Interdomain Routing Security (BGP-4)

A Comparison between S-BGP and soBGP in tackling security vulnerabilities in the Border Gateway Protocol

By **Rostom Zouaghi** and **Stephen Wolthusen**

Royal Holloway University of London
SearchSecurity.co.UK

THE BORDER GATEWAY PROTOCOL (BGP) is the most important protocol for the interconnectivity of the Internet. Although it has shown acceptable performance, BGP suffers from many security issues. In this article, we cover a few of those issues and provide the security requirements for this protocol. We enumerate a few attacks that can be conducted against BGP. The aim of this study is to examine two solutions that endeavour to provide security mechanisms at the protocol level: Secure-BGP (S-BGP) and secure origin BGP (soBGP). The objective of this article is to compare these protocols in terms of security, efficiency, performance, and deployability. Our findings have revealed that ultimately, the solution chosen will be dependent on the desired level of security and the feasibility of deployment. As is often the case with security, a compromise between security and complexity is a major concern and cost-effectiveness is the main driver behind deployment.

1. INTRODUCTION

The Internet has become a fundamental resource in academic institutions, government agencies and small to large businesses, as well as a vibrant part of our daily lives. The smooth functioning of communication in the Internet relies on routing, which is the component that determines feasible paths (or routes) for data to flow from a source to a destination. Computers on the Internet depend on routing information in order to be able to discover and communicate with each other. Currently, the Internet routing infrastructure is intolerably frail due to many shortcomings. It is commonly misconfigured [1], has considerable weak security properties [2] and becomes hard to manage [3]. As a consequence, communication becomes unreliable and unpredictable.

INTERNET ROUTING OVERVIEW

Although it is generally thought that the Internet is a single network that people connect to; it is actually composed of a large number of interconnected networks that are independently operated, called **Autonomous Systems** (ASes). For instance, when a user browses the Internet, the packets sent and received travel across multiple ASes before reaching their destination.

In the Internet, Exterior Gateway Protocols

(EGPs) are used for routing information exchange. Currently, the Border Gateway Protocol (BGP) is the protocol relied on when it comes to routing infrastructure for the Internet.

In interdomain routing, the trivial parameters required for routing are **Autonomous System Numbers** (ASNs) and **Internet Protocol addresses** (IP). Every AS holds an ASN and one or more IP addresses. Public ASNs and IP addresses are assigned to different regions in the world by the Internet Corporation for Assigned Names and Numbers (ICANN). Owing to the complexity in managing the Internet, ICANN has delegated its authority to registries in different world regions [4].

BGP OVERVIEW

In each AS, one or more routers (or "speakers") are assigned to perform interdomain routing by running BGP software, as shown in FIGURE 1. BGP routers are internally (i.e. inside the AS) linked to other internal routers through Internal-BGP links, and externally linked with routers in different ASes through External-BGP. Routing information is propagated across the whole internetwork. This allows reachability information to be available everywhere, which ensures that every node in the internetwork knows how to reach any other node. Because of the flexibility that BGP provides, route determination and selection structure becomes rather complex.

