

A Survey of BGP Security Issues and Solutions

Kevin Butler, Toni Farley, Patrick McDaniel, and Jennifer Rexford

Abstract

The Border Gateway Protocol (BGP) is the *de facto* interdomain routing protocol of the Internet. Although the performance of BGP has been historically acceptable, there are mounting concerns about its ability to meet the needs of the rapidly evolving Internet. A central limitation of BGP is its failure to adequately address security. Recent outages and security analyses clearly indicate that the Internet routing infrastructure is highly vulnerable. Moreover, the design and ubiquity of BGP has frustrated past efforts at securing interdomain routing. This paper considers the vulnerabilities currently existing within interdomain routing and surveys works relating to BGP security. The limitations and advantages of proposed solutions are explored, and the systemic and operational implications of their designs considered. We centrally note that no current solution has yet found an adequate balance between comprehensive security and deployment cost. This work calls not only for the application of ideas described within this paper, but also for further introspection on the problems and solutions of BGP security.

Index Terms

authentication, authorization, BGP, border gateway protocol, integrity, interdomain routing, network security, networks, routing

I. INTRODUCTION

The Internet is a global, decentralized network comprised of many smaller interconnected networks. Networks are largely comprised of end systems, referred to as hosts, and intermediate systems, called routers. Information travels through a network on one of many paths, which are selected through a routing process. Routing protocols communicate reachability information (how to locate other hosts and routers) and ultimately perform path selection. A network under the administrative control of a single organization is called an autonomous system (AS) [1]. The process of routing within an AS is called *intradomain routing*, and routing between ASes is called *interdomain routing*. The dominant interdomain routing protocol on the Internet is the Border Gateway Protocol (BGP) [2]. BGP has been deployed since the commercialization of the Internet, and version 4 of the protocol has been in wide use for over a decade. BGP works well in practice, and its simplicity and resilience have enabled it to play a fundamental role within the global Internet [3]. However, BGP has historically provided few performance or security guarantees.

The limited guarantees provided by BGP often contribute to global instability and outages. While many routing failures have limited impact and scope, others lead to significant and widespread damage. One such failure occurred on 25 April 1997, when a misconfigured router maintained by a small service provider in Virginia injected incorrect routing information into the global Internet and claimed to have optimal connectivity to all Internet destinations.

Because such statements were not validated in any way, they were widely accepted. As a result, most Internet traffic was routed to this small ISP. The traffic overwhelmed the misconfigured and intermediate routers, and effectively crippled the Internet for almost two hours [4]. Since that time, studies such as those conducted by Wang et al. [5] have shown that if even a small number of networks are affected by routing instability, the ramifications can be global in scope.

Loss of connectivity on the Internet can be manifested as anything from an inconsequential annoyance to a devastating communications failure. For example, today's Internet is home to an increasing number of critical business applications, such as online banking and stock trading. Significant financial harm to an individual or institution can arise if communication is lost at a critical time (such as during a time-sensitive trading session). As the number of critical applications on the Internet grows, so will the reliance on it to provide reliable and secure services. Because of the increased importance of the Internet, there is much more interest in increasing the security of its underlying infrastructure, including BGP. Such assertions are not novel: the United States government cites BGP security as part of the national strategy for securing the Internet [6].

Current research on BGP focuses on exposing and resolving operational and security concerns. Operational concerns relating to BGP, such as scalability, convergence time (the time required for all routers to have a consistent view of the network), route stability, and performance, have been the subject of much effort. Similarly, much of the contemporary security research has focused on the integrity, authentication, confidentiality, authorization, and validation of BGP data. These two fields of operational issues and security research are inherently connected. Successes and failures in each domain are informative to both communities.

This paper explores current research in interdomain routing security, exposing the similarities and differences in proposed approaches to building a more secure Internet. The next section provides a brief overview of interdomain routing and BGP. Subsequent sections examine current research addressing BGP and interdomain routing security issues.

II. BORDER GATEWAY PROTOCOL

The Internet consists of tens of thousands of Autonomous Systems (ASes) that use the Border Gateway Protocol (BGP) to exchange information about how to reach blocks of destination IP addresses (called *IP prefixes*). BGP is an incremental protocol—a BGP-speaking router sends an advertisement message when a new route is available, and a withdrawal message when a route no longer exists. BGP is also a path-vector protocol, where each AS adds its AS number to the beginning of the AS path before advertising the route to the next AS. Each router selects a single best BGP route for each destination prefix and may apply complex policies for selecting a route and deciding whether to advertise the route to a neighboring router in another AS.

In this section, we present an overview of interdomain routing in the Internet and describe how most of BGP's security problem stem from (i) uncertainty about the relationship between IP prefixes and the AS numbers of the ASes who manage them, (ii) the use of the Transmission Control Protocol (TCP) as the underlying transport protocol, and (iii) the role of BGP routing policy in setting the attributes in BGP route advertisements.

A. *IP Prefixes and AS Numbers*

An IP address is a 32-bit number, typically represented in dotted-decimal notation with a separate integer for each of the four octets. Addresses are assigned to institutions in blocks of contiguous addresses, represented by the first address and a mask length. For example, the prefix 192.0.2.0/24 contains all addresses where the first three octets are 192, 0, and 2—the 256 addresses 192.0.2.0 to 192.0.2.255. Allocating addresses in blocks leads to smaller routing tables and fewer route advertisements, as most routers need only know how to direct traffic toward the block of addresses, rather than storing a separate routing information for every IP address. Since prefixes have variable length, IP prefix may be contained within another. For example, a router may have routing information for two prefixes 211.120.0.0/12 and 211.120.132.0/22, where the first prefix completely covers the second one. To decide how to forward a data packet, an IP router identifies the longest prefix that matches the destination IP address. For example, a packet with destination IP address 211.120.132.37 would match 211.120.132.0/22, since this prefix is more specific than 211.120.0.0/12.

Initially, institutions received address assignments directly from the Internet Assigned Numbers Authority (IANA), and later from the Internet Corporation for Assigned Names and Numbers (ICANN). More recently, ICANN began to delegate this responsibility to address registries responsible for different parts of the world. For example, the American Registry for Internet Numbers (ARIN) manages the IP address assignments for North America, whereas the Réseaux IP Européens (RIPE) assigns much of the address space for Europe, the Middle East, and North Africa; the Asia-Pacific Network Information Center (APNIC) assigns IP addresses in Asia and the Pacific Rim, the Latin American and Caribbean Internet Address Registry (LACNIC) distributes address space through the Latin American and Caribbean regions, and the African Internet Numbers Registry (AfriNIC) serves the African region. These regional registries can assign IP addresses directly to organizations or other registries, including national registries and Internet Service Providers that may, in turn, assign smaller portions of the address block to other institutions. For example, ICANN delegated the large address block 210.0.0.0/7 to APNIC, which in turn delegated 211.120.0.0/12 to the Japan Network Information Center (JPNIC), which in turn assigned 211.120.132.0/22 to Sony.

Autonomous Systems are assigned AS numbers (ASNs) in a similar manner, with ICANN serving as the ultimate authority for delegating numbers. AS numbers from 1 to 64511 are public and have Internet-wide scope, requiring each number to correspond to a single AS. For example, Sony has been assigned AS number 2527. In contrast, some companies have multiple ASes. For example, AS 701 corresponds to UUNET's North American backbone, whereas AS 702 corresponds to UUNET's European backbone. Public AS numbers can appear in the AS-path attribute of BGP advertisements. However, many institutions do not need a unique AS number. For example, an Autonomous System may connect to a single upstream network that bears sole responsibility for providing connectivity to the rest of the Internet. The customer AS may be assigned a private AS number in the range 64512–65535 for communicating via BGP with its provider. The provider's routers would then advertise the BGP routes on behalf of this customer, without including the private AS number in the path. This allows other service providers to assign the same private AS number to their own customers.

The AS that introduces a destination prefix into the global routing system—by advertising the prefix to neighboring ASes—is called the *originating* AS. For example, Sony could advertise a BGP route to 211.120.132.0/22 with an AS path of “2527” to its upstream provider, which would add its own AS number to the front of the AS path before sending the BGP advertisement to another neighboring AS. However, BGP does not ensure that a BGP-speaking router uses the AS number it has been allocated, or that the AS owns the prefixes it originates. A router can be configured to advertise routes into BGP with any AS number, as long as the neighboring router is configured to accept them. Similarly, a router can originate routes for any destination prefix, including very small address blocks (e.g., 211.120.132.4/30) and address blocks it does not own. The neighboring router will accept these advertisements unless configured to do otherwise, based on prior knowledge of the acceptable prefixes or prefix lengths. This makes the routing system extremely vulnerable to misconfiguration or malicious attack.

An AS can advertise a prefix belonging to another AS—an action known as *prefix hijacking*. Neighboring ASes receiving this announcement may select this route and direct traffic toward the wrong AS; these ASes may, in turn, advertise the BGP route to their own neighbors. If the offending AS simply drops all packets destined to the hijacked addresses, the effect is called a *black hole* and the destinations seem unreachable—at least to the parts of the Internet that believe the bogus BGP routes. If the AS decides to direct the traffic to hosts under its control, the effects can be much more severe. These hosts may impersonate the service provided by the legitimate, hijacked destinations. The AS can then analyze the traffic these hosts receive, possibly receiving sensitive information such as passwords and credit-card numbers.

To ensure that virtually *all* ASes direct traffic to the wrong place, the offending AS may advertise several more-specific prefixes (e.g., 211.120.132.0/24, 211.120.132.64/24, 211.120.132.128/24, and 211.120.132.192/24). Because of the “longest prefix match” rule, IP routers would always forward packets toward the offending AS rather than the real AS that advertised the larger address block 211.120.132.0/22. The canonical example of deaggregation occurred in 1997 when misconfigured routers in the Florida Internet Exchange (AS 7007) deaggregated every prefix in their routing table and started advertising the first /24 block of each of these prefixes as their own. This caused backbone networks throughout North America and Europe to crash, as AS 7007 was overwhelmed by an immense surge in traffic and the BGP routes it was advertised started flapping. This was not a malicious attack, but simply an innocent configuration mistake by the network operators. A well-planned, targeted, malicious attack on BGP could do even more serious harm.

B. Using TCP as the Transport Protocol

A pair of routers exchange BGP advertisement and withdrawal messages by establishing a BGP session that runs over an underlying Transmission Control Protocol (TCP) connection. The TCP connection provides the abstraction of a reliable communication channel that reliably delivers an ordered stream of bytes, obviating the need for BGP to provide error correction or retransmission. BGP neighbors often have a direct physical connection at the IP layer. For example, a router in one AS may have a link connecting to the router in another AS, and the BGP session runs over this link. More generally, the two routers may have to communicate through an intermediate device, such

as a firewall or another router; in this case, the TCP connection must traverse several IP-layer hops. In addition to having external BGP (eBGP) sessions with other ASes, a router may also have internal BGP (iBGP) sessions with other routers in the same AS. These internal sessions are used to disseminate the BGP routes learned from neighboring domains throughout the AS.

