



浅析 SDN 安全需求和安全实现

周苏静

(中兴通讯股份有限公司 南京 210012)

摘要:首先对 SDN 和网络安全相关的架构(如 SANE、Ethane)进行了调研;其次,分析了 SDN 的安全需求和安全应用的现状,包括应用层和控制层之间、控制层和转发平面之间的安全需求研究现状以及在 SDN 上实现安全应用的现状;最后,探讨了 SDN 应用的认证、授权的解决方案,并对策略冲突消解、网络安全应用实现的现状进行了总结。

关键词:软件定义网络;安全;认证;授权

doi: 10.3969/j.issn.1000-0801.2013.09.022

Study on Security in SDN

Zhou Sujing

(ZTE Corporation, Nanjing 210012, China)

Abstract: Security related SDN architecture was investigated, including SANE, Ethane, etc., then current state on security requirement analysis in SDN was reported, which was separated into two parts, one was between application plane and control plane, and the other was between control plane and data plane. Subsequently, the mechanisms of security applications in SDN were discussed, especially the resolutions on application authentication and authorization using OAuth and ABFAB framework. In the end, a summarize in policy conflict resolution and security implementation were given.

Key words: software defined networking, security, authentication, authorization

1 引言

2007 年,作为斯坦福大学 Clean State 的项目成员,Casado M 等人提出了 SANE 网络架构和 Ethane 网络架构,用于提供企业网络中的安全管理^[1]。由于技术本身的优势和相应的技术推广,这种网络架构被重新命名为软件定义网络 (software defined networking, SDN),并被认为是替代传统层次网络架构、解决当前和未来网络爆炸性需求的一种革新技术^[2]。有意思的是,目前的 SDN 版本,例如基于 OpenFlow 的 SDN^[3]对网络安全却很少提及。

鉴于互联网技术的发展历程经验,人们广泛意识到,网络设计的初期就应该考虑到其中的安全问题。于是近年

来,也有不少对 SDN 的安全需求分析^[4,5]、安全解决方案^[6,7]提出,但是这一切都刚刚开始,本文对近年来的 SDN 安全进展做一个初步总结,对其中的解决方案做一个初步分析。

2 SDN 安全性简介

2.1 SANE 架构

SANE^[1]是 Casado M 等人提出的一个理想的网络架构,原型实现后,在 7 个主机构成的 Ethernet 上运行了一个月。SANE 的网络架构主要包含一个集中控制器(DC),其中的交换机、主机均要做相应改造,以支持这种架构,如图 1 所示。

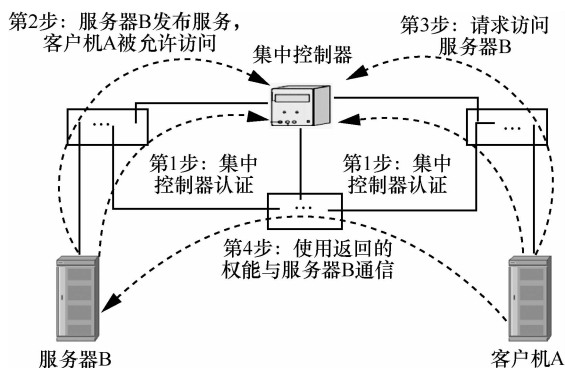


图1 SANE 的架构和流程

集中控制器的功能主要包括:认证所有网元、名称解析、全网拓扑学习、权能生成。其中权能 (capability) 是 SANE 引入的一个数据类型,即加密的路径信息。集中控制器和每个网元之间共享一个唯一密钥,为任意两个网元之间的通信计算路径,并根据路径上的网元和网元的密钥生成一个权能,每个数据报文都携带一个权能,途径上的每个交换机通过检查权能决定是否允许通行。

如图1所示,第1步,服务器B和客户机A都进行集中控制器认证,获得共享的密钥;第2步,服务器B发布服务,设置访问控制列表,其中客户机A被允许访问;第3步,客户机A向集中控制器请求访问服务器B,集中控制器从服务器B的访问控制列表中查到A的权限,计算A到B的路径,生成路径上的权能,发给客户机A;第4步,客户机A访问服务器B,每个 Ethernet 报文中都包含权能,权能有效期(设计为几分钟)后,客户机A如果要继续访问服务器B,就需要再次申请权能。

