****

**信息技术导论·论文**

**专 业 年 级 2015级软件工程**

**课 程 名 称 信息技术导论**

**指 导 教 师 周桂贤**

**学 生 姓 名 陈 涛**

**学 号 20150107030127**

**日 期 2015.12.16**

**成 绩 96**

**教务处制**

**2015年12月16日**

信息系统现状与防护

2015级、软件工程、陈涛、20150107030127

摘要

随着信息技术产业的蓬勃发展，各行各业在信息技术的需求不断增强，在信息化应用方面的要求也在不断提高,信息网络覆盖面也越来越广；利用计算机网络技术可以很好的完成各项工作的用途越来越多，它可以实现无纸化办公,大大地提高了工作的效率。但是,在信息化技术带来便利的同时,各种的网络与信息系统安全问题也逐渐浮出水面,下面本文将结合实际中，信息系统常出现的各种安全隐患，针对系统安全问题做一些探讨。

关键字：信息系统安全，信息技术

1. 信息系统安全的现状

信息系统安全主要是指保障计算机及相关配套设施安全，信息安全性，运行环境安全性，计算机功能的正常发挥，以维护计算机信息系统的安全运行。

据调查显示，欧美等各国在网络安全建设方面投入的资金占网络建设资金的10%左右，而日韩两国则是占8%。总的来看，西方国家网络基础设施的建设比中国完善，发生的网络攻击问题也比中国严重，这也导致这些国家对网络安全问题有更全面的认识和足够的重视，但在全世界范围来看，现代的网络安全建设脚步仍然跟不上现代科技发展和安全危害的更新速度。国外信息安全现状具有以下特点：

(1)各行各业越来越认识到网络安全的重要性，并且意识到安全的必要性，将其作为一项重要工作。

(2)各行业对于网络安全的资金不断增长，而且均明显高于国内水平。据05年全国各行业对网络安全技术的应用状况数据，在各类网络安全技术使用中，“防火墙”的使用率最高(占76.5%)，其次为“防病毒软件”的应用(占53.1%)。05年较04年相比加大了其他网络安全技术的投入。防火墙的使用比例较高最主要是它价格比较便宜、容易安装，并且可在线升级等特点。值得注意的是，05年事业单位对“使用用户名和密码登陆系统”、“业务网和互联网进行物理隔离”等措施非常重视。其他防范措施的使用也比04年都提高了一定比例，对网络安全和信息的保护意识也越来越高。据调查结果，我国在网络安全建设方面投入的资金还不到网络建设资金总额的1%，远低于欧美国家。目前我国的企业对于网络安全这种看不到实在回馈的资金投入普遍表现出不积极的态度。另外，企业经营者对安全性问题经常会抱有侥幸心理，加上缺少专门的技术人员的专业指导，致使我国企业目前的网络安全建设情况参差不齐，都处于不容乐观的状况。

二、信息安全的构造

在不同时期人们对信息安全的理解是不同的，但大概应该包括以下含义：

1. 信息可靠性：信息可靠性是指网络信息系统能够在规定时间内和规定条件下完成规定功能的特性。说到可靠性，信息的可靠性它是系统安全的最基本要求，它也是是构建和维持网络信息系统的目的。
2. 信息可用性：说道信息可用性，它是指保证信息确实能为授权使用者所用，即保证合法用户在需要时可以使用所需信息。

它在网络因为部分受损或需要降级使用时，仍然能够为合法用户提供有效信息的性质。它是用户接收网络信息系统的安全性能。

1. 信息完整性：信息完整性是指信息在存储或传输过程中保持不被修改、不被破坏、不被插入、不延迟、不乱序和不丢失的特性，保证真实的信息从真实的信源无失真地到达真实的信宿。

完整性就是一种面向信息的安全性，其要求保持信息的原样，就是信息正确的生成、正确的存储和传输。

1. 信息保密性：指严密控制各个可能泄密的环节，使信息在产生、传输、处理和存储的各个环节中不泄漏给非授权的个人和实体。

保密性是建立可靠性和可用性的基础之上，但有与其不同，不同之处在于它只是一种安全性手段。

1. 信息不可抵赖性：即指保证信息行为人不能否认自己的行为。

又称作不可否认性。不可抵赖性包括对自己行为的不可抵赖及对行为发生的时间的不可抵赖。通过进行身份认证和数字签名可以避免对交易行为的抵赖，通过数字时间戳可以避免对行为发生的抵赖，也可通过对发送的消息进行数字签名来实现信息的不可抵赖性。

1. 信息可控性：指信息和信息系统时刻处于合法所有者或使用者的有效掌握与控制之下。是对信息内容及传播具有控制能力的性质。除此之外，信息安全还包括身份认证、安全协议、鉴别、可靠性等。

