终端安全管理系统在气象网络中的研究与应用

钟 磊,张斌武,何恒宏
(国家气象信息中心,北京 100081)

摘 要:终端安全管理系统是中国气象局信息安全防护体系的重要组成部分,为业务系统和办公网络的各类终端提供基本的安全保证。但是终端安全管理系统在气象业务环境下还没有形成有效的研究和经验积累。随着全国气象业务系统面临的安全风险不断增加,探索气象业务系统部署终端安全防护系统,保证气象数据的安全性的问题亟待解决。文中以气象业务系统的终端数据安全为出发点,根据中国气象局信息网络一体化建设的需要,结合 CIMISS 等业务系统的数据流转过程,通过研究在业务系统建立终端安全防护机制,引入一定的机器学习算法对安全事件进行分析与分类,在一定的范围内对安全事件进行归纳总结,发现存在的深层次问题并进行针对性整改,从而大幅降低终端用户的安全风险。

关键词:终端安全;气象系统;多级备份;机器学习
中图分类号:TP302.1 **文献标识码**:A **文章编号**:1673-629X(2020)01-0206-05
doi:10.3969/j.issn.1673-629X.2020.01.037

Research and Application of Terminal Security Management System in CMA Network

ZHONG Lei,ZHANG Bin-wu,HE Heng-hong
(National Meteorological Information Center,Beijing 100081,China)

Abstract:Terminal security management system,which is an important part of the information security protection system of China Meteorological Administration,provides basic security guarantee for all kinds of terminals of business system and office network. However,the terminal security management system has not formed an effective research and experience accumulation in the meteorological service environment. With the increasing security risks faced by the national meteorological service system,it is urgent to explore the deployment of terminal security protection system in the meteorological service system to ensure the security of meteorological data. The terminal data security of meteorological service system is taken as the starting point. According to the requirements of the information network integration construction of China Meteorological Administration,combined with the data flow process of CIMISS and other business systems,the terminal security protection mechanism is established in the business system through research,and a certain machine learning algorithm is introduced to analyze and classify security events which are summarized within a certain range. We discover the deep-seated problems and carry out targeted rectification,so as to significantly reduce the security risks of end users.

Key words:terminal security;meteorological system;multi-level backup;machine learning

0 引 言

随着终端用户安全事件和网络攻击行为的不断增加,气象网络面临的安全挑战也越来越大。对近三年气象系统安全事件进行统计分析,终端安全事件每年增长幅度均在 30% 以上。对提取的有关风险事件和恶意文件进行反编译解析,具有针对性的网络攻击和数据窃取的木马植入增幅明显。近年来气象现代化建设不断推进,终端设备的种类越来越多、各终端使用的操作系统不尽相同,对于终端安全防护范围,针对不同业务区域进行针对性部署和防护,实现整体部署,分级管理,综合监控,紧急情况下能够做到整网联动,对终端安全管理系统提出了更高的要求。

国内某些企业和部委,根据自身需要,进行过一些有益的尝试:某国家大型企业,建立以私有云为基础的终端安全管理系统,采用分级管控方式,在终端用户人数过万的情况下,应急响应依然迅速[1-2];国家某部委

收稿日期:2019-01-21 **修回日期**:2019-05-22 **网络出版时间**:2019-09-24
基金项目:国家公益性行业(气象)科研专项(GYHY201406016)
作者简介:钟 磊(1986-),男(满族),工程师,CCF 会员(A8794M),研究方向为网络与空间安全;张斌武,通信作者,高级工程师,研究方向为网络与空间安全。
网络出版地址:http://kns.cnki.net/kcms/detail/61.1450.TP.20190924.1535.034.html

