

国家信息中心主办

第6卷 第6期 2020年6月

Vol.6 No.6 June 2020

信息安全研究

Journal of Information Security Research

监测预警与态势感知专题

基于层次聚类方法的流量异常检测

面向高级持续性威胁的态势感知概念模型

基于异构数据融合的政务网络安全监测平台设计与实现

ISSN 2096-1057



9 772096 105204
邮发代号: 2-41 定价: 38.00 元

Xinxl Anquan Yanjiu

信息安全研究

(月刊 2015 年创刊)

第 6 卷第 6 期 (总第 57 期) 2020 年 6 月

主管单位 国家发展和改革委员会

主办单位 国家信息中心

出版单位 《信息安全研究》杂志社

地址 北京市西城区三里河路 58 号

邮编 100045

电话 +86(10)68557385

网址 <http://www.sicris.cn>

电子信箱 ris@cei.cn

主编 李新友

社长 欧阳鹏

执行主编 崔传桢

副主编 吕欣 马修军

出版日期 每月 5 日

中国标准刊号 ISSN 2096-1057
CN 10-1345/TP

广告经营许可证 京西工商广登字 20170054 号

印刷单位 北京博海升彩色印刷有限公司

国内发行 北京市报刊发行局

订购处 全国各地邮电局 (所)

邮发代号 2-41

定价 38.00 元

战略合作单位 北京龙象之本投资管理有限公司

协办单位 亚信网络安全产业技术研究院

稿件授权声明: 凡向本刊投稿并被录用, 由本刊支付稿酬的稿件, 均视为稿件作者同意以下条款:

1. 文责自负。 作者保证其拥有该作品的完全著作权 (版权), 该作品不涉及政治敏感性和保密问题, 不侵犯任何他人的著作权。

2. 全权许可。 本刊有权以任何形式 (包括但不限于通过媒体、网络、光盘等介质) 使用、编辑、修改该作品, 无须另行征得作者同意, 无须另行支付稿酬。

3. 独家使用。 未经本刊书面许可, 作者不同意任何单位和个人以任何形式使用 (包括但不限于通过媒体、网络、光盘等介质转载、张贴、集结、出版) 该作品, 著作权法另有规定的除外。

版权声明: 未经本刊书面许可, 任何单位和个人不得以任何形式使用 (包括但不限于通过媒体、网络、光盘等介质转载、张贴、集结、出版) 该作品, 著作权法另有规定的除外。

本刊全文已被《中国核心期刊 (遴选) 数据库》《中文科技期刊数据库》《CNKI 中国期刊全文数据库》《超星期刊域出版平台》《博看网》收录。

» 监测预警与态势感知专题

- 474** 基于层次聚类方法的流量异常检测
..... 蹇诗婕 卢志刚 姜波 刘玉岭 刘宝旭
- 482** 面向高级持续性威胁的态势感知概念模型
..... 孙岩炜 刘照辉 蒋仲白 孟祥杰 胡卫华
- 491** 基于异构数据融合的政务网络安全监测平台设计与实现
..... 刘蓓 禄凯 程浩 闫桂勋
- 499** 基于 MEA-LVQ 的网络态势预测模型
..... 张泽 樊江伟 周南
- 506** 基于人工智能的安全态势预测技术研究综述
肖喜生 龙春 彭凯飞 魏金侠 赵静 冯伟华 陈瑞
- 514** KVM 环境下基于异常行为的恶意软件检测技术研究
..... 戴纯兴 刘刚 韩春超 王传国
- 523** 基于流量感知的动态网络资产监测研究
..... 李懂 刘鹏 蔡国庆
- 530** 态势感知在电子政务信息安全中的应用
..... 刘思博 刘鹏
- 537** 政务网站流量安全基线分析研究
..... 蔡国庆 刘鹏 李懂
- 543** 基于控制行为模型的工控系统异常检测方法
..... 安超 周纯杰
- 549** 基于“业务 + 数据”视角的民航网络安全态势感知技术研究
王勇 孙嘉启 淮华瑞
- 555** 铁路云数据中心的安全架构研究
..... 谭剑 王晓莉 饶伟

» 法律法规

- 562** 欧盟委员会 2020 年《欧洲数据战略》研究
..... 吴沈括 崔婷婷
- 566** 虚拟货币的恐怖融资风险及其监管应对
..... 牟丽娟 侯娜