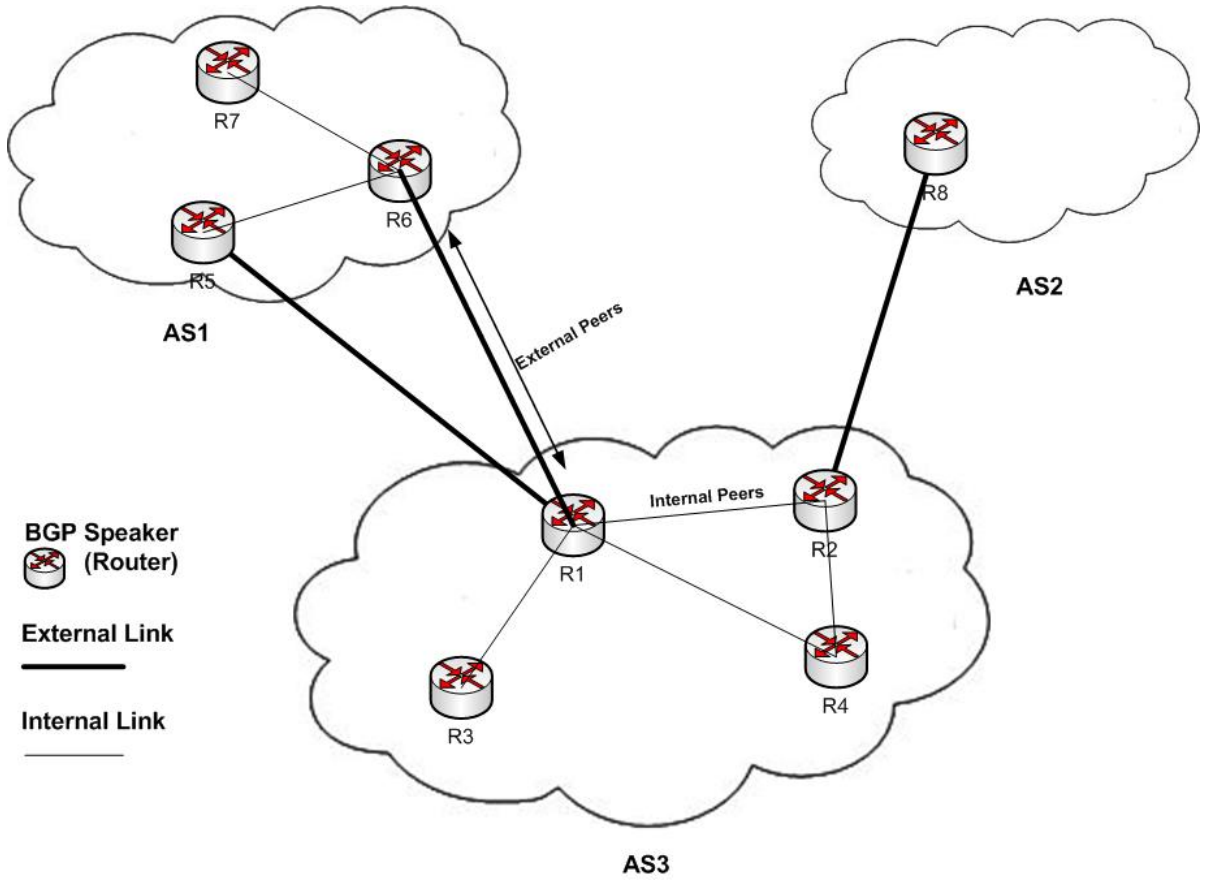
When two routers are configured to talk BGP with each other, they first establish a Transport Control Protocol (TCP) session at port number 179. Knowing the importance of routing information, BGP requires the reliability found in TCP. The latter is a protocol that accomplishes the orderly delivery of messages, detects duplicates, recognises when information has been lost and retransmits it, etc. After establishing the TCP connection, the peers start their communication by exchanging a few specific BGP messages to establish a BGP session. Then, they exchange routing information through **UPDATE** messages

"Routing information is propagated across the whole internetwork. This ensures that every node in the internetwork knows how to reach any other node."

and store it in a database named the Routing Information Base (RIB). Before storing routing information, the latter goes through filters determined by AS's routing policies reflecting not just connectivity but also further considerations such as commercial and security interests. Given that much of this configuration is performed manually, human error is inevitable, leading to a consider-

FIGURE 1

AN EXAMPLE OF A BGP TOPOLOGY



able fraction of BGP announcements being erroneous [5]. A malicious individual can exploit those problems, abetted by a lack of security features as shown below.

2. BGP THREAT ANALYSIS

BGP provides no confidentiality, and only very limited integrity and authentication services. Furthermore, BGP messages can be replayed since they do not use any freshness service. This means that if a malicious individual intercepts an UPDATE message that adds a route, then they can re-send that message after the route has been withdrawn. This causes an invalid route to be present in the RIB.

In addition, no mechanism provides source authentication of messages to BGP speakers. This means that attackers can pretend to be a BGP peer. This could be exploited to inject non-existent routes, routes which send traffic through the attacker's machine, etc.

One of the major issues in BGP is dealing with the quality of routing information transmitted. In other words, the reachability information needs to be trusted. Thus, the announcement of this information needs to be validated by an authoritative AS. However, BGP does not provide an authoritative hierarchy, allowing a malicious or compromised AS to create new non-existent or malicious routes and advertise them. This is further exacerbated by the fact that path attributes cannot be validated through the existing BGP protocol messaging.

