ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.19, No.1, January 2008, pp.167−176
DOI: 10.3724/SP.J.1001.2008.00167

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

SE-BGP:一种 BGP 安全机制*

胡湘江+, 朱培栋, 龚正虎

(国防科学技术大学 计算机学院,湖南 长沙 410073)

SE-BGP: An Approach for BGP Security

HU Xiang-Jiang+, ZHU Pei-Dong, GONG Zheng-Hu

(School of Computer, National University of Defense Technology, Changsha 410073, China)

+ Corresponding author: Phn: +86-731-4574606, E-mail: csriver@126.com, http://www.nudt.edu.cn

Hu XJ, Zhu PD, Gong ZH. SE-BGP: An approach for BGP security. *Journal of Software*, 2008,19(1):167−176.
http://www.jos.org.cn/1000-9825/19/167.htm

Abstract: BGP (border gateway protocol) security is very important to the inter-domain routing security. Many solutions have been proposed, but none has been deployed until now. This paper analyzes the main problems of these approaches. It studies the AS (autonomous system) topology of the Internet, especially the rich-club property, and gives the notion of the AS alliance. It proposes SE-BGP (security enhanced BGP) as a new way for BGP security. An alliance-based security architecture, and a new trust model-TTM (translator trust model) for SE-BGP are constituted. An authentication scheme based on TTM is also designed. Furthermore, the way of how to extend the BGP protocol is considered. The SE-BGP has strong ability of security and good scalability, and the number of the used certificates is about 1% of the traditional solutions.

Key words: BGP (border gateway protocol) security; SE-BGP (security enhanced BGP); AS (autonomous system) alliance; trust model; TTM (translator trust model)

摘 要: BGP(border gateway protocol)协议的安全是 Internet 路由系统安全的关键.目前已提出多种 BGP 安全机制,但都未能得到部署.对 BGP 安全机制的部署问题进行深入分析,利用 AS(autonomous system)结构的 Rich-Club 特性,提出 AS 联盟的概念,设计了一种 BGP 安全机制:SE-BGP(security enhanced BGP).SE-BGP 采用基于 AS 联盟的安全体系结构,使用一种具有分布式认证中心的新的信任模型——TTM(translator trust model).设计了基于 TTM 模型的认证算法,给出了基于现有 BGP 协议的扩充实现方法.与已有的安全机制相比,SE-BGP 在保证安全能力的同时,所需的证书规模大约为原有机制的 1%,具有良好的可扩展性.

关键词: BGP(border gateway protocol)安全;SE-BGP(security enhanced BGP);AS(autonomous system)联盟;信任模型;TTM(translator trust model)

中图法分类号: TP393 **文献标识码**: A

* Supported by the National Natural Science Foundation of China under Grant No.60673169 (国家自然科学基金); the National Basic Research Program of China under Grant No.2003CB314802 (国家重点基础研究发展计划(973)); the National High-Tech Research and Development Plan of China under Grant No.2006AA01Z213 (国家高技术研究发展计划(863))

Received 2006-06-15; Accepted 2006-11-03

域间路由安全对于整个互联网的安全具有重要的意义.美国已将域间路由安全作为国家级战略安全的组成部分.增强域间路由安全的关键之一就是提高域间路由协议的安全性.BGP(border gateway protocol)协议作为当前唯一的域间路由协议,本身存在着巨大的安全隐患[1,2].

BGP 安全性的核心问题就是确保信息发布的可靠性,其中最重要的信息就是地址源信息和路径属性.当前,对于 BGP 的安全性已有很多的研究,然而仍没有一种安全机制得到部署.

本文研究了当前各种机制未能得到部署的关键问题,根据互联网 AS(autonomous system)拓扑连接的特性,设计了一种新的 BGP 安全协议机制.该机制采用基于 AS 联盟的安全体系结构,并在此结构上提出了一种新的信任模型 TTM(translator trust model).认证算法只需获取局部 AS 联盟证书,从而简化了证书的管理,具有较好的可扩展性.

本文第 1 节总结当前的相关研究工作,并分析其中的不足.第 2 节分析当前互联网 AS 拓扑连接关系,提出 AS 联盟的概念.第 3 节基于这种概念设计 SE-BGP(security enhanced BGP)的安全体系结构,并提出一种新的信任模型 TTM.第 4 节基于此模型设计认证算法,并讨论对 BGP 协议的修改.第 5 节论证 SE-BGP 的安全能力和性能,分析其可行性和可部署性.第 6 节分析 SE-BGP 的证书规模.结果表明,SE-BGP 极大地降低了认证所需证书的规模,其全网证书规模大约为传统机制的 1%,具有良好的可扩展性.第 7 节是对文章的总结.

1 BGP 安全研究分析

至今已提出多种 BGP 安全机制,其多数都采用了信息认证的方式.目前所提出的基于 PKI(public key infrastructure)认证的安全机制,都是基于两种安全认证模型,即基于根结点的集中式认证模型和网状信任(Web of trust)模型.