针对自身特点,建立了一套国家级、省级、市级的全网联动性终端安全防护系统,确保该系统业务网络稳定和办公终端的安全。

原国家级系统部署结构示意如图 1 所示。局域网主要业务单位办公区分别部署一套终端安全管理系统,管理服务器采用 HA(high available,高可用性群集)方式增强系统稳定性。部分单位同时配置一套 NAC(network admission control,网络准入控制)系统对接入网络的终端设备进行管控,通过 C/S(client/server,客户端/服务器端)模式,结合 802.1X 协议对用户身份进行鉴别。业务区和集约化平台没有部署必要的终端安全防护,仅依靠必要的 ACL(access control list,访问控制列表)进行逻辑上的隔离防护。

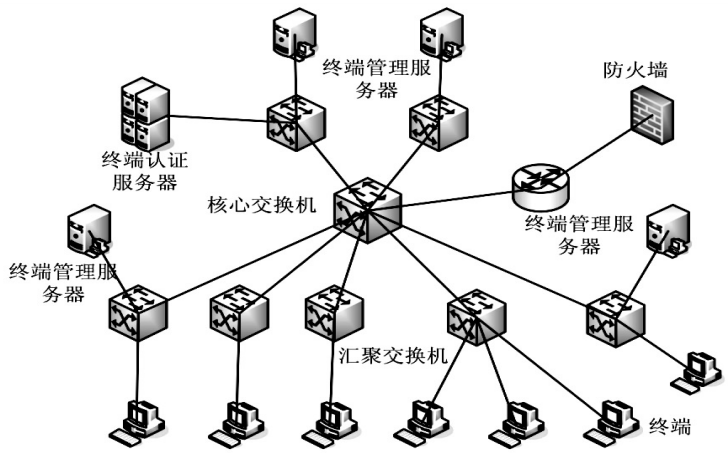

图 1　原有终端安全管理系统部署示意

原有终端安全管理系统的部署方式存在一些弊端:不同单位之间的管理系统相互独立[3],无法进行数据交互,在业务和办公区发生安全事件时,对风险源定位存在很大的困难,影响故障处理速度。原终端安全软件人机交互过程并不友好,对于被系统误认为风险的气象系统软件无法批量进行处理。原有安全终端功能较为单一,造成部分用户需安装同类软件进行互补,相互重叠的功能对系统稳定性和资源占用产生不利影响。原有终端安全管理系统需要开启 802.1X 网络协议与接入层交换机进行联动工作,此种方式对终端的管控较为严格,同时也存在明显的弊端,对无法安装安全终端的设备只能采取 MAC(media access control,介质访问控制)绑定交换机端口的方式进行管控,这会给系统管理员带来大量的繁琐重复性工作[4]。系统没有对业务区终端进行防护,大量业务系统终端面临被攻击和入侵的风险。气象系统由于其数据流程等方面的特殊性,在统一运维、多级管理功能的终端安全管理系统方面还未有相关的研究成果,如何建立信息安全事件快速响应机制也存在空白。

文中以中国气象局局域网未来规划和终端安全需求为基础,对业务区和办公区终端设备统一防护、多级管理进行探究,针对气象行业软件、业务系统数据传输过程、数据迁移防护等原有研究空白进行补充,同时依托机器学习有关算法,以有关历史数据为依据进行针对性优化,从而建立一套安全可靠,适应不同终端系统,符合气象行业未来终端安全发展的管理系统,为全国各级气象部门进行网络建设提供借鉴。

1　技术与设计

1.1　统一运维与多级管理设计

原有终端安全管理系统部分网络架构具有一定的借鉴意义。HA 方式能够增强系统的稳定性,NAC 能够形成较为有效的隔离防护,新的系统将予以保留。新系统建立多级管理系统结构,一级系统负责整个网络的基本管理和策略设置,二级管理负责各单位自身网络的运维,可以根据自身需要进行针对性优化。在出现重大信息安全事件时,可以通过一级服务器直接下发策略,减少审核和响应的事件[5],由于集约化平台的特殊性,采用有别于一般物理设备的轻量级的终端管理方式进行安全防护[6]。