ATTACKS

The absence of security controls and safeguards can be exploited to craft attacks against interdomain routing directly or exploited to realise higher-impact malicious goals.

There are several generic attacks that can be performed against interdomain routing. The first one is eavesdropping; which is the interception and reading of BGP messages. BGP does not protect against replay attacks (i.e. recording and resending messages). In addition, there is no protection against message deletion, insertion and modification attacks. An attacker is also able to remove messages between two speakers, modify and resend them back to the receiver. Thus, interdomain routing is weak against man-in-the-middle attacks. A malicious individual is able to corrupt the communication streams between speakers and become an unnoticed and unknown intermediary. Furthermore, it is vulnerable to denial of service (DoS) attacks.

Generally, these attacks can be conducted by exploiting the TCP or BGP messaging vulnerabilities at all levels [6, 7, 8, 9, 10]. Two of the many attacks that exist are briefly described.

BGP Spoofing Attack: In order to communicate with a speaker in an existing BGP session formed by the speaker itself and its legitimate peer, the attacker needs to acquire more information about the session. They must obtain the source IP address of the peer, through the use of Traceroute for instance [11]. Because in a TCP connection a port number is required, it must be spoofed. Furthermore, the attacker is required to use a correct sequence number (i.e. the way TCP keeps track of the order of packets) and TTL (Time To Live) attribute. TTL is a number that represents the maximum number of hops a packet can take; and is used as a safety mechanism to drop the lost packets. Generally, BGP peer sessions are directly connected, so that the TTL is set to 1. The attacker needs to set the TTL accordingly so that it is received when its value is 1. Crafting this attack is not an easy task since it will require extra BGP session knowledge. However, if accomplished, the targeted speaker will think that the message is legitimate and processes it as if it was sent from its peer, allowing e.g. false route injection, route deletion, etc.

"If attackers can discover the IP address of a BGP speaker, its peer, and the ports used for a session, they can spoof the TCP packets."

Setting up an unauthorised BGP session with a peer: Since a TCP session is required for peers to establish a BGP session, BGP inherits all TCP-based attacks. An attacker can use foot printing and reconnaissance techniques to gather information about an AS. If they can discover the IP address of a BGP speaker, its peer, and the ports used for a session, they can spoof the TCP packets with the source IP address and port number of the peer. By making sure that the TTL arrives with a value not greater than 1, they can establish an unauthorised TCP session with the speaker. This attack can lead to adding false routes or retrieving existing ones for example.

ATTACK SCENARIOS

Based on the above generic attacks, an adversary can construct attacks which achieve substantially greater damage.

Disable an AS: An example would be to disable an AS from receiving routing information. This can be done by using any type of Denial of Service attack to disable BGP speakers. This will cause the targeted AS not to know how to route traffic outside it. This means that it will not be able to respond to any request from its users. If the company relies totally on the Internet, then the cost of the impact of the attack would be large.

Disable critical portions in the internet: Since using generic attacks can lead to disabling different ASes, critical portions in the Internet can be targeted. This can be done by injecting false routes into a global internet routing table. This will make the portion of the Internet unreachable because the access to the AS is non-existent (by deleting the routing information from the table) or altered (by changing a few parameters in the routing table).

Blackhole traffic: Blackholing traffic means that all packets routed will be dropped and will not reach their destination. This attack performs better when it remotely targets an ISP for instance that relies on a single upstream ISP. The attacker needs to persuade the peer to route all the traffic to their router. For instance, they can establish an unauthorised BGP session with the target. Then, send UPDATE messages that route all traffic through the attacker's machine. This way, the adversary receives all packets sent from the targeted ISP and drops all of them, while keeping the BGP session live. This creates a blackhole for the ISP's traffic.

DNS attacks: Many attackers aim to corrupt the Domain Name System (DNS) through routing attacks. This might allow, for instance, the attacker to collect personal users' data such as banking information and passwords. After a successful routing attack, a malicious individual can attack the DNS and lure traffic towards a compromised web server for example. When a user uses a service where credentials are required, the attacker can get hold of them [12]. Other more damaging attacks can be conducted using interdomain routing as a proxy. For instance, the attacker can use a BGP-based attack to masquerade as root DNS servers. This provides the attacker with a huge

amount of flexibility and the potential to cause immense damage to the Internet community.

