计算机信息安全问题及解决对策

文◆广州番禺职业技术学院　王双庆

引言

信息安全的保护方法多种多样，通过合理构造防火墙或者信息加密等有效措施，有利于保证系统的正常运行，确保系统的信息安全。

1 通信计算机信息安全定义

通信计算机信息安全是指以多种电磁波的形式，在计算机信息系统中对资料进行整理和统计的过程。通信计算机信息安全本质是保证系统资料的正确性和稳定性，防止被窃取和篡改等。通信计算机信息安全隐患不仅损害个人利益，还为政府部门、企业单位等机构带来重大损失，甚至破坏国家安全和秩序。

2 计算机信息安全主要问题

2.1 传统安全工具遗漏系统后门的安全防范

传统的安全分析方法往往忽视了系统中存在的安全漏洞，致使防火墙无法有效防范网络攻击。以 ASP 源代码为例，在 IIS 服务器 4.0 之前，ASP 源代码已出现，这是设计者在设计 IIS 服务器时为用户留了一个后门，任何人都能从因特网上获取 ASP 源代码，从而对系统进行攻击。因为攻击方式与普通网络访问的过程非常类似，所以防火墙难以发现攻击行为，为通信计算机信息安全造成隐患。

2.2 非法入侵行为

犯罪分子为了窃取用户的秘密信息，非法入侵用户的计算机系统，修改和破坏系统，严重威胁了计算机信息安全，影响了系统的正常运行。例如，在企业系统中，目前大部分企业实行了信息化，企业的生产和经营数据已完成系统上传，一旦发生企业系统遭受恶意攻击事件，那么企业的核心数据就会被泄露、修改和破坏，对企业的生产运营造成不利影响 [1]。

2.3 通信计算机技术方面存在的漏洞

（1）计算机系统弱点问题。计算机系统弱点是较为普遍的一种现象，即计算机系统本身的设计存在缺陷。虽然漏洞问题没有对信息安全产生直接影响，但在系统运行时会受到木马或黑客攻击，导致信息泄漏。重则使整个电脑系统瘫痪，轻则使用户遭受重大损失。

（2）计算机在运行中缺乏容错和灾难恢复的能力。当出现故障或受到外界损害时，系统无法进行自我调整与自我修复，造成信息损失。

（3）网络风险。网络风险是一种高度随机行为，当计算机和其他节点进行数据交互的时候，木马病毒“趁虚而入”入侵系统，导致用户信息的损失。

2.4 缺乏系统的安全应对措施

（1）虽然计算机网络安全问题得到了充分关注，但针对这一问题的对策却十分有限。许多措施仅是一种警告和宣传，没有真正实现落地执行。

（2）管理机制不健全。由于相应的制度与规范不健全，运营商在软硬件开发过程中未全面考虑用户的使用安全问题，只注重经济效益，在没有安全保障的前提下，仍允许电子产品或服务投入使用，给用户的信息安全带来了潜在的风险。

（3）缺乏相应的技术支持。计算机信息安全问题应对策略地制定，具有较强的专业性和技术性。然而，国内缺乏这一领域的人才，因此造成了计算机网络的安全保障缺少相应的人员支持 [2]。

作者简介：王双庆（1980—），男，湖南衡阳人，硕士研究生，研究方向：计算机。

2.5 计算机信息安全管理人员专业能力较差

由于信息技术的快速发展，网络环境越来越复杂，管理工作的难度也越来越大，因此必须配备专业能力强、技术水平高的技术团队。然而，大部分企业的网络信息管理部门人员水平有限，专业知识不扎实，专业技术不过关，且企业对于专业人才培养的不重视，导致计算机信息安全管理工作开展困难，为计算机信息安全提出了更严峻的挑战。

