Security in Border Gateway Protocol (BGP)

Chapter · December 2014

DOI: 10.4018/978-1-4666-5888-2.ch682

1 author:

Suvradip Chakraborty
Indian Institute of Technology Madras
17 PUBLICATIONS **29** CITATIONS

Encyclopedia of Information Science and Technology, Third Edition

Mehdi Khosrow-Pour
Information Resources Management Association, USA

A volume in the

Information Science REFERENCE
An Imprint of IGI Global

Managing Director:	Lindsay Johnston
Production Editor:	Jennifer Yoder & Christina Henning
Development Editor:	Austin DeMarco & Jan Travers
Acquisitions Editor:	Kayla Wolfe
Typesetter:	Mike Brehm, John Crodian, Lisandro Gonzalez, Deanna Zombro
Cover Design:	Jason Mull

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Encyclopedia of information science and technology / Mehdi Khosrow-Pour, editor.
pages cm
Includes bibliographical references and index.
ISBN 978-1-4666-5888-2 (hardcover) -- ISBN 978-1-4666-5889-9 (ebook) -- ISBN 978-1-4666-5891-2 (print & perpetual access) 1. Information science--Encyclopedias. 2. Information technology--Encyclopedias. I. Khosrow-Pour, Mehdi, 1951-
Z1006.E566 2015
020.3--dc23

2014017131

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book is new, previously-unpublished material. The views expressed in this book are those of the authors, but not necessarily of the publisher.

For electronic access to this publication, please contact: eresources@igi-global.com.

Security in Border Gateway Protocol (BGP)

Suvradip Chakraborty
Jadavpur University, India

Bhaskar Sardar
Jadavpur University, India

INTRODUCTION

Border Gateway Protocol (BGP) is a dynamic routing protocol that routes inter domain traffic, connecting Autonomous Systems (AS's) to form the decentralized backbone of the Internet (Rekhter, et. al., 2006). BGP provides reachability information to the ASs and disseminates external information internally within an AS. With the exponential growth of ASs, BGP has become one of the most critical components of the Internet's infrastructure. Unfortunately, the limited guarantees provided by BGP sometimes contribute to serious instability and outages. While many routing failures have limited impact and scope, others may lead to significant and widespread damage. Most of the risk to BGP comes from accidental failures, but there is also a significant risk that attackers could disable parts or all of network, disrupting communications, commerce, and possibly putting lives and property in danger. BGP's mutual trust model involves no explicit presentation of credentials, no propagation of instruments of authority, nor any reliable means of verifying the authenticity of the information being propagated through the routing system. Hostile attackers can attack the network by exploiting this trust model in inter domain routing to meet their own ends (Butler et. al, 2010). For example, on May 2005, an AS falsely claimed to originate Google's prefix and parts of the internet could not reach Google's search engine for roughly an hour as traffic was misdirected to the attacking AS. This article focuses on the various kinds of attacks on BGP and studies the solutions both in use and proposed to overcome the security vulnerabilities of BGP and discusses the open research issues. The next section provides background information on inter-domain routing and BGP. Subsequent sections focus on the security issues and attacks on BGP and their countermeasures.

