序号：201902

智能安全团队会议纪要

团队工作会议　　2019 年 7 月 19 日

时　间：	2019 年 7 月 19 日（周五）15:15—17:15
地　点：	之江实验室 2 号楼 318 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
记　录：	刘宏岩
编　辑：	刘宏岩

一、会议主题：工作汇报总结与下周工作分配

二、会议概要

周海峰博士强调了 PPT 的制作规范，需要包含 PPT 首页、主题、目录页、上周分配到的研究工作内容页、上周研究任务的完成情况总结页、研究任务具体完成介绍、遇到的问题以及相应的解决方法、下一步研究工作的设想、其它好的想法等。同时强调了参会人员记笔记的重要性，以便团队每一位成员在会后准确无误地贯彻会上达成的决议、提出的意见与建议，最终增强团队的执行力，要求大家逐渐养成开会记笔记的好习惯。此外，为便于大家在各自研究领域快速、系统全面的掌握相关知识，提出由团队统一购买学习书籍与材料（7 月 29 日前汇总研究工作中所需的书籍到沈丛麒师姐处）。

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. ODL 提取“packet-in”数据包的时间要精确到秒级别；
2. 实验拓扑的尽快落地，扩展 vbox 虚拟机的网卡数量；
3. SQL 数据库应根据现有数据进一步挖掘新的模式；
4. AI 算法模块尽快实现落地，实现简单的 demo。

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、杨明亮师兄对每位同学分别进行了点评，具体内容如下：

1. 邓国福：

(1) 介绍了 OvS 中存储数据报关键信息的 sw_flow_key 结构体；

(2) 介绍了 OvS 端口处理数据报流程中几个关键的函数；

(3) 通过在 ovs_dp_process_packet()函数中添加相应的处理逻辑，完成数据报关键信息的提取。

建议：

(1) 展示 PPT 需要改进，需要有封面、标题、目录、上周分配的研究任务、本周任务完成情况总结、遇到的问题、解决的途径、下一步研究工作的设想、以及自己的一些想法等内容；

(2) 需要在平时进一步了解、熟悉 OvS，以便在后续进行更为深入的开发；

(3) 同步搜集 OvS 的相关书籍、材料，后续由团队统一购买。

2. 俞丹瑞：

(1) 实验拓扑架构介绍，各主机 ping 通结果展示；

(2) 拓扑的搭建过程（tap、veth 设备的使用）；

(3) 尽快打通多主机间的网络通信，扩大拓扑规模；

建议：

(1) 需要加快进度；

(2) 尽快打通多主机间的网络通信；

(3) 尽量排除传统网络对 SDN 架构的影响。

3. 许少宇：

(1) Packet-in vector 表基本完成、ovs-vector 正在完成；

(2) 对 SQL 脚本文件以及文件处理代码进行展示；

(3) 原始数据表的展示与目标数据的生成过程。

建议：

(1) 为后续实现数据实时传输至数据库（而非以文件整体传输形式）作相应技术上的准备；

4. 陈述涵：

(1) 学习了 AI 的相关算法，了解一些有关 AI 与网络安全的前沿文献；

(2) ML 方面：学习了周志华教授的《机器学习》一书；

(3) DL 方面：TensorFlow 框架的复现；

(4) SDN 方面：搭建了 OvS 的运行环境。

建议：

(1) 进一步加快学习人工智能、深度强化学习、SDN 等领域的基础知识；

(2) 带着目标去阅读文献。

5. 刘宏岩：

(1) 介绍了 SDN 环境下的“packet-in”数据报的背景；

(2) 介绍了 ODL 控制器收集“packet-in”数据报的相关模块；

(3) 介绍了“packet-in”应用的实现过程，并进行了 demo 演示。

建议：

(1) 学习将信息实时写入数据库中的相关知识；

(2) 在 ODL 控制器内实现流表下发的模块；

(3) 需要在平时进一步了解、熟悉 ODL，以便在后续进行更为深入的开发，同步搜集 ODL 的相关书籍、材料，后续由团队统一购买；

(4) 与金博豪师兄合作总结 ODL 的相关知识，形成技术文档。

杨明亮师兄对目前防护系统的整体架构与具体实现方案进行了介绍，结合方案要求，为团队成员余灿焕师兄、刘宏岩、邓国福师兄、俞丹瑞、许少宇、陈述涵制定、分配了下一周的具体研究工作。具体研究工作安排如下：

（一）余灿焕研究工作安排

1. 在真实网络上重放数据集；
2. 考虑从 OvS 上尽可能获取更多的数据，与邓国福一起负责 OvS，并参加深度强化学习与安全的相关研究。

（二）刘宏岩研究工作安排

1. 结合主流工具获取攻击样本；
2. 研究 DoS/DDoS 攻击机理，攻击样本尽可能覆盖全部攻击类型
3. 数据写入文件，与 SQL 数据库对接。

（三）邓国福研究工作安排

1. 获取 OvS 数据报层全部信息，包括 IP、CPU、Memory；

2. 尽可能多的获取有关数据报的信息。

（四）金博豪研究工作安排

1. L2 层网络冷启动和下发流表模块；
2. 控制器性能指标测试；
3. DoS/DDoS 攻击控制器属性。

（五）俞丹瑞研究工作安排

1. 落实 SDN 真实拓扑网络；
2. 下周实现 LSTM 和分类算法(另外安排了 8 月中旬同陈述涵完成沈丛麒师姐报告的深度强化学习的 TensorFlow 实现)；
3. 各个分类算法之间的性能比较。

（五）许少宇研究工作安排

1. 维护 packet_in table、feature table、vector table；
2. D3 数据可视化。

（六）陈述涵研究工作安排

1. 学习人工智能、深度强化学习等理论知识；
2. 继续学习强化学习与 AI 算法；
3. 实现 TensorFlow 框架；
4. 协助俞丹瑞设计实现 AI 检测与深度强化学习算法(另外安排了 8 月中旬完成沈丛麒师姐报告的深度强化学习的 TensorFlow 实现，具体可联系沈丛麒师姐)；

沈丛麒师姐对论文“Deep Reinforcement Learning based Smart Mitigation of DDoS Flooding in Software-Defined Networks”进行了汇报，介绍了深度强化学习、以及深度强化学习在 SDN 与网络安全中的应用。对论文的设计思路、特征选择和训练过程进行了介绍。

三、研究工作计划

（一） 下周五（7 月 26 日）完成各自的研究工作任务；

（二） 7 月 29 日前汇总研究工作中所需的书籍到沈丛麒师姐处，后续由团队统一购买。

四、下一次会议议题

团队成员对本次会议中安排的研究任务完成情况、遇到的问题、下周的工作计划以 PPT 的形式进行汇报。