ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.20, No.12, December 2009, pp.3223−3239
doi: 10.3724/SP.J.1001.2009.03396

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

一个基于身份的安全域间路由协议*

王 娜[1,2+], 智英建[2], 张建辉[2], 程东年[2], 汪斌强[2]

[1](解放军信息工程大学 电子技术学院,河南 郑州 450004)

[2](解放军信息工程大学 信息工程学院,河南 郑州 450002)

Identity-Based Secure Inter-Domain Routing Protocol

WANG Na[1,2+], ZHI Ying-Jian[2], ZHANG Jian-Hui[2], CHENG Dong-Nian[2], WANG Bin-Qiang[2]

[1](College of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004, China)

[2](College of Information Engineering, PLA Information Engineering University, Zhengzhou 450002, China)

+ Corresponding author: E-mail: tinatwf@gmail.com

Wang N, Zhi YJ, Zhang JH, Cheng DN, Wang BQ. Identity-Based secure inter-domain routing protocol. *Journal of Software*, 2009,20(12):3223−3239. http://www.jos.org.cn/1000-9825/3396.htm

Abstract: The paper proposes a secure inter-domain routing protocol which adopts identity-based cryptographic system—id^{2}r (identity-based inter-domain routing). id^{2}r consists of a key management mechanism, an origin AS verification mechanism LAP (the longest assignment path), and an AS_PATH authenticity verification mechanism IDAPV (Identity-based Aggregate Path Verification). The key management mechanism adopts a distributed and hierarchical key issuing protocol DHKI (distributed and hierarchical key issuing) to solve the inherent key escrow problem in the identity-based cryptographic system. The basic idea of LAP is that all ASes must provide the assignment path and attestations of their announced prefixes, and for a prefix, the AS which provides the longest valid assignment path is its legitimate origin AS. With identity-based aggregate signature scheme, IDAPV generates a route aggregate attestation to guarantee the authenticity of AS_PATH. Performance evaluation results indicate that based on RouteViews data on December 7, 2007, an id^{2}r router only consumes 1.71Mbytes additional memory, which is 38% of S-BGP router; id^{2}r has shorter UPDATE message than S-BGP; convergence time of id^{2}r with hardware implementation of cryptographic algorithm approximately equals BGP.

Key words: BGP; security; identity-based; prefix hijacking

摘 要: 提出了一个采用基于身份密码体制的安全域间路由协议——基于身份域间路由协议(identity-based inter-domain routing,简称id^{2}r).id^{2}r协议包括密钥管理机制、源AS验证机制LAP(the longest assignment path)和AS_PATH真实性验证机制IDAPV(identity-based aggregate path verification).密钥管理机制采用一个分布式层次密钥分发协议(distributed and hierarchical key issuing,简称DHKI),以解决基于身份密码系统固有的密钥托管问题.LAP的基本思想是,任一发出前缀可达路由通告的自治系统都必须提供该前缀的分配路径及证明,只有提供前缀最长有效分配路径的自治系统才是该前缀的合法源AS.IDAPV采用基于身份的聚合签名体制,生成保证AS_PATH路径属性

* Supported by the National Basic Research Program of China under Grant No.2007CB307102 (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.2007AA01Z2A1 (国家高技术研究发展计划(863))

Received 2007-12-21; Revised 2008-04-02; Accepted 2008-05-19

真实性的路由聚合证明.性能评估结果显示,基于 2007 年 12 月 7 日的RouteViews数据,id²r路由器仅额外消耗1.71Mbytes内存,是S-BGP的 38%;更新报文长度明显短于S-BGP;当硬件实现密码算法时,收敛时间几乎接近于BGP.

关键词: BGP;安全;基于身份;前缀支持攻击

中图法分类号: TP309 **文献标识码**: A

Internet域间路由协议BGP(the border gateway protocol,边界网关协议)[1]存在安全缺陷[2]:路由器能够自由地发送任意错误/恶意路由信息,并且这些错误/恶意路由信息会被没有任何阻拦地传播到整个Internet,造成全球网络的不稳定和瘫痪.具体地,域间路由协议BGP主要存在两个安全设计缺陷:① BGP协议允许自治系统(autonomous systems,简称ASes)自由地(不需授权地)通告任意错误/恶意网络层可达信息(network layer reachable information,简称NLRI),会受到一种前缀劫持攻击.当某个自治系统发出一个非本自治系统内前缀的可达路由通告,导致网络中以该前缀为目的地址的全部/部分数据报文被路由到这个自治系统时,称该前缀被这个自治系统劫持.近年来,学者和网络运营商发现了大量的前缀劫持攻击事件[3−12].例如,2004 年 12 月 24 日,AS 9121 错误地发起 106 089 个前缀的路由通告,几乎占所有前缀的 70%[4];2005 年 5 月 7 日,AS 174 劫持了Google公司(www.google.com)的前缀 64.233.161.0/24[5];2006 年 6 月 8 日,AS 23520 劫持了前缀:1/8,2/8,3/8,4/8,5/8,7/8,8/8,12/8[6];2008 年 2 月 24 日,Pakistan Telecom (AS 17557)劫持了YouTube(AS 36351)的前缀 208.65.153.0/24,导致YouTube在 80 分钟内不可达[12]等等.最近研究发现,垃圾邮件发送者经常采用劫持前缀的方式发送垃圾邮件[13,14];② BGP没有验证更新报文AS_PATH路径属性是否真实,易受到AS_PATH篡改攻击.AS_PATH是BGP协议的一个公认强制路径属性,标识更新报文所携带路由信息经过的自治系统.BGP路由器选择最优路由时,除了自治系统之间的商业关系(即LOCAL_PREF),AS_PATH长度是最重要的一项依据.因为BGP没有提供任何AS_PATH真实性验证机制,攻击者能够非常容易地篡改AS_PATH,发动AS_PATH篡改攻击.前缀劫持攻击和AS_PATH篡改攻击会导致网络不可达、流量黑洞、流量窃听,甚至全球网络的不稳定和瘫痪[15,16].并且,只要网络连接性不被破坏,AS_PATH篡改攻击就难以被发现.

针对 BGP 面临的前缀劫持和 AS_PATH 篡改攻击,目前的解决方案分为 3 类:第 1 类是基于密码学的方案[17−20],基本思想是采用密码技术主动地提供路由通告中前缀源AS合法性和AS_PATH真实性的验证机制,弥补BGP协议的安全缺陷,以使前缀劫持和AS_PATH篡改攻击不可能发生;第 2 类是攻击检测方案[21−27],即当攻击发生时尽可能快地检测出攻击;第 3 类方案即Pretty Good BGP(PGBGP)[5]的基本思想是延迟所有新路由的使用直至确定该路由是合法的. PGBGP对短期(short-lived)攻击比长期(long-lived)攻击更加有效,而且因为延迟所有合法新路由的使用,PGBGP中路由的收敛时间显著长于BGP.与攻击检测方案相比,基于密码学的方案要求布署覆盖全网的密钥管理基础设施及修改路由协议和路由器,增加了路由器的处理负担,且当部分地布署时只能够提供有限的安全性[28],不易于布署实现等等.但是我们仍然重点研究了基于密码学的方案,因为攻击检测只是一种当攻击发生时检测出攻击的被动解决方案,它需要快速响应机制的配合才能达到快速有效阻断攻击、降低攻击影响的目的.目前的攻击检测方案只能够检测出AS_PATH最后一跳修改攻击[21].基于密码学的方案却是一个主动解决方案,它的研究也将为设计下一代可信网络中的安全域间路由架构提供宝贵的经验和教训.

基于密码学的典型方案包括有BBN的S-BGP[17]、思科的soBGP[18]、psBGP[19]及SPV[20]等.本文发现,S-BGP,soBGP和SPV采用的集中式源AS验证技术只能保证前缀被它分配路径上的ISP(Internet service provider,Internet服务提供商)授权AS发起,而不能保证被它分配路径上最后一个ISP(即前缀的拥有ISP)授权AS发起,导致这些方案会受到一种上层ISP前缀劫持攻击.虽然psBGP采用分布式源AS验证技术(即如果一个AS做出的前缀声明与任一对等体AS做出的关于该AS的前缀声明一致,就认为这个前缀声明是正确的,该AS是声明中前缀的合法源AS),但是,选择一个可信任的对等体AS是异常困难的.若选择同一ISP下的对等体AS,他们之间可能会彼此串通,psBGP的设计者也不建议作这种选择.但是,如果根据设计者的建议选择不同ISP管理下的对等体AS,一致性验证失败的结果可能是错误的:该AS和对等体AS的前缀声明不一致,仅仅因为对等体AS有意地提供了一个错误的前缀声明.

S-BGP,psBGP和SPV方案要求AS_PATH中每个AS都必须提供一个路由证明,以保证AS_PATH的真实性.路由证明至少包括该AS向外发散路由的AS_PATH、下一跳AS等信息.除SPV外[29],S-BGP和psBGP能够有效地保证AS_PATH的真实性,但是它们采用基于证书的密码体制,要求构建一个覆盖全Internet的公钥基础设施(public key infrastructure,简称PKI)以发布Internet中所有路由器的公钥证书.并且为了快速验证路由证明,在最坏情况下,路由器需要存储Internet中所有路由器的公钥,内存开销庞大,可扩展性差.繁重而复杂的PKI密钥管理和昂贵的内存开销严重阻碍了S-BGP和psBGP在实际中的布署实现.与S-BGP和psBGP不同,soBGP通过构建一个全网AS拓扑图,验证更新报文中AS_PATH的真实性.但是,soBGP不能验证该更新报文是否确实经过AS_PATH所含自治系统以及抵抗AS_PATH填充攻击.