The communication channel between two BGP-speaking routers is vulnerable to attacks. To simplify the discussion of possible attacks, we consider two BGP-speaking routers Alice and Bob, and a malicious third-party, whom we call Charlie. Possible attacks include:

Attacks against confidentiality: Two routers communicating over a channel may be assumed to have a modicum of confidentiality; that is, they may expect that messages they send to each other would not be seen by any other party. However, Charlie could *eavesdrop* on the message stream between Alice and Bob, in an attempt to learn policy and routing information from the two parties. While this information is not necessarily sensitive, many service providers have business relationships that can be inferred from the BGP data (cite Spring). Allowing Charlie to infer these business relationships may be highly undesirable to Alice and Bob. These *passive* attacks are not unique to BGP, as they apply to any protocol that uses TCP for the underlying transport of messages without any additional security infrastructure.

Attacks against message integrity: An additional risk occurs if Charlie becomes an active, unseen part of the communication channel. Charlie can become a *man in the middle* between Alice and Bob, and tamper with the BGP messages. For example, Charlie could *insert* forged BGP messages into the message stream. These messages could introduce incorrect information into the routing system or trigger Alice or Bob to abort the session. Excessive messages could also overwhelm Alice and/or Bob, causing the routers to crash. Charlie could also selectively *delete* messages. For example, BGP speakers exchange periodic keep-alive messages to test that they can still communicate; deleting these messages would cause Alice and/or Bob to think the connection is broken, causing them to tear down the BGP session. Charlie could also *modify* the messages between Alice and Bob, leading them to have inconsistent views of the routing information. Finally, Charlie can launch a *replay* attack, where he records messages between Alice and Bob and resends them at a later time. This allows Charlie to re-assert withdrawn routes or withdraw valid ones.

Denial-of-service attack: The TCP connection between Alice and Bob may itself be the object of a denial-of-service attack, even from a remote adversary that does not have direct access to the link(s) between Alice and Bob. TCP uses a three-way hand-shake (SYN, SYN-ACK, and ACK) to establish the connection between Alice and Bob, and closes the connection with a FIN or RST packet. Charlie could send Bob an RST packet that convinces Bob to close the connection, even though both Alice and Bob want to continue communicating. Alternatively, Charlie could send a large number of SYN packets to Bob without completing the three-way handshake (i.e., without sending the ACK packet). This *SYN flooding* attack would consume Bob's connection state memory, leaving Bob unable to perform any TCP transactions. Bob's neighbors are adversely affected as well because they eventually declare their sessions with Bob to be dead, forcing them to withdraw all of the BGP routes they learned from Bob. After coming back online, Bob announces all of these BGP routes again, forcing the neighbors to switch to new

routes and advertise them to their neighbors. This *route flapping* is detrimental to all routers because it consumes processing and bandwidth resources, and also causes repeated disruptions in connectivity¹.

Want to talk about the Bellovin/Gansner point, but need to figure out where to put it...

In addition, the ability of Charlie to force a BGP session reset can allow the configuration of Alice or Bob to transition into a stable but undesired forwarding state, known as a BGP Wedgie [7].

C. Routing Policy and BGP Route Attributes

Jen to write...

III. BGP SECURITY TODAY

Jen to write.

Written by KB:

To date, the majority of defenses that have been implemented by ISPs to protect BGP have focused on solutions that can be implemented locally or requiring only limited interaction with parties outside the local administrative domain. In particular, protection of the underlying TCP connection and defensive filtering of BGP announcements are the most commonly implemented solutions, with some limited deployment of cryptographic protections between routers. However, these solutions are ultimately limited in the protections they can offer against more complex and sophisticated attacks that target BGP itself. Ultimately, centralized registries shared amongst ASes that are authoritative and accurate are necessary for protecting against this latter class of attacks. In this section, we describe the currently-implemented solutions and levels of protection they provide.

Comments by jrex:

Most work has focused on protecting the underlying TCP connection, and on defensive filtering of BGP announcements. There are limits to what you can do without an authoritative and accurate registry.

Somewhere I should say something about protecting access to the router infrastructure itself, and point to a reference on best-common practices. We don't want to fall off a cliff here and delve into a lot of detail, but we don't want to ignore this important part of the problem.

A. Protecting the BGP Session Between a Pair of Routers

Include enough crypto discussion to explain MAC and pairwise keys, and leave the discussion of PKI and certificates to the next section.

Talk about MD5 and IPSec, and allude to prior work like hop-integrity protocol and the session-level parts of the Smith/Aceves paper.

Refer to Table I

¹In practice, routers typically employ route-flap damping to penalize unstable BGP routes. If a neighbor continually advertises and withdraws a route for a prefix, the router eventually suppresses the route. This can cause parts of the Internet to lose connectivity to the destination prefix, even though the physical paths exist.

	Integrity	Confidentiality	Replay Prevention	DOS Prevention
IPsec (ESP) [8]	yes	yes	yes	yes
IPsec (AH) [9]	yes	no	yes	yes
MD5 Integrity [10]	yes	no	yes	no
HOP Protocol [11]	yes	no	yes	no
GTSM [12]	no	no	no	no
Smith .et al. [13]	yes	yes	yes	no

TABLE I

BGP PEER SESSION SECURITY SOLUTIONS - REQUIREMENTS (COLUMNS) RELATE TO THE GUARANTEES PROVIDED FOR THE AS TO AS PEERING SESSIONS.

Here's the text from "BGP Security Today" that Jen needs to integrate in this subsection

Protecting the TCP connection is an easy way to mitigate attacks on BGP sessions. A popular and inexpensive countermeasure against attacks on TCP is the use of message authentication codes (MACs). Recent enhancements to BGP suggest the use of a TCP extension that carries an MD5 digest [14] based MAC. An MD5 keyed digest [15] of the TCP header and BGP data is included in each packet passing between the BGP speakers. The authenticity of the packet data is ensured because the digest could have only be generated by someone who knows the secret key. A number of variants consider hashing all or part of the TCP and BGP data message using one or more keys [10], which addresses many of the problems of spoofing and hijacking inherent to TCP [16], [17].

Known more generally as cryptographic hash algorithms, digest algorithms compute a fixed-length hash value from an input text. The hash function is cryptographically sound if it is non-invertible (i.e., it is computationally infeasible to find a preimage of a hash value) and collision resistant (i.e., it is computationally infeasible to find two inputs with same output hash value). For MD5, the output is 128 bits in length. To illustrate infeasibility, consider an attempt to find a message that will map to a particular MD5 digest: with a 128-bit digest, one would require on average 2^{127} messages to find the particular message that mapped to the digest value, or 2^{64} messages to find a message that created a *collision*, a different message that maps to the same digest value.²

The MD5 digest mechanism requires that a *shared secret key* be configured manually at each session end-point. This approach is limited in that maintaining shared secrets between potentially thousands of routers concurrently is immensely difficult. Moreover such secrets, if not replaced frequently, are subject to exposure by cryptanalysis.

1) *IPsec*: Many recent proposals have suggested the use of IPsec as a mechanism for securing the BGP session. IPsec is not specific to BGP, but is a suite of protocols that provide security at the network layer [18], [19]. These protocols define methods for encrypting and authenticating IP headers and payload, and provide key management services for the maintenance of long term sessions. The IPsec Internet Security Association and Key Management

²Less messages are required to find a colliding digest value because of the *birthday paradox*, which shows that for n inputs and k possible outputs that can be generated, if $n > \sqrt{k}$, there is a better than 50% chance that a pair of inputs will map to the same output.

Protocol (ISAKMP) defines a framework for key management and negotiating security services [20] while the Internet Key Exchange (IKE) protocol deals with the issues of dynamic negotiation of session keys [21]. The IPsec Authentication Header protocol (AH) [9] and Encapsulating Security Payload (ESP) protocol [8] implement packet level security with differing guarantees. All of these services work in concert to establish and maintain the secret keys used guarantee the confidentiality and authenticity of data passed over IP between two end-points. Within BGP, this is typically used to secure the BGP messages passed between peers.

IPsec is often used as the security mechanism for implementing Virtual Private Networks (VPNs) [22]. If properly configured, it provides the desirable security guarantees for peer sessions, e.g., authenticity of data, integrity, message replay prevention, and data confidentiality. IPsec sessions implement security between peers only. Hence, while they address many issues relating session-local vulnerabilities, they do little to address widespread attacks.

2) *Generalized TTL Security Mechanism*: Originally called the “BGP TTL Security Hack”, the Generalized TTL Security Mechanism (GTSM) provides a method for protecting peers from remote attacks [12]. This approach builds on the premise that in the vast majority of BGP peering sessions, the two peers are adjacent to each other. (Multihop BGP sessions, where peers are more than one hop away from each other, are possible but uncommon in practice.) The time-to-live, or TTL, attribute in an IP packet is set to a value that is decremented at every hop. For example, if a packet traverses four hops from source to destination, the TTL decrements by four. Routers using GTSM set the TTL of an IP packet to its maximum value of 255. When a BGP peer receives a packet, it checks the TTL and if this value is lower than 254 (decremented by one), the packet is flagged or discarded outright. This prevents remote attacks which come from more than one hop away, as those packets will have TTLs lower than the threshold value of 254.

A common practice among network operators is to set the TTL to 1. This accomplishes the same goal as GTSM in that the packet will be discarded if the packet comes from greater than one hop away, and has the added benefit that the check is already incorporated by the IP protocol, meaning that no additional mechanisms are required.

Here’s the text on defenses against peer attacks, which Jen needs to integrate in this subsection.

Summarized in Table I, we begin by considering the features and limitation of the proposed BGP session security solutions. Recall that peer attacks include both passive activity, such as eavesdropping, and actively malicious activities, such as modifying BGP messages. Both forms of attacks are mitigated by IPsec, which introduces authenticated sequence numbering, distribution of shared keys between peers, and encryption. IPsec is assumed to be the underlying network mechanism with S-BGP, soBGP, and IRV (the latter can also use TLS). The IPsec AH mode protects against replay attacks through the use of sequence numbers, and protects message integrity by calculating a message authentication code using a hashing function such as MD5 or SHA-1. The IPsec ESP mode provides AH data integrity and authenticity in a similar manner to AH, and additionally introduces further defenses against eavesdropping, e.g., confidentiality. The hop integrity protocols proposed by Gouda et al. [11] duplicate the services of IPsec: Diffie-Hellman key negotiation, data integrity, and data authentication are provided.