1.2　气象业务支持设计

气象类软件在设计方面与其他软件有一些不同,终端安全管理系统对此类软件做到全局性、整体性可信运行,避免数据拦截造成文件完整性异常。对于业务系统,能够适应各类不同的终端操作系统[7-8]。对 MICAPS 等气象行业进行针对性的优化,对气象业务中存在的短时间大流量传输、多线程读取、多系统转存以及长连接等情况,做出针对性终端策略调整;对业务服务器上部署的安全终端,设计专门的升级服务器,通过缓存加速等方式保证系统升级速度,降低互联网出口带宽压力[9]。

1.3　气象系统集约化平台防护设计

气象系统集约化平台是气象现代化建设的组成部

分,是充分利用服务器物理资源的一次有效尝试。未来,气象系统主要业务会逐步迁移到此平台上,通过在此平台部署针对性二级服务器,对于底层支持直接安装终端安全的集约化设备,采取底层部署,对以此为基础的服务器进行全面防护。除此之外,通过采取功能模块和轮巡方式,对于无法在底层进行防护的终端设备采取对虚拟机上的系统逐台部署、错峰检测的方式进行安全保护[10-12]。

1.4 用户组迁移设计

在原终端安全防护系统中,用户组作为最重要的基础数据,无法进行整体性迁移和调整,在管理服务器出现异常时,其所管辖的用户将失去集中控制和风险文件上报分析的能力。本次新系统将引入快速迁移技术,实现各级管理服务器和备份服务器之间的快速迁移和备份,实现用户无感知的平滑迁移[13]。

1.5 安全域设计

原终端安全防护系统利用 802.1X 网络协议,采取交换机端口联动的方式,对终端进行安全管理。对于部分无法安装安全终端的设备只能采取 MAC 绑定的方式进行控制,在此类终端部署位置出现调整或设备更换时将会衍生较为繁复的配置修改。该研究采取基于终端应用的安全域终端安全管控机制,将根据各二级管理服务器的负责范围,分别设置不同的安全域,未经过终端安全管理系统认证的设备,无法访问安全域内的任何信息[14]。

1.6 数据分析设计

系统后台安全日志信息记录了大量安全事件信息和攻击类型,通过对数据的基本分类导出和有关数据进行人工建议清洗,形成初始数据,再通过机器学习的有关算法进行聚类,从而分析有关事件类型的共同点,在确定主要信息后采用降维算法进一步对核心信息进行提炼。

2 应用与实现

2.1 统一运维与多级管理的实现

在现有网络中,设置终端管理一级服务器,采取 HA 的方式,负责对二级服务器的管理和巡检,在二级服务器异常且无法迁移到备用服务器时,具备接管响应服务的能力;设置业务区域二级管理服务器,针对服务器操作系统的特点,设置对应的终端安全策略;在集约化平台设置备份服务器,用于各级服务器异常时的迁移使用,同时设置二级管理服务器,对集约化平台的各服务器提供终端安全支持[15]。一级管理服务器可以直接对全网终端用户或二级管理服务器下达执行指令;二级服务器可以根据自身需要进行独立管理和策略下发,升级后的网络结构示意如图 2 所示。身份认证系统与各级管理服务器进行联动,为有特别需要的终端提供身份认证服务。