另一方面,近年来,基于身份的密码体制是密码学最活跃的研究领域之一,大量的基于身份密码体制被提出.基于身份的密码学由Shamir在 1984 年首次提出[30],以简化基于证书PKI的密钥管理过程.在基于身份的密码系统中,通信实体的身份如姓名、IP地址、电子邮件地址等作为公钥,私钥由通信双方都信任的第三方——私钥生成器PKG(private key generator)——生成.因此,与基于证书的密码体制相比,基于身份的密码体制显著地减少了建立和管理PKI的开销,且因不再存储和验证公钥证书,也显著地降低了用户的存储开销,减轻了用户的计算负担.同时,近年来,硬件实现椭圆曲线上配对计算的性能也得到了显著提高[31].这些为我们采用基于身份的密码体制实现安全域间路由提供了契机.目前,只有无线ad hoc研究领域的一些学者提出基于身份签密算法的安全路由协议[32].

基于此,本文提出了一个采用基于身份密码体制的安全域间路由协议——基于身份的域间路由协议(identity-based inter-domain routing,简称id^{2}r).id^{2}r基于BGP协议,包括密钥管理机制、基于前缀最长分配路径的源AS验证机制(the longest assignment path,简称LAP)和基于身份聚合签名体制的AS_PATH真实性验证机制(identity-based aggregate path verification,简称IDAPV).密钥管理机制采用一个分布式层次密钥分发协议(distributed and hierarchical key issuing,简称DHKI),以解决基于身份密码系统固有的密钥托管问题.LAP的基本思想是,任一发出前缀可达路由通告的AS都必须提供该前缀的分配路径及证明,只有提供前缀最长有效分配路径的AS才是该前缀的合法源AS.根据文献[21]中前缀劫持攻击的分类,LAP可以抵抗有效前缀劫持、子前缀劫持和未使用前缀劫持,特别是上层ISP前缀劫持攻击.IDAPV采用与S-BGP相同的验证思路,即AS_PATH中的每个AS都必须提供一个路由证明,其中含有更新报文的NLRI域值,AS_PATH属性值及下一跳AS号码.不同之处是,IDAPV采用基于身份的聚合签名体制聚合AS_PATH中所有AS的路由证明成一个路由聚合证明.聚合签名体制是指聚合n个不同用户分别对n个不同消息的签名成一个聚合签名,验证者只需验证这个聚合签名的正确性就能保证n个初始签名的正确性.IDAPV能够有效地抵抗AS_PATH篡改攻击.性能评估结果显示,基于2007年12月7日的RouteViews数据,id^{2}r路由器仅额外消耗1.71Mbytes内存,是S-BGP的38%;id^{2}r的更新报文长度明显短于S-BGP;当硬件实现密码算法时,收敛时间几乎接近于BGP.

本文第1节在简单介绍基于身份密码体制基础上,提出了分布式层次密钥分发协议DHKI.第2节给出一个针对S-BGP的上层ISP前缀劫持攻击实例,分析攻击的发生原因和概率,并提出基于前缀最长分配路径的源AS验证机制LAP.第3节提出基于身份聚合签名体制的AS_PATH真实性验证机制IDPAV.第4节评估id^{2}r的安全性和性能.第5节得出结论.

1 id^{2}r的密钥管理机制

1.1 基于身份的密码体制

设 p 为大素数,G 和 V 分别为 p 阶的加法循环群和乘法循环群.映射 $e:G\times G\to V$ 具有以下性质:

① 双线性:$e(aP,bQ)=e(P,Q)^{ab}$,$\forall a,b\in\mathbb{Z}_p$,$P,Q\in G$;

② 非退化:$\exists P,Q\in G$,使 $e(P,Q)\neq 1$;

③ 可计算性:$\forall P,Q\in G$,存在计算 $e(P,Q)$的有效算法.

实际上,利用椭圆曲线上的Weil对、Tate对或η_T对可构造有效的具有上述性质的双线性映射[31,33].

一个群被称为间隙 Diffie-Hellman(GDH)群,当且仅当该群中判定性 Diffie-Hellman 问题是容易的,而计算性 Diffie-Hellman 问题是困难的.本文默认系统参数 G 是 GDH 群,且 G 上离散对数问题(DLP)是困难的.

本文中,id^{2}r方案采用Cheon,Kim和Yoon在 2004 年提出的CKY基于身份聚合签名体制[34].它包括以下 6 种算法:

① Setup.参数生成算法,由PKG完成.给定GDH群G和生成元P.定义两个密码Hash函数:$H_1:\{0,1\}^*\to G^*$,$H_2:\{0,1\}^*\times G\to \mathbb{Z}_p^*$.PKG随机选取$s\in \mathbb{Z}_p^*$,计算$P_{pub}=sP$.系统的公开参数是$(P,P_{pub},H_1,H_2)$,$s$是系统的主密钥.

② Extract.私钥解析算法.PKG根据用户的身份计算它的私钥.给定用户身份ID,PKG计算用户私钥$D_{ID}=sH_1(ID)$.

③ Sign.签名算法.给定消息m,签名者随机选取$r\in \mathbb{Z}_p^*$,计算$U=rP$,$Q_{ID}=H_1(ID)$,$h=H_2(m,U)$和$V=rQ_{ID}+hD_{ID}$.消息 m 的签名$\sigma(m)=(U,V)$.

④ Verify.签名验证算法.给定消息m的签名$\sigma(m)=(U,V)$,验证者计算$h=H_2(m,U)$,$Q_{ID}=H_1(ID)$.(U,V)是消息m的正确签名当且仅当$e(P,V)=e(Q_{ID},U+hP_{pub})$.

⑤ Aggregate.签名聚合算法.给定一个消息集合$(m_1,\ldots,m_{n-k})$的聚合签名$AggreSig(m_1,\ldots,m_{n-k})=(U_1,\ldots,U_{n-k},V)$和$k-1$ 个消息$(m_{n-k+1},\ldots,m_n)$的签名$(\sigma(m_{n-k+1}),\ldots,\sigma(m_n))$,其中,$\sigma(m_i)=(U_i,V_i)$,$n-k+1\le i\le n$,$1\le k<n$,$n>1$,聚合签名者计算$V'=V+\sum_{i=n-k+1}^{n}V_i$,生成消息集合$(m_1,\ldots,m_n)$的聚合签名$AggreSig(m_1,\ldots,m_n)=(U_1,\ldots,U_n,V')$.

⑥ Aggregate Verify.聚合签名验证算法.给定消息集合$(m_1,\ldots,m_n)$,签名者的身份集合$(ID_1,\ldots,ID_n)$和聚合签名$(U_1,\ldots,U_n,V')$,聚合签名验证者计算$Q_{ID_i}=H_1(ID_i)$,$h_i=H_2(m_i,U_i)$,$1\le i\le n$.聚合签名$(U_1,\ldots,U_n,V')$是正确的当且仅当$e(P,V')=\prod_{i=1}^{n}e(Q_{ID_i},U_i+h_iP_{pub})$.

1.2 DHKI

基于身份的密码体制中,PKG持有整个系统的主密钥,知道系统中所有用户的私钥.实际上,这是非常不安全的.id^{2}r要求密钥管理体制能够安全分发网络中所有RIRs(regional Internet registry,区域性Internet注册机构),ASes和路由器的私钥.基于此,我们提出了一个分布式层次密钥分发协议(distributed and hierarchical key issuing,简称DHKI).DHKI完成CKY体制中Setup和Extract算法功能,生成系统公开参数,安全分发网络中所有RIRs,ASes和路由器的私钥.

Internet每个自治系统内设置一个私钥碎片生成器(a share of private key generator,简称sPKG).根据Shamir门限秘密共享体制[35],分割主密钥s成n份碎片.每个sPKG拥有一份主密钥碎片.定义每个sPKG都是所在自治系统和该自治系统内路由器的主sPKG,其他自治系统和该自治系统内路由器的次sPKG.

定义自治系统AS的公钥ID_{AS}:$AS||Time$,AS域表示自治系统号码,$Time$域表示该ID的有效期;路由器的公钥ID_{router}:$Name||Time||AS$,$Name$域表示路由器的身份信息,如思科路由器的router id等,$Time$域表示ID的有效期,AS域表示路由器所在自治系统的号码.ID_{AS}和ID_{router}中的$Time$,AS域限制了对应私钥的有效期和使用范围,有助于密钥撤销.

基于 Internet 中串通自治系统的个数小于 t 的前提,DHKI 协议详细描述如下(其中,$\sigma_{D_A}(M)$ 表示用户 A 用自己的私钥D_A对消息M的签名):

1. System initialization(系统初始化)

1-1. The System Setup(系统参数生成)

给定GDH群G和生成元P.定义 3 个密码Hash函数:$H_1:\{0,1\}^*\to G^*$,$H_2:\{0,1\}^*\times G\to \mathbb{Z}_p^*$,$H_3:V\to \mathbb{Z}_p^*$.由Internet中所有组织都信任的独立机构如ICANN随机选取$s\in \mathbb{Z}_p^*$,计算$P_{pub}=sP$.系统的公开参数是(P,P_{pub},H_1,H_2,H_3),s是整个系统的主密钥.

ICANN生成RIR的私钥$D_{RIR}=sH_1(RIR)$和$sPKG_i$的私钥$D_{sPKG_i}=sH_1(sPKG_i)(1\le i\le n)$.

根据Shamir(t,n)秘密共享体制,ICANN选择一个大于主密钥s和n的素数q;定义$a_0=s$,随机选择$t-1$个独立的系数$a_1,\ldots,a_{t-1}$,这些都需保密;构建多项式$f(x)=a_0+a_1x+a_2x^2+\ldots+a_{t-1}x^{t-1} \bmod q$;计算主密钥碎片$K_i=f(i)(1\le i\le n)$;最后,销毁主密钥$s$和秘密$(a_1,\ldots,a_{t-1})$.

1-2. Parameter Issuing(参数发布)

ICANN分别离线安全发布RIR的私钥D_{RIR}至RIR,以及主密钥碎片K_i,私钥D_{sPKG_i}和系统公开参数(P,P_{pub},H_1,H_2,H_3)到$sPKG_i$(可与自治系统号码一起分配);ICANN销毁已经安全发布的所有私钥和私钥碎片.

RIR验证$e(D_{RIR},P)\stackrel{?}{=}e(Q_{RIR},P_{pub})$,判断$D_{RIR}$是否正确.其中,$Q_{RIR}=H_1(RIR)$.