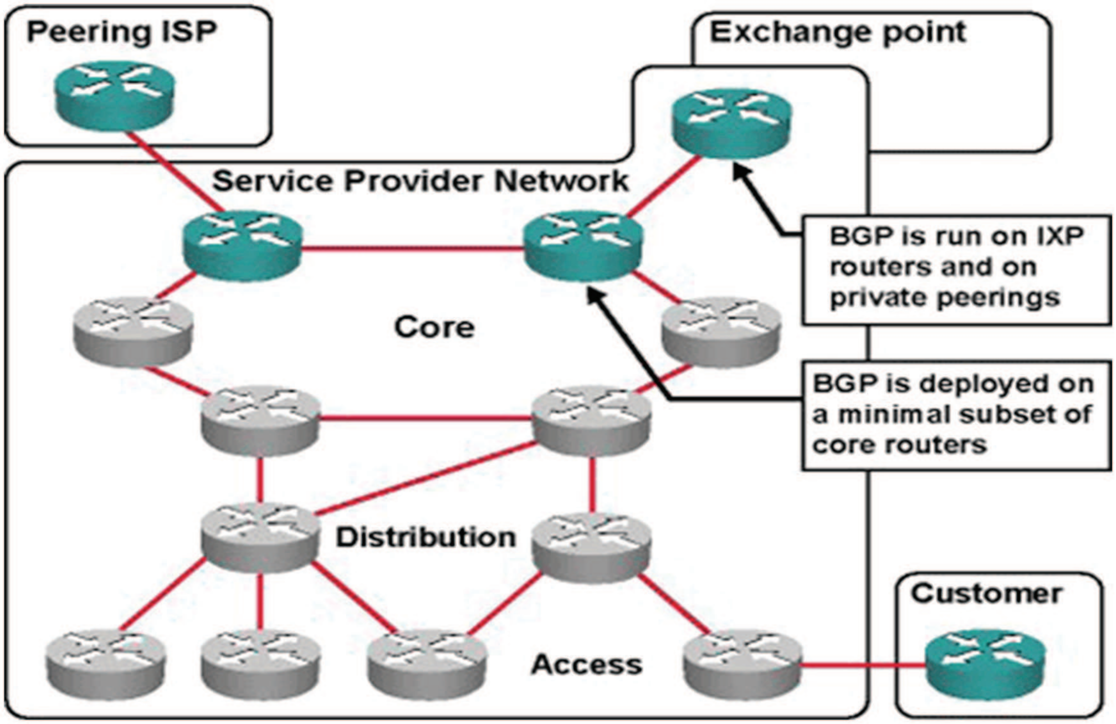
BACKGROUND

The Internet is composed of large number of ASs, which relay traffic to each other on behalf of their customers. The process of routing within an AS is called *intra-domain routing* which is mainly carried out by the Interior Gateway Protocols (IGPs), while routing among the ASs is called *inter domain routing*. BGP is the de-facto interdomain routing protocol that uses *path vector* form of distance vector routing algorithm. All major ISPs use BGP to distribute global routing information, internally and between each other. Figure 1 shows the connectivity model of BGP.

BGP neighbors, called *peers*, are established by manual configuration between routers to create a TCP session on port 179. TCP adds reliability and flexibility to BGP. Once the TCP connection is established between the peers, OPEN messages are exchanged by which BGP speakers can negotiate optional capabilities of the session, including multiprotocol extensions and various recovery modes. Once the OPEN message is acknowledged by the peer router, UPDATE messages are used to exchange reachability information. The other BGP messages include NOTIFICATION message which is sent by a router to indicate the termination of a BGP peering session, ROUTE REFRESH message that is sent to request a retransmission of routing information. A BGP speaker sends 19-byte KEEP-ALIVE message every 30 seconds to maintain the connection. Each BGP route object is a prefix and a set of attributes: <ASPath vector, Origin, Next Hop, Local Preference, Atomic Aggregate…>. One of the most critical attribute for BGP is *ASPath* which is an

DOI: 10.4018/978-1-4666-5888-2.ch682

Figure 1. Border Gateway Protocol (BGP)


Peering ISP
Exchange point
Service Provider Network
Core
BGP is run on IXP routers and on private peerings
BGP is deployed on a minimal subset of core routers
Distribution
Customer
Access

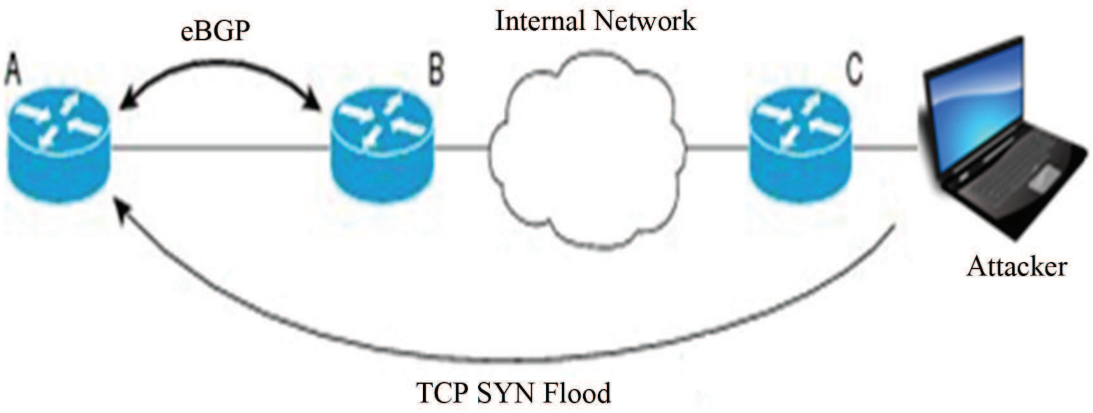
ordered enumeration of AS values that form the path of ASs from the origin AS to the current AS across all possible paths. The originating AS adds it's AS number to the ASPath at first. Each of the transit AS, which imports the route, appends its own AS number to the ASPath before advertising the route to its peers. When a BGP speaker is presented with multiple paths to the same address prefix from a number of peers, the BGP speaker selects the *"best"* path to use which can be influenced by a number of factors and attributes- both *mandatory* which includes shortest ASPath, next hop attributes and *discretionary* (optional) such as local preference, community attribute, atomic aggregate, multi-exit discriminator etc.

BGP SECURITY ISSUES AND THREAT MODEL

BGP does not gaurantee security and privacy of routing traffic. The flaws of BGP have contributed to several major Internet outages. These problems are likely to get worse because cyber warriors, criminals, and even script kiddies have the potential to exploit BGP to deny service, sniff communications, misroute traffic to malicious networks, map network topologies, and trigger network instabilities. The numbers of attacks against BGP are on the rise. A recent attack was targeted against Spamhaus, an organization based in Switzerland responsible for maintaining IP addresses, which is reportedly the largest distributed denial of service attack in the history which saw 300 Gbps of traffic related to this attack.