MD5 authentication can also be used directly with TCP. Early versions of BGP included a similar authentication field which was largely unused. With the addition of MD5 MACing and sequence numbers, TCP can protect the

integrity of a message (i.e., it is protected against modification) and against replay attacks. It does not protect the confidentiality of the message because there is no encryption mechanism specified. In addition, this solution requires that a shared secret be manually configured in both two routers. Unlike the IPsec IKE protocol which dynamically negotiates secret keys, manual configuration of MD5 keys can place significant operational burden on network administrators.

Two of the countermeasures specified by Smith et al. [23] protect the confidentiality and integrity of BGP through the encryption and authenticated sequence numbering; however, use of these extensions require altering BGP, which is seen by many as a prohibitive barrier to adoption. There are hundreds of thousands of routers spanning thousands of organizations on the Internet. Such barriers are cited as motivation for out-of-band solutions such as IRV.

GTSM weakly defends against attackers who are more than one hop away. It does not defend against subverted peers sending malicious information or other similar insider attacks, and it is less useful in multi-hop scenarios where BGP peers are farther than one hop away from each other. The TTL threshold can be lowered to account for how many hops away the peer is, but there will consequently be no defense against attackers the same number of hops away, as those packets will pass unfiltered. Additionally, if an attacker tunnels an IP packet by encapsulating it within another IP packet to a peer one hop away from the victim, the decapsulated packet, with a TTL set to the maximum value, will be able to evade GTSM. GTSM is simple, low cost, and generally effective against unsophisticated attackers. However, the effectiveness of the solution to mitigate motivated attackers is very limited.

Protocols that preserve message integrity also effectively prevent some classes of denial of service attacks. For example, remotely resetting a TCP connection or forcibly closing a BGP session becomes considerably more difficult when sequence numbers must be guessed and, more importantly, when digests relying on shared secrets are used. Distributed denial of service attacks are certainly harmful to BGP operation, as flooding a link could cause timers to expire and information not to arrive. Some protocols, such as IPsec, provide limited forms of DOS prevention, but none adequately address flooding attacks.

The prohibitive favorite solution for BGP peer session security has become IPsec. At this point, IPsec is ubiquitous, well understood, and easy to configure. Proposed solutions, such as the Hop protocol and countermeasures by Smith et al., provide a subset of IPsec functionality using specialized protocols. IPsec was not widely available at the time most these solutions were proposed. Hence, while of historical interest, it is unclear what these protocols offer that IPsec does not already more effectively provide. Solutions such as GTSM and MD5 are currently used because they are easy to implement and low cost. Clearly, these protocols serve as short-term measures, and should not be considered by anyone as long-term solutions to peer session security. Hence, ASes will and should continue to use these inexpensive countermeasures until a strong security service can be deployed in their environment, i.e., IPsec.

B. Defensive Filtering of Suspicious BGP Announcements

Here's the text from "BGP Security Today" that Jen needs to integrate. She'll also grab text from her survey on BGP Routing Policies for more examples.

Defensive routing policies are used to filter bad and potentially malicious announcements, and to manipulate

potentially dangerous attributes of received routes. BGP speakers commonly filter ingress and egress routes based on route policies. The policies filter prefixes that are documented special use addresses (DSUA) prefixes (e.g., loopback addresses), and *bogons* (advertisements of address blocks and AS numbers with no matching allocation data), also known as *martians*. The CIDR report keeps an updated list of bogons [24] which many organizations use to filter announcements. Filtering is also used to removing conflicting announcements. For example, announcements containing private ASes [25] or from unexpected downstream ASes are automatically dropped by some BGP speakers. Additionally, ISPs often filter routes from customers if they relate to prefixes the customer does not own. On a global level, routes from small subnets (advertising smaller than a /24 block) are filtered in order to limit the size of the global routing tables. This is implemented in routers through configuration options to limit the maximum number of prefixes a peer router can send; if the number exceeds the configured maximum, the connection is restarted. This penalizes routers that artificially deaggregate the routes they advertise to their peers.

A policy of careful ingress and egress filtering greatly aids in maintaining security for both the local AS and its neighbors, and is widely held to be the most widely deployed and effective BGP security measure. Filtering, however, is not a replacement for a strong security architecture. The filtering rules are fundamentally limited by the heuristics used, and can only remove announcements which are overtly bad.

BGP attributes such as *multi-exit discriminators*, or MEDs, are another potential vehicle for an attack. For example, MEDs can be used by an adversary to control the egress point of an AS. The community string is an equally dangerous attribute. These strings are used as internal tags to indicate how the route should be treated, and can hence be abused by an adversary to influence the propagation and selection of routes. Other attributes such as “origin type” are used in the route selection process, and also may be misused. Routers frequently defend against all these attacks by clearing or validating the attribute value, e.g., clearing MEDs and community strings, or zeroing the origin type values. Alternately, measurement-based approaches, such as those explored by Feamster et al. [26], are possible. This work identified inconsistent route announcements from a peer AS by determining the existence of inconsistent attributes. These can be symptomatic of the peer attempting to force *cold-potato* routing, exploiting the victim’s network resources to minimize the peer’s costs, and violating the peering agreement.

1) Routing Registries: I may change this text to focus more on the role of registries in constructing the route filters, and how you can’t construct good route filters without accurate information, and use that to segue to the next section which will start by talking about authoritative registries and PKI.

A route registry is a centralized repository of routing policy information [27]. ASes using a registry service insert details of their policy and topological information into the repository for other ASes to query. External applications query this data to validate received routes and policy. Registries may also be used by organizations constructing route filters. For example, an ISP’s customers may register their routes in a route registry, and the ISP will use this information to construct a filter such that the only routes that are valid, and hence not filtered, are those customer routes in the registry. Additionally, valid registry information may be used to assist a transit provider in determining what filtering to perform on peer feeds. However, to use a registry, one must first be assured that the registry itself is secure and accurate; without correct information, the route filters generated will not be accurate. Villamizar et

al. [28] propose an authentication and authorization model for providing data integrity in routing policy systems. One drawback of the registry model is that corporations often consider their peering data, policies and routes to be proprietary information (and are thus reluctant to sharing it), though tools such as Rocketfuel [29] provide accurate maps of internal topology, and algorithms exist for inferring customer and peering relationships [30], [31]. The community-supported registry approach is also limited in that the registry itself is often untrusted; a malicious registry can manipulate the route information at will. Information in routing registries also tends to decay quickly because of a lack of clear incentives for organizations to maintain their information [32]. Increasingly, however, the value of maintaining and securing routing registries has been noted within operational networks, because of their importance in laying the foundation for many proposals to secure interdomain routing. Efforts have therefore been made to clean the route registries of spurious information and to ensure the validity of the information within them. We further explore the importance of valid, authenticated registries in the next section.

IV. BGP SECURITY SOLUTIONS

BGP security is an active area of research. Because this activity is relatively new, no solutions have been universally deployed in the Internet. Network administrators currently mitigate some attacks by implementing local countermeasures. The following section reviews the tools used in the Internet to protect BGP. The subsequent sections describe proposed architectures and countermeasures for BGP security.

A. Cryptographic Concepts and Terminology

Jen's understanding is that this will turn into a discussion about the need for authoritative registries and PKI, and what that involves. This is the basis for the sBGP, soBGP, and IRV discussion. Note: Jen will have already discussed pairwise keys and MD5 in the previous section, so some of the text below can go away.

The solutions that have been presented to date have required minimal reliance on centralized resources. Currently, route filtering and defensive best practices for router configuration are relied upon by the majority of Internet operators to keep their networks secure. However, these types of defensive techniques can only provide a limited amount of protection against certain attacks. For example, accepting routing advertisements from a remote, unknown source requires a level of trust in that remote system originating the advertisement that cannot be adequately expressed without additional measures. There is no currently-practised method for determining that information received from an unknown AS is true or valid. The best immediate solution to alleviate these concerns is the implementation of authoritative registries. For example, ARIN may be queried for ownership information of an address block. However, this information is not updated with any frequency, and many of the address delegations have changed since the original ownership block was issued. Organizations may have folded into bankruptcy or merged into other companies, and hence the ultimate ownership for the space is often unknown. By systematically verifying all aspects of the address space that the regional registries delegate, there can be some degree of confidence that route advertisements and the ASes that advertise them are truly authentic.

Additionally, the use of cryptography for securing routing has been very limited to date. Implementation of any cryptographic solutions is uncommon in large ISPs, and these mostly rely on the use of symmetric cryptography, where keys are negotiated in advance and exchanged between two parties. These solutions do not scale to the Internet as a whole, however. Establishing pairwise keys between every ASes becomes a problem of complexity $O(n^2)$, which becomes virtually intractable when the over 20,000 ASes comprising the current Internet are considered. Clearly, another method for establishing secure relationships between ASes is required.

Key management on a global scale requires the existence of public-key cryptography, managed through a *public-key infrastructure*, or PKI. In this framework, every AS has a *public key*, distributed freely to any other AS in the Internet, and a *private key*, which is never divulged. The PKI handles requests for public keys originating from other ASes. Keys are distributed in a hierarchical manner. For example, an AS's key may be associated with its association, which receives its key from a regional registry which in turn receives its key from IANA, the root of the hierarchy tree. Currently, such an infrastructure does not exist, but there has been considerable research in the field. Notably, Seo et al. [33] explore a PKI for the Secure BGP protocol, discussed in detail later in this section. As we can see, there is a need both for authenticated registries, which can store public keys for the organizations that receive AS numbers and address space from them, and an infrastructure that enables this information to be easily found. The current proposals from the research community for securing BGP rely in large part on the implementation of these. For example, APNIC is exploring the creation of a certificate repository based on registry details, which would form the basis for a PKI [34].

Asymmetric, or public-key cryptography, is used extensively in many of the security solutions. Message confidentiality is ensured through use of *encryption*, where ciphertext is generated using the public key of the message recipient. Only the AS with the correct associated private key will be able to decrypt these messages. The complementary security parameter to confidentiality is integrity, which provides evidence that a message has not been modified in transit. Integrity is accomplished through the use of *digital signatures*, hashes of messages enciphered with the private key of the AS originating the message. To verify the message, the receiving AS requires the public key of the AS that sent the message, which can be retrieved through a PKI, and comparing the hash of the received message it generates with that obtained from the decoded signature. Due to the *non-invertibility* of hash functions, it is virtually computationally infeasible to reverse the hash function and create a message that hashes to the same value. Consequently, one can verify that only the signing AS could have sent the message and that it was not altered during transmission.

In certain BGP solutions, symmetric cryptography is used to provide confidentiality and integrity. Notably, ASes sharing only public keys with each other can negotiate a secret key for use in a BGP session (as symmetric cryptography is much faster than its asymmetric equivalent) through use of a Diffie-Hellman key exchange [35]. Encryption can be performed using the secret key as the encryption and decryption key, and integrity can be assured through use of a *message authentication code*, or MAC. In a similar manner to digital signatures, the contents of a message are hashed and signed with the secret key, which the other AS decrypts and compares against the hash it calculates for the message.

