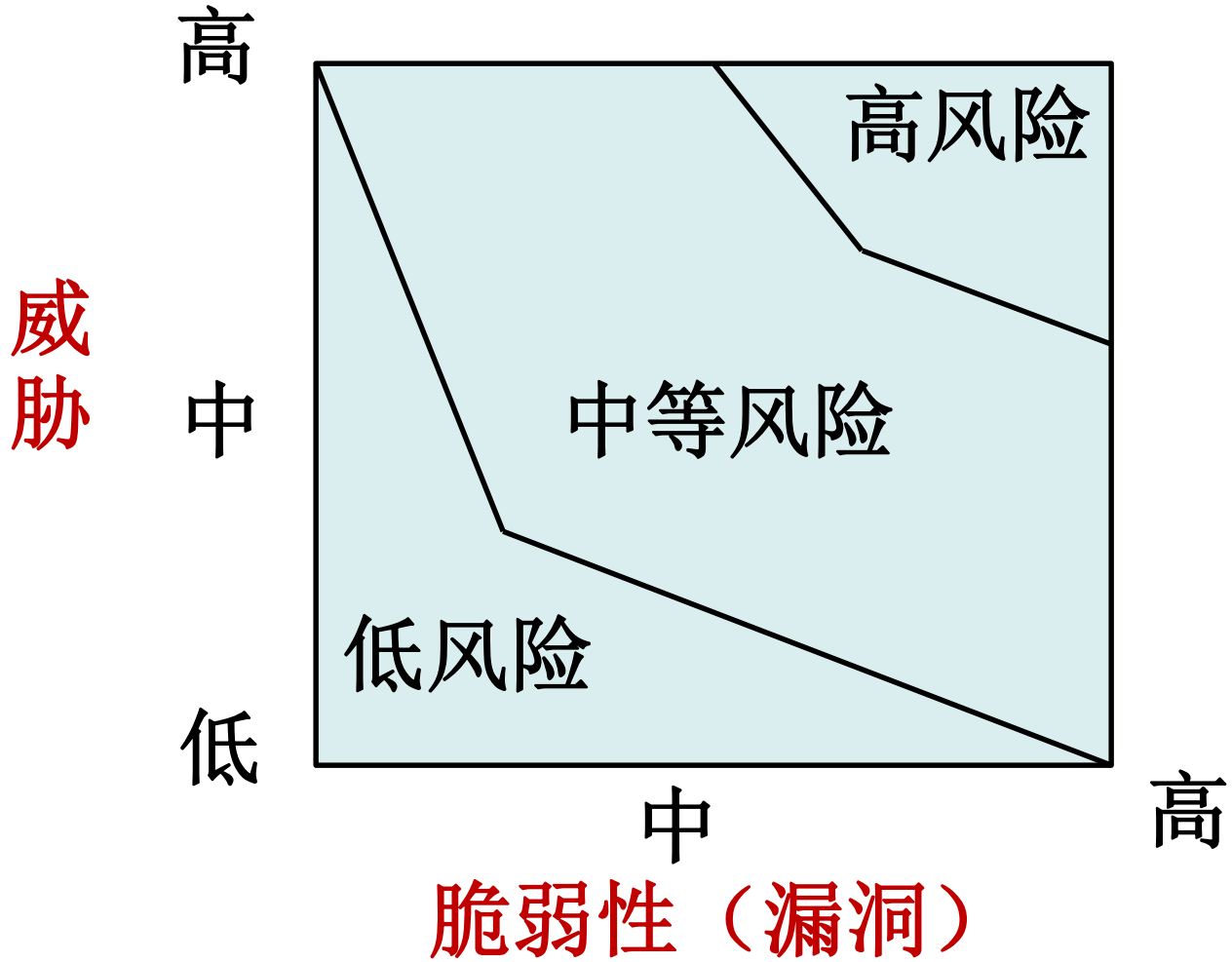
DDOS与僵尸网络


zombie
zombie
zombie
zombie
zombie
zombie
attacker
Command
& Control
Victim's infrastructure

