电子科技大学
University of Electronic Science and Technology of China

信息安全导论

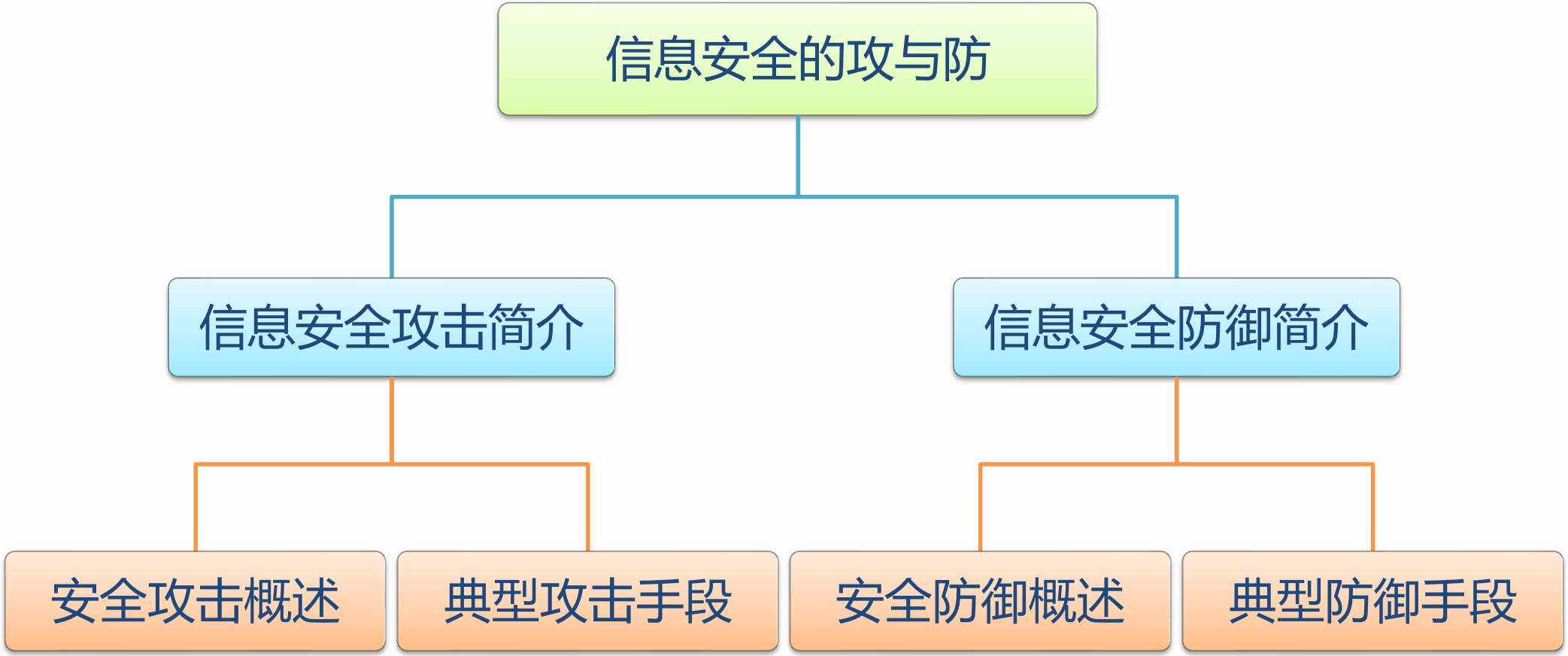
教学模块三：信息安全的攻与防

赵洋 副教授

电子科技大学 信息与软件工程学院

2022年10月8日

内容安排



引言

- 依据《2019年中国互联网网络安全态势报告》，2019年，CNCERT协调处置网络安全事件约10.6万起，其中网页仿冒事件最多，其次是安全漏洞、恶意程序、网页篡改、网站后门、DDoS攻击等事件。

- 勒索病毒、APT攻击、DDoS、网络诈骗成为主流的攻击手段；
- 云服务、工业控制系统、移动应用成为重点攻击对象；
- 数据安全成为最受关注的焦点。

引言

- 网络安全攻防能力对国家的战略安全有着重要的意义
  - 中美黑客大战
    - 2001年4月1日，美国一架侦察机在中国南海上空活动，中国派出两架军用飞机机对其进行监视。不料美机突然转向，向中方飞机直冲过来，导致其机头和左翼与中方一架飞机相撞坠。5月1日，中美黑客之间的“红黑大战”如期打响。中国红客们在攻陷的美国网站主页上留下了“伟大的中华民族万岁”、“美国必须对撞机事件负完全责任”、“抗议美国向台湾出售武器，破坏世界和平”等口号。
    - 截至2001年5月7日，虽然被攻陷的美国网站达到1600多个，包括900多个政府和军方网站。但被美国黑客攻陷的中国网站也高达1100多个，主要网站600多个。

网络安全的本质在对抗

对抗的本质在攻防两端能力较量

第一部分 信息安全攻击简介

重点掌握信息安全攻击的基本概念，了解典型安全攻击的原理和特点

一、信息安全攻击简介

1、安全攻击概述

什么是安全攻击?

- 威胁信息资产安全的行为统称安全攻击。

第一阶段（1998年以前）安全攻击主要来源于传统的计算机病毒，其特征是通过媒介复制进行传染，以攻击破坏个人电脑为目的；

第二阶段（大致在1998年以后）安全攻击主要以蠕虫病毒和黑客攻击为主，其表现为蠕虫病毒通过网络大面积爆发及黑客攻击一些服务网站；

第三阶段（2005年以来）安全攻击手段变得多样化，多数以偷窃资料、控制利用主机等手段谋取经济、军事、政治利益为目的。

一、信息安全攻击简介

1、安全攻击概述

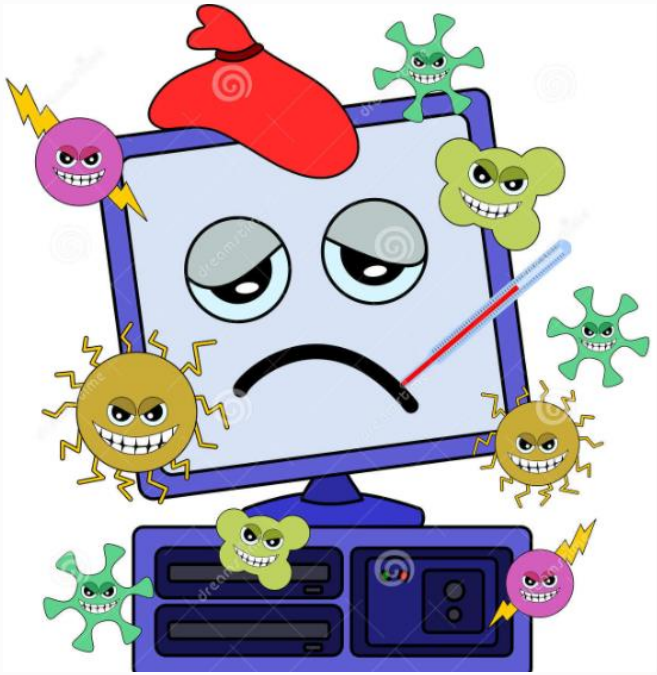
◘ 安全攻击分类

- 从攻击者角度
  - 主动型攻击：如网络监听和黑客攻击等，这些威胁都是对方人为通过网络通信连接进行的；
  - 被动型攻击：一般是用户通过某种途径访问了不当的信息而受到的攻击；
- 从攻击手段及破坏方式
  - 第一类是以传统病毒、蠕虫、木马等为代表的计算机病毒；
  - 第二类是以黑客攻击为代表的网络入侵；
  - 第三类以间谍软件、广告软件、网络钓鱼软件为代表的欺骗类威胁。

