Spring 3-1-2017

BGP Route Attestation: Design and Observation Using IPV6

Michael J. Ham
Dakota State University

BGP ROUTE ATTESTATION: DESIGN AND OBSERVATION USING IPV6 HEADERS

by

Michael J. Ham

A Dissertation Presented in Partial Fulfillment

of the Requirements for the Degree

Doctor of Science in Cyber Security

DAKOTA STATE UNIVERSITY

March 2017

BGP ROUTE ATTESTATION: DESIGN AND OBSERVATION USING IPV6 HEADERS

by

Michael J. Ham

March 2017

Approved:

Dr. Wayne E. Pauli, Chair

Dr. Kyle L. Cronin, Committee

Dr. Mark L. Hawkes, Committee

Accepted and Signed:_____ _____
Wayne E. Pauli, Ph.D. Date

Accepted and Signed:_____ _____
Kyle L. Cronin, D.Sc. Date

Accepted and Signed:_____ _____
Mark L. Hawkes, Ph. D. Date

_____ _____
Mark L. Hawkes Date
Dean for Graduate Studies and Research
Dakota State University

Abstract

This quasi-experimental before-and-after study examined the impacts of using IPv6 extension headers to carry cryptographic Border Gateway Protocol (BGP) route attestation information. Literature was assessed surrounding: the design of BGP, vulnerabilities in BGP, a survey of proposed route attestation solutions, IPv6 extension header design, overhead in cryptography, and factors influencing the adoption of proposed solutions. The literature surveyed showed a need to evaluate IPv6 and its role in helping secure the Internet's routing protocol, BGP. The study resulted in statically significant figures representing the cost associated in an instantiation of using IPv6 extension headers to carry BGP route attestation information. Furthermore, future opportunities for research to improve upon overall BGP security and the inclusion of IPv6 in such models were discussed. The research performed revealed potential pathways for enhancing Internet routing as a whole.

DEDICATION

I dedicate this dissertation to my parents whose untiring love and support made this work possible. I love you to the moon and back!

ACKNOWLEDGEMENTS

I have been looking forward to writing these acknowledgements and have thought about it many times since beginning this dissertation. Writing this section carries a sense of actualization to the dissertation process as brings into view the next chapters of my life. I found it was an easy, yet challenging section to write at the same time. Easy, because of the numerous people that have helped me get to this point, but challenging to convey the enormous amount of gratitude I have for each of them in this short space. Writing this section has been a humbling and amazingly fulfilling experience.

The completion of this dissertation would not have been possible without the support of several people in my life: my family, mentors, teachers, and friends. Your help is what made this possible – you believed in me and inspired me. I gained an abundance of encouragement and motivation by your involvement in this work and in my life.

To my parents, John and Ann who taught me the value of education, commitment to personal beliefs, and what it means to work hard to achieve my goals. You have given me so many opportunities to succeed in pursuing my dreams. I couldn't ask for better parents, thank you for everything you've done along the way. To my older brother, Matthew, an incredible role model, brother, and best friend that has been by my side throughout my life. You've taught me so much over the years and I know there's more to come. I tremendously admire and look up to you. My grandparents, Jim and Barb, your frequent words of encouragement and letting me know you were proud of my work meant a great deal and inspired me to finish this dissertation the right way. Also, to my grandparents John and Lois, who have reminded me of the importance of family and have

supported me in many different ways. I am so blessed to have the amazing family that I do, I love you all very much!

To all of my committee members, I am exceptionally grateful for all the advice and help you have given me throughout this process. Your sound recommendations and mentorship of this research will undoubtedly shape my future endeavors.

To Dr. Wayne Pauli, you've done an excellent job serving as the chair of my committee. Among the many qualities you have, your ability to listen to and share the excitement about my ideas was very impactful and positive to me. I have learned an extraordinary amount from your advice and guidance along the way. Even as this degree concludes, there is much I have to learn from you. If you offer any follow-up classes, I will happily register for them as long as the classroom location remains on your deck.

To Dr. Kyle Cronin, I cannot express enough gratitude for your mentorship and friendship – you've become like family to me. Over the years, you have convinced me that all of this effort would eventually be worth it, and I'm finally starting to see that now. In all of the times that I sought your help along the way, even when you were stuck in an ice house with me, you never once turned down my questions. I am more than grateful for your willingness to help, and to see me succeed. You've been a great friend and supporter - I would not have made it this far without you.

To Dr. Mark Hawkes, thank you for taking on the work of helping with my dissertation and serving on my committee. You have been fantastic to work with and contributed an important perspective on this research. I appreciate your willingness take on this project and encourage me to keep going throughout each step. Thank you for sharing your knowledge and expertise with me along the way.

My friends from DSU, you always make it fun to come to work and be around our campus. Tom, you've been one of the most inspirational teachers that I have had – thanks for being around and always willing to help me. Josh and Pat, you guys set the hook for me on how fun the security world is to be a part of, thanks for all of the entertaining classes and help throughout my career. Kathy, Rob, Scott, and Tyler, its been so much fun getting together for QDFs, camps, security cons, and the DSU road show. I'm sure there will more to come!

I know there are many names of people who have made an impact on my work that I have missed. You are the ones who have been along with me on all sorts of adventures. We've spent time together hunting and fishing, touring breweries, watching Minnesota Wild games, camping, and performing deck inspections together. It was important to be able to unplug and relax in the midst of working on this dissertation – I'm looking forward to getting together with friends more often! I would be remiss not to mention an exceptional dog, Drake, aka B (don't worry, I'll read this to him). Your endearing pursuit of ear scratches and unfaltering desire to fetch were always a welcomed distraction. You reminded me to take care of those around me during this personally consuming process.

It has been a remarkable experience to reflect and think about all of the people have helped me in this journey. Thank you!

TABLE OF CONTENTS

List of Figures

CHAPTER 1: INTRODUCTION

The matter of this quasi-experimental before-and-after study was the impact of using IPv6 to perform Border Gateway Protocol (BGP) routing update attestation and measuring the resulting impacts. The study was designed to measure a method of protecting BGP, which all Internet traffic is dependent on, thus affecting all users. According to Cardona, Vissicchio, Lucente, and Francois (2016) BGP is the standard routing protocol used across the Internet. Despite the critical role BGP plays in directing Internet traffic, the standardized version of the protocol lacks the ability to validate and authorize other BGP speakers to take ownership of a network. The result is a system based solely on trust, leaving systems vulnerable to malicious actors stealing or modifying network traffic. Stolen or modified network traffic may result in denial of service (DoS) or the loss of sensitive information. The transition to a secure implementation of the routing protocol has been hindered by adoptability and limitations in proposed solutions (P. Gill, Schapira, & Goldberg, 2011). Many of the proposed solutions address Internet Protocol version 4 (IPv4), but not IP version 6 (IPv6) which the Internet is moving towards since the available pool of IPv4 addresses is exhausted. As a result, the Internet is forced to adopt IPv6, therefore demonstrating a need to assess security of BGP in the context of IPv6.

The focus of this study was to create and evaluate a model of performing validation and authorization of routing updates in an IPv6 space while quantitatively measuring the performance impact of the solution. As the Internet has adopted BGP-4 as the standard inter-domain routing protocol after its release in 1995 (Traina, 1995), it is important to secure it in an efficient, scalable, and highly-adoptable way. Many existing solutions have suffered poor adoption due to a high cost or poor effectiveness in a

partially deployed environment (Lychev, Goldberg, & Schapira, 2013). P. Gill et al. (2011) indicated the importance of finding such a solution to the existing issues within BGP, citing economic and security implications entering the spotlight of major entities on the Internet.

A common result of increasing the security of a system or process is a negative impact on performance. Chapter 1 details the proposed study of how a model leveraging the efficiencies of IPv6 can provide an adoptable security model for enhancing BGP while minding the performance implications of doing such. The chapter will introduce the background of the study, significance of the study, design of the study, as well as the potential outcomes and resulting impact. Additional dialogue will ascertain key issues that are suggested for research alongside of important questions pertaining to said research. The purpose of this study was to determine whether the efficiencies introduced in the IPv6 protocol may aid a BGP security model in circumventing routing attacks and to measure the performance penalty of participating routers.

Background of the Study

The Internet is composed of countless entities that own networks or IP addresses, and those entities are interconnected through different topologies and configurations. For example, some of these entities may have direct connections between each other, while others may connect through one or more Internet service providers. The methods of establishing an online presence and connecting with other organizations is innumerable. This flexibility of topology design is made possible by interdomain routing protocols.

Interdomain routing is a fundamental component of how the Internet works. As new networks are created and others taken offline, the Internet is in a constantly changing state (Gao, 2001). To cope with the volatile nature of the Internet, interdomain routing

protocols are leveraged by entities participating in Internet communication. These protocols are designed to not only inform other parties of the networks that exist, but offer a roadmap of how to reach those networks (Kuhn, Liu, & Rossman, 2009). The underlying goal of an interdomain routing protocol is to provide an accurate and up-to-date picture of reachable networks alongside of a reliable path by which to reach them (P. Gill, Schapira, & Goldberg, 2013).

The previously described interconnected entities, or autonomous systems, exist within the Internet and interdomain routing ecosystem. Although the definition of an autonomous system (AS) is somewhat ambiguous (Hawkinson & Bates, 1996), Gao (2001) describes an autonomous system as portion of a network operated by an administrative domain. Furthermore, autonomous systems are referred to by a globally unique number assigned by a governing body like the Internet Assigned Numbers Authority (Vohra & Chen, 2012). An autonomous system number may look like AS23122. Examples of these types of administrative domains that own autonomous systems may be Internet service providers (ISPs), universities, and companies. In addition, one administrative domain may operate numerous autonomous systems as a smaller portion of their expanse. Interdomain routing facilitates the communication between these autonomous systems.

Prior to the widespread adoption of BGP, several other external routing protocols were used on the public Internet. Many of those also existed inside of private networks such as the Exterior Gateway Protocol (EGP), Routing Information Protocol (RIP), and Open Shortest Path First (OSPF). Due to the nature of how the Internet has grown and the complex interconnections between networks, significant topological issues arose with the protocols preceding BGP (Traina, 1995). The limitations with protocols such as EGP

became impractical from both technical and operational standpoints. According to Traina (1995), BGP addressed these limitations and matched the IP hop-by-hop archetype necessitated by the Internet's design.

The first version of the BGP came from Lougheed and Rekhter (1989) as a new protocol to enable the exchange of information and routes between autonomous systems. It was deemed as an "inter-autonomous system" routing protocol. Alongside the evolution of the Internet, the BGP protocol developed as well, resulting in several versions that addressed shortcomings in protocols such as EGP. Yakov Rekhter and Li (1995) introduced BGP version four (BGP-4), the currently used standard, in a request for comment (RFC). This version reflected changes and the need for efficiency in performance of such routing protocols.

Since the introduction of BGP-4 in 1995, BGP has become the most widely used inter domain routing protocol. In fact, Jakub et al. (2014) assert that BGP is the only deployed interdomain routing protocol in use on the Internet. BGP is responsible for directing traffic between various autonomous systems across the Internet and on a large scale, serves as the backbone of the Internet (Medhi & Ramasamy, 2007). Since its introduction, BGP is still being used as the de-facto standard for inter domain routing after a decade of use and progression. Effectively, any traffic leaving an autonomous system such as an Internet service provider (ISP) to a second autonomous system will be routed by BGP at some point. The scale of Internet traffic relying on this protocol is colossal.

During BGPs introduction, it was built upon an inherent model of trust. When a BGP speaker announces a new route stemming from a number of events such as a network being added, networks being segmented or deleted, a new shorter path between

endpoints, etc., each neighboring BGP peer does not validate or attest the route information. Rather, the neighbors propagate the route update to their peers (Qi et al., 2012). The result of this model is a lightweight approach to passing information vital to the flow of Internet traffic. BGP does not introduce a significant amount of overhead on the routers participating compared to trust models such as public key infrastructure (PKI) (Peyravian, Roginsky, & Zunic, 2004). Despite the advantages of an inherent trust model, there are significant risks and outcomes if a malicious entity enters the ecosystem.

If the routers responsible for directing traffic between autonomous systems cannot attest the routes that they are receiving due to a lack of support in the BGP-4 protocol specification, a variation of negative impacts may occur to Internet users on a large scale. There have been multiple notable instances of undesirable affects from BGP misconfiguration and possible route hijacking attacks. Regardless of the intent or motivation behind the route redirection via BGP, the impacts are clearly visible and problematic.

One of the most notable BGP hijacking instances is the YouTube hijacking by Pakistani ISP, AS17557 (Bornhauser & Martini, 2011). The YouTube hijacking was the direct result of a sub-prefix hijack attack as according to Bornhauser and Martini (2011) AS17557 advertised a network prefix of 208.65.153.0/24 which belongs to the larger subnet 208.64.152.0/22. Since a larger prefix was advertised to the Internet, BGP peers of AS17557 trusted the route update by the nature of how BGP designed, the larger the prefix, the more trusted. This property aligns with the largest-prefix match rule of BGP. The hijacking by the Pakistani ISP clearly demonstrated a politically motivated denial of service that had greater reach than originally intended by those who introduced it.

A second example of BGP redirection and prefix hijacking occurred in 2013. An ISP in Belarus, GlobalOneBel, intercepted traffic from several countries beginning on July 31, 2013 and continuing through August 19, 2013 (Yun & Song, 2015). As noted by Yun, traffic from various countries' financial institutions, governments, and network service providers were affected including those residing in the United States. In this particular scenario, traffic was intercepted and forwarded on as seen in common Man-In-The-Middle (MITM) attacks rather than creating denial of service (DoS) conditions.

A third, more recent example of BGP route hijacking began on February 2014 via a Canadian ISP. Over the course of this hijacking that lasted nearly four months, attackers compromised 51 networks and 19 different ISPs (Sun et al., 2015). The motivation of this type of attack appeared to be financially driven. Attackers were able to steal approximately $83,000 in Bitcoins, a cryptocurrency according to Sun et al. (2015). It is quite evident from this publicly disclosed incident that BGP route hijacking attacks can affect a relatively significant number of entities while evading detection. Parceling away such a sum of money over the course of several months is no small feat, but the attackers were greatly assisted by the inherent flaws in the protocol.

In light of the outlined incidents in addition to others not documented above, the FCC has identified IP route hijacking as one of the top three areas of concern of cyber security in 2012 (FCC, 2012). Furthermore, the Department of Homeland security included route hijacking via BGP as a primary vulnerability within their Internet routing, access, and connection services function in version 1.0 of the Information Technology Sector Baseline Risk Assessment (Bullock, Haddow, & Coppola, 2015). Similarly Karlin, Forrest, and Rexford (2009) show through their study how nation-sates have been able to impact the flow of Internet traffic through BGP resulting in enforced censorship

and wiretapping. The lack of route attestation is one of the contributing factors to the threats outlined by these agencies and people, which demonstrates a clear need to improve the security of BGP and the devices participating in the protocol.

Statement of the Problem

A critical problem arose from the fact that BGP is the most widely used routing protocol on the publicly facing Internet, yet it lacks fundamental security mechanisms. For example, when following its longest prefix matching property, BGP has no security mechanisms that protect the validity and integrity of routing updates by performing route attestation (Qiu, Gao, Ranjan, & Nucci, 2007). Research clearly showed that due to the lack of security mechanisms built into BGP and the inherent trust model that the protocol is built upon, BGP is susceptible to cyber-attacks including prefix hijacking, IP spoofing, session stealing and others (Murphy, 2006). Misconfigurations in BGP or malicious actors may lead to undesired outcomes (Mahajan, Wetherall, & Anderson, 2002) that can negatively impact network communication on a large scale through denial-of-service, traffic redirection, increase in spam, and information disclosure via stolen traffic (Mcarthur & Guirguis, 2009). The Department of Homeland Security (Bullock et al., 2015) and the Federal Communications Commission (FCC, 2012) have both clearly defined this issue to be of great importance .

There have been several proposed solutions to protecting the authenticity and validity of BGP routing updates (Bruhadeshwar, Kulkarni, & Liu, 2011; Hu, Perrig, & Sirbu, 2004; J. Israr, Guennoun, Mouftah, & Rahman, 2010; Kent, Lynn, & Seo, 2000; Malhotra & Goldberg, 2014; White, 2003; Ying, Zheng, Mao, & Hu, 2009). However, these proposed solutions introduced significant system overhead or had poor adoption rates (Butler, Farley, McDaniel, & Rexford, 2010). Furthermore, according to Butler

(2010), little has been done to assess the security implications of routing BGP over IPv6 and using IPv6 extensions to mitigate risks associated with the trust model of BGP. Therefore, the specific problem is that the interdomain routing protocol used in the Internet lacks a method for performing route attestation without introducing unacceptable amounts of overhead, nor do proposed solutions address IPv6's impact in terms of added efficiencies and built-in security solutions such as IPSec.

The study focused on observing an ecosystem of virtualized routers in an environment that was controlled by the researcher and measured to study performance impacts of participating routers. Virtual routers followed the same rule-sets and purpose of a traditional physical router, but existed entirely in software. This allowed the study to be expanded without requiring additional equipment and the costs associated with it. The process of routing via BGP is not dependent on physical equipment; rather the process and instructions are defined in software. Routers were be measured in normal or typical operation to gain a baseline of performance impacts in an uninfluenced environment. The researcher then introduced the prosed model to mitigate sub-prefix hijacking attacks using IPv6 and evaluated the resulting impact and effectiveness.

Purpose of the Study

The purpose of this quasi-experimental before-and-after study was to measure the feasibility of using IPv6 extension headers in an effort to validate the authenticity of a BGP routing update and describe the performance implications or overhead of doing so. In order to accomplish this goal, a security model was built to leverage IPv6 extension headers in a controlled environment to first determine the feasibility of detecting specific BGP sub-prefix hijacking attacks and secondly mark the appropriate route updates as invalid. Selecting only BGP sub-prefix hijacking attacks significantly narrowed down

the scope of the research while also providing a framework by which BGP events were selected or created for observation. The study was also by nature iterative as it may be repeated with other types of attacks against the BGP protocol.

Significance of the Study

BGP is the de-facto-standard Internet routing protocol and impacts nearly all traffic flowing across the Internet (Hawkinson & Bates, 1996). As Phillipa, Michael, and Sharon (2013) indicate, BGP is the Internet's routing protocol, it is absolutely critical to the operation of the Internet (Mahajan et al., 2002). This includes impacts to users, businesses, governments, and others. Considering the role BGP plays as the Internet's routing protocol, the nature of interdomain routing, and multudinous vulnerabilities, Ola and Constantinos (2004), suggested that successful attacks on BGP can affect signficant numbers of people on a global scale.

IPv6 is replacing IPv4 infrastructure as address space has become quite scarce with many exhaustion milestones being already reached (Jakub et al., 2014). Jakub et al. (2014) noted that nearly every measure of IPv6 adoption has increased by an order of magnitude. With IPv4 address acquisition costs rising and the total available IPv4 addresses shrinking to below 4% remaining, researchers predict that a continued growh of IPv6 and an exhaustion of IPv4 addresses by 2018 (Sebastian, Lachlan, & Grenville, 2014). As a result of the forthcoming exhaustion of IPv4, Internet users and providers alike will have no choice but to begin adoping and actively implementing IPv6 support across their infrastructure.

As sub-prefix hijacking is a significant threat to BGP infrastructure, numerous solutions have been proposed (Bruhadeshwar et al., 2011; Hu et al., 2004; J. Israr et al., 2010; Kent et al., 2000; Malhotra & Goldberg, 2014; White, 2003; Ying et al., 2009).

This study expanded upon the existing research that has been done to improve the security posture of autonomous systems participating in BGP against sub-prefix hijacking attacks. As suggested by Ballani et. al. (2007), there are significant issues associated with solutions to sub-prefix hijacking that need to be rethought and solved.

Due to the already widespread usage of BGP, rising adoptation rates of IPv6, and clear need to revise existing sub-prefix hijacking mitigation methods, this research resides in a highly desirable area. The maturity of IPv6 is developing, as IPv4 address space is limited, and with that protocol stability and efficiences are rising as well (Jakub et al., 2015). Standardization by organizations comprised of network designers, operators, vendors, and researchers on an international scale such as the Internet Engineering Task Force (IETF) shape the way Internet protocols work (Alvestrand, 2004). Proposals to replace the BGP protocol, such as the Inter Domain Routing Protocol (IDRP), have gained little traction and have never been standardized by the IETF making them obsolete (Savola, 2005). From these assertations, the state of inter-domain routing showed a clear need for further research in mitigating specific threats to BGP routing such as sub-prefix hijacking over maturing IP standards as the potential for detrimental impacts is grand.

Nature of the Study

Guided by the proposed research question, the data to be gathered in this study was numerical and analyzed from a pre and post application assessment. According to Creswell (2009) research surrounding experimental design resulting in numeric data to study are best suited under quantitative research. Creswell developed this appropriation of quantitative research methods to the study by specifically outlining their quality of use in performance analysis of systems. This was appropriate as it directly matches the

desired outcomes of the study: to measure the resulting performance impact of using IPv6 extension headers in a model that performs BGP route attestation.

For this study, a quantitative experimental approach was used over other designs such as non-experimental studies or semi-experimental studies. While there are numerous ways to analyze this issue and measure the results of the proposed model numerically, the experimental approach to the study met the needs in accordance with the nature of the study. According to Creswell (2009), the research design is a platform to shape the plans and procedures for a researcher to follow. Therefore, these plans and procedures served as the guiding direction for the data collection of the study along with the analysis of that information. In this study, the models common to other research in the field was adapted to meet the specific requirements outlined in this proposal.

Furthermore, an experimental study will provide a framework for obtaining the desired measurements when evaluating the problem statement of this research. As Keppel and Wickens (2004) describe, an experimental research design encompasses two treatment conditions. The subjects in each condition are treated the same except for one single change is introduced, and the effects are measured after the researcher's intervention. By the nature of what an experiment is, if there was only one change introduced while everything else was kept identical, the measurable observation must have been caused the single introduced change.

In choosing the design of the experimental study, Kumar (2005) suggested analyzing the problem from three different perspectives. These perspectives prompted the researcher to evaluate how many contacts he or she was to have with the subjects, the reference period of the study, and lastly the nature of the study. The result being a deeper review of methodologies as the focus is narrowed. As this study was highly technical in

nature and the analysis was performed in pre-measurement, application of research model, and post measurement, the design of the study was reviewed from the perspective of the nature of the investigation.

Within the categorization of the nature of the investigation, there are three relating study designs: experimental, non-experimental, and semi-experimental (Kumar, 2005). Experimental studies are those where a researcher introduces an intervention in a controlled environment expecting to observe a change, and measuring the change when it happens. Non-experimental studies a researcher attempts to retroactively determine the cause for already observed changes. This study was proactive in the sense that the perceived outcomes had not already been observed, but were to be induced by the researcher's influence; therefore, non-experimental design was not appropriate in this case. Lastly, semi-experimental designs contain properties of both experimental and non-experimental studies. Again, as this study was not focused on the retroactive causation of an observable event, a semi-experimental design was not the best suited.

When further defining the experimental strategy to be used in this study, it was important to consider the desired data to be collected and analyzed. The study was largely focused on measuring the performance impact in a scalable security solution to defending BGP against sub-prefix hijack attacks. As discussed, performance metrics in this type of environment can be easily measured qualitatively. Experimental research that is qualitative can be further separated out into true experiments where subjects are randomly chosen and quasi-experimental where subjects are nonrandomized (Creswell, 2009). As the experimental study was performed in a controlled environment and variables were measured before and after the administration of a researcher-imposed

technical change, the randomization of subjects was not necessary. As a result, the quasi-experimental classification was used.

With respect to the quasi-experimental research design of this study, it was important to define a design that will guide the collection of data and analysis to determine the resulting outcome. While many quasi-experimental research designs exist, a before-and-after design was used. This design dictated that a state of the variables were to be measured before the intervention and then again after the intervention (Kumar, 2005). These measurements formed the ground for analysis of the data. The data represented the quantitative change in performance of a router participating in the BGP sub-prefix hijacking mitigation model using IPv6 headers for transport of route attestation information. A before-and-after design does have certain limitations that are discussed in a future section.

Research Questions

This study focused on one primary research question. The primary research objective was to determine if IPv6 extension headers are used in a model to validate BGP route updates received from a peer router, what the resulting impact in terms of overhead on the participating router were. Therefore, the use of this research is to determine if IPv6 extension headers are a viable tool to mitigate BGP sub-prefix hijacking attacks by performing route attestation, while introducing minimal overhead.

The purpose statement of this study was specified that the research conducted will measure the effectiveness of a proposed model using IPv6 extension headers to mitigate BGP sub-prefix hijacking attacks. To effectively measure this and focus the research, the following question focused the research:

> In a model where IPv6 extension headers are used to successfully perform route attestation of BGP updates, what is the resulting degree of difference exists in terms of router CPU utilization percentage, RAM utilization percentage, route convergence time, and BGP update packet size in comparison to a router not participating in the model?

The above question was used to derive results indicating whether IPv6 extension headers are capable of carrying the necessary information to perform basic BGP route attestation. With a limited amount of space in each IPv6 datagram header, the necessary information to perform route attestation such as authorization of origin had a restricted data size. The model proposed was designed to perform lightweight route validation. The consequential hypothesis of this question was that given a model designed to perform lightweight route attestation, necessary information to perform the task may be carried inside of IPv6 extension headers within constraints defined by the protocol specification without imparting performance overhead.

Furthermore, the research question guided the measurement of the performance impact on the routers participating in the model. Performance impact was measured in terms of CPU usage, RAM consumption, route convergence time, and route update packet size.

Guided by the above question, quantitative measurements were gathered on the model's impact in performance overhead of participating routers. These results, when compared to results gathered of a non-participating router clearly identified the impact of the proposed model. This methodology followed the literature covering experimental design and the measurement of researcher introduced changes in such models (Keppel & Wickens, 2004; Kumar, 2005). The follow-on hypothesis derived from this research

question stated that route attestation will result in performance overhead, but be minimized by the use of IPv6 extension headers due to the protocol improvements compared to IPv4 implementations and eliminating the need to carry attestation information in separate packets.

A hypothesis is defined by Salkind (2010) as a tentative statement describing the relationship between variables in a study. The uncertainty or tentativeness of such statement leads into the purpose of research, to empirically analyze and observe such relationship and report on those findings. Given such definition of hypothesis, one can infer that it is not the duty of the researcher to prove the hypothesis true. Rather, it is the researcher's onus to evaluate the hypothesis given the constraints and paradigms that it defines.

