CS996 Cybersecurity Fundamentals
University of Strathclyde

Individual Report
Andrea Gibb

A Survey of BGP Security Issues and Solutions

Intro

BGP is short for Border Gateway Protocol, it is designed to share and exchange routing information among autonomous systems. Simply put it is the protocol that makes the internet work. On the internet BGP protocol allows information to travel based on decisions adhering to network policies, configured rule-sets and paths. (O.C.S 2013) For this reason, the appropriate term is reachability protocol, rather than routing protocol. The internet is a network of networks, routing protocols such as BGP are designed to aid routers in finding secure, suitable adjacent networks across the world.

Overview

This paper asks the reader to consider the current vulnerabilities and consider cost-effective solutions. The paper offers to explain why no viable solution has been yet been found. The paper's focal point is to investigate the continuing concern and lack of security guarantees within interdomain routing.

As discussed, the BGP is the glue that holds the internet together however, is it highly vulnerable, it does not adequately address security and a review of proposed improvements must be made. The central question in this paper asks, what are the major limitations of BGP. The objective of this study is to review the research conducted in 'A survey of BGP security and issues and solutions' by providing a critical commentary on the strengths and weaknesses of the work in the paper, concluding with a discussion on the relevant topics for the reader to consider.

Investigation

In this section we examine the evidence defining the limitations of BGP. Firstly, we must recognize the solutions in place. BGP employs route attributes to enforce policy routing, for example, local preference, AS path lengths, origin type, and route filtering. These currently-implemented solutions have limited effectiveness, for example paths selected are based on policy, but there is limited information to base the decision, even less capacity or performance information, and static routing would not be suitable as conditions change. Paths also have a destination prefix, meaning limited flexibility. Limited diversity can also occur when unselected paths are not announced to neighbors. This current version has been supporting the internet since 1994 (Goldberg 2010) but with little to no adoption the limitations persist and the BGP essentially stays unchanged. The paper investigates integrity protection, session and message protection, TTL security mechanism (GTSM) and IPsec, all of which provide varying levels of protection in providing stable routing. The paper continues by stating the complications of adopting the investigated solutions. From an operational stand point the BGP security is complicated by the continuous growth of the internet. The growing rate of AS numbers is becoming increasing rich with connectivity, this activity contributes to scalability issues, thus resulting in route filtering as the only widely deployed solution. Filtering and relying on routing registries is difficult as routing registries contain too much information to keep accurate. Unfortunately, many of the solutions require a valid and secure route at the very least, of course there are protocols for securing routes, for

example IPsec, however the implementation of such systems is complex if feasible and as such are not often implemented. Another concern hampering the papers findings is the computation requirements, cryptography while ensuring integrity could overload deployed routers, adding additional complexity to the infrastructure.

Results

In this section we analyze the results for BGP security, the techniques for implementing robust solutions for these problems. The paper suggests several solutions by numerous researchers addressing the severe issues. The internet is notoriously vulnerable to traffic interception attacks, allowing ASes to manipulate BGP to or through their networks. Enabling attackers to increase revenue from customers by snooping, tampering or dropping packets, simply by attracting extra traffic. (H. Ballani 2007)

MD5 password hash works relatively well from over the shoulder attackers, however if an attacker generates lots of fake BGP packets with incorrect hashes, the router will become drowned in MD5 calculations. This is where IPsec comes in, as it addresses all these weaknesses. Unfortunately, IPsec has the ability to protect these BGP sessions but is not widely implemented, and complex when it is. The paper also states localized solutions are a more practical than the current decentralized system, another basic security limitation.

Protecting a connection between two BGP routers heavily relies on the protection of the underlying TCP session and defenses to protect the BGP session. One of the solutions the paper investigates is session and message protection. The five proposed countermeasures aim to secure the message and session environment. The first two countermeasures control the messages by encryption, for example the data between peers uses a secret key shared by all peers and is then further secured by adding sequence numbers to ensure the ordering of the messages. The other three ensure message update protection, this includes an additional update sequence number, new path attribute and timestamp. Encryption and authentication using sequence numbers protects to a certain degree however, this solution relies on shared keys which can be enormously complex with the growing rate of routers in the internet, another solution hindered by scalability. Shared key cryptography is also infrequently used due to the inherent insecurity of having to share a key.

Generalized TTL security mechanism is described as low cost, simple and effective against unsophisticated attackers, this is because GTSM works well in securing peers from remote attacks. However, it poorly defends against peers that are the same number of hops away, meaning the defense mechanism set in place to decrement at every hop is less useful. GTSM is based on the vast majority of protocols established between adjacent routers, however is does not defend well against insider attacks for example packet replay or spoofing. (Gill et, al 200)

The paper lays out an overview of the most relevant and widely proposed solutions paired with varying levels of protection. Many solutions proposed by cryptographic defenses such as, pairwise keying that relies on shared secret keys, hash functions, message authentication, Diffie-Hellman key, public key infrastructure and certificates allowing a chain of trust. However, the BGP sessions must be secured in conjunction, this is where IPsec has proven useful. BGP routers communicate via TCP with no need to deal with error, flow and congestion control. However, TCP in itself is quite insecure. IP packets have no inherent security, IPsec provides an automated solution for three weak areas when sending IP packets, authentication, integrity and confidentiality.

