 DOI: https://doi.org/10.12349/tie.v2i1.5804

Research on computer application based on network information security technology management

Ke Wang

CNOOC Refining & Chemical Co., Ltd., Beijing, 100029, China

Abstract

The application of computer puts forward high requirements for network security, and in practical application, in order to fully ensure the security of network information, relevant technical personnel need to implement comprehensive and scientific management of network information security. At this stage, because the network security system of the computer is not very sound, the computer is likely to be attacked by viruses during use. Based on the recent domestic network information security hotspots and the domestic regulatory situation, this paper proposes network information security technology management measures from the perspectives of multi-factor identity authentication technology, network intrusion detection technology, and information security technology for network mimic defense system.

Keywords

network information; security protection technology; Computer

基于网络信息安全技术管理的计算机应用研究

王珂

中海石油炼化有限责任公司，中国·北京 100029

摘　要

计算机的应用对网络安全性提出了高要求，在实际应用中，要想充分保证网络信息的安全，相关技术人员就需要对网络信息安全实施综合性、科学性的管理。现阶段，由于计算机的网络安全体系还不十分健全，计算机在使用过程中很可能会遭到病毒攻击。本文按照近期国内网络信息安全热点事件和国内监管态势为研究背景，从多因子身份认证技术、网络入侵检测技术、面向网络拟态防御系统的信息安全技术等提出了网络信息安全技术管理措施，以供参考。

关键词

网络信息；安全防护技术；计算机

1 引言

网络信息安全管理（CSIG）是指在保证信息保密、完整性和可用性的基础上，对其进行科学、规范的管理，其管理活动与过程不仅是网络信息安全技术的重要组成部分，也是保护人们用网安全的关键技术。因此，基于网络信息安全技术管理的计算机应用主要以身份信息识别、入侵检测技术为主，以此达到保障计算机应用安全的效果。

2 近期国内网络信息安全热点事件和国内监管态势

2.1 国内网络信息安全热点事件

当前，我国发生了多起以政府机关、科研机构为重点的网络安全事件，网络与信息安全形势依然严峻。根据调查我国最近安全事故如下：

西北理工大学电子邮件系统在六月二十三日遭到网络攻击后，警方进行了调查，初步认定是国外的黑客和犯罪分子所为。其目的是利用电子邮件诱骗教师和学生，对个别教师的个人计算机进行攻击，从而获得重要的资料。上海某机构的资料库出现泄露，数十亿居民的个人资料和防疫资料被盗用，并在暗网上贩卖。可见，网络攻击的主要目标主要为政府机构、教育、公共服务等重要信息基础设施以及掌握个人数据的企事业。一旦网络攻击成功，则会造成被攻击目标的网站域名失效、无法搜索等问题。同时，也会发生诸如数据被窃取、篡改、信息内容安全等问题，对被攻击的企业造成一定的损害，对于个人来说会直接危害到信息安全、公共利益等。

2.2 国内网络信息安全监管态势

我国监管机构按照《网络安全法》、《数据安全法》、《个人信息保护法》等，在网络安全和信息安全方面开展了网络信息安全治理行动，其中包括但不限于：

【作者简介】王珂（1989–），男，中国河南邓州人，硕士，工程师，从事企业信息化和网络安全研究。

2.2.1 个人信息安全治理专项行动

国家邮政局、公安部、国家互联网信息局于 4 月 21 号联合开展了一次为期半年的专项整治活动。此次行动是由邮政、快递行业主管部门联合发起，目的是整治网络上侵犯公民个人信息的违法行为，推动行业提高个人信息保护水平。

2.2.2 网络生态综合治理

公安部实施了“2022 净网”专项行动，其中包括由公安部网安局组织的“净网”动态 IP 代理乱象整治和“网络水军整治”专项行动。

前者是指不法分子通过 IP 动态 IP 代理服务，在不同区域实施攻击、诈骗、赌博、传播淫秽色情等非法活动，整治行动中可从源头上解决问题，切断供应，打击 IP 的动态黑产业。后者是切实履行网络平台的主体责任，加强网络生态综合治理，打击“网络水军”现象，并强化网络生态系统综合治理效能。

