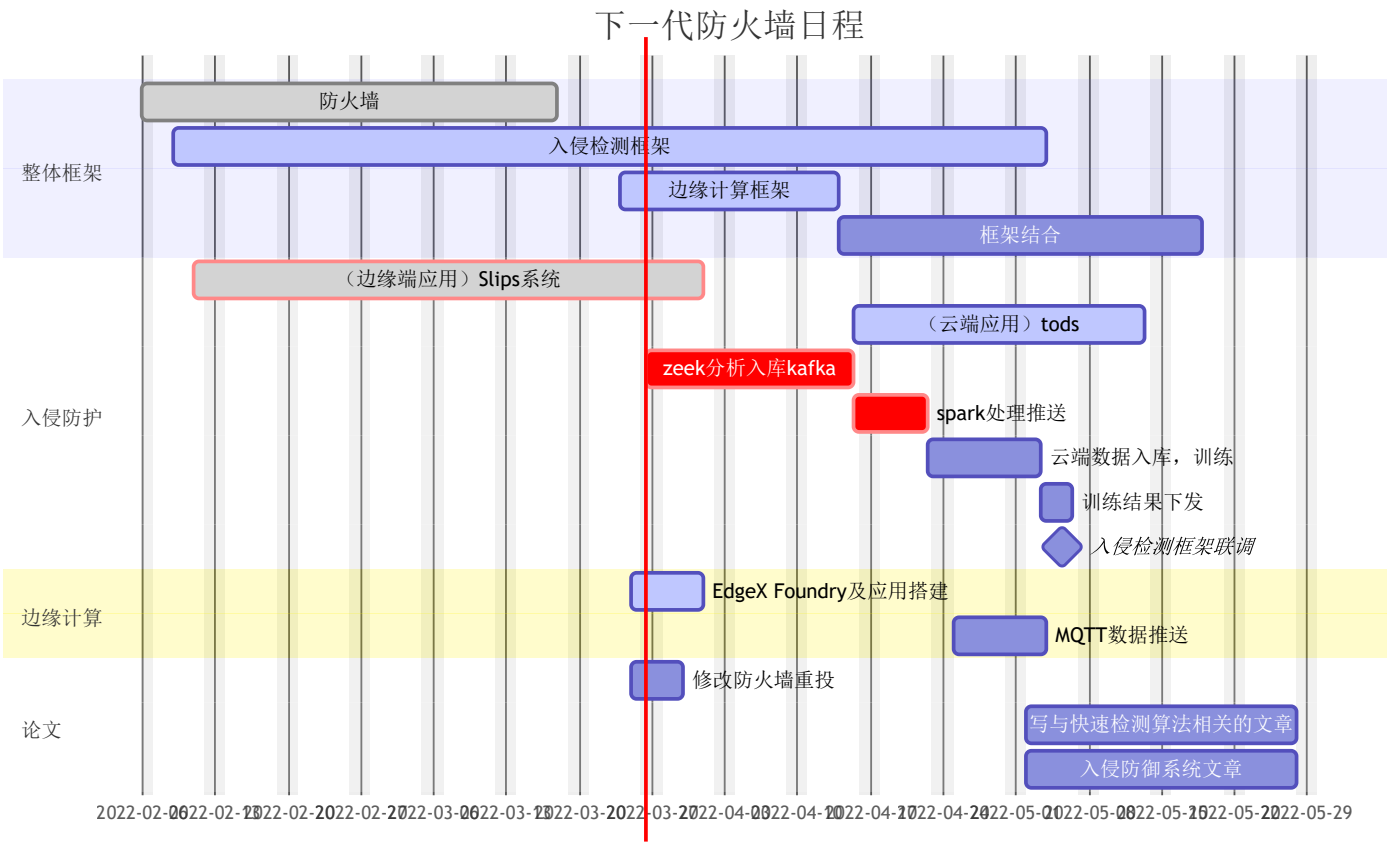
3-26 周总结

日程计划



工作

1、入侵防御Slips平台的测试

之前拟采用Slips平台作为入侵防御系统的一个切入点，本周对该平台进行测试，首先在台式机上完成了对Slips项目的测试。
经过对项目代码的解构，发现其底层主要是用zeek工具，在zeek之上使用其他的安全防护模块。现在已经可以在台式机上面跑通，下周将在工控机上使用docker进行测试。

·其可实现的功能包括：

1、流量数据的机器学习（给定一段时间的正常流量和异常流量，针对未知流量进行分类，主要使用SVM），该部分后期可以进行改造，使用更复杂的算法，但这一工作顺位比较靠后

2、数据泄露探测（给定特定的数据规则，把报文按照自定义的规则匹配）
3、ARP攻击检测（属于具体防护模式）
4、端口探测过滤（属于具体防护模式）
5、将网络上一些汇总的异常公网ip地址（将网路上公开的异常IP地址入库，进行匹配，在与外网相连的环节比较有用，属于具体防护模式）
6、RNN语序预测（该模块待测）

·后续安排

该模块可以很好的作为一个入侵防御系统搭建的切入点，其底层使用zeek对数据包进行拆包分析，可以很好的作为防火墙的补充，由入侵防御系统在zeek处理后进行判别，由防火墙进行包处理。

后续在入侵防御这个模块有两条线并行：
开发入侵检测系统在本地处理数据包（已完成）、转化数据包为便于分析的形式如one-hot编码（未实现）、入库kafka或spark（未实现），在边缘端进行训练（tods系统）
算法
在开发部分最后提到的tods系统可用来做云端训练，这一部分以模型为主，还需要花较多时间来研究，最近我也在开发之余精进算法方面的知识，训练入侵检测模型。

2、边缘计算平台框架搭建

考虑之后还是感觉没有框架与应用就直接谈安全还是没法让人放心，因此我希望先借助edgeX foundry的能力搭建一下边缘计算场景，网络上有一些EdgeX foundry的比赛，主要分为商业应用与工业应用，很多场景都是借助底层的摄像头以及传感器在边缘端实现数据处理与初步分析，在云端完成更为有价值的任务的形式。

在实验室搭建的平台不需要有那么多的复杂应用，但是底层的数据采集以及向云端的数据交互这些与边缘网络密切相关的过程还是需要的，这方面拟采用在边缘计算当中使用比较多的MQTT协议作为中间的转化协议。

EMQ X已经实现了 MQTT broker 与 Kafka的桥接。MQTT broker 用来快速的对大量物联网设备发来的消息做接收处理响应，而Kafka 对这些大量的数据做采集存储，交给数据分析人员来分析处理消息，目前已经完成了MQTT通讯的服务器客户端测试，下面要对MQTT客户端在Python当中实现交互。

3、全部项目代码入库

规范开发流程，将防火墙项目、入侵防御项目代码入云端私人库，便于版本管理与文档编写

目前正在进行的工作是：
安装docker（云端，边缘端均已完成）
安装edgeX（基本完成）

在云服务器（台式机）安装EMQX服务器（已完成）
在边缘设备（工控机）安装paho MQTT（未开始）
研究把zeek入库（网上有疑似可以使用的工具）转化为kafka后持久化（未开始）