International Journal of Recent Trends in Engineering, Vol 2, No. 2, November 2009

Performance Analysis of BGP Security Proposals

Hiren B. Patel
Department of Computer Engineering
S.P.College of Engineering,
Visnagar, India - 384315
hbpatel1976@yahoo.com

Dr. Dhiren. R. Patel
Department of Computer Engineering
S.V.National Institute of Technology,
Surat, India - 395007
dhiren29p@gmail.com

***Abstract* - Border Gateway Protocol (BGP), the only standard for interdomain routing in the Internet, is used to exchange information between Autonomous Systems (ASes). BGP possesses many security vulnerabilities, as it works with the information received from the neighboring routers, and neighbors can lie, deliberately or mistakenly. Many security approaches have been proposed, but due to reasons like increase in performance overhead, problems in real-world deployment etc, none of them have been adopted as a universal solution so far. In this paper, we discuss and analyze performance of many recently proposed security approaches for BGP and their deployment issues that keep them away from real-time implementation. We also suggest recommendations to reduce processing overheads and to maintain performance vs. security tradeoff.**

***Index Terms* – Border Gateway Protocol, BGP, BGP security, Interdomain routing security, routing, Performance Vs. Security tradeoff.**

I. INTRODUCTION

To establish and maintain routing information between Internet domains (Autonomous Systems), the Border Gateway Protocol (BGP) [19] is the standard and only approach available today. BGP works on the principle of word of mouth i.e. each BGP speaker listens and tells others what it has heard from other speakers. This introduces serious security threats, since a nasty (misconfigured or compromised) speaker can forge claims that will then be extended throughout the network, resulting corruption in routing. Many solutions have been proposed to deal with these BGP vulnerabilities. Few of them make use of public key cryptography, digital signatures, hashing etc. to deal with security problems. But these techniques result into overhead in terms of processing, storage, bandwidth etc. that in turn stop them to be adopted as real-time deployable solutions. Due to interests in both cryptographic techniques and Inter-networking, we explore these issues. We have undergone many recently proposed approaches on securing BGP, and analyzed their performance and security trade-offs. This paper presents an overview of this work. We then conclude with some paths for future work.

The rest of the paper is organized as follows. Section 2 gives an overview of recently proposed BGP security approaches followed by performance comparisons and analysis of few of the proposals in section 3. In section 4 recommendations to improve the BGP security are discussed. We conclude and leave with the future scope of the work in section 5 followed by list of references used in section 6.

II. BGP SECURITY PROPOSALS

Before we move on to the security proposals, let us first find out the goals that we want to achieve. Attacks on BGP can broadly be classified into two categories. (i) Inside attacks and (ii) Outside attacks, which in turn be categorized as: (a) AS Number Authentication (b) BGP Speaker Authentication (c) Data Integrity (d) Prefix Origin Verification (e) AS PATH verification. Based on these five goals, we now discuss recently proposed BGP security approaches, along with their operational features, security considerations, scalability and deployment issues.

Secure Border Gateway Protocol (S-BGP) [1] architecture employs three security mechanisms: Public Key Infrastructure (PKI) to support the authentication of ownership, digital signatures covering the routing information and IPsec to provide data and partial sequence integrity. It uses hierarchical distribution of certificates from root to leaves. It is probably the most secure approach proposed so far as it provides Strong guarantee of prefix origin verification and AS_PATH integrity. It is complex, unscalable and computationally expensive to deploy. *Securing BGP Through Secure Origin BGP (soBGP)* [4] uses link state approach to validate routes, web of trust model for authenticating ASes public keys, hierarchical structures for verifying IP prefix ownership and out of band distribution mechanism for root public key certificates. The Deployment Issues is can any entity other than ICANN be trusted for signing ASes public key certificates? *Pretty Secure BGP (psBGP)* [7] uses Centralized trust model for authenticating AS numbers and decentralized trust model for verifying IP prefix ownership. It defends against threats from uncoordinated, misconfigured or malicious BGP speaker in a practical way. It does not require change to BGP protocol and does not require all ASes to adopt it. Following table 1 compares S-BGP, soBGP and psBGP with respect to goals discussed above. In *Working Around BGP: An Incremental Approach to Improving Security and Accuracy of Interdomain Routing* [2], each AS maintains the portion of the registry containing its peering and policy information. It uses dedicated Interdomain Route Validation (IRV) servers (per AS), which communicate via querying one another for routing information. As the IRV queries are transported directly over a secure

transport, it does not incur the signature costs. It is posited that IRV can be deployed in an incremental manner with modest changes to existing router software. Following table 2 shows summary of interdomain routing security.