BGP does not protect integrity, freshness, and origin authentication of messages. It neither validates an AS's authority to announce reachability information nor it ensures the authenticity of path attributes announced by an AS. There are no mechanisms in verifying correctness of routing information. The attacks on BGP can be categorized into the following categories:

Figure 2. TCP SYN Flood Attack



Peer-Peer Attacks

BGP uses TCP as the underlying transport protocol for reliability and flexibility. So, all the attacks that are applicable to TCP also apply to BGP. These include *TCP SYN Flooding* attack where the attacker sends a flood of SYN packets to the other end of the connection (victim) without completing the three-way handshaking mechanism (Figure 2). As a result, the victim is left with too many half open TCP connections and it will run out of connection state memory and will become unable to process legitimate TCP connections resulting in *Denial of Service* attacks where the victim exhausts its processing cycle and memory crashing altogether. Also the BGP peers are vulnerable to *TCP RESET* attacks. If an attacker can eavesdrop the communication between the BGP peers and guess the TCP sequence number that fits the sequence window, he/she can easily send a forged RESET message to the victim. When a RESET is received, the target router drops the BGP session with its peer and both the peers withdraws all the routes learned from each other until recovery takes place which requires manual intervention of the system administrators which may take several minutes to hours, depending on the number of BGP peers affected.

Session Hijacking

In this attack, the attacker masquerades as one of the legitimate BGP peer in a BGP session. The attacker needs to know the source IP address, source port and TCP sequence number. By masquerading as the legitimate BGP peer, the attacker can cause route modification, black hole the traffic or may perform traffic analysis to get hold of private information such as credit card numbers, bank account numbers etc.

Large Scale Routing Attacks

Routing attacks widens the attack domain for the attacker by allowing the attacker to attack the protocol contents and routing infrastructure as a whole.

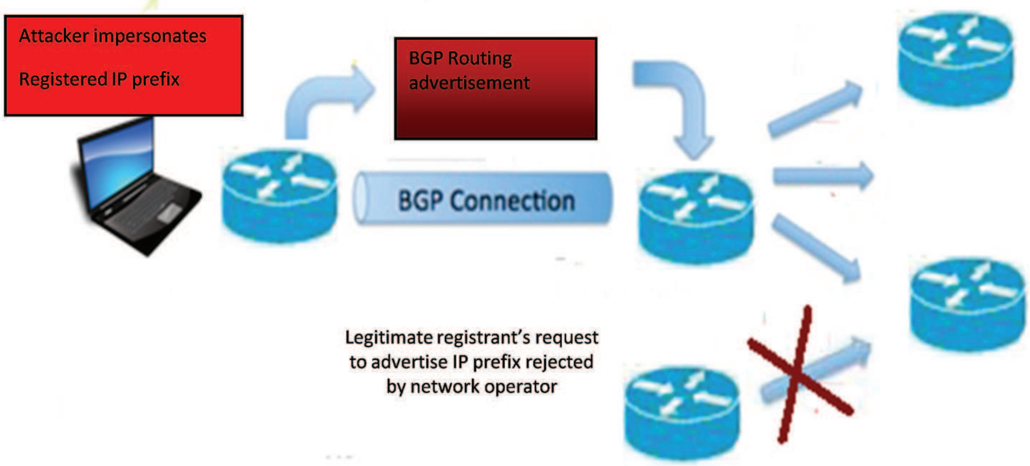
Route Flapping Attack

A "*route flap*" occurs when a route is withdrawn and then re-advertised. When a TCP RESET or TCP SYN flood attack takes place, the victim router goes offline and all its peer routers withdraws all the routes learned from it. However, when the router comes back online, its routing table is recreated and it re-advertises all its routes to its peers. If these series of events continue, the routes advertised by it will disappear and reappear in peer routing tables. This is called *route flapping* and is detrimental to all routers as it not only consumes processing and bandwidth resources but also causes repeated disruptions in connectivity leading to denial of service attacks.

Prefix or Route Hijacking

BGP does not guarantee origin authentication. So an AS can falsely claim to be the legitimate owner of an IP prefix and can advertise the prefix to launch *prefix*

Figure 3. Prefix hijacking


Attacker impersonates
Registered IP prefix
BGP Routing advertisement
BGP Connection
Legitimate registrant's request to advertise IP prefix rejected by network operator

hijacking attack as shown in Figure 3. The concept of BGP prefix hijacking revolves around locating an ISP that is not filtering advertisements (intentionally or otherwise) or locating an ISP whose internal or ISP-to-ISP BGP session is susceptible to a *man-in-the-middle* attack. Once located, an attacker can potentially advertise any prefix they want, causing some or all traffic to be diverted towards the attacker for traffic analysis or manipulation. For example, the famous YouTube's prefix hijack (February 2008) by Pakistan Telecom, black-holed the YouTube's website for more than 2 hours.