信息安全的概念和内涵是不断发展和演变的，尤其是安全具有相对性，随着信息技术及相关技术的发展，人们对安全的形式、方式、意义等的认识都会发生改变。因此，要从动态方面来看待这个问题。

三、信息系统的安全需求

信息系统本身的一些脆弱性，如信息资源的分布性、流动性大，系统所存储与处理的数据高度集中、具有可访问性，信息技术专业性强、隐蔽性程度高，系统内部人员的可控性低，等等。以上缺点在信息系统的运行中容易引发各种各样的危险，对其安全性构成了潜在的威胁。

1、用户身份验证：系统要对进入者的身份进行确认是不是合法的。

2、存取访问控制。系统必须清楚知道合法用户对不同资源拥有怎样的使用权利。

3、信息交换的有效性和合法性。经过以上的身份验证，得知信息交换的双方要对对方的身份进行鉴别以确定信息的有效及合法。不能抵赖、否认收到或发过信息，更不能对信息进行随意删改或伪造；

4、软件和数据的完整性。信息系统的软件和数据不可非法复制、修改或破坏，并且要保证其真实性和有效性。

5、加密。是以某种特殊的算法改变原有的信息数据，使得未授权的用户即使获得了已加密的信息，但因不知解密的方法，仍然无法了解信息的内容。 在航空学中，指利用航空摄影像片上已知的少数控制点，通过对像片测量和计算的方法在像对或整条航摄带上增加控制点的作业。

6、监理。为防止系统出现差错而采取的预防性措施。

7、审计。就是要求对使用系统资源、涉及信息安全的有关操作，应有一个好的审计过，保证不出错。

8、防病毒。要能防止病毒感染。

9、防辐射。要防止电磁辐射被对手拦截后获取信息。

10、防灾。信息系统的灾害主要指火灾、水灾、风灾和地震等自然灾害和恐怖活动、电力中断、网络中断、软硬件出错等人为灾害。

四、信息系统安全的治理

随着信息系统的广泛建立和各种不同网络的互联互通，人们意识到，不能从单个安全功能、单个网络来孤立的、个别的考虑安全问题，而必须从体系结构上系统的、全面地考虑安全管理。也就是说，必须从全局上来治理。按照系统的观点，信息系统安全追求并强调均衡性，因而各项因素管理要互相协调，不能重此轻彼，这就是信息系统安全地综合性原则。要想有效地保护信息安全技术、组织机构与人事管理、信息安全法制建设等方面采取综合治理措施。

1、技术管理

 1）防火墙技术

防火墙是指设置在不同网络或网络安全域之间的一系列部件的组合。它是不同网络或网络安全域之间信息的唯一出入口，能根据企业的安全政策控制出入网络的信息流，且本身具有较强的抗攻击能力。它是提供信息安全服务，实现网络和信息安全的基础设施。

2）身份认证

身份认证是指计算机及网络系统确认操作者身份的过程。目前常见的身份认证方式主要有三种，第一种是使用用户名加口令的方式;第二种是生物特征识别技术(包括指纹、声音、手迹、虹膜等)；第三种也是现在电子政务和电子商务领域最流行的身份认证方式。

2.组织管理

对于任一级别地信息系统，都应有相应级别的、负责信息安全的专门管理机构。

3. 法律保障

信息系统的安全问题的解决最终还是要依靠法制的保障，因此，有必要通过法制手段制定有关的法律规范，强制的贯彻实施信息安全技术与安全管理等措施，保护信息系统的资源不受侵害。

五、总结

信息系统安全管理必须综合考虑各方面的安全问题，全面分析整个系统，信息系统本身存在着来自人文环境、技术环境和物理自然环境的安全风险，其安全威胁无时无处不在。所以，信息系统的运行管理工作应该由一个专门的信息管理机构负责，在一套完整的操作规范与管理规范的约束下，靠全体管理与使用信息系统的人员共同来完成。运行管理的目标是使信息系统在一个预期的时间内能正常地发挥其应有的作用，维护好信息安全，达到应有目的。

参考文献：

[1]额大伟、王兆明.《信息技术导论》.高等教育出版社

[2]陈忠文、麦永浩.《信息安全标准与法律法规》.武汉大学出版社

[7]程胜利、谈冉、熊文龙、程煌.《计算机病毒及其防治技术》清华大学出版社

评语：选题能结合信息系统的现状提出如何进行防护的看法，有现实的理论依据和指导意义，论文结构完整，从如今的现状到如何进行防护做了清晰的阐述。写作认真，文字通顺，反映出作者有良好的信息学科理论知识基础。

附录