Theoretical Framework

Theoretical frameworks as defined by Kumar (2005) are a place of grounding or basis upon which research is conducted. These frameworks and ideas come from a paradoxical explanation that surveying the literature related to a topic will reveal general theories, which can be intertwined into a theoretical framework; yet choosing the right literature to survey is dictated by the chosen theoretical basis. The basis of the theoretical framework that the research will follow stems from a loosely defined framework compiled from ideas presented in relevant literature. As Bryant (2004) noted, the framework will further develop from loose theories into a better-defined guide. From this guide or theoretical framework, the research here was better scoped and more likely to contribute to the intended areas.

The goal of this study was to determine if IPv6 extension headers could be used in a model to perform BGP route attestation while introducing minimal overhead due to

efficiencies in IPv6. According to Lammle (2013) IPv6 brings many enhancements to the IPv4 protocol suite in terms of header structure, address space, field alignment, and includes by default many of the features of IPv4 that were amendments during its lifespan. These enhancements in IPv6, in general, state that packets traversing a pure IPv6 network are more likely to be processed and transmitted in a shorter amount of time when compared to their IPv4 counter parts.

IPv6 extension headers may be able to carry BGP route attestation information sufficiently. In contrast to IPv4 headers where static fields were required and length limitations were imposed, IPv6 allows for optional headers of variable length (Lammle, 2013). The format and design of IPv6 extension headers allows for a faster processing time and more dynamic control of information assigned in each header. In addition, only the destination routers or devices need to process the IPv6 headers, intermediary devices do not (Carpenter & Jiang, 2013).

One way of measuring IPv6 packet efficiency and comparing it to IPv4 in addition to router CPU and memory consumption is measuring the round-trip time (RTT). In studies, IPv6 packets have a smaller round-trip time than IPv4 packets (Yi, Shaozhi, & Xing, 2005) indicating a performance increase than when compared to IPv4. The study performed by Yi et al. demonstrated that in implemented testing scenarios of real unicast data used to mimic web browsing that IPv6 showed a consistently lower RTT compared to IPv4. Unicast packets are the same type of packets that BGP utilizes to exchange route updates, so it was reasonable to suggest the same performance generalization would be seen in BGP route updates while using IPv6.

Definitions

Autonomous System: "An AS is a connected group of one or more IP prefixes run by one or more network operators which has a SINGLE and CLEARLY DEFINED routing policy." (Hawkinson & Bates, 1996)

Control Plane: Path determination part of the routing process where a route from a source is determined to a given destination. (Schuchard et al., 2010)

Data Plane: The part of the routing process where packets are actually forwarded to their destination.(Schuchard et al., 2010)

Interdomain Routing: Moving packets from a device in one autonomous system to a device in another autonomous system.

Overhead: The measurement of additional CPU consumption, memory consumption, route convergence time.

Prefix: "The term "prefix" as it is used here is equivalent to "CIDR block", and in simple terms may be thought of as a group of one or more networks. We use the term "network" to mean classful network, or "A, B, C network"." (Hawkinson & Bates, 1996)

Round-trip Time: The time it takes a packet to be sent to a destination combined with time it takes for the destination to acknowledge the receipt of the packet. (Grigorik, 2013)

Routing: Moving a packet from one device on a network and moving it to a device on a different network (Lammle, 2013)

Route Attestation: A system or process used to guarantee the authenticity and correctness of a routing update. (Qi et al., 2012)

Assumptions

There is no research study that is completely perfect in its design, approach, or certainty; for that reason, a researcher must make assumptions about the study (Bryant, 2004). It is assumed that the measurements taken from the perspective of the participating routers and the overall environment as it converges new route updates was an accurate reflection of the imposed changes to the routing process by the researcher. For example, when the routing engine was modified to leverage the IPv6 headers in carrying route attestation information, the overhead measurements were a direct result of the changed process not coming from an external variable. To control this as best as possible, a virtual environment with dedicated resources was used in a sandbox-type setup. The study was based on open source implementations of the BGP routing architecture for ease of manipulation when compared to proprietary or closed-source solutions. With the open sourced implementations, the study assumed that they were following the proper BGP-4 specifications and using a standardized approach to route processing.

Scope, Limitations, and Delimitations

Scope

The scope of this study was to explore the feasibility of using an IPv6 oriented model to perform route attestation while introducing minimal performance overhead to participating devices. The study used a subset of virtual appliances running open source BGP routing engines to process and enable route updates. The virtual appliances combined with open source software in a controlled environment gave the researcher control of variables being studied as external influences could be minimized in this type of scheme. These virtual routing appliances were configured to use the same hardware

resources, software versions, and configurations to ensure consistency across the devices. The study was not scoped to evaluate the solutions on other hardware platforms, vendor equipment, against routing protocols other than BGP-4, or closed-source software. The rational for excluding the other solutions was that if all participating devices in BGP properly follow the specification of the protocol, it is reasonable to believe that the rules, processes, and procedures for processing BGP route information would be standardized. The routing updates and traffic generated in the environment were controlled by the researcher in an effort to identify if the proposed solution solved the sub-prefix hijacking problem, and what the impact of that solution was. If the study were to use real BGP traffic collected from nodes in the Internet, additional variables, complexities, external influences, and difficulty in accurately identifying sub-prefix hijacking attacks would introduced. These complexities would degrade the purity of the observations taken during the study.

Limitations

Since a control group was not used, a limitation of this quasi-experimental before-and-after study is that the results may not be completely conclusive in whole or in part. This means that the changes discovered through the study possibly only revealed a true change in part or in entirety. In this scenario, control groups were extremely difficult to introduce into the study as variables may have changed between iterations of the researcher's intervention. Furthermore, if the subjects being studied are as close to identical in nature as possible, the random selection of certain subjects is not necessary. As Keppel and Wickens (2004) indicated, perfection is impossible as no two subjects can be exactly the same. The goal in light of Keppel's statement was to minimize any nuisance variables and eliminate confusion that may cause comparisons to be skewed.

Examples of nuisance variables in the study include: the load on the infrastructure supporting the virtual environment may change, the systems could be processing different tasks, etc. In addition, as Keppel and Wickens (2004) suggest with quasi-experimental studies, the statistical methods do not pose much of a challenge in evaluating results. On the other hand, the results need to be interpreted carefully as some incidental characteristics in the group may affect the measurements.

The study was limited to capturing data from routers participating in a controlled and segregated environment. This type of scenario does not allow for external influences, multiple malicious actors, scalability, or as high of volumes of BGP traffic that may be seen on the public Internet. Furthermore, as the BGP traffic was generated and controlled by the researcher, it is expected that the BGP updates followed specification and were not malformed. Malformed traffic may still introduce a change into the BGP environment, but due to its unpredictability, it could not be accounted for reasonably.

Delimitations

The data collected in this study originated from a pure IPv6 environment between participating routers. Realistically on the Internet, there is a mix of IPv4 traffic and IPv6 traffic. A single network environment that has implementations of both the IPv4 and IPv6 protocols within may be referred to as a "dual stack" network because it uses the IPv4 stack alongside of the IPv6 stack. The two instantiations of the protocol are able to communicate with different configurations such as 4to6 tunnels or ISATAP tunnels alongside of many other tunneling technologies (Punithavathani & Radley, 2014). These types of tunnels are designed to allow traffic existing in an IPv4 network to communicate with hosts on an IPv6 network and vice versa through a single router (Horley, 2014).

Effectively, one type of IP traffic may be encapsulated into the other, which could affect the appearance of the BGP messages.

As the study focused on only virtual routers in an environment that is guarded from external influences, the results may change when the same factors are applied to a physical environment. Some factors that exist in a physical environment are not present in the virtual space. While the study focused on the software aspects of BGP routing, it is important to consider the physical aspects when the scope shifts to universal evaluations.

Closed-source software and proprietary vendor implementations of the BGP-4 protocol might not all be following the specification or standardization. This means that they may process BGP messages differently than what was observed in this particular environment, potentially introducing changes in the experiential results.

Additionally, the study was only focused on assessing the model in a VMware ESXi virtualization platform. Other Hypervisors may treat the virtual routers differently, impose limitations on CPU throughput, and process the data differently. If the exact virtual appliances are imported into a different virtual environment, the outcomes could change due to the aforementioned characteristics of hypervisors.

Summary

Chapter 1 provided the objectives necessary to navigate through a quasi-experimental before-and-after study. Evaluation of the deficiencies and potential impacts of implementing a secure BGP implementation were investigated in this chapter (Butler et al., 2010; Lychev et al., 2013; Ming, 2006). This chapter identified an opportunity for further research to be performed in the IPv6 space as it may be used to better the security posture of BGP (Butler et al., 2010). It identified the wide-spread usage of BGP (Jakub et al., 2014) and those users as the stakeholders in the study. Furthermore, the chapter

recognized the scientific and social impacts of the study, demonstrating significance of the contributions to the field.

The theoretical framework of the study formed the basis for which the study was to be conducted and was discussed in this chapter. It has been proven that IPv6 offers efficiencies over its IPv4 counterpart (Lammle, 2013) and the movement towards IPv6 shows a positive trend in adoption rates (Jakub et al., 2014). Those efficiencies coupled with highly adopted BGP security models (Gersch & Massey, 2013; Kent et al., 2000; Wählisch, Maennel, & Schmidt, 2012) contributed to the theoretical framework. Through the realized performance impacts of IPv6 and suggested models, the research questions can be formulated and solutions evaluated.

The quasi-experimental before-and-after research design was adopted for this study and was determined to be an effective instrument for evaluating the research question (Kumar, 2005). The study was scoped and limitations or delimitations that may affect the reproducibility or universality of the study were identified.

Chapter 2 encompasses a literature review that is an all-embracing summary of the state of BGP security, proposed solutions, evaluation taxonomies, and resources pertaining to performance penalties and their measurement. The literature review will provide the background and base information required for the study. In addition, Chapter 2 will provide a historical overview of existing BGP security solutions, their shortcomings, and any existing gaps in the literature addressed. Lastly, a surveying of articles, journals, books, and additional research materials gathered for the study is presented.

CHAPTER 2: LITERATURE REVIEW

Chapter 1 produced the topic of this dissertation: using IPv6 to perform BGP route attestation and measuring the resulting overhead. The chapter also demonstrated the significance of the study as it relates to the widespread usage of the BGP-4 protocol and potential outcomes of compromised BGP traffic. Also included in Chapter 1 is the study's background, problem statement, significance, research questions, and research design. Chapter 2 surveys the literature surrounding the study and provides insight into the operation of BGP, supporting information on IPv6, network prefix context, existing route attestation models, observation and inspection planes, and similar cryptographic solutions. The chapter studies vulnerabilities in BGP as they relate to sub-prefix hijacking as well as motivations and challenges with attribution to attackers. In continuation, Chapter 2 will provide insight into the causes behind low adoption rates of existing security solutions for BGP and the viewpoints of administrative domain operators on the prioritization of adopting a security solution. Lastly, the literature review will provide a means of measuring overhead in routing convergence and cryptographic solutions to give way to measurements of the impact of the solution.

The purpose of the quasi-experimental study was to measure the impact of using IPv6 in a model that performs BGP route attestation to defend against sub-prefix hijacking attacks. Chapter 2 stages formerly proposed and currently implemented solutions of BGP security models at the time of this study such as S-BGP (Kent et al., 2000) and RPKI (Wählisch et al., 2012). Also, the chapter builds an area of observation on what will make a security solution adoptable by evaluating studies of those who are to implement them (Lychev et al., 2013).

Design and Operation of BGP

Since its introduction in 1989 (Lougheed & Rekhter, 1989), BGP has evolved through many changes into its current version, BGP-4. BGP offers Internet peers a way to route information between each other without a central core; that is, they can make decisions based on information gained from their neighbors. Subsequent releases of BGP include BGP-2 (Kirk Lougheed & Yakov Rekhter, 1991) and BGP-3 (K Lougheed & Y Rekhter, 1991) which contained refinements to the preceding protocol specifications. BGP-4, the currently used version of BGP at the time of this research, was first seen on the Internet in 1993, and refined through other Request for Comments (RFCs) including RFC1771 in 1995 and RFC4271 in 2006 (G. Huston, Rossi, & Armitage, 2011). BGP routing tables have grown in population alongside of the protocol as have the number of participating devices since its introduction.

In the introduction of the Secure Border Gateway Protocol (S-BGP), Kent et al. (2000) defined the security for BGP as the intended and truthful operation of BGP. Kent's description of secure operation also alluded to a need for route attestation. For that reason, it was important to understand how BGP operates in an ideal environment. The understanding of BGP's normal operation and processing of functional messages also revealed weaknesses in the design of the protocol that allow for attacks such as sub-prefix hijacking to be carried out.

At a high level, BGP has two main jobs: mapping an IP address prefix to an autonomous system, and building paths between a specified source and a reachable destination (Bruhadeshwar et al., 2011). A BGP speaking autonomous system is able to advertise its ownership of a prefix by sending an update message to its neighboring peers. When a peer receives an update message, it will recursively concatenate its own

autonomous system number to the update and pass the newly formed update out to its peers. The result of this concatenation and redistribution of update messages is that each peer that receives the update will attain an association of a network prefix and a list of autonomous systems that traffic will need to traverse to get to the prefix. The path aggregation can be represented by the following formula $(P, [AS_k\ AS_{k-1}\ AS_0)$ where P is the network prefix, AS_0 is the origin of the route, and the other AS represent the nodes along the path. It is critically important to the operation of BGP that these messages retain their integrity while traversing the Internet (J. Israr et al., 2010). Additionally, since an update is only able to specify a single path, only routers that also share that path may be aggregated into the update message (Kent et al., 2000). When a router receives multiple update messages for the same prefix, it will make a selection based on its configuration and routing policies.

Kent et al. (2000) further defined the correct operation of BGP and associate integrity, timeliness, and authenticity of BGP updates as functional requisites. To recapitulate the idealized or correct operation of BGP as outlined (Kent et al., 2000), the following statements are made:

- Every BGP update received by a participating router is assumed to have originated from the indicated peer; that is, it was not tampered with in transit. This update is also expected to be more current than other previously received routing information for prefixes from that peer. An outdated update will have little use and may negatively affect operation of BGP.
- Each update is received by the intended recipient. The updates are not redirected or lost in transit to the intended recipient.

- A BGP update will originate only from a peer that is authorized to act on behalf of an autonomous system to advertise the routing information contained within.
- The owner of a network prefix was authorized by its parent organization to state that it owns the prefix.
- The first AS in the route is authorized to advertise the prefixes by the owners of the address space.
- Route withdrawal advertisements should originate from a peer that was authorized to advertise the route before the withdrawal was issued.
- The BGP peer that the update message is sent from should correctly apply the information abiding by the BGP rules and policies in its configuration. These rules and policies dictate how the route should be stored, updated, or redistributed as well as if it should be selected or any information can be derived from it.
- Lastly, a recipient of a BGP update message should correctly apply the rules and policies in its configuration as to whether or not the route should be accepted.

The above statements concisely capture the intended operation of BGP. A deviation from these rules indicate a failure in the proper operation and form the base from which the vulnerabilities in the protocol stem.

One area that remained untouched from Kent's rules on the correct BGP operation is how a router processes or selects a route learned from an update. The selection of a route is designed to determine the "best" announcement that can be subsequently

advertised to peers. This process of determining what route is "best" happens through an ordered system of evaluations summarized with the following selection routines (Junaid Israr, 2012; Y Rekhter, Li, & Hares, 2006):

1. A route with a more specific (longer) address prefix is chosen over that of a covering (smaller) address prefix for the same network blocks.
2. The route with the highest value for local-preference is selected. Local-preference is an attribute locally calculated by a recipient of a BGP update message factoring in the locally configured policy.
3. Next, the route with the shortest AS_PATH attribute, a mandatory attribute of BGP update messages. The AS_PATH represents a list or sequence of autonomous systems that the update messages has traversed. Effectively, a smaller number of autonomous systems to pass through is preferred.
4. A route with the lowest multi-exit discriminator (MULTI_EXIT_DISC) attribute will be chosen next. MULTI_EXIST_DISC is an optional attribute in BGP update messages that gives a hint as to what the best path is to an autonomous system with multiple entry points. A lower value for this attribute indicates a more preferable path to choose.
5. If a route to a particular destination network also has an associated Interior Gateway Protocol (IGP) with a lower cost to the next hop, it will be chosen.
6. External Border Gateway Protocol (eBGP) routes are chosen over Internal Border Gateway Protocol (iBGP) routes.

7. Lastly, if iBGP must be used, the route with the lowest BGP identifier value is chosen. A BGP identifier is a numeric representation of a BGP speaker that matches an IP address assigned on that host. This value is calculated on startup.

An understanding of the BGP's intended operation and route selection process revealed areas where the protocol exhibits weaknesses that can be exploited. For example, if a router violates these properties by advertising a prefix that it is unauthorized to do so and the illegitimate prefix is longer than existing routes for the covering prefix, a sub-prefix hijacking attack can occur. By violating these properties, attackers are able to exploit the protocol, as sufficient checks do not exist within the design of the protocol for such deviation.

Distance Vector and Link-State Protocols

The determination of how a routing protocol selects the best path to a destination can be used to classify the protocol into one of two categories: distance vector routing protocols and link state routing protocols (Lammle, 2013). BGP is most closely related to distance vector protocols in the way that it computes various paths to an intended destination. BGP is sometimes referred to as a path-vector protocol. At a high level, distance vector protocols such as BGP calculate a cost to each destination it knows about and sends that cost as a vector to its neighbors. Essentially, distance vector protocols tell neighboring routers what the world looks like from the standpoint of the originating router (Zhao, 2002). On the other hand, link-state routing protocols operate slightly differently and task participating routers to calculate their own best route to a destination using metrics like link speed or availability. According to Zhao (2002), link-state routing protocols flood information about what neighbors they see as raw information; they tell

the world who the neighbors are. Since BGP operates in a space where route updates are composed of aggregate information from an arbitrary number of routers, some of which may not be trusted, it is much more difficult to detect invalid updates than if it used raw routing information.

Vulnerabilities of BGP

Coupled with its age, BGP has several documented and known vulnerabilities that exist within its design and operation that make it vulnerable protocol (Geoff Huston & Michaelson, 2012). BGP has been attacked and compromised as seen in the previously documented examples (Bornhauser & Martini, 2011; Sun et al., 2015; Yun & Song, 2015). Many of the vulnerabilities in BGP stem from three central areas. These areas include the lack of transitive BGP authenticity, freshness, and validity mechanisms from the source of the update through the end node receiving the message. Additionally, BGP offers no solution to validate the authenticity of an advertised network prefix. Lastly, BGP does not have any controls to validate that an update message has not been tampered with throughout its travel or to verify the messages' integrity. Other researchers such as G. Huston et al. (2011) suggested additional vulnerabilities exist in the design of BGP as it has no mechanism to verify its routing information base (RIB) is accurate and up-to-date.

These vulnerabilities may be taken advantage of by malicious actors even unintentionally introduced via misconfigurations. Outside of the neighbor establishment and selection process of BGP, little is done to prevent an autonomous system from faking their prefix ownership, intercepting and tampering with BGP update messages, or posing as another autonomous system number. Either intentionally or accidentally, these principles and flaws within BGP have the ability to significantly disrupt network

resources if introduced. The following subsections will cover BGP vulnerabilities as they pertain to outsider and insider threats, attacker incentives to target BGP, and the sub-prefix hijacking attack method.

Outsider and Insider Threats

By design, BGP operates in a heterogeneous environment, one that contains other peers speaking BGP, but also different protocols such as OSPF and EIGRP. In this environment, BGP will be impacted by decisions made inside and outside of an autonomous system (Zhao, 2002). These two different vantage points raise different concerns when assessing the level of access an administrator may have or what trust relationships exist. Outsider threats to BGP may include a remote autonomous system advertising invalid routing updates that can affect the reachability or integrity of traffic. These types of threats may be actualized by using BGP or any of the other protocols existing in the heterogeneous environment. Therefore, it can be stated that a routing protocol such as BGP is only as secure as the weakest link. Insider threats can introduce the same types of security concerns as outsiders, although they may be harder to detect according to Zhao (2002). An insider may have a greater level of trust, access to private cryptographic keys, and the ability to answer security inquiries correctly.

Incentives to Attack BGP

Since BGP's introduction, the shift in mentality has moved from trusting internal devices and assuming threats reside outside of the network to the realization that threats exist both internally and externally. This paradigm has resulted in autonomous systems operating in the BGP space to slip from the typical operation of BGP knowingly or otherwise. While it is difficult or even impossible to determine the exact cause, motivation, and intent for a malicious entity to leverage weaknesses in BGP for their own

gain, previously documented attacks on BPG can shed some light onto the subject. Junaid Israr (2012) asserted reasons relating to financial, technical limitations of address space, misconfigurations, as well as political.

Economic and financial incentives may be enough incentive for an entity to perform an attack against BGP. It is known that autonomous systems are typically registered by an organization, some of which may be for-profit and competing organizations (Junaid Israr, 2012). Since these organizations need to maintain an online presence participation in BGP is often times necessary. An autonomous system participating in BGP may falsely represent certain networks or destinations in favor of those that are more economically favorable for them. In addition, if an entity is able to intercept network traffic intended for another, they may be able to learn traffic patterns, affect quality of service, or obtain proprietary/sensitive information.

Depletion of IPv4 addresses is a documented and well-known challenge facing organizations with an online presence. Organizations have been allocated blocks of IP addresses in the limited IPv4 space, and may have more available addresses than they are using or intend to use (Geoff Huston & Bush, 2011). The scrutiny of these organizations increases as the depletion of IPv4 addresses becomes more prominent. While IPv6 solutions do exist to the IPv4 limited address space, online partakers may use BGP to illegally take over the unused IPv4 addresses.

Misconfigurations happen in many different ways, and BGP is not immune to the effects of human error. A prime example of a misconfiguration in BGP affecting users unintentionally was seen in the Pakistani YouTube incident (Bornhauser & Martini, 2011). While the state-owned ISP in Pakistan introduced a BGP update affecting the YouTube prefix, it was accidentally advertised outwards towards the ISP's neighbors.

The invalid advertisement affected traffic intended for YouTube in certain regions making it unreachable. The invalid route update was detected after only 5 minutes; however, it took over two hours and the teamwork of multiple sites to fully restore access to YouTube.

Man-in-the-Middle and denial of service (DoS) attacks can be initialized by autonomous systems acting maliciously. An autonomous system owner may want to intercept or black-hole network traffic for a variety of reasons. Some of the motivations for performing such an attack could be security, surveillance, and other harmful intents. In this type of an attack, an autonomous system would falsely identify the ownership or best path to reach an intended destination such that network traffic would be misdirected through their environment. Once the traffic enters the malicious entities environment, the outcomes and degrees of impact are limitless.

Network Prefixes and Sub-Prefix Hijacking

Among the many vulnerabilities within BGP, this study focused primarily on sub-prefix hijacking attacks. These attacks take advantage of the BGP attribute referred to as the "longest prefix match" property. An understanding of network prefixes or subnets is required to understand the vulnerability, and how attackers are able to take advantage of it. This section will outline network prefixes as they exist on the Internet and tie back to the BGP longest-prefix match property.

In both IPv4 and IPv6, network IP addresses are representations of 32-bit and 128-bit binary numbers respectively. Human interaction with IP addresses is not typically in the form of binary numbers; rather, the numbers are represented by decimal in IPv4 and hexadecimal in IPv6 for ease of readability, memorization, and other ease-of-use factors (Lammle, 2013). In an IPv4 address, the 32-bit binary number is divided out

into four separate groups called octets. An octet represents eight binary bits converted into a single integer. These four resulting octets (decimal numbers) are concatenated by periods or dots, and the grouping of the octets is referred to as dotted-decimal notation (Butler et al., 2010). Dotted-decimal notation is the common representation of an IPv4 address. For example, a network host address may be assigned the IP address of 192.168.1.1, which is the dotted decimal notation of the following binary sequence: 11000000101010000000000100000001. IPv6 addresses work much in the same way; however, instead of 32 bits IPv6 uses 128 bits and represents the address as eight groups of four hexadecimal digits per group with the groups separated by colons. An example IPv6 address may look like the following: 2600:1014:b109:55f0:505a:d94f:203c:55f. It is clear to see that the dotted-decimal notation or IPv6 notation is easier to work with than a binary string from a human standpoint. Regardless of the representation or address type, the underlying bits are very important to BGP when considering its longest prefix match property.

IP addresses typically belong to a larger logical grouping of address space called a subnet or a network prefix. For the remainder of the section, the following terms are interchangeably used to represent network prefix: subnet, address group, network block and address block. There are many ways to represent a network prefix in IPv4, but one common method is Classless Interdomain Routing (CIDR) notation. CIDR is a method for representing a network prefix by taking the first IP address in the network block, appending a forward slash (/), and specifying how many bits of the address represent the network (Fuller, Li, Yu, & Varadhan, 1993). For example, a prefix represented as 192.168.1.0/24 in CIDR notation, means that the first address in the network block is 192.168.1.0 and the first 24 bits (three octets or 192, 168, and 1) represent the network.

The remaining 8 bits or the fourth octet in this example can be used for hosts within the network as their IP address.

On the public internet, organizations used to receive IP address blocks directly from the Internet Assigned Numbers Authority (IANA) who has offloaded such duties to the Internet Corporation for Assigned Names and Numbers (ICANN). The duties of assigning IP address blocks has been further separated out in to regional registries that also have the ability to delegate address block assignment in a hierarchical manner (Butler et al., 2010). An example of a regional registry is the American Registry for Internet Numbers (ARIN) who manages prefix assignment in North America. Due to the hierarchical structure of IP address space assignment, it is possible that a network prefix assigned to an organization will belong to a larger network prefix at a higher level. For example, if an organization is assigned an address block such as 138.247.80.0/24, it may have been delegated by the organization that maintains ownership of 138.247.0.0/16. In this scenario, the shorter prefix 138.247.0.0/16 contains the longer prefix 138.247.80.0/24, and is called a cover network. By design of the BGP protocol, if both networks were to exist in a routing table, BGP will look for the route with the longest or more specific prefix in making its routing decision according to Butler et al. (2010). This property and design are what allows for sub-prefix hijacking, where a malicious entity may advertise longer network prefixes knowing that they are more likely to be used by BGP.

Survey of Cryptographic Solutions in BGP

A survey of existing BGP security mechanisms brought to light different cryptographic solutions that have been implemented to address vulnerabilities within the protocol. These solutions aim to enhance the security of BGP by providing for

authentication and protection against the interception and tampering of BGP updates in transit. This section will give an overview of popular solutions while evaluating their characteristics in ease of use and added overheard including the following: pairwise keying, hash functions, message authentication codes (MAC), Diffie-Hellman key negotiation, public key infrastructure (PKI), public key cryptography, route attestations with certificates, and IPsec.

