# 下一代网络与内生安全技术实验室：实验室负责人 吴春明教授

实验室长期从事互联网体系架构与演进、软件定义网络、可编程网络、网络测量、虚拟机漏洞智能发现、工业互联网内生安全领域的研究与应用实践。近年来承担、参与国家重点研发计划包括宽带通信和新型网络、网络空间安全、多模态网络与通信等专项课题十余项，工信部工业互联网创新工程及省级重点研发计划项目十余项。授权和申请国家发明专利八十余件，发表学术论文八十余篇。研究成果在 ACM CCS 2021 和 IEEE/ACM IWQoS 2021 上荣获 Best Paper Awards; 在 IEEE INFOCOM 2021 上荣获 Best Paper Candidates; 2022 年荣获了全球 Pwnie Awards 最具创新研究奖提名；多项安全成果入选近三年世界黑帽大会（BlackHat-Asia）以及 HITB 会议；发现云上系统漏洞 56 项，获得包括 Redhat、Oracle 在内的全球知名厂商 CVE 致谢 22 项。实验室成立的摇光安全战队 FSL 多次参加了国内外网络安全赛事，组员曾荣获包括 XCTF、DEFCON CTF、DataCon 等大赛的冠亚军战绩。实验室培养的研究生荣获多项校级、国家级荣誉，其中陈翔博士生分别荣获 2022-2023 学年浙江大学竺可桢奖学金以及国家一等奖学金。

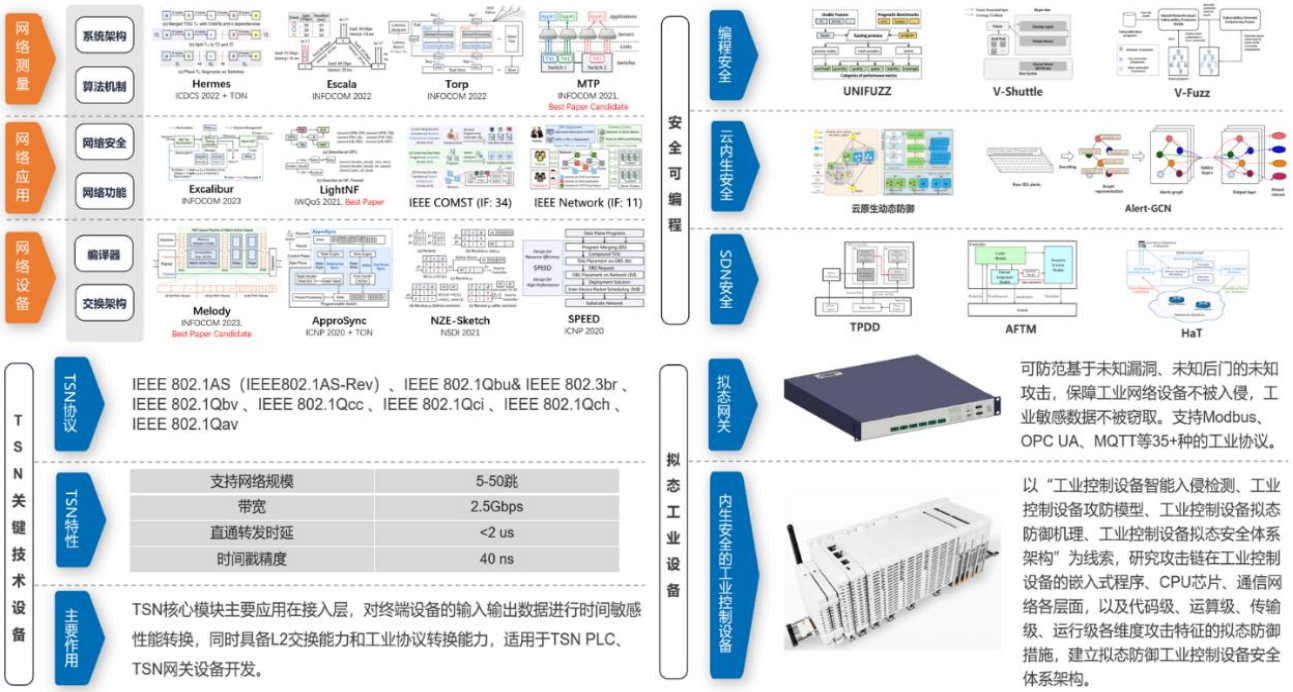


**图 1 实验室主要研究方向一览**

## 近期研究动向与成果：

*1. 网络安全技术*

实验室提出了基于语义感知的虚拟机管理程序的 Fuzzing 框架 V-SHUTTLE，通过解耦化嵌套结构并启用类型感知来实现全自动化的 Fuzzing。V-SHUTTLE 被发表在网络系统安全领域四大顶会之一的 ACM CCS 2021 上，并获得 Best Paper Award，是中国研究团队第二次以第一作者身份获得安全四大会议的 Best Paper 奖项。 V-SHUTTLE 迄今累计发现了 QEMU 和 VirtualBox 两款虚拟机管理程序中