如上所述,SANE 架构的效率比较低,不适合在实际中使用,因此 Casado M 等人又提出了 Ethane 架构^[1]。

2.2 Ethane 架构

Ethane^[1]是个比较实用的提供集中网络安全管理的网络架构,它把 SANE 架构中横向传输的加密的控制报文头,变为纵向传输的加密控制信息——集中控制器和交换机之间通过安全信道传输控制信息。

集中控制器的功能包括认证网元和用户、许可检查、路由计算、交换机管理。Ethane 并没有规定具体的认证方法,Casado M 等人的原型实现中使用证书和 SSL 协议认证交换机和集中控制器,并用 SSL 加密集中控制器和交换机之间的通信。交换机不仅不需要检查权能,甚至不需要目前 Ethernet 交换机和 3 层交换机的一些功能。

2.3 SDN 架构

SDN 架构^[3]如图2所示,SDN 具有如下优点:高可扩展性/高灵活性的网络部署、精细高效的数据流控制等。SDN 提供对网络设备的集中式、自动化管理、统一的策略执行,和目前的网络架构相比提高了可靠性、安全性。而传统的网络安全应用,如访问控制、防火墙、入侵检测、入侵防御等也可利用 SDN 控制器的开放 API 实现或者方便地集成到 SDN 中。

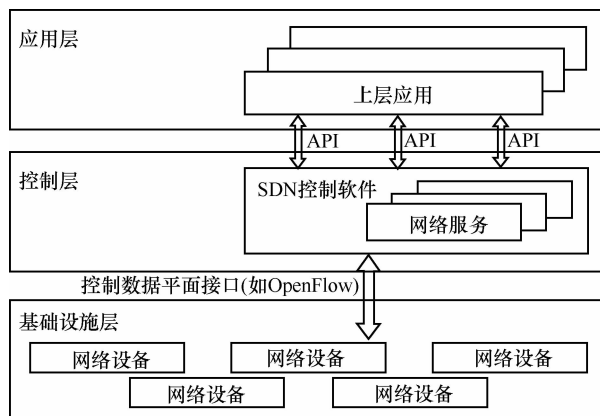


图2 SDN 架构

如上所述,SDN 架构提供了一个平台,可以为它提供安全保障,并提供安全服务。大多数研究者认为,目前积累的网络安全技术完全能够胜任 SDN 的安全需求,如王淑玲等人提出的 SDN 安全技术架构^[8,9]和传统网络安全技术架构基本无差异。但是具体提供哪些安全机制,如何设计、实现,还在研究中。

3 SDN 的安全需求

Hartman S 和 Wasserman M 等人认为 SDN 的安全需求主要发生在应用层和控制层之间,包括应用的授权、认证、隔离以及策略冲突的消解^[5]。

控制层(或控制平面)和基础设施层(或转发平面)之间,在一个交换机被一个控制器控制的情况下,安全威胁模型比较简单,现有的 OpenFlow 中的相关规范经过细化后可以满足安全需求^[4];而一个交换机被多个控制器控制的情况下,安全威胁模型比较复杂,需要考虑控制器之间的授权、增加控制器对交换机资源的细粒度的访问控制,这正是现有 OpenFlow 规范所缺乏的。

对于如何在 SDN 架构上实现传统的网络安全应用,如访问控制、防火墙、入侵检测、入侵防御等,或者如何定义 SDN 控制器的相关 API 以实现上述功能,也是一个值

得研究的课题。

选择哪些网络安全应用在 SDN 架构上实现,也是要考虑的问题,一方面由于 SDN API 的局限,如基于 DPI(深度报文检测)的安全应用不能作为 SDN 的一个应用实现;另一方面,放弃现有的软件实现而在 SDN 上重新实现,所花费的代价是否值得也是一个问题。SDN 架构的优势在于低成本地、灵活地实现一些传统应用,甚至或许能够引出一些创新的网络安全应用/服务。

4 SDN 安全解决方案

4.1 应用的授权、认证、隔离

应用的隔离事关安全,但也是安全网络操作系统会遇到的问题,尤其是虚拟化技术经常遇到的问题,在此不探讨解决方案。下面主要关注应用的授权、认证。

Hartman S 和 Wasserman M 等人探讨了 3 种授权、认证机制应用在 SDN 上的可能性,尤其是在跨域的情况下^[5]:第 1 种,通过代理认证;第 2 种,直接分发跨域的认证凭据(如对称密钥、证书的私钥等);第 3 种,通过联合认证方式(如 OAuth^[10]、ABFAB^[11])。其中最后一种方式,即联合认证方式,具有灵活的特点,便于在多种场合使用。但是参考文献[5]并没有给出 OAuth、ABFAB 在 SDN 上的具体应用方式。