BBN 公司的 Kent 于 2000 年提出的 S-BGP(secure BGP)[3]是当前研究中最为完整、最具代表性的安全机制.S-BGP 采用集中式认证模型,其认证层次与前互联网的地址分配层次相对应.其基本思想是使用资源证书和路径属性签名来验证信息的有效性.

Cisio 公司的 White 于 2003 年提出的 SoBGP(secure origin BGP)[4]则采用了网状信任模型.其 PKI 管理 3 类证书:路由器、路由策略和地址源.与 S-BGP 类似,SoBGP 采用源地址证书进行源地址认证.SoBGP 利用拓扑数据库对路径进行认证,无法保证路径属性不被篡改.

对于互联网这种复杂巨系统,这两种认证模型主要存在以下几点不足:

(1) 基于根结点的集中式认证模型很难得到部署,并且会带来新的互联网管理权之争;而网状认证模型的互操作问题比较显著;

(2) 这两种模型在节点进行认证时,需要获取全局证书信息,证书的管理比较困难,并且这种困难将随着互联网规模的增大而不断地加剧,可扩展性较差.

针对这两种安全机制的不足,很多学者提出了改进的安全机制.Aiello 在 2003 年研究了 Merkle 的密码证明结构,提出了一种 OA(origin authentication)认证服务[5],利用带内传递 OAT(origin authentication tags)信息进行源地址认证.Wan 在 2005 年提出的 psBGP(pretty security BGP)[6],利用“邻居作证”的思想,带内传递 PAL(prefix assertion list)进行源地址认证.这两种机制都避免使用全局的源地址证书.Hu 在 2004 年提出的 SPV(security path vector)[7]则采用一次性签名的机制进行路径认证,使得路径认证不需要 PKI 的支持,并且对称式密钥的使用加快了认证的速度. 2003 年,Goodell 提出了 IRV(inter-domain route validation)[8]服务机制采用了另外的认证思想,即在每个 AS 中建立 IRV 服务器,所有的认证都通过 IRV 服务来实现.Subramanian 在 2004 年提出了 Listen-and-Whisper 机制[9],以数据平面和控制平面两个角度出发看待 BGP 的安全性问题,在对 BGP 和网络基础设施仅做出了极小改动的前提下可以发现潜在的威胁.

然而,这些安全机制在获得某个方面改进的同时又会引入新的问题与不足,尤其是没有解决证书的管理这一关键问题.至今还没有一种安全机制能够得到有效的部署.

本文在分析互联网拓扑特性的基础上提出了一种新的 BGP 安全机制:SE-BGP.SE-BGP 以 AS 联盟为单位

建立 PKI 认证中心,利用了一种新的信任模型——TTM.SE-BGP 在认证的过程中只需局部信息就可进行全局认证,在很大程度上简化了证书的管理,具有良好的规模可扩展性.

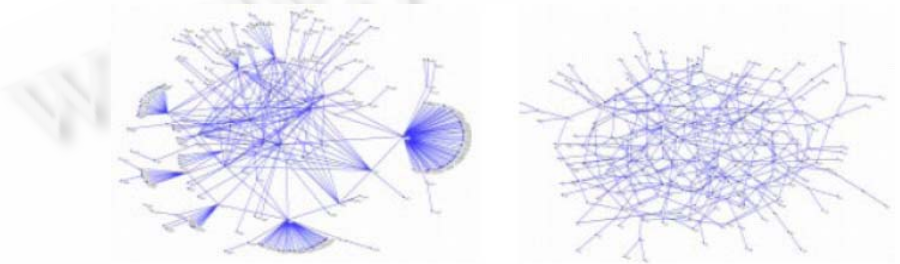
2 AS 自组织性分析

互联网的网络拓扑具有很强的自组织特性,并且这种网络拓扑特性对路由协议有着重要的影响.国外的一些学者已经开始展开这方面的研究,试图将网络拓扑引入到路由协议的设计与分析之中.

互联网由许多 AS 连接而成,AS 之间的关系可分为“提供商-客户”关系和“对等”关系.如果将 AS 看作是图的节点,AS 之间的关系看作节点之间的边,我们就可以得到互联网的 AS 拓扑连接图.目前所提出的 BGP 安全解决方案都未充分考虑到互联网的 AS 拓扑特性.

2.1 AS拓扑特性

1999 年,Faloutsos 通过对 BGP 数据和实时测量数据进行分析,发现 Internet 拓扑存在着幂律特征,即 $P(K)\sim K^{-\gamma}$,γ=2.2.同时,其拓扑连接具有小世界特性,节点之间存在着群聚现象,网络聚集系数为 0.0258(2004 年 3 月).截止到 2006 年 3 月,互联网已使用的 AS 号超过 22 000[10],但是研究数据显示,其中 84%的 AS 为 stub AS.图 1 是互联网中某 300 个 AS 的实际连接图,可以清楚地反映出 AS 拓扑的群聚特性.