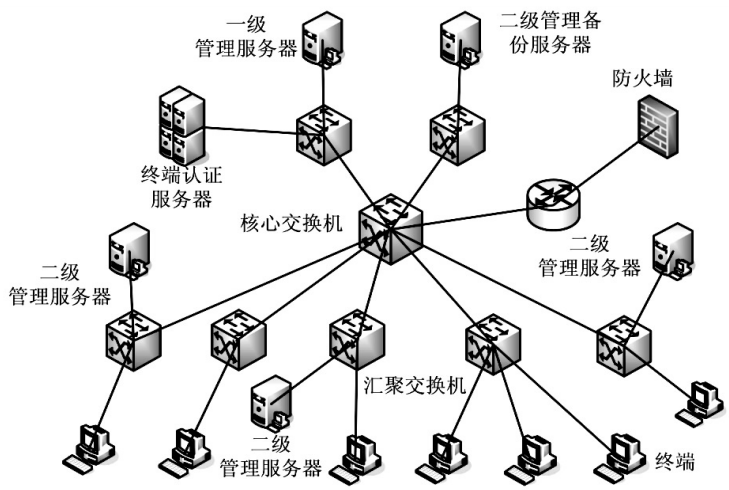

图 2 新终端安全管理系统网络结构示意

2.2 气象业务支持的实现

针对气象行业软件,在一级服务器和二级服务器均采用可信白名单策略,根据文件的 MD5 值等信息进行判断并设置针对性优化,从而保证行业软件运行的兼容性和稳定性。对于气象系统数据传输中长连接,开启专门的支持策略,通过增加窗口等待时间等方式保证此类数据在传输和分发过程中不会因为连接建立时间过长而失效。通过对缓存加速服务器对各级服务器更新的文件进行实时缓存,提高各级服务器有关文件的更新速度,降低互联网出口带宽压力[16]。缓存加速调整配置和缓存网络结构实现流程如图 3 所示。

2.3 集约化平台防护和用户迁移的实现

在集约化平台上,部署针对服务器系统的二级管理服务器,通过终端安全管理系统的终端模块选择,选取业务系统适用的功能模块,针对业务流量特点做针对性策略,从而在保证业务运行稳定的前提下,提高业务系统终端设备的安全性。同时在集约化平台设置终端安全管理系统的备份服务器,通过定期备份各级管

理服务器的数据信息进行同步传输,实现在各级管理服务器异常时,可以通过用户迁移功能和组播技术,完成故障点的处理和用户接入服务器的改变,实现短时间内的各级管理服务的快速恢复[17]。

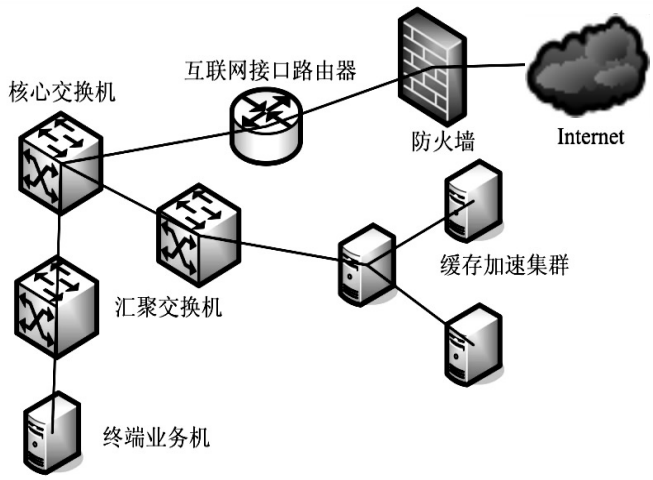

图 3　缓存网络结构实现流程

2.4　安全域的实现

在新终端安全管理系统中,不同的二级服务器管理不同的办公区或业务区,对于安全域的设计,采取二级管理服务器管理范围以外的部分为非安全域[18];各级管理服务器采取设定可信区域方式进行安全域划分,可信区域外的网络均为非安全域,从而保证未经过认证的设备无法访问非安全域的设备,访问行为会被及时隔离,从而保证各级管理服务器的信息安全。

2.5　数据分析算法设计

系统目前已经积累超过 90 万条日志信息,通过人工进行数据清洗。对主要数据采用 GMM(Gaussian mixed model,高斯混合模型)算法,以统计方式为核心进行聚类分析[19],同时采用 PCA(principal component analysis,主成分分析)算法对所得数据进行降维,以减少后续人工分析的工作量。对于数据量大需要频繁读取数据库信息的问题,可以采用空间换时间的办法减少对运算时间的影响[20]。

