边界网关协议BGP-4的安全扩展

徐 恪,熊勇强,吴建平
(清华大学计算机系,北京 100084)

摘 要: 文章分析了边界网关协议BGP4的安全弱点,针对这些安全弱点对协议进行了扩展.通过数字签名技术来保护AS_PATH属性中的信息.为了适应分布式路由协议的特点,提出了分布式的基于RSA的密钥生成算法.通过综合运用这些技术,在基本保持报文长度不变的情况下有效地保护了BGP协议信息的机密性、可信性和完整性.

关键词: 路由协议; BGP; 机密性; 可信性; 完整性
中图分类号: TP393 文献标识码: A 文章编号: 0372-2112 (2002) 02-0271-03

Security Extension of Border Gateway Protocol BGP-4

XU Ke, XIONG Yong-qiang, WU Jiarr ping
(*Department of Computer Science, Tsinghua University, Beijing* 100084, *China*)

Abstract: The security weakness of Border Gateway Protocol (BGP-4) is analyzed. Aiming at the weakness, the protocol are extended with some security properties. Digital signature mechanism is used to protect the AS_PATH information. To satisfy the characteristic of distributed routing protocol, a distributed key generation algorithm based on RSA is presented. By integrating these techniques, confidentiality, creditability and integrity of BGP are protected in keeping the packet length with near constant space.

Key words: routing protocol; BGP; confidentiality; creditability; integrity

1 引言

边界网关协议BGP(Border Gateway Protocol)是一个用于自治系统之间的路由协议,其主要功能是在各BGP实体之间交换网络可达性信息[1].这些信息包括一个路由所穿越的自治系统的列表,它们足以建立一个表示连接状态的图.这样便很容易地解决了路由环路问题,同时使得在自治系统AS(Autonomous System)基础上的路由选择策略成为可能.从这一点上讲,BGP是一个综合了向量-距离算法和链路-状态算法的协议.BGP进行于可靠的传输协议之上,采用传输控制协议TCP(Transfer Control Protocol)作为其底层协议,这样便无须显式地进行分片、重传、确认和排序.

BGP路由协议包括的安全信息很少,它无法对它传递的路由信息提供保护.在这种情况下,运行BGP协议的边界路由器不得不相信它所接收到的所有的Update报文,这相当于它必须信任Internet上的所有边界路由器.这种情况显然是不能接受的.为了解决BGP协议的安全问题,本文首先提出了BGP协议的安全目标,然后定义了能够实现这些安全目标的安全服务,最后提出了解决这些安全问题的具体措施.

2 相关工作

Kumar在文献[2]中分析了路由协议的安全需求,讨论了安全的距离-向量协议和链路-状态协议的通用的安全技术.他定义了两种类型的攻击:来自路由器的攻击和来自链路的攻击.Kumar认为来自路由器的攻击很难被检测到而且对于攻击者本身来说没有太大的价值,因此他主要讨论了防止来自链路的攻击的安全协议.对于距离-向量协议来说,一般的攻击手段是修改或者重传路由更新信息.为了对抗这种类型的攻击,Kumar提出对路由更新信息进行数字签名,同时利用序列号和时间戳机制来保护路由更新,另外还使用了确认和重传机制.

Kumar和Crowcorft在文献[3]中对域间路由协议进行了类似的分析并提出了如何给距离-向量路由协议提供安全保护,他们还特别提到了路径-向量路由协议IDRP.他们提出对相邻节点之间的路由更新信息进行加密.

Smith和Garcia-Lunar Aceves在文献[4]中提出了BGP协议和其它的距离-向量协议的安全框架,但他们没有详细的描述具体的安全措施,而这正是本文的主要工作.

3 BGP要实现的安全目标

目标是为BGP提供认证机制、完整性控制、信息保密和访问控制.具体来说,就是为了:

(1)防止各类攻击者对路由信息进行伪装、修改和重传.

(2)防止破坏性的链路和破坏性的发言者对BGP路由信息的破坏.

(3)不把任何路由信息泄漏给各类攻击者.

