Securing BGP Through Existing Infrastructure and Contractual Chains (CCBGP)

Yuri Cantor, Nancy Griffeth, and Bilal Khan
Department of Computer Science
The CUNY Graduate Center
365 Fifth Avenue New York City, NY 10016, USA

June 17, 2010

Abstract

This paper proposes a novel approach that draws upon the existing architecture and contractual relationships and compares the approach to the main existing techniques for securing BGP against prefix hijacking. We define prefix hijacking as usurping control of IP prefixes through the manipulation of BGP routing tables resulting in a redirection of network traffic away from a *correct* route to a prefix, which traverses all and only the ASes in the route advertisements and abides by BGP policy finally terminating at the AS that owns that prefix route, and onto another route. We further refine our definition to not include those attacks where the attacking AS lies along the correct path but does not actually route packets as it advertises. Our novel approach, termed Contractual Chained BGP, completely eliminates prefix hijacking under certain plausible assumptions[1] and provides support for accountability in the form of forensic traceback. CCBGP applies contracts to build a transient chain of links between AS neighbors and neighbors of neighbors. Because the links are transient, each AS need only be aware of the links in its contractual sphere. Keeping the contractual sphere small limits the computational requirements of creating a chain link while the overlap of the links provides the security of a complete chain.

1 Introduction

The security of the protocols that enable the Internet to function have become essential to the financial, political, and commercial functioning of society. The development of these protocols did not anticipate the current threats, and exactly because security was once a non-issue it is now paramount. This paper seeks to address one well-known and serious BGP vulnerability, prefix hijacking[5].

Specifically this paper borrows from ideas applied in other areas of security to substantially increase the difficulty of prefix hijacking, to provide forensic trace back to the originator of the hijack, and to connect these directly to the relationships between neighboring autonomous systems. Previous recommendations for securing the same BGP vulnerability have relied on costly modifications to the infrastructure and protocol, and as a result these recommendations have not been deployed widely. In contrast this paper proposes a method for defending against prefix hijackings with only a moderate cost for deployment and a seamless integration with the existing infrastructure and protocol. The proposed innovation is to utilize the existing contractual relationship to form decentralized links which when combined create of a chain of trust. The chain of trust can be used both to prevent prefix hijackings and to trace back any attempts to hijack.

[1] Under the assumption of non-collusion between direct neighbors and protocol assumptions which are elaborated in section 4.2.

However, even with the implementation of CCBGP there are still many tools that can help improve security. Specifically, research should continue in how contracts and relationships can be leveraged for security. Answers to the following questions could provide guidance to where security resources are most effectively deployed: Who wants to hijack a prefix versus who actually hijacks prefixes, Why are prefixes hijacked, Which prefixes are hijacked most often, Which tier of AS usually initiates the hijacks, At which tier is security against hijacks most important, Where is collusion is more likely, and What tools can be used or created to enhance security and testing?

References

[1] C. Ellison and B. Schneier. Ten risks of pki: What youre not being told about public key infrastructure. In *Computer Security Journal, V 16, n 1*, pages 1–7, 2000.

[2] Y. Hu, A. Perrig, and M. Sirbu. Spv: secure path vector routing for securing bgp. In *SIGCOMM '04. ACM, In Proceedings of the 2004 Conference on Applications, Technologies, Architectures, and Protocols For Computer Communications (Portland, Oregon, USA, August 30 - September 03, 2004)*, pages 179–192, 2004.

[3] J. Karlin. Pretty good bgp: Improving bgp by cautiously adopting routes. In *In Proc. International Conference on Network Protocols*, 2006.

[4] S. Kent, C. Lynn, and K. Seo. Secure border gateway protocol (s-bgp). In *IEEE Journal on Selected Areas in Communications 18, 4 (Apr.)*, pages 582–592, 2000.

[5] M. Lad, R. Oliveira, B. Zhang, and L. Zhang. Understanding the impact of bgp prefix hijacks. In *ACM SIGCOMM. Poster*, 2006.

[6] P. v. Oorschot, T. Wan, and E. Kranakis. On interdomain routing security and pretty secure bgp (psbgp). *ACM Trans. Inf. Syst. Secur.*, 10(3):11, 2007.

[7] Y. Rekhter and Li. A border gateway protocol 4 (bgp 4). In *IETF RFC 1771*, 1995.

[8] R. White. Securing bgp through secure origin bgp. In *The Internet Protocol Journal 6, 3*, pages 12–22, 2003.

[9] Z. Zhang, Y. Zhang, Y. C. Hu, and Z. M. Mao. Practical defenses against bgp prefix hijacking. In *CoNEXT '07: Proceedings of the 2007 ACM CoNEXT conference*, pages 1–12, New York, NY, USA, 2007. ACM.

[10] C. Zheng, L. Ji, D. Pei, J. Wang, and P. Francis. A light-weight distributed scheme for detecting ip prefix hijacks in real-time. In *SIGCOMM '07: Proceedings of the 2007 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 277–288, New York, NY, USA, 2007. ACM.