The concepts of *certificates* and *attestations* appear in several of the comprehensive solutions for BGP security. Attestations are proofs that an entity is authorized to advertise a particular resource, e.g., a given AS is the owner of a certain address prefix. Attestations can include information on who a resource has been delegated to (e.g., a block of addresses from a larger network block is allocated to another AS) and the parent organization that delegated the resource to the attester (e.g., IANA is the ultimate root for all address ownership), and are signed by the attesting AS or organization. The digital signature ensures the integrity of the attestation, and one can follow the delegation chain, verifying the attestation at each link, back to the source of the original delegation. To verify the attestations, the public key of an AS is required; this information is retrieved through a PKI using certificates. Certificates contain both the public key of the requested AS and a signature attesting to the validity of the certificate, issued by a certification authority, or CA. The CA can be an ISP or a national or regional registry that issues an AS number to the organization, in which case it in turn may have a certificate signed ultimately by a root organization, typically assumed to be IANA. The root certificate is self-signed by IANA in this instance. In a similar manner to attestations, the certificate chain can be verified all the way to the root organization.

B. BGP Security Architectures

Jen's understanding is that this will become a three-part progression through purist but not backwards-compatible sBGP, incrementally-deployable but less-secure soBGP, and out-of-band IRV. Jen says that sometimes there are terminology mismatches that make it difficult to tell which parts of soBGP are similar/different from sBGP; she's owes an read through to identify examples of these kinds of terminology issues.

Recent efforts within the standards bodies and in the research community have attempted to provide comprehensive architectures for BGP security. Each architecture provides an explicit threat model and suite of security services. We focus on the three most comprehensive approaches to BGP security in terms of the increasing flexibility afforded to the user: S-BGP, soBGP, and IRV. As the following sections detail, tradeoffs are made by each protocol in terms of security versus deployability. We start our discussion with S-BGP.

1) S-BGP: Secure BGP (S-BGP) was the first comprehensive routing security solution targeted specifically to BGP [36]. The S-BGP protocol and its associated architecture are currently under consideration for standardization by the Internet Engineering Task Force (IETF), the organization that provides Internet standards. Implementations of S-BGP exist, and its authors are actively experimenting with its use in operational networks.

S-BGP implements security by validating the data passed between ASes using public key certificates. S-BGP supports a pair of PKIs used to delegate address space and AS numbers, and to associate particular network elements with their parent ASes [33]. One PKI is used to authenticate address allocations through a hierarchy stretching from organizations to the providers and regional registries allocating them space, ultimately leading to ICANN (the ultimate authority for address allocation). The second PKI is used to bind AS numbers to organizations and organizations to routers in their network, through issuance of certificates. For example, an organization's AS number is bound to a public key through a certificate. Statements made by the AS are signed using the associated private key. An entity receiving the signed data verifies it came from the AS using the certificate. Because of the

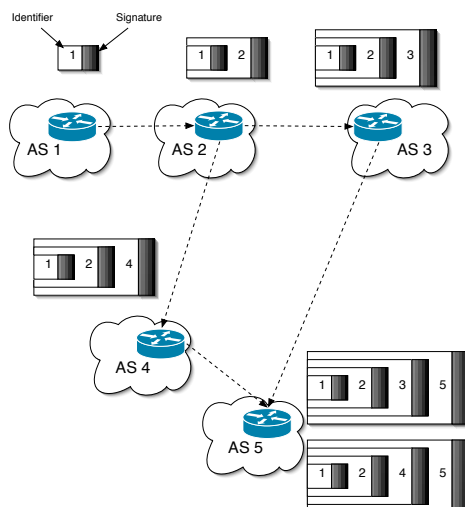


Fig. 1. Route attestations in S-BGP. As UPDATE messages are passed between peers, the receiving peer signs the received message before passing it to another neighbor. The result is an “onion-style” attestation that contains signatures from all routers along the path.

properties of the underlying cryptography, no adversary could have generated the signature, and hence it could have only come from the signing AS.

All data received by a AS in S-BGP is validated using the certificates in the dual PKIs. Address ownership, peer AS identity, path-vectors, policy attributes, and control messages are all signed (and sometimes counter-signed) by the organizations or devices that create them. Because this allows the receiver of the data to unambiguously authenticate the routing information, they can easily detect and remove forged data. However, because of the amount of data and number of possible signers, validation can be extremely costly [37]. These and similar results have raised concerns about the feasibility of S-BGP in the Internet, and led many to seek alternative solutions.

Attestations are digitally signed statements used to assert the authenticity of prefix ownership and advertised routes. *Address attestations* claim the right to originate a prefix, and are signed and distributed *out-of-band*. An out-of-band mechanism does not directly use the BGP protocol to transmit information, instead using choose some external interface or service to communicate relevant data. Each address attestation is a signed statement of delegation of address space from one organization or AS to another. The right to originate a prefix is checked through the validation of a *delegation chain* from ICANN to the advertising AS.

Route attestations are distributed within S-BGP in a modified BGP UPDATE message as a new attribute. To simplify, route attestations are signed by each AS as it traverses the network. All signatures on the path sign previously attached signatures (e.g., are nested). Hence, the validator can validate not only the path, but can validate that *a)* the ASes were traversed in the order indicated by the path, and *b)* no intermediate ASes were added or removed by an adversary. Figure 1 shows a simplified use of route attestations as they propagate between routers.

While S-BGP offers the most comprehensive security guarantees of all proposals by providing full authentication

of origins and the paths to destinations, there are significant barriers that hamper its adoption. A study on S-BGP deployment issues finds that the added overhead of S-BGP countermeasures is equivalent to the CPU and memory provided by a desktop PC [38]. Thus, the hardware requirement is ostensibly minimal, although concerns have been raised over the use of time-averaged statistics. The load in routers is not uniformly distributed, as Internet traffic is bursty in nature [39]. It has also been claimed that S-BGP will cause administrative delays [40]. In addition, assessments of S-BGP through simulation [41] showed that path convergence times would increase by as much as double through adoption of S-BGP, though optimizations to the protocol such as only validating paths when they are selected as optimal may reduce the convergence times. Others have noted the storage requirements for route attestations.

2) *Secure Origin BGP*: Secure origin BGP (soBGP) seeks flexibility by allowing administrators to trade off security and protocol overhead using protocol parameters. In a similar manner to S-BGP, soBGP defines a PKI for authenticating and authorizing entities and organizations. The PKI manages three types of certificates. The first certificate type binds a public key to each soBGP-speaking router. A second certificate type provides details on policy, including the selected protocol parameters and local network topology. This information is stored by the soBGP router receiving the certificate, which uses the information to construct a topology database reflecting the router's view of the network. A third certificate is similar to S-BGP's address attestations in that it embodies address ownership or delegation. All information pertaining to security is transmitted in soBGP between peers via a SECURITY message, a new message type in BGP introduced by soBGP. Thus, in contrast to the out-of-band method of distributing address attestations in S-BGP, the certificates that provide origin authentication are distributed in-band in soBGP, though an out-of-band mechanism for distributing certificates binding keys to routers and topology was later added [42].

soBGP routers use the topology database to validate received routes. Each AS signs and distributes its local topology (i.e., its peers) through the topology certificate to form a global database and corresponding static topology graph, of which each soBGP router should have a consistent view. The database is used to verify received routes: any UPDATE with a path that violates the AS topology is demonstrably bad and dropped. The major difference between the approach taken by soBGP for path authentication and the one taken by S-BGP is that in S-BGP, route attestations are dynamic: they are sent with every BGP UPDATE message and the recipient of the routing information has a real-time view as to the path taken by the message. By contrast, the topology graph and corresponding database used by soBGP is fundamentally static, as the topology will only change when a new policy certificate is issued; thus, a new topology may not be reflected when an UPDATE is received and the path it took may be different from the one reflected in the peer's topology database. Additional infrastructure is required to ensure that the topology updates are synchronized across all ASes. Moreover, forged paths that are consistent with the routing topology will be accepted.

Validating signatures is a computationally expensive operation. soBGP tries to mitigate this cost in the presence of limited resources by authenticating long term structural routing elements (such as organization relationships, address ownership, and topology) prior to participating in BGP. Authenticated data is signed, validated, and stored

at the routers prior to the establishment of the BGP session, and thus their validation does not introduce significant run-time cost. Transient elements (such as paths) are locally checked for correctness, rather than validated through the PKI, e.g., adjacent ASes in the path must be reflected in the topology database.

The soBGP platform provides several deployment options and the ability to be incrementally deployed [42]. One option, for example, allows the operator to choose whether to verify routes before accepting them into the routing table (placing a premium on security) or to accept routes and then verify their authenticity (placing a premium on convergence time). Another example is the option whether to verify a route using the topology graph, or only the first hop after the origin, or to refrain from validation altogether. These options give soBGP a greater ease of deployment than S-BGP, but the number of options could yield issues with interoperability [43]. Further work on soBGP defines RADIUS attributes to support its provisioning [44], but this solution is considered suboptimal. Furthermore, soBGP may not guard against mid-path disruptions [45].

3) *Interdomain Route Validation*: The Interdomain Route Validation (IRV) service is a receiver-driven protocol and associated architecture [46], and is the least centralized of the comprehensive solutions for securing BGP. Unlike S-BGP, IRV's operation is independent of the routing protocol. Every AS in IRV contains an IRV server. Upon reception of an UPDATE message, a receiving BGP speaker will appeal to its local IRV server for an indication of whether the received information is correct (see Figure 2). The local IRV server determines correctness by directly querying the IRV server in the relevant AS for validation of the route information. Where validation from multiple ASes is needed, i.e., to validate a path involving multiple ASes, collections of IRV servers are queried.

The key idea of IRV is that each data item *can be* validated by directly querying the AS from whence it came. A BGP speaker decides which data to trust, which to ignore, and which to validate via an IRV query based on local policy. Hence, the amount of effort expended in validating data is exactly what is required. IRV servers are similar to route registries, but manage information only from the parent AS. IRV approach is arguably more likely to be successful than registries because the AS retains control over the data, and hence is more likely to keep it fresh, accurate, and available.

Where available, a secure underlying network layer (e.g., IPsec) or transport layer (e.g., TLS [47]) is used to secure the communication between IRV servers (i.e., to ensure the authenticity, integrity, and confidentiality of queries and results). IRV servers can tailor responses to queries based on the requesting entity. This allows the IRV to perform access control over the routing data which is useful in limiting the exposure of sensitive data such as policy and peering relationships.