To summarize this section, the results are suggesting that BGP has been successful in providing a number of diverse solutions, however, these solutions show that no single tool or mechanism can comprehensively secure the entirety of BGP.

Knowledge gained

Before reading this paper, I was unaware of the emerging issues, although many security solutions exist, some have been implemented, some have only been proposed. However, they are not widely accepted yet due to computation complexity, financial and scalability. This study has shown that IPsec protocol should be used as it encrypts traffic between two machines over unsecure network. It works by taking a packet (a message sent over the internet) encrypting it, and then encapsulating it within a second packet. This solves the problem of an untrusted network in much the same way a VPN does, as the message can only be decrypted by the intended recipient.

Critical Commentary

This section will discuss the strengths and weaknesses from the results gathered in the paper. Firstly, S-BGP, which uses DSA to authenticate routes, unfortunately deployment was prevented by performance issues when processing latencies. Weaknesses also include the validation cost due to the amount of data and signers involved. Route attestation in S-BGP (onion style), proposes thorough security guarantees by providing extensive authentication of the origins and paths for the full route, however there are still some barriers presented, for example the requirement of substantial storage. (Zhao et al 2005) To mitigate these issues an aggregated path authentication was proposed, this solution takes two efficient cryptographic techniques and combines them, improving efficiency on both speed and space.

Secure origin BGP (soBGP) works in a similar manor to S-BGP by managing three separate certificates using PKI. soBGP targets the need to verify the validity of an advertised prefix, for instance is the originator authorized to advertise this particular route? soBGP can verify a peer advertising a prefix, with at least one valid path to the destination. Another benefit of soBGP that other solutions encounter is that ability to incrementally deploy without impacting other ASes that do not implement soBGP, meaning partial deployment is possible. The main difference between S-BGP and so-BGP is that while S-BGP requires one signature with every update soBGP uses a set of certificates in a comparatively static form. When considering PKI key distribution S-BGP offers a favorable level of security, however it is more complex and expensive to deploy. In terms of security S-BGP takes the lead, even if it leads to slower performance and convergence.

The BGP transport connection MD5 password cryptographic hash is widely used in practice. It provides inexpensive countermeasures, with these measures we can reasonably assume two things. The sender that provided the packet knows the secret password and the TCP contents wasn't modified or tampered with during transit. If an attacker spoofed a TCP reset, the MD5 hash would be missing or incorrect, the router then ignores those packets and the BGP sessions is unaffected. Unfortunately, it is relatively weak and only provides short term solutions for example if a hacker were to generate fake BGP packets with incorrect hashes, the router CPU could overload with MD5 calculations.

Many resent solutions suggest the IPsec mechanism. When deploying secure peer to peer communications, IPsec provides the most comprehensive existing solution, and also protects against denial of service, although limited. This is because although addressing many issues within local sessions, they do little to prevent a widespread attack. Hop integrity protocols and countermeasures provides a subset of IPsec functionality using specialized protocols. IPsec was not widely available at the time of these other solutions being proposed, hence it was unclear what these services provided that IPsec wasn't already providing more effectively. However, IPsec does address all the weaknesses in previous mechanisms, it is a general-purpose security solution with new and improved MD5 password systems. Unfortunately, is it not widely implemented due to the complexity, and in practice it is rarely used.

The most effective and widely used solution is defensive filtering policies, rules set in place to highlight suspicious routes. Defensive filtering filters prefix's according to guidelines, this filters out potentially dangerous or malicious attacks by relying on allocated prefixes, rewriting routes for malformed routes and aggressive filtering for customers, for example customers mirroring expected behavior. However, this only catches obvious errors.

Future considerations

When BGP was developed in the early 1990's security protocols were an afterthought, over the years we've come to understand there are two potential issues when dealing with BGP security issues. You may be communicating with the wrong device or the right device may be delivering the wrong thing. This paper provided an important opportunity to advance the understanding of the vulnerabilities of the BGP. In conclusion these findings lead to an important avenue for future research, so-BGP and S-BGP could be combined for deployment alongside defensive filtering mechanisms, note however this is a significant challenge in practice as it requires voluntary compliance from each provider, and even then, it is difficult to ensure the correct implementation. Future end to end solutions will require collaboration from all users of the system, this includes SPs, enterprise users and vendors.

Works Cited

Orbit-Computer-Solutions.Com(n.d), Computer Training & CCNA Networking Solutions, Orbit-Computer-Solutions.com, retrieved 8 October 2013

Goldberg, S., Schapira, M., Hummon, P. and Rexford, J., 2011. How secure are secure interdomain routing protocols. ACM SIGCOMM Computer Communication Review, 41(4), pp.87-98.

Gill, V., Heasley, J., Meyer, D., Savola, P. and Pignataro, C., 2007. *The generalized TTL security mechanism (GTSM)* (No. RFC 5082).

H. Ballani, P. Francis, and X. Zhang, "A study of prefix hijacking and interception in the Internet," in ACM SIGCOMM, 2007

Meiyuan Zhao, Sean W. Smith, and David M. Nicol, "Aggregated Path Authentication for Efficient BGP Security" Dartmouth Computer Science Technical