$sPKG_i$计算$Q_{sPKG_i}=H_1(sPKG_i)$,验证$e(D_{sPKG_i},P)\stackrel{?}{=}e(Q_{sPKG_i},P_{pub})$,判断$D_{sPKG_i}$是否正确;计算子系统参数$P_{pub}^{sPKG_i}=K_iP$;向网络中的所有其他sPKGs洪泛消息$m_0$,告知自己的公开参数$P_{pub}^{sPKG_i}$和所拥有路由器列表$(1\le i\le n)$.

$$m_0:sPKG_i\rightarrow sPKGs_{\ne i}:\sigma_{D_{sPKG_i}}(p_{pub}^{sPKG_i}\|AS_i\|Routers_{sPKG_i}),1\le i\le n.$$

其中,集合$sPKGs_{\ne i}=\{sPKG_1,\ldots,sPKG_n\}-\{sPKG_i\}$,$AS_i$表示$sPKG_i$所在自治系统号码,$Routers_{sPKG_i}$表示$sPKG_i$所在自治系统拥有路由器列表$(1\le i\le n)$.

获得网络中所有其他sPKGs发布的消息m_0且验证正确后,$sPKG_i$生成sPKGs-AS和sPKGs-Routers映射表并向本ASes内的所有路由器发布公开参数$(P,P_{pub},H_1,H_2,H_3,P_{pub}^{sPKG_1},\ldots,P_{pub}^{sPKG_n})$.

2. Retrieving Private Key(获取私钥)

自治系统和路由器通过该过程获取自己的私钥.以路由器为例说明.在详细描述之前,说明如下:

① 假设自治系统AS中路由器R欲获取自己的私钥.$sPKG_1$是R的主sPKG.R的公钥$ID_j:R\|t_j\|AS$,t_j表示公钥的第j个有效期,$j\ge 0$.

② $\sigma_{D_{sPKG_1}}(ID_j\|X_j)$表示$sPKG_1$为$R$生成的身份证明,公开的盲系数$X_j=x_jP$,$R$任选$x_j\in\mathbb{Z}_p^*$且保持秘密$(j\ge 0)$.

③ R的私钥碎片$D_{ID_j}^i=K_iQ_{ID_j}$,$Q_{ID_j}=H_1(ID_j)$;R验证$e(D_{ID_j}^i,P)\stackrel{?}{=}e(Q_{ID_j},P_{pub}^{sPKG_i})$,以判断$D_{ID_j}^i$是否正确$(j\ge 0,1\le i\le t)$.

④ R的盲私钥碎片$BD_{ID_j}^i=H_3(e(K_iX_j,P_{pub}^{sPKG_i}))D_{ID_j}^i$ $(j\ge 0,1\le i\le t)$.私钥碎片加盲使$sPKG_i$可以秘密传输$D_{ID_j}^i$至R.因为$H_3(e(K_iX_j,P_{pub}^{sPKG_i}))=H_3(e(K_ix_jP,P_{pub}^{sPKG_i}))=H_3(e(P_{pub}^{sPKG_i},P_{pub}^{sPKG_i})^{x_j})$,只有知道秘密$x_j$的路由器才能够去盲、获得私钥碎片$D_{ID_j}^i=\dfrac{BD_{ID_j}^i}{H_3(e(P_{pub}^{sPKG_i},P_{pub}^{sPKG_i})^{x_j})}$ $(j\ge 0,1\le i\le t)$.

⑤ $sPKG_i$对$BD_{ID_j}^i$的签名$\theta_i(BD_{ID_j}^i)=K_iBD_{ID_j}^i$;$R$验证$e(\theta_i(BD_{ID_j}^i),P)\stackrel{?}{=}e(BD_{ID_j}^i,P_{pub}^{sPKG_i})$,以判断$BD_{ID_j}^i$是否由$sPKG_i$发布$(j\ge 0,1\le i\le t)$.

2-1. Initial Off-Line Issuing(初始离线发布)

初始时,R随机选择$x_0\in\mathbb{Z}_p^*$,计算盲系数$X_0=x_0P$,离线提交X_0和初始公钥ID_0至$sPKG_1$.$sPKG_1$离线发布初始私钥碎片$D_{ID_0}^1$和身份证明$\sigma_{D_{sPKG_1}}(ID_0\|X_0)$至$R$.

2-2. Primary sPKG Request(主 sPKG 请求)

当私钥$D_{ID_{j-1}}$将要过期时,R随机选择$x_j\in\mathbb{Z}_p^*$,计算$X_j=x_jP$,向$sPKG_1$发送消息$m_1(j\ge 1)$.

$$m_1:R\rightarrow sPKG_1:\sigma_{D_{ID_{j-1}}}(ID_j\|X_j),j\ge 1.$$

2-3. Primary sPKG Response(主 sPKG 响应)

收到消息m_1后,$sPKG_1$验证$\sigma_{D_{ID_{j-1}}}(ID_j\|X_j)$ $(j\ge 1)$.若签名正确,ID_j是R的最新公钥且R是本自治系统内的路由器,则$sPKG_1$向R发送消息m_2.

$$m_2:sPKG_1\rightarrow R:BD_{ID_j}^1,\theta_1(BD_{ID_j}^1),\sigma_{D_{sPKG_1}}(ID_j\|X_j),j\ge 1.$$

2-4. Secondary sPKG Request(次 sPKG 请求)

初始时,R 获得 $D^1_{ID_0}$ 和 $\sigma_{D_{sPKG_1}}(ID_0 \| X_0)$ 后,验证它们的正确性.

收到消息 m_2 后,R 首先判断 $BD^1_{ID_j}$ 是否由 $sPKG_1$ 发布;去盲、获得 $D^1_{ID_j}$;验证 $D^1_{ID_j}$ 和 $\sigma_{D_{sPKG_1}}(ID_j \| X_j)$ 的正确性.

若上述操作都成功,则 R 分别向其他任意 $t-1$ 个不同的次sPKGs,表示为($sPKG_2 \ldots sPKG_t$),发送消息 m_3;反之,则 R 应该退出私钥获取过程且向系统管理员报告($j\geq 0$).

$$m_3: R \rightarrow sPKG_i: sPKG_1, \sigma_{D_{sPKG_1}}(ID_j \| X_j), j\geq 0, 2\leq i\leq t.$$

2-5. Secondary sPKG Response(次 sPKG 响应)

收到 m_3 后,$sPKG_i$ 验证身份证明 $\sigma_{D_{sPKG_1}}(ID_j \| X_j)$ 是否正确;判断 ID_j 是否是 R 的最新公钥;查询sPKGs-Routers映射表,判断 R 与 $sPKG_1$ 之间是否存在映射关系,即属于相同的自治系统.若上述操作都成功,则 $sPKG_i$ 向 R 发送消息 m_4($j\geq 0, 2\leq i\leq t$).

$$m_4: sPKG_i \rightarrow R: BD^i_{ID_j}, \theta_i(BD^i_{ID_j}), j\geq 0, 2\leq i\leq t.$$

2-6. Private Key Retrieving(私钥生成)

收到 m_4 后,R 判断 $BD^i_{ID_j}$ 是否由 $sPKG_i$ 发布;去盲、获得 $D^i_{ID_j}$;验证 $D^i_{ID_j}$ 是否正确($j\geq 0, 2\leq i\leq t$).若 $D^i_{ID_j}$ 不正确,则 R 向 $sPKG_k$ 重新发送消息 m_3($j\geq 0, 2\leq i\leq t, t<k\leq n$).

最后,R 获得多项式 $f(x)=\sum_{i=1}^{t} D^i_{ID_j} \prod_{r\neq i, r=1}^{t} \frac{x-x_r}{x_i-x_r} \bmod q$,计算私钥 $D_{ID_j}=f(0)(j\geq 0)$.

R 获取私钥的过程如图 1 所示.

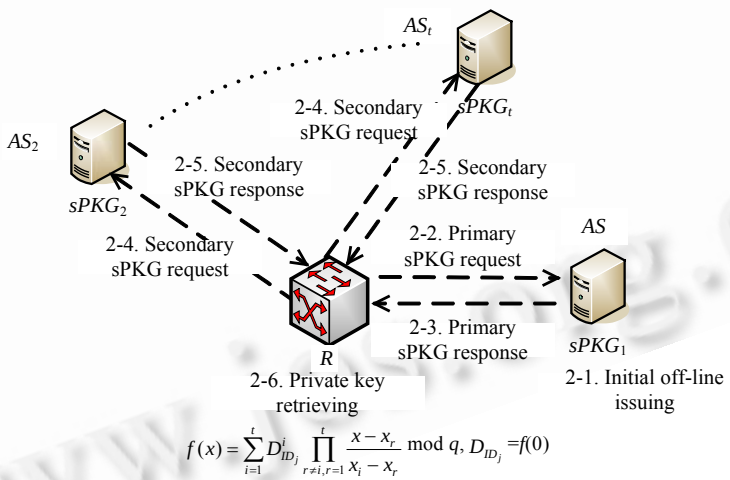


Fig.1 Process of R's private key being retrieved

图 1 R 的私钥获取过程

1.3 安全分析

CKY体制在随机预言模型下是适应性选择消息和身份攻击下存在性不可伪造的[28].在所有参与者都是诚实参与者且不存在不少于 t 个串通参与者的前提下,Shamir秘密共享体制机制能够保证:当把秘密 S 分配给 n 个参与者时,只有参与者集合 P 的子集 A 满足条件 $|A|\geq t$ 时,可以重构 S;只要 $|A|<t$ 就不能重构 S.