CONTENTS 目次

Issue on Monitoring Warning and Situational Awareness

- Flow Anomaly Detection Based on Hierarchical Clustering Method**
..... Jian Shijie, et al (474)
- A Situation Awareness Conceptual Model for Advanced Persistent Threat**
..... Sun Yanwei, et al (482)
- Design and Implementation of Government Network Security Monitoring Platform Based on Heterogeneous Data Fusion**
..... Liu Bei, et al (491)
- Network Situation Prediction Model Based on MEA-LVQ**
..... Zhang Ze, et al (499)
- Survey of Security Situation Prediction Technology Based on Artificial Intelligence**
..... Xiao Xisheng, et al (506)
- Research on Technologies of Windows Malware Detecting Based on Abnormal Behavior in KVM Environment**
..... Dai Chunxing, et al (514)
- Research on Dynamic Network Asset Monitoring Based on Traffic Perception**
..... Li Chong, et al (523)
- Application of Situation Awareness in E-government Information Security**
..... Liu Sibao, et al (530)
- Research on Web Traffic Security Baseline Analysis of Government Website**
..... Cai Guoqing, et al (537)
- Anomaly Detection Method of Industrial Control System Based on Control Behavior Model**
..... An Chao, et al (543)
- A Study of Civil Aviation Network Security Situation Awareness Technology Based on "Business+Data" Perspective**
..... Wang Yong, et al (549)
- Research on Security Architecture for Railway Cloud Data Center**
..... Tan Jian, et al (555)

Laws and Regulations

- The Research on European Commission's European Data Strategy in 2020**
..... Wu Shenkuo, et al (562)
- Terrorist Financing Risk of Virtual Currency and Its Regulatory Response**
..... Che Lijuan, et al (566)

Journal of Information Security Research

Vol.6 No.6 June 2020

Publishing Period: Monthly

Date of Publication: 5th day of each month

International Standard Serial Number:

ISSN 2096-1057

Issues of Domestic Unit: CN 10-1345/TP

Editor-in-Chief: Li Xinyou

Directed by: National Development and Reform Commission

Sponsored by: The State Information Center

Published by: Journal of Information Security Research

Address: No.58 Sanlihe Road, Xicheng District, Beijing

Zip Code: 100045

Website: <http://www.sicris.cn>

E-mail: ris@cci.cn

AD Permit: BAICXBB Ad. No.0410

Distributor: Beijing Press and Publication Bureau

Domestic Issue Code: 2-41

Price: 38.00RMB

编委会顾问

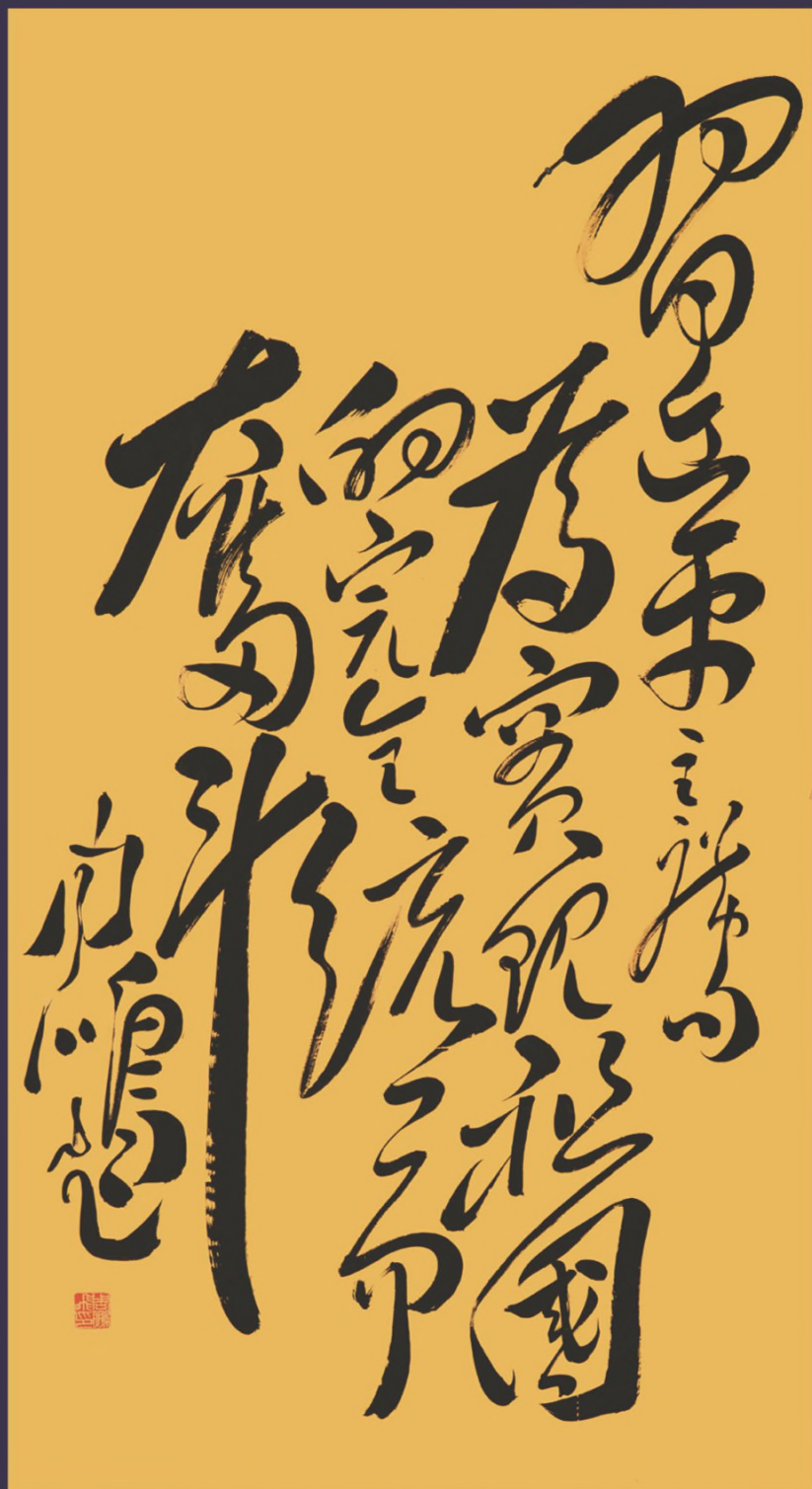
蔡吉人 崔书昆 杜虹 方滨兴 冯登国
顾建国 何德全 吕述望 倪光南 沈昌祥
严明 杨学山 赵战生