TABLE 1
BGP Security Goals Comparison of S-BGP, soBGP and psBGP

Goal	S-BGP	SoBGP	psBGP
AS Number Authentication	Centralized (Multiple Level)	Decentralized (with trust transitivity)	Centralized (depth=1)
BGP Speaker Authentication	One Certificate per BGP Speaker	One Certificate per AS	One Certificate per AS
Data Integrity	IPSec or TCP MD5	IPSec or TCP MD5	IPSec or TCP MD5
Prefix Origination Verification	Centralized (Multiple level)	Centralized (Multiple level)	Decentralized (No trust transitivity)
AS_PATH verification	Integrity	Plausibility	Integrity

Efficient Security for BGP Route Announcements [3] uses the structure of BGP processing to design optimizations that reduce cryptographic overhead by amortizing the cost of private-key signatures (Signature-Amortization) over many messages. Without affecting security, this proposal tries to improve convergence time. It is incrementally deployable.

TABLE 2
Summary of Interdomain Routing Security Efforts

	Hop Integrity	Origin Authentication	Path Validation
S-BGP	Yes	Yes	Yes
IRV	Yes	Yes	Yes
soBGP	No	Yes	Yes

Listen and Whisper: Security Mechanisms for BGP [5] does not rely on a PKI. It alerts network administrators in case of routing inconsistencies are found. Whisper deals with control plane anomalies, including propagating false AS origin information or a fake path. Listen alerts in case of data plane attacks such as inconsistent route advertisements. *SPV: Secure Path Vector Routing for Securing BGP* [6] uses symmetric cryptographic technique to protect ASPATH in contrast with computationally expensive asymmetric cryptography. It requires special purpose hardware. It assumes that multiple conspiring ASes cannot mount coordinated attack. It also assumes that the links between any two ASes are private and authenticated. Due to these security considerations, it is unsafe for deployment. In *Securing BGP through Keychain-based Signatures* [8], the keys used for signature generation and verification form a chain by themselves, resulting in a strong tie between signatures (RSA or Merkle hash tree) that may assist in incremental deployment. It provides strong incremental benefits for partially deployment over the Internet (See table 3). *Pretty Good BGP: Improving BGP by Cautiously Adopting Routes* [9] shows that delaying the acceptance of new routes is a safe and effective method for reducing the spread of bogus routes. Authors claim PGBGP to be incrementally deployable.

Table 3
Comparing S-BGP, SPV and Keychain based mechanisms

	Inc. Benefit	Speed	Memory Usage
S-BGP	Weak	Lowest	Larger
SPV	Strong	13 X	Larger
Keychain-based	Strong	Faster	Smaller

In *Using External Security Monitors to Secure BGP* [13], an External Security Monitor (ESM, additional host) is introduced that checks each message sent by a legacy host against a safety specification. This scheme does not require any modification to existing hardware or software. Virtual ESMs can be created for targets not monitored directly, which enable the deployment of N-BGP at only a subset of routers to secure a larger set of hosts. It is difficult to convince network operator community for an extra hardware. The authors of *Securing BGP Incrementally* [14] believe that the security benefit is determined by calculating the fraction of ASes, which either accept a route containing the malicious ASes or whose routing tables do not contain any route to the prefix of the victim. There are two factors leading to performance improvement. First, high degree ASes learn many paths, so they often have at least one valid path. Second, if a high degree AS picks a good route, that route is propagated to many nonparticipating ASes. *Symmetric Key Approaches to Securing BGP – A Little Bit Trust is Enough* [15] is based on two assumptions, first, reducing the number of path validation costs and second, reducing the cost of each path validation. Two approaches have been proposed. First involving centralized (symmetric) keys management in which trusted servers are required to distribute the keys. Second involving distributed (symmetric) keys management, which is initiated by senders. Authors claim that the schemes are flexible and scalable which makes their deployment feasible. The authors of *Secure Interdomain Routing Registry* [16] present a centralized repository built using identity-based cryptosystem with authorized and verifiable search (RAVS) to construct secure routing information. Search permission generator-SPG (a trusted third party) similar to the private key generator (PKG) in the identity-based cryptosystem is introduced to obtain permissions for searching the registry. The approach does not modify the BGP code and the routing message format resulting in more deployable than previous approaches. The authors claim he method to be incrementally deployed in the Internet.

III. PERFORMANCE ANALYSIS

This section shows comparison of some of the proposals discussed above and analyze them with respect to criterion such as processing, transmission bandwidth and storage requirement.

Securing BGP Through Secure Origin BGP (soBGP) [4] reduces the cost of signature verification by verifying the long standing information such as address ownership, organizational relationships and topology.] As claimed by authors of *Symmetric Key Approaches to Securing BGP – A Little Bit Trust is Enough* [15], the

following table 5 shows improvements in case of signature generation and signature verification compared to S-BGP and SPV for centralized key distribution and distributed key distribution.