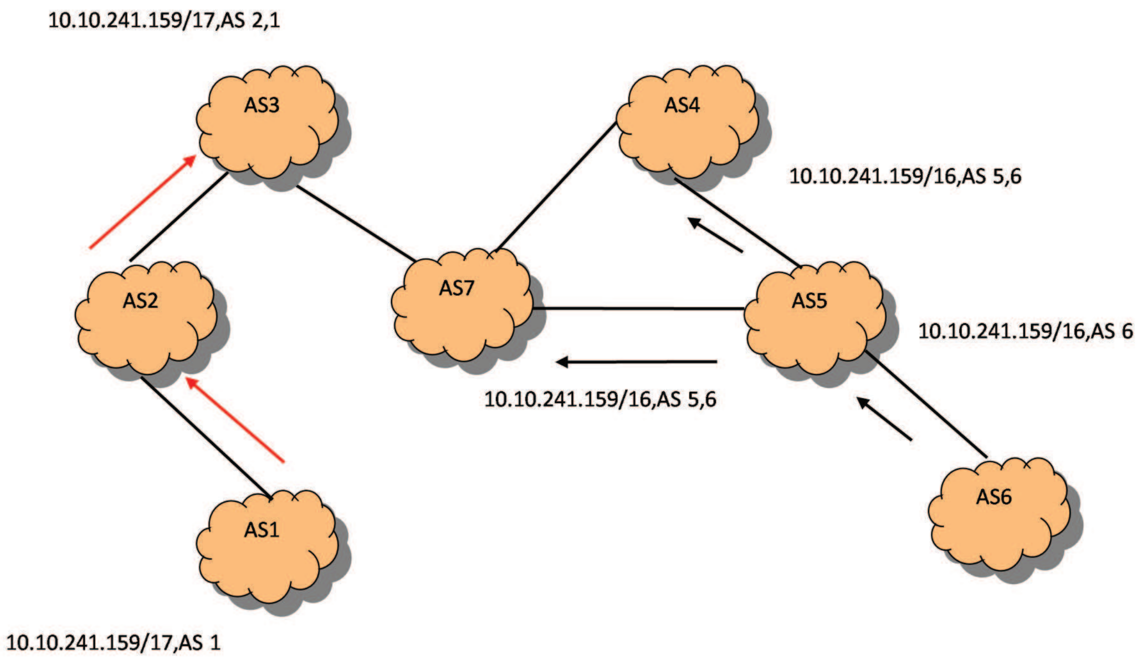
Route Deaggregation

BGP gives preference to more specific prefixes i.e. having longest subnet mask. So if a BGP peer receives a more specific prefix than those in its routing table, it will update its routing table with the more specific prefix and in turn will advertise this learned route to its peers and this advertisement propagates till the destination is reached. While this is normal in some situation, for a router to advertise a more specific prefix due to configuration changes, this can also be caused by router misconfigurations or deliberately advertised by an attacker who is in control of the BGP speaker. It is more powerful than prefix hijacking, as it does not conflict with a legitimate prefix, but is the preferred routing decision, so it can trick the entire Internet. In Figure 4, AS1 announces a more specific prefix 10.10.241.159/17, and so it is preferred over 10.10.241.159/16 which is announced by AS6. For example, such a case of route deaggregation happened in April 1997, when a misconfigured router maintained by a small ISP in Florida injected incorrect routing information into the global Internet claiming to have optimal connectivity to all Internet destinations. As a result, most of the Internet traffic was routed to this ISP leading to network congestion and effectively crippled the Internet for about two hours.

Malicious Route Modification Attacks

An attacker can deliberately tamper with the route attributes in the UPDATE messages to cause all possible route modification attacks. For example, the attacker can intentionally *insert* false AS numbers into the ASPath to make the path longer and hence less attractive to the other ASs so that the path does not get selected (*route injection attack).* A particular variety of route injection attack involves transmission of routes to unallocated prefixes (i.e. private or reserved IP address spaces) called *bogons* or *martians (unallocated route injection attack).* The attacker instead of claiming to originate a prefix can keep the correct originator but shorten the ASPath by *deleting* some of the AS numbers from the ASPath resulting in *ASPath shortening or Route deletion attacks* and since in the absence of any local policy directive a BGP speaker favours a shorter path than other contending routes so it is likely that the traffic will be directed to the attackers network. The attacker can then drop all the traffic

Figure 4. Prefix deaggregation



(*black holing*), modify or eavesdrop the traffic and send it to its legitimate destination (*Path Subversion attack*) or can perform traffic analysis to gain knowledge of private information thereby acting as a *man-in-the-middle*. The attacker can also intentionally insert the AS numbers of the downstream ASs to create *routing loops*. As a result, the packets keep on circulating within the network resulting in unnecessary bandwidth consumption and amplification of traffic increasing the network load. Lastly, the attacker can launch a *replay attack* where the attacker simply relays the legitimate announcements of the BGP speakers at a later stage causing route withdrawals and re-assertions resulting in *routing instabilities.*