3 基于网络信息安全技术管理的计算机应用

3.1 多因子身份认证技术

在人们进入互联网时代后，因网络虚拟化的特点以及业务流动性的特征，各种网络资源的获得越来越多。因此，在进行各种网上交易时，身份验证就显得尤为重要。若用户身份信息被盗用、冒用，其不仅会影响到用户交易行为，也会导致用户无法获取有效的网络资源。因此，在网络信息安全技术的基础上，保证用户的身份是计算机信息安全管理的基础，而传统的身份验证方法已经不能满足对安全性、准确性和灵活性的需求，需要对身份验证技术进行创新和更新。其中，多因子身份认证技术主要包含以下几个关键技术，可以最大程度上保障信息安全、用户身份安全 [1]。

3.1.1 数字签名技术

采用数字签名技术实现用户的身份验证，即利用私钥签名和公钥验证来实现身份验证。当计算机通过国家保密算法，产生了用户私有的公共密钥和私有密钥后，用户可通过数字签名技术加密保护后存储在计算机内部，随后用户公开密钥可以被上传到伺服器，并与使用者账号建立一个安全的联结关系。在进行手势口令检查时，利用用户私有密钥签署数据，然后将其传送到服务端，并通过相应的公钥进行验证。

3.1.2 人脸识别技术

人脸识别技术在计算机应用中应用时期较长，我国人脸生产技术发展较为成熟。该技术是通过对脸部的持续运动（转头、抬头、低头、眨眼）的检测和分析而实现的。计算机所使用的人脸辨识引擎性能优越，稳定可靠，且具有较高的检出率（被正确侦测到的脸部样本量超过上一次样本量）[2]。

3.1.3 时空码技术

时空编码技术是一种准硬件级别的、具有安全性和可靠性的动态多维编码技术。在此采用动态算法、P2P（去中心化）检验等先进技术，将时间、空间、硬件指纹、行为和逻辑加密等多种安全因素结合起来。该技术可保障人们在使用计算机时的凭证安全、远程凭证安全、交易安全，可有效防止偷拍、截屏、病毒、木马等。可以说该技术像是在开放的计算机网络中为设备提供了一个安全的通道 [3]。

3.2 网络入侵检测技术

在信息技术飞速发展的今天，互联网已深入到人们的日常工作和生活中。在人们使用计算机时，内外因素对计算机的攻击也层出不穷，其不仅影响了用户的上网体验，也无法保障计算机使用的安全性。因此，入侵检测技术作为一种主动的动态防护技术，其研究与应用日益受到重视 [4]。

3.2.1 入侵防御概述

入侵防御是一种具有安全性的系统。该方法通过对网络业务进行分析，发现缓冲区溢出攻击、木马攻击、蠕虫攻击等，并在一定程度上实时中断攻击，以此有效地防止病毒入侵计算机内部。入侵防御主要是为了防止内网服务器和客户端受到的内外攻击。该系统能够在检测到网络被入侵的情况下，自动删除或拦截攻击来源，以此达到防止攻击行为的现象出现。例如，某企业在计算机内部边缘设置了防火墙，以保证计算机信息安全。在该组网中，内部网络的使用者可以存取互联网网络伺服器。为了防止内部网络用户访问互联网的网络服务器时受到攻击，企业还需在防火墙上设置入侵防护功能 [5]。

3.2.2 反病毒

计算机恶意程式是一套电脑指令或程式码，用以干扰计算机内部功能或直接破坏数据信息，其影响计算机使用并且会自动复制另一组指令与代码继续对其进行破坏。而反病毒是一种能够通过对病毒文件的身份鉴别和处理，从而防止因病毒导致计算机内部出现数据破坏、权限变更、系统崩溃等问题。在下列情况，可使用反病毒功能确保计算机网络安全性：内联网用户能够接入外部网络，并且常常要从外部网络上下载文件；内联网的伺服器通常会收到使用者上传的数据信息等 [6]。例如，防火墙是一种隔离内外网的网关设备，它包含了使用者主机和服务器。内部网络的使用者可以通过外部网络下载文件，外网使用者可以将档案上传至内部网络服务器，在此为确保内网用户与服务器接收文件的安全性，应在其配置好防病毒功能，若防火墙发现传送文件带有病毒，会执行下列操作：1. 判定病毒文件是否击中了病毒异常；2. 确定病毒文件中有没有应用异常；3. 根据配置文件中的协议和发送方向相应的响应行为来进行处理 [7]。再如，某企业在计算机内部边缘设置了防火墙作为网关，内网用户要从网站和 POP3 服务器上下载文件、邮件；企业通过使用防火墙所具有的防病毒特性来防止病毒文件侵入到被保护的网络中，从而保证了内部网用户和服务器安全。

