期末小结

主讲人：谷利泽

Email：glzisc@bupt.edu.cn

第一讲小结

- 网络空间安全的含义（本身、环境、层次）
- 网络空间安全的主要威胁都有哪些

  窃取、篡改、假冒、抵赖、破坏、中止服务、
  非授权访问、重放、流量分析、盗版、恐吓
- 网络空间安全的主要目标及相关术语解释

机密性、完整性、认证性 、不可否认性、可用性、可控性、可追踪性

“进不来” 身份认证机制 (认证)譬如口令、Ukey、指纹等，“拿不走”授权机制(访问控制譬如防火墙、基于角色授权机制等)，“看不懂” 加密机制譬如AES加解密算法等，“改不了” 完整性机制譬如消息认证码MAC等，“逃不掉” 审计和监控机制譬如数字签名、数字水印等，“打不跨” 备份及可用机制譬如数据备份等

- 了解网络空间安全发展历程（重点：信息保障）

信息保障IA(Information Assurance)的模型(PD2R)中，除了要进行信息安全保护，还应该重视提高安全预警能力、系统的入侵检测能力，系统的事件反应能力和系统遭到入侵引起破坏的快速恢复能力。

第二讲小结

明文、密文、加密算法和解密算法、密钥

- **密码系统的组成**

对称密码体制和公钥密码体制；分组密码和序列密码

- **现代密码体制的分类以及对称密码的分类**

键盘；接线板:增加密钥量(单表代换);轮子:增加加解算法复杂度(多表代换) ;反射器:使得加解密算法相同。

- **Enigma的组成及其各部分的作用**

- **实用密码设备应必备的要素**

安全、性能、成本、易用

《保密系统的通信理论》 《密码学的新方向》

- **现代密码的两次飞跃和两个里程碑事件**

美国数据加密标准（DES）的公布 第一个实用的公钥密码体制RSA

- **分组的设计思想及其含义(扩散P31,混乱P33)**

- *序列密码的特点、应用模型*

运算速度快、密钥相对比较短、没有数据扩展

- **对称密码的优缺点**

密钥分发难以实现；需秘密保存的密钥量大，难以维护；难以实现数字签名和认证的功能。

指要将算法设计成明文每一比特的变化尽可能多地影响到输出密文序列的变化，以便隐蔽明文的统计特性。形象地称为雪崩效应。

指在加解密变换过程中明文、密钥以及密文之间的关系尽可能地复杂化，以防密码破译者采用解析法(即通过建立并求解一些方程)进行破译攻击。

第三讲小结

- Diffie-Hellman(DH)密钥交换方案
- 公钥密码的基本思想
  - 发送方A查找接受方B的公钥。
  - A采用公钥加密算法以B的公钥作为加密密钥对明文加密。
  - A通过不安全信道将密文发送给B。
  - B收到密文后使用自己的私钥对密文解密还原出明文。
- RSA公钥密码的简评
- 公钥密码的加解密模型(密钥分发过程)

(P35)

- 公钥密码的优缺点

密钥分发简单、需秘密保存的密钥量少、可以实现数字签名和认证的功能。

算法运算慢、密钥位数相对比较长、有数据扩展。

第四讲小结

固定长度；正向计算容易；逆向计算不可行；

- Hash函数的性质及其安全性

  抗弱碰触性；抗强碰撞性；雪崩效应。

- Hash函数实现的基本过程

- 消息认证码的含义(目的)及实现的基本过程

  验证信息的来源是真实的
  验证消息的完整性

  P24

- 数字签名的含义及实现的的基本过程

  P33

- 数字证书包含内容及安全性

信息安全中心 BuptISC

第五讲小结

指在未经授权的情况下，在信息系统中安装、执行并达到不正当目的的软件。

可执行代码、恶意目的、强制安装、隐蔽性、破坏性

- 恶意软件的含义和特征

指编制者在计算机程序中插入的破坏计算机功能或者数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。

- 计算机病毒的含义和特点

可执行性、传染性、非授权性、寄生性、隐蔽性、衍生性、破坏性

创造期、传播期、传染期、发病期、发现期、根除期、灭绝

- 计算机病毒的生命周期和主要组成

引导模块、传染模块、表现模块

- 计算机病毒的关键点及简评

传染方式、寄生方式、激活方式

- 那些好习惯能避免计算机病毒入侵

作业4

信息安全中心 BuptISC

2. 通过本讲的学习，应该养成哪些好的习惯避免计算机病毒的入侵？

- ✓ 不要随意开放共享并且设置最大权限以及弱口令；
- ✓ 取消文件夹隐藏共享，显示文件的扩展名；
- ✓ 不要随意安装使用盗版软件或来历不明的软件；
- ✓ 谨慎下载并执行（或打开）软件或文件，尤其电子邮件的附件；
- ✓ 不要浏览一些诱惑的恶意网站；
- ✓ 及时打补丁，尤其常用系统补丁；
- ✓ 杀毒软件要及时升级，并启动监控或定期查杀；
- ✓ 养成做备份的好习惯，重要数据或文件一定要做备份；
- ✓ 时刻有网络安全意识。