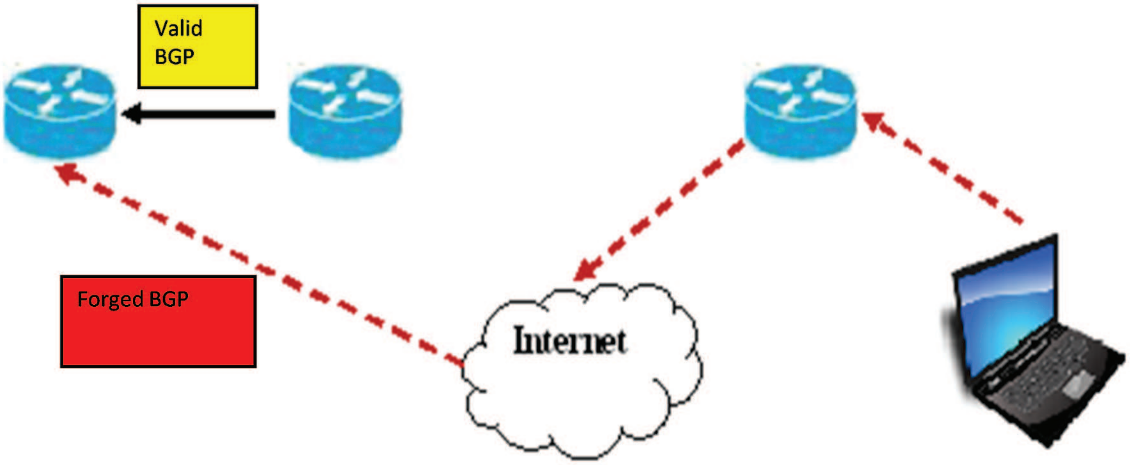
Physical and Link Cutting Attacks

Vulnerabilities in the network infrastructure itself are particularly problematic. Physical attacks on the routing infrastructure may also take place due to power failure, environmental failure in the data centers or a link going down. Link failure may also be caused by link cutting attack. This can be done by both physically attacking a link called *backhoe attack* or the attacker may swamp a link by sending unnecessary traffic causing *congestion*-induced *BGP session failure* and significant routing convergence delays.

BGP Security Solutions and Countermeasures

BGP is a good example of an insecure routing protocol, despite inclusion of few security features and ad hoc efforts by ISPs & vendors. In the current Internet, the possibility of BGP attacks and misconfigurations has been so far mostly dealt with *Best Common Practice* documents from router vendors. These documents typically recommend practical measures to prevent a router from being hijacked, and to avoid fake or incorrect advertisements from being accepted by a router. Some of the documents adopted as a temporary fix to the security problems of BGP are discussed in this section.

Figure 5. The Generalized TTL Security Mechanism



BGP TTL Security Hack (BTSH) or Generalized TTL Security Mechanism (GTSM)

BTSH or GTSM is a technique which utilizes a check on the Time-To-Live (TTL) field of the IP header to protect against attackers single hop away from the victim without controlling either of the BGP speakers. Routers utilizing this mechanism set the TTL field in the IP header to a maximum value of 255. A BGP speaker receiving a packet from its peer monitors the TTL field to see if the value of this field is 254. If it is as intended it assumes that the packet came from the legitimate host. This is illustrated in Figure 5. However, this mechanism is ineffective in case of multihop path between the peers. Moreover, if an attacker can tunnel the intended packet within another IP packet, its TTL value will not change. In that case it will be able to evade GTSM.

TCP MD5 Signature Option

This mechanism can be used to protect the TCP connection between two BGP peers. Message Digest 5 (MD5) is used to protect the integrity of the TCP sessions from TCP SYN flooding and TCP RST attacks. The MD5 digest can only be created by the legitimate owner of the secret key used to create the one way hash. However, this mechanism does not enforce confidentiality of the exchanged messages. Besides, this mechanism assumes that the keys are already distributed apriori between the peers which is not always a realistic assumption because of the privacy involved in key exchange phenomenon.

Route Filtering

Routers can be configured Route Filtering to prevent improper updates of the routing database and propagation of routing information. Many ISPs rely on local policy filters to protect them against configuration errors. UPDATEs originating from an AS pass through *egress filters* allowing operators to filter outgoing prefixes. *Ingress Filtering,* on the other hand, is used to filter the UPDATEs by checking that incoming packets are actually from the networks that they claim to be from by examining the source IP address. However, creating and maintaining such filters is difficult, time consuming, and error prone as the Regional Registries (IRR) databases are not always up-to-date and the ISPs also don't query them too often.

Route Flap Dampening

Route Flap Dampening is a mechanism to minimize the instability caused by route flapping and oscillation over the network. If a router is involved in a route flap it gets a penalty for each flap. Once the cumulative penalty reaches a predefined "suppress−limit", the advertisement of the route will be suppressed. The penalty will be exponentially decayed based on a preconfigured "half−time" where half time refers to the time for the penalty to decay to its half. Once the penalty decreases below a predefined “reuse−limit”, the route advertisement will be unsuppressed.

Sequence Number Randomization

Sequence numbers provide minimum protection against session hijacking and peer spoofing attacks because an attacker must guess the sequence numbers of the messages to hijack the session. However, this is not always difficult for an expert attacker. An attacker can eavesdrop the messages between the peers for some period of time and come up with some pattern for guessing the sequence numbers fitting within the sequence window. TCP sequence number randomization adds value to security where the choice of the initial sequence number (ISN) should be completely random to prevent the attacker from guessing the ISN correctly.