3.3 面向网络拟态防御系统的信息安全技术

在互联网迅速发展的今天，一方面，各种新型的网络系统如 SDN、软件定制网、物联网等层出不穷；另一方面，

社交工程、APT 等新型的攻击手段也日益受到人们的重视。传统网络体系结构大多采用静态架构，无法全面且有效地抵抗攻击者对计算机的检测和攻击，使得网络形势较为严峻，信息安全得不到全面的保障 [8]。为此技术网络信息技术管理角度，提出面向网络拟态防御系统的信息安全技术，具体如下。

3.3.1 拟态防御机理

拟态安全防护技术是为了应对网络空间中的高成本、高不对称性而设计的一种新的安全技术。通过改变系统的异构性和多样性，改变系统的相似性和单一性，并运用动态性和随机性来改变计算机的静态和确定性，以此达到控制系统安全性的目的，在此过程中需要采用不相似性的余度空间对网络攻击进行阻断 [3]。具体来说，拟态防护以异构相同相似执行体为核心功能，动态冗余构架实现动态性和随机性，使内部执行体处于不断变化的状态。其极大地增强了攻击的不确定性，使攻击识别和预测能力变得更加复杂，这给攻击者入侵计算机造成了极端困难，以此达到保障计算机内部信息安全的效果 [9]。

3.3.2 动态异构冗余机制

动态异构冗余（DHR）是模拟防御的核心技术， DHR 通常由输入代理、异构元素池、异构构件集、动态选择算法、执行集体、以及表达式等构成。该模型采用动态选取算法，从多个不同的组件中选取若干异构构件组成执行集体，并将它们的输入分别输入到各个执行个体中，再由多模式判定系统的输出。其优势在于，每个实现的功能都可为随机选择，即随机实施函数的执行者，这会导致系统在不断地变化和不确定的情况下，结构可以重复、重叠，从而大大增加了攻击者的攻击复杂性，有效地干扰了攻击者的连续检测 [10]。可以说，该技术作为一种全新的安全防范机制，网络拟态防御的安全模型与评价问题还处在初级阶段。在此采用本体模型模拟防伪 CMD，既能清楚地描述 CMD 与 DHRE 之间构件的组件关系，同时，还可将安全漏洞、攻击面等本体安全类型也引入到模型中。实验结果显示，在此模型基础上，结合 SWRL 所编写的相应的安全攻击和防御准则，能够在 CMD 系统中以逻辑推理的方式进行安全判定，以此达到计算机信息安全防护效果。

4 结语

在信息技术发展的今天，计算机为人们的生产、生活地带来了诸多便捷，但因计算机内部不稳定因素较多，其安全问题也会随之而来。因此，在加强对计算机信息安全的重视时，需明确网络信息安全技术管理在计算机网络安全防护中的应用，以采取有效的防控技术，进一步完善计算机安全管理系统，增强计算机系统的安全性和稳定性，为人们创设出良好的网络环境。

参考文献

[1] 唐国慧. 基于网络环境下的医院计算机信息管理探讨[J]. 中外交流,2021,28(2):1413-1414.

[2] 张静. 计算机信息管理技术在网络安全应用中的研究[J]. 网络安全技术与应用,2021(3):150-152.

[3] 张东霞,付宁. 网络安全中计算机信息管理技术的应用探索[J]. 北京印刷学院学报,2021,29(5):126-128.

[4] 李芳. 计算机网络技术在企业信息管理中的应用实践[J]. 电脑知识与技术,2021,17(26):183-184.

[5] 吕海翠. 基于网络信息安全技术管理的计算机应用研究 [J]. 中国新通信, 2024, 26 (23): 95-96+118.

[6] 徐洪敏. 基于网络信息安全技术管理的计算机应用研究 [J]. 张江科技评论, 2024, (09): 135-137.

[7] 苏敏. 基于网络信息安全技术管理的计算机应用研究 [J]. 中国新通信, 2024, 26 (10): 29-31.

[8] 崔孟轩,李晓凤. 浅析台词的性格化对演员塑造角色的意义——以话剧《龙须沟》为例 [J]. 参花(上), 2023, (12): 83-85.

[9] 梁瑞. 网络信息安全技术管理的计算机应用探微 [J]. 中国设备工程, 2023, (21): 38-40.

[10] 李红艳. 基于网络信息安全技术管理的计算机应用 [J]. 信息记录材料, 2023, 24 (11): 91-93. DOI:10.16009/j.cnki.cn13-1295/tq.2023.11.006.