Pairwise Keying

Pairwise keying is a cryptographic solution intended to provide for authentication between neighboring nodes. Two nodes or in this case, BGP routers, will establish a shared secret key prior to exchanging route updates (López & Zhou, 2008). While pairwise keying does allow for authentication between nodes, the key management process introduces a significant amount of overhead. Butler Butler et al. (2010) asserted that the runtime or complexity of pairwise key management can be described as $O(n^2)$. This affects scalability and overall management particularly when implemented in large-scale BGP on the Internet. Furthermore, if keys are not frequently changed, they are subject to exposure through cryptanalysis and disclosure amongst personnel that know the secret keys (Butler et al., 2010).

Hash Functions

Digest algorithms or cryptographic hash functions aim to provide a check for message integrity in BGP security solutions The idea of a hash function is that input text is used as a seed to perform some mathematical computation resulting in a unique, nonreversible signature (Al-Hamami, 2014). As Al-Hamami (2014) noted, these hash functions can be described as a one-way function as the resulting signature cannot be used to obtain the original input text. Common hashing functions seen in BGP security

include the Message-Digest 5 (MD5) algorithm (Rivest, 1992) as well as those in the Secure Hashing Algorithm (SHA) classification (Gutierrez, Gallagher, & Director, 2008), especially SHA-1 (Junaid Israr, 2012). A faulting property of hash functions is that two sets of input text may produce the same output hash message; this property is called a collision. When referring to the strength of a hashing algorithm, strength describes the difficulty in using the hash to obtain the original text without running into collisions (Butler et al., 2010). More complex hashing algorithms typically introduce higher levels of computational overhead in comparison to their weaker counterparts.

Message Authentication Codes (MAC)

Message Authentication Codes (MAC) are used in BGP security to provide for integrity checking of a message as well as authenticity for the sending node (Al-Hamami, 2014). Authorized or participating parties should have access to a shared secret key. This key along with the message are fed into a mathematical computation to produce the MAC. When the sending node issues an update or BGP message, the MAC is typically appended to the tail end of the message. A receiving node that also has access to the secret key will compute its own MAC based off the message. If the two MACs match, then the recipient can know that the sender had access to the key (authentication) and the message has not been tampered with in transit (integrity). MAC used by TCP MD5 is often considered too weak due to the cryptographic shortcomings in the MD5 specification while those that incorporate hash functions such as SHA are considered more secure (Jethanandani, Patel, & Zheng, 2013).

Diffie-Hellman Key Negotiation

There are undoubtedly some issues with pairwise-keying, especially when considering the computational management overhead. For that reason, it is important to

have an efficient way for routers to learn about each other's' keys to be comparatively more scalable. The Diffie-Hellman key exchange is a way for two parties with no prior knowledge of each other to exchange a shared secret key (Rescorla, 1999) At a high level, the key exchange works by each participating party generating a private and public key. One party will generate a number based off a combination of their own private key and the other party's public key. The result will be that each party will have computationally generated the same number, which is then used as a key-encryption key in the encryption of data. Effectively, capturing prior messages between the two parties does not give any insight into how to generate or guess the keys, making the shared secret more secure (Butler et al., 2010).

Public Key Infrastructure (PKI)

One of the significant challenges in pair-wise keying when used in a large-scale environment such as BGP on the Internet is the distribution of keys. In pair-wise keying, neighboring nodes need to agree upon shared keys and exchange them via some mechanism. This method does not scale well as it requires more intervention of the network administrators. There is an estimated 35,000 nodes participating in BGP (Butler et al., 2010), thus highlighting the need for scalability. Public Key Infrastructure (PKI) approaches the problem slightly differently, but in a more scalable way. Rather than nodes relying upon shared secret keys, each node will generate a private key along with a public key. The public keys are distributed via the Public Key Infrastructure and are available to participating nodes without manual intervention (Junaid Israr, 2012). These key-pairs are then used in place of shared keys during the generation of cryptographic messages. PKI solutions allow for a hierarchical distribution of pubic keys, which helps with efficient distribution and scalability of the system. As Butler et al. (2010) indicated,

there is ongoing research as to using a trusted authority like the IANA to serve as a top hierarchical node in PKI for BGP.

Public Key Cryptography

BGP sub-prefix hijacking solutions can be separated into two broad encompassing categories: cryptography-based and non-cryptography based (Zheng, Ji, Pei, Wang, & Francis, 2007). In a cryptographic solution, a BGP router must sign and verify either the autonomous system origin or the advertised BGP path. This type of solution has the ability to perform immediate validation and verification of route updates as soon as they are received, but the cryptographic functions introduce overhead that can have significant detrimental impacts on router performance. On the other hand, non-cryptographic solutions often require changes to the router software or additional attributes to be appended to the BGP updates to assist in the detection of invalid or malicious updates.

Numerous types of models exist that attempt to validate route updates coming from peers using strong public key cryptography (M. Zhao, S. W. Smith, & D. M. Nicol, 2005). The central idea of using public key cryptography in validating BGP route updates hinges around each router in an autonomous system digitally signing each piece of information it adds into the route path. When an update is received by a peer, the peer router will then cryptographically validate each of the signatures accompanying the added path data (Butler et al., 2010). According to M. Zhao et al. (2005) introducting cryptography in such a manner has several costs associated with it in terms of generating the signatures, processing the routing path and validating the signatures within the path, and also checking the certificate status to determine if the signing party is still validated. The result from this is larger route updates, slower convergence time, and increases the storage and processing requirements of each participating device.

Cryptography has been analyzed in a number of different applied solutions including attestations. Within cryptography as it relates to BGP security models typically two schemes can be used: asymmetric keys and symmetric keys. In a pair-wise scheme where two neighboring autonomous systems have no prior knowledge of each other the participating parties agree upon a key ahead of time in an offline manner; the trust that they share is then based upon this key (Butler et al., 2010). Lee, Leung, Wong, Cao, and Chan (2007) demonstrated that pairwise keying is often not scalable due to the manual interaction required between parties to update and maintain key pairs. The complexity of this type of key management according to Butler et al. (2010) is $O(n^2)$ in the number of peers. Conversely, asymmetric key models require more computing in key generation, but key management is greatly simplified and more scalable (Butler et al., 2010).

Attestations with Certificates

As previously discussed, route attestation shows that an autonomous system is authorized to advertise a prefix and proves that the autonomous system owns the prefix as well. The IANA is the root authority for delegating the ownership of address blocks to autonomous systems, and those autonomous systems can further delegate the ownership of smaller portions of the blocks (Butler et al., 2010). Attestation or validation of the owners of a prefix are traceable back up the hierarchical structure back to the root.

In order for a participating router to perform attestation in proposed solutions, the PKI is used to obtain the public keys needed for attestation. The key is often times accessed using digital certificates that are issued by a trusted certificate authority. Certificates contain the public key along with a signature indicating the ownership and validity of the information contained within (Junaid Israr, 2012). According to Butler et al. (2010), due to the way that certificates are delegated in a hierarchical structure, they

can often be traced back to a trusted root authority much in the same way that attestations can be traced.

IPsec

Many BGP messages are transmitted over the TCP protocol, which protects against faults that may cause packets to be received out of order, lost, or replayed on a network. TCP by itself does not protect the integrity or provide authentication. This is a common problem within protocols that talk over TCP and exists within the way BGP operates as well. In an attempt to provide integrity checking and authentication between BGP peers, some solutions have looked to IPsec to provide the desired functionality (Butler et al., 2010; Kent et al., 2000). IPsec is a suite of protocols that are able to provide security at the network layer of communications by providing methods for encrypting and authenticating IP headers according to Butler et al. (2010). In addition to encrypting and authenticating IP headers, IPsec also provides methods for key management between peers to help with the establishment and maintenance of secret keys.

IPsec is seen in many secure scenarios such as implementing Virtual Private Networks (VPNs) or providing end-to-end security between nodes. IPsec is also standardized in IPv6, although it is not necessarily required. If it is properly configured, IPsec has the ability to provide certain protections against network attacks such as replays or man-in-the-middle scenarios. In fact, Butler et al. (2010) asserted that IPsec is the most comprehensive solution when compared to other popular ones such as MD5 Integrity (Heffernan, 1998) and the General TTL Security Mechanism (GTSM) (V. Gill, Heasley, Meyer, Savola, & Pignataro, 2004) although it may have a higher cost.

Despite the advantages and protections that IPsec offers, it may not be suitable for protecting a BGP update message throughout its entire transit. In BGP there are four types of control messages: open, update, keepalive, and notification (Y Rekhter et al., 2006). The message types of *open*, *keepalive*, and *notification* are unique because they occur between two nodes and are not forwarded to other peers. The update message on the other hand is more characteristic of a broadcast message in the sense that a BGP speaking router may forward a single update message to multiple destinations. Bruhadeshwar et al. (2011) stated that in such a case, update messages cannot be protected solely through IPsec due to their broadcast-like nature. Furthermore, as routers process update messages and append their path, they must modify the contents of the message, which poses additional challenges for IPsec. Bruhadeshwar et al. (2011) also identified IPsec as an appropriate security mechanism for query and answer sessions, which may be leveraged in route attestation.

In contrast to IPv4 where it was an add-on to the protocol, IPsec exists and is built into IPv6 as a standard and mandatory feature (Lammle, 2013). In addition to being built into IPv6, IPsec does share many attributes with its IPv4 counterpart. For example, applications may still chose between two different supporting protocols including Encapsulating Security Payload (ESP) and Authentication Headers (AH) (Shue, Gupta, & Myers, 2007). To facilitate the establishment and periodic refresh of the cryptographic keys, IPsec leverages the Internet Key Exchange (IKE) protocol (Harkins & Carrel, 1998). According to Shue et al. (2007), when analyzing the performance of IPsec, IKE typically accounts for most of the overhead in the protocol compared to supporting protocols like ESP. However, when a significant number of packets are being processed, the relationship may invert and IKE will account for less overhead. As overhead may

impact adoption rates of protocols, this relationship needs to be taken into account when implementing IPsec.

IPv6 Extension Headers

In addition to IPsec, IPv6 has additional properties that may assist with performing route attestation. According to Lammle (2013) among the many improvements in the IPv6 protocol over IPv4 are extension headers. IPv4 has been adapted and added on to many times since its introduction. Due to its longevity, certain requirements that protocols have were simply not thought of in the original design of IPv4 such as IPsec. Therefore, the complicated add-ons and compensations that exist to give IPv4 the required functionality make certain implementations more difficult to use and negatively impact the efficiency of the protocols (Lammle, 2013).

IPv6 extension headers are one of the improvements added into the specification. They are described as any header following the initial 40 bytes of the packet that also precedes the packet's upper-layer header (Carpenter & Jiang, 2013). These extension headers are intended to be used by the originating node to send information and are not processed by any intermediary nodes along the path until the packet reaches its destination (Deering, 1998). This is an important property of the extension headers as Carpenter and Jiang (2013) noted, it allows for nodes without understanding of the header to continue passing the information along. Compatibility with the use of the extension headers is then required on the sending and final destination nodes.

When looking at IPv6 extension headers in the lens of performing route attestation for BGP, the Authentication Header stands out as particularly interesting. The Authentication header has the ability to provide integrity and origin authentication for packets traversing an IPv6 connection (Kent, 2005). These two properties combined with

another that will account for correctness of an update can feasibly be combined to perform attestation. In addition, since the Authentication header is built into the IPv6 protocol, the overhead can be examined in comparison to solutions who rely on external sources of authentication.

Existing Route Attestation Models

This section provides an investigation into existing route attestation models that have been introduced and studied to provide authorization and validation of BGP route updates. The literature review of these models is intended to objectively highlight crucial strengths and weaknesses of the models. The lack of models pertaining specifically to IPv6 is an important issue in the area as IPv6 adoption has been slow to adoption but increasing as IPv4 space is exhausted. The existing models address BGP version 4 of the protocol that is the same version used in IPv6, so relevant information is gained from this exploration in terms of challenges, future study, impacts, and implementations of these models. The literature review of existing route attestation models will include both control plane and data plane prevention taxonomies as well as the following proposed solutions: Secure BGP (S-BGP), RPKI, Secure Origin BGP (soBGP), and ROVER.

Control Plane and Data Plane Prevention Taxonomies

Many of the BGP solutions proposed aim to ensure that BGP sends and receives control messages such as updates and route withdrawals properly. This focus places the solutions into the control plane of the protocol (Butler et al., 2010). The control plane in BGP handles the logic of keeping an updated router information base (RIB) that maintains adjacencies of neighboring networks (Vissicchio et al., 2013). Most detection methods for BGP sub-prefix hijacking reside in the control plane according to Zheng et al. (2007). By the nature of BGP convergence and the control plane's responsibility for

determining a path to a given destination (Schuchard et al., 2010), sub-prefix hijacking attacks directly affect the control plane.

In BGP, the data plane is slightly abstracted from the control plane in that its intended purpose is to handle the actual transmission and forwarding of packets that can contain route update and other BGP messages (Schuchard et al., 2010). Certain models have been proposed to measure metrics in the data plane about the distance and reachability of remote networks learned through BGP (Zheng et al., 2007). The data plane has visibility into metrics such as hop-count and similarity between autonomous system paths that form the foundation of Zheng's model. This type of model requires numerous systems distributed throughout the BGP domain in order to form a comprehensive and accurate view of the stable routing environment.

Questions arise as to whether or not BGP can be secured entirely in the control plane or the data plane. It is often seen only security one element of a protocol or system that has numerous mechanism may actually reveal additional vulnerabilities within that protocol (G. Huston et al., 2011). If one secures only the control plane, they may assume that the BGP speaker can trust the autonomous system path it receives in a BGP update. However, without also securing the data plane the actual transmission of the data may still be susceptible to being sent down an untrusted path via the data plane. G. Huston et al. (2011) suggested that there is a law of diminishing return that applies when adding incremental security features in such a scenario the added benefit in light of the complexity tapers off as well.

S-BGP

One frequently rerenced model is the Secure Border Gateway Protocol (S-BGP) designed by Kent et al. (2000). The S-BGP model uses public keys as a new path

attribute and introduces IPSec into the route update process. At a high level, this model works on two PKI's: one for IP address allocation and the other for the assignment of autonomous systems and router associations wihtin those routers. Through the use of certificates, address/route attestations, and IPSec the authors of S-BGP were able to migitate certain vulnerabilities within BGP including sub-prefix hijacking. S-BGP has been refered to as the most comprehenssive solution for protecting against BGP attacks (Gersch & Massey, 2013). However, there were significant performance impacts wihtin the implementation when considering processing, transmission bandwidth, storage and memory on the routers with the latter two being the largest issue. Accoridng to M. Zhao et al. (2005), these implications are a contributing reason to the solution not being implemented wide-spread.

RPKI

RPKI is a model that was developed by the Internet Engineering Task Force (IETF) in an effort to secure BGP and interdomain routing implementations (Wählisch et al., 2012). Similar to S-BGP, RPKI uses a certificate hierarchy to create relationships between autonomous systems and gives them the authority to authorize the origin of route updates. A limitation of this particular model is it does not take into account a malicious entity may spoof their autonomous system and then perform attacks such as sub-prefix hijacking. Adoption of RPKI is relatively low and is estimated to authroize only 4% of the Internet's routes (Malhotra & Goldberg, 2014). RPKI is an important model to study because it is gaining the most traction in implementation (Goldberg, 2014).

soBGP

A third proactive, cryptographic solution that has been introduced and studied is Secure Origin BGP (soBGP). Through it's design, soBGP implements certificates to address specific questions related to secure routing objectives. These questions help a router identify a peer transmitting an update and determine their key, define authorization, discover peer routers, and control what should be done with a route update. Although the protocol is not specifally designed to defend against any one attack, it does by nature prevent sub-prefix hijacking attacks as the maliciuos entity would not be authorized to inject such a route into BGP (White, 2003). An advantage of soBGP over S-BGP is that it does not require encryption mechanism to be run directly on the router; the encryption processing can take place elsewhere. This design should reduce the overhead and negative impacts of requiring router to perform all of the cryptographic functions.

ROVER

ROVER much like S-BGP, soBGP, and RPKI is another model that successfully can mitigate sub-prefix hijacking attacks and like RPKI securely maps an autonomous system to a subnet (Malhotra & Goldberg, 2014). ROVER operates slightly different than RPKI and bases its functinality off of an already adopted standard reverse-DNS (rDNS) rather than heavy modification to an exsting infrastructure. Using a trusted DNS server, an autonomous system can register their ownership of address blocks through the use of a new Secure Route Origin (SRO) DNS record. This would allow routers receiving a BGP update to validate that the origination point of the udpate was authorized to do so.

Each of these solutions share similar characterisitcs in the sense that they are based on some form of public key infrastructure which is used to assist in the route attestation. Furthermore, each of the models are proactive in that they validate routes recived immediately before allowing changes to be made to a router's routing table. They can be classified as a proactive cryptographic prevention solution operating in the data-plane.

Adoption of Existing BGP Route Attestation Models

Regardless of the type of model, proposed solutions to improve the BGP security posture against sub-prefix hijacking attacks remain largely unadopted. Considering the massive scale of the Internet and autonomous systems within, it is impractical to make a clean cutover to where all participating BGP speakers adopt a more secure implementation. This type of change would require thousands of organizations who are not governed by a central authority to adopt new standards that may not work well unless a large portion of the organizations adopt them (Goldberg, 2014). This is similar to the scenario of IPv6 and DNSSEC (Herzberg & Shulman, 2013) on the Internet; even though the protocols offer distinct advantages over their predecessors, the Internet is slow to adopt them as it creates additional work, computational overhead, and may force systems to be upgraded. The advantages do not outweigh the accompanying burden in some administrative domains.

With the global scale of BGP and the aforementioned lack of regulation on the adoption of new secure protocols, a solution will need to be able to work in a partial deployment. Realistically, this introduced the assumption that while a secure BGP solution is operating in partial deployment, an autonomous system may need to accept legacy or insecure routes from destination networks that do not participate (Lychev et al.,

2013). The research performed by Lychev et al. suggested that even partial deployments of secure BGP instances could improve the overall nature of interdomain routing in certain scenarios depending on the hierarchical level of the implementing autonomous system.

Since securing BGP and implementing improvements to the protocol will require each autonomous system to make the adaptation, one should understand how autonomous system operators prioritize secure routes. Lychev et al. (2013) surveyed 100 autonomous system operators on how they prioritize secure routes over insecure routes and classified them into three models. The three models included:

1. Security 1st where secure routes are always preferred over insecure routes.
2. Security 2nd where a secure route is preferred over an insecure route if it is calculated to be less costly route is available.
3. Security 3rd where a secure route is preferred over an insecure route if and only if a less costly and shorter insecure route does not exist. This means that the secure route must be the shortest and have the least cost associated with it to be chosen.

Lychev et al. determined through their survey that the security 1st model was least popular in a partial deployment scenario while the security 3rd model was the most popular among autonomous system operators. The operators of those autonomous systems cited the risk of lost revenue and uncertainty of the adaptation as contributing factors for choosing security 3rd. Nonetheless, a secure BGP protocol in partial deployment was found to contribute to the overall security of routing updates demonstrating the feasibility of such application.

The scale of the Internet is global and it continually changes and becomes a denser, richer environment. This property of the Internet makes it infeasible to have a "flag day" where all participating autonomous systems may adopt a new transition to any technology including those that secure BGP (G. Huston et al., 2011). The result of this will be a piecemeal deployment of any solution where the idea of a transition period becomes an ongoing or indefinite factor.

In addition to issues faced with autonomous system operators electing to adopt a secure BGP standard and the scale of the Internet, there are also technical implications imposed by many of the solutions that may be a barrier to the option of security enhancements. Cryptographic solutions may require the routers to implement crypto hardware accelerators or absorb the performance penalty in terms of hardware overhead (Goldberg, 2014). There is clearly a tradeoff between solutions that perform address proof validation offline and those that attempt to do it in real-time using cryptographic solutions(M. Zhao et al., 2005). Other solutions require modifications the actual update messages and come with their own challenges in updating router operating to acknowledge the changes. As G. Huston et al. (2011) concluded in their survey of BGP security solutions, there is a cost in improving no matter the solution; security needs to become an essential part of BGP rather than a desirable property.

Measuring Overhead in Routing and Cryptography

As overhead is a limiting factor in the adoption rates of BGP security solutions, it is important to understand and measure sources of overhead. Routers have a finite amount of resources when considering time for a routing table to fully converge, the size of the routing table, as it is stored in memory on the router, processing load, and scaling capability of the protocol. The first metrics including convergence time, memory

consumption, and CPU consumption are easily measured quantitatively and can be used to measure the impact of security enhancements to BGP. The last metric mentioned by G. Huston et al. (2011), scaling capability, is much more difficult or even impractical to measure as the scale of the Internet and its volatile nature introduce many variables; thus scalability is a metric that is largely understood in its fullest extent. These same metrics and associated measurements are used by the authors of S-BGP to evaluate performance and operational issues as well (Kent et al., 2000). S-BGP is often touted as the most comprehensive BGP security proposal to date (M. Zhao et al., 2005) which builds the importance of these measurements.

Routing table convergence times are another factor that comes up in the measurement and the impact of proposed BGP security solutions. Route convergence is the measurement of time from when a routing update is sent and when participating routers settle on a stable route (Dan et al., 2002). This is an especially important property of BGP as changes in the Internet topology need to be replicated out quickly. If there are large delays from when a topology change takes place and when all routers in the BGP space are aware of the new stable route, networks may effectively become unreachable to certain autonomous systems. The very purpose of a routing protocol is to provide quick adaptive changes in an evolving topology to ensure reachability of systems.

Existing Infrastructure as Functional Components

BGP speaking routers need a way to look up the ownership of a subnet in order to determine if an advertised route it authorized. As Gersch and Massey (2013) indicated through their research, DNS and reverse-DNS are already deployed in a global scale, are well understood, and have had significant amounts of testing. Reverse-DNS (rDNS)

serves as a platform for resolving an IP address into a domain name, thus attributing ownership of the IP address (Howard, 2015).

The naming conventions of a proposed solution for leveraging rDNS to attribute network prefix ownership need to follow a standardized approach to ease adoption. Multiple naming conventions have been proposed to address this (Eidnes, de Groot, & Vixie, 1998; Gersch & Massey, 2013; Thomson, Huitema, Ksinant, & Souissi, 1995). By and large, solutions proposed by the IETF (Thomson et al., 1995) have become the standard and are widely adopted.

One problem with using DNS or any central authority is an attacker may be able to spoof the origin of the message making it appear that it has originated from a trusted location. This type of problem is particularly relevant when observing email communications (Delany, 2006). Delany's DomainKeys (Delany, 2007) solution is built around the principal that if a recipient of an email can irrefutably determine the origination point of an email and whether or not that source was authorized to do so, granular filtering and acceptance policies can be applied. This draws a parallel to a recipient of a BGP route update. If that recipient was able to determine beyond doubt the origination of an update and if that source was authorized to do so, sub-prefix hijacking attacks will be easy to detect in nature.

DomainKeys is a solution that relies heavily upon DNS to store and distribute cryptographic keys (Delany, 2007). The cryptographic signatures are used as a method of signing and authenticating the origination of a message. From the cryptographic authentication system an authorization system can be developed. In the case of this research, the authorization component builds from the previously discussed rDNS model. DomainKeys have been frequently discussed by the IETF (Crocker, Hansen, &

Kucherawy, 2011; Hansen & Hallam-Baker, 2009) and are further developing increased adoption rates.

Summary

The research studied in Chapter 2 provided an overall viewpoint of the state of BGP security and identified properties of a successful BGP security model. An examination of existing route attestation models is performed to identify existing factors that contribute to the adoptability or lack thereof in such models. Through validity testing and measurements of overhead presented in the reviewed literature, similar methodologies will be utilized in Chapter 3. Route attestation methods are further evaluated by studying the research presented to determine the routing plane in which a successful route attestation model may operate. Finally, methods of effectively weighing performance implications in terms of overhead in routing and cryptographic solutions are studied in an effort to provide consistent measurements and common understanding of the proposed solution.

CHAPTER 3: RESEARCH METHODS

Chapter 2 surveyed literature that applies to the background of this research study. The purpose of this study was to evaluate the performance implications on a router participating in a model where IPv6 extension headers are used to perform BGP route update attestation. In the following sections, Chapter 3 will present the research methods that will be used in this proposed research study. Furthermore, the chapter will both discuss and justify how the model is apposite to the study. Lastly, important details surrounding the research method will be presented including: design of model, data collection methods, instrumentation, legitimacy, dependability and data analysis methods.

Research Method and Design Appropriateness

Quasi-experimental design is intended to investigate what effect a treatment has on an outcome variable (Salkind, 2010) where participants are not randomly assigned. Furthermore, according to Balasubramanian, Raman, and Selvakumar (2013), before-and-after studies are designed to be used when a researcher is able to establish a before observation prior to any interventions are introduced into the sample population. This negates the need for a researcher to retroactively reconstruct the before observations. In essence, a quasi-experimental before-and-after study is designed to measure the resulting effects of an intervention on a non-randomly assigned study group. This will take into account the measurement of primary variables as they relate to the hypothesis.

The proper identification of a research method is crucial to designing a research study. According to Salkind (2010), quantitative research methodologies are commonly used in scientific investigations of quantifiable properties and their relationships. On the other hand, qualitative research methodologies are often found in social and human

studies where resulting data is a representation of general themes or interpretations from the study (Creswell, 2009). Although quantitative and qualitative research methodologies do produce different types of results, Salkind (2010) indicated that the methodologies should not be antithetical. In fact, due to necessity, many research processes contain aspects of both quantitative and qualitative methods. In this study, quantitative data was used primarily to describe the performance implications of using IPv6 extension headers in a BGP route attestation model.

In the light of BGP being the only routing protocol across the public Internet that facilitates the exchange of routing information between autonomous systems such as ISPs, performance is an important measurement. The nature of this study, as described in Chapter 1, was to numerically measure the performance impacts of routers participating in an IPv6 BGP route attestation model compared to routers not participating in the model. Since several studies have been performed to measure similar metrics in IPv4 BGP attestation models using quantitative methods (Biersack et al., 2012; Kent et al., 2000; M. Zhao et al., 2005), this study also used quantitative methods to measure the resulting performance impacts. The chosen quantitative methodologies provided numerical insight into the relationship being studied with statistical analysis on observed results.

