

信息安全学报

Journal of Cyber Security



中国科学院 信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING, CAS



SKLOIS
信息安全国家重点实验室



科学出版社
Science Press

目 次

基于抽象语法树的智能化漏洞检测系统	1
陈肇炫, 邹德清, 李 珍, 金 海	
深度学习模型的中毒攻击与防御综述	14
陈晋音, 邹健飞, 苏蒙蒙, 张龙源	
基于指令集随机化的抗代码注入攻击方法	30
马博林, 张 铮, 陈 源, 邬江兴	
MVX-CFI: 一种实用的软件安全主动防御架构	44
姚 东, 张 铮, 张高斐, 邬江兴	
Explore-Exploit: 一种模拟真实网络渗透场景的安全竞赛	55
章 秀, 刘宝旭, 龚晓锐, 于 磊, 宋振宇	
软件定义网络中资源消耗型攻击及防御综述	72
徐建峰, 王利明, 徐 震	
网络入侵检测技术综述	96
蹇诗婕, 卢志刚, 杜 丹, 姜 波, 刘宝旭	
基于底层数据流分析的恶意软件检测方法	123
韩锦荣, 张元瞳, 朱子元, 孟 丹	
物联网蜜罐综述	138
游建舟, 吕世超, 孙玉砚, 石志强, 孙利民	

Contents

Intelligent vulnerability detection system based on abstract syntax tree	1
<i>CHEN Zhaoxuan, ZOU Deqing, LI Zhen, JIN Hai</i>	
Poisoning Attack and Defense on Deep learning Model: A Survey	14
<i>CHEN Jinyin, ZOU Jianfei, SU Mengmeng, ZHANG Longyuan</i>	
The Defense Method for Code-Injection Attacks Based on Instruction Set Randomization	30
<i>MA Bolin, ZHANG Zheng, CHEN Yuan, WU Jiangxing</i>	
MVX-CFI: a practical active defense framework for software security	44
<i>YAO Dong, ZHANG Zheng, ZHANG Gaofer, WU Jiangxing</i>	
Explore-Exploit: A Security Competition Modeling the Real-world Network Penetration Scenario	55
<i>ZHANG Xiu, LIU Baoxu, GONG Xiaorui, YU Lei, SONG Zhenyu</i>	
Survey on Resource Consumption Attacks and Defenses in Software-Defined Networking	72
<i>XU Jianfeng, WANG Liming, XU Zhen</i>	
Overview of Network Intrusion Detection Technology	96
<i>JIAN Shijie, LU Zhigang, DU Dan, JIANG Bo, LIU Baoxu</i>	
Malware Detection Method Based on Low-level Data Flow Analysis	123
<i>HAN Jinrong, ZHANG Yuantong, ZHU Ziyuan, MENG Dan</i>	
A Survey on Honeypots of Internet of Things	138
<i>YOU Jianzhou, LV Shichao, SUN Yuyan, SHI Zhiqiang, SUN Limin</i>	