3. BGP SECURITY

The following section provides a high-level overview selection of current and proposed security mechanisms for BGP, but is by no means comprehensive.

CURRENT SECURITY MECHANISMS FOR BGP

Generally, the protection mechanisms used nowadays endeavour to protect TCP or BGP sessions from attacks. Moreover, traffic filtering is used extensively in border routers.

TCP MD5 authentication: Most ISPs use TCP MD5 authentication to protect BGP sessions mostly against message injection. The proposed solution is a mathematical cryptographic one way function known as Hashed Message Authentication Code (HMAC) applied at every exchanged message [13]. A password/key needs to be provided manually at both ends of the session. Considering thousands of routers used concurrently, maintaining shared secrets manually between them becomes gradually more complicated. Moreover, MD5, as a cryptographic function, has its weaknesses.

IPsec: Although much more effective than the previous solution, IPsec is not widely used by ISPs. It is commonly used for tunnelling VPNs over the Internet between endpoints when transmitting confidential or important data [14, 15]. This security mechanism can be used to protect BGP sessions from integrity violation, replay and DoS attacks through its Authentication Header protocol (AH). It can also be extended to providing confidentiality via its Encapsulating Security Payload (ESP). In addition, it can dynamically negotiate secret keys and has an implemented key management mechanism. This safeguard can be efficient against BGP session local vulnerabilities, but does not address other attacks.

Generalised TTL security mechanism (GTSM): This is a security mechanism that uses the TTL attribute in the packet [16]. It prevents attackers from remotely sending BGP spoofed messages. This mechanism does not protect from any other security violation.

SECURITY REQUIREMENTS

The previous solutions, used by ISPs to temporarily protect their interdomain routing, are weak

against other attacks. In order to protect interdomain routing, the solution needs to consider many parameters that relate to the protocol itself:

- Any security architecture must not rely on mutual trust amongst subscribers and ISPs.
- The solution must scale within the BGP architecture and protocol.
- The resources required for the solution should be in the same range as BGP.
- The security services required (i.e. integrity, freshness and data origin authentication) must be assured by the traffic itself.
- BGP routers should be capable of validation of the whole chain of ASes in the path.

From the previously derived requirements, the main focus on securing BGP deals with UPDATE messages and the environment that they depend on. Vardar has provided three main security problems for BGP: Hop Integrity, Origin Authentication, and Path Validation [10]. Hop integrity means that the data integrity and source authentication at each hop in the path can be verified by every BGP speaker. Origin Authentication represents the evidence that the data received is from the claimed sender. It represents the validation of claims of address ownership from ASes. Path validation assures that each BGP speaker in the route must be reachable by the previous one. In other words, it verifies that the path is physically existent in the Internet map. This guarantees that malicious UPDATE messages containing false routes are disclosed.

4. SOLUTIONS FOR SECURING INTERDOMAIN ROUTING

The mechanisms built to secure BGP are numerous. However, we cover two competitive protocols. The first is Secure-BGP (S-BGP) [17]. The concept was developed by Kent, Lynn and Seo and published in April 2000. The second one is secure origin BGP (soBGP) [18]. It was designed mainly by CISCO engineers and published in 2003 as a draft for discussion.

SECURE-BGP

Secure-BGP is based on three different security mechanisms that endeavour to satisfy the BGP security requirements. The S-BGP architecture uses Public Key Infrastructures (PKIs), Attestations, and IPsec.

Public key infrastructure for S-BGP: Key management on such a large scale as the Internet neces-

sitates the existence of public key cryptography where every AS is provided with a pair of public and private keys. This requires a Public Key Infrastructure (PKI) for key management [19]. The

"Attestations are used to verify that the advertising AS was authorised by the owners of the IP prefixes."

hierarchy used follows the same scheme as the Internet's making IANA/ICANN the root Certificate Authority (CA). The latter provides keys for RIRs (i.e. Regional Internet Registries) which in turn supply for major ISPs and so on [20]. As a consequence, every operational AS will be associated with a pair of public/private keys. The cryptographic mechanism that provides the required security services is digital signatures [21]. When a speaker sends a message, it signs it with its signature key (i.e. private key). When the peer receives it, it can verify it with the verification key (i.e. public key) of the sending speaker. PKI and digital signatures help provide secure identification of BGP speakers, ASes and IP address blocks. Moreover, it supports AS number ownership and BGP router authorisation to represent an AS.