Quantitative data results in numeric values that can be measured and used to test the effects of researcher intervention (Kumar, 2005). The researcher intervention in this study was the introduction of the attestation model where the BGP routing process was modified to verify route updates. Numeric values obtained through quantitative research allows researchers to understand the performance and scalability of software systems

(Liu, 2009). To better define the scope of this study, numeric results were analyzed rather than broad generalizations that may be seen in qualitative work.

According to Creswell (2009) the selection of a research design methodology takes into account a few factors including the type of data being collected, analysis of the data, and interpretation of the results. Despite research being a mix of methods, this study aligned most closely with quantitative research. From within the quantitative research category, a researcher must understand the available methodologies when determining the design appropriateness.

Creswell (2009) further classified quantitative research into two methods of inquiry: survey and experimental, while Salkind (2010) also suggested correlational research and casual-comparative research. Although different variations of these methods of inquiry exist to describe relationships between variables, experimental research was the most appropriate for this study. Experimental research aligns with the purpose and nature of this study as there was at least one independent variable that received intervention while other dependent variables were measured. These variables represented the participation in the model, performance impacts, and scalability as described in subsequent sections.

Survey-based research is intended to generalize opinions, trends, or attitudes via structured interviews or questionnaires (Creswell, 2009). Due to the highly technical nature of this research, survey-based research was not suitable as there were not human-subjects being studied or intervened with in the research. Furthermore, the intent and data gathered from survey-based research represents descriptive data about the current status of variables within the study (Salkind, 2010) as opposed to the relationship between variables through descriptive statistical analysis.

Correlational research is another similar option in research design to experimental research. According to Salkind (2010), correlational research does have the ability to show relationships between variables and is limited by the lack of randomness in participants. However, correlational research aims to describe these relationships between variables in naturally occurring situations as opposed to experimental design. Experimental design is the process where a researcher intervenes or acts upon variables seeking an outcome. Therefore, correlational research was not suitable for this study because the variables were not naturally occurring.

Casual-comparative or ex post facto research is a third research approach that falls within the quantitative research scope. Casual-comparative studies measure differences within existing or established groups (Salkind, 2010). This type of research also examines the groups from a retrospective lens in the sense that the events within the groups have already occurred. As a result, of the events occurring in the past, any variable manipulation is impossible, making this approach inappropriate for the study.

In contrast, experimental research focuses on whether or not a specific treatment results in an influenced outcome. Taking into account the goals and data collection methods described by Creswell (2009), this study used an experimental research strategy. This strategy allowed for researcher intervention and variable manipulation as well as control of the groups being studied.

Within the experimental research strategy, Salkind (2010) identified two sub-categories: true experimental research, and quasi-experimental research. True experimental research requires that participants be randomly selected and placed into either control or experimental groups prior to the researcher's intervention. Random

selection is beneficial as it can provide for proper casual relationships between dependent and independent variables (Salkind, 2010).

On the other hand, quasi-experimental research differs from true experimental research as the researcher may not or should not randomly assign participants to control and experimental groups. While quasi-experimental studies cannot show a true cause and effect as a result, they can be used to show relationships between variables (Salkind, 2010). This study was not being performed in a production or live environment, rather the study focused on a simulated and highly controlled environment. The simulated environment provided consistency amongst the attribute variables as they could not be actively changed or controlled Kumar (2014) and further eliminated outside influences on them. In the proposed environment, if all participants were identical, or duplicates of each other, the randomization of an experimental study was not needed. In this case, since technical objects were being studied and originated from copies of a master template, they were as close to identical as possible. A benefit of randomization is the allowance of all participants to have an equal an independent chance of being in a control or experimental group (Creswell, 2009). This state of randomization or the lack thereof is what dictated that a quasi-experimental study was most appropriate in this scenario.

Lastly, the researcher needs to take into account the nature of the study when defining an experimental investigation. There are three scopes in which a researcher may look at the study's nature. The first being an experimental study where the researcher intervenes introducing an effect and measuring an outcome or the cause. On the opposite end of the spectrum, a researcher may observe the outcome of an intervention and try to determine the effect; this is known as non-experimental. Additionally, there exists a hybrid of the two approaches known as semi-experimental where a researcher

retrospectively associates the effects with outcomes. These three definitions given by Kumar (2005) further clarified why this study was an experimental study in nature as opposed to non-experimental or semi-experimental.

Research Question, Hypothesis, and Variables

This study aimed to measure the extent of the relationship between routers participating in a BGP model to perform route attestation with IPv6 headers and the resulting performance impacts. The research question which guided the study is: *In a model where IPv6 extension headers are used to successfully perform route attestation of BGP updates, what is the resulting degree of difference exists in terms of router CPU utilization percentage, RAM utilization percentage, route convergence time, and BGP update packet size in comparison to a router not participating in the model?* This research question was answered through a systemic gathering and analysis of numerical data obtained from the participating routes.

The hypothesis is a statement of predictions about the relationships among variables that the researcher intends to ascertain (Creswell, 2009). As previously described, the hypothesis for this study was: *Given a model designed to perform lightweight route attestation, necessary information needed to perform the attestation may be carried inside of IPv6 extension headers within constraints defined by the protocol specification without imparting performance overhead.* This hypothesis guided the study and shaped the variables, data collection methods, and analysis of results.

Population

In an effort to align with goals of quasi-experimental research design, the routers that composed the population were as similar as possible. Virtual machines are software instantiations of computers that run operating systems and applications (Patterson &

Hennessy, 2013). Virtual machines are backed by physical hardware on a host referred to as a hypervisor or virtual machine manager (VMM). The relationship between a hypervisor and a virtual machine is that the hypervisor or "host" provides the physical resources needed for the virtual machine referred to as the "guest". To facilitate creating a group of similar routers to be studied, virtual machines were used, as they are easily copied and duplicated. The duplication of a single virtual machine into a larger group of virtual machines produced a population with an extremely similar identity between all routers.

The virtual machines used in the study were running pfSense, an open source firewall operating system based off the FreeBSD distribution, a variant of the BSD operating system. Due to the lineage and origin, pfSense is technically a variant of the BSD operating system. One of the major contributing factors to selecting pfSense as the operating system for the virtual machines was the open source nature of the project. Open source software includes code that has been published publicly for consumers of the project to copy, modify, and redistribute (Fitzgerald, 2011). Furthermore, according to Fitzgerald (2011), since the software or operating system is open source, royalties and fees no longer become a limiting factor as long as those using the code respect and quote the primary contributions. These properties of open source software allowed for the researcher to implement the proposed model programmatically. Furthermore, open source software allows the study to be repeated by other entities more easily by protecting them from the royalties, fees, and accessibility of closed-source software.

In addition to being open source, pfSense has a large community of users ranging from single instances to larger enterprise consumers that have many installations. Because of the high adoption rates and community support of the pfSense project, the

pfSense distribution is a viable alternative to systems built and maintained by major vendors such as Cisco, SonicWALL, WatchGuard, and others (Ribeiro & Pereira, 2009). The wide-adoption, scalability, open source code, and expansive feature set of pfSense made it an optimal choice for this study.

For the purpose of simplification in taking measurements while collecting data, the topology only accounted for one BGP speaker in each autonomous system at a time. This model did simplify the operation on of BGP on the Internet, but most security protocols pertaining to BGP focus on inter-autonomous system communication (M. Zhao et al., 2005). Furthermore, routing instability can be attributed to dropped packets, network congestion, and abnormal network activities. To keep the assessment of the model's performance as focused as possible, these network anomalies were not accounted for in the study. The study assumed that the network used by the model is in a reliable, predictable, and functional state.

To serve the virtual machines or routers, a piece of software called a hypervisor was required. Hypervisors are software instantiations that present hardware interfaces to operating systems by serving resources and isolating virtual machines from each other (Natanzon et al., 2013). Two main types of hypervisors; those that are native and those that are hosted within an operating system. According to Natanzon et al. (2013), native hypervisors are installed directly on top of hardware similar to an operating system whereas hosted hypervisors run under a host operating system. Native hypervisors are often referred to as "Type I" whereas hosted hypervisors are referred to as "Type II" (Iqbal, Pattinson, & Kor, 2015). Due to concerns with efficiency of hypervisors and eliminating external variables such as a host operating system, this study implemented

native hypervisor. Examples of native hypervisors include VMware ESXi and Xen (Desai, Oza, Sharma, & Patel, 2013).

A single hypervisor hosted the virtual environment that the model and simulation results were performed in. In addition, the hypervisor was free of other virtual machines so that only those being studied were running. The exclusion of other virtual machines was again intended to reduce the possibility of unintended influences affecting measurements from within the hypervisor. In addition, the hypervisor was isolated from other networks and servers itself as to not impose any external influences on the system hosting the virtual machines. By keeping the system isolated and as purpose-driven as possible, the risk of impurities in the data were lessened.

Research Model and Design

The basis of the problem in the study was that a BGP message recipient does not validate route updates before accepting them. To provide a vector for BGP speakers to attest routing updates, the resulting artifact was built upon proven models and methodologies that have been implemented to solve similar issues. These grounds provided for a more easily adoptable solution and one that has been established in certain capacities. This section will detail the research from two lenses: the introduction of a condition into the environment and the treatment of said condition.

BGP sub-prefix hijacking attacks are a situation where unauthorized BGP speaking peers claim specifically defined networks that they do not own. Essentially, the advertisements of these unauthorized networks appear the same way that authorized route advertisements do to receiving routers. When a router receives any route advertisement, the process of convergence happens. Convergence includes everything that takes place on a router from the time a BGP route is sent and when the receiving router stabilizes its

routing table. This convergence process can result in a measurement of the time it takes for a router to receive an update, process the update and either commit or reject the update form the routing table.

This process of convergence was a primary measurement of the overall impact of introducing a model to perform BGP route attestation in terms of performance and overhead. As previously stated, convergence happens through the processing of both valid and invalid routing updates. Therefore, in order to measure the resulting data, convergence was forced on participating routers by the introduction of valid and invalid routing updates from a trusted peer. These routing updates did not only simulate real routing updates, but they also covered the sub-prefix hijacking scenario. Using route introduction as the condition to cause convergence gave insight into the overhead of the proposed model as well as the effectiveness in performing route attestation.

The second piece of the research design in addition to the condition is the treatment. In the scope of this study, the treatment was the introduction of a model to perform route attestation on received routes to allow legitimate route updates and disallow other updates. This treatment or model is detailed in the subsequent design characteristics and procedures.

One of the cornerstones of the proposed model was a trusted and secure Central Authority (CA). Numerous examples show that due to the design of the BGP-4 protocol, participating routers cannot simply trust each other as they have been. The plentiful route hijacking attacks that have taken place (Butler et al., 2010) support this idea. The CA was a standalone component that routers were able to query much like a traditional DNS server. The CA served the following roles and asserted these properties.

1. The CA provided ownership information of an autonomous system through reverse and standard DNS queries. These attributing DNS records were named in a scalable, standardized fashion as discussed in the literature review such as ip6.arpa (Eidnes et al., 1998). This property provided authorization for an autonomous system to advertise a prefix.
2. Resource records used in the DNS lookups mapped from the network prefix and resolved to the owner/authorized advertising autonomous system for that prefix. Also contained in a DNS record for the prefix was a public key generated by the autonomous system owner.
3. Information contained within and disturbed in the DNS system was assumed to also be accurate from the vantage point of the routers. Validation was achieved through this property. Trust information was established with PKI infrastructure.
4. PKI keys stored and distributed with DNS modeled the scheme seen in DomainKeys (Delany, 2007). These provided a mechanism for authentication.

The above assets of the central authority facilitated authorization, validation, and authentication of a BGP speaker and the route update. This follows the standards for route attestation prescribed by Delany (2007).

A second critical component in the artifact was the actual BGP speaking routers. Communication between BGP routers and the CA happened over IPv6, which natively establishes IPSec tunnels for secure delivery of information. To supplement the communication with the central authority over IPv6, extension headers were used to carry authentication information. Carrying data in the extension headers resolved the need for

a large amount of extra network traffic in terms of packets sent. In addition, as the IPv6 extension headers are 64-bit aligned, the processing of such headers is more efficient than the processing of IPv4 counter parts. Routers participating in the new model followed this high-level process as a BGP update message is prepared for delivery and received:

1. A BGP speaking router used the private key (public key is available in the public DNS records) to sign any BGP advertisements originating from the autonomous system.
2. The resulting signature of signing the BGP advertisement was be placed into one of the IPv6 extension headers and the update was transferred to the recipient routers.
3. When a router received the BGP update message, it processed the headers and extracted the signature.
4. With the signature in hand, the router performed a DNS lookup on the advertised network and claimant autonomous system. From that information, the public key was sent back by the trusted DNS system.
5. The public key was then be used to determine if the signature associated with the BGP was generated with the associated private key, and based on the results of that test, the validity of the update was determined.

For the routers to participate in this type of model, they needed to run a modified BGP software engine as this design was not in the BGP-4 specification (Yakov Rekhter & Li, 1995). The model was able to identify sub-prefix hijacking attacks as the malicious actor would not be able to generate the correct signature in the update assuming the keys are secure and the DNS system is uncompromised as stated above.

Sampling Frame

Sampling is a method of studying a subset of a whole population with the intent of providing an estimate of the prevalence of an unknown outcome on the larger population (Kumar, 2014). The process of sampling has both advantages and disadvantages that affect the accuracy of results produced by a study. According to Kumar (2014) sampling is beneficial in situations where a population may not be studied in its entirety or financial and human resources do not allow the whole population to be studied. If the researcher chooses a sample appropriately and the tolerance of error is acceptable, the results produced will be reasonably accurate. On the other hand, sampling a population at best can only provide an estimate of the outcome on a population. Effectively, error is possible when sampling, but can be calculated for and minimized through correct inquiry and population selection (Kumar, 2014).

Due to the infeasibility of implementing this model across routers on the Internet in production environments, a representative sample was used. Certain barriers exist that make studying the Internet routers as a whole impractical including cost, closed-source software, and the immense scale of the Internet. Due to the unknown number of routers in the public Internet as it is a highly volatile environment, non-random sampling was used. Kumar (2014) suggested non-random sampling is acceptable in such environments where the total population is unknown. Again, due to similar issues with the size of environment and available routers to be studied, a purposive sampling approach was used. Purposive sampling allowed for the researcher to choose the sub-population based upon necessary requirements (Kumar, 2014) such as following BGP implementation as specified in the original protocol design.

In order for this study to satisfy the goals of a sampling frame and describe the potential impacts of implanting such a model in a larger population on the Internet, the routers needed to be representative of those actively being used. To achieve a representative population of real routers on the Internet, routers running pfSense were studied. The rationale behind choosing pfSense was the open source nature of the operating system and its implementation of the OpenBGPD service for providing BGP routing. OpenBGPD is an open source project that extends BGP functionality to operating systems such as pfSense. Furthermore, OpenBGPD has been noted for its compliance with standards documents indicating its correct operation of the protocol (Bakker, Jasinska, Raszuk, & Hilliard, 2013). This helped bridge the gap between the sample population and the Internet population of BGP speaking routers as the correct operation of BGP should be present in both groups.

From a hardware standpoint, pfSense machines are present on the publicly facing Internet and would consist of the same components as far as CPU, RAM, and network interfaces as traditional routers. Those pfSense routers in the Internet population would be represented by the non-random sample population in that sense. Numerous vendors of physical and virtual routers beyond those running pfSense have slightly different architectures and components such as application-specific integrated circuit (ASIC) chips in their devices (Ganegedara, Jiang, & Prasanna, 2014). Those components may affect the results of this study as they are applied to such devices, but that is beyond the scope of what is being measured and observed. In a pure hardware scope, the study focused on the overhead in CPU and memory utilization, which can be applied more universally to all routers.

In essence, the software operations of BGP speaking routers was accounted for in the sample population by choosing an accepted and correct implementation of the protocol provided by OpenBGPD. The hardware measurements taken in the sample population were designed to take into account components that routers universally share regardless of vendor. These two contributing factors to the composition of the purposive sample group help suggest what an implementation of the model outside of the sampling frame may result in. When interpreting results, the researcher needs to know that a limitation of sampling and more specifically non-random sampling is that the results are an estimation of the impacts on a population as a whole (Kumar, 2014).

Data Collection

Virtual routers participating in the BGP environment were the primary source of data to be collected throughout the study. The data collection took place using various operating system tools within the virtual routers alongside of reporting systems that exist within the host or hypervisor virtualization environment. Measurements were collected to cover the areas of CPU performance, RAM utilization, bandwidth utilization/consumption, and route convergence times on all participating routers. These measurements showed how the model affected each router individually and gave insight into the scalability of the model as more routers are added.

When investigating the impact on BGP security solutions the most important metrics are BGP convergence time, message size, and memory costs rather than CPU utilization (M. Zhao et al., 2005). Specifically, M. Zhao et al. (2005) argued that convergence time better demonstrates the impacts of computational overhead pertaining to security protocols as opposed to CPU utilization. Convergence time demonstrated the amount of time it took for a route update to be sent, received, processed, and forwarded if

necessary. According to Liu (2009), CPU consumption is a very important metric when assessing software performance which is closely related to this study. Therefore, CPU utilization was gathered in addition to the other metrics.

The virtualized routers ran the pfSense operating system, which is based off the FreeBSD distribution. FreeBSD is the base upon which pfSense is built, therefore it is a closely-related operating system that has gained a reputation for being free, highly stable, powerful, and efficient (Chen & Zhu, 2014). Since pfSense is based off FreeBSD, technically a version of the BSD operating system, it has many of the same tools and utilities designed to measure CPU utilization, bandwidth consumption, RAM consumption, and other metrics. These performance monitoring tools and utilities have been used in various studies (Seo, Hwang, Moon, Kwon, & Kim, 2014; Zhao, 2002) and provide accurate and valid measurements. The usage of built-in utilities that are widely implemented is their general acceptance among the community of users as a quasi-standard.

One of the pivotal tools that was used in the study to monitor performance and consumption of relevant computing resources is called "vmstat". This utility has the ability to show quantitative system performance metrics in the following areas: processes, memory, paging, disks, faults, and CPU (Lucas, 2008). Furthermore, vmstat is able to display performance measurements in real-time or as snapshots in time. This gives flexibility to how the information can be interpreted, either as instantaneous readings or as a summarization of events over time. The metrics of CPU, memory, and bandwidth consumption were used collectively to describe overall overhead. A researcher should consider that the actual measurement of CPU, memory, and bandwidth consumption could itself have a performance impact on the system. This potential performance impact

was accounted for as vmstat has been used in other studies minding performance (Weikuan, Yandong, & Xinyu, 2014; Xiao, Song, & Chen, 2013; Yu & Lan, 2016) and was ran in all tests, theoretically introducing the same if any performance impacts.

Convergence time in BGP is the time span from when a speaker announces an update until the entire network returns to a stable state (Meiyuan Zhao, Sean W Smith, & David M Nicol, 2005). The originating peer of a BGP update message generated an entry into a log file with the exact time that the message was advertised to peers. As each neighboring router received the update and stabilized their routing tables, they too generated timestamps of the event. The convergence time could then be calculated by subtracting the time of the origination message from the last routing table stabilization time. This calculation represented the convergence time of all routers participating in the security model, which could then be compared to the same environment that did not participate in the security model. To ensure consistency, the participating routers had their clocks synchronized to a central system such as a Network Time Protocol (NTP) server.

Bandwidth consumption can take shape of many different measurements such as packets per second, size of packets or messages, time the line is in use, and others. Since the model introduces a fixed number of additional packets when compared to traditional BGP message processing, there was an increase of total packets transmitted. Therefore, the measurement of additional packets in this study was excluded. As M. Zhao et al. (2005) identified message size as an important metric of assessing BGP security proposal performance, the study focused on that measurement. Message update size can be measured by accounting for all packets received and transmitted during the transaction

and totaling the number of bytes in those packets. This represents the total bandwidth consumed for an update message.

When sampling performance or scalability issues in software designs, one of the first and most important measurements to take is that of CPU utilization on each of the systems being tested (Liu, 2009). Since computers are time-based, performance monitoring happens at set intervals called samples. Specifically related to processor performance, the samples can be measured with processor time. Every processor has an idle thread, which effectively consumes CPU cycles while there is no work for the processor to do. Essentially, this idle thread represents the utilization or lack thereof of the CPU. According to Liu (2009), processor time can be calculated by monitoring the time that an idle thread is active during a sample interval, and subtracting it from the interval duration. This formula was taken into account when measuring the processor performance and the data can be obtained from vmstat.

RAM may be simpler to measure as far as utilization is concerned than compared to measuring the use of a processor. Since every computer system has a finite amount of RAM available, the measurement of how much is available and how much is consumed can provide an accurate representation of its utilization (Tanaka, 2005). When RAM is over utilized, computer systems will offload some of the memory contents to disk which is known as paging. If no paging is occurring while the measurement of memory utilization is taken, the measurement will show an accurate representation according to Tanaka (2005).

These metrics were queried from the operating system level within the virtual machine and logged to a file that exists on the host. This allowed a baseline to be gathered of the routers operating in a controlled environment. Once a baseline was

established for the virtual routers, the attestation model could be introduced and the same performance counters were used to gather the new set of data. If the data collection process occurred in the exact same way, this should negate the introduced performance hit of additional logging. Once all of the tests had been run, the results were compiled into a computational program for analysis and validation. By pulling all of the results into a single repository, the data could analyzed and evaluated centrally.

To provide a more-accurate overview of the results from the model simulations, multiple iterations of the tests were done. In similar tests, M. Zhao et al. (2005) suggested that 20 iterations of each test was sufficient to provide mean values of the results using descriptive statistics. By running multiple iterations for each simulation, those participating in the model and those not participating, would help account for any external influences that may impact the testing despite isolation efforts, and assist with providing validity and reliability of the data. The results in the report contain the mean values gathered across the multiple iterations of each instance.

Instrumentation

The instrumentation of the research exercise details how pertinent information is going to be gathered (Creswell, 2009). The instruments used to gather data for the study were those discussed in the Data Collection section. These instruments were responsible for gathering CPU utilization, bandwidth consumption, RAM consumption, and route convergence times. The instruments used to collect this data were designed for measuring those specific data sources by design and were not modified by this study.

As Creswell (2009) noted, if existing instruments are being used in an unmodified form, the researcher must consider the established validity and reliability of such tools. Certain areas surrounding the validity of the instrument need to be considered depending

on the nature of what is to be collected. The three main areas of validity to look for in chosen instruments include: content validity, predicative or concurrent validity, and construct validity (Creswell, 2009). Effectively, these forms of validity cover ground that an instrument measures what it is intended to measure, accurately predicts a criterion measure, or measures hypothetical constructs and concepts.

For this study, content validity was of the most importance. Content validity is significant as the tools available to measure metrics such as CPU consumption, RAM utilization, and route convergence times are observational in nature. The nature of those tools aligned well with the design of the study, which was a before-and-after comparison of the model minding the researcher's intervention. Predictive validity did not align as well because the study was not designed to predict the impact of the model; rather it was to measure the actual impact of the proposed mode. Furthermore, construct validity was not suited as well as content validity as the study was not intended to measure a certain explanatory variable that is not directly observable.

Validity and Reliability

Establishing the quality of research results can be described as the researcher's duty to establish the validity and reliability of research performed (Kumar, 2014). The terms validity and reliability both are used in describing the quality of research results, but they are not the same. Creswell (2009) noted that validity is not a companion of reliability or even generalizability. Validity should answer the simple question as to whether or not the researcher is measuring what he or she thinks they are measuring (Kumar, 2005). Therefore, it is important for the researcher to understand how validity should be described in the context of this research.

When viewing validity, the same connotations do not exist in quantitative research as they do in qualitative research. According to Creswell (2009), qualitative validity is determined if the research checks the accuracy of findings by implementing a set of certain procedures, whereas Venkatesh, Brown, and Bala (2013) state that quantitative validity refers to the legitimacy of findings. Furthermore, in quantitative research, two key issues that define validity are addressed, those issues being reliability and validity of measures.

Due to the nature and design of this quasi-experimental study, quantitative validity methods were more appropriate because the data collected is numeric, measurable data. Kumar (2014) constructed the definition of content validity as the instruments' ability to measure what they are designed to measure. One method of validating tools used to measure computational performance metrics is to collect the same metrics with another tool (Fortier & Michel, 2003). Testing measurements with multiple tools is popular when modeling is used to study the research problem. Fortier and Michel (2003) suggested that when a real system is available instead of a conceptual model, real system measurements are the most reliable means of validation as opposed to multiple simulated measurements. This study employed the operation of virtual routers actively participating in the proposed BGP route attestation model rather than the research being carried out in a simulated fashion. As a result, real system measurement was used to perform validation.

Reliability is another important part of evaluating a research instrument in addition to validity. Reliability is defined as the repeatability or consistency of a research instrument's measurements (Creswell, 2009). In essence, reliability is the repeatability of a measurement. An estimation of reliability describes a relationship between the

consistency and stability of the instrument that shows the predictability and accuracy of the measurements (Kumar, 2014). A higher degree of consistency and stability observed in an instrument indicates a stronger presence of reliability of the instrument.

To obtain this estimation of reliability, two main lenses may be used: how reliable an instrument is, and how unreliable an instrument is. If an instrument produces consistent measurements in the same or even similar environments, the should be considered reliable (Kumar, 2014). On the other hand, if collected measurements show a degree of difference when the instrument is used in the same or similar environments, the level of error can be used to describe how unreliable the instrument is. This forms an indirect relationship, the higher degree of error in the measurements, the lower degree of reliability of the instrument. Likewise, the lower degree of error or deviation in results indicates a higher degree of reliability of the instrument.

Of the different ways in measuring the reliability of an instrument, Kumar (2014) suggested observing two groups: internal and external consistency procedures. External consistency employs two separate processes of data collection that are used to verify the reliability of the measure. Within the external consistency group methods that exist are the "test/re-test" method as well as running parallel forms of the same test. Both methods provide the same insight into external consistency and circumstantially one method may fit a study better than the other method.

The test/re-test method is a repeatability test where the researcher takes measurements with an instrument, and the instrument is administered a second time within the same or as close to the same conditions as possible (Kumar, 2014). The resulting ratio is an indication of how reliable the instrument is; that is, the higher the ratio the higher reliability. The test/re-test method is particularly advantageous because

the method allows the researcher to test the instrument against itself, thus eliminating some complications that can arise when determining reliability. In certain studies such as a survey, the test/re-test method may be unfavorable as it can educate users in the test phase, possibly skewing the results. Unintended consequences such as user education during testing are not observed in technical studies where human subjects are not used.

