

国家信息中心主办

QK1716181

第3卷 第7期 2017年7月

Vol.3 No.7 July 2017

信息安全研究

Journal of Information Security Research

特别策划：网络强国系列

众人科技，自主研发信息安全核心技术



僵尸网络综述

工业控制系统安全及异常检测研究进展

基于 CC 的安全性规格形式化描述及验证方法

ISSN 2096-1057



9 772096 105167
邮发代号：2-41 定价：20.00 元

万方数据

信息安全研究

(月刊 2015年创刊)

第3卷第7期(总第22期) 2017年7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://ris.sic.gov.cn
电子信箱 ris@cei.gov.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 20.00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《CNKI中国期刊全文数据库》、《中国核心期刊(遴选)数据库》、《中文科技期刊数据库》、《超星期刊域出版平台》、《博看网》收录。

特别策划

578 众人科技,自主研发信息安全核心技术
..... 谈剑峰

» 赛博物理系统(CPS)专题

589 僵尸网络综述
..... 崔丽娟 马卫国 赵巍 景秋实

601 基于时间自动机的CPS安全建模和验证
..... 苏琪 王婷 陈铁明 陈蓉蓉

610 动态可验证的异步理性秘密共享方案
..... 郝星然 贾恒越 段美姣

617 基于CC的安全性规格形式化描述及验证方法
..... 闫靖晨 程京德

624 工业控制系统安全及异常检测研究进展
..... 张凯一 陈铁明 严春

633 基于贝叶斯假设检验的CPS控制层攻击检测方法
..... 王卯宁 朱建明

638 基于国际标准CC和CEM的计算机系统信息安全
评估认证支持平台 宝达 陈惠琳 孙文 程京德

» 技术应用

647 云数据传输加密及完整性校验方案
..... 陈庄 叶成荫 齐锋

652 基于密码技术的健康医疗大数据安全保障体系研究
..... 张静 张洪亮

657 一种专用网络中的信息隐藏检测方法
..... 张建平 李洪敏 卢敏

» 专家视点

661 国际网络治理新形势 呼吁新动能新格局
——联合国2017年WSIS论坛综述
..... 方兴东 徐济涵 陈帅

668 黑客比赛对国家网络安全人才培养的影响
..... 谈剑峰 周强 张安琪

CONTENTS 目次

Special Report

PeopleNet, Independently Developing Core Technology
of Cyber Information Security Tan Jianfeng (578)

Issue of Cyber-Physical System

A Survey of Botnet Cui Lijuan, et al (589)

Modeling and Verifying Security Properties of Cyber-Physical System
Based on Timed Automata Su Qi, et al (601)

A Dynamic and Verified Rational Secret Sharing over an Asynchronous Channel
..... Hao Xingran, et al (610)

A Formal Specification and Verification Method for Security
Specification Based on CC Yan Jingchen, et al (617)

Research Survey on Industrial Control Systems Security and Intrusion Detection
..... Zhang Kaiyi, et al (624)

Research on Bayesian Hypothesis Test-Based Detection Method of
CPS Control Layer Attacks Wang Maoning, et al (633)

A Supporting Environment for IT System Security Evaluation Based on
CC and CEM Bao Da, et al (638)

Technical Applications

Scheme of Encrypted Cloud Data Transmission and Achieve the Data
Integrity Valid Chen Zhuang, et al (647)

Research on Security System of Healthcare Big Data Based on
Cryptographic Technique Zhang Jing, et al (652)

The Research of a Method to Detect Information Hiding in the Private
Network Zhang Jianping, et al (657)

Expert Viewpoint

International Internet Governance in New Situation, Calling for a New
Pattern of Energy — A Summary of WSIS Forum 2017
..... Fang Xingdong, et al (661)

The Influence of Hacking Competitions on the Cultivation of the National
Cybersecurity Talents Tan Xiaofeng, et al (668)

Journal of Information Security Research

Vol.3 No.7 July 2017

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://ris.sic.gov.cn>

E-mail: ris@cei.gov.cn

AD Permit: BAIC XBB Ad. No.0410

Distributor: Beijing Press and Publication Bureau

Domestic Issue Code: 2-41

Price: 20.00RMB

编委会顾问

蔡吉人 崔书昆 杜虹 顾建国 何德全
吕述望 倪光南 宁家骏 卿斯汉 沈昌祥
严明 杨学山 赵战生

编委会主任 杜平

编委会秘书长 吴亚非

编委会委员

方滨兴 陈钟 陈嘉兴 陈尚义 陈晓桦
程学旗 丁珂 丁丽萍 杜跃进 方勇
封化民 冯登国 谷大武 顾健 郭莉
何政 胡昌振 胡红钢 胡红升 贾焰
荆继武 康海燕 孔祥维 李涛 李建彬
李建华 李京春 李守鹏 李欲晓 李舟军
林鹏 林东岱 林家骏 刘云 刘宝旭
罗森林 马智 马民虎 孟丹 孟小峰
闵京华 潘柱廷 任卫红 孙伟 孙德刚
谭晓生 王楠 王军 王智 王宝生
王丽娜 王小云 温巧燕 吴文玲 吴志军
肖新光 徐立臻 杨义先 叶红 云晓春
张力 张健 张兴 张宏莉 张焕国
张建标 张建军 张玉清 赵粮 赵淦森
赵有健 钟力 周民 周文 周琳娜
朱岩 朱建明 邹维



油画：乱笔系列

表现内在心灵的意向油画

张鹏野，男，1967年8月生于中国黑龙江，职业艺术家、中国美术家协会会员，曾进修中央美术学院实验艺术系研究生班。作品多次参加国内外展览并获奖。

乱笔系列主要表现了作者内在心理状态，乱笔中丰富的色彩对比打破了他无序的心情，这个时期似乎要说明尽管内心世界存在着阴暗，外面的世界却没有那么令人恐惧的感觉。他用下意识的乱笔画法在画布上倾泻了心绪和情感，增添了作品的力度和感情，创作出了体现心灵状态的意象风景。