(a) The real topology graph of 300 nodes in the Internet (b) A random graph

(a) 互联网中 300 个节点的实际连接图 (b) 随机图

Fig.1 Internet AS topology graph

图 1 互联网 AS 拓扑连接特性示意图

2003 年,Zhou 在进一步研究 Internet 的 AS 拓扑过程中发现,AS 拓扑不仅具有 dissortative mixing 特性,同时也存在 rich-club 现象,即高度节点之间存在很强的集团性,低度节点则具有很高的聚集系数[11,12].也就是说,AS 节点总是聚集成不同的集合,集合中的节点通过少数高度数节点与集合外的节点相连,并且高度数节点之间具有很高的聚集度.图 1 也能清晰地反映出 rich-club 现象.为进一步分析网络的这种群聚现象,我们引入以下定义:

定义 1. 所谓“AS 联盟(AS alliance)”指的是一组 AS 节点,这组 AS 节点只通过少数的节点与组外其他节点相连和转发流量;这些少数的节点也称为“关键节点”.

在这种意义上,互联网是由 AS 联盟通过关键节点之间的相互连接而形成的.

AS 拓扑中,AS 联盟的形成是由互联网的连接特性和成长特性所决定的.互联网的商业关系对于互联网的连接特性和成长特性至关重要.在现实情况中,这些关键节点往往也是 ISP 的数据转发中心,相比之下,具有较高的安全能力和数据处理能力,同时也会具有较高的信任依赖度(即其他多个 AS 都对其表示出某种信任依赖).从这个意义上讲,网络的拓扑特性也反映出网络的信任关系特性.即具有相同信任依赖的 AS 节点聚集成集,而大量较高信任度的节点具有很高的连接度.这一现象,我们可称为信任关系的 rich-club 现象.

2.2 AS拓扑特性发展预测

当前,互联网的规模发展迅速,2005 年 7 月已经分配了 39 000 个 AS 号,预计到 2013 年,16 位 AS 号将全部

分配完.PFP(positive-feedback preference)模型[13]由于能够模拟 rich-club 现象而成为目前最准确的 Internet 网络拓扑模型.通过 PFP 模型,我们可以对互联网拓扑的发展作出预测.结果表明,未来随着互联网规模的增大,网络的平均路径长度则会减小,但其密率特性和 rich-club 特性几乎保持不变.这是因为互联网的连接特性和成长特性并不会发生本质的改变.

3 SE-BGP 的体系结构和信任模型

3.1 整体结构

我们根据 AS 拓扑的特性提出了一种新的 BGP 的安全机制——SE-BGP.SE-BGP 使用 IPSec 保证 AS 之间的会话安全.与 S-BGP 相似,SE-BGP 需要 PKI 的支持.我们将建立了 PKI 的 AS 联盟称为“安全 AS 联盟”,记作 SA,同时将关键节点记做 *T*.在安全 AS 联盟中的局部范围内,采用的源认证和地址认证的方式与 S-BGP 相类似.数字签名的算法选择 DSA(digital signature algorithm),DSA 的签名过程可以对一些参数进行预处理,可以极大地提高签名的速率.由于安全 AS 联盟中节点通过关键节点与 AS 联盟外的节点相连,可通过关键节点之间的制约与合作,使得 AS 联盟中的节点仅仅通过局部信息就可对 AS 联盟外的源地址信息和路径信息进行认证.

图 2 举例说明了一个可能的 AS 联盟连接图.图中有 4 个安全 AS 联盟.

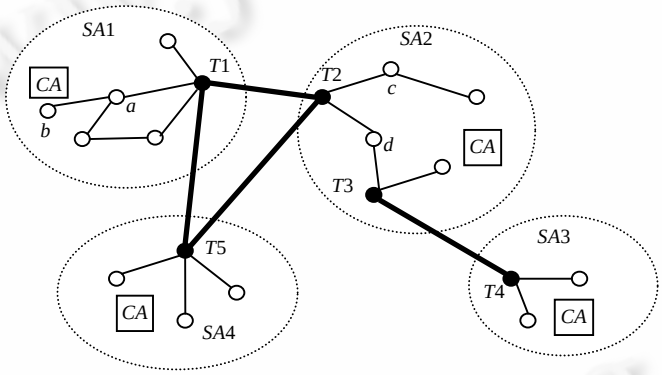


Fig.2 AS alliance link graph

图 2 AS 联盟连接图

3.2 AS联盟生成算法

要利用 AS 联盟特性,首先要确立 AS 联盟生成的算法和原则.AS 联盟的生成可以按照下述方法生成:首先从 rich 节点中确立关键节点(一般是较大 ISP 的数据转发中心)作为 AS 联盟中的第 1 个节点,然后将这个关键节点的所有非其他关键节点的客户节点加入到 AS 联盟中.如果加入的节点还有非其他关键节点的客户节点,则继续将其加入,直到 AS 联盟中的所有非其他关键节点的客户节点都加入到这个 AS 联盟为止.出于实际操作的考虑,我们可能需要对 AS 联盟的范围进行调整.