A second method of performing external reliability testing is to run parallel forms of the same test. Kumar (2014) described this approach as creating a second instrument that is designed to measure the same results and administering both instruments at the same time against different populations. Reliability is determined if both of the instruments produce similar results at the end of administration. A parallelized approach is disadvantageous because of the difficulty in creating two instruments that are designed to measure the same phenomenon and deemed valid. Furthermore, the inconsistencies in population groups may also hinder the usability of this method. This approach does however remediate the problem of recall or user education as seen in the test/re-test external reliability testing.

For this research, a test/re-test methodology was used to determine external consistency. The rationale for choosing the test/re-test procedure takes into account both the population being studied as well as the instrumentation used to measure quantitative results related to computational overhead and route convergence times. Since the population was not human or learning by nature, rather the population was composed of virtual routers, the problem of recall did not exist. Secondly, the software used to measure CPU performance, RAM utilization, bandwidth utilization/consumption, and route convergence as previously described composed an instrument to measure overhead. These pieces of software were consistent with other related research (Seo et al., 2014;

Zhao, 2002). Those studies that utilized a similar toolset as outlined in the Data Collection section ran the tests numerous times and presented mean scores of the measurements, not in parallel execution. Running numerous tests and quantifying the results most closely aligns with the test/re-test procedure.

In addition to external consistency, internal consistency needs to be considered as well in certain circumstances. The goal of internal consistency is to ensure that any items measuring the same phenomenon should produce similar results (Kumar, 2014). Internal consistency is commonly observed when dealing with human subjects in a survey or test related technique. The idea being that multiple questions measuring the same type of data should produce similar results, thus indicating internal consistency. In this research, the instruments used to collect data were specifically designed to take the measurements related to overhead, and were not modified or adapted to suit a different purpose. In that scenario, a test/re-test method serves to estimate the reliability of empirical measurements most easily (Carmines & Zeller, 1979).

Data Analysis

Data analysis encompassed multiple areas to summarize the individual test results into meaningful and manageable results. While many different variations of data analysis exist and are applicable in different studies, there are central concepts to what data analysis should provide. Two key categorizations of data analysis exist, those being descriptive and inferential statistics (Babbie, 2013). Nonetheless, the intended result is the same, to interpret and present the data into a succinct summarization.

Choosing the appropriate categorization of data analysis is important to accurately make statements about general populations or to describe what is happening in a studied situation. Inferential statistics are commonly used when a research studies a sample

population and uses those observations to make larger generalizations (Rugg, 2007). On the other hand, descriptive statistics are designed to describe what is happening in a population or data set. Given the high-level nature of what inferential and descriptive statistics are intended to represent, descriptive statistics more closely aligned with the research goals in this study. The primary rationale for analyzing the data with descriptive statistics was that the study focused on an entire, controlled population rather than piecing out a sample of a larger population.

Descriptive statistics can be further broken down into two sub categories: central tendency and degree of spread. Central tendency is one of the most common methods of descriptive statistics as it aims to determine where the average set of values resides (Salkind, 2010). These values from central tendency may include mean, median, and/or mode. Salkind (2010) described the degree of spread as how data is disturbed with measurements of range. To maintain consistency with other similar studies (M. Zhao et al., 2005), mean values were used to describe performance and route convergence overhead.

Certain challenges do exist in performing statistical analysis of network data problems and computational performance monitoring. One of the primary challenges is the enormity of data that can be collected (Heard & Adams, 2014). Another challenge that relates particularly to network data is the correlation or timing of events.

To facilitate the analysis of this data, Kumar (2014) suggested that the data should undergo three primary steps including: editing the data, reducing the data, and analyzing the data. For this study, computational programs were used to better the fluency and accuracy of these three tasks. These computational programs were primarily used in the data analysis phase to perform complicated calculations used to derive descriptive

statistics (Kumar, 2014). Cleaning and reducing the data was an important part of making the collected data more manageable.

A primary set of goals for this process was to remove samples collected before and after the researcher's intervention, remove invalid results, and categorize the measurements. Once that was done, measures of central tendency or measures of spread were used to present trends or changes among the variables. Once the data was cleaned and categorized, the actual analysis was performed in order to test the hypothesis of the research and to draw conclusions. The results from the analysis will be detailed in Chapter 4.

Summary

The purpose of this quasi-experimental quantitative study was to determine what degree of overhead is introduced into BGP speaking routers when a model for route attestation is implemented. Chapter 3 provides details and insights into the overall design of the study, the technical objects being studied, and what methods will be leveraged. Areas surrounding the instrumentation, validity, reliability, and data analysis were also addressed in this chapter. Chapter 4 will detail the results of the study along with design characteristics and analysis of findings.

CHAPTER 4: RESULTS

The purpose of this quasi-experimental before-and-after study was to measure the extent of the relationship between routers participating in a BGP model to perform route attestation with IPv6 headers and the resulting performance impacts. Performance metrics were further defined as CPU utilization, RAM utilization, bandwidth consumption, and route convergence time. Measurements were taken to describe performance on virtual routers running the open source operating system, pfSense, in an isolated environment as described in Chapter 3. To summarize the collection methods, CPU utilization and RAM utilization were gathered using the vmstat utility. Bandwidth consumption was collected by running packet captures on both the router originating updates as well as a DNS server responsible for serving cryptographic keys used in attestation. Lastly, route convergence time was obtained through code changes in the OpenBGPD service on the routers. Chapter 4 describes the data that was collected as it pertains to answering the research question.

Data Collection

As described in Chapter 3, routers running in the virtual environment were subjected to a series of tests to obtain data describing the performance impacts of the proposed attestation model. A single set of virtual routers and virtual networks were used to gather the performance data in all tests. Using a single set of virtual routers and virtual networks provided consistency between resources allocated and device configurations. The OpenBGPD configuration used on each of the routers was unchanged throughout the study, and can be found in Appendix A. Details about the BGP environment are described by the OpenBGPD configurations including neighbor adjacencies and network

prefixes owned. In addition, the DNS server contained a TXT record populated with a public key that provided ownership for each network prefix. An example of the TXT record used for a DNS zone configuration can be found in Appendix B. A depiction of the network used in the study is represented below in Figure 1. Router AS1000 served as the sender of BGP update messages while router AS2000 received the updates and processed them. The Client workstation was used to remotely access the virtual routers via secure shell (SSH) in order to retrieve statistics and initiate each trial.

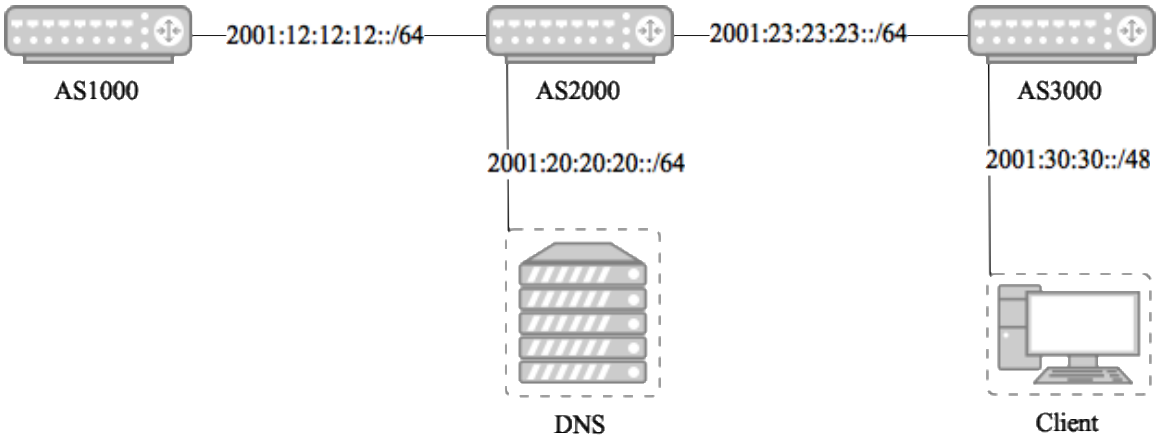

Figure 1. Network diagram representing the virtual environment used in data gathering phase.

Statistical data on receiving host's RAM and CPU performance utilization was gathered using the vmstat utility. This data was appended to a log file residing on the receiving host's file system and analyzed in CSV format. The vmstat utility was set to gather data on CPU and RAM consumption every 0.5 seconds throughout the duration of the trail. The receiving host logged vmstat output immediately before the BGP updates were sent and ceased logging the output immediately after the last BGP update was processed. Data gathered from vmstat was in a raw output format from the utility and was later sanitized and converted to CSV format in Microsoft Excel for analysis. A new log file was created for each trial performed and the summarized output can be found in Appendix C.

To obtain quantitative results about bandwidth consumption in the BGP updates received by a host, a packet capture utility, Wireshark, was used. Wireshark allowed for a host to record packets entering or exiting a network interface without modifying them. This technique is also known as a passive packet capture. The passive packet captures were run from the router originating the BGP update as to not impart additional or unaccounted for overhead on the host receiving the update. Even though the packet captures were passive in nature, RAM and processor resources were needed to interpret and store the data. By nature of the TCP protocol that is responsible for carrying BGP messages across a network, the packets were the same on the sending and receiving routers.

Initially, metrics were to be gathered for each trial consisting of 20 BGP updates to align with the study by M. Zhao et al. (2005). However, due to the speed of processing 20 route updates and the relative ease of gathering more data points, the desired sample size was increased to 1,001 updates per trail. Three trials were run without the attestation model as well as with the attestation model. As a result, more data was collected during the study, and provided a truer representation of the costs associated with the model. Furthermore, the increase in data collected allowed the trials to be run for a longer period and gave insight into the reliability of the data collection instruments.

In each trial, the sending router, AS1000, initiated 1,001 BGP updates, which were delivered to the receiving router, AS2000. Three trials were run in the environment before the attestation model was introduced, and three trials were run after the model was implemented. In total, the trials resulted in 3,003 convergence data points to be examined in each model. Having an equal number of data points between samples guaranteed that each treatment condition contributed equally to the results of the study

(Keppel & Wickens, 2004). Additionally, the BGP routing updates sent during the testing phases contained identical message contents and were initiated via a shell script to further promote consistency in timing and delivery. These convergence metrics were logged in comma-separated value (CSV) format on the Client host and later analyzed using Microsoft Excel. These summarized metrics can be found in Appendix D.

Results

Analysis of the data gathered through the trials describes the impact on performance that the BGP route attestation model had on participating routers. Guided by Kumar (2014), the collected data was organized, reduced, and analyzed to provide descriptive statistical results. The following sections detail the results as they pertain to BGP route attestation performance impacts: CPU Performance, RAM Utilization, Bandwidth Consumption, and Route Convergence Time.

Descriptive Observations: CPU Performance

CPU performance metrics were gathered via the vmstat utility, which polled every 0.5 seconds during each of the trials. According to (Weaver et al., 2013) a measurement of user and system CPU time, called process time, is an effective measurement to evaluate the performance of a program. The output of vmstat represented the process time in three different columns that showed user time, system time, and idle time as percentages of the total processor capacity. As Weaver et al. (2013) indicated, the sum of user time and system time forms process time. The process time served as the measurement describing performance on the participating routers as depicted in Appendix C.

A router running OpenBGPD while processing BGP update messages averaged 0.55% processor consumption. After the BGP update attestation model was introduced,

the average processor consumption of the router attesting BGP update messages was 4.17%. Overall, an increase of 3.62% processor time was observed relative to the trials where no route attestation was performed. This increase demonstrated the additional performance overhead imparted on a router that obtained the sender's public key through DNS and used it to verify the cryptographic signature of the BGP update message.

Descriptive Observations: RAM Utilization

Another important measurement in determining the overhead resulting from using IPv6 headers to carry BGP update attestation information was RAM utilization. Again, vmstat was used to gather information on the size of the free memory list belonging to the receiving router. The free list represents a linked-list of pages in memory that are readily available for a virtual memory manager (VMM) to allocate (Bacon, Cheng, & Shukla, 2013). In the duration of this study, the free list size decreased throughout the time the router was processing BGP updates for each trial. This indicated that the blocks of memory used to process the update had not been returned to the free table as the process BGP process was continually running.

By knowing the size of the free list before the trials of updates were sent, and the size of the free list after the router was done processing all of the messages, a sum of memory consumption could be calculated and averaged out for each update message. The resulting value showed the amount of RAM utilization for the duration of the trial. These memory consumption measurements were gathered as the receiving router was processing BGP update messages. Averaged figures representing the delta in free memory pages for each trial can be found in Appendix C.

On average, during the unsinged update trials, the free table decreased by 1.15MB or approximately 1,150KB. Therefore, the average amount of memory accessed per BGP

update was 1.15KB. As far as the signed update trials, the free table decreased by an average of 24.97MB per trail or 24,970KB. As a result, an average of 24.95KB was consumed by the receiving router to process and attest each signed BGP update message. In total, an increase of 23.81KB of RAM overhead was introduced per BGP update by the attestation model.

Descriptive Observations: Bandwidth Consumption

Bandwidth consumption as previously defined in this study is the number of bytes transmitted and received by a host while processing a BGP update message. In particular, bandwidth measurements were taken only in the lens of the host receiving the update message. Other relevant packets beyond the BGP update messages included the DNS queries sent to and from the DNS server used for route attestation.

Adhering to the definition of a quasi-experimental before-and-after study (Kumar, 2014), unmodified BGP update messages were gathered and served as a baseline for bandwidth consumed in a route advertisement. These packets displayed what the receiving host acknowledged in terms of bandwidth on an incoming BGP update. Analysis of the packet captures showed that each update message was 155 bytes in total. In the unmodified environment, no additional packets were needed to complete the update transaction. The format of a standard IPv6 packet carrying a BGP update and the attribution of the size of the packet can be seen in Figure 2. The depiction of the packet shows the minimum costs in terms of bandwidth consumed for BGP updates sent in an environment following the IP and BGP specifications. Understanding the minimum size and structure of the BGP update packets helps establish a baseline to measure any increases from the route attestation model. A bassline will also be used to demonstrate

where an observed size increase can be attributed to, and how the packet structure is modified by the model.

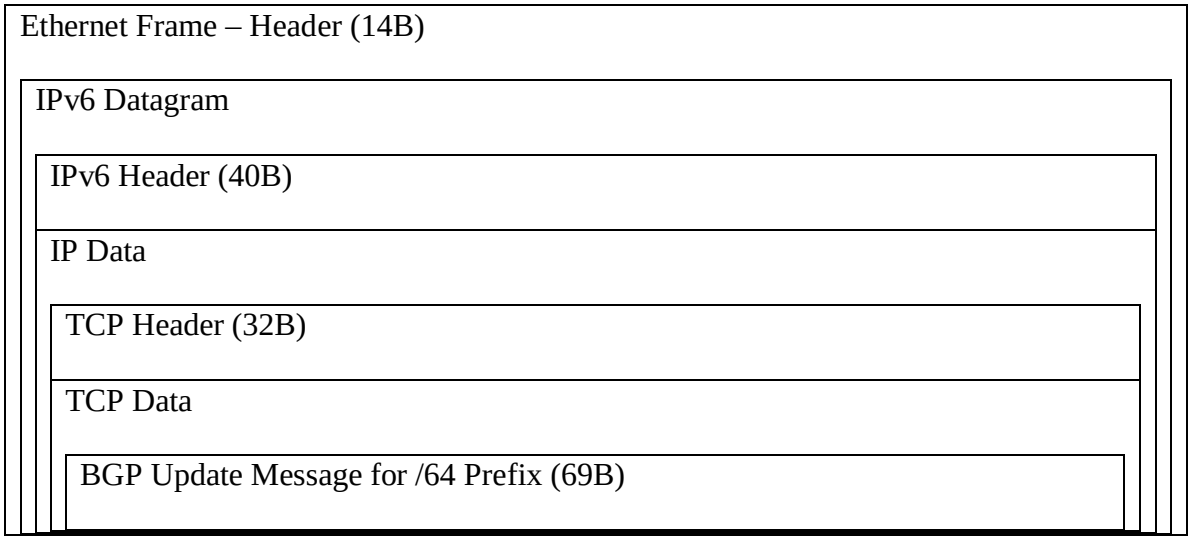

Figure 2. Standard format of an IPv6 packet carrying a BGP message with size shown in bytes.

A condensed packet dissection obtained from the passive packet capture can be found in Appendix E. The packet dissection shows that the environment was producing valid and compliant BGP update packets as presented in Figure 2 above. Confirming the generated BGP update packets were valid contributes to the validity and significance of comparative measurements made in the route attestation model. Such measurements were made to demonstrate the effects of using IPv6 extension headers to carry route attestation information have on packet size and bandwidth consumption.

In the modified model, IPv6 extension headers were used to carry attestation information by means of a cryptographic signature. In particular, the Authentication Header was used to transport the signature. Analysis from the passive packet captures obtained the model showed an increase in size of the update messages which is to be expected. Much like a signature on a document where the signees' name consists of letters on paper, the BGP sender's attestation signature consists of bytes in a packet

header. Regardless of the format, a signature adds data to the medium carrying it; in this case, the medium was the packet Authentication Header.

In the attestation model, a signed BGP update message consisted of 295 bytes. When comparing the unsigned BGP updates at 155 bytes to the signed BGP updates at 295 bytes, a 140-byte increase in bandwidth consumption was observed. Because the actual BGP update messages remained unchanged, the entirety of the increase in packet size resulted from adding an Authentication Header containing the signature of the message.

By the IPv6 specification for Authentication Headers, a minimum of 12 bytes are consumed in specifying the format and contents of the header (Kent, 2005). The 12-byte cost in adding an Authentication Header is therefore unavoidable. An additional 128 bytes existed in the Authentication Header that were composed the signature of the update message. In total, the size of the Authentication header was 140 bytes. A different length signature could be used in signing the packets, which would affect the total packet size of the message directly. A larger key-pair may be used to generate the message signature, but would also impart additional overhead on the receiving node in terms of incoming bandwidth consumed. Larger key-pairs in RSA signing schemes such as the one used in this study result in larger signatures.

With the programmatic changes to the BGP service, a packet carrying attestation information had the format shown in Figure 3. The depiction of the modified packet clearly shows how the model modified the structure by the addition of the Authentication Header. All other portions of the packet retained the same size and structure of the unmodified BGP update as previously shown in Figure 2. Comparison on the unmodified and modified packets clearly shows where an increase of packet size occurred due to the

Authentication Header. Furthermore, no other elements of the packet were modified by the model, thus attributing the 140-byte increase that was observed directly to the Authentication Header.

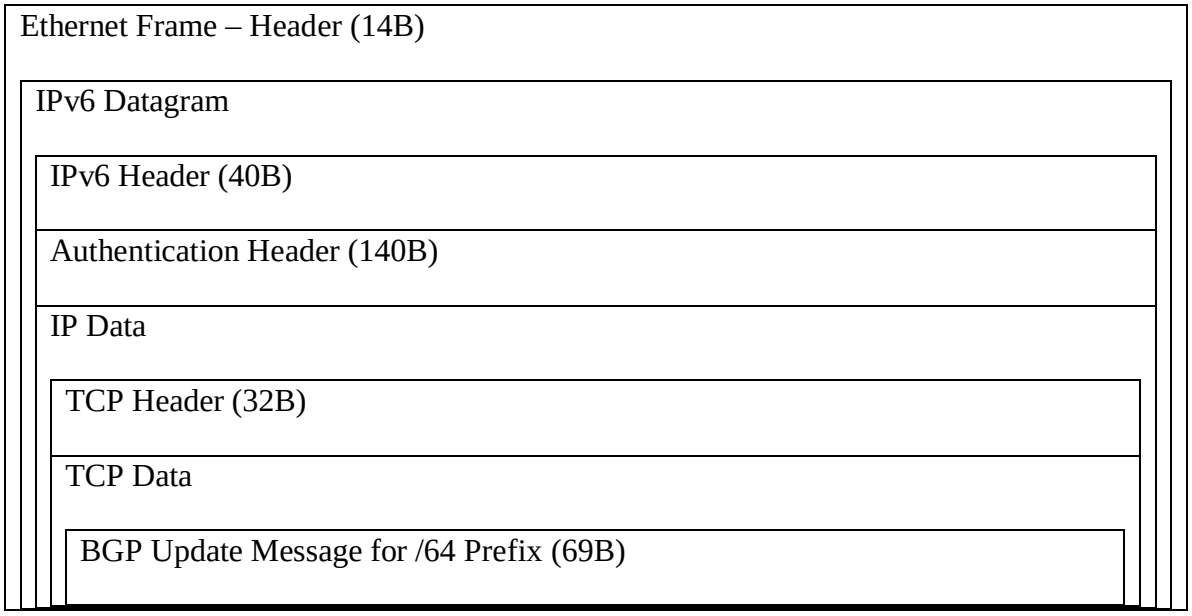

Figure 3. Format of a modified IPv6 packet carrying a BGP message and attestation data with size shown in bytes.

Appendix F contains an abbreviated packet dissection obtained from the passive packet capture detailing the modified packet. The dissection of the modified packet shows the detailed addition of the Authentication Header as well as its attestation contents. Further analysis of the packet dissection reveals that the only change between the unmodified packet and the packet carrying attestation data was the addition of the IPv6 Authentication Header. Therefore, by comparative analysis, the Authentication Header was the source of bandwidth overhead in carrying the signature.

A more detailed view of the Authentication Header shows the fixed fields that cannot be changed as well as the variable length field used to contain the 128-byte message signature. The following five fields within the Authentication Header have a static length and imparted a 12-byte cost: Next Header, Payload Length, Reserved, and

Security Parameters Index. The remaining field, Integrity Check Value, is a variable length field, and held the 128-byte update signature in this study as shown in Figure 4.

Next Header (1B)	Payload Length (1B)	Reserved (2B)
Security Parameters Index (4B)		
Sequence Number (4B)		
Integrity Check Value (variable, 128B in this study)		

Figure 4. IPv6 Authentication Header format with size shown in bytes.

An additional source of increased bandwidth consumption in the attestation model was introduced by the necessary DNS queries initiated by the receiving host. As outlined in the model's design, a router receiving a BGP needed to obtain the sender's public key to validate the authenticity and authorization of the update. For every BGP update packet that the receiving router acknowledged, two DNS packets were created. These DNS packets were composed of one query packet from the receiving router to the DNS server, and one response from the DNS server to the querying router.

DNS query packets originated from the receiving node and asked the DNS server to return the sender's public key, which was held in a TXT record. The query packets used to ask the DNS server for the key were each 154 bytes long. In response, the DNS server's reply that contained the public key consisted of a single DNS query response packet of 383 bytes in length. Again, this response may vary based on the key size chosen for the cryptographic signature. In this model, DNS overhead introduced in obtaining the sender's public key was 537 bytes in total. A summarized DNS conversation gathered from the packet capture can be found in Appendix G.

In summary, the attestation efforts introduced by this model resulted in a 677-byte increase in bandwidth consumed. In total, the transaction of a receiving and validating a

BGP update message costed the receiving router 832 bytes as compared to 155 bytes in an unsigned update. Within the 677 bytes of overhead, 154 of the bytes were transmitted by receiving router as outgoing bandwidth, and the remaining 523 bytes of data were received by the router as incoming bandwidth. An autonomous system operator may view different costs in terms of ingress and egress bandwidth as the costs may affect the adoptability of the model.

Descriptive Observations: Route Convergence Time

To gather convergence timing metrics, the researcher modified the OpenBGPD source code to include timestamps for route received events as well as when routes were placed into the routing table. The programmatic changes can be observed in Appendix H. Other than the addition of timestamp routines, OpenBGPD remained otherwise unmodified in the before portion of the study. In the after portion of the study where the source code included attestation methods, the timing routines were unmodified from the prior sequence. Therefore, the same modification existed in both before and after the intervention, thus eliminating variances between the two tests.

Before the attestation model was introduced, data was gathered to describe the processing time it took the BGP service to receive an update and commit it to the routing information base. When OpenBGPD received an update to the Session Engine (SE), the process responsible for handling BGP messages, it performed a check to determine what type of message was received. After the message-type was determined, any updates were sent over to the Route Decision Engine (RDE) for processing. The RDE then determined update validity and placed the prefix from the update in the routing table or discarded it accordingly. At this point, the processing of the update was finished and a measurement was taken. Therefore, the collection of this data spanned from when the route was

deemed and update by the SE until the point at which it was processed or discarded by the RDE.

As aforementioned in the Data Collection section, trials of 1,001 updates were studied. In total, 3,003 updates were processed in the unattested environment and 3,003 additional updates were processed with the attestation model in place. An average convergence time was calculated to serve as a baseline in typical BGP operation, which formed a baseline to perform relative comparison against. The average convergence times are displayed in Appendix D.

Averages were calculated of all 3,003 updates that were gathered between the three different trials for unsigned and signed updates. The average processing time for OpenBGPD receiving an update on the SE and accepting it in RDE without attestation routines was 0.000211 seconds. When attestation routines were added to perform the public key lookup and cryptographic signature verification, the average increased to 0.018330 seconds. In relative comparison, the signed updates took 0.018119 seconds longer to process on average.

The increase in convergence time includes the retrieval of the sender's public key through DNS as well as the cryptographic validation of received BGP messages. On an average across the attested route updates, DNS query and response time took 0.000689 seconds. The data collected from all three trials as describing overhead imparted by the DNS transactions can be found in Appendix I. The remaining increase in route convergence time compared to the unattested model can be attributed to the processing of the cryptographic message signature.

Statistical Analysis

Many different methodologies exist to demonstrate the applicability of a study to larger populations demonstrating statistical significance (Keppel & Wickens, 2004). Choosing the most appropriate model for evaluating research requires the analysis and understanding of factors contributing to the measured results (Creswell, 2009). Salkind (2010) asserted that when collecting data in an experiment, the outcome is always susceptible to a degree of unpredictability by chance. Due to the degree of unpredictably by chance is therefore necessary to identify areas within a study that can be described in terms of statistical significance.

Statistical significance is used in order to show that any difference observed in the analyzing the results is an outcome of the researcher's intervention, not chance given the research hypothesis (Keppel & Wickens, 2004). Tests are used to prove or disprove the research hypothesis and demonstrate statistical significance by the ability to reject the null hypothesis. Keppel and Wickens (2004) described the null hypothesis as the exact opposite of a research hypothesis. Guided by definition, the null hypothesis in this study would be that the BGP route attestation model adds no additional cost in terms of performance overhead.

Identifying a Method to Demonstrate Statistical Significance

The research proposal of this study did not specifically identify a method for determining statistical significance. Not identifying a method for determining significance in the proposal promoted the opportunity for the researcher to select appropriate tests based on the sample size and types of data collected. Factors including the number and variety of data points were taken into consideration as well as the focus of answering the research question contributed to the choice of method.