IRV tries to remove the computational and storage costs from the critical path of routing. Validation of path information is discretionary; that is, the algorithm for determining when and how an UPDATE message should be validated is chosen by each AS. The IRV server can query every AS along the path of a given update, or choose to only query a subset of the ASes based on previous associations (e.g., ASes known to provide trusted information may not be queried). Stronger guarantees can be achieved if every update is fully validated, while better performance can be maintained if the updates are checked only periodically or partially and queries made when the results appear suspicious (as determined by heuristics). Caching previous queries can also improve performance, while storing

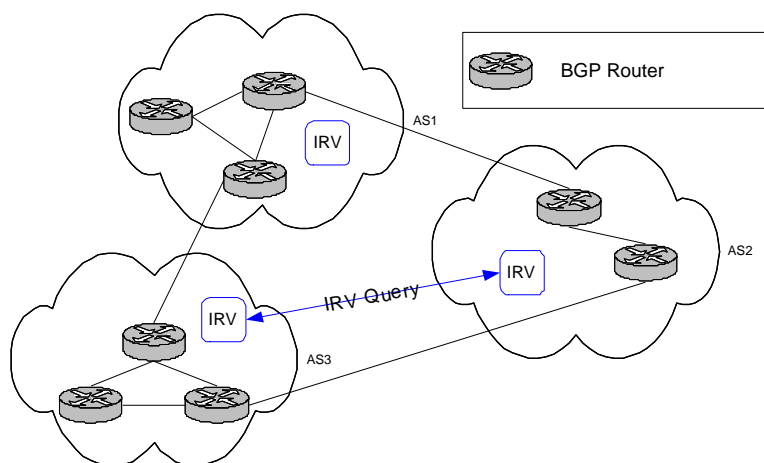


Fig. 2. ASes running the IRV protocol query the appropriate authorities for validation of received routing data.

received route advertisements and withdrawals can allow for debugging and failure detection. All of this occurs between IRV servers, and not routers. Hence, costs are controllable by the AS, and resources demands are largely external to the routers.

The central limitation of IRV is that it needs a functioning network to be useful: a client indirectly uses the network to communicate with the foreign AS to query the appropriate AS IRV server. This presents problems both in bootstrapping the process and in recovering from outages. Solutions to this problem include optimistic routing (e.g., use received routes immediately and validate possible), AS collaboration (e.g., exchange routing data via gossip-style protocols [48]), and using static routes to IRV servers. Additionally, IRV requires more analysis of infrastructure requirements and operational semantics to be a viable security alternative.

C. Experimental Systems

Jen's understanding is that we'll take a stab at organizing this around key challenges, like "reducing computational overhead" or "avoiding global PKI", if possible. We'll also remove the stuff related to protecting the BGP session, since Jen will cover those earlier. Also, we're removing Listen, as it is not really all that related. Also, the idea is that we'll pull in the text from the next section – on evaluating the architectures – rather than having a separate section for that.

Note from Jen: Perlman's thesis seems tricky to integrate here, as it is pretty broad. I wonder if we should hit Perlman's thesis in the Introduction of the paper instead, and only highlight the parts most relevant to BGP here. In the Introduction, we could talk about the notion of Byzantine behavior, for instance, to set the stage.

A number of works have sought solutions to the myriad security issues in interdomain routing security. Some focus on more formal properties of routing, while others explore the application of novel cryptographic structures that provide strong security guarantees. This section sketches a number of these works in broad detail. We begin

in the following subsection by reviewing the some of the early works in BGP security.

1) Early Approaches: Radia Perlman's thesis [49] was the first significant work addressing routing security. The dissertation is particularly notable for examining *Byzantine behavior* within routing protocols. Byzantine behavior occurs when any routing element exhibits arbitrarily faulty or malicious behavior. For a protocol to provide security in this environment, it must display *Byzantine robustness*; that is, in the face of malicious or faulty behavior from other hosts, all non-faulty hosts in the system should reach a decision on a particular message's contents within a finite time period (termination), this decision should be the same among all non-faulty hosts (agreement), and the message should be the one sent by the source node (validity). Perlman develops a link-state protocol that satisfies the properties for Byzantine robustness. Perlman's link-state solution does not effectively scale to networks the size of the Internet, and hence is not suitable for interdomain routing. However, some conceptual elements of Byzantine robustness are present in almost every proposed definition of BGP security. For example, assessing the validity (as defined by Perlman) of received routes and policy is the central goal of the three architectures defined in the preceding section.

Jen thinks the session-level parts of the Smith work are getting removed from here, and discussed at a high level in the previous section, in the context of prior work related to, and superceded by, IPSEC

Smith and Garcia-Luna-Aceves [13] proposed five countermeasures to secure interdomain routing. These countermeasures enhance the BGP protocol by modifying both the session environment and the BGP message attributes. Two countermeasures aim to protect BGP control messages by encrypting all BGP data between peers (using a secret key shared by the peers) and adding sequence numbers to enforce a total ordering on the messages. The other three countermeasures offer protection for UPDATE messages and include the addition of an UPDATE sequence number or timestamp, addition of a new path attribute, PREDECESSOR, that identifies the last AS before the destination AS, and digital signatures (signed by the peer) of all fields in the UPDATE message whose values are fixed.

Smith and Garcia-Luna-Aceves's countermeasures are similar to those provided by S-BGP, where the session encryption and sequencing provides confidentiality and ordering, the peer signatures guarantee authenticity of the full BGP path. However, the authors' claim that the session encryption provides integrity is technically incorrect: encryption alone does not provide integrity. However, exploiting the vulnerabilities exposed to a lack of integrity of ciphertext is somewhat difficult in this case.

2) Hop Integrity Protocols: Jen thinks that this text is going away, with some aspects moving to the previous section, in relating to IPSEC. Jen may need some help on this because she is, frankly, pretty clueless...

Within the context of interdomain routing, *hop integrity* is the property that peers can detect any modification or replay of exchanged information. Gouda et al. [11] propose a suite of protocols that also provide security at the IP layer. As with the Smith approach discussed above, sequence numbers and message MACs are used to ensure

integrity and ordering. Gouda et. al. extend this approach by suggesting a Diffie-Hellman [35] style protocol³ that uses public key certificates to negotiate and refresh the secret keys shared by peers. Due to its wide deployment and flexibility, IPsec has supplanted this proposal as the way to perform hop integrity.

3) *Reducing Computational Overhead*: The following solutions base their security on facets of the S-BGP schemes, either with regards to address or route attestations. Each solution offers a different method of reducing the computational costs, associated with attestations while providing a similar level of security for either origin or path authentication to S-BGP itself, often by devising more efficient cryptographic proof systems.

Origin Authentication (OA) is a method of validating address ownership such that prefix hijacking and related attacks are not possible. One effort directly investigates origin authentication (OA) by examining the semantics, design and application of OA services [50]. The semantics of address delegation are formalized, and various cryptographic structures for asserting the address block ownership and delegation are explored. In particular, the authors study cryptographic proof structures [51], [52] for carrying delegation attestations (i.e., cryptographic proofs of delegation). To simplify, a cryptographic proof structure is a structure for asserting the validity of a set of statements. The authors approximate the delegation hierarchy by extracting the nested announcements made within the protocol. They found that the delegations were very stable over time, making them ideally suited to a class of proof structures based on Merkle hash trees [51]. A simulation shows that on-line origin authentication is possible using this construction, a feat which was previously thought to have been too computationally expensive to be feasible.

Hu et al. hu:03 proposed a solution that uses traditional secret key cryptography to authenticate received path vectors. In their solution, each AS on an UPDATE's path shares a secret key with a previously identified validator known as the *destination AS*. The originating AS computes a MAC using a shared key over a concatenation of an initial authenticator value (e.g., 0), the path, and the fields that do not change (e.g. ORIGIN attribute, NLRI, etc.). The MAC is included in the UPDATE and propagated using BGP. Each of the subsequent ASes perform the same operation but use the received MAC as the authenticator value. This ensures that each subsequent MAC covers not only received information, but also the authenticator value of the preceding hop. Upon receiving the MAC, the destination recursively validates the MACs using the known secret keys. In essence, this is symmetric key equivalent to the recursive signatures specified in S-BGP, where MACs are used instead of digital signatures. The destination AS can validate all the MACs because it knows all the secret keys.

Hu et al. extended their work in path authentication with the *Secure Path Vector* protocol (SPV) [53]. SPV implements path validation using a string of one-time signatures [54], [55] generated from a single root value. Also known as off-line signatures, one-time signatures allows the signer to perform the heavyweight cryptographic operations prior to use, and the later signing operation is very fast. SPV extends this approach to allow a single off-line signature to generate potentially many signatures. To simplify, in SPV, the originator of a prefix establishes

³Diffie-Hellman protocols use public key cryptography to negotiate shared secrets between parties over an untrusted media, e.g., a public network. This protocol and its variants are the most widely used protocol for performing *key negotiation*.

a single root value used to seed the generation of one-time signature structures for each hop in the PATH. Signatures and signing material (to be used by the next hop) are forwarded to each hop in the route propagation. Receivers of the route use initiator generated an initial validation token to verify the one-time signatures, and ultimately the path. The operation of SPV is extremely lightweight, where hashing is used as the primary cryptographic mechanisms. However, this efficiency comes at a cost; SPV is a very complex protocol involving the manipulation and communication of a significant amount of state. More generally, however, the security of SPV is in some cases based on probabilistic arguments. In particular, the authors argue that reduced exposure (in time) to forgery vulnerabilities is sufficient to mitigate attacks. While this may be acceptable for some constrained environments, it is unclear whether such arguments are appropriate in the larger Internet.

Another method of performing path authentication was suggested by Zhao et al. [56]. This scheme suggested the use of *signature amortization* [41], where any BGP UPDATE messages sent to the same group of peers requires only one signature for the group, rather than n signatures for n peers, and aggregating UPDATE messages in the output buffers of a router and building a Merkle hash tree for all unsigned messages, so they are collectively signed with only one signature operation. Additionally, the scheme uses previous work by the authors in adapting *aggregate signatures* to BGP [57]. Aggregate signatures allow for multiple signatures, each having been signed on a different message by a different user, to be aggregated into one signature. While signature aggregation can decrease the computational overhead of signatures, it introduces increased memory requirements. Conversely, while aggregate signatures introduce a small computational overhead, they are space-efficient. By selecting various parameters to optimize time and space complexity, the optimal solution presented displays much faster convergence times than S-BGP with memory requirements cut by over two-thirds.

