

国家信息中心主办
中国科技核心期刊

第8卷 第10期 2022年10月
Vol.8 No.10 Oct. 2022

信息安全研究

Journal of Information Security Research

数据安全与隐私计算专题

多方安全计算框架下的智能合约方法研究

基于零信任的动态访问控制模型研究

工业互联网环境下高效分布式匿名异构跨域认证方案

第10期

CN 10-1345/TP

ISSN 2096-1057



1.0>

9 772096 105228

邮发代号: 2-41 定价: 38.00 元

万方数据

信息安全研究

第八卷 第十期

二〇二二年十月

Xinxi Anquan Yanjiu

信息安全研究

(月刊 2015 年创刊)

第 8 卷第 10 期 (总第 85 期) 2022 年 10 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

执行董事兼社长 李 阳
常务副社长 潘 静

总编辑 李新友
副总编辑 马修军 刘 蓓
融媒体主编 崔传桢

出版日期 每月 5 日
国际标准连续出版物号 ISSN 2096-1057
国内统一连续出版物号 CN 10-1345/TP
广告经营许可证 京西市监广登字 20210016 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

协办单位 亚信安全 龙象之本
合作单位 360 集团 安恒信息
恒安嘉新 航天云网
绿盟科技 蚂蚁集团
明朝万达 奇安信集团
青藤云安全 数字认证
天融信集团 信安世纪

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。 作者保证其所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。

本刊是中国科技核心期刊, 入选 CCF T3 优秀期刊目录, 全文被《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。

» 数据安全与隐私计算专题

- 954 数据安全与隐私计算**
..... 祝烈煌 刘哲理
- 956 多方安全计算框架下的智能合约方法研究**
..... 凡 航 徐 葳 王倩雯 王云河
- 964 工业互联网环境下高效分布式匿名异构跨域认证方案**
..... 邓昊天 彭洪涛 祝烈煌 安 鹏 吴 桐 张 川
- 974 一种前向安全的盲币协议设计与分析**
..... 董顺宇 唐 波 刘金会
- 984 基于安全容器的券商 APP 用户隐私威胁行为管控**
技术研究 宋士明
- 990 一种适用于大规模场景的匿名电子投票系统**
..... 高小龙 王 玉 安 鹏 唐 波 刘金会
- 1000 基于微服务与隐私计算技术的数据安全共享服务平台**
..... 安 鹏 张卓晖 喻 波
- 1008 基于零信任的动态访问控制模型研究**
..... 张刘天 陈丹伟
- 1018 基于密钥矩阵派生的云计算密钥存储方案**
..... 池亚平 莫崇维 王志强 梁家铭 薛德凡
- 1028 基于 SGX 的云外包计算信任问题解决方案研究**
..... 王 冠 尹 煜
- 1035 面向交通流量预测隐私保护的联邦学习方法**
..... 傅思敏 王 健 鹿全礼 赵阳阳
- 1043 基于置乱变换的图像关键信息隐藏算法**
..... 刘红雨 王晓磊 张艳明 孙 尧 李巍巍

CONTENTS 目次

Issue on Data Security and Privacy Computing

Data Security and Privacy Computing

.....Zhu Liehuang, et al (954)

Research on Smart Contract Method in the Framework of Secure

Multi-party Computation Fan Hang, et al (956)

Efficient Distributed Anonymous Heterogeneous Cross-domain

Authentication Scheme for Industrial Internet of Things

..... Deng Haotian, et al (964)

Design and Analysis of a Forward Security Blindcoin Protocol

..... Dong Shunyu, et al (974)

Research on User Privacy Threat Behavior Management and Control

Technology of Brokerage APP Based on Security Container

..... Song Shiming (984)

An Anonymous E-voting System for Large Scale Scenarios

..... Gao Xiaolong, et al (990)

Data Security Sharing Service Platform Based on Microservices and

Privacy Computing Technology An Peng, et al (1000)

Research on Dynamic Access Control Model Based on Zero Trust

..... Zhang Liutian, et al (1008)

Key Storage Scheme for Cloud Computing Based on Key Matrix

Derivation Chi Yaping, et al (1018)

Research on SGX-based Cloud Outsourcing Computing Trust

Problem Solution Wang Guan, et al (1028)

A Privacy-Preserving Federated Learning Method for Traffic Flow

Prediction Fu Simin, et al (1035)

Key Information Hiding Algorithm of Image Based on Scrambling

Transformation Liu Hongyu, et al (1043)

Journal of Information Security Research

Vol.8 No.10 Oct. 2022

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

Director: Li Xinyou

Editor-in-Chief: Lü Xin

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@cei.cn

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 李京春 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

编委会秘书长 吕欣

编委会委员

安德智 贝宇红 陈晓桦 陈兴蜀 陈钟
程 度 程学旗 杜彦辉 杜跃进 段海新
范 渊 方 勇 封化民 谷大武 顾 健
郭 莉 郭艳卿 胡爱群 胡红钢 胡红升
黄伟庆 贾 焰 晋 钢 荆继武 康海燕
孔祥维 李 晖 李 剑 李建彬 李建华
李守鹏 李 涛 李小明 李欲晓 李舟军
林东岱 林家骏 林雪焰 刘宝旭 刘东红
刘吉强 刘建伟 刘 云 罗森林 马民虎
马 智 孟小峰 潘 泉 彭长根 秦 安
卿 昱 任 奎 任卫红 苏金树 苏 洲
孙德刚 孙 伟 谭晓生 谭毓安 唐春明
田俊峰 田志宏 王宝生 王 标 王 军
王美琴 王志海 王志强 韦 韬 温巧燕
文伟平 翁 健 吴文玲 吴云坤 吴志军
席 卿 肖新光 许光全 许 力 杨 庚
杨满智 杨义先 叶 红 叶晓虎 于 锐
俞能海 云晓春 张 滨 张功萱 张宏莉
张焕国 张 健 张建标 张建军 张庆勇
张仕斌 张小松 张玉清 赵 波 赵淦森
赵有健 郑 东 郑 方 周福才 周琳娜
周 民 周世杰 周 文 朱建明 朱 岩
祝烈煌 邹德清 邹 维