DHKI协议保证了:① 系统主密钥的秘密性.系统主密钥被分割成 n 个碎片,且被分发到 n 个不同的sPKG;在Internet中串通自治系统的个数小于 t 的前提下,sPKGs不知道也无法恢复系统主密钥.ICANN在生成主密钥碎片后,销毁主密钥;② 私钥的秘密性.sPKG仅生成私钥碎片,因而它不知道完整私钥;通过使用仅请求自治系统/路

由器知道的秘密x加盲私钥碎片,这些私钥碎片又被秘密地从sPKG传输到请求自治系统/路由器.基于Internet中RIR个数确定且不发生变化的假设,DHKI协议设计ICANN根据主密钥一次性生成所有RIRs的私钥,且安全离线分发私钥后,ICANN销毁这些私钥;③ 私钥的正确性.sPKG对盲私钥碎片的签名使请求自治系统/路由器能够确认该私钥碎片是否来自于正确的sPKG;自治系统/路由器可以验证获得私钥碎片的正确性. DHKI也提供RIR验证私钥正确性的方法.最后,DHKI协议能够抵抗恶意sPKG假冒攻击.每个sPKG都保存sPKGs-AS和sPKGs-Routers映射表,因而在sPKG不会执行任意危害本AS操作的假设下,任意sPKG假冒其他用户(自治系统或者路由器)请求私钥碎片的行为都能够被检测出.例如,当$sPKG_i$生成$sPKG_j$中路由器R'的身份证明,向$sPKG_k$请求R'的私钥碎片时,$sPKG_k$验证sPKGs-Routers映射表,发现路由器R'与$sPKG_i$不在相同自治系统内,从而拒绝$sPKG_i$的恶意请求($1\le i,j,k\le n, i\ne j\ne k$).

2 id^{2}r的源AS验证机制

2.1 上层ISP前缀劫持攻击

2.1.1 对 S-BGP 的上层 ISP 前缀劫持攻击实例

S-BGP采用并行于IP地址实际分配系统的地址分配PKI发布地址分配证书.地址分配证书实现分配前缀ISP,前缀和获得前缀ISP的绑定.获得前缀ISP使用与地址分配证书(公钥证书)对应的私钥签名自治系统生成地址证明.图 2(b)是并行于图 2(a)所示IP地址实际分配系统的地址分配PKI.当APNIC分配地址($Prefix_1$,$Prefix_2$,$Prefix_3$,$Prefix_4$,$Prefix_5$)至ISP_1时,ISP_1生成自己的公/私钥对,并上传自己的公钥至APNIC,由APNIC发布自己的公钥证书.与一般公钥证书不同,S-BGP要求公钥证书包括分配的地址空间.例如,ISP_1的公钥证书可表示为$PKC(APNIC,Prefix_1,Prefix_2,Prefix_3,Prefix_4,Prefix_5,ISP_1)$.从而,公钥证书也称为地址分配证书.$ISP_1$使用私钥签名$AS_1$生成地址证明$[AS_1]_{PKC(APNIC,Prefix_1,Prefix_2,Prefix_3,Prefix_4,Prefix_5,ISP_1)}$.$[M]_{PKC}$表示使用与公钥证书PKC对应的私钥签名消息$M$.当 ASes 收到路由通告后,需获得通告前缀的地址证明及相应 ISP 的公钥证书,以验证通告前缀的源 AS 是否合法.

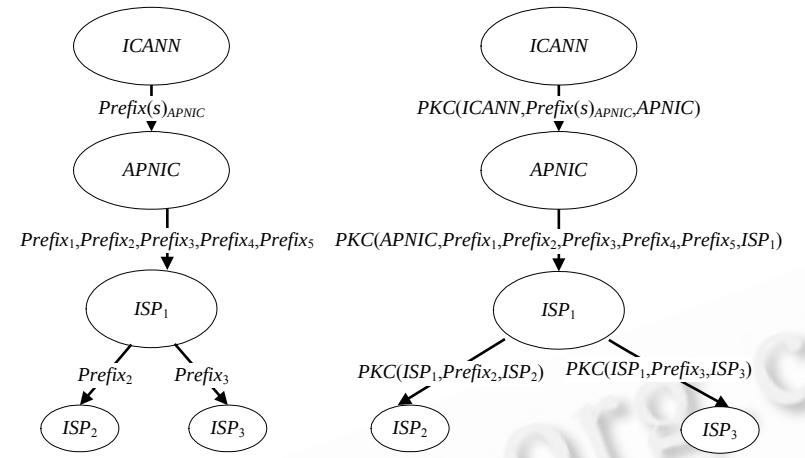
在图 3(a)所示拓扑中,AS_2多宿主(multi-homing)于AS_1和AS_5,且AS_2与AS_1间的链路是备份链路.为便于说明,本文视一个自治系统为一个BGP路由器.正常情况下,AS_2向AS_5发出$Prefix_2$可达的路由通告,其中AS_PATH为{2};向AS_1也发出$Prefix_2$可达的路由通告,但其中AS_PATH为{2 2 2 2}.基于BGP最优路由选择规则,AS_6和AS_7将选择从AS_5学习到的路由作为到达$Prefix_2$的最优路由.假设图 3(a)中的网络都被布署S-BGP,通过以下步骤,AS_1仍可劫持前缀$Prefix_2$(如图 3(b)所示):

① AS_1发出$Prefix_2$可达的路由通告,其中AS_PATH为{1};

② 根据BGP最优路由选择规则,AS_6和AS_7选择从AS_1学习到的路由.因为AS_6和AS_7与AS_1,AS_5之间都是peer-peer的商业关系,且从AS_1学习到路由的AS_PATH短于从AS_5学习到的.

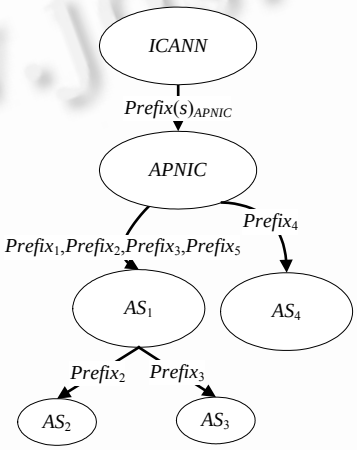
③ 根据S-BGP源AS验证机制,AS_6和AS_7验证AS_1是否是$Prefix_2$的合法源AS:使用ISP_1的公钥证书$PKC(APNIC,Prefix_1,Prefix_2,Prefix_3,Prefix_4,Prefix_5,ISP_1)$验证地址证明$[AS_1]_{PKC(APNIC,Prefix_1,Prefix_2,Prefix_3,Prefix_4,Prefix_5,ISP_1)}$是否正确.显然,该地址证明正确;且$ISP_1$的公钥证书含有$Prefix_2$,因而$AS_6$和$AS_7$认为$ISP_1$“授权”$AS_1$通告$Prefix_2$,即$AS_1$是$Prefix_2$的“合法”源AS.

最终,AS_6和AS_7选择从AS_1学习到的路由作为到达$Prefix_2$的最优路由.AS_6和AS_7及其连接网络发起的到达$Prefix_2$的数据流都被转发到AS_1,AS_1成功劫持前缀$Prefix_2$.



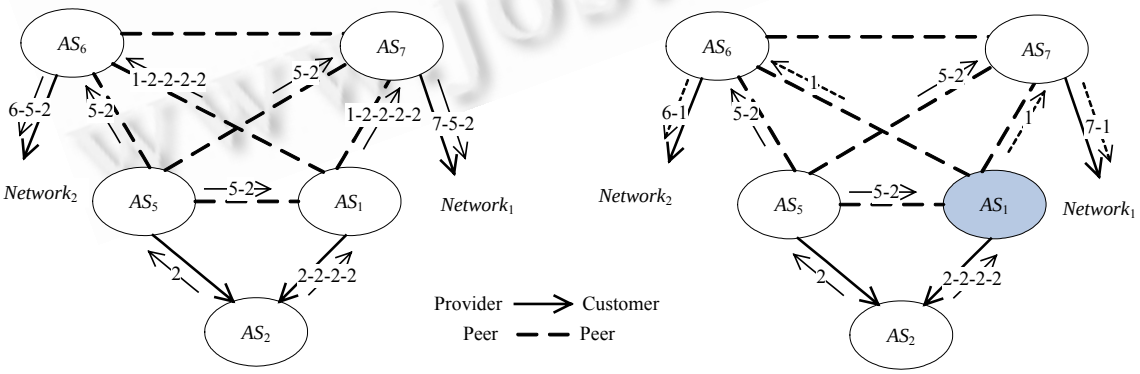
(a) IP address assignment structure
(a) IP地址分配结构

(b) Address assignment PKI paralleling Fig.2(a)
(b) 并行于图2(a)的地址分配PKI



(c) IP address AS-based assignment structure
(c) IP地址AS分配结构

Fig.2
图 2



(a) Network topology
(a) 网络拓扑图

(b) Up-Layer ISP prefix hijacking attack
(b) 上层ISP前缀劫持攻击

Fig.3
图 3

2.1.2 上层 ISP 前缀劫持攻击分析

分析上述攻击过程发现,AS_1成功劫持$Prefix_2$的直接原因虽然是ISP_1公钥证书含有$Prefix_2$,但根本原因是S-BGP只保证前缀被它分配路径上的ISP授权通告,而不能保证被拥有ISP(即ISP_2)授权通告.因为攻击由$Prefix_2$拥有ISP的上层ISP(即ISP_1)发起,称为上层ISP前缀劫持攻击.

Internet 中,当客户网络只有一个提供商网络时,所有到达客户网络的数据报文都通过提供商网络,因此该提供商网络没有劫持客户网络前缀的必要.但是,当客户网络拥有多个提供商网络,且所有到达客户网络的数据报文都不经过其中某个提供商网络时,该提供商网络可能劫持它分配给客户网络的前缀,发起上层 ISP 前缀劫持攻击.上层 ISP 前缀劫持攻击的发生概率:

$$P(\text{Internet 中上层 ISP 前缀劫持攻击发生})\approx P(\text{Internet 中有多个提供商网络的客户网络})=\frac{\text{Number of multi-homed ASes}}{\text{Number of all ASes}}.$$

总之,即使Internet中所有ASes都被布署S-BGP,仍有 70%的ASes[36]可能会受到一种上层ISP前缀劫持攻击.

SoBGP,SPV甚至源AS验证机制OA(origin authentication)[37]都存在与S-BGP相同的安全缺陷,会导致上层ISP前缀劫持攻击.因篇幅所限,本文不再展开说明.