An alternate method of amortizing the costs of computation is based on considering the *reference locality* of BGP advertisements [58]. The authors in this work base their cryptographic constructions on the BGP updates retrieved from the Route Views data archive and notice that paths are generally stable, and the number of new paths grows fairly slowly. Leveraging these facts, based on data analysis, the authors suggest alternative path authentication mechanisms to S-BGP route attestations that maintain a similar level of security while dramatically reducing the number of signature validations required. The cost in this approach is a commensurate increase in the bandwidth requirements because of the large cryptographic proof systems that are distributed. The authors claim that the constructions proposed are compatible with other solutions and could benefit from space-saving measures like the aggregate signatures proposed by [56], based on the orthogonality of this approach to existing solutions.

4) *Alternatives to PKI*: Prior to the creation of BGP version 4, Kumar and Crowcroft [59] provided an analysis of threats to interdomain routing and described security mechanisms used in the proposal IDRIP protocol [60]. Designed as a superset of BGP and EGP, IDRIP is an interdomain routing path vector protocol. The protocol uses an encrypted checksum transmitted with all routing messages transmitted between routers. The checksum authenticates the message and is encrypted based on an algorithm agreed upon by the two routers. Additionally, authenticated timestamps and sequence numbers are provided as anti-replay mechanisms. The authors asserted, however, that malicious entities masquerading as sources will be unsuccessful in a hop-by-hop routing protocol, neglecting to

consider prefix hijacking. The authors further asserted that link level encryption is impractical due to computation cost, as is digitally signing every routing packet. While largely true at the time the authors designed the protocol (1993), this is clearly no longer the case. IDRPs failed to catch on and later advances made cryptographic operations feasible. Hence, while this proposal highlighted important requirements for routing security, it is not appropriate for current networks.

The *Pretty Secure BGP* (psBGP) [61] system introduces an addresses origin authentication service within a larger comprehensive architecture for BGP security similar to that suggested for S-BGP [33]. Path authentication is performed using an optimized version of S-BGP introduced by Nicol et al. [37]. The central philosophy of their work is that while ASes can be managed within a PKI (because there are relatively few and the list is stable), it is not possible to manage addresses through a centralized PKI such as those promoted by previous systems. Origin authentication is implemented in a decentralized system in which each AS creates a prefix assertion list (PAL). The PAL contains address ownership assertions of the local ASes and its peers. An origin claim is validated by checking the consistency between the PALs of peers around the advertising origin. In this way, psBGP provides a very weak form of origin authentication: *any* AS can bear witness to the validity of an origin claim.⁴ The assumption that any two of the over 20,000 ASes will not collude is seen as somewhat difficult to support in the general Internet. Moreover, psBGP requires an AS place its trust in the alien ASes to regulate IP addresses, most of which possess no existing relationships or often knowledge of each other.

5) *Detecting and Mitigating Anomalies*: The following solutions often share in common with solutions from the previous subsection that they are designed to be used without a PKI. They have the additional feature, however, that they are primarily based on detecting anomalies in routing or the surrounding infrastructure, and use this information to mitigate threats to routing.

An IP prefix should generally only be originated by a single AS [1]. A multiple origin AS (MOAS) conflict occurs when a prefix is simultaneously originated by more than one AS. Such events can legitimately occur in the natural course of operation where, for example, a multi-homed AS transitions between preferred routes. In some cases, however, these MOAS conflicts directly indicate prefix hijacking. A recent study of MOAS conflicts showed potential causes included prefixes associated with exchange point addresses (which link ASes), multi-homing without BGP or with private AS numbers, and faulty configurations [62]. An enhancement BGP was proposed that uses community attributes [63] to distinguish between valid and invalid MOAS conflicts [64] in responses to these operational oddities. A list of ASes authorized to announce a given prefix is appended to the community attribute. This list can then be used to determine if an MOAS conflict is valid. Because the community attribute is optional and transitive, routers can drop this information without causing an error. Because they are not authenticated, the advertisements can be forged or altered by malicious routers. However, the authors suggest that forged routes can be detected by flagging prefixes received with multiple, conflicting AS lists. An application of this idea was a proposal

⁴The authors consider other modes in which *k-out-of-n* peers asserting validity are required for the origin to be accepted. However, this is only useful in weeding out highly connected colluding pairs.

to employ path filtering based on the heuristics such as those used for MOAS detection to protect BGP routes to top-level DNS servers from modification, because of the importance of DNS to the network infrastructure [65]. This is possible because routes to popular destinations were found to be stable, and the DNS is highly redundant, with top-level servers distributed in both number and geography.

Kruegel et al. [66] consider the use of intrusion detection to identify forged origin announcements, and discover several metrics used to identify bogus announcements (e.g., strange aggregation, tracking of historical associations between prefixes and ASes). One interesting aspect of this work is its dependence on operational issues: the detection criteria are not derived from the BGP specification, but arise from the evaluation of common configurations and AS behavior. In particular, the method observes ownership over time. Any departure from normal ownership behavior (a new AS begins to announce the address, or a new MOAS occurs) is considered to be malicious and is flagged. However, the prefix ownership lists are pre-computed and not dynamic in nature.

A further extension to the work in MOAS detection is the *Prefix Hijacking Alert System* (PHAS) [67], which builds on the concept of prefix ownership. PHAS is predicated on the notion that a prefix owner is the only entity that can differentiate between real routing changes and those that take place as a result of a prefix hijacking attack. To that end, routing updates from the Route Views and RIPE repositories are examined and if there are changes to the originator of a route, the owner of that prefix is notified through email, optimally set up along multiple paths in case the common path has been hijacked. The system is incrementally deployable in that to join the system, a prefix owner need only register with the PHAS server; however, this server is also a single point of failure in the system, and if it is compromised, it could send out numerous false alarms to prefix owners. Additionally, the system relies on the validity of entities registering their prefixes; there is no protection against an adversary making a false registration. This situation could be ameliorated if authenticated, secure registries were available.

Hu and Mao examined prefix hijacking in greater detail and provided a mechanism for detecting prefix hijacking attacks in real time [68]. Their solution is based on fingerprinting techniques for networks and hosts. A number of criteria, including the operating systems of machines within a given prefix, and the identifier field within IP packets, TCP and ICP timestamps, are used to characterize a particular network prefix, with information collected by probes sent to various hosts within the network of interest. If there are conflicting origin ASes advertised, which is potential evidence of a prefix hijacking attack, the collected fingerprints are compared against probes sent to all origins. Differentiation between fingerprints will provide evidence that updates have been received from different originating machines, and that a newly-advertised prefix with sufficiently different characteristics is not the original network advertising a new path, but rather an adversary attempting to hijack the prefix. This approach relies on a real-time BGP UPDATE monitor, which will send differentiating probes if prefixes are advertised from multiple locations. The availability of the monitor is critical, as if updates are delayed, the ability to take measures such as probing and subsequent decision making will be compromised. Subsequent work investigated how to optimally place route monitors within the Internet to maximize prefix hijacking detection coverage [69].

The *Whisper* protocols [70] are designed to validate the initial source of path information. The protocol do not provide explicit route authentication. Rather, it seeks to alert network administrators of potential routing

inconsistencies. In its weakest form, a hash chain is used in a similar fashion to the cumulative authentication mechanism described by Hu et al. [71]. A random value is initially assigned to each prefix by the originator. The value is repeatedly hashed at each hop as it is propagated from AS to AS. Received paths are validated by receiving routers by comparing received hash values; if the hash values are the same, then they must have come from the same source (because they represent the same repeated application of the hash function). Stronger protocols are proposed that increase security by making the initial value less knowable using heavyweight modular exponentiation. One variant uses a construction similar to RSA [72]⁵, where a random initial value is exponentiated (modulo a prime group) by the AS numbers of the ASes a route traverses. Because of the mathematical properties of the prime group, the intermediate AS values can be factored out and the result unambiguously associated with a single initial value. Another variant using a series of hash constructions is complicated by the fact that only the route originator can verify the route because of the non-invertibility of secure hash functions. Thus, the recipient would have to query the originator as to the veracity of the route, which is often outside of the purview of the originator's knowledge.

Another alerting system recently proposed is *Pretty Good BGP* (PGBGP) [73]. The key insight in this work is that misconfigurations and prefix hijacking attacks could be mitigated if routers exercise a certain amount of judgement with the routes that they adopt into their routing tables. With PGBGP, an amount of state is maintained through historical routing data to determine what routes to prefixes should be considered normal. When incoming routes are received that do not adhere to these origins, they are flagged as suspicious for 24 hours, using the data from Mahajan et al. [74] that shows most misconfigurations and hijack attempts last for less than this amount of time. The routes are avoided while they are suspicious unless there are no suitable alternative routes. The results of this work show that this solution may often protect ASes against hijacking attacks, with some important caveats. An administrator deploying this solution must be cognizant of their business relationships with providers and customers and ensure that events such as provider changes (which result in new paths to destinations) are accounted for so that convergence is not affected; additionally, sufficiently equipped adversaries can or engineer the set of routes the system is forced to accept, in a routing equivalent of the link-cutting attack by Bellovin and Gansner [75].

D. Factors Complicating Adoption of Security Solutions

BGP security is complicated by operational considerations. Interdomain routing is stressed by the continuous growth of the Internet. Around 30,000 AS numbers have already been assigned. Due to the increasing number of ASes, There are predictions that if current trends continue, the AS number space will be exhausted by as early as 2009 [76]. This growth contributes to the number of routing update messages a router receives, thus adding to routing table growth, which in turn leads to scalability issues. The graph in Figure 3 shows BGP updates from the CIDR report for 1988 to 2003. The number of updates a BGP router keeps in its forwarding table has grown linearly, thus making scalability a major issue. Any security measures must consider these scalability issues [77], [78].

⁵The initial published protocol inherited the *common modulus* limitation from RSA. The authors provide alternate constructions which address this problem in later versions of the paper.

Solution Definition			Security Services		
System	In Use	Style	Topo. Auth.	Path Auth.	Origin Auth.
Route Filtering	yes	anomaly	<i>weak</i>	<i>weak</i>	<i>weak</i>
Route Registries	yes	anomaly	<i>weak</i>	<i>weak</i>	<i>weak</i>
S-BGP	no	crypto	strong	strong	strong
soBGP	no	crypto/anom.	strong	none	strong
IRV	no	crypto/anom.	strong	strong	strong
Origin Auth. (Aiello et. al.)	no	crypto	none	none	strong
Path Auth. (Hu et. al.)	no	crypto	strong	strong	none
SPV	no	crypto	strong	strong	none
Listen	no	anomaly	none	none	<i>weak</i>
Whisper	no	anomaly	none	<i>weak</i>	none

TABLE II

GLOBAL BGP SECURITY SOLUTIONS - REQUIREMENTS (COLUMNS) RELATE TO THE GUARANTEES PROVIDED FOR GLOBAL AS DATA. *Deployed* INDICATES WHETHER THE SOLUTION IS PRESENTLY IN OPERATIONAL USE. *Style* INDICATES WHETHER THE SOLUTION IS BASED ON A CRYPTOGRAPHIC PROTOCOL OR AN ANOMALY DETECTION SERVICE. THE AUTHENTICITY SERVICES INCLUDE: TOPOLOGY (ARE PATHS CONFORMING TO THE CORRECT TOPOLOGY), PATH (ARE ALL PATHS AUTHENTICATED), AND ORIGIN (ARE ORIGINS AUTHENTICATED). WE A SYSTEM IS STRONG IF IT PROVIDES AUTHENTICITY GUARANTEES, AND WEAK IF IT RECEIVED DATA IS PROBABILISTICALLY AUTHENTIC/CORRECT.

