**北京航空航天大学**

计算机学院

**信息安全学习报告**

作者：周美廷\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

学号：76066002\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# 目录

[一． 信息安全概念 3](#_Toc482214849)

[1. 检测 3](#_Toc482214850)

[网站 3](#_Toc482214851)

[网络 4](#_Toc482214852)

[2. 主要威胁 5](#_Toc482214853)

[实现目标 5](#_Toc482214854)

[安全威胁 5](#_Toc482214855)

[主要来源 5](#_Toc482214856)

[3. 相关技术 6](#_Toc482214857)

[4. 目标 6](#_Toc482214858)

[二． 网络安全 8](#_Toc482214859)

[1. 主要特性 8](#_Toc482214860)

[2. 主要关系 8](#_Toc482214861)

[3. 影响因素 8](#_Toc482214862)

[4. 技术原理 9](#_Toc482214863)

[安全服务 9](#_Toc482214864)

[安全机制 9](#_Toc482214865)

[5. 操作工具 9](#_Toc482214866)

[防火墙 9](#_Toc482214867)

[安全策略 10](#_Toc482214868)

[系统安全 10](#_Toc482214869)

[电子商务 10](#_Toc482214870)

[协议安全 10](#_Toc482214871)

[6. 预防措施 11](#_Toc482214872)

[网安措施 11](#_Toc482214873)

[商交措施 12](#_Toc482214874)

[安全防范意识 12](#_Toc482214875)

[三． 加密 13](#_Toc482214876)

[1. 应用 13](#_Toc482214877)

[电子商务 13](#_Toc482214878)

[VPN 13](#_Toc482214879)

[数据安全 13](#_Toc482214880)

[加密技巧 13](#_Toc482214881)

[四． 身份识别 14](#_Toc482214882)

[1. 工作方式 14](#_Toc482214883)

[口令方式： 14](#_Toc482214884)

[标记方式： 14](#_Toc482214885)

[2. 新型身份识别技术 14](#_Toc482214886)

[五． 访问控制 15](#_Toc482214887)

[1. 访问控制实现的策略 15](#_Toc482214888)

[2. 访问控制的类型 15](#_Toc482214889)

[ 基于对象的访问控制模型 15](#_Toc482214890)

[ 基于任务的访问控制模型 15](#_Toc482214891)

[ 基于角色的访问控制模型 15](#_Toc482214892)

# 信息安全概念

*““The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards.” – Gene Spafford*

信息安全主要包括以下五方面的内容：保密性、真实性、完整性、未授权拷贝和所寄生系统的安全性。网络环境下的信息安全体系是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制（数字签名、消息认证、数据加密等），直至安全系统，如UniNAC、DLP等，只要存在安全漏洞便可以威胁全局安全。信息安全是指信息系统（包括硬件、软件、数据、人、物理环境等）受到保护，不遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。

## 检测

### 网站

网站安全检测是通过技术手段对网站进行漏洞扫描，检测网页是否存在漏洞、网页是否挂马、网页有没有被篡改、是否有欺诈网站等，提醒网站管理员及时修复和加固，保障web网站的安全运行。

1. 注入攻击检测Web网站是否存在诸如SQL注入、SSI注入、Ldap注入、Xpath注入等漏洞，如果存在该漏洞，攻击者对注入点进行注入攻击，可轻易获得网站的后台管理权限，甚至网站服务器的管理权限。
2. XSS跨站脚本检测Web网站是否存在XSS跨站脚本漏洞，如果存在该漏洞，网站可能遭受Cookie欺骗、网页挂马等攻击。
3. 网页挂马检测Web网站是否被黑客或恶意攻击者非法植入了木马程序。
4. 缓冲区溢出检测Web网站服务器和服务器软件，是否存在缓冲区溢出漏洞，如果存在，攻击者可通过此漏洞，获得网站或服务器的管理权限。
5. 上传漏洞检测Web网站的上传功能是否存在上传漏洞，如果存在此漏洞，攻击者可直接利用该漏洞上传木马获得WebShell。
6. 源代码泄露检测Web网络是否存在源代码泄露漏洞，如果存在此漏洞，攻击者可直接下载网站的源代码。
7. 隐藏目录泄露检测Web网站的某些隐藏目录是否存在泄露漏洞，如果存在此漏洞，攻击者可了解网站的全部结构。
8. 数据库泄露检测Web网站是否在数据库泄露的漏洞，如果存在此漏洞，攻击者通过暴库等方式，可以非法下载网站数据库。
9. 弱口令检测Web网站的后台管理用户，以及前台用户，是否存在使用弱口令的情况。
10. 管理地址泄露检测Web网站是否存在管理地址泄露功能，如果存在此漏洞，攻击者可轻易获得网站的后台管理地址。