的 56 个未知漏洞，其中 22 个授予了 CVE 编号，得到了厂商的公开致谢。其核心模块已在蚂蚁集团进行了实际部署与应用，成果的最大贡献在于有效保障了绝大多数互联网云厂商基础支撑软件的安全。

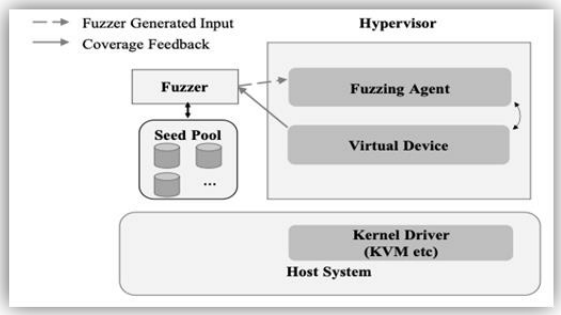


图 2 V-SHUTTLE 的工作流程


图 3 ACM CCS 2021 最佳论文奖

进而深入研究虚拟机管理程序中的异步时钟管理模块，在虚拟机管理程序中有许多设备使用异步时钟来处理它们的任务，例如网络、USB、磁盘和加解密设备等等，其目的是避免调用线程的阻塞，从而提高软件的响应能力。通过研究发现，攻击者可以利用异步时钟进行一些竞争条件攻击，并益于漏洞的利用。基于此，实验室提出了一种新的攻击利用技巧 Timekiller，利用异步时钟机制，使得原本难以利用的单个堆溢出写漏洞变得可利用。结合堆溢出写漏洞和 Timekiller 攻击技巧，成功实现一套针对 QEMU/KVM 的虚拟机逃逸方法。Timekiller 入围了 HITBSecConf2023-Phuket 黑客大会。

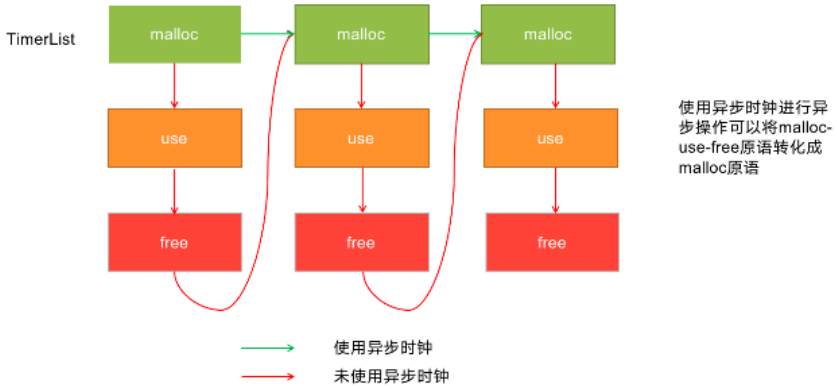


图 4 Timekiller 核心思想

## *2. 可编程网络测量技术*

网络智能化成为未来网络的一大发展趋势，该趋势将面临优化互联网路由控制技术，解决传统网络控制调度的弊端，降低管理成本的同时提升用户体验。如何利用有限的网络资源快速部署测量系统，迅捷精准地捕捉网络流量的变化、获得高精度的测量结果对于智能化网络的研究与发展意义重大。实验室提出的 LightNF 框架在可编程网络中提供了自动化的网络测量任务部署方案：首先提供了一套基于高层次用户意图的编程原语，允许网络管理员使用这套原语来构建任意的网络测量任务；随后，LightNF 调用其自动化网络测量任务分析及部署优化框架，计算由用户构建的网络测量任务在底层网络中的最佳部署方案，并自动部署至底层网络可编程交换机，满足部署需求的同时屏蔽底层细节，使整体网络测量任务部署过程保持高效、高性能、高精度的优势。LightNF 发表于计算机网络领域国际会议 IEEE/ACM IWQoS 2021 会议上，并获得大会唯一最佳论文奖（图 5、图 6）。

在可编程网络测量场景中，Sketch 具备低资源开销和理论上的精度保证，因此是一类至关重要的网络测量算子。然而，在全网范围内部署 Sketch 却需要在最优性和可扩展性之间进行权衡：（1）大多数解决方案依赖混合整数线性规划（MILP）求解器获取最优部署决策，但耗时长，难以扩展到大规模部署场景；（2）其它解决方案利用启发式算法提升了可扩展性，但引入了较高的网络资源和性能开销。实验室提出了一种可扩展且近似最优的全网 Sketch 部署框架 Eagle，核心思想是将全网 Sketch 部署分解为多个子问题，从而（1）同时优化交换机资源开销和数据报处理的端到端性能，保证了全网 Sketch 部署的近似最优性，且（2）将一系列用于加速问题求解的技术纳入子问题求解中，保证了全网 Sketch 部署的可扩展性。与现有解决方案相比，Eagle 在复杂网络拓扑环境下将 Sketch 部署加速了 255 倍，同时最小化了 Sketch 部署的最优性损失。研究成果发表于计算机通信网络领域的顶级旗舰会议 ACM Special Interest Group on Data Communication（SIGCOMM）2024（图 7）。