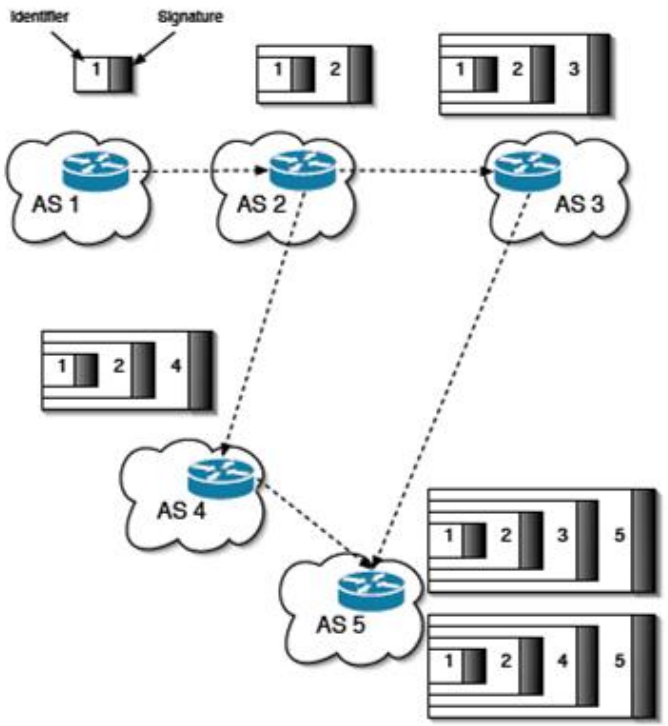
Attestations: Attestations form a trivial part of S-BGP since they are used to encapsulate authorisation information within UPDATE messages. This uses digital signatures ensuring authenticity and integrity of data provided in messages. Moreover, they are utilised to check that each AS along the path was authorised to advertise the route by the previous AS. In addition, attestations are used to verify that the advertising AS was authorised by the owners of the IP prefixes contained in UPDATE messages to advertise them. For backward compatibility, attestations are carried in an optional attribute within BGP messages. It contains digital signatures covering the whole route.

S-BGP provides two attestations used for different services. Route attestations are issued by ASes and used to provide path authentication. Address attestations are issued by the organisation that owns the prefix and used for AS authentication.

IPSEC: IPsec is used to secure point-to-point communication between BGP speakers. As stated before, it provides different services: integrity, anti-replay and anti-DoS attacks. These are the security services required for UPDATE messages. It has proven to give great stability when implemented and used in VPNs (Virtual Private Networks).

FIGURE 2

ROUTE VALIDATION



In order to validate a route, attestations and certificates are used in conjunction to verify the chain or attestations in the path. This starts from the last AS that advertised the route to the first one, as shown in FIGURE 2. When the first one is validated, it means that each subsequent AS in the path has been authorised to advertise the route for the address blocks by the previous AS along the path.

SECURE ORIGIN BGP

soBGP is based on a few mechanisms, mainly certificates, to provide different security services for interdomain routing. soBGP uses a different approach to S-BGP but has a few similarities.

As authentication and web of trust: The most important point to start with is to have a secure way of authenticating peers. soBGP overcomes this issue through the use of a certificate dedicated for AS authentication between peers. This certificate is called entity certification, or EntityCert [23]. An EntityCert binds an AS number to at

least one public key. EntityCert is classified as an X.509v3 certificate. A few keys are distributed and configured manually to have a high level of trust. They are completely trusted by any AS since they were verified and authenticated beforehand, such as top-level backbone service providers and key authentication service providers. The trusted AS can use its key to sign EntityCerts of other validated ASes. Then, the web of trust can start where the new trusted ASes can sign other ASes' certificates after validating their authenticity. This way, these EntityCerts will form a web of trust based on top-level trusted entities.