### 网络

1. 结构安全与网段划分

网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；根据机构业务的特点，在满足业务高峰期需要的基础上，合理设计网络带宽；

1. 网络访问控制

不允许数据带通用协议通过。

1. 拨号访问控制

不开放远程拨号访问功能（如远程拨号用户或移动VPN用户）。

1. 网络安全审计

记录网络设备的运行状况、网络流量、用户行为等事件的日期和时间、用户、事件类型、事件是否成功，及其他与审计相关的信息；

1. 边界完整性检查

能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断；能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

1. 网络入侵防范

在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击、网络蠕虫攻击等入侵事件的发生；当检测到入侵事件时，记录入侵源IP、攻击类型、攻击目的、攻击时间等，并在发生严重入侵事件时提供报警（如可采取屏幕实时提示、E-mail告警、声音告警等几种方式）及自动采取相应动作。

1. 恶意代码防范

在网络边界处对恶意代码进行检测和清除；维护恶意代码库的升级和检测系统的更新。

1. 网络设备防护

对登录网络设备的用户进行身份鉴别；对网络设备的管理员登录地址进行限制；主要网络设备对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别

## 主要威胁

### 实现目标

* 真实性：对信息的来源进行判断，能对伪造来源的信息予以鉴别。
* 保密性：保证机密信息不被窃听，或窃听者不能了解信息的真实含义。
* 完整性：保证数据的一致性，防止数据被非法用户篡改。
* 可用性：保证合法用户对信息和资源的使用不会被不正当地拒绝。
* 不可抵赖性：建立有效的责任机制，防止用户否认其行为，这一点在电子商务中是极其重要的。
* 可控制性：对信息的传播及内容具有控制能力。

### 安全威胁

1. 信息泄露
2. 破坏信息的完整性
3. 拒绝服务（DoS，Denial　of　Service）
4. 非法使用(非授权访问)
5. 业务流分析
6. 假冒
7. 旁路控制
8. 授权侵犯
9. 特洛伊木马 (Trojan Horse)
10. 陷阱门
11. 抵赖：这是一种来自用户的攻击
12. 重放
13. 计算机病毒
14. 人员不慎
15. 媒体废弃
16. 物理侵入：侵入者绕过物理控制而获得对系统的访问。
17. 窃取：重要的安全物品被盗。
18. 业务欺骗：某一伪系统或系统部件欺骗合法的用户或系统自愿地放弃敏感信息等等。

### 主要来源

* 自然灾害、意外事故
* 计算机犯罪
* 人为错误，比如使用不当，安全意识差等
* "黑客" 行为
* 内部/外部泄密
* 信息丢失
* 电子谍报，比如信息流量分析、信息窃取等
* 信息战
* 网络协议自身缺陷，例如TCP/IP协议的安全问题等等
* 嗅探器

## 相关技术

* 用户身份认证
* 防火墙
* 网络安全隔离
* 安全路由器
* 虚拟专用网(VPN)
* 安全服务器
* 电子签证机构--CA和PKI产品
* 安全管理中心
* 入侵检测系统（IDS）
* 入侵防御系统（IPS）
* 安全数据库
* 安全操作系统
* DG图文档加密