天融信科技集团

证券代码: 002212

研发中心
6实验室
7博士后
工作站 1研究院
2员工
6000+技术
4000+

防火墙

连续21年排名第一

安全服务

前三

VPN

前三

WAF

前三

安全管理

前三

网闸

前三

态势感知

领导者

EDR

领导者

IDPS

前列

安全资源池

前列

数据来源于IDC、CCID等历年报告

领导者象限

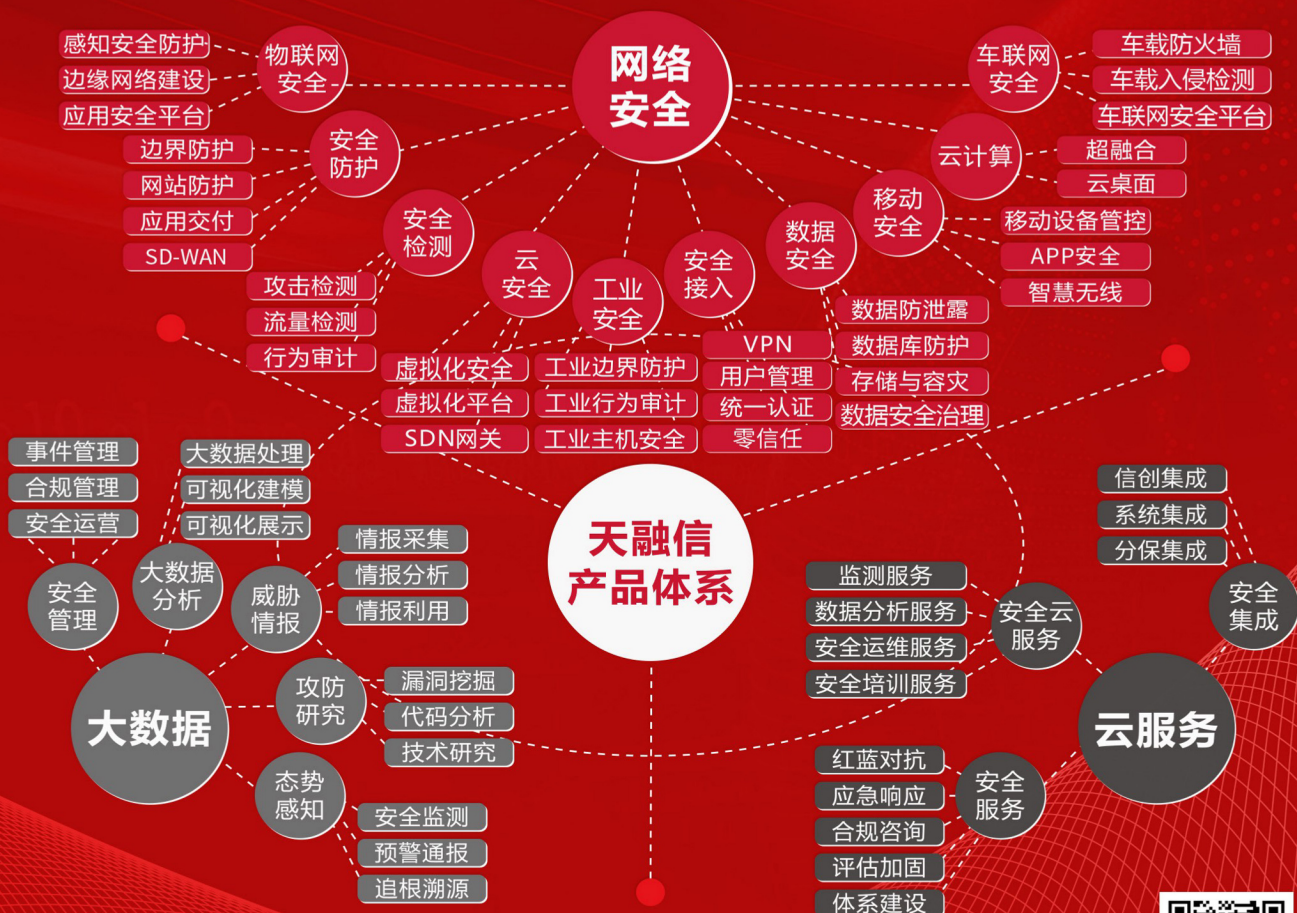
工控防火墙

工控漏洞扫描

工控主机卫士

工控安全
监测审计工控安全隔离
与信息交换工控安全
集中管理工控入侵检测
与审计

工控安全服务



地址: 北京市海淀区西北旺东路10号院西区11号楼东侧天融信科技集团

邮编: 100193 | 电话: 010-82776666 | 网址: www.topsec.com.cn

天融信官方微信