互联网中有 51%的节点属于 Multi-homed stub 节点,这些节点会同时属于不同的 AS 联盟.由于 stub 节点并不转发域间流量,因此,虽然同时属于不同的 AS 联盟,也并不会影响所属 AS 联盟的完整性.

3.3 联盟内认证中心

AS 联盟内的认证中心 CA(certificate authority)可由“权威”部门(例如,政府、大型 ISP 等)进行组织和管理.安全 AS 联盟中的每一个节点都需要向认证中心提出证书申请,认证的范围包括地址分配单元和 AS 号.认证中心在对申请进行核实后,向 AS 节点发布证书.证书的主要内容包括 ASN、地址分配单元以及相应的公钥.

SE-BGP 的一个特别之处在于,与安全 AS 联盟中关键节点相连的其他安全 AS 联盟中关键节点也需要在这个安全 AS 联盟中进行认证.如图 2 所示,安全 AS 联盟 *SA*1 与 *SA*2 相连.*SA*1 中的关键节点 *T*1 要在 *SA*2 中申请

证书;同样,*SA*2 中的节点 *T*2 也要在 *SA*1 中申请证书.

安全认证中心还要发布一个“关键节点连接表”,表中记录着安全区的关键节点以及与这个关键节点相连的其他安全区的关键节点.安全联盟中的任何一个节点都需要获取这个表.图 2 中,*SA*2 的关键节点连接表见表 1.

Table 1 Key node lists table

表 1 关键节点连接表

*K*_IN	*K*_OUT
*T*2	*T*1
*T*2	*T*5
*T*3	*T*4

3.4 TTM模型

按照上述结构,我们提出一种新的信任模型——转换者信任模型 TTM.TTM 基于分布式的 PKI 结构.与传统的网状结构不同,每个 CA 之间并不相互认证证书.其信任关系的传递是通过关键节点的特殊能力实现的.TTM 结构如图 2 所示.关键节点 *T*1,*T*2 同时拥有两套公钥证书.即 *T*1,*T*2 都具有 *SA*1 和 *SA*2 中的公钥证书.

首先定义两个函数:

$S_k(m)$表示节点 k 对其发布的信息 m 进行签名;

$V_k(s)$表示用节点 k 的公钥对签名 S 进行验证;

那么对于节点 k,接受其发布信息 m 的条件为

$$V_k(S_k(m))=m.$$

不失一般性,如图 2 所示,我们假设 *SA*2 中的节点 c 需发布信息 m 到 *SA*1 中的节点 b.当 *T*2 收到 c 的信息,通过认证后,用 *SA*1 中的 CA 分配的密钥对 m 进行签名,签名的内容记为 $m_{c\text{-}T2}$.当 *T*1 收到 *T*2 传递的信息时,用 *SA*2 中的 CA 分配的公钥验证 m,用 *SA*1 中的公钥验证并验证 $m=m_{c\text{-}T1}$,若通过验证,则对 m 用 *SA*1 中的私钥进行签名,签名的内容记为 $m_{c\text{-}T1}$.因此,节点 b 收到的信息为明文 m'和两个签名 $S_{T1}(m_{c\text{-}T1})$和 $S_{T2}(m_{c\text{-}T2})$.

此时,节点 b 接受其发布信息 m 的条件为

$$m'=V_{T1}(S_{T1}(m_{c\text{-}T1}))=V_{T2}(S_{T2}(m_{c\text{-}T2})).$$

这里我们做一个假设:

假设 1. 两个关键节点之间不进行“合谋”,即两个关键节点之间不对相同的虚假信息进行签名和传递.

由于节点 b 拥有 *T*1 和 *T*2 的公钥,因此,b 可以验证:

$$m'=V_{T1}(S_{T1}(m_{c\text{-}T1}))=V_{T2}(S_{T2}(m_{c\text{-}T2})).$$

即 $m'=m_{c\text{-}T1}=m_{c\text{-}T2}$.

又由于 *T*1 已经验证:

$$V_{T2}(S_{T2}(m_{c\text{-}T2}))=V_k(S_k(m))=m.$$

即 $m_{c\text{-}T2}=m$,且由假设 1,不存在 $m_{c\text{-}T1}=m_{c\text{-}T2}\neq m$.

综上,若 b 通过认证 $m'=m_{c\text{-}T1}=m_{c\text{-}T2}$,则必有 $m'=m$.

