

国家信息中心主办
中国科技核心期刊

第8卷 第3期 2022年3月
Vol.8 No.3 Mar. 2022

信息安全研究

Journal of Information Security Research

深度学习安全与对抗专题

面向自然语言处理领域的对抗攻击研究与展望

联邦学习安全威胁综述

人脸深度伪造检测综述

第3期

CN 10-1345/TP

ISSN 2096-1057



邮发代号: 2-41 定价: 38.00元

信息安全研究 第八卷 第三期

Xinxi Anquan Yanjiu

信息安全研究

(月刊 2015年创刊)

第8卷第3期(总第78期) 2022年3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

社长 李新友
主编 吕欣
副主编 马修军
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
航天云网 恒安嘉新
绿盟科技 蚂蚁集团
明朝万达 奇安信集团
数字认证 青藤云安全
信安世纪 天融信

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。

» 深度学习安全与对抗专题

- 202 面向自然语言处理领域的对抗攻击研究与展望
..... 金志刚 周峻毅 何晓勇
- 212 针对深度强化学习导航的物理对抗攻击方法
..... 桓琦 谢小权 郭敏 曾颖明
- 223 联邦学习安全威胁综述 王坤庆
刘婧 李晨 赵语杭 吕浩然 李鹏 刘炳莹
- 235 生成对抗网络技术与研究进展
..... 梁晨 王利斌 李卓群 薛源
- 241 人脸深度伪造检测综述
..... 孙毅 王志浩 邓佳 李霖 杨彬 唐胜
- 258 深度伪造生成和检测技术综述
..... 张煜之 王锐芳 朱亮 赵坤园 刘梦琪
- 270 基于安全洗牌和差分隐私的联邦学习模型安全防护方法
..... 粟勇 刘文龙 刘圣龙 江伊雯
- 277 一种基于差分隐私的可追踪深度学习分类器
..... 胡韵 刘嘉驹 李春国

- 292 基于异构属性图的自动化攻击行为语义识别方法
..... 薛见新 王星凯 张润滋 顾杜娟 刘文懋
- 301 基于动态污点分析的程序脆弱性检测工具设计与实现
..... 石加玉 彭双和 石福升 李勇

» 专家视点

- 311 高度重视人工智能安全问题 谭毓安

CONTENTS 目次

Issue on Security of Deep Learning in Adversarial Settings

Research and Prospect of Adversarial Attack in the Field of Natural

Language Processing Jin Zhigang, et al (202)

Physical Adversarial Attacks Against Navigation Based on Deep

Reinforcement Learning..... Huan Qi, et al (212)

A Survey on Threats to Federated Learning

..... Wang Kunqing, et al (223)

Technology and Research Progress of Generative Adversarial

Networks Liang Chen, et al (235)

A Survey of Deep Face Forgery Detection Sun Yi, et al (241)

The Review of Generation and Detection Technology for Deepfakes

..... Zhang Yuzhi, et al (258)

Security Protection Method of Federated Learning Model Based on

Secure Shuffling and Differential Privacy ... Su Yong, et al (270)

A Traceable Deep Learning Classifier Based on Differential Privacy

..... Hu Yun, et al (277)

Semantic Recognition for Attack Behavior Based on Heterogeneous

Attributed Graph Xue Jianxin, et al (292)

Design and Implementation of Program Vulnerability Detection Tool

Based on Dynamic Taint Analysis Shi Jiayu, et al (301)

Expert Viewpoint

Great Attention to Artificial Intelligence Security Issues ...Tan Yu'an (311)

Journal of Information Security Research

Vol.8 No.3 Mar. 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

AD Permit: BAIC XBB 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 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 李小勇 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 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

绿盟智能安全运营平台 (ISOP)

全场景 | 实战化 | 智能运营

1 个中心 · 6 大能力 · 3 大特点 · 3 大价值



- 日志威胁集中管理
- 资产安全管理



- 威胁分析与溯源
- 自动化响应流程



- 漏洞生命周期管理
- 可信任运营服务



以“实战化安全运营”为核心，围绕 IPDR 打造纵深能力及安全运营的横向场景化能力，构建“全场景、智能、实战化”的安全运营平台，实现“全面防护，智能分析，自动响应”的防护效果与基于安全治理、等保合规、安全运营的体系化能力，更好地支撑企业常态化安全运营体系建设。



绿盟科技微信公众平台

nsfocus.com
服务热线 400-818-6868