Table 5: Improved Signature generation and verification compared to S-BGP and SPV

Key Distribution	**Signature**	**S-BGP**	**SPV**
Centralized	Generation	NA	42% Improved
	Verification	98% Improved	96% Improved
Distributed	Generation	Same	90% Improved
	Verification	98% Improved	95% Improved

Table 6 shows that cost of signing and verifying BGP messages with two versions of Keychain-based signature schemes (KC-RSA and KC-MT) in [8]. Also average and maximum delay is illustrated (Table 7). Memory consumption while signing messages is also reduced when compared to S-BGP and SPV security proposals. (Table 8)

Table 6: Speed Of Individual Operations (in µs)

Operations	S-BGP	SPV	KC-RSA	KC-MT
Sign	3802	703	800	90
Verify	4607	191	350	111

Table 7: Delay In Normal Traffic (in s)

Proposals	Delay (s) (avg/max)
S-BGP	0.600 / 3.201
SPV	0.038 / 0.215
KC-RSA	0.183 / 1.038
KC-MT	0.015 / 0.088

Table 8: Memory Consumption Of Signatures (in MB)

ASN	RIB	ASPATH	S-BGP	SPV	KC-RSA	KC-MT
1221	211721	3.555	28.7	253	25.8	152.5
4637	163918	3.356	21	185	20	111.5
7660	167288	4.46	28.5	250.8	20.4	151.2

IV. CONCLUSIONS AND FUTURE WORK

A number of proposals have been devised to address BGP vulnerabilities. However, their performance under security constraints affects BGP's behavior and the limitations of routing equipments to actually adopt them. In this paper we have studied many of the recently proposed BGP security protocols and examined their performance issues.

It is hard to analyze time and memory consumption requirements of BGP either with mathematics or with simulation. Efforts need to be put for applying more efficient cryptographic operations to improve performance in terms of convergence time, message size, or storage costs. Besides signature-based schemes, there are a number of proposals that use database and other techniques intensively. In future, with the help of large scale simulations, many of these discussed techniques can be compared with various criterion, and the simulation results can be used to formulate a novel (may be hybrid) method which not only take care of BGP vulnerabilities but also deal with deployment issues.

V. REFERENCES

[1] S. Kent, C. Lynn, and K. Seo. "Secure Border Gateway Protocol (Secure-BGP)". IEEE Journal on Selected Areas in Communications, 18(4):582–592, April 2000.
[2] G.Goodell,W.Aiello, T.Griffin,J. Ioannidis, P. McDaniel and A. Rubin. "Working Around BGP: An Incremental Approach to Improving Security and Accuracy of Interdomain Routing".2002.
[3] D. Nicol, S. Smith and M Zhao. "Efficient Security for BGP Route Announcements". May-2003.
[4] R. White, "Securing BGP through secure origin BGP," Internet Protocol J., vol. 6, no. 3, pp. 15–22, Sep. 2003.
[5] L. Subramanian, V. Roth, I. Stoica, S. Shenker, and R. H. Katz, "Listen and whisper: Security mechanisms for BGP," presented at the USENIX Symp. Networked Systems Design Implementation, Mar. 2004.
[6] C. Hu, A. Perrig, and M. Sirbu, "SPV: Secure path vector routing for securing BGP," in Proc. ACM SIGCOMM, pp. 179–192, Aug. 2004.
[7] T. Wan, E. Kranakis, and P. C. v. Oorschot, "Pretty secure BGP (psBGP)," presented at the Network and Distributed System Security Symp., Feb. 2005.
[8] H. Yin, B. Sheng, H. Wang and J. Pan. "Securing BGP through Keychain-based Signatures", 2006.
[9] T. Wan, E. Kranakis, and P. C. v. Oorschot, "Pretty secure BGP (psBGP)," presented at the Network and Distributed System Security Symp., Feb. 2005.
[10] G. Huston. "Measures of Self-Similarity of BGP Updates and Implications for Securing BGP". Passive and Active Measurement Workshop, April 2007.
[11] S. Kodeswaran, P.Kodeswaran, A.Joshi and F.Perich. "Utilizing Semantic Policies for Managing BGP Route Dissemination" 2007.
[12] Z. Zhang, Y. Zhang, Y. Hu and Z. Mao. "Practical Defenses Against BGP Prefix Hijacking". CoNEXT'07, New York, NY, U.S.A., December-2007.
[13] P. Reynolds, O. Kennedy, E. Sirer, F. Schneider. "Using External Security Monitors to Secure BGP". 2007.
[14] M. Suchara, I. Avramopoulos and J. Rexford. "Securing BGP Incrementally". CoNEXT'07, New York, U.S.A., Dec-2007.
[15] B. Bruhadeshwar, S. Kulkarni, A. Liu. "Symmetric Key Approaches to Securing BGP – A Little Bit Trust is Enough". 2008.
[16] E.Kim, L.Xiao, K.Nahrstedt and K. Park. "Secure Interdomain Routing Registry." IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 3, NO. 2, JUNE 2008.
[17] K. Al-Saud, H. Tahir, M. Saleh and M. Saleh. "Impact of MD5 Authentication on Routing Traffic for the Case of: EIGRP, RIPv2 and OSPF". Journal of Computer Science 4 (9): 721-728, ISSN 1549-3636, 2008.
[18] T. Farley, P. McDaniel, K. Butler, "A Survey of BGP Security Issues and Solutions", in ACM Journal, 2004.
[19] Y. Rekhter and T. Li, "A border gateway protocol 4 (BGP-4)", RFC 1771, Mar. 1995.
[20] R. Kuhn, K. Sriram, D. Montgomery, "Border Gateway Protocol Security", National Institute of Standards and Technology. Special publication 800-54. July 2007.