3 计算机信息安全问题应对措施

3.1 加强网络秩序建立

要想大幅度提高信息系统的安全水平，就必须保证其具有有序性。首先，相关部门根据网络发展和运行过程中的实际状况，制订有针对性的管理机制，并对现行制度的缺陷进行全方位改进，充分发挥制度体系的约束和规范功能，监督网络使用者正常、有序的上网行为。其次，安全健康网络环境，不仅需要管理者充分发挥职责，还需要所有的网络使用者参与进来，只有增强网络使用者的安全意识和自我约束能力，才能使信息安全得到有效保障，同时进一步提高管理工作的质量和效率。最后，建立健全审查与奖惩机制，在增加审核次数和强度的基础上，对违反法律法规的行为作出有效的惩戒措施，对遵守网络秩序的行为给予奖励，激发公众的积极性和主动性，共同维护网络安全。

3.2 优化计算机访问控制技术

工作人员应定期开展系统升级工作，建立健全访问控制机制，保证系统的正常运转。加大对用户访问信息的审核力度，增加接入请求阻截机制，将非法入侵行为扼杀于萌芽状态。当系统收到用户的访问请求时，必须对其进行充分审查，以防止不正当的手段对系统进行访问。此外，网络系统访问机制应定期优化，提高网络系统对访问请求的辨别能力，及时拦截违规访问和不明访问等行为，为网络系统中的各项信息提供安全保障。

3.3 提高计算机远程网络通信的速率

一方面，企业应购置先进的计算机通信技术设备，引入先进的计算机软件，定期对计算机硬软件系统进行优化升级，提升网络信息通信的效率与稳定性，有效处理信息在传输中产生的信息畸变、信息延时等问题。另一方面，全方位升级改造通信生产企业经营模式，为计算机远程网络通信服务业提供优质的软硬件设施，确保网络信息通信的速率与质量。企业应构建一套更科学、更完善的计算机远程网络通信服务链条，完善计算机通信技术中的缺点，有效提升信息传输的稳定性与可靠性[3]。

3.4 数据加密管理

（1）通信密码。利用 SSL/TLS 等保密通信协议以及加密信道，对数据进行加密保护。SSL/TLS 采用公开密钥加密与对称加密相结合的方法进行保密通信。用户端与伺服器“握手”时，密码运

