计算机学院科研团队情况介绍表

团队名称	互联网安全实验室			团队负责人	陈焰
联 系 人	陈焰	Email	newyale@zju.edu.cn	电话	18506822396

主要情况介绍：

团队负责人陈焰为浙江大学任特聘教授，IEEE Fellow，浙大-美国西北大学互联网安全联合实验室主任。2003 年获加州大学伯克利分校计算机科学博士，主要研究方向为 Internet 系统安全， 网络安全和管理。2005 年获得美国能源部青年成就奖（Early CAREER Award），2007 年获得美国国防部（Air Force of Scientific Research）青年学者奖（Young Investigator Award），2004 和 2005 年分别获得 Microsoft 可信计算奖（Trustworthy Computing Awards），2010 年网络顶会ACM SIGCOMM 最佳论文提名,和 2018 年系统顶会 ACM ASPLOS 最具影响力论文奖。担任 ACM/IEEE ToN 的副主编及等多个著名国际会议程序委员会主席，并担任 ACM CCS 2011 主席。今年来在CCS, NDSS, USENIX Security, IEEE S&P, TDSC, TIFS等权威期刊和会议上发表了多篇论文。Google Scholar 的数据显示，论文总引用过万次，H-index指数为 58。主要研究方向为网络和系统安全、软件安全。详见http://list.zju.edu.cn.

交流合作：本团队与 Northwestern University（美国）互联网安全技术实验室有密切合作。基本上所有项目都有双方学生共同参与合作研究。本实验室的博士生也会到美方实验室访问 1-2 年。详见 http://list.cs.northwestern.edu.

团队主要成员

姓名	职称	研究方向	联系方式
陈焰	特聘教授 博导	网络和系统安全、软件安全	newyale@zju.edu.cn
陆魁军	副教授，硕士生导师	物联网、网络安全、网关安全技术	lukj@zju.edu.cn

目前承担的主要项目：

1. 针对高级持续性威胁的端点防御与响应系统

APT 网络攻击对国家、社会和企业造成了严重的安全威胁和巨大的经济损失。现有研究多针对APT 网络攻击的某一阶段提出防御策略，缺少对内在机理、攻击手段和演化规律的理解，难以应对APT 网络攻击的持续性、隐蔽性、多样性和动态性发展趋势。为此，本项目针对检测与溯源问题，研究面向 APT 网络攻击链的智能检测与溯源理论和技术体系。首先研究攻击的数据特征，建立跨层域异构数据的高效采集、存储和融合方法。再次，研究攻击的演进和载体，建立面向APT 网络攻击全链和

新型载体的智能检测方法。同时，研究攻击的时空演化模型，实现基于时序模式和时空模型的 APT 网络攻击溯源方法。最后，实现面向 APT 网络攻击链的智能检测与溯源的原型系统，对提出的理论模型和关键技术进行验证。我们在研发防御黑客攻击的各种手段，涉及到各种各样的任务，例如操作系统的底层实现，大数据的语义分析，快速的智能算法，形象的数据展现等等。

2. 云原生安全研究

本项目主要研究云原生的安全问题，研究微服务，serverless和Docker等安全问题。并从docker和微服务的自动化安全配置方面入手，首创基于命名空间感知的全栈信息收集、行为监控及入侵检测。同时研究Docker, Kubernetes, Istio的自动化配置生成，自动产生微服务访问控制策略的服务网格插件。

主要研究成果：

实验室研究工作多次获美国自然科学基金、Motorola、NEC、华为等资助。负责人已有 100 余篇论文发表在 IEEE/ACM Transactions on Networking (ToN), IEEE Transactions on Computers (TC)等顶级期刊和SIGCOMM，IEEE Symposium on Security and Privacy (Okland)等顶级会议。

实验室注重培养学生科研创新及工程实践能力，负责人所指导的毕业生均进入国际著名高校或公司任职，如 Johns Hopkins University, 香港科技大学、Google、NEC Labs America、Bell Labs、微软亚洲研究院等。