编委会主任 王小云

编委会委员

安德智 陈钟 陈嘉兴 陈尚义 陈晓桦
陈兴蜀 程学旗 丁珂 丁丽萍 杜彦辉
杜跃进 段海新 方勇 封化民 谷大武
顾健 郭莉 郭艳卿 何政 胡爱群
胡昌振 胡红钢 胡红升 贾焰 荆继武
康海燕 孔祥维 李晖 李剑 李涛
李建彬 李建华 李京春 李守鹏 李小勇
李欲晓 李舟军 林鹏 林东岱 林家骏
刘云 刘宝旭 刘吉强 罗森林 马智
马民虎 孟丹 孟小峰 闵京华 潘泉
潘柱廷 秦玉海 任卫红 孙伟 孙德刚
谭晓生 田俊峰 王标 王军 王楠
王智 王宝生 王丽娜 温巧燕 翁健
吴文玲 吴志军 肖新光 徐立臻 许光全
杨庚 杨义先 叶红 俞能海 云晓春
张健 张兴 张功萱 张宏莉 张焕国
张建标 张建军 张仕斌 张玉清 赵波
赵粮 赵淦森 赵有健 钟力 周民
周文 周琳娜 周世杰 朱岩 朱建明
祝烈煌 邹维 邹德清

周鹏飞先生书法作品选



草书，习近平主席句：为实现祖国的完全统一而奋斗

形神兼备，毛体书法艺术的新探索

周鹏飞，现任中国文物交流中心艺术总监，1970年出生于山东，父亲是知名画家周经纬。自幼学习书法，初学何绍基进而临习祝枝山草书，后又研习怀素狂草。1987年，周鹏飞决定以毛体为突破口，每日练笔不辍。北大书法班和多年的军旅生涯，给了他广阔的成长天地。他钟情致力于光大毛体书法，从形似到神似，从继承到创新，开辟了毛体书法新天地，2014年，被中国非物质文化遗产保护中心评定为“毛体书法非物质文化遗产传承人”。

周鹏飞的这幅毛体草书作品内容是习近平主席句“为实现祖国的完全统一而奋斗”，为祝贺2020年两会胜利闭幕而书写。整体感极强。书写流畅潇洒、气势磅礴、神采飞扬，笔法有力浑厚，层次丰富，给我们带来了毛体书法艺术新感觉。表现了作者不忘初心、牢记使命，期望早日完成祖国完全统一大业，弘扬中华民族优秀传统文化为己任的艺术家情怀，也体现了作者的爱国之情和文化自信。