Waledac僵尸网络

- 感染全球各地数十万台PC，据信每天能发出逾15亿封的垃圾邮件

风险=脆弱性+威胁



风险损失

- 信息资源损失
  - 机密性 (Confidentiality, C)
  - 完整性 (Integrity, I)
  - 可用性 (Availability, A)
  - 真实性 (Authenticity)
- 可归结为三大类
  - 信息破坏
  - 信息泄密
  - 假冒或否认

风险损失

- 系统损失
  - 系统被非法访问
  - 造成系统资源（网络以及主机等）运行不正常或瘫痪，丧失可用性

信息系统安全概念与内涵

- 信息系统安全
  - 信息安全，强度内容安全，包括知识产权与数据两个方面的安全
  - 网络安全，强调保护信息网络基础设施等
- 三个层次
  - 通信保密 （communication security）
  - 信息防护（information protection）
  - 信息保障（information assurance）

基于通信保密的信息系统安全概念

- 信息系统安全的基本概念和内涵是**信息保密**，采用的基本技术是**加密**，或者称为密码技术
- 计算机未出现前，密码技术就广泛使用在战争情报中
  - 通信手段：无线电报等
  - 如二战时期德国的Enigma机械密码机
  - 破解该密码机使用了Alan Turing设计并建造的计算机！

基于通信保密的信息系统安全概念

- 早期密码技术
  - 替代密码术
  - 换位密码术
- 1949年，信息论之父C. E. Shannon (香农)发表《保密系统的通信理论》，标志着密码学开始科学与理性的轨道
  - 密码与编码学

Dr. Chunhua Chen
chunhuachen@scut.edu.cn

基于通信保密的信息系统安全概念

- 计算机时代的信息保密
  - 通信方式：计算机网络通信 (1969，ARPANet)
  - 1976，W. Diffie和M. E. Hellman发表《密码学的新方向》以及1977年美国公布《数据加密标准(DES)》
    - 密码学出现：对称密钥体系和非对称密钥体系
  - 量子计算技术的深入进展，旧的密码算法受到安全方面的威胁，量子密码得到发展

基于信息系统防护的信息系统安全概念

- 在防护的概念下，信息系统安全的内涵，从机密性的基础上，扩充为完整性、可用性、真实性和可控性。
- 信息系统防护，是一种被动的防御思想，具体目标：
  - 系统保护
  - 信息内容保护
- 防护的概念，经历了计算机安全和计算机网络安全两个阶段

基于信息系统防护的信息系统安全概念

- 计算安全阶段
  - 计算机本身的安全问题，其软硬件所遭受的威胁不仅有滥用、自然灾害，还有病毒
  - 数据库系统中，数据的完整性保护问题
  - 标志事件：1970，美国发布的“可信计算机系统评价准则”，又称橘皮书
    - 计算机系统安全包括4个方面：安全政策、可说明性、安全保障和文档
    - 7个等级（D、C1、C2、B1、B2、B3、A1）

基于信息系统防护的信息系统安全概念

- 计算机网络安全阶段
  - “网络就是计算机”，信息系统的内涵函括了计算机网络~
  - 计算机网络的威胁程度，远远超过单机时代！
  - 保护计算机网络安全，就可以解决信息系统的主要安全问题！
  - 标志事件：2001年，美国发布的“信息时代的关键基础设施保护”和2002年的“网络安全国家战略”

基于信息保障的信息系统安全概念

- 1995年，美国国防部在《信息保障技术框架》(IATF)中提出PDR模型中体现了信息保障的概念，之后不断深化与发展了保障的内涵。
- PDR：Protection-Detection-Response
  - 防护-检测-响应
- 检测是一种主动防御的思想
- 在保障的概念下，信息系统安全的内涵又增加了可验证性和不可否认性等安全属性

PDR模型中信息保障的内涵

- 从被动防御到主动防御
  - 网络时代，被动防御效果一般，安全事件快速增长
  - 理想的系统安全需要一种检测机制，以便动态地发现危机
  - 发现问题后，需要响应机制来及时处理和恢复，加强防护
  - 强调系统在遭受攻击情况下，仍能稳定运行

