序号：201903

智能安全团队会议纪要

团队工作会议　　2019 年 7 月 29 日

时　间：	2019 年 7 月 29 日（周五）15:30—17:30
地　点：	之江实验室 2 号楼 307 会议室
主　持：	周海峰
出　席：	杨明亮、沈丛麒、余灿焕、金博豪、邓国福、俞丹瑞、许少宇、陈述涵、刘宏岩、周诗莹
记　录：	刘宏岩
编　辑：	刘宏岩

一、会议主题：工作汇报总结与未来工作分配

二、会议概要

杨明亮师兄对上周工作进行了总结提出了目前工作存在的几项问题：

1. 开发代码、脚本提交 GitHub 托管，提高协作效率；
2. ODL 控制器尽快落地实验环境；
3. OVS 追踪内核进程对 netdev_frame_hook()函数的调用；
4. 数据重放需要增加多种攻击手段，如低攻击流量；
5. SQL 数据库方面需要实时持续对数据图进行更新。

接下来，团队成员对上周的工作进行了展示汇报，周海峰博士、杨明亮师兄分别进行了点评，提出了要求，具体内容如下：

1. 金博豪：

   (1) 介绍 ODL l2switch 模块、下流表模块及其具体实现；

   (2) 介绍了 DoS 攻击时，ODL 各项性能指标的主要变化。

   要求：

   (1) ODL 控制器尽快落地实际的实验环境；

   (2) 获取相邻交换机间的时延，历史数据形成流量矩阵。

2. 邓国福：

   (1) OVS 已经可以获取数据报层面的所有信息，但 CPU/MEMORY 信息

的获取需要进一步的研究；

(2) 发掘了 TTL、数据报长度等新的数据报模式；

(3) 从 OVS 源码层面分析得到了 ovs 中添加网桥和端口命令以及数据包接收的流程。

要求：

(1) 展示 PPT 的有很大进步；

(2) 追踪内核进程对 netdev_frame_hook()函数的调用；

(3) 为数据报打标签获得端到端时延，尽量发现新特征。

3. 俞丹瑞：

(1) 打通了两台主机间的网络拓扑；

(2) LSTM、决策树、SVM、BP 神经网络算法的具体现实和结果展示；

要求：

(1) 发掘更好的深度学习模型，如 RNN、CNN；

(2) AI 模块要加强与数据库模块的联动。

4. 许少宇：

(1) Packet-in vector 表完成、ovs-vector 表缺少数据；

(2) D3 数据展示实现了动态更新。

要求：

(1) D3 数据展示尽量实现动态实时更新效果。

5. 陈述涵：

(1) 实现了强化学习算法，阅读有关 AI 与网络安全的前沿文献；

(2) 动手实现了一些主流的深度学习框架。

要求：

(1) 首先提升知识面的广度，广泛查阅前沿文献；

(2) 协助俞丹瑞同学实现 RNN、CNN。

6. 余灿焕：

(1) 介绍了几种常见的 DoS/DDoS 攻击手段；

(2) 介绍了几种常见攻击工具的使用，如 Hping3；

(3) 数据集重放的配置，包括 IP 映射、MAC 映射。

要求：

(1) 学习更多的攻击工具，增加现有的攻击方式；

(2) 注意攻击的时序问题，增加攻击的真实性。

周海峰博士与杨明亮师兄对上周成员工作进行了总结和点评，结合方案要求，为团队成员刘宏岩、邓国福、俞丹瑞、许少宇、陈述涵制定、分配了下一阶段的具体研究工作。具体研究工作安排如下：

（一）刘宏岩研究工作安排

1. 解决 ODL 控制器资源问题，搭建临时 SDN 控制平面；

2. 务必丰富合理攻击样本，考虑攻击的多样性；

3. 对数据时序性加以考虑，持续对 AI 模块反馈问题提供数据支持。

（二）邓国福研究工作安排

1. 进一步准确提取 OVS 的 CPU、MEMORY 数据；

2. 深入捕捉 Linux 内核模块进程，提高 CPU、MEMORY 的精度；

3. 进一步获取数据包层面其他数据信息。

（三）俞丹瑞研究工作安排

1. 横向比较各类分类器性能，寻找合适分类算法；

2. 对数据特征提出合理反馈，对分类结果异常（过低或过高）进行调整；

3. 代码层面切实落地 RNN 算法。

（四）许少宇研究工作安排

1. D3 可视化界面优化，提供多维度多角度可视化；

2. 协同 AI 模块参与新特征的设计。

（五）陈述涵研究工作安排

1. 继续学习强化学习与 AI 算法；

2. 协助俞丹瑞同学设计实现 AI 检测与强化学习算法。

（六）余灿焕研究工作安排

1. 协助指导刘宏岩同学完成数据重放、设计新的攻击方式；

2. 与邓国福同学合作，从 OvS 上尽可能考虑获取更多种类的潜在特征数据。

（七）金博豪研究工作安排

1. 进一步对控制器性能和指标进行研究，提出新的指标 CPU、MEMORY、IO；

2. 负责已完成的流表和冷启动控制器模块投入实际环境，切实投入实验环

境；

3. 获得链路时延、点到点时延，形成流量矩阵。

沈丛麒师姐主要介绍了新型 DDoS 攻击场景的初步论文调研情况，本周继续整理新型 DDoS 的实际攻击问题与场景，并调研传统 DDoS 的典型人工智能解决方案。

三、研究工作计划

（一）本周服务器到位；

（二）下周一（8 月 5 日）前完成每人的阶段目标。

四、下一次会议议题

项目组成员对**研究工作进展**、**存在的问题**、**下周的工作计划**以 PPT 的形式进行汇报。