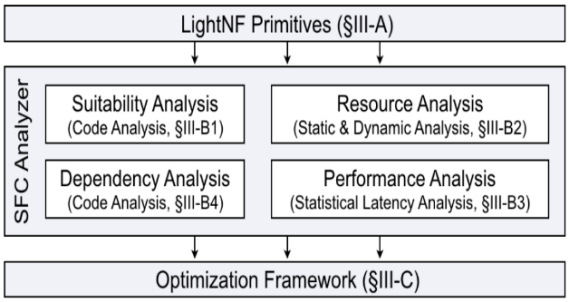


图 5 LightNF 的架构设计


图 6 IEEE/ACM IWQoS 2021 最佳论文奖

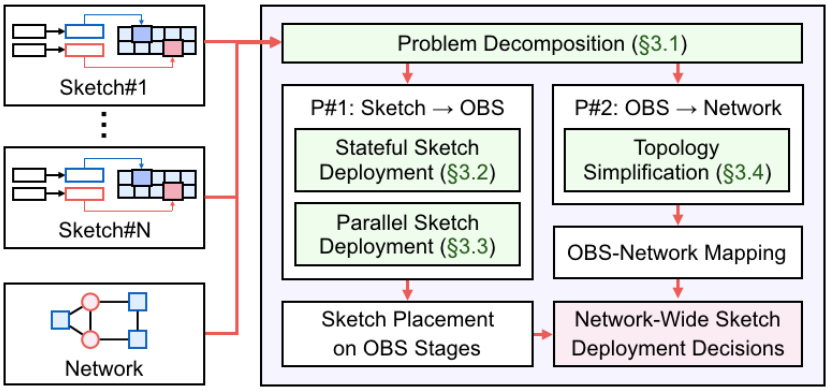


图 7 ACM SIGCOMM 2024 论文的 Eagle 框架

### *3. 云 WAF 安全与智能攻防*

实验室研究并评估了云环境 Web 应用防火墙（Web Application Firewall，WAF）的安全性，提出了基于语义解析树及上下文无关文法的攻击载荷变异方法，研发了能对云 WAF 进行自动化攻击的框架 AutoSpear。AutoSpear 在真实云上环境对 Amazon AWS、F5、Fortinet、Cloudflare、ModSecurity 等

国内外主流厂商的 WAF 实施了安全评估与漏洞发现。在实现最高 99%攻击成功率的情况下，成功发现了若干主流厂商 WAF 存在的高危安全漏洞。AutoSpear 的相关成果入围 Black Hat Asia 2022。此外，将内生安全、拟态防御技术应用于 WAF 系统之中，成功部署于国家电网省级公司内网、教育部大科学装置平台内网等系统中，并防护省级多家三甲医院官网、千岛湖旅游门户网站等公网系统，年均拦截内外网恶意请求近亿条。


图 8 AutoSpear 在世界黑帽大会上亮相

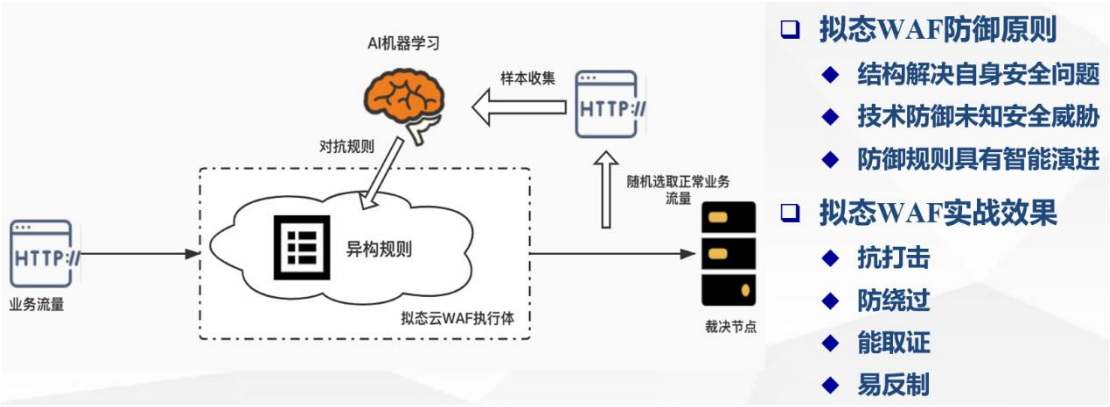


图 9 拟态云 WAF 的架构设计

*4. 国内外安全竞赛*

实验室成立的摇光安全战队 FSL 多次参加了国内外网络安全赛事，组员曾荣获包括 XCTF、DEFCON CTF、DataCon 等大赛的冠亚军战绩。


图 10 实验室摇光安全战队斩获佳绩