PDR模型中信息保障的内涵

- 从静态防御到动态防御
  - 信息系统在需求、建设、安全漏洞、网络拓扑和网络威胁等多个方面呈现动态性
  - 动态的防御强度利用检测工具，随时了解和评价系统的安全状态，发现新的威胁和弱点，并作出及时响应和加固，以使得系统处于“风险最低”状态。

PDR模型中信息保障的内涵

- 技术与管理从分离到融合
  - 信息安全保障单靠技术难以实现，要依赖人、技术和管理三者共同完成，管理作用是非常突出的。
  - PPDR模型中增加了**安全策略**的概念，强度要充分考虑人的管理因素。
  - 安全策略是根据风险分析产生的描述系统中哪些资源要得到保护，以及如何实现对它们的保护等内容，是安全保障的核心！

信息系统安全体系

- 信息系统安全体系的形成是通过对于系统的风险分析提出安全需求，制定出安全策略，再根据安全策略，决定系统的安全功能-安全服务，并通过相应的安全机制来实现需要的安全服务。
- 包括两大部分内容：
  - 安全服务，即安全机制所提供对付安全威胁的功能及其配备位置。
  - 安全机制，是安全服务的具体实现。

信息系统安全体系标准

- 任何信息系统的安全体系都要结合系统的实际建立
- 标准可以提供一个指导原则和约束条件
- 《信息处理系统 开放系统互连 基本参考模型 第2部分：安全体系结构》
  - GB/T 9387.2 1995
  - 相当于：ISO/IEC 7498-2

ISO/IEC 7498-2

- 提出了一个建立在OSI参考模型7层协议之上的信息安全体系结构标准，并定义了5类安全服务，8种特定安全机制，5种普通安全机制，确定了安全服务与安全机制的关系，并确定了安全管理。

7 应用层
6 表现层
5 会话层
4 传输层
3 网络层
2 链路层
1 物理层

OSI安全体系的安全服务

- 鉴别服务
  - 通过对于通信的对等实体（主体）和数据源的鉴别和确认来对抗假冒性攻击以及重放性攻击
  - 网络层鉴别-主机地址鉴别
  - 传输层鉴别-进程地址鉴别
  - 应用层鉴别-人员账户鉴别

OSI安全体系的安全服务

- 访问控制服务
  - 防止系统资源的非授权访问
  - 通过建立访问实体（主体）与资源（客体）之间的访问关系（如读、写与运行等）形成授权机制，决定主体在什么条件下，为了什么目的才可以访问哪些客体。
  - 通常先用户鉴别，后对合法用户进行访问控制
  - 可配置在网络、传输和应用层

OSI安全体系的安全服务

- 机密性服务
  - 用于防止被动攻击（攻击者获取信息）
  - 防止数据的非授权泄露，包括
  - 数据机密性保护，是攻击中难以从数据项中推断出敏感信息
  - 业务流机密性保护，是攻击者不能通过观察通信业务流推断出其中的敏感信息

OSI安全体系的安全服务

- 完整性服务
  - 用于对抗主动攻击(攻击者修改数据)
  - 保护数据在存储、传输等过程中不被非授权修改（如插入，篡改，重排序或者延迟），以提供真实准确的数据

OSI安全体系的安全服务

- 抗抵赖服务
  - 提供证据来证实某通信实体的诚实性，包括
    - 有数据原发证明的抗抵赖：防止发送方抵赖
    - 有数据交付证明的抗抵赖：防止接收方抵赖

OSI安全体系中安全服务配置

OSI层次 安全服务	1	2	3	4	5	6	7
鉴别服务/访问控制服务	N	N	y	y	N	N	y
机密性服务(数据机密性|连接机密性)	y	y	y	y SSL/TLS	N	y	y
完整性服务(带恢复功能的连接完整性)	N	N	N	y	N	N	y
抗抵赖服务	N	N	N	y	N	N	y