第六讲小结

一种高级访问控制设备，置于不同网络安全域之间，它通过相关的安全策略来控制(允许、拒绝、记录)进出网络的访问行为。

指通过一个公共网络建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全和稳定的隧道，能提供与专用网络一样的安全和功能保障。

- 防火墙、包过滤、DMZ、VPN的含义
- 防火墙能实现的那些功能

包过滤：
- 基于源IP地址
- 基于目的IP地址
- 基于源端口
- 基于目的端口

IP与MAC的绑定
- 基于时间
- 基于流量(带宽)
- MAP(地址/端口映射)
- VPN功能
- 日志审计

- MAP的好处以及VPN实现的功能

数据保密性、数据完整性、身份认证性

- 防火墙的主要性能参数

吞吐量、时延、丢包率、并发连接数、平均无故障时间、最大允许加载规则数

- 防火墙发展的简评
- 入侵检测、漏洞扫描系统、漏洞、安全补丁的含义

对企图入侵、正在进行的入侵或已经发生的入侵进行识别的过程。

对网络和主机的安全性进行风险分析和评估的软件，是一种能自动检测远程或本地主机系统在安全性方面存在弱点和隐患的程序包。

指硬件或软件存在的的安全缺陷，从而使得攻击者能够在未授权的情况下访问、控制系统。

软件开发厂商为堵塞安全漏洞，提高软件的安全性和稳定性，开发的与原软件结合或对原软件升级的程序。

第七讲小结

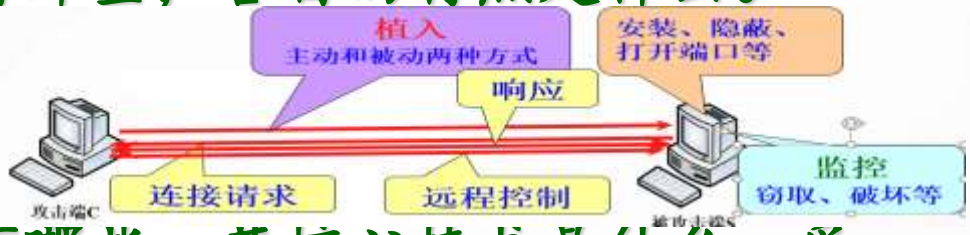
明确的对象、目标有区别、手段有差别

- 网络攻击含义以及它与病毒对比有哪些不同。P10

截取攻击(机密性)、篡改攻击(完整性)、伪造攻击(认证性)、阻断攻击(可用性)、重放攻击

- 从安全属性看，攻击类型有那些，各自的特点是什么。

- 简要描述木马攻击的过程。P22



- 木马攻击的主要实现技术有哪些，其核心技术是什么，采用方式有哪些。

植入技术、自动启动技术、隐蔽技术、远程监控技术

植入技术

主动(漏洞)、被动(欺骗或不经意)

阻止或拒绝合法使用者存取网络服务的一种破坏性攻击方式。

- DoS的含义及以TCP三次握手为例描述DoS攻击基本思想。P39

- 简要描述分布式拒绝服务(DDoS)的攻击过程。P42-47

- 简要描述APT攻击的过程

第八讲小结

身份认证的作用和意义(重要性)

1.身份认证就是确保身份的真实性，能够抵御假冒攻击。

2.身份认证是权限管理和审计等应用的基础，否则，这些应用无法实现。

3.身份认证往往是信息系统中安全保护的第一道设防，它的失败可能导致整个系统的失败。

- 信息系统自身安全的基本要素包括那些
  身份认证、访问控制、安全审计、数据备份
- 零知识证明含义
  指证明者试图使验证者相信某个论断是正确的，但却不向验证者提供任何有用的信息
- 基于Hash函数实现口令认证的好处
  明文口令不存储在任何地方；
  口令是以其散列值传输和存储，保证口令的安全性；
  系统管理员不知道终端用户口令。
- 基于Hash函数口令更改和验证的过程
- 基于Ukey的单向身份认证协议

身份认证技术：所知(口令)、所有(Ukey)、所是(指纹)