IPsec

IP Security (IPsec) may also be applied to protect BGP sessions. When configured to operate between routers, tunnel mode will typically be applied. Authentication of BGP sessions can be achieved using either “IP Authentication Header (AH)” or “IP Encapsulating Security Payload (ESP)” with the Null Encryption option.

Other Countermeasures

The first comprehensive protocol that addressed the security issues of BGP came in the form of *Secure BGP (S-BGP)* (Kent et al, 2004). S-BGP adds strong authorization and authentication capabilities to BGP based on Public-Key Infrastructure (P.K.I.) using digital certificates for origin authentication and route verification. S-BGP uses *Address Attestations* to authorize an AS to originate routes advertisements for a particular network prefix and *Route Attestations (RAs)* which an AS creates to authorize a neighbor to advertise prefixes. In S-BGP, certificates are issued to each ISP (or subscriber) that owns (or has the right to use) a portion of the IP address space starting with the *Internet Assigned Numbers Authority* and continuing through a *Regional Internet Registry*, and, if applicable, an ISP. Anyone in possession of the certificate can digitally sign the prefixes advertised by it using its private key which can be easily verified by its downstream neighbors using its public key. Each AS then signs the ASPath using their private keys. The router verifies the signature on each RA and verifies the correspondence between the signer of the RA and the authorization to represent the AS in question. If all of these checks pass, the UPDATE is valid. However, there are several issues that prevent the widespread deployment of this mechanism. S-BGP requires router hardware support with appropriate storage and signature processing capabilities. Route aggregation is another problem for S-BGP as it requires that all UPDATES be signed by the prefix owner. Also S-BGP is vulnerable to *colluding attacks* in presence of two or more compromised routers.

Secure Origin BGP (soBGP) (J. Ng, 2004) was created by the CISCO engineers as a lightweight alternative to S-BGP that provides a trade-off between security and performance. It makes use of three certificates- *Entity Certificate or EntityCert* which addresses the issue of key distribution and ties an AS number to a public key (or a set of public keys) corresponding to a private key the AS uses to sign various other certificates, *Authentication Certificate or AuthCert* which ties an AS to a block of addresses that the AS advertises and *Policy Certificate or PolicyCert* which contain an AuthCert and authenticates per-AS or pre-prefix policies and AS connectivity information, and it is used to verify the validity of a route. So instead of relying on a hierarchical PKI infrastructure, soBGP uses a Web-of-Trust model to validate certificates, relying on the existing relations between ISPs. However, it requires router support and upgradation of software in the supporting devices. Because of so many options soBGP offers to system administrators it gives rise to interoperability challenges. Besides soBGP introduces a new message type in BGP called *SECURITY* message and the certificates used in soBGP are non-standard.

Inter-domain Route Validation (IRV) (Goodell et al., 2003) is used to secure BGP that relies on out-of-band communication with a route originator to verify the correctness of a route. Every AS provides a dedicated server called an *Interdomain Routing Validator (IRV)* to maintain a database of information describing Internet routes and capable of providing authoritative responses relating to prefixes originated by this AS. When a BGP speaker receives a route update from its peer it queries the dedicated IRV of its domain which further queries its upstream IRV server to confirm the validity of the route object. So this mechanism offloads the burden of transmitting the routing information as well as the credentials from the forward path of routing. However, there are a lot of issues and lack of clarity regarding how the IRV response is to be verified. Besides, this mechanism presents problems in bootstrapping and recovery as it is indirectly using the network to query the appropriate IRV server.

Apart from these proposals a lot of other experimental systems and anomaly detection schemes have also been proposed. *Secure Path Vector (SPV)* (Hu et al., 2004) uses symmetric-key cryptography for securing against the truncation and modification attacks. It makes use of *Merkle Hash Trees* and single one way *hash chains* for path validation and is much faster than S-BGP providing tradeoffs between security and CPU usage. *Prefix Hijack Authentication System* (Lad et al, 2006) utilizes a routing database containing BGP route updates to identify IP prefix hijack events. ***i**-SPY* (Zhang et al., 2008) provides a real-time, accurate, light-weight, easily and incrementally deployable victim notification system through lightweight prefix-owner-based active probing from prefix hijack detection. Listen and Whisper is a protocol for control plane and data plane verification. Listen passively probes the data plane and checks whether the underlying routes to different destinations work. Whisper uses cryptographic functions along with routing redundancy to detect bogus route advertisements in the control plane. *AS-CRED* (Chang et al.,2013) is a reputation and alert service for inter-domain routing that not only detects anomalous BGP updates, but also provides a quantitative view of AS' tendencies to perpetrate anomalous behavior. *The Resource Public Key Infrastructure (RPKI)* (Lepinski & Kent, 2012) provides a way for the holders of Internet number resources (that is, IP addresses and AS numbers) to formally demonstrate their right to use these resources, to bind prefix and origin AS information, and for third parties to verify assertions made about these resources. The RPKI uses restricted X.509 v3 certificate profiles, with a number of specially designed extended attributes chosen for routing security purposes. A technique to detect anomalous BGP packets in real time using Failure Quality Control was proposed by Mujtaba et al (2012). Mohapatra et al (2013) proposed a simple validation technique called *BGP prefix Origin Validation* that partially satisfies the requirements of AS origin authentication by relying on a database (RPKI or others) to provide validation information.