通过以上对于 TTM 工作原理的分析,我们不难得到以下定理:

定理 1. 两个安全 AS 联盟直接互联时,若两个互连的关键节点没有合谋,则一个安全 AS 联盟的节点所发布的信息对于另一个安全 AS 联盟内的节点来说是可认证的,并且验证的过程仅需验证节点所在安全 AS 联盟内的局部证书.

当两个安全 AS 联盟通过另一个安全 AS 联盟进行连接时,我们可以得到定理 2.

定理 2. 当两个安全 AS 联盟通过另一个安全 AS 联盟进行连接时,若任何两个互连的关键节点没有合谋,则一个安全 AS 联盟内的节点所发布的信息对于另一个安全 AS 联盟内的节点来说是可验证的,并且验证的过程仅需验证节点所在安全区内的局部证书.

通过对于定理 1 的证明进行简单的扩展,我们不难得到定理 2 的证明.

证明:不失一般性,如图 2 所示,安全 AS 联盟 *SA*1 和 *SA*3 通过 *SA*2 相连接,假设 *SA*3 要对 *SA*1 发布的信息进行认证.由定理 1,*SA*1 发布到 *SA*2 的信息可以被 *SA*2 中的节点以及 *SA*3 的关键节点所认证;同样,由定理 1,*SA*2 发布到 *SA*3 的信息可以被 *SA*3 中的节点所认证.因此,*SA*3 可对 *SA*1 发布的信息进行认证,并且认证只使用了本安全 AS 联盟内的局部信息. □

以上的定理可以拓展到多个 SA 相连接的问题上.

TTM 信任模型与传统信任模型的区别在于,传统的信任模型通过 CA 之间证书的传递来传播信任关系,而 TTM 则充分利用 AS 拓扑特性和信任关系的特性,利用关键节点进行签名转换,从而在带内传递信任关系.因此,TTM 极大地简化了证书的管理.这一点对于互联网这种复杂的巨系统来说具有非常重要的意义.

从另一个角度来看,这种认证方式有点类似于我们人类社会中的排队列.人们在排队列时,并不需要从头开始对齐,而只需验证是否与前两个人是否处在同一条直线上即可.如果队列中的每一个人都能准确地做到这一点,则这个队列最终是一条直线.TTM 也正是利用了关键节点的“线性叠加”特性,可通过局部信息认证而达到全局信息的认证.

4 SE-BGP 的认证算法

我们利用 TTM 模型设计了 SE-BGP 的源地址认证算法和路径认证算法.SE-BGP 需要修改 BGP 协议,增加两个新的属性,分别用于源地址认证和路径认证.在安全 AS 联盟内,其认证方式与 S-BGP 相似;而对于 AS 联盟间的认证,则是利用关键节点的特殊能力.任何认证都只需本地 AS 联盟的证书.

4.1 新增的属性

SE-BGP 需要增加两个属性:*AS_Security_Source* 用于地址源认证和存放源节点以及关键节点对于地址源信息的签名,*AS_Security_Source* 中最多包含两个签名;*AS_Security_Path* 用于路径认证和存放任何节点对于路径信息的签名,其需要签名的路径信息包括已经经过的路径(含本身)、下一节点和时间等其他需签名的信息.只有源节点和关键节点才会更新 *AS_Security_Source*,而任何节点都会更新 *AS_Security_Path*.

4.2 认证和更新算法

当节点需要发布一条 Update 信息时,它需要同时修改 *AS_Security_Source* 和 *AS_Security_Path* 属性.当节点收到一条 Update 信息时,首先对源地址信息和路径信息进行认证,然后对 *AS_Security_Source* 和 *AS_Security_Path* 属性作相应的修改,并向下传递.

在同一个安全 AS 联盟内,由于任何节点都可以获取其他节点的地址源证书和公钥,因此很容易对源地址信息和路径信息进行认证;而对于不同 AS 联盟之间,则需通过关键节点来进行认证.下面重点讨论 AS 联盟之间的认证算法.

SE-BGP 中的关键节点和非关键节点的处理是不同的.对于关键节点,由于其拥有两套以上的公钥证书,因此其使用的原则为:用来源节点的 AS 联盟内的公钥证书进行认证,用目的 AS 节点联盟内的私钥签名.

其认证和更新采用以下算法:

算法 1. 关键节点认证与更新.