2.2 LAP

2.2.1 IP 地址 AS 分配系统

根据 IP 地址实际分配系统中 ISPs 之间的层次关系,这些 ISPs 拥有的自治系统之间也形成一个相应的层次结构,本文称这种层次结构为 IP 地址 AS 分配系统.IP 地址分配系统中的 ICANN 和 Internet 注册机构不拥有 ASes,故这些机构仍存在于 IP 地址 AS 分配系统中.

LAP 基于 IP 地址 AS 分配系统.基于 IP 地址实际分配系统的源 AS 验证机制(如 S-BGP)要求密钥管理机制管理 Internet 中所有 ISP 的密钥,如 S-BGP 的地址分配 PKI;而 LAP 仅要求管理 Internet 中所有自治系统的密钥,密钥管理相对简单.

针对一个 ISP 可能拥有多个自治系统的实际情况,本文视这些自治系统彼此独立且在 IP 地址 AS 分配系统中位于相同一层.如果该 ISP 继续向下分配地址,它需要从拥有的多个自治系统中选出一个主自治系统.主自治系统拥有本自治系统被授权通告的前缀,分配给下层 ISP 的前缀以及从上层 ISP 获得但是未分配的前缀.其他自治系统是从自治系统.从自治系统仅拥有该自治系统被授权通告的前缀.

图 2(a)所示的IP地址实际分配系统中,APNIC分配前缀($Prefix_1$,$Prefix_2$,$Prefix_3$,$Prefix_4$,$Prefix_5$)到ISP_1,其中指定前缀包括$Prefix_1$和$Prefix_4$,分配前缀包括$Prefix_2$,$Prefix_3$和$Prefix_5$;ISP_1进一步地分配$Prefix_2$到ISP_2, $Prefix_3$到ISP_3.ISP_1拥有主自治系统AS_1和从自治系统AS_4,且授权AS_1通告$Prefix_1$,AS_4通告$Prefix_4$;ISP_2拥有AS_2,ISP_3拥有AS_3.最终获得如图 2(c)所示的IP地址AS分配系统.

2.2.2 APAs 定义

定义 1(分配证明). 在IP地址AS分配系统中,假设自治系统AS_{issuer}分配前缀$prefix_{ASsubscriber}$到$AS_{subscriber}$,定义($prefix_{ASsubscriber}$,$AS_{subscriber}$)的分配证明是$\sigma_{D_{AS_{issuer}}}(AS_{issuer}, prefix_{AS_{subscriber}}, AS_{subscriber}, SN_{AS_{subscriber}})$.$SN_{ASsubscriber}$为$AS_{subscriber}$分配证明序列号,初始为 0.

定义 2(分配路径证明). 在IP地址AS分配系统中,假设前缀p的分配路径是(AS_t,AS_{t-1},…,AS_2,AS_1,IR),定义(p,AS_t)的分配路径和证明(assignment path and attestations,简称APAs)是($AS_t||AS_{t-1}||\ldots||AS_2||AS_1||IR$, $\sigma_{D_{IR}}(IR, prefix_{AS_1}, AS_1, SN_{AS_1})\|\sigma_{D_{AS_1}}(AS_1, prefix_{AS_2}, AS_2, SN_{AS_2})\|\ldots\|\sigma_{D_{AS_{t-1}}}(AS_{t-1}, AS_t, SN_{AS_t})$).其中,$prefix_{AS_i}$含有前缀 p,$1\le i\le t-1$.

在图 2(c)所示的IP地址AS分配系统中,($Prefix_4$,AS_4)的APAs是($AS_4||APNIC$, $\sigma_{D_{APNIC}}(APNIC,Prefix_4,AS_4, SN_{AS_4})$),($Prefix_2$,$AS_2$) 的 APAs 是 ($AS_2||AS_1||APNIC$, $\sigma_{D_{APNIC}}(APNIC,Prefix_1,Prefix_2,Prefix_3,Prefix_5,AS_1, SN_{AS_1})\|$

$\sigma_{D_{AS_1}}(AS_1,Prefix_2,AS_2,SN_{AS_2})$).

2.2.3 APAs 的分发

APAs 分发机制应该保证:① 前缀源 AS 发布该前缀的 APAs;② 分发过程中 APAs 的完整性;③ APAs 分发路径不包括 IP 地址 AS 分配系统中该前缀源 AS 的上层 AS,以防止 APAs 被删除.因为 IP 地址 AS 分配系统中,某 AS 的上层 AS 可能就是实际中为该 AS 提供连接服务的 Transit AS.这也是 LAP 不采用更新报文分发 APAs 的原因之一.其他原因包括更新报文长度有限,最大长度仅是 4 096 字节;若更新报文携带 APAs,路由器需验证其中 APAs 的正确性,大大增加路由器处理负担,且带宽浪费严重,因为任一路由器都会收到多个重复的 APAs.

本文建议 LAP 机制采用多个同步知识库存储、分发 APAs.该方法与 S-BGP 地址证明的分发方法类似.自治系统签名拥有前缀的 APAs、生成(AS,签名 APAs);ISP NOC(network operation center,网络运行中心)收集它拥有自治系统的(AS,签名 APAs),上传到一个知识库中;同时,ISP NOC 从知识库下载所有的(AS,签名 APAs).知识库周期性地彼此交互以保持同步.

2.2.4 源 AS 验证

从知识库中下载所有的(AS,签名 APAs)后,ISP NOC 对每个(AS,签名 APAs)依次执行以下操作,最终生成一个全球前缀和 AS 映射表.

① 验证(AS,签名 APAs)中签名 APAs 是否正确,且判断其 AS 是否是 APAs 分配路径中的第 1 个自治系统;

② 若步骤①操作成功,则验证 APAs 是否正确性,验证算法如图 4 所示;

③ 若 APAs 正确,则获得前缀的分配路径;

④ 对相同前缀,若存在多个分配路径,选择最长的分配路径,建立前缀与最长分配路径中第 1 个自治系统的映射关系;

⑤ 对相同前缀,若存在多个最长分配路径,则建立前缀与这些最长分配路径中第 1 个自治系统的映射关系.

```
1.  BOOL APA_verification(APA,apa) {
2.    prefix prefix=get_prefix(apa);
3.    path   path=get_path(apa);
4.    attestations attests=get_attestations(apa);
5.    int path_length=get_path_length(path);
6.    int attests_length=get_attestations_length(attests);
7.    BOOL succeed=FALSE;
8.    while ((path_length==attests_length+1)
            && (attests_length≠0)) {
9.      AS AS_issuer=get_last_AS(path);
10.     AS AS_subscriber=get_last_second_AS(path);
11.     attestation aa=get_first_attestation(attests);
12.     if ((it is succeed to verify aa with AS_issuer's public key)
          && (prefixs in aa includes prefix)
          && (AS in aa equals AS_subscriber)
          && (sequence number in aa equals AS_subscriber's
              sequence number))
        then {
13.                 path=path−AS_last;
14.                 attests=attests−aa;
15.                 path_length−−;
16.                 attests_length−−;
17.                 succeed=TRUE;
18.           }
19.     else return FALSE;
20.   }
21.   return succeed;
22.   }
```

Fig.4 APAs verification algorithm

图 4 APAs 验证算法

ISP NOC生成全球前缀和AS映射表后,离线下发到所拥有自治系统中的id²r路由器.当id²r路由器收到更新报文时,首先查询全球前缀和AS映射表,判断更新报文通告前缀与更新报文的发起AS之间是否存在映射关系.若存在,进一步地处理报文;反之,直接丢弃该报文.APAs分发和源AS验证过程如图 5 所示.

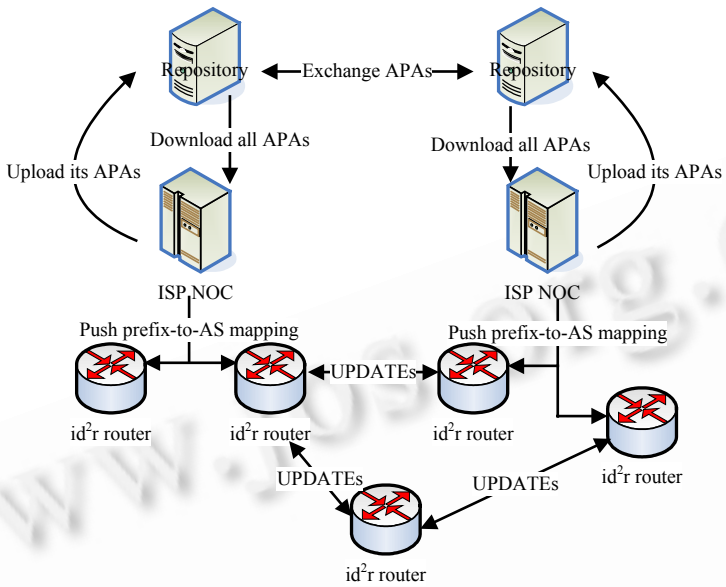


Fig.5 ATAs distribution and origin AS verification

图 5 ATAs 分发及源 AS 验证

2.2.5 安全性分析

恶意自治系统难以伪造前缀的最长分配路径证明.分以下两种情况说明:① 某个自治系统希望伪造一个前缀的最长分配路径证明,但它不位于该前缀的分配路径上,那么它至少需要伪造一个由前缀源 AS 或源 AS 的上层 AS 生成的分配证明.在这种情况下,恶意自治系统伪造前缀最长分配路径证明的难度取决于所用密码体制的安全性.② 若一个位于某前缀分配路径上的自治系统希望伪造一个该前缀的最长分配路径证明,那么它只能是该前缀源 AS 的上层 AS.在这种情况下,即使成功伪造了一个将前缀分配给某个无辜自治系统的分配证明,它也不能发布含有伪造分配证明的 APAs.因为 LAP 机制要求只有前缀的源 AS,即那个无辜自治系统,才能够发布该 APAs.

LAP 机制能够抵抗 APAs 重放攻击,因为前缀分配证明中含有时间信息(即分配证明序列号).当前缀的分配状态发生变化时,需要更新相关 APAs.LAP 假设所有自治系统都会主动执行 APAs 更新操作.实际中,该假设是合理的.例如,当某个 ISP 收回它已分配的前缀时,该 ISP 一定会要求收回前缀的原源 AS 更新自己的 APAs.