## 目标

* 保密性(Confidentiality)是指阻止非授权的主体阅读信息。它是信息安全一诞生就具有的特性，也是信息安全主要的研究内容之一。更通俗地讲，就是说未授权的用户不能够获取敏感信息。对纸质文档信息，我们只需要保护好文件，不被非授权者接触即可。而对计算机及网络环境中的信息，不仅要制止非授权者对信息的阅读。也要阻止授权者将其访问的信息传递给非授权者，以致信息被泄漏。
* 完整性(Integrity)是指防止信息被未经授权的篡改。它是保护信息保持原始的状态，使信息保持其真实性。如果这些信息被蓄意地修改、插入、删除等，形成虚假信息将带来严重的后果。
* 可用性(Availability)是指授权主体在需要信息时能及时得到服务的能力。可用性是在信息安全保护阶段对信息安全提出的新要求，也是在网络化空间中必须满足的一项信息安全要求。
* 可控性(Controllability)是指对信息和信息系统实施安全监控管理，防止非法利用信息和信息系统。
* 不可否认性(Non-repudiation)是指在网络环境中，信息交换的双方不能否认其在交换过程中发送信息或接收信息的行为。

除了上述的信息安全五性外，还有信息安全的可审计性(Audiability)、可鉴别性(Authenticity)等。信息安全的可审计性是指信息系统的行为人不能否认自己的信息处理行为而信息安全的可见鉴别性是指信息的接收者能对信息的发送者的身份进行判定。它也是一个与不可否认性相关的概念。

# 网络安全

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

## 主要特性

* 保密性
* 完整性
* 可用性
* 可控性
* 可审查性

## 主要关系

* 全方位的安全体系：与其它安全体系（如保安系统）类似，企业应用系统的安全体系应包含：
* 访问控制：通过对特定网段、服务建立的访问控制体系，将绝大多数攻击阻止在到达攻击目标之前。
* 检查安全漏洞：通过对安全漏洞的周期检查，即使攻击可到达攻击目标，也可使绝大多数攻击无效。
* 攻击监控：通过对特定网段、服务建立的攻击监控体系，可实时检测出绝大多数攻击，并采取相应的行动（如断开网络连接、记录攻击过程、跟踪攻击源等）
* 加密通讯：主动的加密通讯，可使攻击者不能了解、修改敏感信息。
* 认证：良好的认证体系可防止攻击者假冒合法用户。
* 备份和恢复：良好的备份和恢复机制，可在攻击造成损失时，尽快地恢复数据和系统服务。

## 影响因素

* 自然灾害、意外事故；计算机犯罪； 人为行为，比如使用不当，安全意识差等；黑客” 行为
* 网络安全威胁主要包括两类：渗入威胁和植入威胁。渗入威胁主要有：假冒、旁路控制、授权侵犯；
* 植入威胁主要有：特洛伊木马、陷门。
* 陷门：将某一“特征”设立于某个系统或系统部件之中，使得在提供特定的输入数据时，允许安全策略被违反。
* 目前我国网络安全存在几大隐患：影响网络安全性的因素主要有以下几个方面。

## 技术原理

### 安全服务

* 对等实体认证服务
* 访问控制服务
* 数据保密服务
* 数据完整性服务
* 数据源点认证服务
* 禁止否认服务

### 安全机制

* 加密机制
* 数字签名机制
* 访问控制机制
* 数据完整性机制
* 认证机制
* 信息流填充机制
* 路由控制机制
* 公证机制

## 操作工具

### 防火墙

Internet防火墙能增强机构内部网络的安全性。防火墙系统决定了哪些内部服务可以被外界访问；外界的哪些人可以访问内部的哪些服务，以及哪些外部服务可以被内部人员访问。

### 安全策略

安全策略建立全方位的防御体系，甚至包括：告诉用户应有的责任，公司规定的网络访问、服务访问、本地和远地的用户认证、拨入和拨出、磁盘和数据加密、病毒防护措施，以及雇员培训等。所有可能受到攻击的地方都必须以同样安全级别加以保护。

### 系统安全

操作系统的安全控制：如用户开机键入的口令（某些微机主板有“ 万能口令” ），对文件的读写存取的控制（如Unix系统的文件属性控制机制）。

网络接口模块的安全控制。在网络环境下对来自其他机器的网络通信进程进行安全控制。主要包括：身份认证，客户权限设置与判别，审计日志等。

网络互联设备的安全控制。对整个子网内的所有主机的传输信息和运行状态进行安全监测和控制。主要通过网管软件或路由器配置实现。

### 电子商务

电子商务安全从整体上可分为两大部分：计算机网络安全和商务交易安全。

1. 计算机网络安全的内容包括：
2. 未进行操作系统相关安全配置
3. 未进行CGI程序代码审计
4. 拒绝服务（DoS，Denial　of　Service）攻击
5. 安全产品使用不当
6. 缺少严格的网络安全管理制度
7. 计算机商务交易安全的内容包括：
8. 窃取信息
9. 篡改信息
10. 假冒
11. 恶意破坏