收稿日期: 2000-01-05; 修回日期: 2001-05-25
基金项目: 国家自然科学基金(No. 90104002); 国家"八六三"计划重大项目(No. 863-306-ZD-07-01)

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

4 BGP 的安全扩展

BGP 协议交换的信息可以分为两类: 在物理网络上直接相邻的 BGP 发言者之间交换的信息和由直接相邻的 BGP 发言者转发的其他发言者发送来的信息. 直接相连的 BGP 发言者之间交换的信息包括发送方认为应该发送给接受方的关于目的地址的路由更新信息. BGP 发言者转发的信息包括描述给定地址的路由属性的信息. 根据这两类不同的信息, 我们提出了下面两类安全对策.

通用 BGP 报文保护:

(1) 在 BGP 对等体建立连接时进行认证, 通过认证后协商会话密钥. 用此会话密钥加密所有的 BGP 报文. 这种方式可以保证路由信息的机密性(confidentiality).

(2) 增加报文序列号用于防止报文被攻击者重传或删除.

BGP Update 报文保护:

(1) 增加 UPDATE 序列号或者时间戳来防止攻击者重传 UPDATE 报文.

(2) 由发出 UPDATE 报文的 BGP 发言者或者进行了最近的一次聚合操作的 BGP 发言者对 UPDATE 报文的所有的不变的域进行数字签名. 这样就提供了完整性保护, 同时提供了认证机制.

4.1 BGP 报文保护

提供 BGP 报文保护的目的是为了在 BGP 对等体之间认证(Authentication)、保密性(Confidentiality) 和完整性(Integrity).

4.1.1 密钥生成与分发

在大规模的分布式路由系统中, 每个实体都可能与其他实体所有通信, 密钥的分配管理更是个极为复杂的问题. 为了解决这一问题, 提出了基于 RSA(Rivest Shamir Adleman)[5] 的分布式密钥生成算法, 使用该算法, 可以保证所有生成的密钥在整个系统里唯一的, 从而在不降低加密强度的基础上增强系统的扩展性.

分布式密钥生成

在一个典型的分布式路由系统中, 相同管理层次上的所有路由器地位都是平等的, 不存在任何特殊的实体. 很自然的, 考虑在系统中使用一种分布式的密钥生成方案, 对应于某种密钥管理层次(可直接映射为路由管理层次), 由分布的地位平等的密钥生成器来生成其管理区域的路由器的密钥, 如图 1 所示. 图 1 中的自治域是一个灵活的概念, 可以把它和自治系统 AS 相对应以简化密钥管理, 子域可以对应于自治系统中的不同区域.

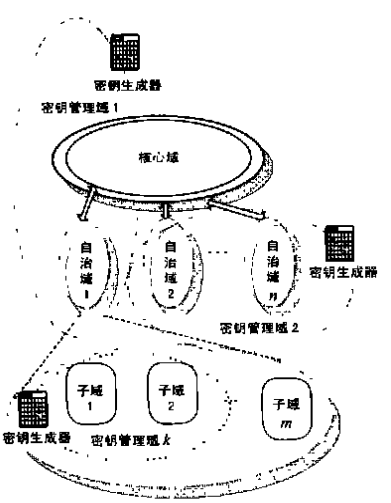

图 1 分布式密钥生成示意图

算法思想是, 首先, 给每一个密钥生成器分配一个全局唯一的密钥种子范围, 这个范围包含了其负责区域的全局标识 $[Z', i']$(网络区域 $Z=(z_1, z_2, \cdots, z_n)$ 以及局部标识 i); 其次, 保证其产生的密钥的某个固定部分落在此密钥种子范围内. 进一步来说, 假设第 g 个密钥生成器的密钥种子范围为 $[L_g, U_g]$, 我们将产生如下的密钥, 其低 m 位就落在此区间内, 用公式表示如下:

$$L_g \le (n \bmod 2^m) \le U_g$$

其中, n 是公钥, m 是公钥的固定部分位数(即低 m 位). 在这里, 采用了分布式的密钥生成方法, 而且不需要一个能被所有人信任的特殊的路由器; 一个被某路由器信任的密钥生成器并不一定为其他路由器所信任. 这样就不再需要一个单独的受信实体, 在消除了单一失效点的同时, 也减少了产生系统瓶颈(尤其当使用密钥管理中心/密钥服务器生成和分发密钥时)的可能性.