分发APAs由可信第三方机构完成且在分发过程中APAs不经过前缀分配路径上任一ASes,因而APAs在分发过程中不会被修改或删除.id²r路由器直接从本ISP NOC下载全球前缀和AS映射表,因而全球前缀和AS映射表也不会被修改.

3 id²r的AS_PATH验证机制

id²r的AS_PATH验证机制IDAPV引入路由聚合证明保护AS_PATH路径属性不被篡改,且新定义可选传输路径属性Route Aggregate Attestations以携带路由聚合证明,及Router Identities以携带更新报文穿过路由器的身份信息.当要向外发散路由时,路由器首先使用私钥签名NLRI,AS_PATH和下一跳AS号码生成自己的路由证明,然后采用签名聚合算法聚合自己的路由证明和原Route Aggregate Attestations属性携带的路由聚合证明,生成新的Route Aggregate Attestations属性.

具体地,收到id²r路由通告报文(如图 6 所示)后,路由器R执行以下操作:

① 根据Router Identities携带的路由器身份信息,生成该报文穿过路由器的公钥序列($ID_{R_{AS_1}},...,ID_{R_{AS_n}}$),其中, $ID_{R_{AS_i}} = R_{AS_i} \| t_j \| AS_i, 1 \le i \le n$;

② 根据($ID_{R_{AS_1}},...,ID_{R_{AS_n}}$),使用聚合签名验证算法,验证Route Aggregate Attestations中$AggreSig((IP_1,AS_1,AS_2),\ldots,(IP_1,AS_1,\ldots,AS_n,AS))$的正确性;

③ 若验证失败,路由器直接丢弃该报文;反之,根据 BGP 协议定义的路由处理过程,进一步处理该报文;

④ 如果要向外发散路由,路由器使用自己的私钥 D_{ID_j} 签名路由通告报文的$NLRI(IP_1)$、新的AS_PATH属性$(AS,AS_n,\ldots,AS_1)$和下一跳AS号码(AS_{n+2})生成自己的路由证明 $\sigma_{D_{ID_j}}(IP_1\|AS_1\|\ldots\|AS_n\|AS\|AS_{n+2})$;

⑤ 使用签名聚合算法聚合自己的路由证明 $\sigma_{D_{ID_j}}(IP_1\|AS_1\|\ldots\|AS_n\|AS\|AS_{n+2})$和$AggreSig((IP_1,AS_1,AS_2),\ldots,(IP_1,AS_1,\ldots,AS_n,AS))$,生成新的Route Aggregate Attestations属性值:$AggreSig((IP_1,AS_1,AS_2),\ldots,(IP_1,AS_1,\ldots,AS_n,AS,AS_{n+2}))$;

⑥ 添加自己的身份信息 R 到 Router Identities 中,生成新的 Router Identities 属性;

⑦ 向外发散新的路由通告:$\{IP_1,(AS,AS_n,\ldots,AS_1),(R,R_{AS_n},...,R_{AS_1}),AggreSig((IP_1,AS_1,AS_2),\ldots,(IP_1,AS_1,\ldots,AS_n,AS,AS_{n+2}))\}$.

图 6 中的IP_1表示AS_1发起的网络层可达性信息,$(AS_n,\ldots,AS_1)$表示AS_PATH路径属性,($R_{AS_n},...,R_{AS_1}$)表示Router Identities路径属性,$AggreSig((IP_1,AS_1,AS_2),\ldots,(IP_1,AS_1,\ldots,AS_n,AS))$/ $\sigma_{D_{R_{AS_1}}}(IP_1\|AS_1\|AS_2)$ 表示Route Aggregate Attestations路径属性, $\sigma_{D_{R_{AS_1}}}(IP_1\|AS_1\|AS_2)$ 表示路由器 R_{AS_1} 对(IP_1,AS_1,AS_2)的签名, R_{AS_i} 表示该路由通告穿过自治系统AS_i中路由器的身份信息$(1\le i\le n)$.

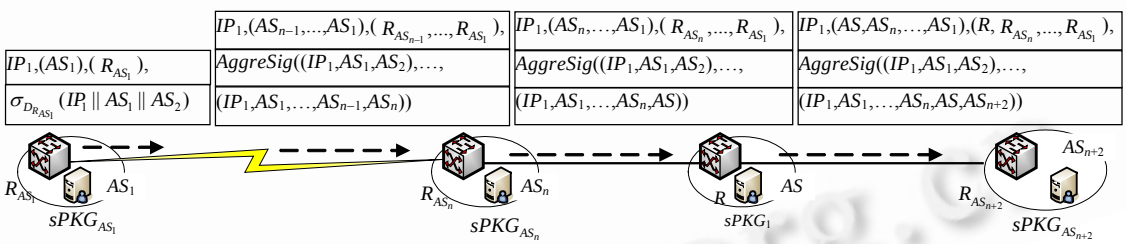


Fig.6 Figure sketches the transmission process of an id²r route announcement

图 6 id²r路由通告报文发散过程

4 评 估

4.1 安全性评估

根据文献[21]中前缀劫持攻击的分类,id²r可抵抗有效前缀劫持、子前缀劫持、未使用前缀劫持,特别是上层ISP前缀劫持攻击.以第 2.1.1 节针对S-BGP的上层ISP前缀劫持攻击为例详细说明.假设图 3(a)中网络都被布署id²r,AS_1欲劫持前缀$Prefix_2$:

① AS_1发出$Prefix_2$可达的路由通告,其中AS_PATH为{1};

② 根据BGP最优路由选择规则,AS_6和AS_7选择从AS_1学习到的路由;

③ 根据LAP,AS_6和AS_7查询AS_1与$Prefix_2$之间是否存在映射关系,以判断AS_1是否被授权发起前缀$Prefix_2$.LAP中,前缀只与提供其最长分配路径和证明的自治系统之间建立映射关系.因为AS_1发布的$Prefix_2$分配路径不是最长的(AS_2发布的才是最长的);根据第 2.2.5 节分析,恶意自治系统不能够伪造前缀的最长分配路径证明,即AS_1不能够伪造$Prefix_2$的最长分配路径;AS_2发布的$Prefix_2$分配路径及证明不经过AS_1,AS_1无法将其修改或删除.从而导致AS_1和$Prefix_2$之间不会存在映射关系,即AS_1非法发起前缀$Prefix_2$.

最终,AS_6和AS_7不会选择从AS_1学习到的路由作为到达$Prefix_2$的最优路由.id^{2}r阻止了上层ISP前缀劫持攻击的发生.

本文忽略覆盖(covering)前缀劫持攻击,因为只有当劫持者成功伪造覆盖前缀的有效最长分配路径和证明,且到达子前缀的路由被撤销时,劫持者才能成功劫持覆盖前缀.id^{2}r没有提供对有效前缀错误路径(valid prefix with false path)劫持攻击的保护,因为它由AS_PATH验证机制完成.

id^{2}r有效地验证了AS_PATH的真实性,可抵抗任意AS_PATH篡改攻击.现以AS_PATH缩短攻击为例说明.在如图 7 所示的拓扑中,正常情况下,AS_7分别从AS_5和AS_6收到AS_1发起前缀(如 61.52.0.0/16)的两个路由通告,其中,AS_PATH属性分别为{AS_5 AS_3 AS_1}和{AS_6 AS_4 AS_1}.AS_7与AS_5/AS_6之间是peer-peer关系,且这两个AS_PATH属性的长度相同,AS_7将根据其他属性(如ORIGIN,MED等)选择到达 61.52.0.0/16 的最优路由.但是,当AS_7从AS_5收到具有缩短AS_PATH属性({AS_5 AS_1})的路由通告时,它将选择该恶意路由作为到达 61.52.0.0/16 的最优路由,发生AS_PATH缩短攻击(如图 8 所示).假设图 7 中所有自治系统都被布署id^{2}r,如果AS_5仍要发起相同的AS_PATH缩短攻击,它必须根据真实的路由聚合证明 $AggreSig$((61.52.0.0/16,AS_1,AS_3),(61.52.0.0/16,AS_1,AS_3,AS_5),(61.52.0.0/16,AS_1,AS_3,AS_5,AS_7))伪造路由聚合证明$AggreSig$((61.52.0.0/16,AS_1,AS_5),(61.52.0.0/16,AS_1,AS_5, AS_7)).基于id^{2}r所采用密码机制的安全性,对AS_5而言,这是一项不可能完成的任务.