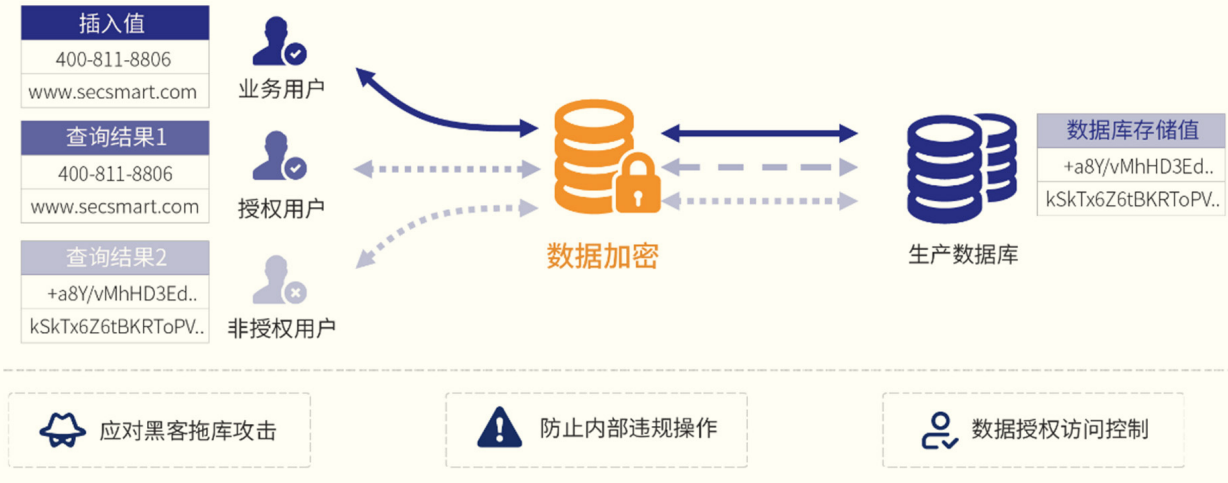

图 1 数据加密逻辑图

算法则与金钥资讯会被交换。服务器将公开密钥发给客户，然后客户再用这个公开密钥对其进行加密，只有服务器才能将其解密，保证了通信的保密性。在“握手”结束之后，SSL/TLS 就会创建一个加密信道，利用对称密码算法对全部的数据进行加密。即使资料信息被监听，攻击者也不能了解资料的具体内容。此外，SSL/TLS 还提供了一种基于 MAC 的数据完整性检验机制，见图 1。

（2）认证和授权。认证和授权机制是保障计算机信息安全的重要手段，它可以有效对用户进行认证，并对其进行授权。ACL 是一种通用的认证和授权机制，根据使用者的识别与使用权限等级定义存取权限。设定 ACL 将敏感资料仅由被授权的使用者存取，采用公开密钥加密的方式，将用户的标识和公共密钥相结合，通过认证的方式验证用户身份。双重认证需要附加的认证要素，如移动电话认证、指纹认证或者硬件认证，以增强系统的安全性，降低被窃听的风险。

3.5 强化反病毒能力

电脑信息的安全水平在很大程度上依赖于系统的防病毒功能，为了确保信息安全，在计算机系统和程序中安装防火墙。首先，要想提高防火墙的防病毒能力，软件工程师必须理解和熟悉当前各类病毒的特征、攻击规律和入侵原理等，进一步开发出具有针对性的防御杀毒程序，并定期对防火墙进行改进和优化[4]。其次，由于病毒本身具有复制和伪装的特点，因此，软件工程师在构建防火墙时，应加强对动态监视、伪装识别等功能的关注。最后，由于互联网技术的飞速发展，病毒的种类越来越多，给计算机信息系统带来的威胁也越来越大，这就要求网络安全管理者应时刻保持高度的警觉，增强对病毒及其隐患的敏感度，将病毒带来的损失降到最低。

3.6 加大对计算机信息安全管理人员的培养力度

科技人才是保障网络信息系统安全的重要力量，因此，应提高计算机信息安全管理部门工作人员的专业素养，建设一支强有力的人才队伍。首先，解决计算机网络人才教育滞后的问题，在经费、师资等方面加大投入，并与先进的教学方式相结合，以市场需求为培养对象，以学生为中心，进行教学工作，从而更好地提升教学效果，使本专业的学生得到全面发展，打造出一批优质的人才资源。其次，企业在招聘人才的过程中，要提高选拔标准，不仅要重视求职者的学历，还要对求职者的实践经验、应用能力、技术水平、理论知识等方面全面考察，并定期对员工进行能力和知识的培训。

结语

在我国目前的信息化建设和应用中，信息安全已经成为一个非常重要的问题。通信电脑是信息技术应用之载体，其资讯储存量较大，确保信息的安全性显得尤为重要。当前，在计算机应用中，因其相应的机制存在问题，造成了计算机应用中的网络安全得不到保证。所以，在使用电脑时，应持续增强使用者的信息安全意识，从保护自己的信息安全着手，通过科技的更新和完善提升电脑的安全性。

引用

[1] 马怡璇,李浩升,黄强,等.基于模糊理论的信息安全风险评估系统[J].电子设计工程,2023(4):123-127.

[2] 杨忠铭.计算机信息安全及其防火墙技术应用[J].数字通信世界,2023(1):126-128.

[3] 任高明.计算机信息系统维护与网络安全漏洞处理方法[J].信息记录材料,2020(7):183-184.

[4] 王懿嘉.计算机信息系统维护与网络安全漏洞处理策略分析[J].无线互联科技,2020(10):20-21.