《信息安全导论》课程报告（一）

——副标题

|  |  |  |
| --- | --- | --- |
| 小组成员 | 学 号 | 分 工 |
|  |  |  |
|  |  |  |
|  |  |  |
| 杨扬 | 2020340106014 | 写报告 |

**摘 要**：

自21世纪以来，由于计算机系统的高速发展，用户借由互联网构建起巨大的网络空间；互联网的形成为攻击者创造了绝佳的入侵条件，因此，信息安全正在变得越来越重要。本文通过给出信息和信息安全的定义并介绍信息安全的历史，以期让读者对信息安全这一概念产生系统性认知。

关键词：计算机，信息，信息系统，互联网，信息安全

（正文格式不限，要求格式规范，正文字数不少于2000字，强调对调研问题的分析，必须给出针对性的总结）

# 什么是信息安全

香农的经典理论指出，信息是用来消除不确定性的东西。我们可以认为，在人类社会中传播的有价值的东西都是信息。

信息因为其消除不确定性的性质，需要确保其在传输过程中不受破坏、更改和泄露——由此产生了保护信息传输的学科，即信息安全。经过多年发展，信息安全学科产出了入侵检测技术，数字签名技术，信息加密技术等一系列成果，其目的是保护信息的保密性、完整性、可用性、可控性和不可否认性。

息传输的学科，即信息安全。经过多年发展，信息安全学科产出了入侵检测技术，数字签名技术，信息加密技术等一系列成果，其目的是保护信息的保密性、完整性、可用性、可控性和不可否认性。

# 信息安全学科发展史

## 信息安全的起源——古代密码学

信息是用来消除不确定性的东西，信息安全学科是关于保护/窃取信息的学科。信息安全自古有之，古代的政治领袖就已经在使用信息安全技术保证内部通讯不被泄露——最广为人知的例子是发明了凯撒密码的凯撒大帝。凯撒密码是一种最简单的加密方式，仅仅改变了字母排列顺序；但事实证明它是有效的，凯撒的敌人从未破译过凯撒密码，而历史上记载最早的破解凯撒密码的记录存于凯撒死后九百多年——阿尔肯迪的频率分析著作。

生活在21世纪的我们知道，加密信息所需要的数学知识极高，脱离了古代人所掌握的范畴。因此，古代人的信息安全水平较差，与之密切相关的密码学也仅堪称作起源。

## 信息安全的发展——从古代到现代

随着科学技术的发展，人类社会在步入近现代的同时逐步建立起了密码学这一学科，并且借助其他学科的发展成果，最终建立起了现代信息安全学科。

### 古代信息安全

在古代，并不存在现代的信息系统概念。因此古代的信息安全主要围绕密码学展开。

从古代的单表置换密码，人们改造出了多表置换密码这一加/解密方式；值得一提的是，在古代与近代，密码学并未步入社会，仅仅在战争中被大规模应用。

随着电子密码机的出现，密码学第一次迎来了大规模应用，它的发展也随之大大加快。然而此时的密码学还不能被称为一门科学，直到1949年香农将信息论引入密码，奠定了密码学的理论基础。自70年代开始，我们所熟知的DES标准与RSA体系公之于世，后者较高的保密性创造了巨大的价值。

除了加密/解密以外，密码学还衍生出了诸如散列算法一类用于校验的成果。值得一提的是，这些成果也为巩固信息系统安全做出了很大贡献。

### 现代信息安全

步入信息时代，信息往往由信息系统管理与传输。围绕“保护信息系统”这一命题，现代信息安全学得到了深刻发展。

#### 信息系统与其受到的威胁

信息系统是由各种软硬件组成的，以处理信息流为目的的系统。它掌管信息的输入、输出与处理，在信息流通过程中扮演主要角色。然而，因为信息具有价值，信息系统不断受到来自内外的威胁，导致信息泄露、更改和破坏，影响系统运行。

1903年，英国发明家Ambrose Fleming当众入侵了由Guglielmo Marconi发明的一台安全性极高的电报装置，篡改了接收器接受的内容，使其对着观众播放粗鄙之语。这是近代发生的第一次接近现代人认知的“黑客入侵”事件。

自20世纪90年代开始，人类社会逐渐步入信息化时代。互联网这一概念出现，并大大加速了信息流通的速度，确保了信息的时效性不受损。与此同时，随着互联网的发展，针对现代计算机系统的危险也随之出现。在互联网时代的初期，计算机系统的防护措施往往做得很差——直接修改中断向量表，替换操作系统或BIOS提供的中断服务程序（篡改运行中的操作系统内核），以使自己的程序代码藏身中断向量区、在条件合适时可以继续执行的TSR技术（即程序终止驻留内存技术），在当时竟然是普通软件的必修技术之一。以2021年的观念来审视这些DOS系统时代的程序，DOS系统无疑是不合格的——安全防护基本没有，普通软件堪比病毒。运行于这种载体上的信息系统，完全做不到保密，所以上一个时代的网民或多或少体验过病毒泛滥的痛苦。

上述的案例展示了信息系统可能遇到的威胁。我们可以将信息系统所受的威胁总结为以下几类：

信息泄露，信息完整性破坏，越权访问，洪水攻击，物理破坏，假冒凭证

新的技术带来了新的问题，也带来了新的解决方案——数字签名、权限控制、访问过滤等新技术。

#### 数字签名、权限控制与访问过滤

上文中提到，随着密码学发展，产生了一种叫做散列函数的映射。数字签名，指代利用散列函数确保信息传输完整的技术，具体细节如下：

发送者将原文用私钥通过散列函数加密后发给接收者，接收者用散列函数加密原文后与公钥解密后的原文对比，从而确认信息完整与否。

权限控制是用于应对上文中诸如DOS时代计算机病毒行为的一类越权操作的解决方案。现代操作系统（2021年）多采用带有权限控制的文件系统，以免计算机病毒越权执行恶意操作。

访问过滤指禁止特定连接者连接到信息系统内，包括内容过滤、用户过滤等不同机制，往往和权限控制体系一同部署，用于确保只有该访问系统的用户能够访问，隔绝入侵者。最高级别的访问过滤即物理隔离，可以避免绝大多数的非法访问。

## 总结

基于飞速发展的密码学理论与计算机科学，人类已经能构建可靠性和安全性较高的信息系统。随着信息科学的发展，信息安全科学的发展必定大大加速，进入新的阶段。