OAuth^[10]本质上是一种授权协议,用于用户或一个应用授权给另一个用户或应用访问其拥有的资源,而不泄露第一个用户或应用的认证凭据(如密钥等)。OAuth 架构的实体包括被授权方(client)、授权方(resource owner)、授权服务器(authorization server)、资源服务器(resource server)。

OAuth 的工作流程包括授权码(authorization code)方式、隐式授权(implicit grant)方式、资源主口令(resource owner password credential)方式、客户密钥(client credential)方式。其中,资源主口令方式是 OAuth 为了兼容引入的授权方式,客户密钥方式和上述第 2 种直接分发跨域密钥类似,而隐式授权方式是简化的授权码方式,为了方便 JavaScript 实现的被授权方。

OAuth 还有一种基于断言(assertion)的框架^[12],是为了兼容其他的身份认证管理系统。OAuth 的断言框架中,有一种是客户端代表用户的场景,和授权代码方式类似,被授权方利用第三方 token service 发来的断言向授权服务器请求访问令牌。断言框架的优点是能够兼容很多断言形式,如资源主的授权签名。

综上所述,认为适于 SDN 架构的 OAuth 是授权码方式,是可以在断言框架下实现的授权码方式。两个不同控制器上的应用分别作为被授权方和资源主,资源主所在的控制器上的一个模块或者一个独立于两个控制器的服务器可以作为授权服务器。

具体地,如图 3 所示,App2 为被授权方,App3 为资源主,App2 要访问 App3 的资源,就要从 AS 获得访问令牌。一种方式是 App2 直接从 App3 获得断言,使用断言从 AS 获得访问令牌;另一种方式是 App3 把 App2 的资源请求转向到 AS,AS 对 App3 认证后,通过 App3 给 App2 发放授权码,App2 使用授权码从 AS 获得访问令牌。App3 也可以是控制器 2 的一个模块,这时 App2 直接向控制器 2 申请访问资源。

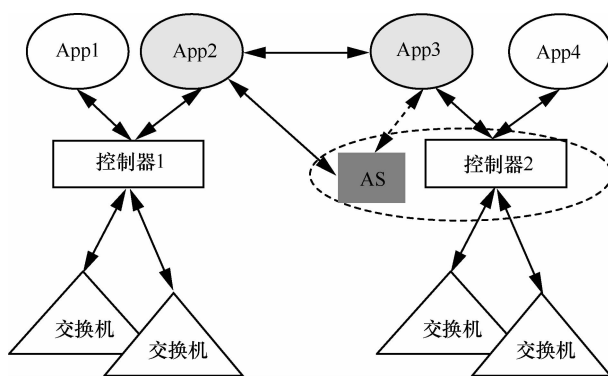


图 3 OAuth 在 SDN 上的一个应用

ABFAB 架构^[11]主要提供统一或联合认证,其中的实体包括用户(client)、认证依赖方(relying party, RP)、认证提供方(identity provider, IdP)。其中被授权方和 IdP 之间有长期关系,例如被授权方是 IdP 的注册用户,双方共享密钥;RP 和 IdP 有联盟关系,RP 依赖 IdP 提供的认证结果;RP 根据 IdP 提供的认证结果为被授权方提供相对应的服务。

利用 ABFAB 架构为 SDN 提供跨域认证,可以将两个控制器上的模块、应用或独立的认证服务器作为 RP,互相作为对方的 IdP。

具体的例子如图 4 所示,App2 想访问控制器 2 控制的资源,控制器上的 RP 模块请求 App2 所属的 IdP 认证,从 IdP 获得认证结果,决定是否授权给 App2 相应的资源。

OAuth 和 ABFAB 也可结合使用,例如,App3 利用 ABFAB 获得对 App2 的认证结果后,给 App2 发放断言,App2 使用该断言从 AS 获得访问令牌,如图 5 所示。