GMM 算法核心代码如下:

```
pGamma = Px . * repmat(pPi,N,1);
pGamma = pGamma ./ repmat(sum(pGamma,2),1,K);
Xshift = X-repmat(pMiu(kk, :),N,1);
pSigma(:,:,kk) = (Xshift' * (diag(pGamma(:, kk)) * Xshift))/Nk(kk);
pMiu = centroids; % 均值,也就是 K 类的中心
pPi = zeros(1,K); % 概率
pSigma = zeros(D, D, K); % 协方差矩阵
Xshift = X-repmat(pMiu(k, :),N,1);
inv_pSigma = inv(pSigma(:,:,k)+diag(repmat(threshold,1,size(pSigma(:, :, k),1))));% 方差矩阵求逆
tmp = sum((Xshift * inv_pSigma) . * Xshift, 2);
coef = (2 * pi)^(-D/2) * sqrt(det(inv_pSigma)); % det 求矩阵的行列式
Px(:,k) = coef * exp(-0.5 * tmp);
```

PCA 算法核心代码如下:

```
function [newX,T,meanValue] = pca_row(X,CRate)
% 每行是一个样本
% newX  降维后的新矩阵
% T 变换矩阵
% meanValue  X 每列均值构成的矩阵,用于将降维后的矩阵 newX 恢复成 X
% CRate 贡献率
% 计算中心化样本矩阵
meanValue = ones(size(X,1),1) * mean(X);
X = X-meanValue;% 每个维度减去该维度的均值
C = X' * X/(size(X,1)-1);% 计算协方差矩阵
% 计算特征向量,特征值
[V,D] = eig(C);
% 将特征向量按降序排序
[dummy,order] = sort(diag(-D));
V = V(:,order);% 将特征向量按照特征值大小进行降序排列
d = diag(D);% 将特征值取出,构成一个列向量
newd = d(order);% 将特征值构成的列向量按降序排列
% 取前 n 个特征向量,构成变换矩阵
sumd = sum(newd);% 特征值之和
for j = 1:length(newd)
i = sum(newd(1:j,1))/sumd;% 计算贡献率,贡献率 = 前 n 个特征值之和/总特征值之和
if i>CRate%
cols = j;
break;
end
end
T = V(:,1:cols);% 取前 cols 个特征向量,构成变换矩阵 T
newX = X * T;% 用变换矩阵 T 对 X 进行降维
end
```

3 应用结果

通过系统架构的调整和机器学习算法进行优化后,将近 6 个月的安全事件数量与去年同期进行对比,安全事件数量出现较为明显的下降,业务终端的安全性得到大幅提高。应用前后安全事件数据对比如图 4 所示。

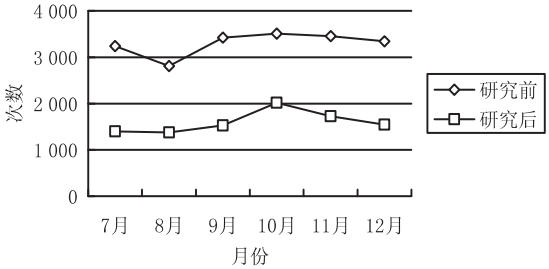

图 4 研究前后同期安全事件次数对比

4 结束语

通过保留原有终端安全管理系统部署结构方面的优势,结合气象现代化建设的趋势和用户需求,实现了气象局域网网络终端安全管理系统的统一监管和分级管理,为局域网综合一体化建设奠定了基础。弥补了原终端安全管理系统在终端功能上的一些不足,提高了业务区和集约化平台的终端的安全防护,实现了在终端安全管理服务器异常情况下的高效解决方案。采取应用准入方式的终端管控技术,解决了原终端安全管理系统使用 802.1X 协议进行管控中存在的不足,提高了全网的安全性和管理效率。该研究对国内气象系统终端安全建设具有一定的参考价值和借鉴意义。

