浅析SDN安全需求和安全实现

Analysis of Security Requirements and Implementation in SDN

周苏静

(中兴通讯股份有限公司 南京 210012)

大摘要:

首先对SDN和网络安全相关的架构进行了调研。SANE是一个理想的网络架构,主要包含一个集中控制器和每个网元之间共享的一个唯一密钥,为任意两个网元之间的通信计算路径,每个数据报文都携带用于存放加密路径信息的权能(capability),路径上的每个交换机通过检查权能决定是否允许通行。SANE架构安全性有余,但效率不足,不适合实际中使用。Ethane架构是一个比较实用的提供集中网络安全管理网络架构,它把SANE网络架构中横向传输的加密控制报文头,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,已经和目前的SDN架构,如OpenFlow的SDN架构没有太大的差别。

SDN和目前的网络架构相比提高了可靠性、安全性,同时提供了一个平台,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,但是具体提供哪些安全机制、如何设计、实现,还在研究中。

本文报告了SDN的安全需求和安全应用的现状。

(1)应用层和控制层之间

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。

(2)控制层和转发平面之间

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;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,这是现有的OpenFlow规范所缺乏的。

(3)如何在SDN架构上实现传统的网络安全应用

如何在SDN架构上实现访问控制、防火墙、入侵检测、入侵防御等传统网络安全应用,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。

本文探讨了SDN应用的认证、授权的解决方案。

(1)应用的授权、认证、隔离

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,尤其是跨域的情况下: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、ABFAB)。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。但是并没有给出OAuth、ABFAB在SDN上的具体应用方式。

笔者认为适于SDN架构的OAuth是授权码方式,可以是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客户端和resource owner,resource owner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AS。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或作为RP,互相作为对方的IDP。OAuth和ABFAB也可结合使用。

(2)策略冲突的消解

Porrasy等人提出一种安全加固的的控制平面操作系统FortNOX。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等级,控制层操作系统的本地应用产生的策略具有中等优先等级,其他提供业务的应用被分配为最低优先等级。

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。

(3)网络安全应用的实现

Shin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,FRESCO本身作为SDN应用层的一个应用,运行在控制层操作系统上。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,如把扫描导引到蜜罐。

关键词:软件定义网络;安全;认证;授权