A summary of the proposed BGP security solutions is given in table II. Currently, the only solutions deployed in wide use are the use of routing filtering and some reliance on routing registries, which are only moderately effective at best. As discussed in section III, many solutions require secure and valid route registries as a minimum for their effectiveness; for example, this information is necessary for correctly communicating address ownership and delegation, and is a necessary first condition for implementing real origin authentication solutions. Accomplishing even this goal is non-trivial because of the amount of invalid information in the registries and the number of legacy allocations that exist. Ensuring the accuracy of the registries accomplishes many goals beyond security, however, as ISPs can use this information to identify customer and peers and to clarify what filtering policies are and should be. This is a necessary first step that will aid network operators and security researchers in myriad ways.

Another major concern that hampers adoption is the perception within the operations community that the computational requirements (e.g., symmetric and public-key cryptography) of many current solutions will overload deployed routers, and the cost of upgrading those routers, if it is even feasible, or replacing them outright, is prohibitive. Regardless of which platform is picked, the solutions will add additional complexity, infrastructure, and cost to the network, and could potentially affect convergence [40]. BGP convergence is a major issue, and under certain circumstances, the protocol may not converge at all [79], [80]. However, solutions that reduce the costs of cryptography, such as those discussed in section IV-C3, may mitigate some of these concerns.

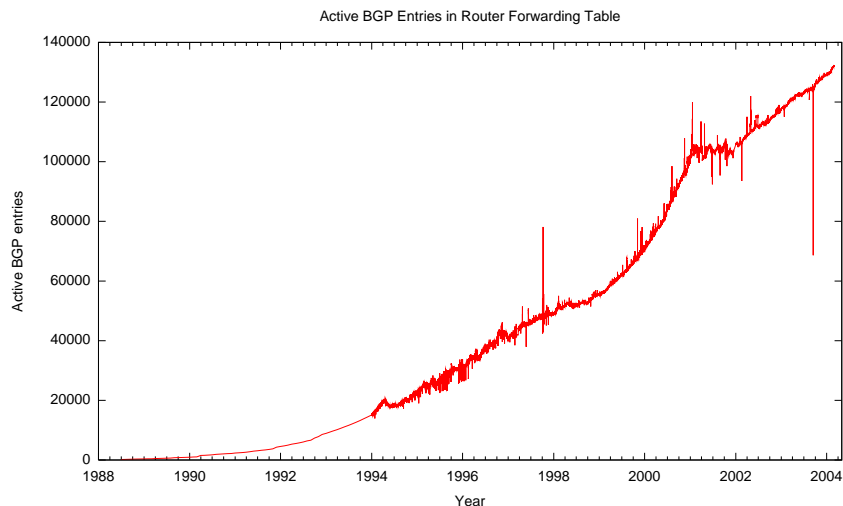


Fig. 3. 1988-2003 routing table updates from the CIDR report (<http://www.cidr-report.org/>)

Potential measures that could be implemented include more robust modeling of security protocols through formal analysis to understand the security obtained; Aiello et al. [50], Butler et al. [58], and van Oorschot et al. [61] explore formal semantics in their works. Understanding how to adopt these solutions and the effect of that adoption through modeling is another way to evaluate solutions; preliminary work in this area has been performed by Chen et al. [81]. Finally, robust simulation of the security schemes across a common testbed may help the community determine the tradeoffs necessary for solution adoption and assist in the parameterization or hybridization of these schemes, (e.g., combining facets of signature amortization schemes and using them in conjunction with one or more anomaly detection schemes). Very detailed network simulators such as *ns2* [82] are often best used for simulating detailed events in a small network setting, but may be difficult to scale to a sufficient scale for modeling the global network encompassed by BGP, and are not made with the protocol in mind. Simulators such as SSFNet [83] address many of the demands made by a protocol such as BGP, but fully modeling the workings of the over 20,000 ASes that comprise the Internet may still not be feasible without extremely large-scale and highly parallelized solutions, or abstracting away details that may not be relevant to security. A common simulator and framework for its deployment such as DETER [84] may be the most appropriate method for fully evaluating solutions, along with small-scale deployments, with input from both the research and operational communities.

V. FUTURE DIRECTIONS IN BGP SECURITY RESEARCH

We turn our attention now to work that can impact how BGP security is approached, and techniques that may be used to improve aspects of BGP's operation, improving security at the same time.

A. Routing Frameworks and Policies

A study on the performance impact of incrementally deploying router-assisted services shows that choosing the right deployment strategy for a new protocol or service can mean the difference between success and failure [85]. Suggestions have been made for designing a routing architecture in large networks such that scalability requirements are met [86]. A model and middleware for routing protocols, SPHERE, decomposes routing protocols into fundamental building blocks to support hierarchical design [87]. Another approach towards analysis of routing security is performed by Pei et al. [88], who suggest defining a defense framework for intra- and interdomain routing protocols. This includes classifying areas of protection into fields such as cryptographic protection schemes and semantics validation. Each of these efforts aims to provide a foundation for designing an interdomain routing security solution. Additionally, best common practices (BCPs) build resistance into BGP routing [17]. Armed with BCPs and other tools, the Internet can be made more secure by simply protecting the most connected nodes. One study shows that protecting most connected nodes provides significant security gains [89]. Finally, an overview of route filtering and S-BGP as countermeasures to BGP attacks is given in [90].

B. Cryptographic Constructions

Future BGP security research can exploit new cryptographic constructions to efficiently and securely protect the routing fabric. For example, many security techniques involve the use of digital signatures. New and improved signatures may aid in the efficiency of signature-based countermeasures [91], [92]. One study also suggests an efficient, low cost protocol for signing routing messages [93]. One area of particular interest is the field of forward-secure digital signatures [94], where the public key of a digital signature is fixed but the private key, used for signing, changes with time. This ensures that if the key is compromised, messages from the past cannot be forged, thus preserving non-repudiability of past signatures. Recent work has shown that forward-secure signatures can have performance figures competitive with traditional signatures if properly configured for the application [95].

C. Attack Detection

Detecting attacks is an active field of research. The PAIR algorithm [96] is an approach to discover, and recover from, inconsistencies in distance-vector routing. It may be possible to employ similar techniques in a path-vector protocol such as BGP. Protocols that detect and route around faults may also yield valuable insights [97]. The ability to recover from routing attacks and failures is crucial to infrastructure reliability. One study shows that path faults in BGP can at times take up to 30 minutes to repair [98]. In certain cases, some end-to-end routing failures may not be reflected in BGP traffic at all [99]. Being able to detect attacks before they occur is clearly the best alternative, and tools such as secure traceroute [100] and AS-level traceroute [101] to detect malicious routing may aid in this effort.

VI. CONCLUSION

BGP has been quite successful in providing stable interdomain routing, and is surprisingly robust. It was originally thought in many circles that the ISO's Interdomain Routing Protocol (IDRP) [60] would be the successor to BGP,

but because of diminishing interest in network protocols other than IP, BGP is the only interdomain routing protocol in wide use [102]. Moreover, because of its huge installed base, BGP will continue to play a crucial role in Internet routing. As such, BGP will adapt to changing needs of its constituency. This evident even now: multi-protocol extensions are increasingly used to route IPv6 packets [103].

Interdomain routing security has progressed since being first investigated by Perlman, but few production environments are demonstrably more secure than they were when she began that work. Some operators are using incremental solutions that offer some protection, but comprehensive solutions have not been deployed. Solving the issue of BGP security is very difficult because of the scale and complexity of the Internet. Every network in the world communicating with other organizations through the Internet uses BGP, and errors in configuration and operation can have a global impact. This survey has examined the threats to BGP and proposed solutions to ensure its security. While they have not been implemented yet in practice, and while their adoption may be difficult, good progress *has* been made. In the end, a methodology to securing BGP may be one of the best way to ensure that the Internet remains a reliable and useful vehicle for private and public communication.

REFERENCES

- [1] J. Hawkinson and T. Bates, "Guidelines for creation, selection, and registration of an autonomous system (AS)," 1996, rFC 1930.
- [2] Y. Rekhter and T. Li, "A Border Gateway Protocol 4 (BGP-4)," Mar. 1995, rFC 1771.
- [3] J. Stewart, *BGP4: Inter-Domain Routing in the Internet*. Reading, MA: Addison-Wesley, 1999.
- [4] R. Barrett, S. Haar, and R. Whitestone, "Routing snafu causes Internet outage," *Interactive Week*, April 25 1997.
- [5] L. Wang, Z. Zhao, D. Pei, R. Bush, D. Massey, A. Mankin, S. Wu, and L. Zhang, "Observation and analysis of BGP behavior under stress." IMW workshop 2002, 2002.
- [6] Department of Homeland Security, "The national strategy to secure cyberspace," Feb. 2003.
- [7] T. Griffin and G. Huston, "BGP Wedgies," *Internet Engineering Task Force*, Nov. 2005, RFC 4264.
- [8] S. Kent and R. Atkinson, "IP Encapsulating Security Payload," Nov. 1998, rFC 2406.
- [9] —, "IP Authentication Header," Nov. 1998, rFC 2402.
- [10] A. Heffernan, "Protection of BGP sessions via the TCP MD5 signature option," Aug. 1998, rFC 2385.
- [11] M. G. Gouda, E. N. Elnozahy, C.-T. Huang, and T. M. McGuire, "Hop integrity in computer networks." Osaka, Japan: Eighth International Conference on Network Protocols, Nov. 2000.
- [12] V. Gill, J. Heasley, and D. Meyer, "The Generalized TTL Security Mechanism (GTSM)," RFC 3682, Feb. 2004.
- [13] B. Smith and J. Garcia-Luna-Aceves, "Efficient security mechanisms for the border gateway routing protocol," *Computer Communications*, vol. 21, no. 3, pp. 203–210, 1998.
- [14] R. Rivest, "The MD5 Message-Digest Algorithm," Apr. 1992, rFC 1321.
- [15] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," RFC 2104, Apr. 1997.
- [16] S. P. in the TCP/IP Protocol Suite, "Steven m. bellovin," *Computer Communications Review*, vol. 2, no. 19, pp. 32–48, 1989.
- [17] B. Green, "BGP security update: Is the sky falling?" Jun. 2002, nANOG 25.
- [18] S. Kent and R. Atkinson, "Security architecture for the Internet Protocol," Nov. 1998, rFC 2401.
- [19] R. Thayer, N. Doraswamy, and R. Glenn, "IP Security Document Roadmap," Nov. 1998, rFC 2411.
- [20] D. Maughan, M. Schertler, M. Schneider, and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)," Nov. 1998, rFC 2408.
- [21] D. Harkins and D. Carrel, "The Internet Key Exchange," RFC 2409, Nov. 1998.
- [22] B. Gleeson, A. Lin, J. Heinanen, G. Armitage, and A. Malis, "A Framework for IP Based Virtual Private Networks," RFC 2764, Feb. 2000.
- [23] B. Smith and J. Garcia-Luna-Aceves, "Securing the Border Gateway Routing Protocol." London, UK: Global Internet '96, Nov. 1996.