本次建设和研究还存在一些不足:部分系统对数据的安全性和私密性有着特殊的要求,新建设的终端安全系统还暂时无法满足全部的要求;基于应用的准入控制,需要对安全域进行严格的划分,现有网络对于业务和办公的界限还存在模糊,使安全域的范围控制无法做到最优,同时在安全域的终端被黑客利用产生攻击时,攻击阻断还无法做到最快。未来的课题将针对以上的不足继续进行探究与完善。

参考文献:

[1] 杨庆明,杜保东. 桌面终端安全防护技术企业网管理中的应用研究[J]. 计算机安全,2010(10):77-79.

[2] 张文丽,郭 兵,沈 艳,等. 智能移动终端计算迁移研究[J]. 计算机学报,2016,39(5):1021-1038.

[3] 李清宝,张 平,曾光裕. 一种基于完整性保护的终端计算机安全防护方法[J]. 计算机科学,2015,42(6):162-166.

[4] 陈 璐,陈华智,邓 松,等. 电力内网终端的安全接入控制方法研究[J]. 电力信息与通信技术,2014,12(6):1-5.

[5] JIANG P,WANG Y J,CAI F D. Large data analysis of power mobile network information security terminal architecture based on power big data[J]. Electrotechnics Electric,2017,24(1):63-65.

[6] 彭 珺,高 珺. 计算机网络信息安全及防护策略研究[J]. 计算机与数字工程,2011,39(1):121-124.

[7] 严丽云,杨新章,陆 钢,等. 移动互联网时代终端安全问题及解决方案分析[J]. 电信科学,2014,30(12):145-152.

[8] 孙 庭,姚辉军,庄 崟. 基于广电网络的智能终端安全解决方案[J]. 电视技术,2014,38(6):67-70.

[9] 张栋毅. 校园网络安全分析与安全体系方案设计[J]. 计算机应用,2011,31(z2):116-118.

[10] YU Tao,CHEN Peng,WANG Yao,et al. Research and application of enterprise network security access control and terminal security coordinated prevention and control technology[J]. Shaanxi Coal,2017,36(5):13-16.

[11] 崔 勇,宋 健,缪葱葱,等. 移动云计算研究进展与趋势[J]. 计算机学报,2017,40(2):273-295.

[12] YURGIN N,SECNIK K,LAGE M J. DDoS detection and defense:client termination approach[J]. Value in Health,2005,8(6):157.

[13] 卢志培,姚国祥,罗伟其. 基于 802.1x 的 NAC 模型的设计与实现[J]. 计算机工程,2010,36(7):147-149.

[14] YING H,LUO Y,HAN L,et al. Mobile terminal security monitoring system based on distributed agent[C]//International conference on education,management,computer and medicine.[s.l.]:[s.n.],2017.

[15] 钱 扬. 企业网网络准入控制及终端安全防护研究[D]. 广州:华南理工大学,2012.

[16] 杨启超,徐开勇,尚 京,等. 基于虚拟化的多网安全办公系统研究与设计[J]. 科学技术与工程,2014,14(22):240-244.

[17] RAMAKI A A,AMINI M,ATANI R E. RTECA:real time episode correlation algorithm for multi-step attack scenarios detection[J]. Computers & Security,2015,49:206-219.

[18] 周 诚,李伟伟,莫 璇,等. 一种网络安全脆弱性评估方法[J]. 江苏大学学报:自然科学版,2017,38(1):68-77.

[19] LIU X,CHEN F,LU Y C,et al. Spatial prediction for multivariate non-Gaussian data[J]. ACM Transactions on Knowledge Discovery from Data,2017,11(3):1-27.

[20] LE A,KRISHNAMURTHY P,TIPPER D,et al. Modeling and simulation of wireless link quality (ETT) through principal component analysis of trace data[C]//ACM symposium on performance evaluation of wireless ad hoc,sensor,and ubiquitous networks. Miami,Florida,USA:ACM,2011:89-96.