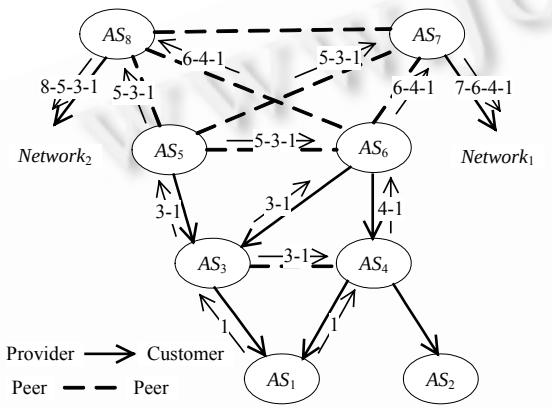


Fig.7 A network topology

图 7 网络拓扑图

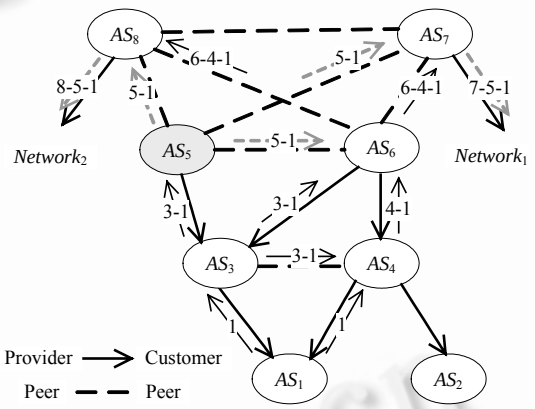


Fig.8 AS PATH shortening attack

图 8 AS_PATH 缩短攻击

4.2 性能评估

4.2.1 内存空间

id^{2}r路由器需存储全球前缀和AS映射表及公开参数(P,P_{pub},H_1,H_2,H_3, $P_{pub}^{sPKG_1}$,...,$P_{pub}^{sPKG_n}$);S-BGP路由器需存储全球前缀和AS映射表及Internet中所有S-BGP路由器的公钥.假设N_{AS}表示Internet中自治系统的数目,$E(N_{prefixes})$表示每个自治系统发起前缀数目的数学期望值;$M_{\mathrm{id}^2\mathrm{r}}^1$表示id^{2}r路由器存储全球前缀和AS映射表的内存开销,$M_{\mathrm{id}^2\mathrm{r}}^2$表示id^{2}r路由器存储基于$\mathbb{F}_{3^{97}}$公开参数的内存开销,$M_{\mathrm{id}^2\mathrm{r}}$表示id^{2}r路由器的额外总内存开销;$M_{\mathrm{S\text{-}BGP}}^1$表示S-BGP路由器存储全球前缀和AS映射表的内存开销,$M_{\mathrm{S\text{-}BGP}}^2$表示S-BGP路由器存储基于 1 024 bit RSA算法的Internet中所有其他S-BGP路由器公钥及自己公私钥的内存开销(每个AS中只有一个S-BGP路由器),$M_{\mathrm{S\text{-}BGP}}$表示S-BGP路由器的额外总内存开销.忽略公开参数中哈希函数H_1,H_2和H_3占用的内存空间.获得等式(1)~等式(6).

$$M_{\mathrm{id}^2\mathrm{r}}^1=N_{AS}\times(2+4\times E(N_{prefixes})) \tag{1}$$

$$M_{\mathrm{id}^2\mathrm{r}}^2=49+24.5\times N_{AS} \tag{2}$$

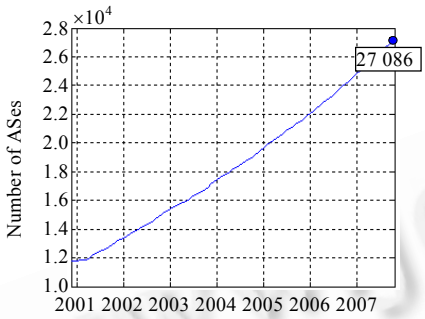
$$M_{\mathrm{id}^2\mathrm{r}}=M_{\mathrm{id}^2\mathrm{r}}^1+M_{\mathrm{id}^2\mathrm{r}}^2=4\times N_{AS}\times E(N_{prefixes})+26.5\times N_{AS}+49 \tag{3}$$

$$M^1_{\text{S-BGP}} = M^1_{\text{id}^2\text{r}} = N_{AS} \times (2+4\times E(N_{prefixes})) \quad (4)$$

$$M^2_{\text{S-BGP}} = 128\times(N_{AS}+1) \quad (5)$$

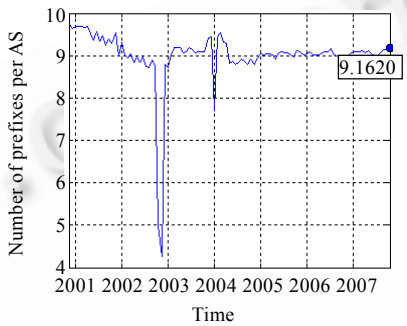
$$M_{\text{S-BGP}} = M^1_{\text{S-BGP}} + M^2_{\text{S-BGP}} = 4\times N_{AS}\times E(N_{prefixes}) + 130\times N_{AS} + 128 \quad (6)$$

基于 2001 年至今的RouteViews[38]数据,N_{AS}和$E(N_{prefixes})$的变化分别如图 9(a)和图 9(b)所示.根据式(1)~式(3)和图 9(a)~图 9(c)给出了 $M^1_{\text{id}^2\text{r}}, M^2_{\text{id}^2\text{r}}$ 和 $M_{\text{id}^2\text{r}}$ 的变化曲线,根据式(4)~式(6)和图 9(a)、图 9(b)、图 9(d)给出了 $M^1_{\text{S-BGP}}, M^2_{\text{S-BGP}}$ 和$M_{\text{S-BGP}}$的变化曲线.总之,如图 9(e)所示,2007 年 12 月 7 日,与BGP路由器相比,id^{2}r路由器仅额外增加了 1.71M 字节的内存空间,是 S-BGP 路由器额外增加内存空间的 38%.



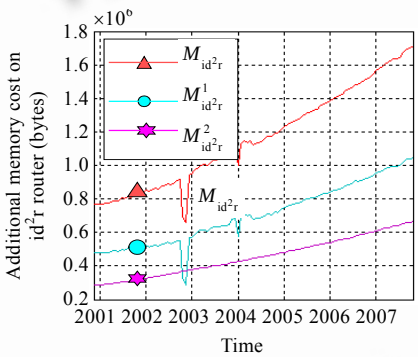
(a) Growth of N_{AS}

(a) N_{AS}增长图



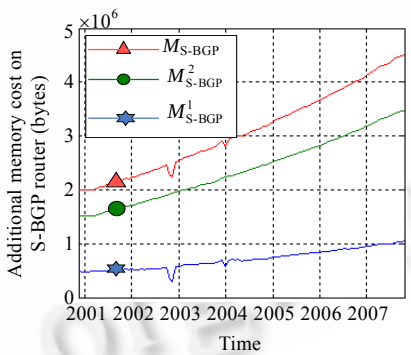
(b) Movement of $E(N_{prefixes})$

(b) $E(N_{prefixes})$变化图



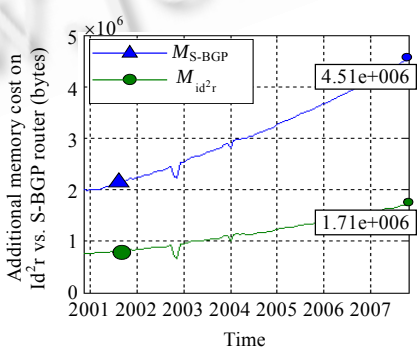
(c) Growth of $M^1_{\text{id}^2\text{r}}, M^2_{\text{id}^2\text{r}}$ and $M_{\text{id}^2\text{r}}$

(c) $M^1_{\text{id}^2\text{r}}, M^2_{\text{id}^2\text{r}}$ 及 $M_{\text{id}^2\text{r}}$ 增长图



(d) Growth of $M^1_{\text{S-BGP}}, M^2_{\text{S-BGP}}$ and $M_{\text{S-BGP}}$

(d) $M^1_{\text{S-BGP}}, M^2_{\text{S-BGP}}$ 及$M_{\text{S-BGP}}$增长图



(e) Comparison between $M_{\text{id}^2\text{r}}$ and $M_{\text{S-BGP}}$

(e) $M_{\text{id}^2\text{r}}$ 与$M_{\text{S-BGP}}$的比较

Fig.9

图 9

4.2.2 更新报文大小

因为采用 out-of-band 方式分发 APAs,LAP 机制没有增加更新报文长度.IDAPV 机制新增加了两个可选传输路径属性Route Aggregate Attestations和Router Identities.在基于 $\mathbb{F}_{3^{97}}$ 的CKY体制和 1024 bit的RSA,DSA算法下,$\Delta_{id^2r(CKY)}=28.5k+24.5$ 字节,$\Delta_{S\text{-}BGP(RSA)}=128k$字节和$\Delta_{S\text{-}BGP(DSA)}=40k$字节.$\Delta$表示更新报文与BGP更新报文长度的增量,$k$表示AS_PATH长度.如图 10 所示,id^{2}r更新报文长度短于S-BGP,虽然它比S-BGP多增加了一个新的路径属性Router Identities.

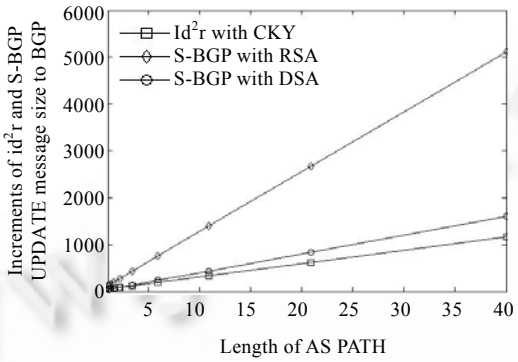


Fig.10 Increments of id^{2}r and S-BGPUPDATE message size to BGP

图 10 id^{2}r和S-BGP更新报文与BGP更新报文长度的增量

4.2.3 平均收敛时间

建议采用TCAM(ternary content addressable memory)技术实现全球前缀和AS映射表的快速查询.TCAM技术可达到 100M/s的查表速度.基于 2007 年 12 月 7 日的RouteViews数据,全球前缀和AS映射表大小为 1.05M,从而查询全球前缀和AS映射表引入延迟 1.05ms.在全互联网络拓扑上,采用SSFNET[39]仿真id^{2}r引入的平均收敛时间延迟.仿真参数设置如下:最小路由通告间隔(MRAI)M=30s,链路延迟ld=0.002s,更新报文的最小处理延迟$p_{\min}$=0.01s,最大处理延迟$p_{\max}$=1.0s.表 1 给出了配对计算,RSA签名和验证算法的运行时间.表 2 给出了id^{2}r/S-BGP路由器在验证和生成路由证明上花费的时间(k表示AS_PATH长度,$t_p/t_v/t_s$表示配对计算/RSA验证/RSA签名算法占用的时间).仿真结果(如图 11 所示)表明,在硬件实现配对计算时,id^{2}r的收敛时间显著缩短,几乎接近于BGP收敛时间.