Advertisement authorisation: Having the web of trust in place with EntityCerts, providing a proof for the authorisation for each AS to advertise certain block of addresses is the next step. soBGP uses another certificate to provide this security service. **Authorisation certificates** or AuthCerts are used to bind an AS to the IP address space they are allowed to advertise.

Policy certificate: AuthCerts are not advertised independently, but encapsulated into certificates that include a set of policies the originator enforces to the advertised prefixes. **PrefixPolicyCerts** enclose an authorisation certificate, the policies applied to the prefix within the certificate, and a signature signed by the authorised AS. This allows the originator to enforce a few policies.

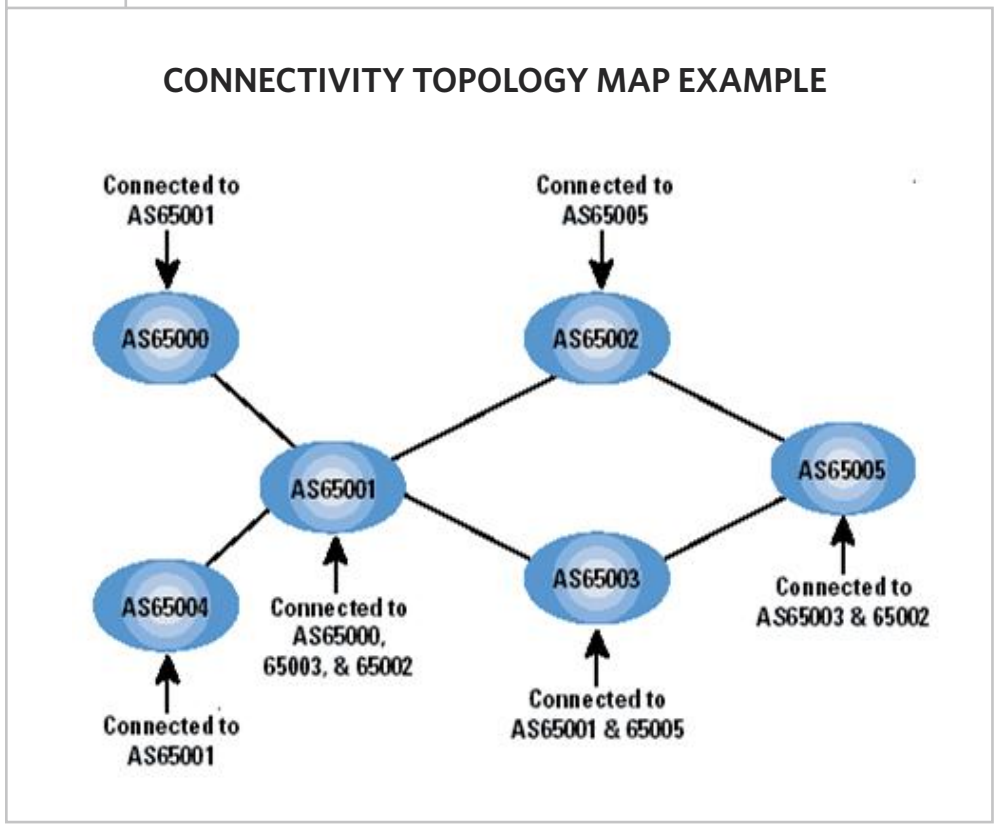
"A few keys are distributed and configured manually to have a high level of trust. They are completely trusted by any AS since they were verified and authenticated beforehand."

Topology map: Secure origin BGP designed a way to verify that a given advertiser AS of a route has a real path to the destination, through the use of certificates named **ASPocilyCerts**. Every AS creates this certificate by signing with its private key a list of its peers. This way, an internetwork topol-

ogy map is assembled. For example, in FIGURE 3, AS65003 sends an UPDATE message to AS65005 claiming it is capable of reaching AS65004 through the path {65003, 65001, 65004}. The receiving AS (i.e. AS 65005) can verify that AS65003 has revealed concrete information. AS65005 checks the ASPolicyCert of AS65003 ensuring that it is connected to AS65001, then the ASPolicyCert of AS65001 validating that it is connected to AS65003. Adding the different border policies between ASes, the topology map can provide more flexibility and preciseness.

For all these certificates, soBGP uses a new BGP message that handles the transportation of those security mechanisms. The new SECURITY message is used to carry specifically soBGP certificates [24].