与此同时我们并没有降低任何安全性, 因为在 RSA 加密体制中, 加密密钥 e 是依赖于公钥的模数部分 n 的, 而 n 是唯一的. 这样一来, 只有公钥的模数部分 n 需要被生成, 下面将给出一种基于 RSA 的密钥生成算法; 每当需要生成密钥时, 可从密钥生成器 g 的密钥种子范围中随机选取一个种子数 $r \in [L_g, U_g]$, 再将它作为公钥的模数部分(即 n)的低 m 位, 换句话说, 就是要求: $n \equiv r \pmod{2^m}$ 为达到此目的, 可用如下的算法生成: (设公钥的模数部分 n 约为 $2L$ 位)

(1) 随机生成 L 位的大素数 p;

(2) 计算 $q_0 = (r * p^{\varphi(2^m)-1}) \pmod{2^m} + 2^{L-1}$;

(3) 随机选取整数 i_0, 计算 $q = q_0 + i * 2^m$, $i = i_0, i_i + 1, \cdots$; 直至 q 为素数; 若失败, 则返回第 1 步;

(4) 由上节中计算 RSA 密钥的一般公式计算: $n = p * q$; 选取 e、d 满足 $(e, \varphi(n)) = 1$; $d * e \equiv 1 \bmod \varphi(n)$.

由算法可知,

$q = ((r * p^{\varphi(2^m)-1}) \bmod 2^m) + 2^{L-1} + i * 2^m$. 所以, 素数 q 的位数不低于 L 位, 因而, n 的位数约为 $2L$ 位. 此外, $q \equiv (r * p^{\varphi(2^m)-1}) \pmod{2^m}$.

所以, $n \equiv p * q \pmod{2^m}$

所以, $n \equiv p * (r * p^{\varphi(2^m)-1}) \pmod{2^m}$

而 $p^{\varphi(2^m)} \equiv 1 \pmod{2^m}$

故 $n \equiv r \pmod{2^m}$, 符合系统设计要求.

密钥的分发

在分布式路由系统中, 每个参与路由的实体(Ri)都由信任实体(TE, Trusted Entity)配置一个证书(Ci), 以证实此路由实体的基本信息, 如路由的拥有者等. 在密钥的分发中, Ri 将证书(Ci)、本实体的公钥(Pi)以及本路由器的基本信息(Ii)用本路由器的私钥(Vi)加密签名, 生成密钥证书串(Pi, Ci, Ii, $S(Vi, Pi, Ci, Ii)$)(S 为签名函数), 然后向外广播以进行密钥分发.

4.1.2 身份认证与报文加密

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

在 BGP 连接建立的时候, BGP 对等体之间将首先通过交换证书和密钥证书串进行身份认证, 然后交换会话密钥, 以后这条连接上的所有的 BGP 信息都是由会话密钥加密的. 这种加密提供了信息的保密性, 同时保证了 KEEPALIVE 报文、NOTIFICATION 报文和 UPDATE 报文中某些域的完整性. 当检测到发生了错误时, BGP 发言者将发送一个 NOTIFICATION 报文之后断开连接.

身份认证的过程如下: (刚才已经讨论了密钥的分发过程, 所以下面我们假定 BGP 对等体互相知晓对方的公钥)

(1) 请求建立连接的 BGP 对等体($B1$)向对方($B2$)发送一条使用对方的公钥加密的包括自己的标识和一个随机数 $R1$ 的报文.

(2) $B2$ 收到以后, 使用自己的私钥解密, 然后组织一条包括 $R1$, 会话密钥 K 和 $B2$ 自己生成的随机数 $R2$ 的报文并用 $B1$ 的公钥加密, 然后发送给 $B1$.

(3) $B1$ 收到以后, 看到该报文中有自己刚刚生成的随机数 $R1$, 因此它可以肯定对方是真的 $B2$ 而不是冒充的, 为了证明自己的身份, $B1$ 把 $B2$ 生成的随机数 $R2$ 用会话密钥 K 加密后发送给 $B2$.