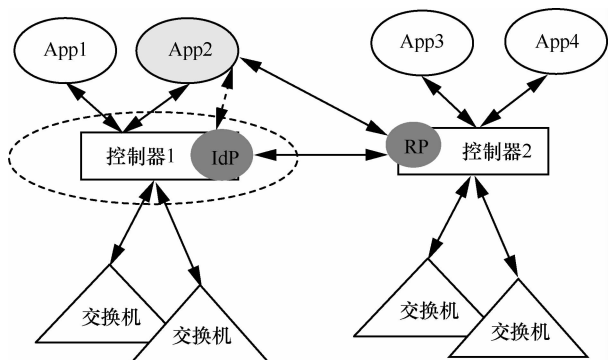


图4 ABFAB在SDN上的一个应用

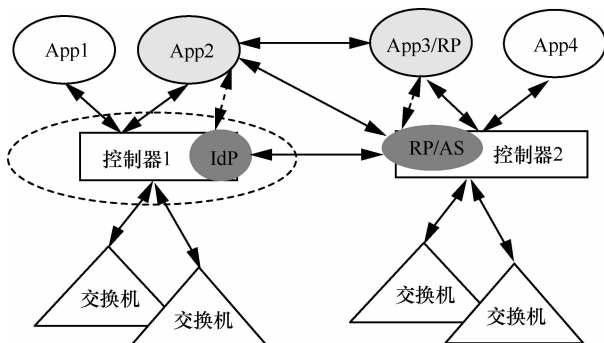


图5 OAuth和ABFAB同时在SDN上的一个应用

4.2 策略冲突的消解

Porrasy P等人提出一种安全加固的控制平面操作系统 FortNOX^[6]。FortNOX通过扩展开源的NOX操作系统的Send_Openflow_Command模块,增加了策略冲突消解功能。来自不同应用的策略被设定不同的安全等级,如来自安全应用,即可信任的应用,如防火墙、入侵检测、入侵防御等提供安全服务的应用的策略具有最高优先级,控制层操作系统的本地应用产生的策略具有中等优先级,其他提供业务的应用被分配最低优先级。

扩展后的FT_Send_Openflow_Command汇集所有应用产生的策略,验证接收到的来自应用的策略携带的数字签名,对策略进行源认证;检查策略冲突是否存在,并根据应用的优先级决定策略冲突发生时的动作。

4.3 网络安全应用的实现

Shin S等人提出了一个在SDN架构上开发网络安全应用的开发环境FRESCO^[7],FRESCO本身作为SDN应用层的一个应用,运行在上面所述的安全加固的控制层操作系统(增强的NOX)上。

FRESCO包含实现若干基本安全模块,如扫描探测,复杂的安全应用模块通过对基本模块的组合实现,如把扫描引导到蜜罐。

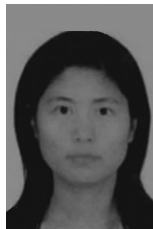
5 结束语

本文对SDN和网络安全相关的架构进行了调研,分析了SDN的安全需求和安全应用的现状,探讨了SDN应用的认证、授权解决方案。

参考文献

- 1 Casado M. Architectural support for security management in enterprise networks. Doctoral Dissertation, Stanford University, 2007
- 2 ONF. Software-Defined Networking: the New Norm for Networks. ONF White Paper, 2012
- 3 ONF. OpenFlow Switch Specification Version 1.3.1, 2012
- 4 Wasserman M, Hartman S. Security Analysis of the Open Networking Foundation (ONF) OpenFlow Switch Specification. IETF Draft (draft-mrw-sdnsec-openflow-analysis), 2013
- 5 Hartman S, Wasserman M, Zhang D. Security Requirements in the Software Defined Networking Model, IETF Draft (draft-hartman-sdnsec-requirements), 2013
- 6 Porrasy P, Shinz S, Yegneswaran V, et al. A security enforcement kernel for OpenFlow networks. Proceedings of the ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking (HotSDN), Helsinki, Finland, August 2012
- 7 Shin S, Porras P, Yegneswaran V, et al. FRESCO: modular composable security services for software-defined networks. Proceedings of the ISOC Network and Distributed System Security Symposium, San Diego, CA, February 2013
- 8 王淑玲,李济汉,张云勇等. SDN架构及安全性研究. 电信科学, 2013(3)
- 9 郭春梅,张如辉,毕学尧. SDN网络技术及其安全性研究. 信息安全, 2012(8)
- 10 Hardt D. The OAuth 2.0 Authorization Framework. IETF RFC6749, 2012
- 11 Howlett J, Hartman S, Tschofenig H, et al. Application Bridging for Federated Access Beyond Web (ABFAB) Architecture. IETF Draft (draft-ietf-ABFAB-arch), 2012
- 12 Campbell B, Mortimore C, Jones M, et al. Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants. IETF Draft (draft-ietf-oauth-assertions), 2013

[作者简介]



周苏静,女,博士,中兴通讯股份有限公司高级预研工程师,主要研究方向为信息安全。

(收稿日期:2013-06-04)