(1) 查找 AS 联盟内的完整路径,检查其状态,若不正确,则抛弃该路径,并结束算法;

(2) 对地址源信息进行认证和更新:

a. 地址源认证:

若 *AS_Security_Source* 中只有一个签名(源节点签名),则检查证书;

若 *AS_Security_Source* 中只有两个签名(含源节点签名),则验证签名是否一致并检查证书;

若 *AS_Security_Source* 中只有两个签名(不含源节点签名),则验证签名是否一致.

b. 地址源认证签名更新:

若目的 AS 和来源 AS 节点不在同一个 AS 联盟内,则 *AS_Security_Source* 中的签名队列前移,并将自己对于验证后的地址源信息签名加入到队列中;

否则:

若签名队列为 1,则队列前移,并将自己对于验证后的地址源信息签名加入到队列尾;

若签名队列为 2,则将自己对于验证后的地址源信息签名替换队列尾;

(3) 对路径信息进行认证和更新:

a. 对 *AS_Security_Path* 中的签名进行认证,如果不正确,则退出算法;

b. 若目的来源 AS 为相邻安全 AS 联盟的关键节点,且目的节点为本 AS 联盟内节点,则将 *AS_Security_Source* 中的签名队列清空,只保留最后一个元素,将自己对于验证后的地址源信息签名并加入到队列中;否则,将自己对于验证后的地址源信息签名并加入到队列中.

对于非关键节点,由于只有本安全 AS 联盟内的证书和密钥,因此只需处理本 AS 联盟内节点和相邻 AS 联盟的关键节点的认证信息,其认证和更新算法如下:

算法 2. 非关键节点认证与更新.

(1) 查找 AS 联盟内的完整路径,检查其状态,若不正确,则抛弃该路径,并结束算法;

(2) 对地址源信息进行认证,验证 *AS_Security_Source* 中两个签名所认证的信息是否一致;

(3) 对路径信息进行认证和更新:

a. 对 *AS_Security_Path* 中的签名进行认证;

b. 路径认证签名更新,将自己对于验证后的地址源信息签名并加入到队列中.

5 安全能力分析

5.1 源认证和路径认证

在同一安全区内,由于任何节点都能获取本区内其他节点的公钥证书,可以通过验证每个节点的证书和签名来实现地址源认证和路径认证.

表面上看,SE-BGP 比 S-BGP 增加了一个前提条件,即关键节点之间不能合谋.然而这个条件并不苛刻:首先,节点之间的合谋攻击是当前所有 BGP 协议安全机制都不能防范的.完全防范这种攻击很难在协议层实现.例如,S-BGP 不能防护“带外合谋”;其次,在 S-BGP 中,合谋的节点可能是全局网络中的任意节点,而 SE-BGP 将合谋节点的范围限制在了关键节点之间,或同一 AS 联盟内的节点之间.从而,SE-BGP 比 S-BGP 有着更好的防范能力.

5.2 性能分析

由于要采用认证,SE-BGP 在处理、带宽、存储等方面都带来了额外的开销.

SE-BGP 采用 DSA 数字签名算法,签名的长度采用 320 位.模拟结果表明,在 1GHz 的处理器上,采用预处理后,其签名的时间由 6.5ms 降为 0.3μm,验证的时间为 5.1ms.

当前的互联网大概每分钟有一次 BGP 更新报文,每个报文平均携带 3.6 个 AS,而且当前绝大多数 AS 的连接度小于 60,因此,对于绝大多数 BGP 路由器来说,其平均每秒只处理一次更新报文.从上面的 SE-BGP 的行为模式我们可以知道,每个更新报文一般只会携带 2 个源地址认证.因此,每个 BGP 平均每秒进行不超过 5.6 次的验证和 1 次签名(只有关键节点进行 2 次签名).即便是遇到峰值,扩大 20 倍,也只进行 120 次验证和 20 次签名,所需时间大约为 600ms.

SE-BGP 平均会使 BGP 报文长度大约增加 240 字节.

通过以上分析我们可以看出,SE-BGP 在地址源认证上比 S-BGP 增加了一次验证,而在路径认证的长度方面却小于 S-BGP.就目前的条件看,完全可以满足 SE-BGP 所带来的在处理、带宽以及存储等方面的开销.

5.3 部署选择

SE-BGP 的部署需要对 BGP 协议软件进行修改,并且需要路由器进行升级,以适应安全认证所带来的额外

开销.因为 SE-BGP 本身就是利用 AS 联盟特性,所以,SE-BGP 支持渐进式的部署.可先在适当的 AS 联盟首先建立安全 AS 联盟和 AS 联盟认证中心 CA.

通过 SE-BGP 的工作模式,我们不难得到如下结论:当多个安全联盟互联时,若其互联是密闭的,则安全联盟节点之间的域间流量是受保护的.

由于互联网中的流量也具有不均衡性,因此,我们可以考虑首先在流量密集的 AS 联盟首先部署 SE-BGP,从而使得仅用少量的部署就能获得较大的收益.

已经建立安全联盟的节点与非安全区内的节点之间的互通由单个节点所采用的例外处理来决定.这样增加了 SE-BGP 渐进式部署中的灵活性.

6 可扩展性分析

在当前的基于 PKI 的各种安全机制中,所采用的证书形式各不相同.为了进行统一的分析,我们假设每个 AS 具有一个"单元"的证书.同时,我们考虑 3 个指标:全网的证书规模 C、单个 AS 节点所需的证书规模 Cs 以及一个证书改变时所影响的 AS 范围 Ca.