### 协议安全

* TCP/IP协议数据流采用明文传输
* 源地址欺骗（Source address spoofing）或IP欺骗（IP spoofing）
* 源路由选择欺骗（Source Routing spoofing）
* 路由选择信息协议攻击（RIP Attacks）
* 鉴别攻击（Authentication Attacks）
* TCP序列号欺骗（TCP Sequence number spoofing）
* TCP序列号轰炸攻击（TCP SYN Flooding Attack），简称SYN攻击
* 易欺骗性（Ease of spoofing）

## 预防措施

### 网安措施

1. 保护网络安全
2. 全面规划网络平台的安全策略
3. 制定网络安全的管理措施
4. 使用防火墙
5. 尽可能记录网络上的一切活动
6. 注意对网络设备的物理保护
7. 检验网络平台系统的脆弱性
8. 建立可靠的识别和鉴别机制
9. 保护应用安全。

保护应用安全，主要是针对特定应用（如Web服务器、网络支付专用软件系统）所建立的安全防护措施，它独立于网络的任何其他安全防护措施。虽然有些防护措施可能是网络安全业务的一种替代或重叠，如Web浏览器和Web服务器在应用层上对网络支付结算信息包的加密，都通过IP层加密，但是许多应用还有自己的特定安全要求。

由于电子商务中的应用层对安全的要求最严格、最复杂，因此更倾向于在应用层而不是在网络层采取各种安全措施。

虽然网络层上的安全仍有其特定地位，但是人们不能完全依靠它来解决电子商务应用的安全性。应用层上的安全业务可以涉及认证、访问控制、机密性、数据完整性、不可否认性、Web安全性、EDI和网络支付等应用的安全性。

1. 保护系统安全。
2. 在安装的软件中，如浏览器软件、电子钱包软件、支付网关软件等，检查和确认未知的安全漏洞。
3. 技术与管理相结合，使系统具有最小穿透风险性。如通过诸多认证才允许连通，对所有接入数据必须进行审计，对系统用户进行严格安全管理。
4. 建立详细的安全审计日志，以便检测并跟踪入侵攻击等。

### 商交措施

1. 加密技术
2. 对称加密

对称加密又称私钥加密，即信息的发送方和接收方用同一个密钥去加密和解密数据。

1. 非对称加密

非对称加密又称公钥加密，使用一对密钥来分别完成加密和解密操作，其中一个公开发布（即公钥），另一个由用户自己秘密保存（即私钥）。

1. 认证技术
2. 数字签名

数字签名如同出示手写签名一样，能起到电子文件认证、核准和生效的作用。

1. 数字证书

数字证书是一个经证书授权中心数字签名的包含公钥拥有者信息以及公钥的文件数字证书的最主要构成包括一个用户公钥，加上密钥所有者的用户身份标识符，以及被信任的第三方签名第三方一般是用户信任的证书权威机构（CA），如政府部门和金融机构。

1. 电子商务的安全协议。
2. 安全套接层协议SSL。

SSL协议位于传输层和应用层之间，由SSL记录协议、SSL握手协议和SSL警报协议组成的。

1. 安全电子交易协议SET。

SET协议用于划分与界定电子商务活动中消费者、网上商家、交易双方银行、信用卡组织之间的权利义务关系，给定交易信息传送流程标准。

### 安全防范意识

1. 主机安全检查
2. 主机物理安全

如果服务器只能放在开放式机架的机房，那么可以这样做：

1. 将电源用胶带绑定在插槽上，这样避免别人无意中碰动你的电源；
2. 安装完系统后，重启服务器，在重启的过程中把键盘和鼠标拔掉，这样在系统启动后，普通的键盘和鼠标接上去以后不会起作用(USB鼠标键盘除外)
3. 跟机房值班人员搞好关系，不要得罪机房里其他公司的维护人员。这样做后，你的服务器至少会安全一些。