(4) $B2$ 收到这条报文后, 发现 $B1$ 送来了自己刚刚生成的随机数 $R2$, 因此 $B2$ 也可以肯定对方是真正的 $B1$. 至此, 身份认证过程完成. 在这以后, 所有的报文都可以使用会话密钥 K 加密传输了.

4.1.3　报文序列号

每条报文都有序列号. 在连接建立的时候序列号被初始化为 0, 以后每发送一个报文序列号就加 1. 如果检测到某个序列号被跳过或者出现了重复, BGP 发言者将在发送一个 NOTIFICATION 报文之后断开连接. 序列号的范围必须足够大保证它很难循环到 0. 即使循环到 0 也没有关系, 这时原有连接将被断开, 然后会重新建立一个新的连接, 序列号会从 0 开始重新计数.

4.2　UPDATE 域保护

这类保护措施保护了前面提到的第二类 BGP 信息. 这类措施只提供了认证机制和完整性控制, 因为对于这类信息来说它的接收者是整个 Internet 上的所有授权的 BGP 发言者. 每条 UPDATE 报文都包括序列信息来防止重传(Replay)攻击. 这个序列信息是由产生路由的 BGP 决策过程生成的, 它可以采用序列号或者时间戳的形式. 为了保证 UPDATE 报文中不变信息的完整性和真实性, 它将由初始的 BGP 发言者进行数字签名. 数字签名使用公钥机制, 使用刚才讨论的密钥生成算法生成的密钥. UPDATE 的数字签名信息保存在 UPDATE 报文的 Maker 域中, 它的计算包括以下的域: UPDATE 报文序列号、不可行路由长度(Unfeasible Route Length)、撤销路由(Withdrawn Routes)、ORIGIN、ATOMIC_AGGREGATE、AGGREGATOR、PREDECESSOR 和 NLRI.

5　结论

本文对 BGP 协议进行了安全扩展. 通过数字签名技术来保护 AS_PATH 属性中的信息. 为了能够适应分布式路由协议的特点, 提出了基于 RSA 的分布式密钥生成算法. 使用了这些技术, 就可以保证 BGP-4 协议信息的安全交换. 在保证安全性的同时, 报文的大小可以基本保持不变. 本文介绍的协议扩展已经在国家"863"重大项目"高性能安全路由器"中实现, 在实验环境中运行情况良好. 目前"高性能安全路由器"已经通过"863"专家组的验收, 正在进行产业化工作.

参考文献:

[1] Rekhter Y, Li T. A Border Gateway Protocol 4(BGP-4) [S]. RFC 1771, Mar. 1995.

[2] B Kumar. Integration of security in network routing protocols [J]. ACM SIGSAC Review, 1993, 11(2): 18-25.

[3] B Kumar, J Crowcroft. Integrating security in inter-domain routing protocols [J]. ACM Computer Communication Review, 1993, 23(4): 36-51.

[4] B R Smith, J J Garcia-Lunar-Aceves. Efficient security mechanisms for the border gateway routing protocol [J]. Computer Communications, 1998, 21(2): 203-210.

[5] R L Rivest, A Shamir, L Adleman. A method for obtaining digital signatures and public key cryptosystems [J]. Communications of the ACM, 1978, 21(2): 120-126.

作者简介:

徐　恪　男. 1974 年生于江苏省洪泽. 于清华大学计算机系获博士学位. 主要研究领域为计算机网络体系结构, 高性能路由器体系结构, 分布式实时操作系统, 系统性能评价和算法分析与设计.

熊勇强　男. 1974 年生于江西省安义. 于清华大学计算机系获博士学位. 主要研究领域为计算机网络体系结构, 分布式网络安全体系结构, 密码算法和高性能路由器体系结构.

吴建平　男. 1953 年生于山西太原. 清华大学计算机系教授, 博士生导师, 中国教育科研计算机网专家委员会主任, 网络中心主任, 教育部"长江学者奖励计划"特聘教授. 主要研究领域为计算机网络体系结构, 计算机网络协议测试, 形式化技术. 已在国内外核心刊物和重要国际学术会议上发表了 100 多篇文章.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net