Choosing the correct test to demonstrate statistical significance takes into account several factors about a study including variances in a population, number of data points collected, and the research hypothesis (Terrell, 2012). In addition, the number of independent and dependent variables were taken into account as well as the quantitative nature of the study. The independent variable in this analysis was observed to have two levels: environment using the attestation model, and environment not using the attestation model. Alongside of the independent variable, measurements were taken to describe the dependent variable, route convergence times. In a scenario where there is one independent variable with two levels and one independent variable, Terrell (2012) recommended the use of a t-test to evaluate statistical significance.

Statistical Significance

Multiple tests are designed to demonstrate statistical significance (Keppel & Wickens, 2004; Salkind, 2010; Terrell, 2012). T-test and F-tests are among the statistical significance tests for evaluating contrasts recommended by Keppel and Wickens (2004). F-tests may be used to indicate variance between populations, which then contribute to the calculation of the t-tests. Keppel and Wickens (2004) noted that t-tests are effective in providing conclusions where groups may contain unequal sample sizes or variances. F-tests were first calculated to determine the population variances and indicated that the samples did not share the same variance. For this study, t-tests were used to evaluate statistical significance because of the difference in variance of the measured route convergence times.

Proper statistical procedures were followed throughout the t-test calculations (Keppel & Wickens, 2004; Terrell, 2012). Data was analyzed and calculations were performed using Microsoft Excel. To calculate the variance and t-test statistics, the

collected data on route convergence times were split into two groups: routers not using the attestation model, and routers participating in the attestation model. After separating the collected data into two groups, calculations were performed to determine each sets' mean and sum squared deviates. The mean and sum squared deviates were used in determining the populations variance, standard deviation, and t-value.

Sample Variance

Sample variance provides insight into the spread and variability of data values (Ross, 2004).The first major calculation in determining the type of t-test to be used was to find the variance of the sample. Acceptable degrees of freedom in a t-test are in part dictated by knowing the sample variances, specifically if the variances are equal or not (Terrell, 2012). A method of computing variance in samples is defined by Ross (2004) as an average of the squared differences of each measurement from the mean of the sample. Another common methodology of calculating variance in applied research is through the computation of an f-test (Keppel & Wickens, 2004). Due to the applied nature of this study, the f-test was chosen to calculate sample variances.

Variance was calculated by performing an f-test two-sample test. The f-test computations were run using Microsoft Excel as suggested by Salkind (2010) to obtain sample variances. For the signed update set of data, the calculated variance was 0.00032874. As far as the unsigned update set of data, the calculated variance was much smaller at 5.2916×10^{-9}. The resulting F value was then calculated as a ratio of variances in the unsigned update data set and the signed update data set. F for this study was calculated as 62124.60722. The information gained from the f-test dictated the type of t-test to be used to evaluate the statistical significance of the data which assumed unequal variances (Terrell, 2012).

Calculation and Evaluation of Statistical Significance

Next, a t-test statistic was calculated to estimate the population mean and evaluate the null hypothesis. The t-test statistic was calculated by assuming unequal variances in two samples as guided by the results of the f-test. This study focused on comparing results of new model to an established one, which aligns with applied research. A one-tailed, directional approach was used as Keppel and Wickens (2004) suggested that it is best suited for applied research. Additionally, Terrell (2012) stated that a one-tailed directional test is most appropriate in research where a directional hypothesis is to be evaluated as it is in this study.

One of the first steps to computing a t-test result is to determine the alpha level, also referred to as the significance level (Terrell, 2012). An alpha level of 0.05 was chosen giving a 95 percent confidence interval, which is most common among researchers (Keppel & Wickens, 2004; Terrell, 2012). The t-test was performed with 3,002 degrees of freedom and was used to determine a level of significance (*p*-value) between the unsigned and signed samples. Given the desired confidence interval and the degrees of freedom of the test, the critical one-tail value needed to demonstrate statistical significance was calculated as 1.64536 (Terrell, 2012). Additionally, the *p*-value was calculated as less than 0.00001, significantly less than the alpha level of 0.05. Analysis of the data revealed a t-value of 54.76270, which is well above the required critical value of the t distribution. Therefore, the null hypothesis is rejected and the difference between sample means statistically shows the increase in route convergence time when using the proposed model.

Other Measurements

The other measurements gathered in the study are examined under a slightly different lens than the route convergence times. CPU performance and RAM utilization measurements resulted in less descriptive data points as they represent the mean over all 3,003 updates in each sample. Nonetheless, the same t-test procedure was calculated against each of the metrics across the trials. CPU consumption averages were higher in the attestation model as compared to those measurements gathered in the model where no attestation was performed. Computation of the t-value for CPU performance showed statistical significance with calculation of 8.18693 and a *p*-value of 0.00730. Average RAM utilization was higher in the model where route attestation was being performed across all three trials and resulted in a t-value of 31.53878 and a *p*-value of 0.00050.

Bandwidth consumption was not analyzed for statistical significance as the costs associated with the attestation model were fixed. As OpenBGPD was assumed to be implementing BGP correctly (Bakker et al., 2013), the modifications to the packet contents and structure would be the same across a larger population that also correctly implements BGP. Key sizes and all other data structures remain the same in the model design, and therefore would impart the same bandwidth consumption increases as defined in the descriptive observations. Other routers adopting the model should have the same observations in terms of bandwidth consumption assuming that they elected the same implementation of the mode.

Summary

The quantitative results of the research study were presented in Chapter 4. As dictated by the before-and-after design, a series of tests were performed on a set of

routers running BGP with no route attestation model implemented. After the initial set of data was collected on the environment, the researcher introduced the route attestation model and performed the same tests on the environment. Together, the series of tests formed a comparative foundation on which to draw descriptive statistics.

Microsoft Excel was used to analyze the results from both scenarios that were obtained from log files and terminal output within the environment. The analysis on the data was performed through two lenses: descriptive analysis and analysis for statistical significance. The descriptive analysis of the quasi-experimental before-and-after study showed that the introduction of a model where IPv6 headers are used to carry BGP attestation information caused performance overhead. The additional performance overhead was observed in all areas measured during the study including CPU performance, RAM utilization, bandwidth consumption, and route convergence time. Attribution of the performance overhead was discussed and is further detailed in Chapter 5. Additionally, a t-test statistical model was used to evaluate the statistical significance of measurements as they pertained to CPU performance, RAM utilization, and route convergence times. The increases in performance overhead observed in all three categories was found to be statistically significant. Finding statistical significance furthered the case that the observations were in fact a result of the researcher's intervention on the environment, the intervention being an introduction of the attestation model.

Chapter 5 will detail the study's limitations as they pertain to research design, impact of external variables, specific security risks mitigated, and considerations surrounding the cryptographic model used. Furthermore, findings interpretations about the CPU performance, RAM utilization, bandwidth consumption, and route convergence

times will be presented. Lastly, the researcher's recommendations and identified opportunities for future research related to the study are detailed in the subsequent sections.

CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS

Attacks on BGP, specifically sub-prefix hijacking, have the potential to cause widespread outages and impact resources across the Internet (Bornhauser & Martini, 2011; Yun & Song, 2015). Furthermore, since BGP is the public routing protocol used to facilitate communication between Autonomous Systems, the possible consequences of attacks on BGP are vast (Cardona et al., 2016). Therefore, providing security mechanisms to protect BGP against such attacks is critical in the continued accessibility of Internet resources (Bullock et al., 2015; FCC, 2012; Mahajan et al., 2002).

Several different BGP security mechanisms have been introduced and designed to mitigate the risks of successful attacks being carried out (Bruhadeshwar et al., 2011; Hu et al., 2004; J. Israr et al., 2010; Kent et al., 2000; Malhotra & Goldberg, 2014; White, 2003; Ying et al., 2009). However, none of the aforementioned solutions have addressed the associated security issues still present in the IPv6 implementation of BGP (Butler et al., 2010). Additionally, previously proposed solutions suffered from poor adoption rates due to the perceived overhead and cost associated with them (P. Gill et al., 2011).

The specific problem addressed by this research is that extremely limited research has been done on using IPv6 in an effort to protect BGP against attacks such as sub-prefix hijacking. This study proposed a model to address the sub-prefix hijacking shortcoming of BGP through an examination of literature on attacks against BGP, cryptographic solutions, IPv6 packet structure, IPv6 security mechanisms, and proposed BGP security solutions. The proposed model used IPv6 extension headers to carry BGP update attestation information generated by a cryptographic solution, and studied the resulting performance-related impacts.

Limitations

The choice of research design and methodology may have imposed certain limitations regarding the results of the study. As Kumar (2014) indicated, a before-and after design does not allow one to draw conclusive evidence that change can be credited to the researcher's intervention. In part, conclusive results cannot be obtained due to the non-random sampling and selection of the population. As seen with true experiments, random sampling eliminates certain differences in the characteristics of the devices being studied (Creswell, 2009). Since this study was done under a quasi-experimental design, the careful duplication and resource allocation of virtual routers minimized possible differences in the population to diminish the impact of non-random sampling. Other disadvantages exist within before-and-after studies as they result in a measurement of total change. This means that the baseline measurements are compared to those taken after researcher intervention. As a consequence, extraneous and independent variables cannot be quantified as to their direct contribution of change (Kumar, 2014).

While effort and planning was put forth to eliminate outside variables affecting the results of the study, it is not possible to entirely account for all possible variables. A segmented virtual environment was used to host the set of routers, DNS server, and client machine that were used for each test performed. This environment provided for a consistently configured set of routers and devices while maintaining the exact underlying hardware and resource allocation. Type I hypervisors as used in this study have a complex nature in terms of potentially unaccounted for influences on the results, as do the routers that were studied. In both the hypervisor and the router, there are many necessary supporting processes that perform tasks both known and unannounced to reporting software. Therefore, throughout the study, it is conceivable that variables

unaccounted for may have affected the overall results. Additionally, the point of variance due the enormity of data in a computer network study and correlation of timing is underlined by Heard and Adams (2014).

This study aimed to provide a system to attest BGP routes in order to protect a recipient from sub-prefix hijacking attacks. Other attacks against BGP such as Denial of Service (DoS), neighbor spoofing, subversion, or redirection attacks may still affect routers operating BGP (Ola & Constantinos, 2004; Qi, Xinwen, Xin, & Purui, 2015). No attacks or threats to BGP other than sub-prefix hijacking were intended to be mitigated by the proposed attestation model. Other undesirable impacts to BGP caused by misconfigurations and accidental route advertisements may be avoided using the attestation model. Such cases of misconfigurations may occur where an autonomous system operator accidentally advertises a route belonging to another autonomous system. While the mitigation of such misconfigurations could be an effect, it is unintended.

Part of the attestation model was based on a similar concept as seen in Domain Keys (Hansen & Hallam-Baker, 2009). As in Domain Keys, the model required a sender of a message to publish their public keys into a DNS record. The idea being that the sender of a message signed their message with a private key, and the recipient decoded the message using the public key obtained from the sender's DNS record. This key-pair was used to create and decode a signature providing attribution and authenticity of an update message. Similar problems to those observed in DKIM existed in the attestation model. For example, if an attacker were able to capture a valid update message in transit to the intended recipient, the attacker would also have captured the signature of the message. A captured signature could allow the attacker to perform a replay attack, thus relaying false information appearing to originate from the valid sender (Kahate, 2013).

Furthermore, storing the cryptographic keys within a DNS record imposed certain limits on the size of the key which may affect overall cryptographic strength. Technically speaking, a DNS TXT record can be a maximum of 65,535 bytes, but are more practically implemented at just a few hundred bytes (Cheshire & Krochmal, 2013). According to Cheshire and Krochmal (2013), constituent strings within DNS TXT records are limited to 255 bytes. The 255-byte limit forced a restriction on the length of public key able to be stored in one record, and therefore affects the potential effectiveness of a cryptographic signature. A shorter cryptographic signature may be more susceptible to the deciphering or derivation of a sender's public key, compromising the attestation information.

Lastly, the skills of the researcher may have affected the validity of the study. The researcher's limited experience and research expertise attribute to the possibility of impact in soundness. During the study, an assumption was made that the researcher did indeed possess the needed skills and mentorship to conduct and report on a study of this design and nature.

Findings and Interpretations

Literature shows that BGP is susceptible to cyber-attacks that can result in compromise to availability and integrity of services across the Internet (Bornhauser & Martini, 2011; Sun et al., 2015; Yun & Song, 2015) . While solutions have been proposed to secure BGP in IPv4 space, little has been done to assess and enhance the protocol's security in IPv6 (Butler et al., 2010). Furthermore, adoption rates of BGP security solutions are affected by negative impacts to performance and route convergence times as identified by network administrators (Lychev et al., 2013). These given facts led the focus of this quasi-experimental before-and after study to investigate the possibility of

using IPv6 extension headers to carry route attestation information. An attestation model was built to evaluate the quantitative costs of performing BGP route attestation with the IPv6 extension headers. The following discussion delivers a summary of the numeric findings and interpretations that were discussed previously in Chapter 4 as they describe the following metrics: CPU performance, RAM utilization, bandwidth consumption, and route convergence times.

CPU Performance

Metrics on CPU performance were gathered over the course of three trials totaling 3,003 BGP updates for unattested routes as well as 3,003 BGP updates for attested routes. When compared to an environment where no route attestation was being performed on BGP updates, the attestation model required a higher percentage of CPU time consumption. On average, processing the signed update messages increased processor time consumed by 3.62%. The bar graph in Figure 5 shows the comparison of average CPU percentage consumed during each trial in the signed and unsigned BGP update models. A clear increase in CPU consumption was observed in the signed update model, with the highest average increase being 5.01%. Again, while there is a notable increase when compared to the unsigned model, the overall increase is a relatively small portion of the router's overall processing resources.

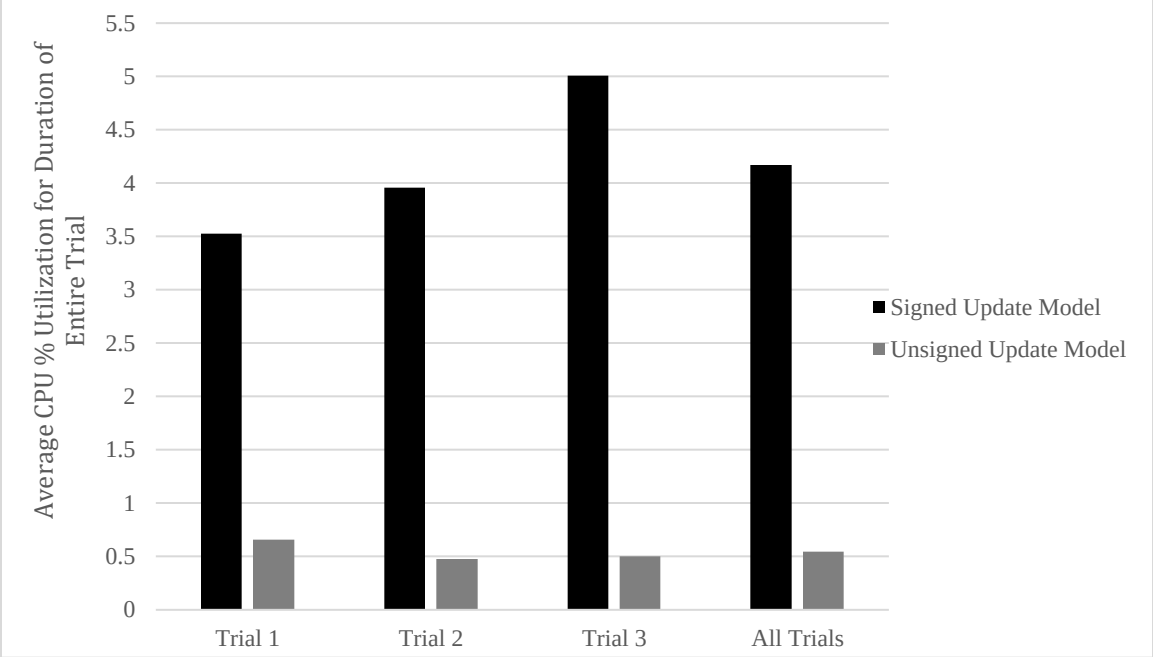

Figure 5. Average CPU consumption % for the trials in both attested and unattested models.

Statistical significance was primarily evaluated using a t-test statistical method, which showed a strong indication of statistical significance in the measurements. The observed increase in CPU processing time was likely due to the cryptographic routines required to validate the sender's message signature. Software-based cryptography has been shown to be resource intensive and often times a cause of overhead in security models (Mathew et al., 2015).

RAM utilization

RAM utilization was measured simultaneously with CPU performance measurements, using vmstat. On average, in an unattested model, an attested BPG route update took 24.97KB extra memory when compared to updates carrying no attestation information. The bar graph displayed in Figure 6 shows the average amount of RAM it took for the router receiving the BGP update message to process it. While the increase in RAM utilization looks large on the chart, the data sizes are relatively small compared to

the router's overall memory capacity of 1GB in this study. The overall memory consumption of the router was increased by 0.002497% when performing route attestation.

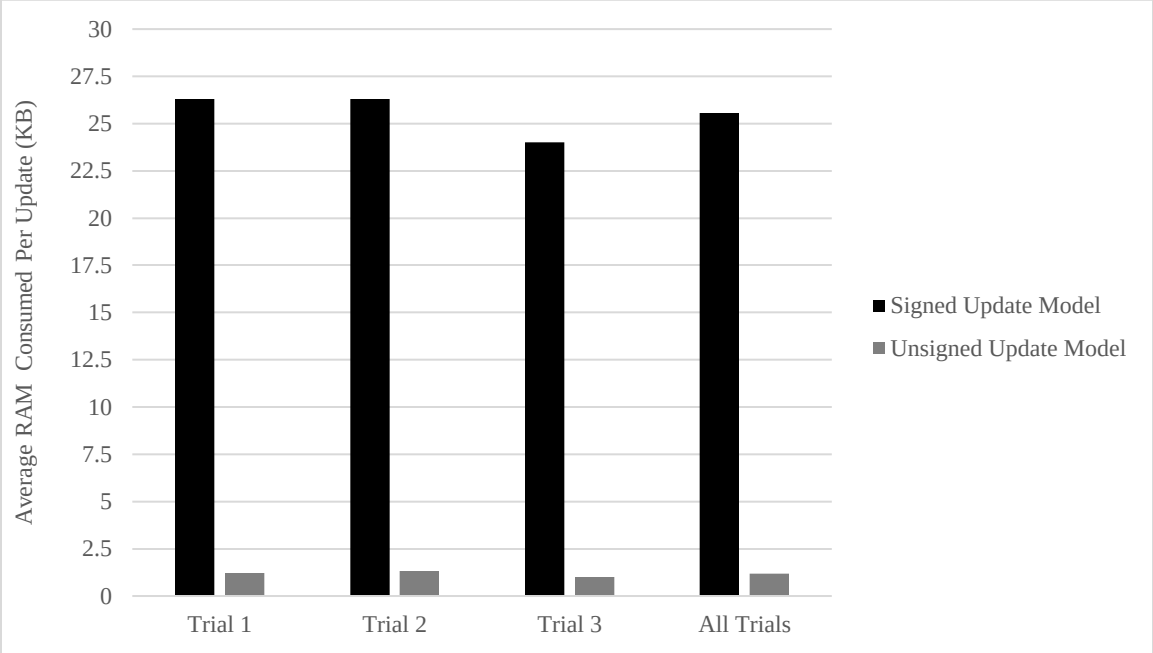

Figure 6. Average RAM utilization per update processed for each trial in the attested and unattested models.

Statistical significance t-test showed this result to be statistically significant in the analysis phase of interpreting the results. RAM consumption may also be attributed to the cryptographic routines as Mathew et al. (2015) indicated. Additionally, RAM was used to store the sender's attestation signature obtained from the IPv6 authentication header. Both the storage of the signature and cryptographic processing contributed fixed and variable costs in RAM utilization respectively.

Bandwidth Consumption

Bandwidth consumption metrics were gathered for each signed and unsigned update sent across the network throughout the duration of the trials using the Wireshark utility. Due to the way specifications designate the IPv6 Authentication Header format

(Carpenter & Jiang, 2013), BGP message size, DNS query, and DNS response sizes, a fixed cost in terms of bandwidth consumption was exposed. The added bandwidth consumption when compared to an environment where no attestation was taking place stemmed from two areas: retrieval of the sender's public key and the BGP update message signature. Over the course of each DNS transaction used to acquire the sender's public key, 537 extra bytes were exchanged between the querying router and the trusted DNS server. The IPv6 authentication header introduced 12 bytes of header formatting and an additional 128 bytes of cryptographic signature, or 140 total bytes of overhead. In whole, 677 bytes of bandwidth overhead were introduced by the model per update.

Figure 7 shown below depicts the sources of the aforementioned costs in terms of the increases in bandwidth consumption. These costs did not exist in the unattested BGP routing environment, and are therefore a representation of the overall bandwidth overhead introduced by the attestation model. The data can be separated out into two categories for further explanation: DNS retrieval of the sender's public key, and attestation signatures carried in IPv6 Authentication Headers.

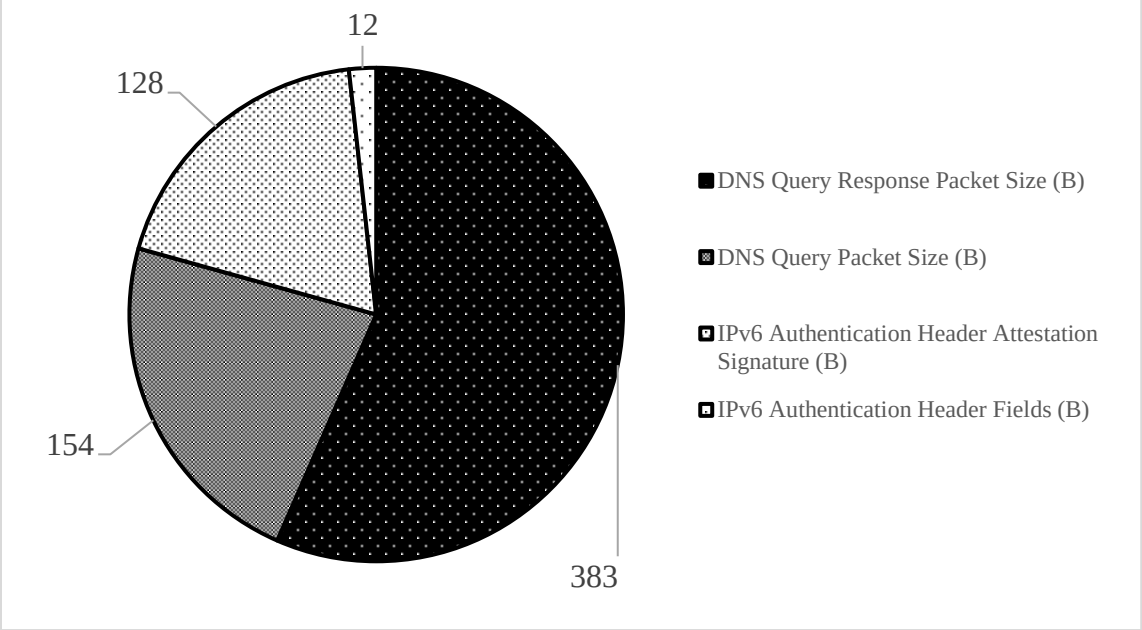

Figure 7. Pie chart representing the attribution of bandwidth consumption overhead.

The largest source of bandwidth consumption overhead introduced by the model was from the DNS query and response packets. The query packet was used by the sender to ask the trusted DNS server for the sender's public key. The response packet was sent from the trusted DNS server back to the querying router and contained the sender's public key. Only certain information contained within the DNS packets was essential to the attestation process. In the query packet, the attesting router identified the network to be attested. In response, the DNS server's reply contained the sender's public key. These two pieces of information introduced unavoidable overhead given the chosen cryptographic methods. The rest of the data transmitted through the query and response can be classified as overhead introduced by DNS.

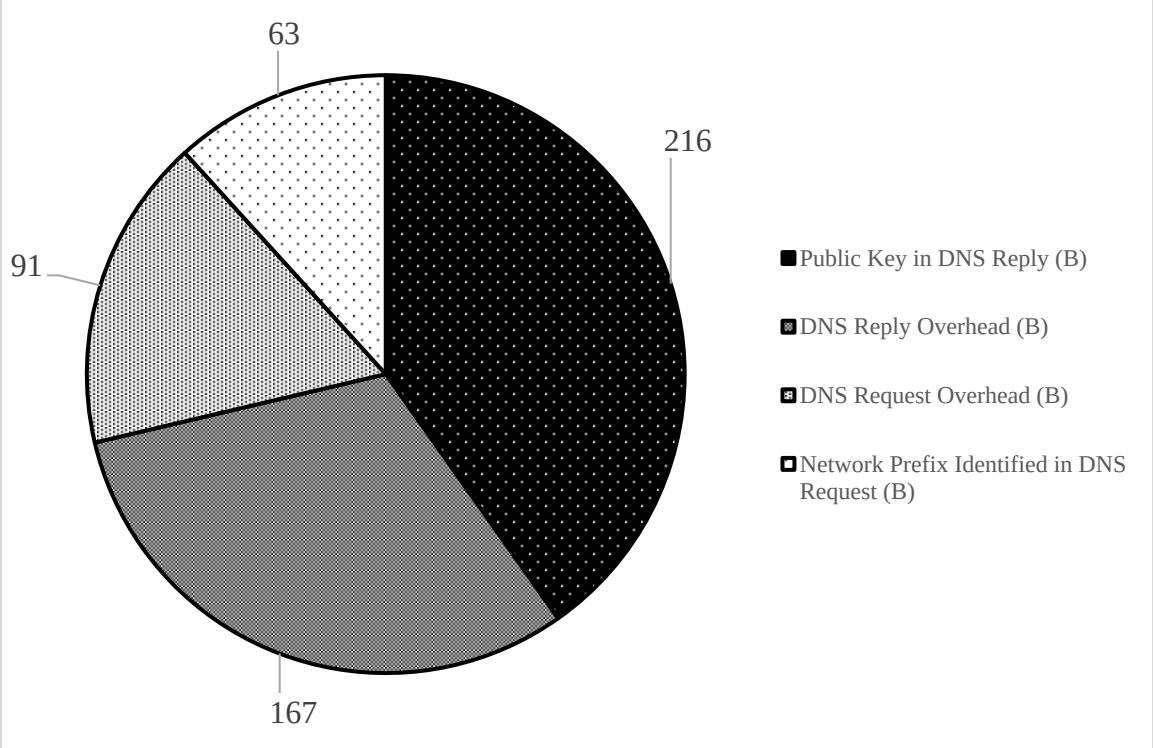

Figure 8. Pie chart showing critical attestation information for public key retrieval and DNS transaction overhead.