# 加密

## 应用

### 电子商务

现在人们开始用RSA（一种公开/私有密钥）的加密技术，提高信用卡交易的安全性，从而使电子商务走向实用成为可能。

许多人都知道NETSCAPE公司是Internet商业中领先技术的提供者，该公司提供了一种基于RSA和保密密钥的应用于因特网的技术，被称为安全插座层（Secure Sockets Layer，SSL）。

也许很多人知道Socket，它是一个编程接口，并不提供任何安全措施，而SSL不但提供编程接口，而且向上提供一种安全的服务，SSL3.0现在已经应用到了服务器和浏览器上，SSL2.0则只能应用于服务器端。

### VPN

现在具有加密/解密功能的路由器已到处都是，这就使人们通过互联网连接这些局域网成为可能，这就是我们通常所说的虚拟专用网（Virtual Private Network ，VPN）。当数据离开发送者所在的局域网时，该数据首先被用户端连接到互联网上的路由器进行硬件加密，数据在互联网上是以加密的形式传送的，当达到目的LAN的路由器时，该路由器就会对数据进行解密，这样目的LAN中的用户就可以看到真正的信息了。

### 数据安全

现在电脑已经进入千家万户，并且在商业办公中起着不可替代的作用。电脑中保存的重要数据和机密的数据的安全已经成为所有电脑使用者十分重视的问题。无论是个人的电脑数据或公司的电脑数据，如果一旦泄密，造成的损失和影响将是巨大的。

### 加密技巧

1. 不要使用老的加密算法
2. 使用企业支持的最长的加密密钥
3. 多层加密
4. 安全存储加密密钥
5. 确保正确实施加密
6. 不要忽视外部因素

# 身份识别

## 工作方式

### 口令方式：

原则：

1. 容易记忆；不易猜中；不易分析。
2. 口令管理可通过单项函数来解决，即计算机不存储口令，只存储口令的单项函数，其识别过程如下：
3. 用户将口令传送给计算机；
4. 计算机完成口令单向函数值的计算。
5. 计算机把单向函数值和机器存储值比较。

### 标记方式：

标记是一种个人持有物，它的作用类似于钥匙，用于启动电子设备，标记上记录着用于机器识别的个人信息。

## 新型身份识别技术

1 远距离指纹扫描

2 耳朵

3 气味

4 心跳

5 声音

6 虹膜

7 眼周区域

8 步态

9 汗液

10 先进脸部识别系统

# 访问控制

## 访问控制实现的策略

* 入网访问控制
* 网络权限限制
* 目录级安全控制
* 属性安全控制
* 网络服务器安全控制
* 网络监测和锁定控制
* 网络端口和节点的安全控制
* 防火墙控制

## 访问控制的类型

### 基于对象的访问控制模型

基于对象的访问控制（OBAC Model：Object-based Access Control Model）：DAC或MAC模型的主要任务都是对系统中的访问主体和受控对象进行一维的权限管理。当用户数量多、处理的信息数据量巨大时，用户权限的管理任务将变得十分繁重且难以维护，这就降低了系统的安全性和可靠性。

### 基于任务的访问控制模型

基于任务的访问控制模型（TBAC Model，Task-based Access Control Model）是从应用和企业层角度来解决安全问题，以面向任务的观点，从任务（活动）的角度来建立安全模型和实现安全机制，在任务处理的过程中提供动态实时的安全管理。

### 基于角色的访问控制模型

基于角色的访问控制模型（RBAC Model，Role-based Access Model）：RBAC模型的基本思想是将访问许可权分配给一定的角色，用户通过饰演不同的角色获得角色所拥有的访问许可权。这是因为在很多实际应用中，用户并不是可以访问的客体信息资源的所有者（这些信息属于企业或公司），这样的话，访问控制应该基于员工的职务而不是基于员工在哪个组或是谁信息的所有者，即访问控制是由各个用户在部门中所担任的角色来确定的，例如，一个学校可以有教工、老师、学生和其他管理人员等角色。