FIGURE 3



5. S-BGP VS. SOBGP

S-BGP and soBGP were designed to overcome certain security issues in interdomain routing. They both tackle the problems differently with a few similarities.

S-BGP and soBGP rely on the same cryptographic primitives (i.e. mainly digital signatures). However, the extensiveness of their use is dissimilar. While S-BGP requires a signature at every UPDATE, soBGP

uses a set of certificates in a relatively static way. Clearly, there is a tradeoff between security and cost.

In terms of key distribution, PKIs in S-BGP offer a better security level than soBGP. However, they are more complex and expensive to implement and deploy. Although, the web of trust of soBGP is more flexible and avoids the issue of a single point of failure; the trust is distributed and therefore harder to manage. Moreover, its definition is still fuzzy and the security level is still debatable.

"In terms of level of security, S-BGP dramatically takes the lead. Although it has not covered all of the issues, it provides well structured and secure measures."

For the exchange of security elements, the best solution that does not include additional design issues is S-BGP's new attribute included in the ordinary BGP-4 message. Moreover, S-BGP provides better security for message exchange because they are dynamically signed. In terms of performance, soBGP performs better because all certificates can be signed by another external entity. However, the fact of having another type of message can cause issues in deployment and backward compatibility.

In terms of level of security, S-BGP dramatically takes the lead. Although it has not covered all of the issues, it provides well structured and secure measures. Origin authentication is provided by utilising PKI and address attestations. Path validation is accomplished through route attestations. In addition, hop integrity is supplied through IPsec with integrity and source authentication for every hop. The issue with S-BGP is complexity, especially with the PKIs. As quoted by Bellovin, "Complexity is the enemy of Security", the issue that S-BGP encounters is cost and ability for routers used nowadays to scale with the required performance. soBGP is more lightweight and therefore a better choice on this side. However, there is still the issue of integrity of messages which is not ensured since it uses the new SECURITY message. Route validation is met at a very weak level. soBGP provides a static path plausibility rather than authenticity and no hop

integrity. Although it provides a policy checking mechanism, it becomes more complex when more policies come into play. Furthermore, both path authentication and policy checking require additional topology and policy databases respectively, increasing complexity and dependence.

6. CONCLUSION

Interdomain routing has received quite a lot of interest in the last decade, due to its importance to many organisations and the whole Internet community. Today, and for nearly two decades, the Internet has viewed BGP as an effective protocol that could cope with its scale of growth. However, BGP has shown many weaknesses and vulnerabilities to malicious behaviour and inappropriate configuration. Many countermeasures were built to secure BGP, but these are not part of the protocol and some of them employ weak security mechanisms. Many solutions for securing interdomain routing have been proposed. However, majorly only a few have been discussed over the last five years. Two of them were analysed: S-BGP and soBGP. Both of these protocols have a similar aim which is to protect BGP-4. However, through their design, they seek to secure it differently.

After comparing both S-BGP and soBGP, we tried to objectively come up with a conclusion. In terms of security, S-BGP is far more complete than soBGP. It provides clear security requirements that work well theoretically. However, the complexity in S-BGP is immense. This leads to slow performance and convergence. Moreover, the practicality of deployment for S-BGP is still questionable. Although soBGP is lightweight and overcomes some of these performance issues, it merely provides good origin authentication and only affords path plausibility service. This means that paths can be changed and an attacker can intrude into the path. While S-BGP provides full path authentication, soBGP provides a weaker

"For nearly two decades, the Internet has viewed BGP as an effective protocol that could cope with its scale of growth."

static service for protecting the authenticity of paths. S-BGP on its own provides point-to-point connection security measures through the use of IPsec. Now, the problem relies on performance and complexity. There is a tradeoff between the level of security required, performance and complexity issues. However, S-BGP is a much better solution to be further researched. By trying to provide less extensive cryptographic primitives and a better way to deploy it, S-BGP can be the next step towards a more secure Interdomain Routing. ■

ABOUT THE AUTHORS

Rostom Zouaghi completed the MSc degree in Information Security (with Distinction) in 2008 and recently started a PhD in information security. His interests lie in the fields of network security, distributed algorithms and cryptographic algorithms. In his PhD, he is conducting research in mobility-aware routing and security protocols for MANETs.