假设互联网中总的 AS 节点的规模为 N,rich 节点的范围为 β%,rich 节点之间的连接概率为 p.

对于传统的信任模型,有:$C=N^2$,$Cs=N$,$Ca=N$.

在 SE-BGP 中:

关键节点的数量 $K=N\times\beta/100$.

平均每个安全联盟的 AS 节点数 $n=\dfrac{N}{N\times\beta/100}=\dfrac{\beta}{100}$.

非关键 AS 节点所需的证书规模 $Cn=n\times(n+pK)\times K=\dfrac{100}{\beta}\times N+\dfrac{\beta}{100}pN^2, n>>1$.

关键 AS 节点证书规模 $Ck=(K\times p\times n)\times K=\left[\left(\dfrac{\beta}{100}\times N\right)\times p\times\dfrac{100}{\beta}\right]\dfrac{\beta}{100}\times N=\dfrac{\beta}{100}pN^2$.

总的证书规模 $C'=Cn+Ck=\dfrac{100}{\beta}\times N+\dfrac{2\beta\times p}{100}\times N^2$.

比照当前 AS 的拓扑特性[9],我们取 β=1,p=0.3,则 $C'=100N+\dfrac{6}{1000}\times N^2$.

又因为 N>20000,所以,$C'<\left(\dfrac{1}{200}+\dfrac{6}{1000}\right)N^2$,即 SE-BGP 中,总的证书规模大约为传统模型的 1%.

在 SE-BGP 中,只有 1%的节点为关键节点,其 $Cs'=\left(\dfrac{\beta}{100}\times N\right)\times p\times\dfrac{100}{\beta}=pN=0.3N$. 同样,$Ca'$=0.3$N$.而对于 99%的非关键节点,其 $Cs'=Ca'(n+pK)=100+\dfrac{3}{1000}N$.

表 2 对比了 SE-BGP 与基于传统信任模型安全机制的证书规模.

Table 2 The number of certificates

表 2 证书规模

N	C		Cs			Ca		
	Traditional solutions	SE-BGP	Traditional solutions	SE-BGP		Traditional solutions	SE-BGP	
				Key nodes	Normal nodes		Key nodes	Normal nodes
23 000	5.29×10^8	5.54×10^6	23 000	6 900	169	23 000	6 900	169
48 000	2.3×10^9	1.86×10^7	48 000	14 400	244	48 000	14 400	244
64 000	4.1×10^9	3×10^7	64 000	19 200	292	64 000	19 200	292

从表中我们可以看到,在 SE-BGP 中,占 99%的普通节点其证书的规模和影响范围远小于传统的安全模式.当网络规模达到 64 000 个 AS 时,其普通单个节点的证书规模平均仅为 292 个,只有传统模式的 0.6%.这是由于

SE-BGP 的源认证和路径认证仅需要局部 AS 联盟内的证书,而不需要全局证书.而且联盟之间的信息认证通过带内传递关键节点的认证签名,避免采用 CA 之间的证书链.证书规模的减小不仅有利于规模的可扩展性,而且会在很大程度上降低由于带外控制而带来的管理开销.

图 3~图 5 说明了网络规模扩展时其证书规模的发展趋势.