FUTURE RESEARCH DIRECTIONS

BGP is becoming increasingly more complex due to incorporation of new features such as *BGP Flow Specification,* support for *Virtual Private Network*, *Multiprotocol BGP (M-BGP)* for IPv6 support. BGP is susceptible to malicious users and core router ownage. GTSM, sequence number randomization, route filtering etc are the current *Best Common Practice* for BGP till any comprehensive security solution is provided that can trade off between security and performance. It is also susceptible to unintentional router misconfigurations which are equivalent to malicious attacks. Most of the solutions provided till date rely on centralized key management techniques and on the implicit assumption of the existence of a global PKI. So attempts are required to provide *decentralized security solutions* for BGP and on efficient *anomaly detection and intrusion detection* schemes. Some of the research directions on BGP also include *traffic engineering* (inbound and outbound traffic control), protecting the routing infrastructure and implementing router based defense against Distributed DOS attacks. The total number of ASs currently supported is about 64,555 which call for *increased scalability requirements* for BGP. Moreover, BGP does not support real-time applications as failure recovery can take minutes to hours. It can get worse due to multihoming. Much of the research focus on overlay networks as to whether they are the answer to BGP's bad performance.

CONCLUSION

BGP is a robust and stable inter-domain routing protocol in the Internet. This article reviewed recent efforts to secure BGP in the Internet. The article focused mainly on the attack strategies and threat model and also discusses the countermeasures and recent proposals to secure BGP. Current research on BGP mainly focuses on resolving both operational and security concerns. Till any comprehensive security mechanism is not deployed, the operators continue to use temporary measures including TCP MD5 signatures, log changes, filtering and limiting the number of prefixes, protecting routes towards route servers and protecting the router infrastructures. Besides efforts are being made to deploy IPSec as a comprehensive security solution for BGP. Any deployable security strategy of BGP should provide high certainty of route validation, low processing overhead on routers and minimal impact on BGP route stabilization.

REFERENCES

Butler, K., Farley, T., McDaniel, P., & Rexford, J. (2010). A survey of BGP Issues and Solutions. *Proceedings of the IEEE*, *98*, 100–122. doi:10.1109/JPROC.2009.2034031

Chang, J., Venkatasubramanian, K. K., Andrew, G. W., Kannan, S., Lee, I., Boon, T. L., & Sokolsky, O. (2013). AS-CRED: Reputation and Alert Services for Inter-domain Routing. *Systems Journal, IEEE*, *7*(3). doi:10.1109/JSYST.2012.2221856

Goodell, G., Aiello, W., Griffin, T., Ioannidis, J., McDaniel, P., & Rubin, A. (2003). Working around BGP: An incremental approach to improving security and accuracy of interdomain routing. In *Proceedings of Network and Distributed System Security Symposium (NDSS)*, 75–85. doi: 10.1.1.20.3884

Hu, Y. C., Perrig, A., & Sirbu, M. (2004). SPV: Secure path vector routing for securing BGP. *ACM SIGCOMM Computer Communication Review*, *34*, 179–192. doi:10.1145/1030194.1015488

Kent, S., Lynn, C., & Seo, K. (2000). Secure Border Gateway Protocol (S-BGP). *IEEE Journal on Selected Areas in Communications*, *18*(4), 582–592. doi:10.1109/49.839934

Lad, M., Massey, D., Pei, D., Wu, Y., Zhang, B., & Zhang, L. (2006). PHAS: A prefix hijack alert system. In *Proceedings of the 15th conference on USENIX Security Symposium* (15).

Lepinski, M., Kent, S. (2012). An infrastructure to Support Secure Internet Routing. *Internet Engineering Task force (IETF), RFC 6480*.

Mohapatra, P., Scudder, J., Ward, D., Bush, R., Austein, R. (2013). BGP Prefix Origin Validation. *Internet Engineering Task Force (IETF), RFC 6811*.

Mujtaba, M., Nanda, P., & He, X. (2012). Border Gateway Protocol Anomaly Detection Using Failure Quality Control Method. In *Proceedings of the IEEE 11th International Conference on Trust, Security and Privacy in Computing* (pp. 1239-1244). doi: 10.1109/Trustcom.2012.100

Ng, J. (2004). *Extensions to BGP to Support Secure Origin BGP (soBGP). Network Working Group*. Internet Draft.

Rekhter, Y., Li, T., & Hares, S. (2006). A Border Gateway Protocol 4 (BGP-4). *Networks Working Group, RFC 4271*.

Zhang, Z., Zhang, Y., Hu, Y. C., Mao, Z. M., & Bush, R. (2010). ISPY: detecting IP prefix hijacking on my own. [TON]. *IEEE/ACM Transactions on Networking*, *18*, 1815–1828. doi:10.1109/TNET.2010.2066284

ADDITIONAL READING

Abuzneid, A., Stark, B. J. (2010). Improving BGP Convergence Time via MRAI Timer. *Novel Algorithms and Techniques in Telecommunications and Networking,* 105-110. doi: 10.1007/978-90-481-3662_9-17

Bellovin, S., & Gansner, E. (2003). Using Link Cuts to Attack Internet Routing. *AT&T Labs research. Draft:* http://www.research.att.com/smb/papers/ index.html.