- 指纹身份认证的重要安全指标和主要方式
  错误接受率、错误拒接率
  辨识(一对多匹配)、验证(一对一对比)
- 访问控制(权限)含义和功能
- 安全审计的含义和好处

第九讲小结

自然灾害、硬件故障、软件故障、恶意代码、人为错误

- 数据安全的原因有那些；(数据为什么要备份？)
- 数据备份和数据恢复的含义；
- 数据备份的简评；

  恢复点指标RPO：指当灾难发生后，系统和数据能够恢复到的时间点要求。
- 应用恢复的主要指标是什么，其含义是什么？

  恢复时间目标RTO：是从灾难发生造成业务中断，直到使业务能够得以继续所需要的时间。
- 集中存储的好处(相比早期附属存储形式相比)；
- RAID的关键目标及RAID5的特点；
- 容灾的含义、分类及灾难的后果有哪些；
- 了解Share78 容灾国际标准分级原则及各级主要特点。

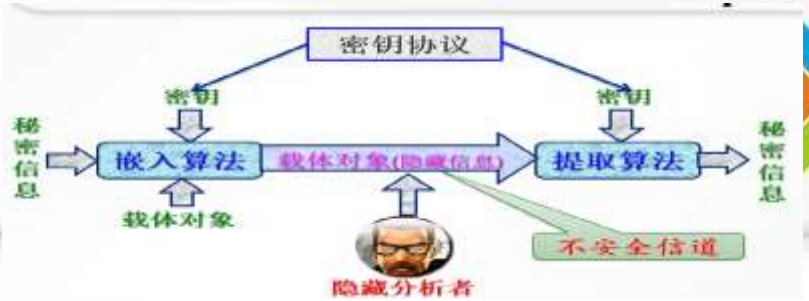
有形资产灾难(直接损失)

- ✓ 硬件系统的损毁
- ✓ 软件系统的崩溃
- ✓ 企业生产的中断

无形资产灾难(间接损失)

- ✓ 数据信息的丢失
- ✓ 业务服务的中止
- ✓ 企业信誉的受损

第十讲小结



- 隐写术(信息隐藏)技术模型以及其主要特征

  不可感知性、鲁棒性、隐藏容量

- 数字水印的含义及主要特点 透明性、鲁棒性、安全性

  永久镶嵌在其他数据（宿主数据）中具有可鉴别性的数字信号或模式，并且不影响宿主数据的可用性。

- 基于非盲水印的检测过程

- 数字水印的主要应用

- 隐写术(信息隐藏)与数字水印的主要区别

	隐写术(信息隐藏)	数字水印
载体内容	无关，一般一对一	有关，一对多
主要用途	用于保密通信	用于版权标识
前提	一般不知有信息隐藏(如果已怀疑有隐藏信息，则已经不安全)	可以公布有水印存在
主要攻击	隐写分析(分析是否正常载体)	水印擦除
主要考核	不可感知性	安全性

第十一讲小结

- 大数据下为何个人信息问题突出
- 简述应从几个方面实现个人信息防护
- 个人如何避免或减少个人信息泄露
- 社工攻击与网路攻击的对比
- 社工攻击的特点
- 个人如何预防和抵御社会工程学攻击

第十二讲小结

- 信息安全管理的主要遵循原则
- PDCA模型
- 安全技术与安全管理的关系
- 安全态势感知的含义及三个层次
- 习主席的重要讲话
- 了解安全态势感知的实现过程

网络安全和信息化是相辅相成的。安全是发展的前提，发展是安全的保障，安全和发展要同步推进。要树立正确的网络安全观，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。

英文缩写的中英文解释

DES (Data Encryption Standard) 数据加密标准

AES (Advanced Encryption Standard) 高级加密标准

RSA (Rivest, Shamir, Adleman) 公钥密码算法

MAC（Messages Authentication Code）消息认证码

DMZ （DeMilitarized Zone） 隔离区或非军事化区

VPN（Virtual Private Network）虚拟专用网

IDS (Intrusion Detection System) 入侵检测系统

IPS （Instrusion Prevention System）入侵防御系统

DDoS (Distributed Denial of Service) 分布式拒绝服务

APT (Advanced Persistent Threat) 高级持续性威胁

RAID (Redundant Array of Independent Disks) 磁盘阵列

期末考试安排(考试时间和地点)

信息安全中心
BuptISC

- 考试日期：2023.12.27(星期三)
- 考试时间：13:00至14:30(第6，7节)

  注：提前10分钟到

- 考试地点：沙河校区N104教室
- 考试方式：闭卷

答疑

信息安全中心
BuptISC