

北 京 邮 电 大 学

本科毕业设计（论文）开题报告

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	物联网技术中心	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				

1. 选题的背景和意义

随着云计算、移动互联网以及大数据等新技术的发展和成熟，SDN 体系架构的出现为目前网络问题的解决提供了新的方向。但随着 SDN 相关网络设备的出现，安全问题成为制约其发展的一个重要因素，因此 SDN 安全性研究具有较高的研究价值和应用前景。

本选题通过研究 SDN 的网络技术架构原理及目前的发展现状，进而对 SDN 架构中的安全特点、安全威胁进行分析。设计出一种面向安全的 SDN 架构，对 SDN 应用进行访问控制，包括应用的注册，访问控制器相关资源时进行身份认证和权限管理，从而在北向接口方面增强 SDN 的安全能力。

2. 研究的基本内容和拟解决的主要问题

2.1 研究的基本内容

- 1) 学习和研究 SDN 架构的特点和原理，存在的安全问题以及主要解决思路。
- 2) 选取一种 SDN 开源控制器，研究该控制器的架构原理和运行机制，掌握在该控制器内进行开发的流程和方法。
- 3) 学习和研究当前 SDN 安全技术中关于应用的权限管理方法和主流的访问控制技术，完成应用访问权限管理系统的设计。
- 4) 在选取好的控制器的基础上编程实现新的安全模块即应用访问权限管理系统。
- 5) 将完成的系统置于整体的架构中进行测试和分析，并完成论文的撰写。

2.2 拟解决的主要问题

为了在已有的开源控制器的基础上完成对应用的认证和权限管理，需要解决大致如下几个问题：

- 1) 需要定义一组完整的权限集合。针对选取的控制器上应用程序访问的资源进行细粒度的权限定义，这些权限反映了开发人员开发 SDN 应用时所能够对控制器北向接口资源进行的操作，在应用程序读取网络状态和写入网络策略时使用。具体的定义方法还需对控制器的相关资源进行研究。
- 2) 如何解决应用的身份认证问题。目前网络安全中身份认证主流的方法是使用证书进行认证。应用在注册时候会向系统写入身份信息，作为其身份证明的安全证书。如何利用安全证书识别应用的身份，拒绝非法应用的接入的具体过程有待进一步研究学习。
- 3) 如何解决应用对资源的访问控制问题。在应用注册时已经被授予相关权限的基础上，能否利用其它属性，如应用的注册商，有效期，访问资源时的时间等，结合当前主流的访问控制技术，实现一种基于属性的访问控制策略，使应用对资源的访问控制具有较高的灵活性。
- 4) 如何解决在之前选取好的控制器内进行新模块开发的问题。应用的访问权限管理系统是作为新的安全模块加入到控制器中，因此需要借助相关文档和源代码研究，学习和掌握在控制器内添加一个新的模块的开发和调试过程。
- 5) 系统如何对应用的非法访问进行记录。最常用的方法是采用日志管理。能否寻找一种开源的日志框架，对越权的访问进行实时记录审计是关键。同时日志管理也能为以后恶意应用的鉴别提供依据。

3.研究方法及措施

根据本课题的研究内容和拟解决的主要问题，主要采用以下方法进行研究：

- 1) 阅读相关的文献资料，理解 SDN 架构的原理和特点，学习 SDN 的安全技术以及发展现状。为访问权限管理系统的设计提供参考。
- 2) 选择一种 SDN 开源控制器。通过研究该控制器的源代码和相关文档，理解其运行机制和原理，学习该控制器源代码中使用的框架，掌握该控制器模块化开发的方法。
- 3) 系统设计。对访问权限管理系统进行需求分析，初步得出大体架构，再对各功能模块进行细化，如应用注册流程的设计，访问控制策略的设计等。
- 4) 系统实现。作为控制器的新增的安全功能模块，系统的最终实现需要依赖控制器原有的开发环境。因此需要提前学习实现过程中需要的编程技术。此外网络管理员需要通过 web 页面和访问权限管理系统进行交互，因此还需要提前学习前端的相关编程技术。在此基础上按照之前的设计方案，编程实现系统的各项功能。
- 5) 系统测试。在访问权限管理系统编程实现后，作为控制器的安全模块，需要在 SDN 整体架构中进行测试，已验证预期的安全功能是否实现。
- 6) 开发文档记录。对系统的设计与实现过程，实际开发中可能发生的改动、遇到的问题以及解决办法进行记录。形成较为完整的说明文档。

4.研究工作的步骤与进度

第 1-3 周：了解毕设课题目标及内容，查找国内外相关文献资料。对 SDN 架构的原理和特点、存在的典型安全问题、已有的安全技术进行研究。

第 4-6 周：选取一种 SDN 开源控制器，研究该控制器的使用和模块开发方法，学习和掌握源代码在北向接口方面应用程序接入控制器的实现机制和原理；对 SDN 应用的访问权限管理系统完成整体上的功能设计；

第 7-12 周：依据之前的系统设计方案对各个模块进行具体实现，在后续的开发过程根据实际需要和可能出现的问题进行一定的调整，完成后对系统进行充分的调试和完善，并在整体架构中进行测试和检验。

第 13-16 周：完成本科毕业设计论文，准备答辩。

5.主要参考文献

- [1]Shin S, Song Y, Lee T, et al. Rosemary:A Robust, Secure, and High-performance Network Operating System[J]. 2014:78-89.
- [2]Ferguson A D, Guha A, Liang C, et al. Participatory Networking: An API for Application Control of SDNs[J]. Computer Communication Review, 2013, 43(4):327-338.
- [3]Porras P, Cheung S, Fong M, et al. Securing the Software-Defined Network Control Layer[J]. 2015.
- [4]Shin S, Porras P, Yegneswaran V, et al. FRESCO: Modular Composable Security Services for Software-Defined Networks.[J]. Proceedings of Network & Distributed Security Symposium, 2013.
- [5]Shin S, Yegneswaran V, Porras P, et al. AVANT-GUARD: scalable and vigilant switch flow management in software-defined networks[C]// ACM Sigsac Conference on Computer & Communications Security. ACM, 2013:413-424.
- [6]Wen X, Chen Y, Hu C, et al. Towards a secure controller platform for openflow applications[C]// ACM SIGCOMM Workshop on Hot Topics in Software Defined NETWORKING. ACM, 2013:171-172.
- [7]Klaedtke F, Karame G O, Bifulco R, et al. Access control for SDN controllers[C]// ACM SIGCOMM Workshop on Hot Topics in Software Defined NETWORKING. ACM, 2014:1325-1335.
- [8]王蒙蒙, 刘建伟, 陈杰, 毛剑, 毛可飞. 软件定义网络:安全模型、机制及研究进展[J]. 软件学报, 2016, (04) :969-992.
- [9]王淑玲, 李济汉, 张云勇, 房秉毅. SDN 架构及安全性研究[J]. 电信科学, 2013, (03) :117-122.
- [10]刘捷. 基于 XACML 的云计算访问控制系统的设计与实现 [J]. 信息与电脑(理论版), 2015, (18) :22+26.

指导教师签字		日期	年 月 日
--------	--	----	-------

注：可根据开题报告的长度加页。