

主管：中华人民共和国公安部
主办：公安部第三研究所
中国计算机学会（计算机安全专业委员会）

ISSN1671-1122
CN31-1859/TN
中文核心期刊
中国科技核心期刊
中国科学引文数据库来源期刊

信息安全

NETINFO SECURITY

等级保护

基于安全硬件的云端数据机密性验证方案

技术研究

自组织网络环境下的节点认证机制研究

基于改进V-detector算法的入侵检测研究与优化

理论研究

基于物理不可克隆函数的Kerberos扩展协议及其形式化分析

ISSN 1671-1122



2020年 12月 第12期

总第240期

万方数据

☐ 等级保护

- 1 基于安全硬件的云端数据机密性验证方案 尤玮婧, 刘丽敏, 马悦, 韩东

☐ 技术研究

- 9 自组织网络环境下的节点认证机制研究 余北缘, 刘建伟, 周子钰
- 19 基于改进 V-detector 算法的入侵检测研究与优化 何泾沙, 韩松, 朱娜斐, 葛加可
- 28 一种自适应的异常流量检测方法 张新跃, 胡安磊, 李炬嵘, 冯燕春
- 33 一种基于双线性配对的天地一体化网络安全身份认证方案 赵国锋, 周文涛, 徐川, 徐磊
- 40 一种量子密钥池的双向使用方案 冯雁, 刘念, 谢四江
- 47 基于语义的网络交易论坛虚拟身份同一性识别 张璇, 袁得崙, 金波
- 54 基于 XGBoost 和 LightGBM 双层模型的恶意软件检测方法 徐国天, 沈耀童
- 64 基于 StarGAN 的生成式图像隐写方案 毕新亮, 杨海滨, 杨晓元, 黄思远
- 72 基于混合特征的深度自编码器的恶意软件家族分类 谭杨, 刘嘉勇, 张磊
- 83 一种针对恶意软件家族的威胁情报生成方法 王长杰, 李志华, 张叶

☐ 理论研究

- 91 基于物理不可克隆函数的 Kerberos 扩展协议及其形式化分析 张正, 查达仁, 柳亚男, 方旭明

☐ 网域动态

- 98 “第 15 届政府 / 行业信息化安全年会”在京顺利召开
- 99 新基建 新安全 | 湾区创见 · 2020 网络安全大会在深圳召开
- 100 “第十一届中国信息安全法律大会”在京举行
- 101 “第十四期网络安全创新发展高端论坛”召开

C O N T E N T S

1	An Intel SGX-based Proof of Encryption in Clouds	YOU Weijing, LIU Limin, Ma Yue, HAN Dong
9	Research on Node Authentication Mechanism in Self-organizing Network Environment.....	YU Beiyuan, LIU Jianwei, ZHOU Ziyu
19	Research and Optimization of Intrusion Detection Based on Improved V-detector Algorithm.....	HE Jingsha, HAN Song, ZHU Nafei, GE Jiake
28	A Method of Adaptive Abnormal Network Traffic Detection	ZHANG Xinyue, HU Anlei, LI Jurong, FENG Yanchun
33	A Secure Identity Authentication Scheme for Space-ground Integrated Network Based on Bilinear Pairing.....	ZHAO Guofeng, ZHOU Wentao, XU Chuan, XU Lei
40	A Bi-directional Use Scheme of Quantum Key Pool	FENG Yan, LIU Nian, XIE Sijiang
47	Virtual Identity Identification Based on Semantic for Network Trading Platform.....	ZHANG Xuan, YUAN Deyu, JIN Bo
54	A Malware Detection Method Based on XGBoost and LightGBM Two-layer Model.....	XU Guotian, SHEN Yaotong
64	Generative Steganography Scheme Based on StarGAN	BIXinliang, YANG Haibin, YANG Xiaoyuan, HUANG Siyuan
72	Malware Familial Classification of Deep Auto-encoder Based on Mixed Features	TAN Yang, LIU Jiayong, ZHANG Lei
83	A Threat Intelligence Generation Method for Malware Family	WANG Changjie, LI Zhihua, ZHANG Ye
91	PUF-based Kerberos Extension Protocol with Formal Analysis.....	ZHANG Zheng, ZHA Daren, LIU Yanan, FANG Xuming

敬告：

本期所有文字和图片未经本刊书面许可，不得转载。

本刊已被中国科技核心期刊、中国科学引文数据库来源期刊、中国学术期刊全文数据库、中文科技期刊数据库(全文版)等数据库收录,如果作者不同意文章被收录,请在来稿时向本刊声明,本刊将做适当处理。



科来网络全流量安全分析系统（TSA）

实时协议鉴别：流量识别是安全分析的第一步，决定了未知威胁的感知能力，科来TSA可以实现多达上万种协议与应用鉴别能力。

感知未知威胁：未知的网络攻击行为往往藏在正常的流量里面。通过各类元数据的恶意网络行为模型匹配技术，科来TSA可以感知隐藏在网络流量中APT攻击、特种木马、安全后门等未知威胁。

攻击回溯取证：只要是网络攻击，就一定会产生网络流量数据。科来TSA不仅保存网络行为和主机行为，同时还保存全部原始数据包数据，并提供PB级数据的秒级搜索，为安全事件的分析与取证提供更多依据。

CSNA网络分析认证

网络分析技术是网络管理的关键技术，CSNA认证培训致力于让用户掌握该项技术，提升解决网络安全问题和网络运维问题的能力。



CSNA-A：通过培训，提升学员解决网络安全问题和网络运维问题的能力，使学员能熟练运用相关产品为用户提供全面的网络分析服务。

CSNA-E：通过培训，掌握常见协议原理，理论结合实操，使学员充分了解网络分析思路并掌握网络分析技巧，熟练使用各种网络分析工具进行网络分析，达到独立进行网络故障排查及分析定位的目标。

CSNA-S：通过培训，使学员在安全数据包实战中掌握未知攻击的异常行为及分析思路，见识各类罕见的高级网络攻击方法，从而提高针对高级未知网络攻击的对抗能力。



科来成立于2003年，是以网络分析技术为核心的高科技企业，一直致力于网络分析技术的研究与推动，将网络分析技术应用于网络安全态势分析、网络故障诊断、网络性能优化等领域，并提供网络分析认证培训和相关技术服务。

电话：400-6869-069

官网：www.colasoft.com.cn