Figure 8 graphically represents the breakdown of bandwidth consumption overhead imparted by the DNS transactions used to obtain the route originators public key. The largest portion of overhead came from the transfer of the actual public key associated with the sender. This 216-byte cost would be unavoidable in scenarios that used the same RSA public key size to represent the owner of a network prefix. In the original query, a 63-byte cost was also unavoidable, as the recipient of the update had to identify the network that it was requesting the key for. Therefore, a total of 258 bytes of bandwidth overhead were introduced by the DNS protocol itself. Despite the overhead related to the protocol itself, DNS was chosen as it is widely accepted and understood in the public Internet space by autonomous system operators. However, in an effort to minimize the impact of the model, a different protocol that shares the adoptability aspects of DNS may be considered for the retrieval of a sender's public key.

Following the increases caused by DNS, the second largest contributor of bandwidth consumption in the attestation model was the inclusion of a message signature on each BGP update. The attestation model required the sender of a BGP update message to cryptographically sign the message and place the contents into an IPv6 Authentication Header. A result of using the Authentication header was less transmitted packets between the sender and receiver of a BGP update and therefore, less bandwidth consumed.

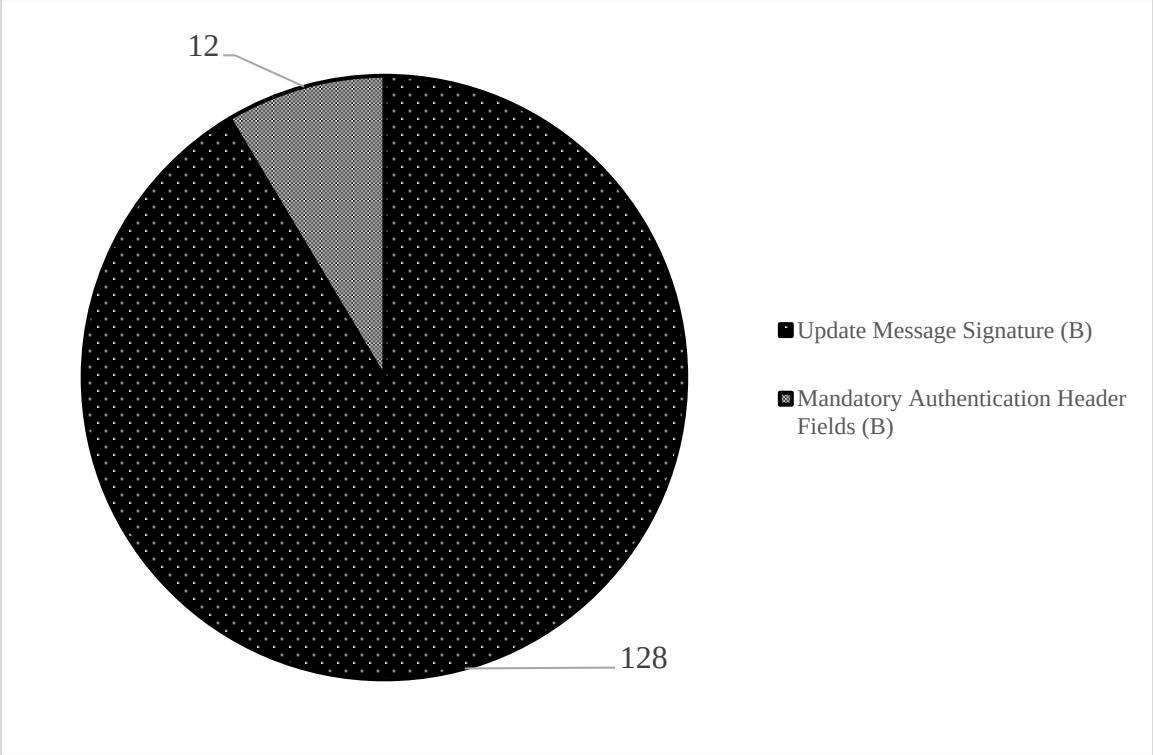

Figure 9. Pie chart displaying IPv6 Authentication header size and BGP update message signature size.

Figure 9 depicts the size relationship between the IPv6 Authentication Header's mandatory fields and the size of the BGP update message signature. The minimized impact on bandwidth overhead is clearly visible as only 12 unnecessary bytes of data are transmitted in addition to the required 128 bytes of the message signature. At a minimum, if an additional IPv6 packet was sent to carry the message signature, 40-bytes

would be introduced for the traditional IPv6 packet header. Extension headers remove the need for additional packets and in examples such as this, have a lower cost. No matter the carrier, the message signature will be a fixed size in all models using the same type of RSA public and private key pairs. Overall, a very marginal amount of bandwidth consumption overhead was introduced in relation to using the Authentication Header.

Unlike the other measurements in this study, bandwidth consumption was not analyzed for statistical significance. The bandwidth overhead introduced by the model would have the same impacts to other routers that properly implement IPv6 authentication headers, the BGP protocol, and chose the same cryptographic key sizes. Due to the universality of these measurements, statistical analysis for significance was omitted.

Route Convergence Times

The last significant measure of this study described route convergence times, or the time it took a router to receive, process, and commit a BGP update to the routing table. On average, attested route updates took 0.018119 second longer for the router to converge on when compared to unattested route updates. As with CPU processing time and RAM utilization, these measurements were shown to be statistically significant using t-tests. Many contributing factors composed this increase in route convergence time, as it is essentially a measurement of the attestation model's delay. DNS transactions caused an average of 0.000689 seconds delay in that the querying router had to generate a request and wait for the trusted DNS server to respond. Furthermore, the cryptographic routines also accounted for the increase in route convergence time. The relationship between the DNS transactions and the cryptographic routines are depicted in Figure 10.

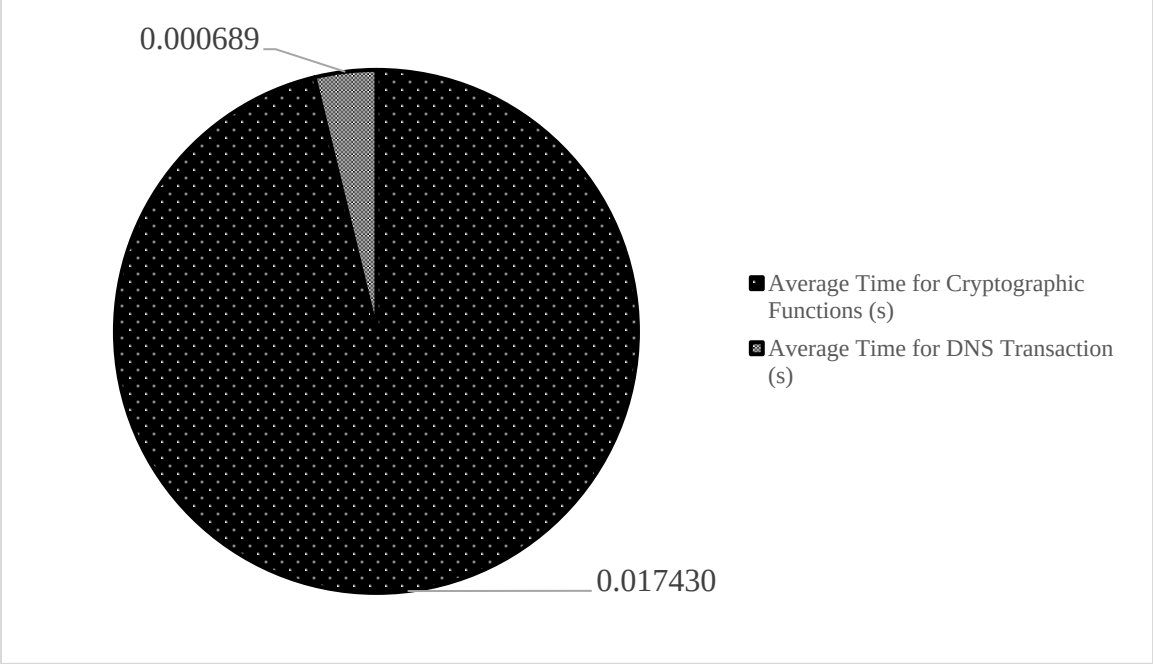

Figure 10. Relationship between overhead in convergence time caused by DNS transactions and cryptographic functions.

Recommendations

This study pursued the relationship between implementing a BGP route attestation model using IPv6 extension headers and the resulting impacts to router performance. A review of literature showed a clear need to improve the overall security of BGP against various attacks, including sub-prefix hijacking. Several studies showed that such protections were possible in the IPv4 implementations but exploration into IPv6 solutions was extremely limited. Furthermore, the previously proposed solutions were associated with high performance costs to the operation of the routers, which directly affected their adoptability. Idealistically, the overall benefits of enhanced security and protection of network resources would be the top priority of network operators, but such is not the case. Usability and end user experience are often prioritized over security.

Guided by the preparation, literature review, design of the model, implementation of the model, and analysis of the results, recommendations can be made. These

recommendations encompass viewpoints and insight gained from the performance of the study. This section addresses recommendations in the following areas: using IPv6 extension headers for route attestation, reducing performance costs in the attestation model, motivation to adopt secure routing models, and the need for additional research on the subject.

Using IPv6 Extension Headers for Route Attestation

A proof-of-concept BGP route attestation model was created and implemented in this study. The attestation model showed that IPv6 extension headers could be successfully used to carry signatures of a BGP message to prove authenticity and authorization. The study demonstrated that IPv6 extension headers could be used to carry signature information efficiently due to the performance driven qualities that surround them while imparting a limited amount of bandwidth overhead. In addition to the enhanced performance of IPv6 headers compared to IPv4 headers, other extension headers exist to promote encrypted communication between endpoints.

In the study, the Authentication Header was used to carry the cryptographic signature of the BGP update message. As seen in Chapter 4, the overhead imparted by the header itself was only 12 bytes. When compared to other means of exchanging keys with additional packets, the cost comparison favorably aligns with the use of extension headers. Other internal routing protocols are already using Authentication Headers to provide integrity, authentication, and confidentially of routing exchanges such as OSPFv3 (Coltun, Ferguson, Moy, & Lindem, 2008). These types of extension headers are proven effective in internal routing and they should be tapped into for securing external routing protocols such as BGP in a similar fashion.

Overall, efficiencies and security gained from using extension headers further necessitates the need for more entities to adopt IPv6 in place of IPv4. The movement of autonomous systems to the IPv6 space will enhance the adoptability of such models. As IPv6 matures, the headers and processing times are likely to follow, and use will be widened across autonomous systems.

Reducing Performance Costs in the Attestation Model

Performance costs were introduced by the attestation model; a common observation when implementing security enhancements in applications. Cryptographic operations impart overhead on an environment, and their costs need to be evaluated accordingly. In the proposed attestation model, costs in terms of bandwidth consumed per route update under 677 extra bytes and only two additional packets were transmitted. Similarly, route convergence times also increased from the unattested model, but still measured in a just over one-hundredth of a second to process. Likewise, RAM and CPU consumption showed 23.81KB and of 3.62% increases respectively.

These costs were all depicted as deltas from a model where no BGP route attestation was in place. While the costs were in cases substantially higher in percentage increases, their real numeric increases describe the impact more truthfully. True costs should be evaluated by potential adopters of any security model including the one proposed in this research when determining the adoptability and impact on an environment.

Reducing costs in the proposed attestation model of this study can be done in many areas. The two most impactful areas to reduce overhead would be the retrieval of a sender's public key as well as the cryptographic processing of the signed message. Using DNS to store a sender's public key has been done in other accepted models such as

domain keys for email integrity (Crocker et al., 2011). While it does help verify an owner of a domain or a net block in this case, several limitations exist that make DNS a less attractive option when considering the future.

The biggest drawback to using DNS as a host for the public key is the limitation of key size to 255 bytes (Cheshire & Krochmal, 2013). As the ability for systems to solve cryptographic problems increases, the response has been to use longer key pairs or algorithms that are more complex. When limited to 255 bytes held within a single TXT record, the potential length of key pairs is severely limited. Therefore, the longevity of such solutions is minimal and alternatives to key storage should be explored.

Additionally, the transactions for DNS proved costly to transmit the 216 bytes representing the sender's public key. When considering the DNS transaction to retrieve the sender's public key, approximately 48% of the transaction did not carry data directly related to attestation. The additional data was comprised of packet headers and fields specifically related to the DNS protocol. Therefore, DNS is an effective, but costly method of querying and retrieving public keys. Furthermore, when considering the limitations of the key size, the opportunity to evaluate different key delivery mechanisms is apparent.

Outside of the DNS realm, a large contributor to the increase in route convergence times was attributed to the cryptographic routines. These routines were responsible for parsing the IPv6 packet to retrieve the message signature, and resigning the message with the sender's public key. If the transmitted signature matched the newly calculated signature, the message was deemed valid. Certain challenges existed with this model as the cryptographic implementations were done entirely in software. Routers should be using hardware-based cryptographic processors or application specific integrated circuits

(ASICs) to lessen the resulting overhead. Keshavamurthy, Upadhyaya, and Gopal (2011) exemplify how such hardware accelerators can be used to improve cryptographic calculation times. This study and other similar attestation models would benefit from such enhancements.

Motivation to Adopt Secure Routing Models

Autonomous system operators are strongly encouraged to investigate and weigh the cost of adopting a secure routing model against the risk of potential routing attacks. There is no governing body on the Internet enforcing networks move to secure routing, adopt IPv6, or make changes to advance the state of the Internet. Therefore, the realization of the need to adopt secure routing falls on researchers and network administrators alike.

In certain scenarios, the benefit of adopting a secure routing model is obvious. For example, when YouTube was affected by a sub-prefix hijacking attack in 2008, the adverse effects lasted for approximately two hours twenty minutes. (Bornhauser & Martini, 2011). Consider the average increase in time for route convergence by this model of 0.018119 seconds per update. For the cost of the model to outweigh the time YouTube was affected by the adverse BGP route, YouTube would have needed to see approximately 463,602 BGP updates. That is not an unforeseeable amount of BGP updates for a large organization, but this would be the number for a single routing incident. Additionally, the initial problem may have been avoided altogether by the use of such a model.

When these types of measurements and metrics are evaluated, additional performance costs are better put into perspective. The potential positive impact of such models can outweigh the cost associated with running environments in insecure routing

models. All routing protocols, not just BGP, should be continually evaluated and built upon to offer enhanced security to protect the integrity and authorization of routes, but equally as important, adoptability needs to be considered.

Need for Future Research

In addition to the statistically significant outcomes, this study shows a clear necessity for further research. Literature illustrates that BGP speaking networks are continually affected by sub-prefix hijacking attacks from malicious and unintentional actors (Ballani et al., 2007; Biersack et al., 2012; Bornhauser & Martini, 2011; Wählisch et al., 2012). Costs associated with the adverse effects of sub-prefix hijacking can substantial in terms of downtime, disruption to service, and economic side effects. As IPv4 address depletion continues and IPv6 address adoption grows, further research should to be done in securing protocols the Internet depends on. To further the research, this study be explored further to reduce performance costs and address adoptability issues. Similar models have been developed and studied; different combinations of ideas or the introduction of new suggestions will progress the field in a positive direction.

Recommendation for Future Research

The problem identified throughout the literature review upheld the idea that BGP, the Internet's routing protocol, is impacted by many shortcomings in security. One of those shortcomings allows an attacker to hijack traffic intended for a destination by advertising a more specific or longer prefix. This type of attack is known as sub-prefix hijacking. An examination of the literature revealed that proposed solutions to the shortcomings in BGP resulted in high costs in terms of overhead, and left the IPv6 protocol unevaluated. This study analyzed one method of leveraging the performance benefits and extendibility of IPv6 headers to protect BGP against sub-prefix hijacking

attacks. Although this study provided insight into the cost of the model in terms of CPU performance, RAM utilization, bandwidth consumption, and route convergence times, other areas of interest remain for future study. This section is intended to provide recommendations and insight into related areas of interest for future research.

The two largest sources of overhead in this study resulted from the retrieval of the public key via DNS and the cryptographic signature validation. Minimizing those impacts could further benefit the model by reducing overhead and increasing the adoptability. Similar challenges existed in the Domain Keys Identified Mail (DKIM) solution that this model was in part based upon (Keshavamurthy et al., 2011). Hardware accelerators are being developed for performing cryptographic functions including digital signing, hashing, and authentication (Mathew et al., 2015). Keshavamurthy et al. (2011) demonstrated a significant increase in performance in RSA-sign and verify operations when using hardware acceleration such as the IBM Power7+ processor (Blaner et al., 2013) or Intel's Xeon v3 processors. Their results showed a 49.84% increase in speed of performing DKIM operations by simply moving the cryptographic functions to a hardware accelerator. As this study used RSA-sign and verify operations in a very similar structure and programmatic environment, similar performance increases may also be observed by using hardware accelerators.

DNS costs associated with retrieving the sender's public key also contributed to a major increase in performance overhead for both bandwidth consumption and convergence times alike. Without restricting the fundamental ways DNS is implemented in IPv6, future investigation should consider ways to reduced overhead. Callahan, Allman, and Rabinovich (2013) specified that performance-driven tactics such as caching or pre-fetching DNS queries as well as load balancing between DNS servers might

minimize the perceived impact of performing lookups. In this model, similar tactics such as DNS pre-fetching during idle time on the router may be able to shift some of the delay to less crucial times in the BGP routing process. Pre-fetching and caching operations impart overhead as well in terms of RAM and CPU utilization (Callahan et al., 2013), and analysis would need to be done in order to determine if that strategy is worth the cost.

Additionally, software optimizations may be introduced into the OpenBGPD routing system as well as the proposed attestation model. While the researcher intended to implement the model minding the limiting behaviors of the code changes, there may still be opportunities for further optimization. Programmers should analyze new algorithms or models after they are implemented (Malik, 2014). Asymptotic notation or Big-O notation could be used to describe the operation of OpenBGPD and the attestation model. Once the algorithms are analyzed to determine their limiting behaviors can be augmented to reduce overall runtime with more efficient algorithms.

Furthermore, parallel processing of the attestation model and the OpenBGPD route decision engine may improve overall performance. Both the attestation model and the route decision engine filter and disseminate routes in a linear fashion. Retrieving the sender's key and validating the message signature could be done alongside of the standard route evaluation in a parallel implementation. This likely would not reduce CPU and RAM utilization as the attestation methods still have a cost, but the results may be improved from an overall convergence timing aspect. Certain barriers do exist in parallel programming that make some instantiations perform worse than their nonparallel counterparts perform. On small distributions of a problem set synchronization of code between processes may cost more than the time saved through the parallel operations

(Bauer, 2014). Again, further research should be done on using parallel programming in routing environments as certain barriers

Summary

Problems identified by this research study resolved that BGP is susceptible to harmful attacks such as sub-prefix hijacking, and proposed solutions carried a high cost without recognizing potential impacts in an IPv6 environment. This study evaluated the degree of impact using IPv6 extension headers would have on an environment when used to perform BGP route attestation. Together, these principles were combined to create a research question and hypothesis that directed the research in establishing an outcome.

The research showed that IPv6 extension headers are capable of carrying cryptographic route attestation information. Statistically significant figures showed that the model did impart overhead on a router running BGP in the following areas: CPU performance, RAM utilization, bandwidth consumption, and route convergence times. Extension headers reduced the performance overhead by the use of efficient header processing and minimizing extra packets needing to be sent to perform attestation. While the study was performed on the open source pfSense platform and OpenBGPD, they were assumed to be in correct operation by the protocol specification. Overall, the model shows an opportunity to expand upon the research performed in this study on other factors that may lessen the observed performance impacts while still providing route attestation.

This study adds to the overall body of knowledge pertaining to public routing protocol security in the IPv6 space. In addition, the research performed in the study show the applicability of leveraging IPv6 enhancements over IPv4 in an effort to improve security. These enhancements also encourage the community to be mindful of the need

to migrate to IPv6 and to consider the security implementations of doing so. Lastly, the study supplies new literature and perspective to BGP security solutions and prospective pathways to better secure the public Internet routing infrastructure.

REFERENCES

Al-Hamami, A. H. (2014). *Handbook of Research on Threat Detection and Countermeasures in Network Security*: IGI Global.

Alvestrand, H. T. (2004). *A Mission Statement for the IETF* (No. RFC 3935).

Bacon, D. F., Cheng, P., & Shukla, S. (2013). And then there were none: a stall-free real-time garbage collector for reconfigurable hardware. *Commun. ACM, 56*(12), 101-109. doi:10.1145/2534706.2534726

Bakker, N., Jasinska, E., Raszuk, R., & Hilliard, N. (2013). *Internet Exchange BGP Route Server Operations* (No. RFC 7948).

Balasubramanian, S., Raman, H. P., & Selvakumar, S. (2013). SHS-HTTPS enforcer: enforcing HTTPS and preventing MITM attacks. *SIGSOFT Softw. Eng. Notes, 38*(6), 1-4. doi:10.1145/2532780.2532802

Ballani, H., Francis, P., & Zhang, X. (2007). A study of prefix hijacking and interception in the internet. *SIGCOMM Comput. Commun. Rev., 37*(4), 265-276. doi:10.1145/1282427.1282411

Bauer, B. E. (2014). *Practical parallel programming*: Academic Press.

Biersack, E., Jacquemart, Q., Fischer, F., Fuchs, J., Thonnard, O., Theodoridis, G., . . . Vervier, P. (2012). Visual analytics for BGP monitoring and prefix hijacking identification. *Network, IEEE, 26*(6), 33-39. doi:10.1109/MNET.2012.6375891

Blaner, B., Abali, B., Bass, B. M., Chari, S., Kalla, R., Kunkel, S., . . . Sandon, P. A. (2013). IBM POWER7+ processor on-chip accelerators for cryptography and active memory expansion. *IBM Journal of Research and Development, 57*(6), 3:1-3:16. doi:10.1147/JRD.2013.2280090

Bornhauser, U., & Martini, P. (2011, 4-7 Oct. 2011). *About prefix hijacking in the Internet.* Paper presented at the 2011 IEEE 36th Conference on Local Computer Networks (LCN).

Bruhadeshwar, B., Kulkarni, S. S., & Liu, A. X. (2011). Symmetric Key Approaches to Securing BGP - A Little Bit Trust Is Enough. *Parallel and Distributed Systems, IEEE Transactions on, 22*(9), 1536-1549. doi:10.1109/TPDS.2011.19

Bryant, M. T. (2004). *The portable dissertation advisor*. Thousand Oaks, Calif. :: Corwin Press.

Bullock, J. A., Haddow, G. D., & Coppola, D. P. (2015). *Introduction to homeland security : principles of all-hazards risk management* Retrieved from https://nls.ldls.org.uk/welcome.html?ark:/81055/vdc_100026049873.0x000001

Butler, K., Farley, T. R., McDaniel, P., & Rexford, J. (2010). A Survey of BGP Security Issues and Solutions. *Proceedings of the IEEE, 98*(1), 100-122. doi:10.1109/JPROC.2009.2034031

Callahan, T., Allman, M., & Rabinovich, M. (2013). On modern DNS behavior and properties. *SIGCOMM Comput. Commun. Rev., 43*(3), 7-15. doi:10.1145/2500098.2500100

Cardona, J. C., Vissicchio, S., Lucente, P., & Francois, P. (2016). "I Can't Get No Satisfaction": Helping Autonomous Systems Identify Their Unsatisfied Interdomain Interests. *IEEE Transactions on Network and Service Management, 13*(1), 43-57. doi:10.1109/TNSM.2016.2525003

Carmines, E. G., & Zeller, R. A. (1979). *Reliability and Validity Assessment*. Beverly Hills, Calif: SAGE Publications, Inc.

Carpenter, B., & Jiang, S. (2013). *Transmission and Processing of IPv6 Extension Headers* (No. RFC 7045).

Chen, Y., & Zhu, A. (2014, 26-28 April 2014). *The design and implementation of firewall based on FreeBSD.* Paper presented at the 2014 International Conference on Information Science, Electronics, and Electrical Engineering (ISEEE).

Cheshire, S., & Krochmal, M. (2013). *DNS-Based Service Discovery* (No. RFC 6763).

Coltun, R., Ferguson, D., Moy, J., & Lindem, A. (2008). *OSPF for IPv6* (No. RFC 5340).

Creswell, J. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches*: SAGE Publications, Incorporated.

Crocker, D., Hansen, T., & Kucherawy, M. (2011). *DomainKeys Identified Mail (DKIM) Signatures* (No. RFC 6376).

Dan, P., Xiaoliang, Z., Lan, W., Massey, D., Mankin, A., Su, S. F., & Lixia, Z. (2002, 2002). *Improving BGP convergence through consistency assertions.* Paper presented at the INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE.

Deering, S. E. (1998). *Internet Protocol, Version 6 (IPv6) Specification* (No. RFC 2460).

Delany, M. (2006). Method and system for authenticating a message sender using domain keys: Google Patents.

Delany, M. (2007). *Domain-based email authentication using public keys advertised in the DNS (DomainKeys)* (No. RFC 4879).

Desai, A., Oza, R., Sharma, P., & Patel, B. (2013). Hypervisor: A survey on concepts and taxonomy. *International Journal of Innovative Technology and Exploring Engineering, 2*(3), 222-225.

Eidnes, H., de Groot, G., & Vixie, P. (1998). *Classless IN-ADDR.ARPA delegation* (No. RFC 2317).

FCC. (2012). FCC Advisory Committee Adopts Recommendations to Minimize Three Major Cyber Threats, Including an Anti-Bot Code of Conduct, IP Route Hijacking Industry Framework and Secure DNS Best Practices. *Targeted News Service*, n/a.

Fitzgerald, B. (2011). *Adopting Open Source Software : A Practical Guide*. Cambridge, Mass: The MIT Press.

Fortier, P. J., & Michel, H. E. (2003). *Computer Systems Performance Evaluation and Prediction*. Burlington, MA: Digital Press.

Fuller, V., Li, T., Yu, J., & Varadhan, K. (1993). *Classless inter-domain routing (CIDR): an address assignment and aggregation strategy* (No. RFC 1338).

Ganegedara, T., Jiang, W., & Prasanna, V. K. (2014). A Scalable and Modular Architecture for High-Performance Packet Classification. *IEEE Transactions on Parallel and Distributed Systems, 25*(5), 1135-1144. doi:10.1109/TPDS.2013.261

Gao, L. (2001). On Inferring Autonomous System Relationships in the Internet. *IEEE ACM TRANSACTIONS ON NETWORKING, 9*(Part 6), 733-745.

Gersch, J., & Massey, D. (2013, July 30 2013-Aug. 2 2013). *ROVER: Route Origin Verification Using DNS.* Paper presented at the 22nd International Conference on Computer Communications and Networks (ICCCN).

