**北 京 邮 电 大 学**

**本科毕业设计（论文）中期进展情况检查表**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 学院 | | 计算机学院 | | 专业 | | 计算机科学与技术 | | 班级 | 2013211305 |
| 学生姓名 | | 彭聪 | | 学号 | | 2013211289 | | 班内序号 | 08 |
| 指导教师姓名 | | 孙岩 | | 所在单位 | | 计算机学院 | | 职称 | 教授 |
| 设计（论文）题目 | | （中文）面向安全的SDN架构的研究与设计 | | | | | | | |
| （英文）Research and Design of Security Architecture for SDN | | | | | | | |
| 目  前  已  完  成  任  务 | 1. 任务目标   在对SDN架构的原理和特点进行研究学习的基础上，选取一种SDN开源控制器，在控制器内开发一个完整的安全模块即应用访问权限管理系统，完成对接入控制器的SDN应用的权限管理和访问控制，包括身份认证，权限检查以及访问控制策略等。   1. 系统总体架构   **XACML**  **访问控制**  **应用身份**  **信息管理**  **身份认证**  **应用权限管理**  **权限检查**  **内存数据库**  **日志记录**  **前端页面**  应用访问权限管理系统整体的框架图如上图所示，分为八个模块，并选取floodlight作为系统实现所依赖的开源控制器。其中前端页面包含四个子页面，包括应用身份信息管理页面，权限信息管理页面，属性控制管理页面，网络视图页面。应用身份信息管理页面具有应用的注册，身份信息的查询，修改，应用注销等功能，与后台的应用身份信息管理模块进行数据交互。权限信息管理页面具有应用权限初始化，权限查询，权限增加，权限删除等功能，与后台的应用权限管理模块进行数据交互。属性控制管理页面具有创建基于属性的访问控制策略的功能，与后台的XACML访问控制模块进行数据交互，为XACML判决提供策略依据。网络视图页面整合了floodlight本身具有的全局网络拓扑视图webUI界面，使整个系统的功能比较完整，系统管理员可以通过此页面查看整个网络中各个网络节点以及节点之间的链路等信息。  后台各模块采用Restlet框架，把身份信息、权限信息等数据封装成REST资源，实现web-service服务，从而达到与前端页面交互的功能。  应用身份信息管理模块负责维护应用的身份信息，身份信息包括应用ID，应用名称，应用密钥，应用注册商等属性，将身份信息等数据存储在内存数据库中，实现了信息的增删改查等功能。  权限管理模块负责调整应用所具有的权限，同时将权限信息存储在内存数据库中，实现了对应用的权限授予，查询，移除等功能。  当应用在北向接口接入floodlight控制器，对控制器的资源的发起访问时：  身份认证模块通过应用的ID和应用密钥对应用进行身份识别。若为未经注册的非法应用，则认证结果为拒绝；若为合法应用，则认证结果为通过，再交给权限检查模块进行权限的核查。  权限检查模块首先在内存数据库中通过的ID找到应用的权限列表，然后查看应用是否具有访问该资源的权限，如果具有，则通过审核，最后交给XACML访问控制模块进行基于属性的访问请求的判决。如果不具有，则被视为越权访问，应用无法访问该资源。  XACML访问控制模块采用了一种用于决定请求/响应的通用[访问控制](http://baike.baidu.com/item/%E8%AE%BF%E9%97%AE%E6%8E%A7%E5%88%B6)策略语言和执行授权策略的访问控制算法XACML，实现了基于属性的访问控制。首先通过与属性控制管理前端页面交互得到关于主体属性（应用注册商）和环境属性（允许访问的时间段）这两个属性的访问控制策略policy,然后把通过身份认证和权限检查的应用的访问请求转化为Request，策略执行点PEP通过上下文处理器把Request交给策略决策点PDP进行评估，PDP把请求Request和访问控制策略policy进行匹配，若应答结果Response为Permit，则允许访问，若是Deny则拒绝。这种基于属性的访问控制策略在一定程度上使得访问控制具有较好的灵活性。  日志记录模块：采用java日志框架logback实现。当应用的访问请求在身份认证模块、权限检查模块、XACML访问控制模块中的判决结果为拒绝（即不允许访问）的时候， 日志记录模块会将这些非法的访问请求记录到日志文件中，为以后恶意应用的检测提供依据。   1. 已完成部分   目前已成功安装和使用floodlight,并在floodlight内开发一个新的安全模块（应用访问权限管理系统AAPS），已经实现的模块有前端页面、应用身份信息管理、权限管理、身份认证、权限检查、日志记录、内存数据库等模块。管理员可以通过前端页面注册一个新的应用，同时对应用的权限进行初始化授予，当应用访问控制器资源时，身份认证和权限检查模块均能对应用的访问做出正确的判决结果。日志记录模块也能对非法的访问请求进行记录。 | | | | | | | | |
|  | 是否符合任务书要求进度 符合 | | | | | | | | |
| 尚  需  完  成  的  任  务 | 除了现在已经完成的功能之外，目前系统的XACML访问控制模块尚未完成，在完成XACML访问控制模块后，还需要对系统的功能进行整体的调试：   1. 完成XACML访问控制模块，管理员能够对应用注册商和允许访问的时间段进行设置，   实现基于属性的访问控制功能。   1. 将各个模块整合，进行整体的调试，解决调试过程中各个模块可能出现的问题。 2. 对调试完毕的系统置于SDN架构中进行功能测试和性能分析。 | | | | | | | | |
| 能否按期完成设计（论文） 能 | | | | | | | | |
| 存  在  问  题  和  解  决  办  法 | 存  在  问  题 | | 前端页面和后台模块的数据交互、日志文件的记录还存在一定的BUG。 | | | | | | |
| 拟  采  取  的  办  法 | | 对进行数据交互的部分程序、日志文件记录的部分程序继续调试修改。 | | | | | | |
| 指导教师签字 | | |  | | 日期 | | 年 月 日 | | |
| 检查小组意见 | | | 负责人签字： 年 月 日 | | | | | | |