Christain, R., & Tauber, T. (2007). *BGP Security Requirements*. Routing Protocol Security Requirements, Internet-Draft.

Eddy, W. (2007). TCP SYN Flooding Attacks and Common Mitigations. *Network Working Group, RFC 4987*.

Gill, V., Heasley, J., & Meyer, D., (2004). The Generalized TTL Security Mechanism (GTSM). *Network Working Group, RFC 3682*.

Heffernan, A. (1998). Protection of BGP Sessions via the TCP MD5 Signature Option. *Network Working Group, RFC 2385.*

Huston, G., Rossi, M., Armitage, G. (2011). Securing BGP- A Literature Survey. *IEEE Communication Surveys & Tutorials, 13 (2)*, 1-24. doi: 10.1109/SURV.2011.041010.00041

Kent, S. (2005). IP Authentication Header., *Network Working Group, RFC 4302.*

Kent, S. (2005). IP Encapsulating Security Payload (ESP). in Network Working Group, RFC 4302.

Kent, S., Lynn, C., Mikkelson, J., & Seo, K. (2000). Secure border gateway protocol (S-BGP)-real world performance and deployment issues, in *Proc. ISOC Symposium Network and Distributed System Security (NDSS),* 103–116.

Kent, S., Seo, K. (2005). Security Architecture for the Internet Protocol. *Network Working Group, RFC 4301.*

Kuhn, R., Sriram, K., & Montgomery, D. (2007). Border Gateway Protocol Security: Recommendations of the National Institute of Standards and Technology. *NIST Special Publication 800–54 (BCP document for the team of Telecom Industry and US Government agencies).*

Mahajan, R., Wetherall, D., & Anderson, T. (2002). Understanding BGP Misconfiguration. *In Proceedings of ACM Sigcomm, 32(4),* 3-16. doi: 10.1145/633025.633027

Merkle, R. C. (1980). Protocols for public key cryptosystems. *In IEEE Symposium on Security and Privacy, 0,* 122-133

Meyer, D. (2003). University of Oregon Route Views Project. http://www.routeviews.org/

Montgomery, D., & Murphy, S. (2006). Toward Secure Routing Infrastructures. *IEEE Security and Privacy*, *4*(5), 84–87. doi:10.1109/MSP.2006.135

Murphy, S. (2006). BGP Security Vulnerabilities Analysis. *Network Working Group, RFC 4272.*

NSFOCUS. (2013). *Analysis of DDoS Attacks on Spamhaus and recommended solution*. Beijing, China.

Qiu, S. Y., Monrose, F., Terzis, A., & McDaniel, P. D. (2006). Efficient techniques for detecting false origin advertisements in inter-domain routing. *2nd IEEE workshop on Secure Network Protocols*, 12-19. doi: 10.1109/NPSEC.2006.320341

RIPE. (2008). You Tube Hijacking. A RIPE NCC RIS case study. *web:* http://www.ripe.net/views/study-youtube-hijacking.html.

Smith, B. R., & Garcia-Luna-Aceves, J. J. (1996). Securing the border gateway routing protocol. In Proceedings of Global Internet '96, 81–85.

Villamizar, C., Chandra, R., & Govindan, R. (1998). BGP route flap damping. *Network Working Group, RFC 2439*

Wan, T., Oorschot, P. V., & Kranakis, E. (2007). A selective introduction to border gateway protocol (BGP) security issues. *In Proceedings of NATO Advanced Studies Institute on Network Security and Intrusion Detection.*

Wan, T., & Oorschot, V. P. C. (2005). Analysis of BGP prefix origins during Google's May 2005 outage. *IEEE International Parallel & Distributed processing Symposium, proceedings of the 20th international conference on Parallel and Distributed Processing*, 353-353. doi: 10.1109/IPDPS.2006.1639679

Zhao, M., Smith, S. W., & Nicol, D. M. (2005). The performance impact of BGP security. *IEEE Network*, *19*(6), 42–48. doi:10.1109/MNET.2005.1541720

KEY TERMS AND DEFINITIONS

AS: Autonomous System.

Border Gateway Protocol (BGP): The sole interdomain routing protocol responsible for finding rouing paths between the ASs.

Denial of Service Attack: An attack in which an attacker does not allow the legitimate users to access the required service(s) by disrupting connectivity or creating instabilities.

Interdomain Routing: The process of exchanging routing information between the ASs.

Internet Protocol Security (IPSec): A suite of protocols providing security at the IP layer

Intradomain Routing: The process of exchanging routing information within an AS. The dominant intradomain routing protocols are RIP, OSPF, IS-IS etc.

IP: Internet Protocol.

Message Digest 5 (MD5): A cryptographic one way hash function used for maintaining integrity of the transit messages.

SBGP: Secure BGP.

Transmission Control Protocol (TCP): A transport layer protocol that provides error control and flow control and thus provides reliability and flexibility.