Gill, P., Schapira, M., & Goldberg, S. (2011). Let the market drive deployment: a strategy for transitioning to BGP security. *SIGCOMM Comput. Commun. Rev., 41*(4), 14-25. doi:10.1145/2043164.2018439

Gill, P., Schapira, M., & Goldberg, S. (2013). A survey of interdomain routing policies. *SIGCOMM Comput. Commun. Rev., 44*(1), 28-34. doi:10.1145/2567561.2567566

Gill, V., Heasley, J., Meyer, D., Savola, P., & Pignataro, C. (2004). *The Generalized TTL Security Mechanism (GTSM)* (No. RFC 3682).

Goldberg, S. (2014). Why is it taking so long to secure internet routing? *Commun. ACM, 57*(10), 56-63. doi:10.1145/2659899

Grigorik, I. (2013). *High Performance Browser Networking: What every web developer should know about networking and web performance*: " O'Reilly Media, Inc.".

Gutierrez, C. M., Gallagher, P., & Director, C. F. (2008). Secure hash standard.

Hansen, T., & Hallam-Baker, P. (2009). *DomainKeys Identified Mail (DKIM) Service Overview* (No. RFC 5585).

Harkins, D., & Carrel, D. (1998). *The Internet Key Exchange (IKE)* (No. RFC 2409).

Hawkinson, J., & Bates, T. (1996). *Guidelines for creation, selection, and registration of an Autonomous System (AS)* (No. RFC 1930).

Heard, N., & Adams, N. M. (2014). *Data Analysis for Network Cyber-security*. London, UK: Imperial College Press.

Heffernan, A. (1998). *Protection of BGP sessions via the TCP MD5 signature option* (No. RFC 2385).

Herzberg, A., & Shulman, H. (2013, 14-16 Oct. 2013). *DNSSEC: Security and availability challenges.* Paper presented at the IEEE Conference on Communications and Network Security (CNS), 2013.

Horley, E. (2014). *Practical IPv6 for Windows Administrators*: Apress.

Howard, L. (2015). *Reverse DNS in IPv6 for Internet Service Providers* (No. RFC draft-howard-isp-ip6rdns-05).

Hu, Y.-C., Perrig, A., & Sirbu, M. (2004). *SPV: Secure path vector routing for securing BGP.* Paper presented at the ACM SIGCOMM Computer Communication Review.

Huston, G., & Bush, R. (2011). Securing bgp with bgpsec. *FR o MTHEED i T o R The process of adding security to various components of Internet architecture reminds me a little bit of the extensive seismic retrofit-ting that has been going on in California for decades. The process is slow, expensive, and occasionally intensified by a strong earthquake*, 2.

Huston, G., & Michaelson, G. (2012). Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs).

Huston, G., Rossi, M., & Armitage, G. (2011). Securing BGP - A Literature Survey. *IEEE Communications Surveys & Tutorials, 13*(2), 199-222. doi:10.1109/SURV.2011.041010.00041

Iqbal, A., Pattinson, C., & Kor, A. L. (2015, 14-16 Dec. 2015). *Performance monitoring of Virtual Machines (VMs) of type I and II hypervisors with SNMPv3.* Paper presented at the 2015 World Congress on Sustainable Technologies (WCST).

Israr, J. (2012). *Design of Lightweight Alternatives to Secure Border Gateway Protocol and Mitigate against Control and Data Plane Attacks.* (NR98011 Ph.D.), University of Ottawa (Canada), Ann Arbor. Retrieved from http://www.ezproxy.dsu.edu:2048/login?url=http://search.proquest.com/docview/1356683089?accountid=27073 ProQuest Dissertations & Theses Global database.

Israr, J., Guennoun, M., Mouftah, H. T., & Rahman, M. (2010, 6-10 Dec. 2010). *Credible-BGP: A Hybrid Cryptosystem to Secure BGP.* Paper presented at the Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE.

Jakub, C., Mark, A., Jing, Z., Scott, I.-J., Eric, O., & Michael, B. (2014). Measuring IPv6 adoption *Proceedings of the 2014 ACM conference on SIGCOMM %@ 978-1-4503-2836-4* (pp. 87-98). Chicago, Illinois, USA: ACM.

Jakub, C., Mark, A., Jing, Z., Scott, I.-J., Eric, O., & Michael, B. (2015). Measuring IPv6 adoption: improving the transparency of the RPKI. *ACM SIGCOMM Computer Communication Review, 44*(4), 87-98.

Jethanandani, M., Patel, K., & Zheng, L. (2013). *Analysis of BGP, LDP, PCEP, and MSDP Issues According to the Keying and Authentication for Routing Protocols (KARP) Design Guide* (No. RFC 6952).

Kahate, A. (2013). *Cryptography and Network Security*: McGraw Hill Education.

Karlin, J., Forrest, S., & Rexford, J. (2009). *Nation-State Routing: Censorship, Wiretapping, and BGP*. Retrieved from ArchiveGrid database.

Kent, S. (2005). *IP Authentication Header* (No. RFC 4302).

Kent, S., Lynn, C., & Seo, K. (2000). Secure border gateway protocol (S-BGP). *IEEE Journal on Selected Areas in Communications, 18*(4), 582-592.

Keppel, G., & Wickens, T. D. (2004). *Design and analysis : a researcher's handbook*. Upper Saddle River, N.J. :: Pearson Prentice Hall.

Keshavamurthy, V., Upadhyaya, S., & Gopal, V. (2011, 4-7 Oct. 2011). *Accelerated Processing of Secure Email by Exploiting Built-in Security Features on the Intel EP80579 Integrated Processor with Intel QuickAssist Technology.* Paper

presented at the 2011 IEEE 30th Symposium on Reliable Distributed Systems Workshops.

Kuhn, R., Liu, S., & Rossman, H. (2009). Practical Interdomain Routing Security. *IT Professional, 11*(6), 54-56. doi:10.1109/MITP.2009.131

Kumar, R. (2005). *Research methodology : a step-by-step guide for beginners* (2nd ed. ed.). London :: SAGE.

Kumar, R. (2014). *Research methodology : a step-by-step guide for beginners* (Fourth edition. ed.). Los Angeles :: SAGE.

Lammle, T. (2013). *CCNA ICND2 study guide* Retrieved from EBSCOhost http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=642377

Lee, J. C., Leung, V. C. M., Wong, K. H., Cao, J., & Chan, H. C. B. (2007). Key management issues in wireless sensor networks: current proposals and future developments. *IEEE Wireless Communications, 14*(5), 76-84. doi:10.1109/MWC.2007.4396946

Liu, H. H. (2009). *Software Performance and Scalability : A Quantitative Approach*. Hoboken, N.J.: Wiley-Blackwell.

López, J., & Zhou, J. (2008). *Wireless sensor network security* Cryptology and information security series ; v. 1; Cryptology and information security series ; v. 1., Retrieved from EBSCOhost http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=244448

Lougheed, K., & Rekhter, Y. (1989). *A Border Gateway Protocol (BGP)* (No. RFC 1105).

Lougheed, K., & Rekhter, Y. (1991). *A Border Gateway Protocol 3 (BGP-3)* (No. RFC 1163).

Lougheed, K., & Rekhter, Y. (1991). *A Border Gateway Protocol 3 (BGP-3)* (No. RFC 1267).

Lucas, M. (2008). *Absolute FreeBSD : The Complete Guide to FreeBSD* (Vol. 2nd ed). San Francisco: No Starch Press.

Lychev, R., Goldberg, S., & Schapira, M. (2013). BGP security in partial deployment: Is the juice worth the squeeze? *Computer Communication Review, 43*(4), 171-182.

Mahajan, R., Wetherall, D., & Anderson, T. (2002). Understanding BGP misconfiguration. *SIGCOMM Comput. Commun. Rev., 32*(4), 3-16. doi:10.1145/964725.633027

Malhotra, A., & Goldberg, S. (2014). RPKI vs ROVER: comparing the risks of BGP security solutions. *SIGCOMM Comput. Commun. Rev., 44*(4), 113-114. doi:10.1145/2740070.2631435

Malik, D. S. (2014). *C++ Programming: Program Design Including Data Structures*: Cengage Learning.

Mathew, S., Satpathy, S., Suresh, V., Anders, M., Kaul, H., Agarwal, A., . . . Krishnamurthy, R. (2015). 340 mV–1.1 V, 289 Gbps/W, 2090-Gate NanoAES Hardware Accelerator With Area-Optimized Encrypt/Decrypt GF(2 4) 2 Polynomials in 22 nm Tri-Gate CMOS. *IEEE Journal of Solid-State Circuits, 50*(4), 1048-1058. doi:10.1109/JSSC.2014.2384039

Mcarthur, C., & Guirguis, M. (2009, Nov. 30 2009-Dec. 4 2009). *Stealthy IP Prefix Hijacking: Don't Bite Off More Than You Can Chew.* Paper presented at the Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE.

Medhi, D., & Ramasamy, K. (2007). *Network Routing : Algorithms, Protocols, and Architectures*. Amsterdam: Morgan Kaufmann.

Ming, Y. (2006, 8-11 Oct. 2006). *Security Enhancements to Routing Protocols for Backbone Networks.* Paper presented at the Systems, Man and Cybernetics, 2006. SMC '06. IEEE International Conference on.

Murphy, S. (2006). *BGP Security Vulnerabilities Analysis* (No. RFC 4272).

Natanzon, A., Schechner, T., Kedem, O., Kedem, Z., Ahal, S., & Karamanolis, C. (2013). Methods and apparatus for providing hypervisor level data services for server virtualization: Google Patents.

Ola, N., & Constantinos, D. (2004). Beware of BGP attacks. *SIGCOMM Comput. Commun. Rev. %@ 0146-4833, 34*(2), 1-8. doi:10.1145/997150.997152

Patterson, D. A., & Hennessy, J. L. (2013). *Computer Organization and Design: The Hardware/Software Interface*: Elsevier Science.

Peyravian, M., Roginsky, A., & Zunic, N. (2004). Non-PKI methods for public key distribution. *Computers & Security, 23*(2), 97-103. doi:10.1016/j.cose.2004.01.011

Phillipa, G., Michael, S., & Sharon, G. (2013). A survey of interdomain routing policies. *SIGCOMM Comput. Commun. Rev. %@ 0146-4833, 44*(1), 28-34. doi:10.1145/2567561.2567566

Punithavathani, D. S., & Radley, S. (2014). Performance Analysis for Wireless Networks: An Analytical Approach by Multifarious Sym Teredo. *The Scientific World Journal, 2014*, 8. doi:10.1155/2014/304914

Qi, L., Mingwei, X., Jianping, W., Xinwen, Z., Lee, P. P. C., & Ke, X. (2012). Enhancing the Trust of Internet Routing With Lightweight Route Attestation. *Information*

Forensics and Security, IEEE Transactions on, 7(2), 691-703. doi:10.1109/TIFS.2011.2177822

Qi, L., Xinwen, Z., Xin, Z., & Purui, S. (2015). Invalidating Idealized BGP Security Proposals and Countermeasures. *Dependable and Secure Computing, IEEE Transactions on, 12*(3), 298-311. doi:10.1109/TDSC.2014.2345381

Qiu, J., Gao, L., Ranjan, S., & Nucci, A. (2007, 17-21 Sept. 2007). *Detecting bogus BGP route information: Going beyond prefix hijacking.* Paper presented at the Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on.

Rekhter, Y., & Li, T. (1995). *A Border Gateway Protocol 4 (BGP-4)* (No. RFC 1771).

Rekhter, Y., Li, T., & Hares, S. (2006). *A Border Gateway Protocol 4 (BGP-4)* (No. RFC 4271).

Rescorla, E. (1999). *Diffie-Hellman Key Agreement Method* (No. RFC 2631).

Ribeiro, A., & Pereira, H. (2009). *L7 Classification and Policing in the pfSense Platform.* Paper presented at the 21st International Teletraffic Congress (ITC 21), Paris, France.

Rivest, R. (1992). *The MD5 message-digest algorithm* (No. RFC 1321).

Ross, S. M. (2004). *Introduction to Probability and Statistics for Engineers and Scientists* (Vol. 3rd ed). Amsterdam: Academic Press.

Rugg, G. (2007). *Using Statistics : A Gentle Introduction*. Maidenhead, England: McGraw-Hill Education.

Salkind, N. J. (2010). *Encyclopedia of Research Design*. Thousand Oaks, Calif: SAGE Publications, Inc.

Savola, P. (2005). *Reclassification of RFC 1863 to Historic* (No. RFC 4223).

Schuchard, M., Mohaisen, A., Kune, D. F., Hopper, N., Kim, Y., & Vasserman, E. Y. (2010). *Losing control of the internet: using the data plane to attack the control plane*. Paper presented at the Proceedings of the 17th ACM conference on Computer and communications security, Chicago, Illinois, USA. http://dl.acm.org/citation.cfm?doid=1866307.1866411

Sebastian, Z., Lachlan, L. H. A., & Grenville, A. (2014). Capturing ghosts: predicting the used IPv4 space by inferring unobserved addresses *Proceedings of the 2014 Conference on Internet Measurement Conference %@ 978-1-4503-3213-2* (pp. 319-332). Vancouver, BC, Canada: ACM.

Seo, K.-T., Hwang, H.-S., Moon, I.-Y., Kwon, O.-Y., & Kim, B.-J. (2014). Performance comparison analysis of linux container and virtual machine for building cloud. *Advanced Science and Technology Letters*, *66*, 105-111.

Shue, C. A., Gupta, M., & Myers, S. A. (2007). *Ipsec: Performance analysis and enhancements.* Paper presented at the IEEE International Conference on Communications, 2007. ICC'07. .

Sun, Y., Edmundson, A., Vanbever, L., Li, O., Rexford, J., Chiang, M., & Mittal, P. (2015). *RAPTOR: routing attacks on privacy in tor*. Paper presented at the 24th USENIX Security Symposium (USENIX Security 15).

Tanaka, B. K. (2005). Monitoring virtual memory with vmstat. *Linux Journal*, *2005*(140), 5.

Terrell, S. R. (2012). *Statistics Translated : A Step-by-Step Guide to Analyzing and Interpreting Data* (Vol. 1st ed). New York: The Guilford Press.

Thomson, S., Huitema, C., Ksinant, V., & Souissi, M. (1995). *DNS Extensions to Support IP Version 6* (No. RFC 3596).

Traina, P. (1995). *BGP-4 Protocol Analysis* (No. RFC 174).

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS quarterly, 37*(1), 21-54.

Vissicchio, S., Vanbever, L., Pelsser, C., Cittadini, L., Francois, P., & Bonaventure, O. (2013). Improving Network Agility With Seamless BGP Reconfigurations. *IEEE/ACM Transactions on Networking, 21*(3), 990-1002. doi:10.1109/TNET.2012.2217506

Vohra, Q., & Chen, E. (2012). *BGP Support for Four-Octet Autonomous System (AS) Number Space* (No. RFC 6793).

Wählisch, M., Maennel, O., & Schmidt, T. C. (2012). Towards detecting BGP route hijacking using the RPKI. *ACM SIGCOMM Computer Communication Review, 42*(4), 103-104.

Weaver, V. M., Terpstra, D., McCraw, H., Johnson, M., Kasichayanula, K., Ralph, J., . . . Moore, S. (2013, 21-23 April 2013). *PAPI 5: Measuring power, energy, and the cloud.* Paper presented at the 2013 IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS).

Weikuan, Y., Yandong, W., & Xinyu, Q. (2014). Design and Evaluation of Network-Levitated Merge for Hadoop Acceleration. *IEEE Transactions on Parallel and Distributed Systems, 25*(3).

White, R. (2003). Securing BGP through secure origin BGP (soBGP). *Business Communications Review, 33*(5), 47-53.

Xiao, Z., Song, W., & Chen, Q. (2013). Dynamic Resource Allocation Using Virtual Machines for Cloud Computing Environment. *IEEE Transactions on Parallel and Distributed Systems, 24*(6), 1107-1117. doi:10.1109/TPDS.2012.283

Yi, W., Shaozhi, Y., & Xing, L. (2005, 27-30 June 2005). *Understanding current IPv6 performance: a measurement study.* Paper presented at the 10th IEEE Symposium on Computers and Communications, 2005. ISCC 2005. Proceedings. .

Ying, Z., Zheng, Z., Mao, Z. M., & Hu, Y. C. (2009, June 29 2009-July 2 2009). *HC-BGP: A light-weight and flexible scheme for securing prefix ownership.* Paper presented at the IEEE/IFIP International Conference on Dependable Systems & Networks, 2009. DSN '09.

Yu, L., & Lan, Z. (2016). A Scalable, Non-Parametric Method for Detecting Performance Anomaly in Large Scale Computing. *IEEE Transactions on Parallel and Distributed Systems, 27*(7), 1902-1914. doi:10.1109/TPDS.2015.2475741

Yun, J.-K., & Song, J.-H. (2015). Enhancing Secure AS Path BGP (SAPBGP) for Efficient Comparison.

Zhao, M., Smith, S. W., & Nicol, D. M. (2005). Evaluating the performance impact of PKI on BGP security. *Multiple Paths to Trust*, 144.

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

Zhao, X. (2002). *Towards a fault -tolerant border gateway protocol.* (3076453 Ph.D.), North Carolina State University, Ann Arbor. Retrieved from http://www.ezproxy.dsu.edu:2048/login?url=http://search.proquest.com/docview/305573792?accountid=27073 ProQuest Dissertations & Theses Global database.

Zheng, C., Ji, L., Pei, D., Wang, J., & Francis, P. (2007). *A light-weight distributed scheme for detecting IP prefix hijacks in real-time.* Paper presented at the ACM SIGCOMM Computer Communication Review.

APPENDIXES

APPENDIX A: OPENBGPD ROUTER CONFIGURATIONS

This appendix contains the OpenBGPD device configuration files (bgpd.conf) that were used on each of the participating routers in the study.

Router 1 (AS100)

```
AS 1000
fib-update yes
holdtime 90
router-id 192.168.1.1
log updates
network 2001:12:12:12::/64
neighbor 2001:12:12:12::2 {
     descr "ASN2000"
     announce all
     remote-as 2000
     local-address 2001:12:12:12::1
}
deny from any
deny to any
allow from 2001:12:12:12::2
allow to 2001:12:12:12::2
```

Router 2 (AS2000)

```
AS 2000
fib-update yes
holdtime 90
router-id 192.168.1.1
log updates
network 2001:23:23:23::/64
network 2001:12:12:12::/64
network 2001:20:20:20::/64
neighbor 2001:23:23:23::2 {
     descr "ASN3000"
     announce all
     remote-as 3000
     local-address 2001:23:23:23::1
}
neighbor 2001:12:12:12::1 {
     descr "ASN1000"
     announce all
     remote-as 1000
     local-address 2001:12:12:12::2
}
deny from any
deny to any
allow from 2001:23:23:23::2
allow to 2001:23:23:23::2
allow from 2001:12:12:12::1
allow to 2001:12:12:12::1
```

Router 3 (AS3000)

```
AS 3000
fib-update yes
holdtime 90
router-id 192.168.1.1
log updates
network 2001:23:23:23::/64
network 2001:30:30::/48
neighbor 2001:23:23:23::1 {
     descr "ASN2000"
     announce all
     remote-as 2000
     local-address 2001:23:23:23::2
}
deny from any
deny to any
allow from 2001:23:23:23::1
allow to 2001:23:23:23::1
```

APPENDIX B: DNS ZONE CONFIGURATIONS

The following is an excerpt from the DNS server configuration showing a TXT record that contains a public key. The public key obtained through a DNS record query by routers performing route attestation on a received update. The TXT record was 216 bytes in size.

```
;
;  Zone records
;

*                           TXT    (
"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCttCmLEmA3hH/wsk/u29
xPpRj+LlNFsEwg2P1IvNtVDcQaOhlPlqmUzXrztawANPXHlMjIR+Uzzsbzh
49Y4GZWw3dUMvE0KD76jz4RXQmtbh+nMNKKC3vDoDfFI6gT5trHZdWqLW0q
Lg8zaZKsjZqO8FBp6Sb8iI9QqryptKdVXwIDAQAB" )
```

APPENDIX C: SUMMARIZED VMSTAT OUTPUT

For the charts below, each row with a trial number represents the average gathered over 1,001 updates. Rows with the All heading are representations of the three trials combined, being 3,003 updates.

Table C1

Summarized vmstat output collected from router receiving BGP updates with no route attestation model in place.

Trial	**RAM Consumed (KB)**	**Avg. RAM/Update (KB)**	**Process Time %**
1	1,224	1.22	0.655104063
2	1,308	1.31	0.478691774
3	1,000	1.00	0.504468719
All	3,532	1.18	0.546115702

Table C2

Summarized vmstat output collected from router receiving BGP updates with route attestation model in place.

Trial	**RAM Consumed (KB)**	**Avg. RAM/Update (KB)**	**Process Time %**
1	26,340	26.31	3.529236868
2	26,340	26.31	3.958415842
3	24,036	24.01	5.005842259
All	76,716	25.55	4.169402495

APPENDIX D: AVERAGE ROUTE UPDATE PROCESSING TIMES

Trial	**Unsigned Update Average Time (s)**	**Signed Update Average Time (s)**
1	0.000244	0.019270
2	0.000193	0.018162
3	0.000195	0.019295
All	0.000211	0.018330

APPENDIX E: UNMODIFIED BGP UPDATE PACKET

```
IPv6, Src: 2001:12:12:12::1, Dst: 2001:12:12:12::2
    Version: 6
    Traffic class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Flowlabel: 0x0009783c
    Payload length: 101
    Next header: TCP (6)
    Hop limit: 1
    Source: 2001:12:12:12::1
    Destination: 2001:12:12:12::2
Transmission Control Protocol, Src Port: 24213 (24213), Dst
    Port: 179 (179), Seq: 1, Ack: 1, Len: 69
Border Gateway Protocol - UPDATE Message
    Marker: ffffffffffffffffffffffffffffffff
    Length: 69
    Type: UPDATE Message (2)
    Withdrawn Routes Length: 0
    Total Path Attribute Length: 46
    Path attributes
        Path Attribute - ORIGIN: IGP
            Flags: 0x40
            Type Code: ORIGIN (1)
            Length: 1
            Origin: IGP (0)
        Path Attribute - AS_PATH: 1000
            Flags: 0x40
            Type Code: AS_PATH (2)
            Length: 6
            AS Path segment: 1000
        Path Attribute - MP_REACH_NLRI
            Flags: 0x80
            Type Code: MP_REACH_NLRI (14)
            Length: 30
            Address family identifier (AFI): IPv6 (2)
            SAFI: Unicast (1)
            Next hop network address (16 bytes)
            Number of Subnetwork points of attachment: 0
            NLRI (9 bytes)
                2001:30:30:fc17::/64
```

APPENDIX F: MODIFIED BGP UPDATE PACKET

```
IPv6, Src: 2001:12:12:12::1, Dst: 2001:12:12:12::2
    Version: 6
    Traffic class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Flowlabel: 0x0000007b
    Payload length: 241
    Next header: Authentication Header (51)
    Hop limit: 10
    Source: 2001:12:12:12::1
    Destination: 2001:12:12:12::2
    Authentication Header
        Next header: TCP (0x06)
        Length: 0x8c
        AH SPI: 0x00000001
        AH Sequence: 1
        AH ICV:67c68635991af7400c2f8bf1280dbc12962ffc20b...
Transmission Control Protocol, Src Port: 24213 (24213), Dst
    Port: 179 (179), Seq: 1, Ack: 1, Len: 69
Border Gateway Protocol - UPDATE Message
    Marker: ffffffffffffffffffffffffffffffff
    Length: 69
    Type: UPDATE Message (2)
    Withdrawn Routes Length: 0
    Total Path Attribute Length: 46
    Path attributes
        Path Attribute - ORIGIN: IGP
            Flags: 0x40
            Type Code: ORIGIN (1)
            Length: 1
            Origin: IGP (0)
        Path Attribute - AS_PATH: 1000
            Flags: 0x40
            Type Code: AS_PATH (2)
            Length: 6
            AS Path segment: 1000
        Path Attribute - MP_REACH_NLRI
            Flags: 0x80
            Type Code: MP_REACH_NLRI (14)
            Length: 30
            Address family identifier (AFI): IPv6 (2)
            SAFI: Unicast (1)
            Next hop network address (16 bytes)
            Number of Subnetwork points of attachment: 0
            NLRI information (9 bytes)
                2001:30:30:fc17::/64
```

APPENDIX G: REPRESENTATION OF DNS QUERY AND RESPONSE

```
DNS Query:
Source: 2001:20:20:20::1
Destination: 2001:20:20:20::2
Protocol: DNS
Length: 154
Standard query 0xf271 TXT
     7.1.c.f.0.3.0.0.0.3.0.0.1.0.0.2
Queries:
Name: 7.1.c.f.0.3.0.0.0.3.0.0.1.0.0.2: type TXT, class IN

DNS Response:
Source: 2001:20:20:20::2
Destination: 2001:20:20:20::1
Protocol: DNS
Length: 383
Standard query response 0xf271 TXT
     7.1.c.f.0.3.0.0.0.3.0.0.1.0.0.2 TXT OPT
Queries:
Name: 7.1.c.f.0.3.0.0.0.3.0.0.1.0.0.2: type TXT, class IN
Answers
     TXT:MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCttCmLEmA3hH
     /wsk/u29xPpRj+LlNFsEwg2P1IvNtVDcQaOhlPlqmUzXrztawANPXH
     lMjIR+Uzzsbzh49Y4GZWw3dUMvE0KD76jz4RXQmtbh+nMNKKC3vDoD
     fFI6gT5trHZdWqLW0qLg8zaZKsjZqO8FBp6Sb8iI9QqryptKdVXwID
     AQAB
```

APPENDIX H: PROGRAMATIC PATCHES APPLIED TO OPENBGPD

The accompanying online archive shows the programmatic changes applied to the OpenBGPD source code to gather timing statistics as well as the implementation of the attestation model. These programmatic changes are displayed in the format of a diff-patch, which examines the differences between the original OpenBGPD source code as compared to the changes necessary for compilation on pfSense and those required for this study. Patches on the online archive are used to modify the bgpd process, the parent process of OpenBGPD.

Files and Directories:

- signed_bgpd/pfsense_patches
- timed_bgpd/pfsense_patches

Location of online repository:

https://github.com/DSUmjham/Dissertation

APPENDIX I: DNS ROUND TRIP TRANSACTION TIMES

Trial	DNS Query Round Trip Time Avg. (s)
1	0.000693
2	0.000568
3	0.000806
All	0.000689