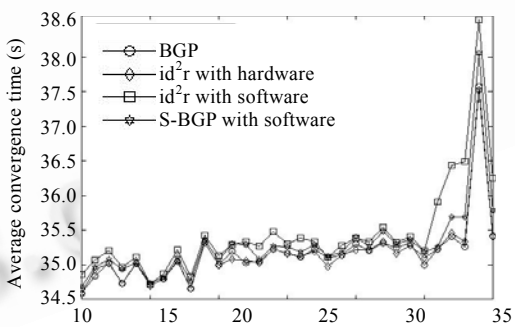


Fig.11 Average convergence time of id^{2}r, S-BGP and BGP

图 11 id^{2}r,S-BGP和BGP的平均收敛时间

Table 1 Running time of algorithms

表 1 算法运行时间

	Algorithm	Running time (ms)
Software (200MHz CPU)	Duursam-Lee on $\mathbb{F}_{3^{97}}$ [40]	43.0
	1024-bit RSA signing[41]	50.0
	1024-bit RSA verification[42]	2.5
Hardware	JMTE on $\mathbb{F}_{3^{97}}$ [31]	0.027

Table 2 Time of id^{2}r/S-BGP router on verifying and generating route attestations

表 2 id^{2}r/S-BGP路由器在验证和生成路由证明上所花费的时间

	Cryptographic operation time
id^{2}r update message	$(k+1)\cdot t_p$
S-BGP update message	$k\cdot t_v+t_s$

5 结束语

本文发现,目前一些典型的域间路由安全方案(如S-BGP)存在安全缺陷,易受到一种上层ISP前缀劫持攻击.同时,繁重复杂的PKI密钥管理和昂贵的内存开销也使这些安全方案在实际中难以实现和布署.与S-BGP相比,本文提出的id^{2}r基于前缀分配路径的长度验证前缀的合法源AS,能够抵抗上层ISP前缀劫持攻击,且采用基于身份的密码学,具有密钥管理简单、性能优化的特点,更易于实现和布署.但是,我们仍需要进一步完善id^{2}r.例如,解决当小规模布署时只能提供有限安全保护的问题.需要说明的是,虽然id^{2}r基于BGP协议,但id^{2}r中的LAP机制可应用于下一代域间路由协议,如HLP[42],以建立全球前缀和AS映射表.

References:

[1] Rekhter Y, Li T, Hares S. A border gateway protocol 4 (BGP-4). RFC4271, 2006.

[2] Murphy S. BGP security vulnerabilities analysis. RFC4272, 2006.

[3] Wow, AS7007! 1997. http://www.merit.edu/mail.archives/nanog/1997-04/msg00340.html

[4] Popescu AC, Premore BJ, Underwood T. Anatomy of a leak: AS9121. 2005. http://nanog.org/mtg-0505/underwood.html

[5] Karlin J, Forrest S, Rexford J. Pretty good BGP: Improving BGP by cautiously adopting routes. In: David L, ed. Proc. of the IEEE Int'l Conf. on Network Protocols. Washington: IEEE Computer Society Press , 2006. 290−299.

[6] Karlin J. A fun hijack: 1/8, 2/8, 3/8, 4/8, 5/8, 7/8, 8/8, 12/8 briefly announced by AS 23520 (today). 2006. http://www.merit.edu/mail.archives/nanog/2006-06/msg00082.html

[7] Con-Ed steals the net. 2006. http://www.renesys.com/blog/2006/01/coned steals the net.shtml

[8] Wan T, Oorschot C. Analysis of BGP prefix origins during Google's May 2005 outage. In: Spirakis P, ed. Proc. of the Security in Systems and Networks. Washington: IEEE Computer Society Press, 2006. 8−15.

[9] Boothe P, Hiebert J, Bush R. Short-Lived prefix hijacking on the Internet. In: Proc. of the NANOG 36 Meeting. 2006. http://www.nanog.org/mtg-0602/pdf/boothe.pdf

[10] Karlin J. As 8437 announced a quarter of the net for half of an hour. 2006. http://www.merit.edu/mail.archives/nanog/2006-8/msg00366.html

[11] Lad M, Oliveira R, Zhang B, Zhang L. Understanding resiliency of Internet topology against prefix hijack attacks. In: Anderson T, ed. Proc. of the Dependable Systems and Networks (DSN). Washington: IEEE Computer Society Press, 2007. 368−377.

[12] Pakistan hijacks youtube. 2008. http://www.renesys.com/blog/2008/02/pakistan_hijacks_youtube_1.shtml

[13] Ramachandran A, Feamster N. Understanding the network-level behavior of spammers. In: Christophe D, ed. Proc. of the ACM SIGCOMM. Washington: ACM Press, 2006. 291−302.

[14] Sauver JS. Route injection and spam. In: Proc. of the Messaging Anti-Abuse Working Group (MAAWG) 8th General Meeting. 2006. http://www.uoregon.edu/~joe/maawg8/maawg8.pdf

[15] Nordstrom O, Dovrolis C. Beware of BGP attack. ACM Computer Communications Review, 2004,34(2):1−8.

[16] Ballani H, Francis P, Zhang X. A study of prefix hijacking and interception in the Internet. In: Jun M, ed. Proc. of the ACM SIGCOMM. Washington: ACM Press, 2007. 265−276.

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

[18] White R. Securing BGP through secure origin BGP (soBGP). The Internet Protocol Journal, 2003,6(3):15−22.

[19] Wan T, Kranakis E, Oorschot C. On interdomain routing security and pretty secure BGP (psBGP). ACM Trans. on Information and System Security, 2007,10(3):11.

[20] Hu C, Perrig A, Sirbu M. SPV: Secure path vector routing for securing BGP. In: Yavatkar R, ed. Proc. of the ACM SIGCOMM. Washington: ACM Press, 2004. 179−192.

[21] Lad M, Massey M, Pei D, Wu Y, Zhang B, Zhang LX. PHAS: A prefix hijack alert system. In: Angelos K, ed. Proc. of the USENIX Security Symp. 2006. Berkeley: USENIX Assciation, 2006. 153−166.

[22] Krugel C, Mutz D, Robertson K, Valeur F. Topology-Based detection of anomalous BGP messages. In: John M, ed. Proc. of the RAID. Berlin: Springer-Verlag, 2003. 17−35.

[23] Hu X, Mao M. Accurate real-time identification of IP prefix hijacking. In: Deborah S, ed. Proc. of the IEEE Security and Privacy. Washington: IEEE Computer Society Press, 2007. 3−17.

[24] Zhao X, Pei D, Wang L, Massey D, Mankin A, Wu F, Zhang LX. Detection of invalid routing announcement in the Internet. In: Farnam J, ed. Proc. of the DSN. Washington: IEEE Computer Society Press, 2002. 59−68.

[25] Zheng C, Ji L, Pei D, Wang J, Francis P. A light-weight distributed scheme for detecting IP prefix hijacks in real-time. In: Jun M, ed. Proc. of the ACM SIGCOMM. Washington: ACM Press, 2007. 277−288.
[26] Huston G. Auto-Detecting hijacked prefixes? In: Proc. of the RIPE 50 meeting. 2005. http://www.ripe.net/ripe/meetings/ripe-50/resentations/index.html
[27] Qiu J, Gao L, Ranjan S, Nucci A. Detecting bogus BGP route information: Going beyond prefix hijacking. In: Bruno C, ed. Proc. of the Securecomm. Washington: IEEE Computer Society Press, 2007. 381−390.
[28] Chan H, Dash D, Perrig A, Zhang H. Modeling adoptability of secure BGP protocols. In: Luigi R, ed. Proc. of the ACM SIGCOMM. Washington: ACM Press, 2006. 279−290.
[29] Raghavan B, Panjwani S, Mityagin A. Analysis of the SPV secure routing protocol: Weaknesses and lessons. ACM SIGCOMM Computer Communication Review, 2007,37:29−38.
[30] Shamir A. Identity-Based cyrptosystems and signature schemes. In: Blakely R, ed. Proc. of the Advances in Cryptolog-CRYPTO'84. Berlin: Springer-Verlag, 1984. 47−53.
[31] Beuchat JL, Shirase M, Takagi T, Okamoto E. An algorithm for the η_T pairing calculation in characteristic three and its hardware implementation. 2006. http://eprint.iacr.org/2006/327
[32] Pan J, Cai L, Shen X. Promoting identity-based key management in wireless ad hoc networks. In: Yang X, ed. Proc. of the Wireless/Mobile Network Security-Springer Series on Signals and Communication Technology. Berlin: Springer-Verlag, 2007. 83−102.
[33] Boneh D, Lynn B, Shacham H. Short signature from the Weil pairing. In: Proc. of the Advances in Cryptology—AsiaCrypt 2001. 2001. 514−532.
[34] Cheon J, Kim Y, Yoon H. A new ID-based signature with batch verification. 2004. http://eprint.iacr.org/2004/131
[35] Shamir A. How to share a secret. Communications of the ACM, 1979,24:612−613.
[36] Oliveira R, Zhang B, Zhang L. Observing the evolution of Internet AS topology. In: Proc. of the ACM SIGCOMM. 2007. 313−324.
[37] McDaniel P, Aiello W, Butler K, Ioannidis J. Origin authentication in interdomain routing. Computer Networks: The Int'l Journal of Computer and Telecommunications Networking, 2006,50(16):2953−2980.
[38] http://www.routeviews.org/, 2007.
[39] The SSFNET project. 2007. http://www.ssfnet.org
[40] Paulo SL, Berreto M. A note on efficient computation of cube roots in characteristic 3. 2004. http://eprint.iacr.org/2004/305
[41] Zhao M, Smith SW, Nicol D. Aggregated path authentication for efficient BGP security. In: Atluri V, ed. Proc. of the ACM CCS 2005. Washington: ACM Press, 2005. 128−138.
[42] Subramanian L, Caesar M, Ee CT, Handley M, Mao M, Shenker S, Stoica I. HLP: A next generation interdomain routing potocol. In: Roch G, ed. Proc. of the ACM SIGCOMM. Washington: ACM Press, 2005. 13−24.

王娜(1980－),女,河南济源人,博士生,讲师,主要研究领域为网络路由及安全技术.

智英建(1978－),男,博士生,主要研究领域为流媒体技术.

张建辉(1978－),男,博士生,讲师,主要研究领域为网络路由技术.

程东年(1957－),男,博士,教授,主要研究领域为宽带信息网络体系结构,网络安全协议,网络性能分析技术.

汪斌强(1963－),男,博士,教授,博士生导师,主要研究领域为宽带信息网络.