一、信息安全攻击简介

2、常见的安全攻击手段——计算机病毒

- 什么是计算机病毒?
  - 狭义的计算机病毒
    - 计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码
  - 广义的计算机病毒
    - 任何能够引起计算机故障，破坏计算机数据，影响计算机系统的正常使用的程序代码



一、信息安全攻击简介

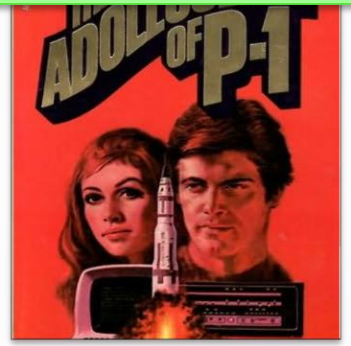
2、常见的安全攻击手段——计算机病毒

◘ 计算机病毒的起源

冯.诺伊曼

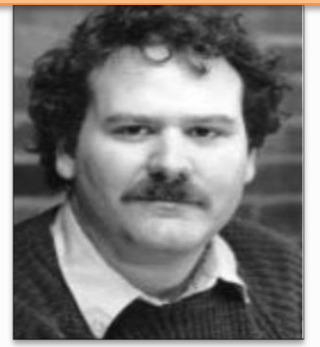
1949年在论文《复杂自动装置的理论及组织的进行》里，指出存在可以自我复制的程序。

托马斯·丁·雷恩



1977年在科幻小说《Adolescence of P-1》中，描写了一种可以在计算机中互相传染的病毒。

弗雷德·科恩



1983年，弗雷德·科恩在南加州大学写出了第一个可自我复制并具有感染能力的程序。

一、信息安全攻击简介

2、常见的安全攻击手段——计算机病毒

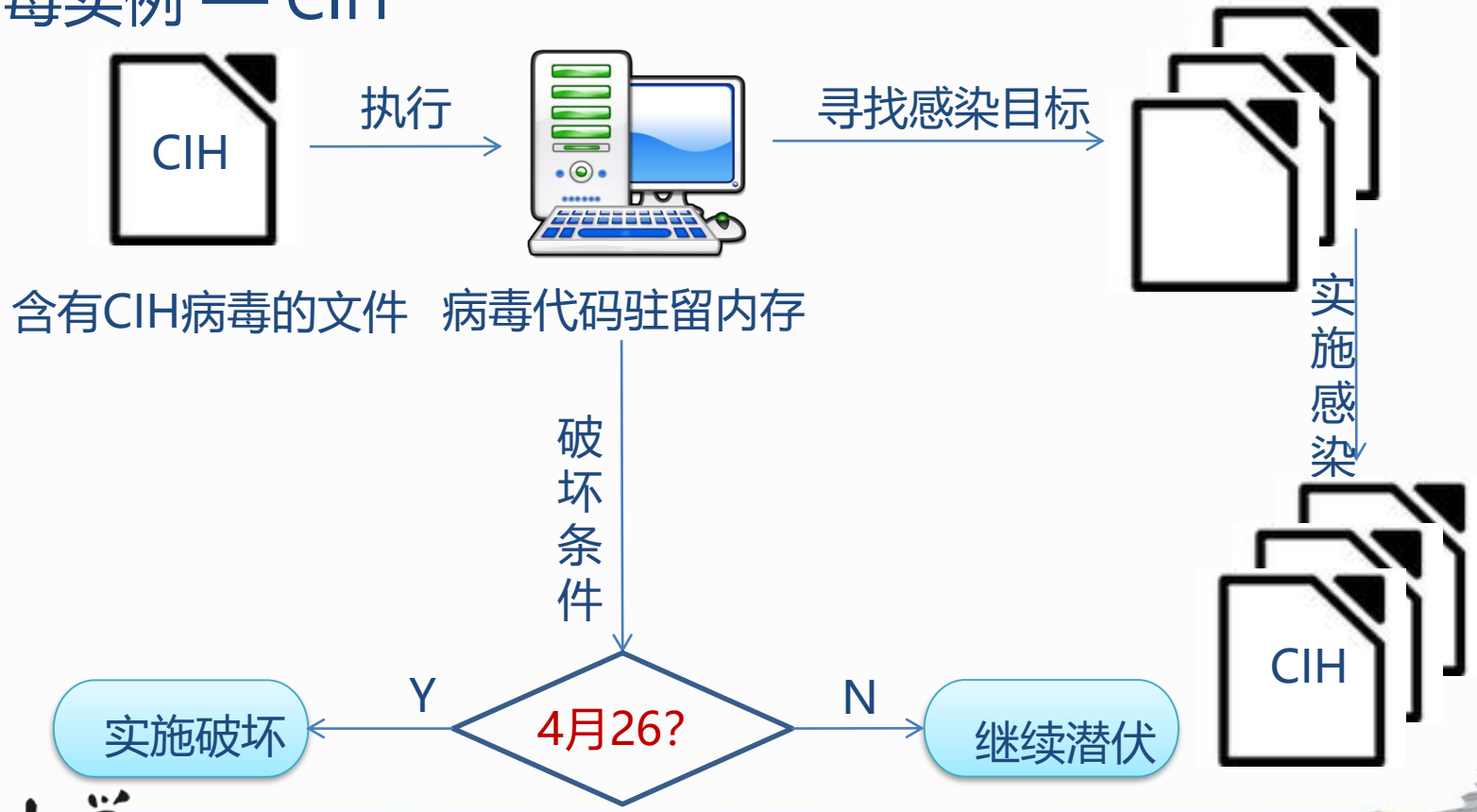
- 传统型病毒
  - 特点
    - 传统型病毒有一个「宿主」程序，所谓宿主程序就是指那些让计算机病毒藏身的地方。被感染病毒的文件通过移动存储、电子邮件等方式在主机间传播，并在被执行时，适机感染主机中的其他文件。传统型病毒通常具有寄生性、传染性、潜伏性、触发性和破坏性。

  - 工作原理
    - 宿主程序被执行时，病毒代码就会获得执行的机会。

一、信息安全攻击简介

2、常见的安全攻击手段——计算机病毒

- 传统型病毒实例 — CIH



一、信息安全攻击简介

2、常见的安全攻击手段——计算机病毒

- 蠕虫病毒
  - 特点
    - 蠕虫是一种可以自我复制的代码，一般不需要寄生在宿主文件中，主要通过网络传播，通常无需人为干预就能传播。蠕虫主要具有自传播性、隐蔽性和破坏性等特性。
  - 工作原理
    - 蠕虫病毒首先通过漏洞扫描发现网络中存在漏洞的主机、然后利用漏洞实施攻击，攻击成功后，将该蠕虫程序迁移至被控制主机，该主机会成为新增的传染源源头，同时在本机实施破坏行为。

一、信息安全攻击简介

2、常见的安全攻击手段——计算机病毒

- 蠕虫病毒实例 — WannaCry

① 传播：被感染主机自动扫描网络主机，判断445端口是否开放；

② 攻击：如果端口开放，利用SMB漏洞（永恒之蓝）发起攻击；

③ 传播：如果攻击成功，将病毒程序注入目标主机；

④ 破坏：执行病毒程序，遍历本地文件系统，依据文件类型和大小执行加密文件删除源文件等破坏操作；

⑤ 扩散：目标主机成为攻击主机之一，执行①~⑤。

一、信息安全攻击简介

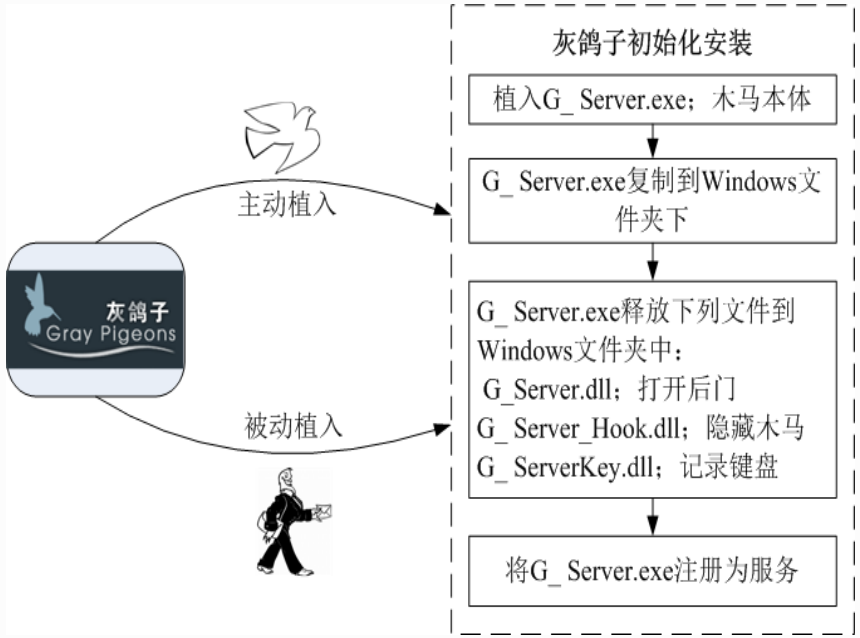
2、常见的安全攻击手段——计算机病毒

- 常见的计算机病毒—特洛伊木马
  - 特点
    - 一种特殊的后门程序，可以用来远程控制另一台主机，隐蔽性和非授权性是特洛伊木马的最显著特点。
  - 工作原理
    - 基于客户端和服务端的通信、监控程序。客户端的程序用于远程控制，可以发出控制命令，接收服务端传来的信息。服务端程序运行在被控计算机上，一般隐藏在被控计算机中，可以接收客户端发来的命令并执行，将客户端需要的信息发回。

一、信息安全攻击简介

2、常见的安全攻击手段——计算机病毒

- 特洛伊木马实例 — 灰鸽子



一、信息安全攻击简介

2、常见的安全攻击手段——计算机病毒

- 防范计算机病毒
  - 加强安全防御
    - 安装防毒软件；
    - 使用基于客户端的防火墙，关闭445，139，3389等端口；
    - 打开你的防毒软件的自动升级服务，定期扫描计算机；
    - 备份重要数据。
  - 提高安全意识
    - 在使用光盘、U盘或活动硬盘前，做病毒扫描；
    - 关注下载安全，下载要从比较可靠的站点进行，下载后做病毒扫描；
    - 关注电子邮件安全，来历不明的邮件决不要打开，决不要轻易运行附件；
    - 警惕欺骗性的病毒。

一、信息安全攻击简介

- 测试点3-1
  - 假设你在网站上观看视频时，你看到一个弹出窗口要求你安装定制的解码器，才能正常观看视频。如果同意安装，你的计算机有可能会面临什么威胁？
  - 以表格方式对比传统型病毒、蠕虫和木马的特点，指出各自专属的特征。

	主要特征	破坏行为	专属特征
传统型病毒			
蠕虫			
木马			

一、信息安全攻击简介

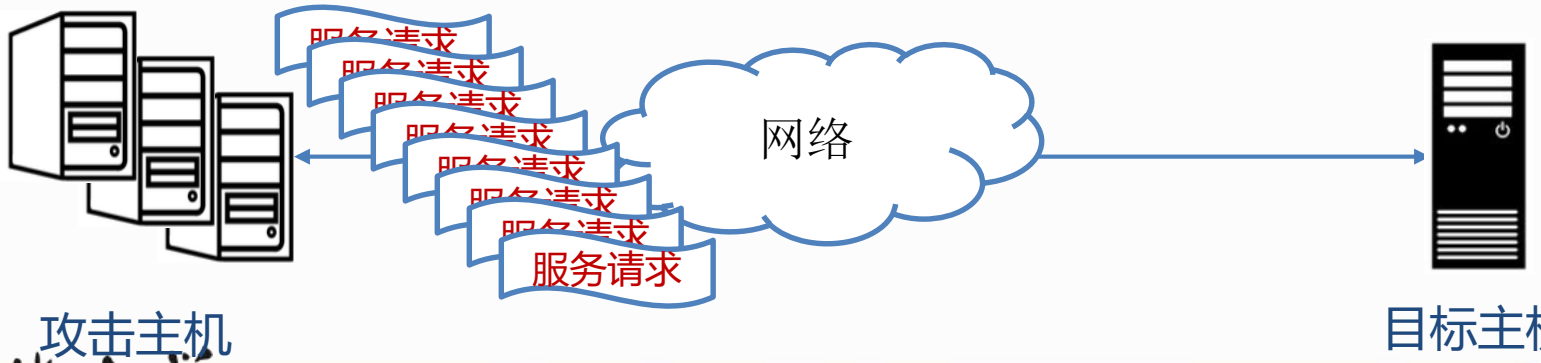
3、常见的安全攻击手段 —— 网络入侵

- 什么是网络入侵?
  - 一般是指具有熟练编写、调试和使用计算机程序的技巧的人（Hacker），利用这些技巧来通过网络非授权访问系统受限资源的行为，一般被称为破解cracking
- 网络入侵的过程
  - 前期准备：明确入侵目的、确定入侵对象以及选择入侵手段；
  - 实施入侵：真正的攻击阶段，主要包括扫描探测和攻击；
  - 后期处理：攻击者为了清除入侵痕迹而进行现场清理。

一、信息安全攻击简介

3、常见的安全攻击手段 —— 网络入侵

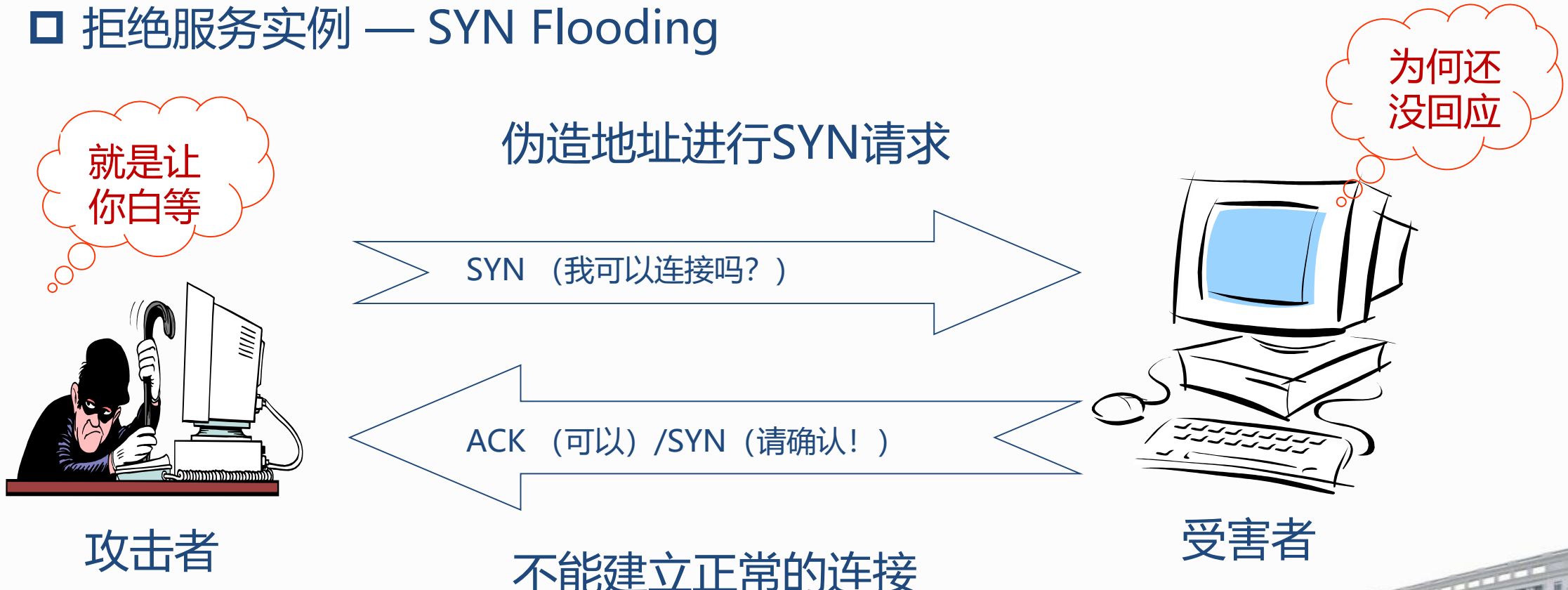
- 拒绝服务（DoS）
  - 是指攻击者利用网络通信协议的缺陷或产生大量的网络流量，导致服务器崩溃或迫使服务器停止提供服务或网络阻塞。
  - 分布式DDoS是指不同位置的多个攻击者同时向一个或数个目标发动DoS攻击，或者一个攻击者控制了位于不同位置的多台机器并利用这些机器对受害者同时实施DoS攻击。



一、信息安全攻击简介

3、常见的安全攻击手段 —— 网络入侵

- 拒绝服务实例 — SYN Flooding



一、信息安全攻击简介

3、常见的安全攻击手段 —— 网络入侵

□ 口令攻击

➢ 通过获取系统管理员或其他殊用户的口令，获得访问系统的权限。

1 获取账号信息

- 获取目标系统的用户帐号及其它有关信息一般可以利用一些网络服务来实现，如Finger、Whois、LDAP等信息服务

2 猜测用户口令

- 根据用户的个人信息猜测用户的口令，如生日、姓名、电话号码、家庭住址等

3 探测用户口令

- 采用穷举方式或口令字典对用户口令进行探测，常见的弱口令，直接使用单词作为口令

4 破解用户口令

- 探测目标系统的漏洞，伺机取得口令文件，破解取得用户口令

一、信息安全攻击简介

3、常见的安全攻击手段 —— 网络入侵

- 设置安全口令
  - 基本原则
    - 易记、不易猜
    - 长度、广度、深度
    - 别少于6位
    - 定期更换
    - 区别使用
    - 忘掉生日，姓名和字典吧！

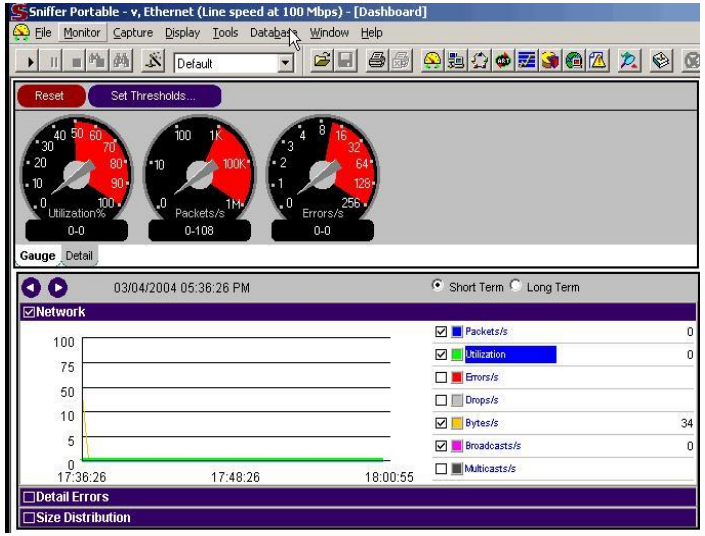
最坏的习惯是把口令写下来，并在不同系统使用相同的口令！

一、信息安全攻击简介

3、常见的安全攻击手段 —— 网络入侵

◘ 嗅探攻击

- 利用计算机的网络接口截获目的地为其它计算机的数据包的一种手段。
- 网络嗅探的工具被称为嗅探器（sniffer），是一种常用的收集网络上传输的有用数据的方法；嗅探攻击一般是指黑客利用嗅探器获取网络传输中的重要数据。网络嗅探也被形象地称为网络窃听。



一、信息安全攻击简介

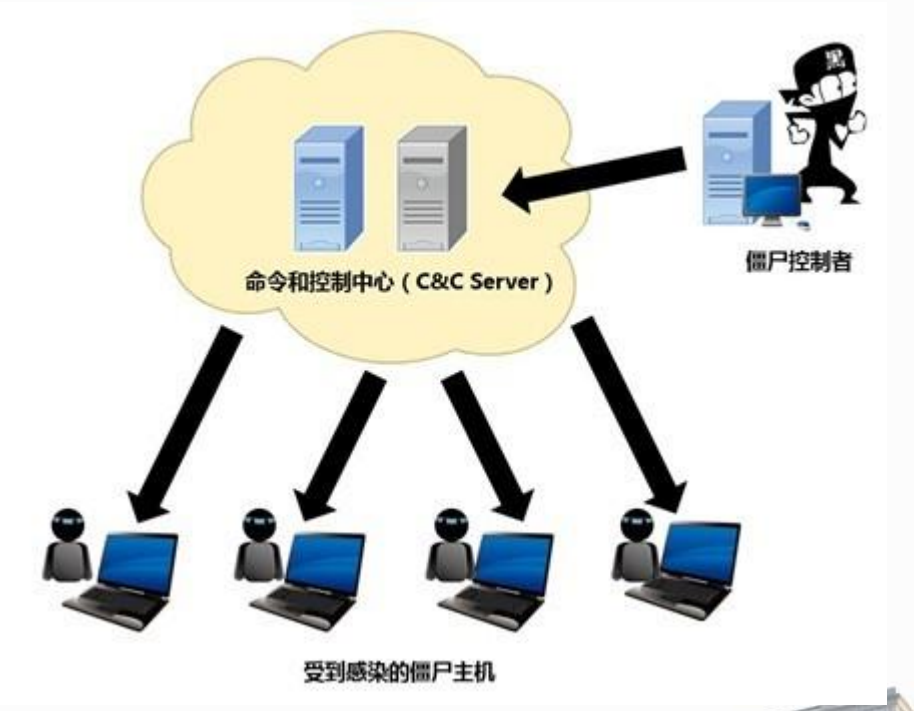
3、常见的安全攻击手段 —— 网络入侵

- 欺骗类攻击
  - 构造虚假的网络消息，发送给网络主机或网络设备，企图用假消息替代真实信息，实现对网络及主机正常工作的干扰破坏。
  - 常见的假消息攻击有IP欺骗、ARP欺骗、DNS欺骗、伪造电子邮件。

一、信息安全攻击简介

3、常见的安全攻击手段 —— 网络入侵

- 利用型攻击
  - 通过非法技术手段，试图获得某网络计算机的控制权或使用权，达到利用该机从事非法行为的一类攻击行为的总称。
  - 被控制的主机被称为“跳板” 或“肉鸡”。



一、信息安全攻击简介

4、常见的安全攻击手段 —— 诈骗类攻击

- 诈骗类攻击（网络钓鱼）
  - 诈骗类威胁是指攻击者利用社会工程学的思想，利用人的弱点（如人的本能反应、好奇心、信任、贪便宜等）通过网络散布虚假信息，诱使受害者上当受骗，而达到攻击者目的的一种网络攻击行为；
  - 准确地说，社会工程学不是一门科学，而是一门艺术和窍门，它利用人的弱点，以顺从你的意愿、满足你的欲望的方式，让你受骗上当。

一、信息安全攻击简介

5、常见的安全攻击手段 —— APT攻击

◘ APT（Advanced Persistent Threat）攻击

- 首先，这种攻击行为首先具有极强的隐蔽能力，通常是利用企业或机构网络中受信的应用程序漏洞来形成；
- 其次，APT攻击具有很强的针对性，攻击触发之前通常需要收集大量关于用户业务流程和目标系统使用情况的精确信息，情报收集的过程更是社工艺术的完美展现。

Google极光攻击

信息收集

- 攻击者尽可能地收集特定的Google员工信息

入侵员工主机

- 攻击者利用一个动态DNS供应商，建立一个托管伪造照片网站的WEB服务器，引诱员工点击

密码嗅探

- 攻击者入侵受害人机器，持续监听并最终获得该雇员访问Google服务器的账号口令等信息

信息窃取

- 攻击者使用该雇员的凭证成功渗透进入Google的邮件服务器，获取特定Gmail账户的邮件内容信息

一、信息安全攻击简介

6、常见的安全攻击手段 —— 发展趋势

- 针对新技术、新应用、以及新服务的攻击手段层出不穷；
- 关键基础设施及工业控制系统成为安全攻击的重要目标；
- 有组织的安全攻击行为变得普遍，具有更强的破坏能力；
- 攻击目的更为复杂，与国家、政治、经济问题相互交织。

一、信息安全攻击简介

- 测试点3-2
  - 通过查阅资料，进一步对APT攻击进行了解，并以一种APT攻击的流程为例，对APT攻击的特点进行阐述。
  - Ping是系统提供的用于检测网络连通性的程序，有人认为这样的程序不会对计算机系统的安全造成损害，因此没有危害性，谈谈你自己的观点，并加以说明。

网络安全的本质在对抗

对抗的本质在攻防两端能力较量

第二部分 信息安全防御简介

重点掌握信息安全防御的基本概念，了解常见安全防御技术的功能和工作原理

二、信息安全防御简介

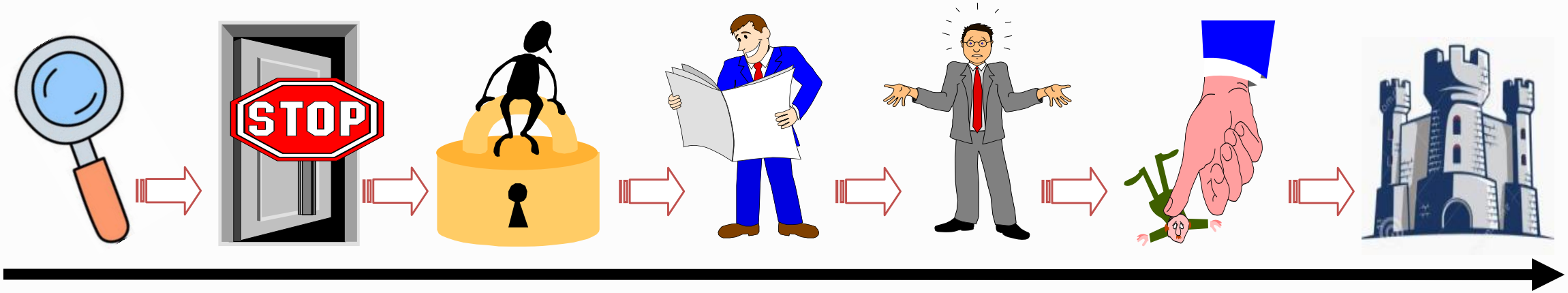
1、常见的安全防御手段概述

- 什么是常见的安全防御手段?
  - 指针对信息安全攻击的防护、检测、反应等综合性手段、方法和技术。
    - 安全防御是一个综合性的安全工程，不是几个安全产品能够完成的任务。
    - 防御需要解决多层面的问题，除了安全技术之外，安全管理也十分重要，实际上提高用户群的安全防范意识、加强安全管理所能起到效果远远高于应用几个网络安全产品

二、信息安全防御简介

1、常见的安全防御手段概述

- 典型的常见的安全防御手段场景（纵深防御）

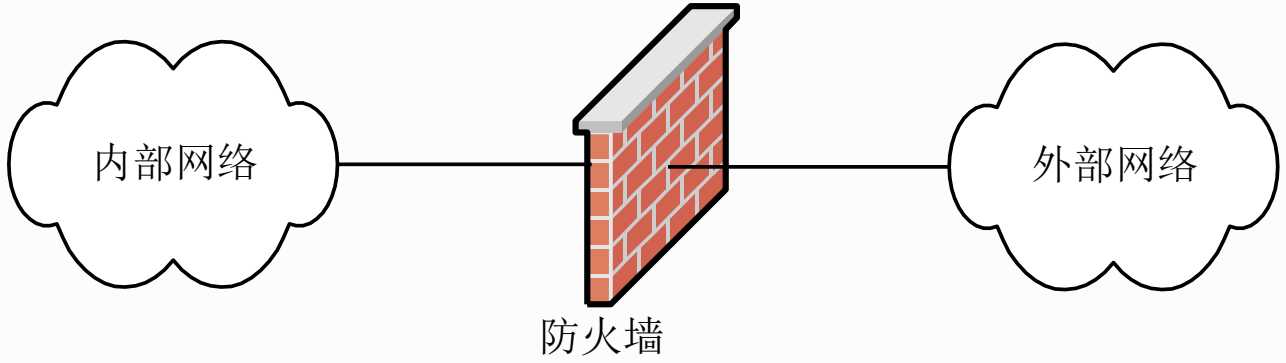


藏不住	进不来	拿不走	看不懂	改不了	逃不掉	打不跨
态势感知	身份认证	访问控制	数据机密性	数据完整性	审计\监控\签名	备份\容错容灾

二、信息安全防御简介

2、常见的安全防御手段——防火墙

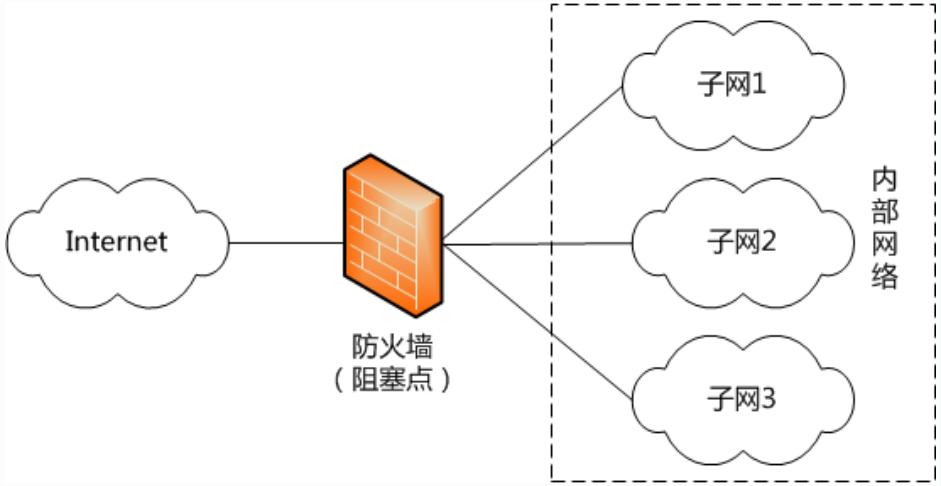
- 什么是防火墙?
  - 一个由软件和硬件设备组合而成、在内部网络和外部网络之间构造的安全保护屏障，从而保护内部网络免受外部非法用户的侵入。
  - 简单地说，防火墙是位于两个或多个网络之间，执行访问控制策略的一个或一组系统，是一类防范措施的总称。



二、信息安全防御简介

2、常见的安全防御手段——防火墙

- 防火墙设计目标
  - 有效地控制内外网之间的网络数据流量，做到御敌于外。
- 防火墙的结构和部署考虑
  - 防火墙必须部署在阻塞点上，内网和外网之间的所有网络数据流必须经过防火墙
  - 只有符合安全策略的数据流才能通过防火墙；
  - 要求防火墙具有审计和管理的功能，具有可扩展性和健壮性。



二、信息安全防御简介

2、常见的安全防御手段——防火墙

- 防火墙的分类
  - 从应用对象划分
    - 企业防火墙的主要作用是保护整个企业网络免受外部网络的攻击；
    - 个人防火墙则是保护个人计算机系统的安全。
  - 从实现形式划分
    - 硬件防火墙采用特殊的硬件设备，有较高性能，可做为独立的设备部署，企业防火墙多数是硬件防火墙；
    - 软件防火墙是一套安装在某台计算机系统上来执行防护任务的安全软件，个人防火墙都是软件防火墙。

二、信息安全防御简介

2、常见的安全防御手段——防火墙

- 防火墙实例 — 企业级硬件防火墙

- 防火墙实例 — 软件防火墙

360 安全卫士

KASPERSKY lab

RISING 瑞星

Norton

二、信息安全防御简介

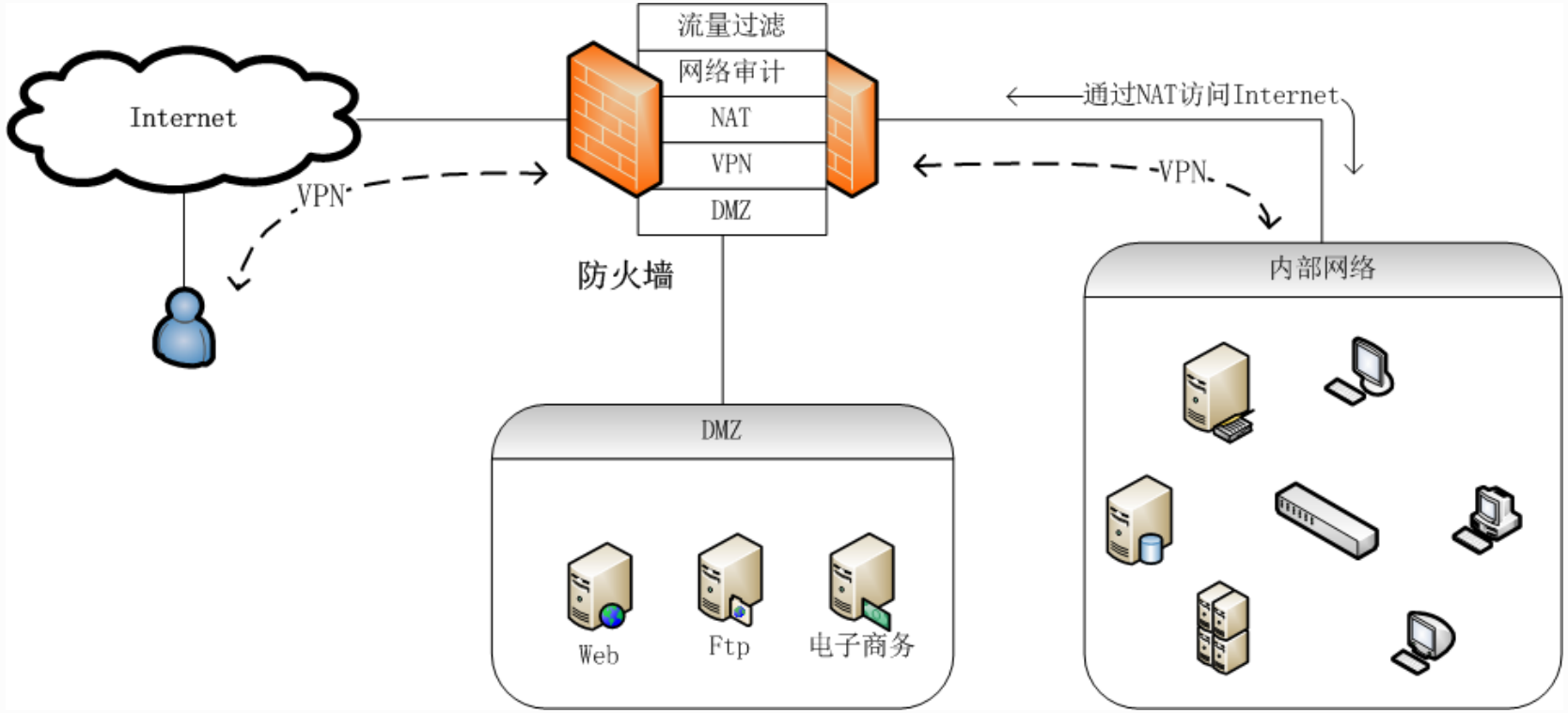
2、常见的安全防御手段——防火墙

- 防火墙主要作用
  - 网络流量过滤
    - 通过在防火墙上进行安全规则配置，可以对流经防火墙的网络流量进行过滤。
  - 网络监控审计
    - 防火墙记录访问并生成网络访问日志，提供网络使用情况的统计数据。
  - 其他安全服务
    - NAT，DMZ，VPN等

二、信息安全防御简介

2、常见的安全防御手段——防火墙

- 典型的企业级防火墙应用模式



二、信息安全防御简介

2、常见的安全防御手段——防火墙

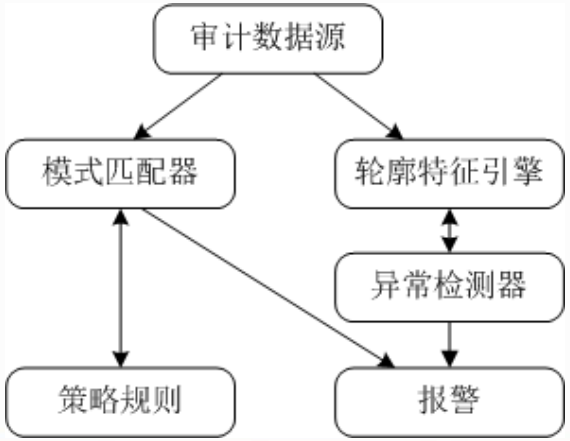
- 防火墙的局限性
  - 防火墙无法检测不经过其的流量，比如通过内部提供拨号服务接入公网的流量；
  - 防火墙不能防范来自内部人员恶意的攻击；
  - 防火墙不能阻止被病毒感染的和有害的程序或文件的传递，如木马；
  - 防火墙不能防止数据驱动式攻击，如一些缓冲区溢出攻击。

3、常见的安全防御手段——入侵检测系统

- 什么是入侵检测系统?
  - Intrusion Detection System（IDS）是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全系统。
  - 一般认为防火墙属于静态防范措施，而入侵检测系统为动态防范措施，是对防火墙的有效补充。
    - 假如防火墙是一幢大楼的门禁，那么IDS就是这幢大楼里的监视系统。

3、常见的安全防御手段——入侵检测系统

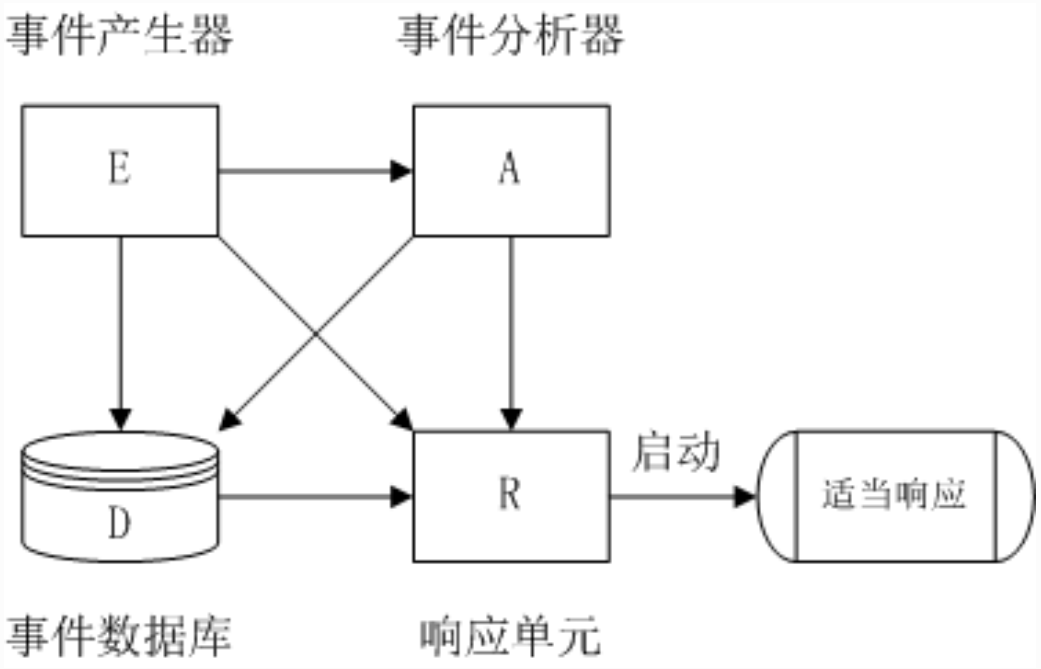
- 入侵检测起源
  - 1980年，James P. Anderson，《Computer Security Threat Monitoring and Surveillance》此报告被公认是开山之作；
  - 1984-1986年，Dorothy Denning和 Peter Neumann，实时入侵检测系统模型，IDES(Intrusion Detection Expert System)。



二、信息安全防御简介

3、常见的安全防御手段——入侵检测系统

- CIDF通用模型
  - CIDF（Common Intrusion Detection Framework，一个美国国防部赞助的开放组织）提出。



二、信息安全防御简介

3、常见的安全防御手段——入侵检测系统

基本术语

- 事件：当网络或主机遭到入侵或出现较重大变化时，称为发生安全事件，简称事件。
- 报警：当发生事件时，IDS通过某种方式及时通知管理员事件情况称为报警。
- 响应：当IDS报警后，网络管理员对事件及时作出处理称为响应。
- 误用：误用是指不正当使用计算机或网络，并构成对计算机安全或网络安全的造成威胁的一类行为。
- 异常：网络或主机的正常行为进行采样、分析，描述出正常的行为轮廓，建立行为模型，当网络或主机上出现偏离行为模型的事件时，称为异常。

3、常见的安全防御手段——入侵检测系统

- 基本概念（续）
  - 入侵特征：也称为攻击签名（Attack Signature）或攻击模式（Attack Patterns），一般指对网络或主机的某种入侵攻击行为（误用行为）的事件过程进行分析提炼，形成可以分辨出该入侵攻击事件的特征关键字，这些特征关键字被称为入侵特征。
  - 感应器（sensor）：布置在网络或主机中用于收集网络信息或用户行为信息的软硬件，称为感应器。感应器应该布置在可以及时取得全面数据的关键点上，其性能直接决定IDS检测的准确率。

二、信息安全防御简介

3、常见的安全防御手段——入侵检测系统

□ 入侵检测系统工作过程

1 信息收集

- 入侵检测的第一步是信息收集，收集内容包括系统和网络的数据及用户活动的状态和行为。信息收集工作一般由由放置在不同网段的感应器来收集网络中的数据信息（主要是数据包）和主机内感应器来收集该主机的信息。

2 信息分析

- 将收集到的有关系统和网络的数据及用户活动的状态和行为等信息送到检测引擎。当检测到某种入侵特征时，会通知控制台出现了安全事件。

3 结果处理

- 当控制台接到发生安全事件的通知，将产生报警，也可依据预先定义的相应措施进行联动响应。如可以重新配置路由器或防火墙、终止进程、切断连接、改变文件属性等。

二、信息安全防御简介

3、常见的安全防御手段——入侵检测系统

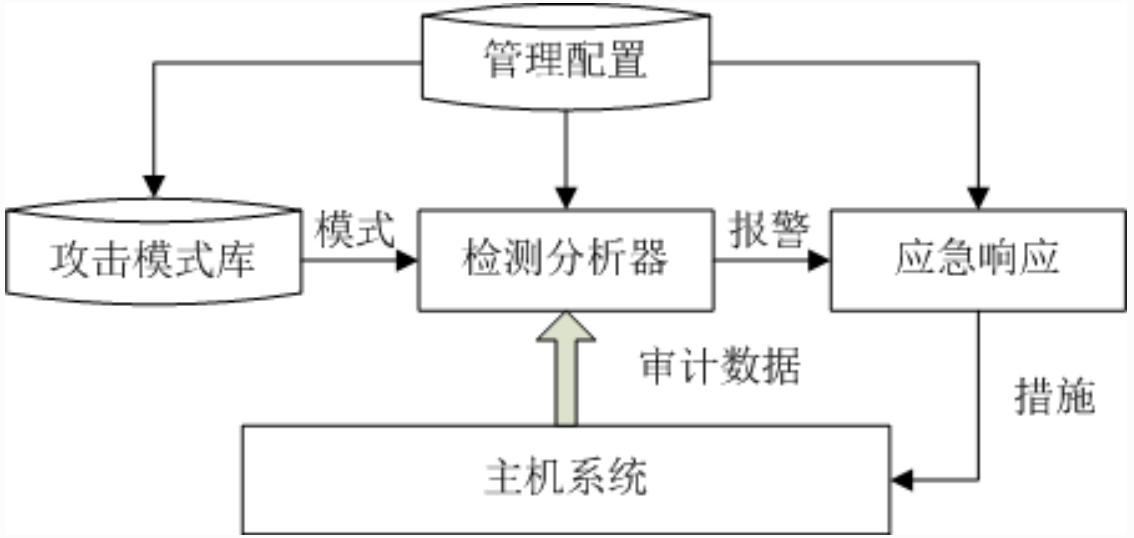
- 入侵检测主要功能
  - 监测并分析用户、系统和网络的活动变化；
  - 核查系统配置和漏洞；
  - 评估系统关键资源和数据文件的完整性；
  - 识别已知的攻击行为；
  - 统计分析异常行为；
  - 操作系统日志管理，并识别违反安全策略的用户活动。

二、信息安全防御简介

3、常见的安全防御手段——入侵检测系统

□入侵检测系统分类

- ➢ 以数据源为分类标准
  - – 主机型入侵检测系统（HIDS）

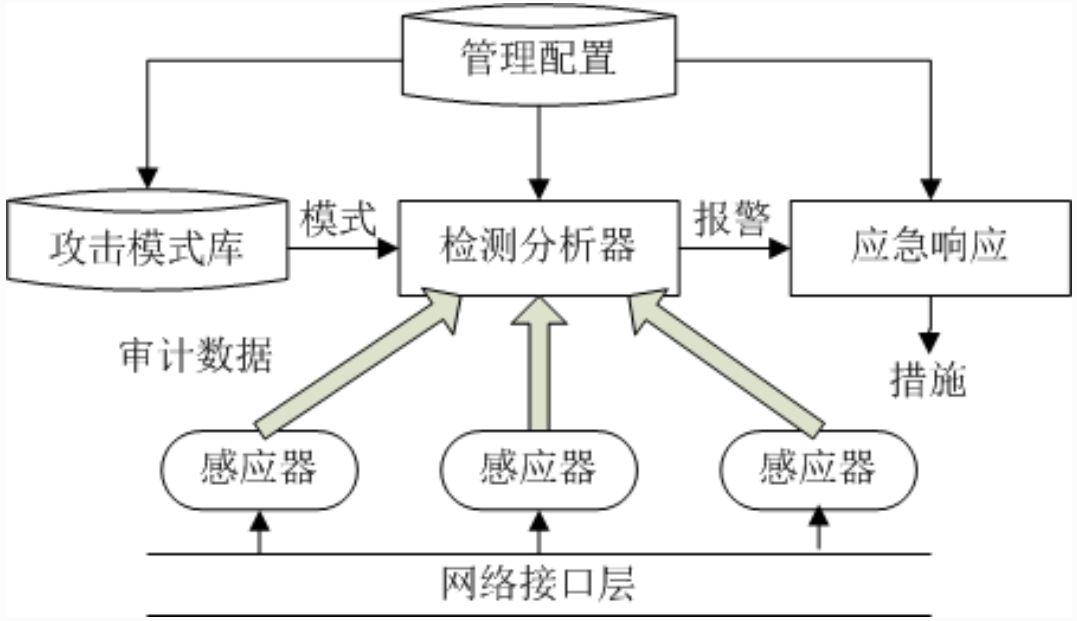


二、信息安全防御简介

3、常见的安全防御手段——入侵检测系统

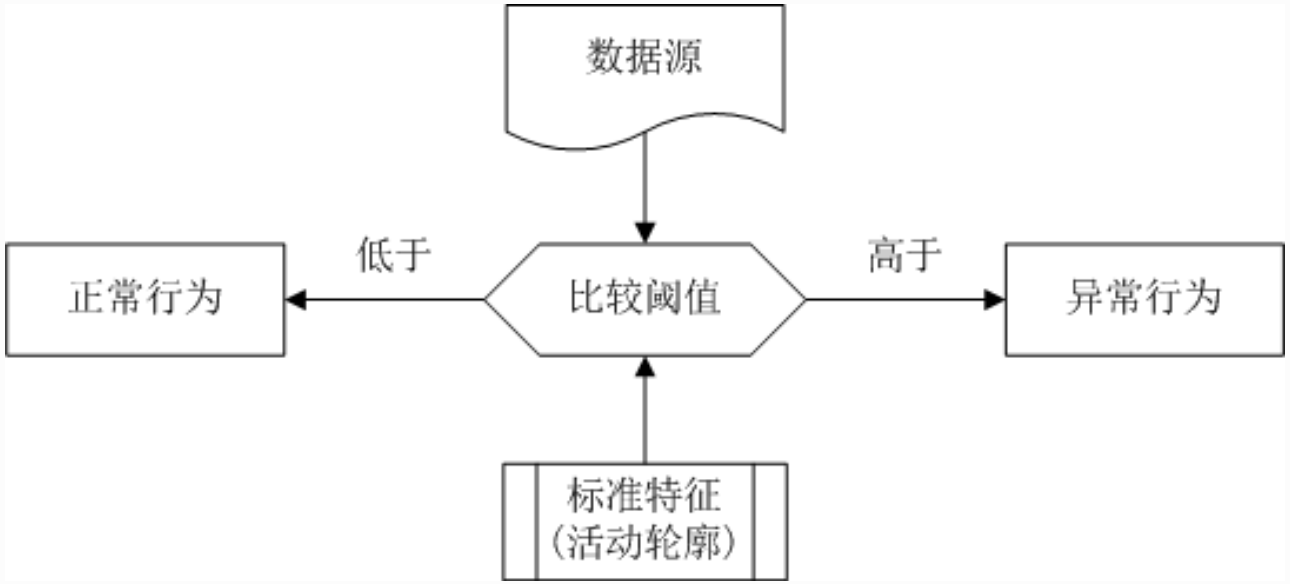
□入侵检测系统分类

- ➢ 以数据源为分类标准
  - – 网络型入侵检测系统（NIDS）



3、常见的安全防御手段——入侵检测系统

- 入侵检测系统分类
  - 以检测技术为分类标准
    - 基于异常检测（Anomaly Detection）的IDS



3、常见的安全防御手段——入侵检测系统

- 入侵检测技术概述
  - 误用检测技术
    - 主要基于规则进行检测，包括：专家系统、特征分析、状态转换分析、模型推理、完整性校验等
  - 异常检测技术
    - 异常检测是一种与系统相对无关、通用性较强的入侵检测技术。异常检测主要针对用户行为数据、系统资源使用情况进行分析判断。包括：统计分析、预测模型、系统调用监测以及基于人工智能的异常检测技术等。

二、信息安全防御简介

4、常见的安全防御手段——入侵诱骗系统

- 什么是入侵诱骗?
  - 入侵诱骗是指用通过伪装成具有吸引力的网络主机来吸引攻击者，同时对攻击者的各种攻击行为进行分析，进而找到有效的应对方法。
  - 入侵诱骗也具有通过吸引攻击者，从而保护重要的网络服务系统的目的。
  - 常见的入侵诱骗技术主要有蜜罐（Honeypot）和蜜网（Honeynet）技术。

5、常见的安全防御手段——入侵响应系统

- 什么是入侵响应?
  - 入侵响应指发现或检测到入侵后，为确保被保护目标的机密性、完整性、可用性等安全目标，针对入侵所采取的措施和行动。
  - 入侵检测系统的响应技术可以分为主动响应和被动响应。
    - 主动响应是系统自动阻断攻击过程或以其他方式影响攻击过程;
    - 被动响应是报告和记录发生的事件。

二、信息安全防御简介

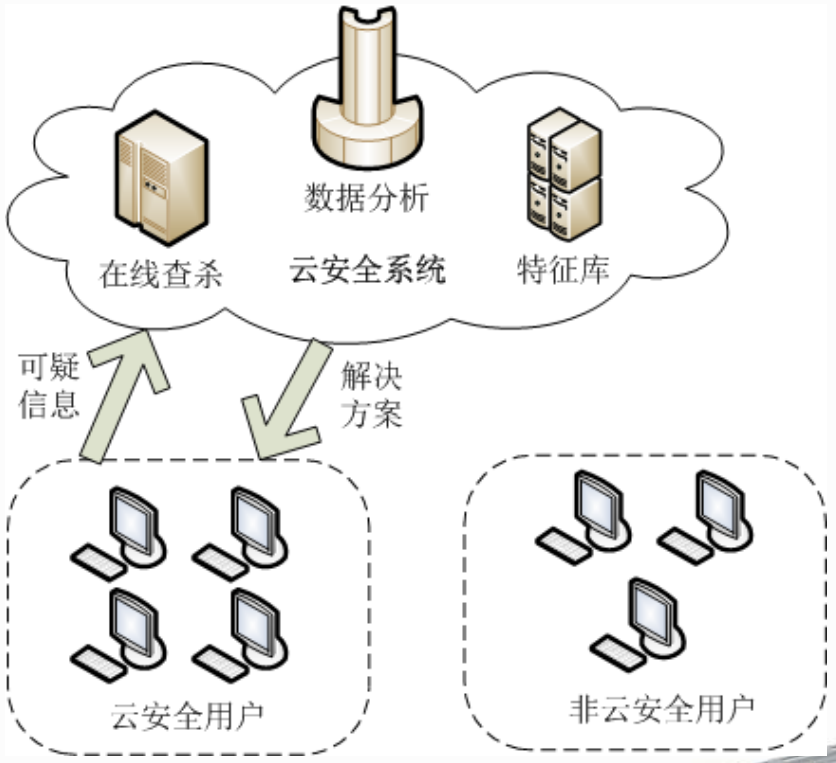
6、新型的安全防御手段——态势感知

- 什么是态势感知?
  - 态势感知的概念最早在军事领域被提出，覆盖感知、理解和预测三个层次。并随着网络的兴起而升级为“网络态势感知（Cyberspace Situation Awareness，CSA）”。旨在大规模网络环境中对能够引起网络态势发生变化的安全要素进行获取、理解、显示以及最近发展趋势的顺延性预测，进而进行决策与行动。
  - “加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力。”

二、信息安全防御简介

7、新型的安全防御手段——云安全

- 什么是云安全?
  - 云安全是通过网状的大量客户端对网络中软件行为的异常监测，获取互联网中木马、恶意程序的最新信息，传送到Server端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。目前“云安全”也被称为“云杀毒”。



二、信息安全防御简介

- 测试点3-3
  - 防火墙和网闸都能提供在网络边界上的安全防护作用，请分析两者在功能上的相同与不同之处。
  - 漏报率和误报率是入侵检测系统（IDS）重要的性能指标，有人认为采用异常检测技术的IDS误报率很高，没有实用价值，请给出你的判断并说明判断理由。

结束语

感 谢 聆 听!

zhaoyang@uestc.edu.cn