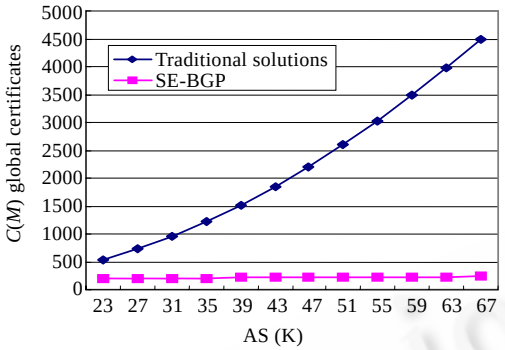


Fig.3 The number of global certificates

图 3 全网证书规模

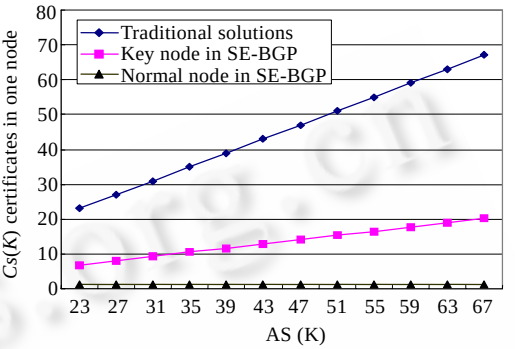


Fig.4 The number of total certificates in a single node

图 4 单个节点证书规模

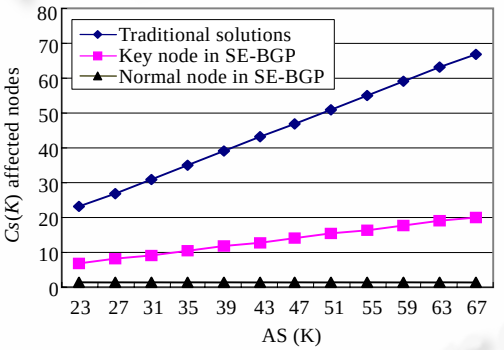


Fig.5 The number of nodes affected by a single node

图 5 单个节点影响范围

从以上的图中我们可以看出,随着互联网 AS 规模的不断扩展,SE-BGP 的全网证书规模、单个 AS 节点所需的证书规模以及单个节点影响的 AS 范围的发展趋势远远小于传统的安全机制.尤其是对于网络中占 99%的绝大多数普通节点,其发展趋势近似于常数.因此,SE-BGP 具有良好的规模可扩展性.

7 结 论

域间路由安全对于互联网的安全具有十分重要的意义,BGP 协议的安全性是域间路由安全的关键技术.源地址认证和路径认证是 BGP 安全所要解决的首要问题.

本文在研究 BGP 安全需求和当前研究成果的基础上,利用互联网的拓扑连接规律,提出了一种新的 BGP 安全机制:SE-BGP.SE-BGP 采用局部 PKI 的认证机制,同时具有一些新的特点:首先,SE-BGP 利用了 AS 拓扑连接的 rich-club 特性,提出了 AS 联盟的概念,避免了全局集中式认证所带来的负面影响;其次,SE-BGP 在信任传播上采用 TTM 模型,充分利用关键节点的特性,通过关键节点之间的制约和合作,避免了证书的全局传播,从而“局部控制,全局最优”;第三,SE-BGP 在规模、性能和管理方面具有良好的可扩展性,并在渐进式部署性上有着更好的支持.

SE-BGP 为 BGP 安全性提供了一种新的有意义的解决机制.

References:

[1] Murphy S. BGP security vulnerabilities analysis. IETF Internet RFC, RFC4272, 2006. ftp://ftp.rfc-editor.org/in-notes/rfc4272.txt

[2] Butler K, Farley T, McDaniel P, Rexford J. A survey of BGP security. Technical Report, AT&T Labs—Research. 2005. http://www.patrickmcdaniel.org /pubs/td-5ugj33.pdf

[3] Kent S, Lynn C, Seo K. Secure border gateway protocol (S-BGP). IEEE Journal on Selected Areas in Communications, 2000,18(4): 582−592.

[4] White R. Architecture and deployment considerations for secure origin bgp (soBGP). IETF Internet draft: draft-white-sobgp-architecture-01, 2006. http://www.ietf.org/internet-drafts/draft-white-sobgp-architecture-02.txt

[5] Aiello W, Ioannidis J, McDaniel P. Origin authentication in Interdomain routing. In: Proc. of the 10th ACM Conf. on Computer and Communications Security. Washington: ACM, 2003. 165−178.

[6] Wan T, Kranakis E, van Oorschot PC. Pretty secure BGP (psBGP). Technical Report, TR-04-07, SCS, 2004. http://www.scs.carleton.ca/~kranakis/Papers/TR-04-07.pdf

[7] Hu YC, Perrig A, Sirbu M. SPV: Secure path vector routing for securing BGP. ACM SIGCOMM Computer Communication Review, 2004,34(4):179−192.

[8] Goodell G, Aiello W, Griffin T, Ioannidis J, McDaniel P, Rubin A. Working around BGP: An incremental approach to improving security and accuracy of interdomain routing. In: Proc. of the ISOC NDSS 2003. San Diego, 2003. 75−85.

[9] Subramanian L, Roth V, Stoica I, Shenker S, Whisper RL. Security mechanisms for BGP. In: Proc. of the 1st Symp. on Networked Systems Design and Implementation (NSDI 2004). San Francisco: USENIX, 2004. 127−140.

[10] 2006. http://www.caida.org/analysis/routing/astypes/

[11] Zhou S, Mondragon RJ. The rich-club phenomenon in the Internet topology. IEEE Communications Letters, 2004,8(3):180−182.

[12] Zhang GQ, Zhang GQ. Research on Internet correlation. Journal of Software, 2006,17(3):490−497 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/17/490.htm

[13] Zhou S, Mondragon RJ. Accurately modeling the Internet topology. Physical Review E, 2004,70(066108). http://www.adastral.ucl.ac.uk/~szhou/PDF files/PhyRevE_70_066108.pdf

附中文参考文献:

[12] 张国强,张国清.Internet 网络的关联性研究.软件学报,2006,17(3):490−497. http://www.jos.org.cn/1000-9825/17/490.htm

胡湘江(1975－)男,湖南长沙人,博士生,主要研究领域为路由安全.

龚正虎(1945－),男,教授,博士生导师,主要研究领域为高速路由与交换技术,网络管理.

朱培栋(1971－),男,博士,副教授,主要研究领域路为路由技术,网络安全.