Dr. Stephen Wolthusen is a lecturer in information security at Royal Holloway, University of London, with research interests in information assurance and the use of formal methods in security. Dr. Wolthusen teaches the courses in Network Security and Digital Forensics on the M.Sc. in Information Security at Royal Holloway.

REFERENCES:

[1] R. Mahajan, D. Wetherall, and T. Anderson. "Understanding BGP Misconfiguration". In Proc. ACM SIGCOMM, pages 3.17, Pittsburgh, PA, Aug. 2002.

[2] S. Murphy, A. Barbir, and Y. Yang. "Generic Threats to Routing Protocols". Internet Engineering Task Force, Oct. 2004. http://www.ietf.org/internet-drafts/draft-ietf-rpsec-routing-threats-07.txt, expired April 2005.

[3] N. Feamster, J. Borkenhagen, and J. Rexford. "Guidelines for Interdomain Traffic Engineering". ACM Computer Communications Review, 33(5):19.30, Oct. 2003.

[4] IANA/ICANN, "Number Resources", URL: http://www.iana.com/numbers

[5] CNET News. "Router Glitch Cuts Net Access", URL: http://news.com.com/2100-1033-279235.html, April 1997.

[6] S. Convery et. al. "An Attack Tree for the Border Gateway Protocol", Technical Report, Internet Engineering Task Force, November 2002.

[7] S. Murphy. "BGP Security Vulnerabilities Analysis", Network Working Group, Internet Engineering Task Force, January 2006, RFC 4272.

[8] P. Savola, "Backbone Infrastructure Attacks and Protections", Technical Report, Internet Engineering Task Force, January 2007.

[9] B. R. Greene and P. Smith. "BGPv4 Security Risk Assessment", ISP Essentials Supplement, Cisco Press Publications, June 11th, 2002..

[10] Tuna Vardar, "SECURITY IN INTERDOMAIN ROUTING", Helsinki University of Technology, T-110.551 Seminar of Internetworking, 2004.

[11] Z. M. Mao, J. Rexford, et. al. "Towards an Accurate AS-Level Traceroute", ACM SIGOMM, Germany, August 2003.

[12] L. Gao et. al. "Stable Internet routing without global coordination", IEEE/ACM Transactions on Networking, p. 681-692, December 2001.

[13] H. Krawczyk et. al. "HMAC: Keyed-Hashing for Message Authentication", Internet Engineering Task Force, April 1997, RFC 2104.

[14] S. Kent and R. Atkinson. "Security Architecture for the Internet Protocol", Internet Engineering Task Force, November 1998, RFC 2401.

REFERENCES CONTINUED:

[15] R. Thayer et. al. "IP Security Document Roadmap", Internet Engineering Task Force, November 1998, RFC 2411.

[16] V. Gill et. al. "The Generalized TTL Security Mechanism (GTSM)", Internet Engineering Task Force, February 2004, RFC 3682.

[17] S. Kent, et. al. "Secure Border Gateway Protocol (Secure-BGP)", IEEE Communications Vol. 18, No. 4, pp. 582-592, April 2000.

[18] R. White. "Securing BGP Through Secure Origin BGP", The Internet Protocol Journal – Vol. 6, No 3, Cisco Systems, September 2003.

[19] S. Chokhani et. al. "Internet x.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", Network Working Group, Internet Engineering Task Force, March 1999, RFC 2527.

[20] K. Seo et. al. "Public-key Infrastructure for the Secure Border Gateway Protocol (S-BGP)", Anaheim, CA, USA: IEEE DARPA Information Survivability Conference and Exposition II, June 2001.

[21] Alfred J. Menezes, P. Van Oorschot, and S. Vanstone. "Handbook of Applied Cryptography", CRC Press, 1996.

[22] K. Butler et. al. "A Survey of BGP Security Issues and Solutions", AT&T Labs Research, January 2008.

[23] B. Weis. "Secure Origin BGP (soBGP) Certificates", Internet Engineering Task Force, Cisco Systems, draft-weis-sobgp-certificates-02.txt, July 2004.

[24] J. Ng. "Extensions to BGP Transport soBGP Certificates", Interdomain Routing Working Group, Cisco Systems, draft-ng-sobgp-bgpextensions-01, May 2005.