OSI安全体系安全机制

- 基本安全机制
  - **加密机制**，为数据提供机密性保护，通常采用密码、信息隐藏等方法实现
  - **数据签名机制**，提供认证或者抗抵赖服务
  - **访问控制机制**，提供数据机密性、完整性和可用性等保护
  - **完整性机保护制**，具体技术有鉴别码(抗修改)，顺序号(防乱序)，时间标记(防重放，防丢失)等

OSI安全体系安全机制

- 基本安全机制
  - **通信业填充机制**，提供业务流机密性保护的反分析机制
  - **路由选择控制机制**，支持动态地或预定地选择路由，以便只使用物理上安全的子网络、中继站或链路进行通信
  - **公证机制**，有可信第三方提供的安全保护机制
  - **鉴别交互机制**，提供对等实体鉴别，采用的技术有鉴别信息（如口令）和密码技术

安全机制与安全服务之间的关系

安全机制 / 安全服务		加密	数字签名	访问控制	数据完整性	鉴别交换	通信业务填充	路由选择控制	公证
鉴别服务	对等实体	y	y	N	N	y	N	N	N
	数据源发	y	y	N	N	N	N	N	N
访问控制服务		y	N	y	N	N	N	N	N
机密性服务(连接/无连接的机密性)		y	N	N	N	N	N	y	N
完整性服务(连接完整性)		y	N	N	y	N	N	N	N

OSI安全体系安全机制

- 普通安全机制
  - **安全标记机制**，可为某资源指定安全属性约束
  - **事件监测机制**，对与安全有关事件的监测
  - **安全审计跟踪机制**，记录并调查安全事件
  - **安全恢复机制**，安全事件处理后进行系统恢复
  - **可信功能机制**，提供对某些硬件和软件可信赖的保证，如可信计算安全模块等

信息安全管理

- IATF提倡一种“纵深防御策略”，依赖“人、技术和运作管理”协调完成，即一个由组织、技术和管理保障体系组成的系统
- 安全管理中，安全策略是核心，是整个信息系统安全的依据。
- 安全策略是在一个特定的环境(安全区域)里，为保证提供一定级别的安全保护所必须遵循的一系列条例和规则。

信息安全管理

- 安全策略的作用是建立一个具有指导性的安全技术和管理规范，是进行系统分析分析的基础上，对控制策略，安全模型，安全等级，评价标准等提出的一个基本框架性文件。
  - 对系统安全的定义、总体目标和保护范围
  - 安全管理的总体定以、具体权责要求等
  - 安全教育等其他内容等

信息安全管理

- 安全管理活动
  - 安全服务管理
  - 安全机制管理
  - 安全事件处理管理
  - 安全审计管理
  - 安全恢复管理
  - 安全行政管理
  - 系统安全管理

信息系统的安全标准

- 可分为3大类
  - 针对信息系统（包括产品）的安全评测准则
    - 1983，美国《可信计算机系统评估准则》，又称橘皮书
    - 2001，中国GB 17895-1999《计算机信息系统安全保护等级划分准则》
  - 针对使用信息系统的组织的安全管理标准
    - ISO/IEC 17799:2000《信息技术 信息安全管理实用准则》
    - 中国《计算机信息系统安全保护条例》
  - 针对不同安全产品的互操作性的互操作标准
    - 数据加密标准DES
    - 安全电子邮件标准SMIME

信息系统安全立法

- 1994《中华人民共和国计算机信息系统安全保护条例》
- 1997《计算机信息网络国际联网安全保护管理办法》
- 2000《计算机病毒防治管理办法》
- 2001《计算机软件保护条例》
- 2004《中华人民共和国电子签名法》
- 个人隐私保护方面等... ...

信息系统安全的防御原则

- 信息系统的安全是防御式安全，必须坚持预防为主，并可遵从如下已经取得共识的信息系统安全防御原则
  - 木桶原则，又称均衡防护原则
  - 成本效益原则
  - 可扩展性原则
  - 分权制衡原则
  - 最小特权原则
  - 失效保护原则
  - 公开揭露原则
  - 可评估原则

Further Reading: