

网络安全 – 概述

曹越

国家网络安全学院

武汉大学

yue.cao@whu.edu.cn

个人介绍

教育经历

- 武汉工程大学，通信工程专业，本科
- 英国萨里大学，移动通信系统专业，硕士
- 英国萨里大学，电子工程专业，博士

工作经历

- 英国萨里大学，5G创新研究中心，博士后
- 英国诺森比亚大学，计算机与信息科学系，讲师/高级讲师
- 英国兰卡斯特大学，计算机与通信系统学院，国际讲师
- 北京航空航天大学，交通科学与工程学院，教授
- 武汉大学，国家网络安全学院，教授

研究方向：智能交通系统

- 交通与能源---新能源汽车充/换电、自主泊车、无人机任务决策优化
- 网络与通信---边缘计算，车联网通信，群智感知
- 安全与定位---信任管理、异常检测、位置隐私

课程介绍

网络安全

信息系统安全

安全策略及其原则

课程介绍

网络安全

信息系统安全

安全策略及其原则

课程安排

课堂讲授 + 上机实践

了解和掌握网络与信息安全的基本原理、技术、及最新研究成果

具有网络安全与信息安全的理论基础和基本实践能力

考勤 + 作业 + 期末笔试的评估方式

网络安全 vs 信息安全

网络安全更注重在网络层面，例如通过部署防火墙、入侵检测等硬件设备来实现链路层面的安全防护

信息安全的层面要比网络安全的覆盖面大的多，信息安全是从数据的角度来看安全防护

信息安全包括网络安全，信息安全还包括操作系统安全，数据库安全，硬件设备和设施安全，物理安全，人员安全，软件开发，应用安全等

通常采用的手段包括：防火墙、入侵检测、审计、渗透测试、风险评估等，安全防护不仅仅是在网络层面，更加关注的应用层面，可以说信息安全更贴近于用户的实际需求及想法

本课程的目的

提高安全意识

掌握网络攻防技术的原理、方法和工具

信息系统的安全解决方案

掌握Internet的安全性

课程基础知识

密码学

计算机网络 (TCP/IP)

操作系统 (UNIX和Windows)

程序设计

参考书籍

《密码学与网络安全》

《网络安全》

《计算机网络-自顶向下方法》

其他准备知识

- **TCP/IP**
- **OS**
- **Windows NT/2000**

目录

1. 网络安全概论
2. 网络攻击行径分析
3. 网络侦查技术
4. 拒绝服务攻击
5. 缓冲区溢出攻击
6. 程序攻击
7. 欺骗攻击
8. 利用处理程序错误攻击
9. 访问控制技术

目录

- 10. 防火墙技术**
- 11. 入侵检测技术**
- 12. VPN技术**
- 13. 网络病毒防治**
- 14. 无线网络安全防护**
- 15. 安全恢复技术**
- 16. 取证技术**
- 17. 信息系统安全保障系统**

信息化出现的新问题

IT泡沫破裂

失业，再就业的起点更高（对汽车行业的冲击）

互联网经营模式是什么？（游戏厅-网游-手游）

网上信息可信度差（诈骗，窃取）

垃圾电子邮件

安全

➤ **病毒**

➤ **攻击**

.....

网络安全的定义

网络安全指信息系统的硬件、软件及其系统中的数据受到保护，不会遭到偶然的或者恶意的破坏、更改、从而系统能连续、可靠、正常地运行，服务不中断。

网络安全简单的说是在网络环境下能够识别、消除不安全因素的能力。

信息化与国家安全 - 信息战

“谁掌握了信息，控制了网络，谁将拥有整个世界。”

— （美国著名未来学家阿尔温.托尔勒）

“今后的时代，控制世界的国家将不是靠军事，而是信息能力走在前面的国家。”

— （美国总统克林顿）

“信息时代的出现，将从根本上改变战争的进行方式。”

— （美国前陆军参谋长沙利文上将）

网络安全形势严峻 - 信息及数据泄露

2016年规模较大的信息泄露事件

▶ 2015年：

12月末	美国1.9亿选民信息泄露
------	--------------

▶ 2016年：

1月	俄罗斯邮件网站Mail.ru约5700万登录凭证在网上出售
----	-------------------------------

4月	5000万土耳其公民信息泄露
----	----------------

4月	5500千万菲律宾选民信息泄露
----	-----------------

4月	9340万墨西哥选民个人信息数据库曝光
----	---------------------

5月	1.17亿LinkedIn账户登录信息泄露
----	-----------------------

5月	4000万成人社交网站Fling用户的凭证在暗网售卖
----	----------------------------

6月	俄罗斯社交网站VK.com1亿登录凭证被盗
----	-----------------------

8月	俄罗斯搜索引擎Rambler约1亿用户信息网上曝光
----	---------------------------

9月	雅虎5亿账户信息泄露
----	------------

10月	MongoDB 5800万商业用户信息泄露
-----	-----------------------

12月	影片分享网站Dailymotion 8520万用户名及邮件泄露
-----	---------------------------------

12月	雅虎确认一起早在2013年的账户信息泄露，这次的数字是10亿
-----	--------------------------------

仅在2016年前10个月，全球已约有3000起公开的数据泄露事件，22亿条记录被披露，已经超过2015年全年。

2019年 Facebook 事件

网络安全形势严峻 - 网络攻击

2016年影响较大的网络攻击事件

▶ 2015年：

12月末 乌克兰70万家庭断电

▶ 2016年：

1月 飞机零件制造商FACC遭商业邮件欺诈(BEC)，损失5000万欧元

1月 比利时银行Crean遭BEC攻击，损失7千万欧元

3月 孟加拉银行被黑客转走8100万美元

4月 德国Gundremmingen核电厂确认系统中存在恶意软件

6月 美国民主党国家委员会被黑客入侵，电子邮件及文档被披露

8月 全球第三大航空公司达美航空数百航班被取消，上千航班被延误，无数乘客滞留

8月 黑客组织“影子经济人”盗取了NSA大量黑客工具和漏洞利用包，并在网上售卖

8月 全球第四大的电线电缆厂商Leoni AG遭BEC，被骗4460万美元

9月 统计显示，针对奥运会的DDoS攻击最高达540Gbps

9月 知名安全研究人员 Brian Krebs 的安全博客网站被DDoS攻击，攻击带宽达665Gbps

9月 世界最大的主机托管公司之一OVH，声称遭到规模达1Tbps的DDoS攻击

10月 国际原子能署披露，德国某核电厂在二、三年曾遭受扰乱性网络攻击

一是**DDoS规模和数量的激增**。主要原因是DDoS工具的自动化和服务化，再加上物联网设备的爆发。

二是**勒索软件**。某勒索软件作者兼分发者，仅上半年就勒索到1.21亿美元，净利润达9400万美元。

三是**商业邮件欺诈(BEC)攻击**。2013年10月至2016年5月间，美国和其他79个国家，共发生22143起企业邮件诈骗案件，被骗总金额高达31亿美元。

网络安全形势严峻 - 漏洞攻防

2016年漏洞类型统计

漏洞类型	漏洞数量	占比
缓冲区溢出	1207	15.31%
权限许可和访问控制	853	10.82%
信息泄露	842	10.68%
跨站脚本	573	7.27%
输入验证	552	7.00%
资源管理错误	171	2.17%
SQL注入	135	1.71%
数字错误	119	1.51%
跨站请求伪造	118	1.50%
路径遍历	89	1.12%

2016年，截止12月15日，绿盟漏洞公告平台漏洞数量为3460个，中国国家信息安全漏洞库(CNNVD)漏洞数量8071个，国家信息安全漏洞平台(CNVD)漏洞数量9600个，CVE漏洞数量突破1万，均比去年同期有所增长，增长幅度约在10%至15%之间。

硬件、软件、协议

网络安全行业发展引来新机遇 - 政策法规（国内）

- 2015年12月27日，全国人大常委会通过《中华人民共和国反恐怖主义法》。
- 2016年1月15日，全国首部大数据地方法规《贵州省大数据发展应用促进条例》经人大表决通过。
- 4月19日，习近平总书记在网络安全和信息化工作座谈会上发表讲话。
- 6月25日，习近平主席和俄罗斯总统普京发布《中华人民共和国主席和俄罗斯联邦总统关于协作推进信息网络空间发展的联合声明》。
- 7月，中共中央办公厅、国务院办公厅印发《国家信息化发展战略纲要》，此为规范和指导未来10年国家信息化发展的纲领性文件。
- 8月22日，中央网信办发布《关于加强国家网络安全标准化工作的若干意见》
- 10月，工业和信息化部印发《工业控制系统信息安全防护指南》
- 11月7日，第十二届全国人大常委会第二十四次会议通过《中华人民共和国网络安全法》

网络安全行业发展引来新机遇 - 政策法规（国外）

- 2016年1月1日，俄罗斯《互联网隐私法案》生效。
- 2月18日，奥巴马政府成立“国家网络空间安全强化委员会”促进未来十年内美国的网络安全。
- 4月起，欧盟30个国家的超700名安全专家，长达7个月的演练，涉及针对无人机、云技术、移动恶意软件和物联网等多种不同威胁。
- 6月14日，北大西洋公约组织宣布，“网络”将正式成为各北约成员国的战场。
- 7月6日，欧洲议会通过《网络和信息系统安全指令》。
- **8月1日，欧美隐私盾协议全面实施。**
- 11月21日，美国国防部公布“漏洞披露政策”，允许自由安全研究人员通过合法途径披露国防部公众系统存在的任何漏洞。
- **11月30日，英国议会通过《2016调查权法》，该法律要求网络公司和电信公司收集客户通信数据，并存储12个月的网络浏览历史记录，给警察、安全部门和政府提供了空前的数据访问权力。**

信息安全的级别

按照范围和处理方式的不同，通常将信息安全划分为三个级别：

➤ 第1级为**计算机安全（基础）**

- 设备安全、操作系统安全、数据库安全等
- 设计漏洞

➤ 第2级为**网络安全（核心）**

- 处理、存储、传输等
- 协议漏洞

➤ 第3级为**信息系统安全（目标）**

- 用户透明

课程介绍

网络安全

信息系统安全

安全策略及其原则

安全的要素

可用性： 授权实体有权访问数据。

机密性： 信息不暴露给未授权实体或进程。

完整性： 保证数据不被未授权修改。

可控性： 控制授权范围内的信息流向及操作方式。

可审查性： 对出现的安全问题提供依据与手段。

安全威胁的来源

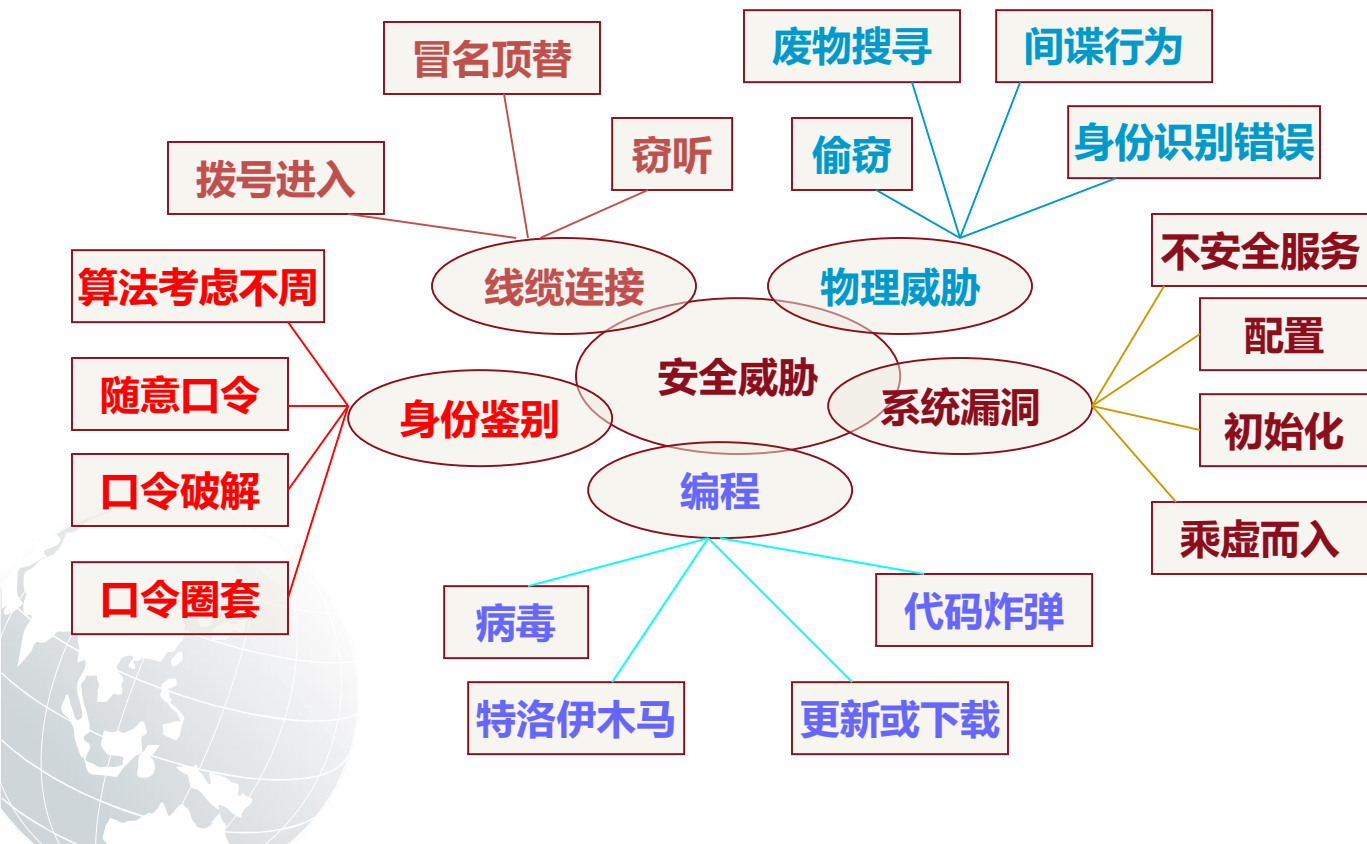
外部渗入：未被授权使用计算机的人。

内部渗入者：被授权使用计算机，但不能访问某些数据、程序或资源，它包括：

- **冒名顶替：**使用别人的用户名和口令进行操作；
- **隐蔽用户：**逃避审计和访问控制的用户；

滥用职权者：被授权使用计算机和访问系统资源，但滥用职权者。


安全威胁的几种类型



安全的目标

保障安全的基本目标就是要能具备

- 安全保护能力
- 隐患发现能力
- 应急反应能力
- 信息对抗能力



信息对抗能力已经不只是科技水平的体现，更是综合国力的体现。未来的战争无疑是始于信息战，以网络为基础的信息对抗将在一定程度上决定战争的胜负

网络安全的根源

信息系统自身安全的脆弱性

信息系统面临的安全威胁

安全管理问题

黑客攻击

网络犯罪

为什么会感染恶意代码

网络安全的根源 - 信息系统自身的安全脆弱性

指信息系统的硬件资源、通信资源、软件及信息资源等，因可预见或不可预见、甚至恶意的原因，而可能导致系统受到破坏、更改、泄露和功能失效，从而使系统处于异常状态，甚至崩溃瘫痪等的根源和起因。

这里我们从以下层面分别进行分析：

- 硬件组件
- 软件组件
- 网络和通信协议

安全漏洞简介

漏洞也叫脆弱性（Vulnerability），是计算机系统在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷和不足。

漏洞一旦被发现，就可使用这个漏洞获得计算机系统的额外权限，使攻击者能够在未授权的情况下访问或破坏系统，从而导致危害计算机系统安全。

脆弱性与漏洞存在的原因

支持Internet运行的TCP/IP协议栈原本只考虑互联互通和资源共享问题，并未考虑也无法兼顾解决来自网际的大量安全问题

基于TCP/IP的Internet是在可信任网络环境中开发出来的成果，体现在TCP/IP协议上的总体构想和设计本身，基本未考虑安全问题，并不提供人们所需的安全性和保密性

TCP/IP协议最初设计的应用环境是互相信任的

硬件、软件漏洞的例子？

网络安全的根源 - 信息系统面临的安全威胁

基本威胁

- 威胁信息系统安全的因素是多方面的，目前还没有统一的方法对各种威胁加以区别和进行准确的分类。

威胁信息系统的主要方法

- 不同威胁的存在及其重要性是随环境的变化而变化的

威胁和攻击的来源

基本威胁

安全的基本目标是实现信息的机密性、完整性、可用性。

对信息系统这3个基本目标的威胁即是基本威胁

- **信息泄漏**
- **完整性破坏**
- **拒绝服务**
- **未授权访问**

基本威胁1 - 信息泄漏

信息泄漏指敏感数据在有意或无意被泄漏、丢失或透露给某个未授权的实体。

信息泄漏包括：信息在传输中被丢失或泄漏；通过信息流向、流量、通信频度和长度等参数等分析，推测出有用信息。

基本威胁2 - 完整性破坏

以非法手段取得对信息的管理权，通过未授权的创建、修改、删除等操作而使数据的完整性受到破坏。

基本威胁3 - 拒绝服务

信息或信息系统资源等服务能力下降或丧失。

产生服务拒绝的原因：

- 受到攻击所致，攻击者通过对系统进行非法的、根本无法成功的访问尝试而产生过量的系统负载，从而导致系统的资源对合法用户的服务能力下降或丧失。
- 信息系统或组件在物理上或逻辑上受到破坏而中断服务。

基本威胁4 - 未授权访问

未授权实体非法访问信息系统资源

- **非法访问：假冒和盗用合法用户身份攻击、非法进入网络系统进行违法操作**

或授权实体超越权限访问信息系统资源。

- **越权访问：合法用户以未授权的方式进行操作等形式。**



特洛伊木马



黑客攻击



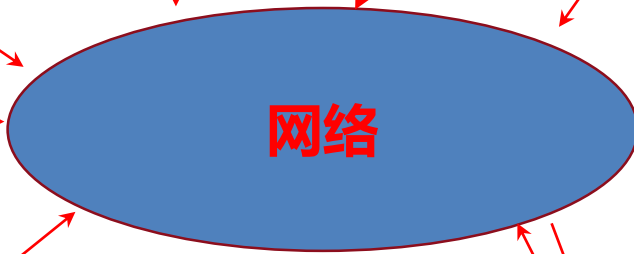
后门、隐蔽通道



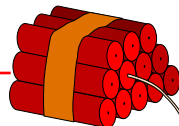
计算机病毒



信息丢失、篡改、销毁



网络



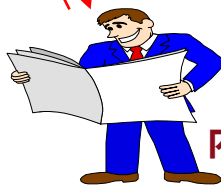
拒绝服务攻击



逻辑炸弹



蠕虫



内部、外部泄密

网络安全的根源 - 安全管理问题

管理策略不够完善，管理人员素质低下，用户安全意识淡薄，有关的法律规定不够健全。

管理上权责不分，对计算机安全不重视，少数管理权过大，而实际工作中又不需要。

管理不严格，缺乏系统的整体培训。

没有保密意识，系统密码随意传播，导致出现问题时相互推卸责任的局面。

网络安全的根源 - 黑客攻击

黑客 (hacker) , 源于英语动词hack, 意为 “劈, 砍” , 引申为 “干了一件非常漂亮的工作” 。

在早期麻省理工学院的校园俚语中, “黑客” 则有 “恶作剧” 之意, 尤指手法巧妙、技术高明的恶作剧。

他们通常具有硬件和软件的高级知识, 并有能力通过创新的方法剖析系统。

网络黑客的主要攻击手法有: 获取口令、放置木马程序、网页的欺骗技术、电子邮件攻击、通过一个节点攻击另一节点、网络监听、寻找系统漏洞、利用帐号进行攻击、窃取特权。

黑客的分类



白帽子创新者

- 设计新系统
- 打破常规
- 精研技术
- 勇于创新

没有最好，
只有更好

MS
Linux

灰帽子破解者

- 破解已有系统
- 发现问题/漏洞
- 突破极限/禁制
- 展现自我

计算机
为人民服务

漏洞发现
软件破解
工具提供

黑帽子破坏者

- 随意使用资源
- 恶意破坏
- 散播蠕虫病毒
- 商业间谍

人不为己，
天诛地灭

入侵
CIH者

网络安全的根源 - 网络犯罪 -1

网络人口的惊人增长，但是，这种新的通讯技术，突飞猛进，尚未规范，也带来很多法律问题。

各国网络的广泛使用，网络人口的比例越来越高，素质又参差不齐，网络成为一种新型的犯罪工具、犯罪场所和犯罪对象。

网络犯罪中最为突出的问题有：

- 网络色情泛滥成灾，严重危害未成年人的身心健康；
- 软件、影视唱片的著作权受到盗版行为的严重侵犯；
- 网络商务备受诈欺困扰，信用卡被盗刷，购买的商品石沉大海，发出商品却收不回货款；
- 更有甚者，已经挑战计算机和网络几十年之久的黑客仍然是网络的潜在危险。

网络安全的根源 - 网络犯罪-2

网络犯罪的类型

- 网络文化污染
- 盗版交易
- 网络欺诈
- 名誉毁损
- 侵入他人主页、网站、邮箱
- 制造传播计算机病毒
- 网络赌博
- 网络教唆、煽动各种犯罪

网络安全的根源 - 为什么会感染恶意代码

- 浏览网页
- 使用即时通讯工具
- 浏览邮件
- 下载文件
- 远程攻击
- 局域网攻击
- 使用移动存储介质

为什么会感染恶意代码 - 浏览网页 1

大家一定遇到过这种情况：在浏览过某网页之后，浏览器主页被修改，或者每次打开浏览器都被迫访问某一固定网站，或者浏览器遇到错误需要关闭，或者出现黑屏蓝屏，或者处于死机状态，或者疯狂打开窗口并被强制安装了一些不想安装的软件。

如果同时出现多种以上现象，那么很不幸，你肯定是中了恶意网站或恶意软件的毒了。

为什么会感染恶意代码 - 浏览网页 2

黑客在网页中注入恶意代码并诱使用户访问的方式叫做“网页木马攻击”，简称“网马”。

“网马”是近年来黑客最流行的攻击方式，网页中含有网马常常称为“被挂马”。

这些含有网马的网页往往包括：

- 遭到黑客攻击的网站
- 黑客网站
- 含有不健康内容的网站
- 反动网站

为什么会感染恶意代码 - 浏览网页 3

黑客在网页中挂载网马，希望利用浏览者系统存在的某些漏洞将恶意代码植入浏览者的系统。

这种漏洞好比一条黑客用来传输恶意代码的“公路”，但是这条公路被“河流”切断。如果用户访问被挂马的网页，就相当于为黑客搭建了一座桥，黑客将可以顺利到达你的系统。



为什么会感染恶意代码 - 使用即时通讯工具 1

即时通讯工具(Instant Messenger, 简称IM)已经从原来纯娱乐休闲工具变成生活工作的必备工具, 这些工具包括: MSN、QQ、旺旺、百度HI、ICQ等。

由于用户数量众多, 再加上即时通讯软件本身的安全缺陷, 例如内建有联系人清单, 使得恶意代码可以方便地获取传播目标, 这些特性都能被恶意代码利用来传播自身。

为什么会感染恶意代码 - 使用即时通讯工具 2

金山毒霸全球反病毒监测中心的监测数据认为，目前MSN、QQ等即时通工具已成为继网页之后病毒传播的第二大渠道。

臭名昭著、造成上百亿美元损失的求职信(Worm.Klez)病毒就是第一个可以通过ICQ进行传播的恶性蠕虫，它可以遍历本地ICQ中的联络人清单来传播自身。

为什么会感染恶意代码 - 使用即时通讯工具 3

黑客如何通过即时通讯工具攻击我们？

实例：MSN或者QQ经常接收到一些可疑的消息，试图欺骗用户接收。



为什么会感染恶意代码 - 浏览邮件 1

由于Internet使用的广泛，电子邮件传播速度相当神速，商务联络、公文传递、好友联系经常使用电子邮件传递，最常见的是通过Email交换Word格式的文档。

黑客也随之找到了恶意代码的载体，电子邮件携带病毒、木马及其他恶意程序，会导致收件者的计算机被黑客入侵。

为什么会感染恶意代码 - 浏览邮件 2

大家也许认为Word文档不是可执行程序，不会具有危害性。实际上，word文件、图片、压缩文件、文本文件都可能具有危害性。

为什么会感染恶意代码 - 下载文件

大家经常从网站、FTP服务器、BBS论坛和P2P下载一些工具、资料、音乐文件、视频文件、游戏安装包，而这些文件都可能包含恶意代码。很多病毒流行都是依靠这种方式同时使成千上万台计算机染毒。

这是因为在这些平台上发布的文件往往没有严格的安全管理，没有对用户上传的文件进行安全验证，或者即使进行了验证但是黑客使用了病毒变形、加壳等技术逃过杀毒软件的查杀。

为什么会感染恶意代码 - 远程攻击 1

一个远程攻击是这样一种攻击，其攻击对象是远程计算机；也可以说，远程攻击是一种专门攻击除攻击者自己计算机以外的计算机（无论被攻击的计算机和攻击者位于同一子网还是有千里之遥）。

“远程计算机” 确切的定义是：“一台远程计算机是这样一台机器，它不是你正在其上工作的平台，而是能利用某种协议通过Internet或任何其他网络介质被使用的计算机”。

为什么会感染恶意代码 - 远程攻击 2

黑客进行远程攻击一般利用漏洞进行。

这种漏洞跟前面“网马”所利用的漏洞不同，这种漏洞相当于一从攻击端到达目标机器的直通“路”。



为什么会感染恶意代码 - 远程攻击 2

这就意味着，只要一台计算机处于联网状态，即使这台计算机的使用者不做任何操作，这台计算机也可能受到黑客入侵。

这是一种危害性非常大、渗透力非常强的攻击方式。Conficker蠕虫就是通过MS08-067漏洞进行远程攻击。

为什么会感染恶意代码 - 局域网攻击

局域网攻击是指攻击者可以利用局域网的一些机制攻击局域网内的其他用户。这类攻击包括：共享资源入侵、Ping洪水攻击和ARP欺骗攻击等。

其中，以ARP欺骗攻击最为流行，效果明显，威力惊人。

通过欺骗局域网内访问者PC的网关MAC地址，使访问者PC错以为攻击者更改后的MAC地址是网关的MAC，导致网络不通。此种攻击可让攻击者获取局域网上的数据包甚至可篡改数据包，且可让网络上特定计算机或所有计算机无法正常连线。

为什么会感染恶意代码 - 使用移动存储介质 1

可能大家都遇到当U盘插入到电脑时，杀毒软件就急不可待的弹出警告提示的异常状况。

随着时代的发展，移动硬盘、U盘、数码相机SD卡、MP3、MP4等移动设备也成为了新攻击目标。而U盘因其超大空间的存储量，逐步成为了使用最广泛、最频繁的存储介质，为计算机病毒寄生的提供更宽裕的空间。

当前“自动播放”（Autorun）技术经常受到病毒木马的“青睐”。

为什么会感染恶意代码 - 使用移动存储介质 2

恶意代码如何通过移动存储介质传播？

实例：U盘的双击命令、右键菜单名称和命令可以被任意修改。



课程介绍

网络安全

信息系统安全

安全策略及其原则

管理安全等级划分

第一级：用户自主保护级

- 实施计划管理

第二级：系统审计保护级

- 实施操作规程管理

第三级：安全标记保护级

- 实施标准化过程管理

第四级：结构化保护级

- 实施安全生态管理

第五级：访问验证保护级

- 实施安全文化管理

什么是信息保障（PDRR）

保护（Protect）

- 采用的手段保障信息的保密性、完整性、可用性、可控性和不可否认性。

检测（Detect）

- 利用高级术提供的工具检查系统存在的可能提供黑客攻击、白领犯罪、病毒泛滥脆弱性。

反应（React）

- 对危及安全的事件、行为、过程及时作出响应处理，杜绝危害的进一步蔓延扩大，力求系统尚能提供正常服务。

恢复（Restore）

- 一旦系统遭到破坏，尽快恢复系统功能，尽早提供正常的服务。

常用措施

- 完善安全管理制度
- 采用访问控制措施
- 运行数据加密措施
- 数据备份与恢复
- 建立敏感的安全意识

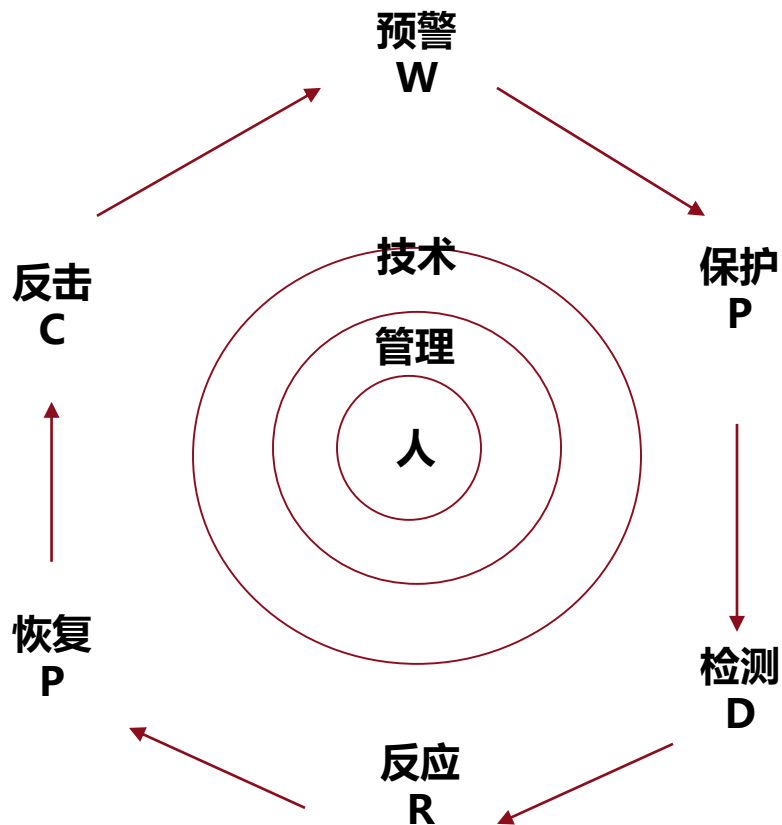
信息保障体系

- 法律与政策体系
- 标准与规范体系
- 人才培养体系
- 产业支撑体系
- 技术保障体系
- 组织管理体系

信息系统安全管理准则

- 管理策略
- 组织与人员
- 资产分类与安全控制
- 配置与运行
- 网络信息安全与通信安全
- 异常事件与审计
- 信息标记与文档
- 物理环境
- 开发与维护
- 作业连续性保障
- 符合性

信息安全管理中的地位



信息安全管理层次与内容

宏观管理（政府）

- 方针
- 政策
- 法规
- 标准

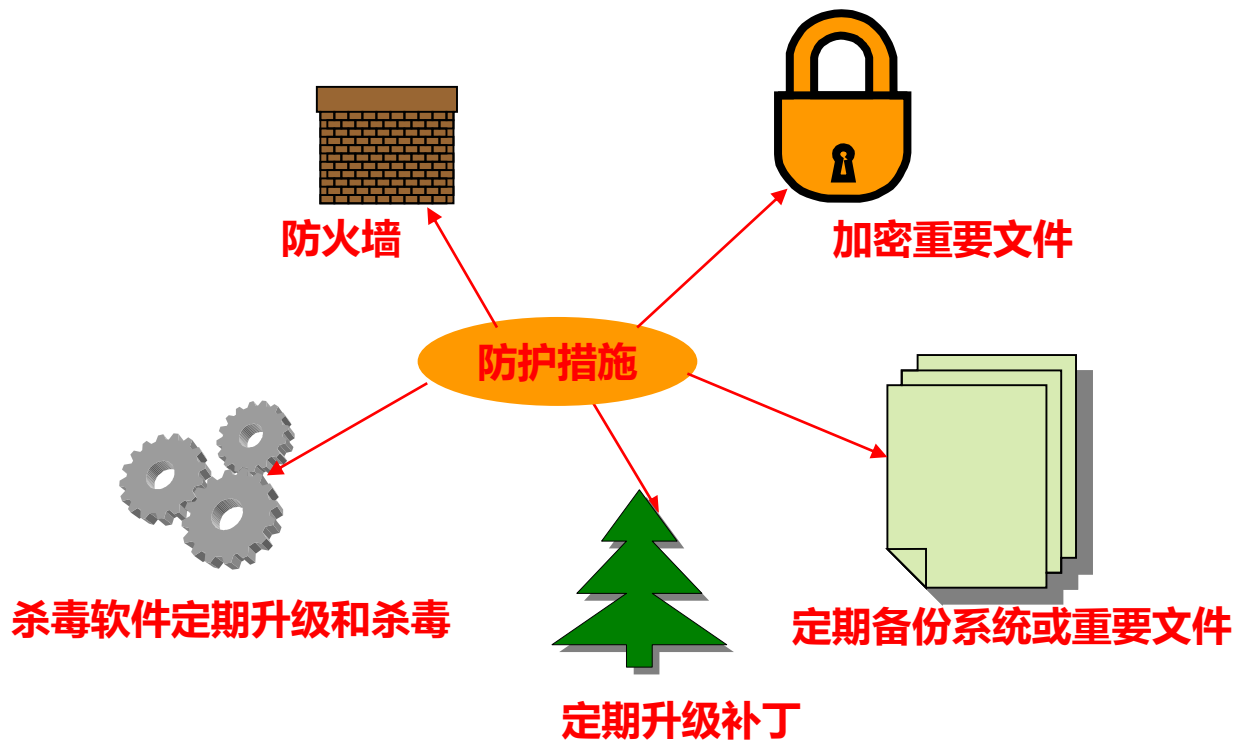
微观管理（机构）

- 规章
- 制度
- 策略
- 措施

信息安全管理的发展



个人用户防护措施



防止黑客入侵

关闭不常用程序和服务

关闭不常用端口



及时升级系统和软件补丁

发现系统异常立刻检查

课程介绍

网络安全

信息系统安全

安全策略及其原则

网络安全策略及其原则

安全策略，是针对那些被允许进入某一组织、可以访问网络技术资源和信息资源的人所规定的、必须遵守的规则。

即：网络管理部门根据整个计算机网络所提供的服务内容、网络运行状况、计算机安全状况、安全性需求、易用性、技术实现所付出的代价和风险、社会因素等许多方面因素，所制定的关于计算机安全总体目标、计算机安全操作、计算机安全工具、人事管理等方面的规定。

制定安全策略的目的

目的1 - 让所有用户、操作人员和管理员清楚，为了保护技术和信息资源所必须遵守的原则。

目的2 - 提供一个可以获得、能够配置和检查的用于确定是否与计算机和网络系统的策略一致的基准。

安全策略的必要性 - 1

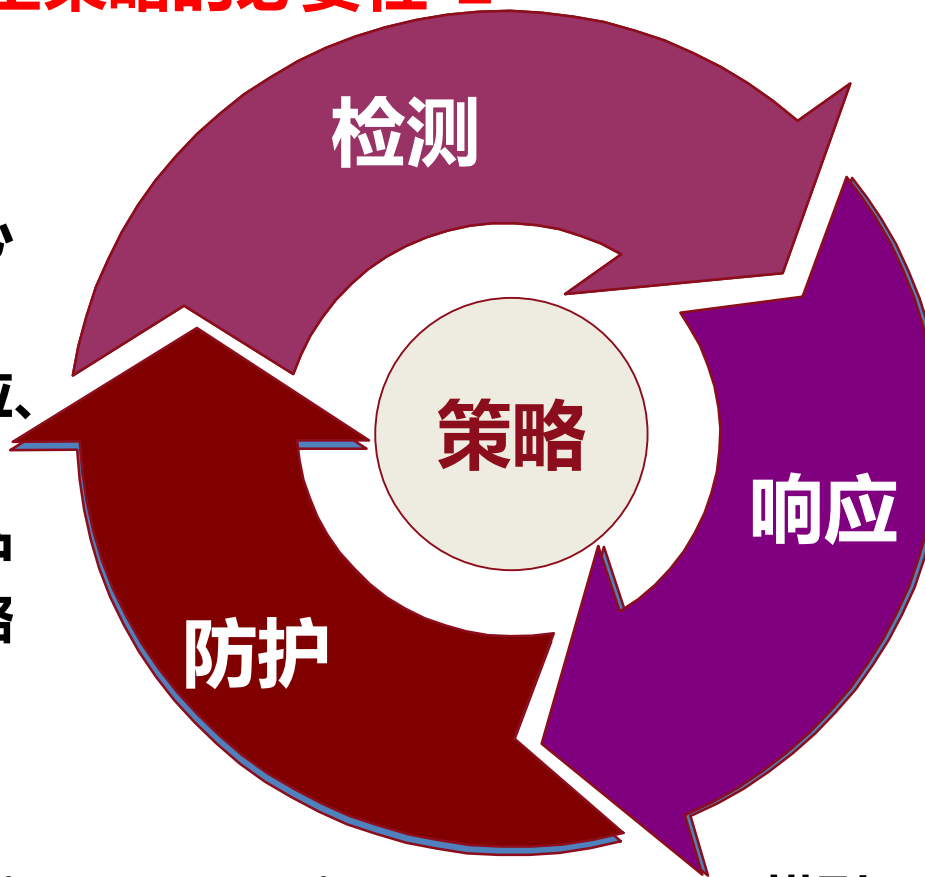
网络管理员在作安全策略时的依据，在很大程度上取决于网络运行过程中的安全状况，网络所提供的功能以及网络的易用程度。

安全策略应以要实现目标为基础，而不能简单地规定要检验什么和施加什么限制。

在确定的安全目标下，应该制定如何有效地利用所有安全工具的策略。

安全策略的必要性-2

- 强调了策略的核心作用
- 强调了检测、响应、防护的动态性
- 检测、响应、防护必须遵循安全策略进行



(Policy、Protection、Detection、Response) 模型

PPDR与PDRR区别

PDRR安全模型强调网络保护不再是简单的被动保护，而是保护、检测、响应和恢复的有机结合。因此，PDRR模型不仅包含了安全防护的概念，而且还包含了主动恢复概念。

在PDRR安全模型中检测显得非常重要的一步。检测的目的是检测网络攻击，检测本地网络中的非法信息流，检测本地网络中的安全漏洞，有效防范网络攻击。通信部分检测技术包括入侵检测技术和网络安全扫描技术。

PPDR中，所谓管理和策略的部分，仅仅列上Policy，显然不全面。比如，策略难于包含组织、运作等管理内涵。

网络安全策略的基本原则

适用性原则

可行性原则

动态性原则

简单性原则

系统性原则

适用性原则

网络的安全管理是一个系统化的工作，因此在制定安全管理策略时，应全面考虑网络上各类用户，各种设备，各种情况，有计划有准备地采取相应的策略，任何一点疏忽都会造成整个计算机安全性的降低。

可行性原则

安全管理策略的制定还要考虑资金的投入量，因为安全产品的性能一般是与其价格成正比的，所以要适合划分系统中信息的安全级别，并作为选择安全产品的重要依据，使制定的安全管理策略达到成本和效益的平衡。

动态性原则

安全管理策略有一定的时限性，不能是一成不变的。

由于网络用户在不断地变化，网络规模在不断扩大，网络技术本身的发展变化也很快，而安全措施是防范性的。

所以安全措施也必须随着网络发展和环境的变化而变化。

简单性原则

网络用户越多，网络管理人员越多，网络拓扑越复杂，采用网络设备种类和软件种类越多，网络提供的服务和捆绑越多，出现安全漏洞的可能性就越大。

因此制定的安全管理策略越简单越好，如简化授权用户的注册过程等。

系统性原则

网络的安全管理是一个系统化的工作，因此在制定安全管理策略时，应全面考虑网络上各类用户，各种设备，各种情况，有计划有准备地采取相应的策略。

任何一点疏忽都会造成整个计算机安全性的降低。

安全策略的特点

有效的安全策略都是起码应该具有以下特点：

- 发布：必须通过系统正常管理程序，采用合适的标准出版物或其他适当的方式来发布。
- 强制执行：在适当的情况下，必须能够通过安全工具来实现其强制实施，并在技术确定不能满足要求的情况下强迫执行。
- 人员责任规定：必须明确规定用户、系统管理员和公司管理人员等各类人员的职责范围和权限。

学习建议

信息安全内容广阔

- 密码学
- 网络安全
- 系统安全

涉及到许多其它领域的知识（交通、能源、生物工程等）

学习方法

- 阅读一些系统性较强的教材
- 找到经典的论文
- 案例研究

谢谢!