- [24] T. Bates, P. Smith, and G. Huston, "CIDR report for 27 January 07," <http://www.cidr-report.org/>, Jan. 2004.
- [25] J. Stewart, T. Bates, R. Chandra, and E. Chen, "Using a Dedicated AS for Sites Homed to a Single Provider," *Internet Engineering Task Force*, January 1998, RFC 2270.
- [26] N. Feamster, Z. M. Mao, and J. Rexford, "BorderGuard: Detecting Cold Potatoes from Peers," in *Proceedings of the 2004 Internet Measurement Conference*, Taormina, Italy, Oct. 2004.
- [27] T. Bates, E. Gerich, L. Joncheray, J.-M. Jouanigot, D. Karrenberg, M. Terpstra, and J. Yu, "Representation of IP routing policies in a routing registry," RFC 1786, Mar. 1995.
- [28] C. Villamizar, C. Alaettinoglu, D. Meyer, S. Murphy, and C. Orange, "Routing policy system security," Dec. 1999, rFC 2725.
- [29] N. Spring, R. Mahajan, and D. Wetherall, "Measuring ISP Topologies with Rocketfuel." Pittsburgh, PA, USA: ACM SIGCOMM 2002, Aug. 2002.
- [30] L. Gao, "On inferring autonomous system relationships in the Internet," *IEEE/ACM Transactions on Networking*, vol. 9, no. 6, pp. 733–745, 2001.
- [31] L. Subramanian, S. Agarwal, J. Rexford, and R. Katz, "Characterizing the Internet hierarchy from multiple vantage points." New York, NY, USA: IEEE INFOCOM 2002, Jun. 2002.
- [32] T. Griffin, "*personal communication*," Jun. 2003.
- [33] K. Seo, C. Lynn, and S. Kent, "Public-key infrastructure for the Secure Border Gateway Protocol (S-BGP)." Anaheim, CA, USA: IEEE DARPA Information Survivability Conference and Exposition II, Jun. 2001.
- [34] APNIC, "The APNIC Resource Certification page," <http://mirin.apnic.net/resourcecerts/>, Nov. 2006.
- [35] W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, November 1976.
- [36] S. Kent, C. Lynn, and K. Seo, "Secure Border Gateway Protocol (S-BGP)," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 4, Apr. 2000.
- [37] D. Nicol, S. Smith, and M. Zhao, "Efficient security for BGP route announcements," Feb. 2002, dartmouth Computer Science Technical Report TR-2003-440.
- [38] S. Kent, C. Lynn, J. Mikkelsen, and K. Seo, "Secure Border Gateway Protocol (S-BGP) real world performance and deployment issues." ISOC Symposium on Network and Distributed System Security, Feb. 2000.
- [39] S. Uhlig and O. Bonaventure, "Understanding the long-term self-similarity of Internet traffic." Coimbra, Portugal: 2nd International Workshop of Quality of Future Internet Services, Sep. 2001.
- [40] C. Meyer and A. Partan, "BGP security, availability, and operator needs," Jun. 2003, nANOG 28.
- [41] D. M. Nicol, S. W. Smith, and M. Zhao, "Evaluation of efficient security for BGP route announcements using parallel simulation," *Simulation Modelling Practice and Theory*, vol. 12, no. 3-4, pp. 187–216, Jul. 2004.
- [42] R. White, "Deployment considerations for secure origin BGP (soBGP)," Oct. 2002, Internet Draft.
- [43] S. Kent, "Securing the Border Gateway Protocol: A status update." Torino, Italy: Seventh IFIP TC-6 TC-11 Conference on Communications and Multimedia Security, Oct. 2003.
- [44] C. Lonvick, "RADIUS attributes for soBGP support," Jan. 2003, Internet Draft.
- [45] S. Bellovin, "SBGP - Secure BGP," Jun. 2003, nANOG 28.
- [46] G. Goodell, W. Aiello, T. Griffin, J. Ioannidis, P. McDaniel, and A. Rubin, "Working around BGP: An incremental approach to improving security and accuracy of interdomain routing." San Diego, CA, USA: ISOC NDSS'03, Feb. 2003, pp. 75–85.
- [47] T. Dierks and C. Allen, "The TLS protocol version 1.0," Jan. 1999, rFC 2246.
- [48] B. Baker and R. Shostak, "Gossips and Telephones," *Discrete Mathematics*, no. 2, pp. 191–193, 1972.
- [49] R. Perlman, "Network layer Protocols with Byzantine Robustness," Ph.D. dissertation, Massachusetts Institute of Technology, Cambridge, MA, Oct. 1988, mIT/LCS/TR-429.
- [50] P. McDaniel, W. Aiello, K. Butler, and J. Ioannidis, "Origin authentication in interdomain routing," *Computer Networks*, vol. 50, no. 16, pp. 2953–2980, Nov. 2006.
- [51] R. Merkle, "Protocols for public key cryptosystems." Oakland, CA: IEEE Symposium on Research in Security and Privacy, Apr. 1980.
- [52] M. Naor and K. Nissim, "Certificate Revocation and Certificate Update," in *Proceedings of the 7th USENIX Security Symposium*, San Antonio TX USA, jan 1998, pp. 217 – 228.

- [53] Y.-C. Hu, A. Perrig, and M. Sirbu, “SPV: Secure Path Vector Routing for Securing BGP,” in *ACM SIGCOMM*. ACM, August 2004.
- [54] S. Even, O. Goldreich, and S. Micali, “On-Line/Off-Line Digital Signatures,” *Journal of Cryptology*, vol. 9, no. 1, pp. 35–67, 1996.
- [55] C. Wong and S. Lam, “Digital Signatures for Flows and Multicasts,” *IEEE/ACM Transactions on Networking*, vol. 7, no. 4, pp. 502–513, August 1999.
- [56] M. Zhao, S. W. Smith, and D. M. Nicol, “Aggregated path authentication for efficient BGP security,” in *Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS’05)*, Nov. 2005, alexandria, VA, USA.
- [57] —, “Evaluating the performance impact of PKI on BGP security,” in *Proceedings of the 4th Annual PKI R&D Workshop*, Feb. 2005, gaithersburg, MD, USA.
- [58] K. Butler, P. McDaniel, and W. Aiello, “Optimizing BGP Security by Exploiting Path Stability,” in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS’06)*, Alexandria, VA, USA, Nov. 2006.
- [59] B. Kumar and J. Crowcroft, “Integrating security in inter-domain routing protocols,” *ACM SIGCOMM Computer Communication Review*, vol. 23, no. 5, pp. 36–51, Oct. 1993.
- [60] ISO, “Intermediate System to Intermediate System Inter-Domain Routeing Information exchange protocol,” Jul. 1992, dIS 10747.
- [61] P. C. van Oorschot, T. Wang, and E. Kranakis, “On Inter-domain Routing Security and Pretty Secure BGP (psBGP),” *ACM Transactions on Information and System Security (TISSEC)*, 2007, To appear.
- [62] X. Zhao, D. Pei, L. Wang, D. Massey, A. Mankin, S. F. Wu, and L. Zhang, “An analysis of BGP multiple origin AS (MOAS) conflicts.” San Francisco, CA, USA: ACM SIGCOMM Internet Measurement Workshop, 2001, Nov. 2001.
- [63] R. Chandra, P. Traina, and T. Li, “BGP community attribute,” Aug. 1996, rFC 1997.
- [64] X. Zhao, D. Pei, L. Wang, D. Massey, A. Mankin, S. Wu, and L. Zhang, “Detection of invalid routing announcement in the Internet.” Washington DC, USA: IEEE DSN 2002, Jun. 2002.
- [65] L. Wang, X. Zhao, D. Pei, R. Bush, D. Massey, A. Mankin, S. Wu, and L. Zhang, “Protecting BGP routes to top level DNS servers,” vol. 14, no. 9, pp. 851–860, Sep. 2003.
- [66] C. Kruegel, D. Mutz, W. Robertson, and F. Valeur, “Topology-based detection of anomalous BGP messages,” in *Proceedings of the 6th Symposium on Recent Advances in Intrusion Detection (RAID)*, Sep. 2003, pp. 17–35.
- [67] M. Lad, D. Massey, D. Pei, Y. Wu, B. Zhang, and L. Zhang, “PHAS: A Prefix Hijack Alert System,” in *Proceedings of the 15th USENIX Security Symposium*, Aug. 2006, vancouver, BC, Canada.
- [68] X. Hu and Z. M. Mao, “Accurate Real-time Identification of IP Prefix Hijacking,” in *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA, USA, May 2007.
- [69] Y. Zhang, Z. Zhang, Z. M. Mao, Y. C. Hu, and B. M. Maggs, “On the Impact of Route Monitor Selection,” in *Proceedings of the ACM Internet Measurement Conference (IMC)*, San Diego, CA, USA, Oct. 2007.
- [70] L. Subramanian, V. Roth, I. Stoica, S. Shenker, and R. Katz, “Listen and Whisper: Security mechanisms for BGP.” San Francisco, CA, USA: First Symposium on Networked Systems Design and Implementation, Mar. 2004.
- [71] Y. Hu, A. Perrig, and D. Johnson, “Efficient security mechanisms for routing protocols.” San Diego, CA, USA: Internet Society Network and Distributed Systems Security 2003, Feb. 2003.
- [72] R. Rivest, A. Shamir, and L. M. Adelman, “A method for obtaining digital signatures and public-key cryptosystems,” vol. 21, no. 2, pp. 120–126, Feb. 1978.
- [73] J. Karlin, S. Forrest, and J. Rexford, “Pretty Good BGP: Improving BGP by Cautiously Adopting Routes,” in *Proceedings of IEEE ICNP 2006*, Santa Barbara, CA, USA, Nov. 2006.
- [74] R. Mahajan, D. Wetherall, and T. Anderson, “Understanding BGP misconfiguration.” Pittsburgh, PA, USA: ACM SIGCOMM 2002, Aug. 2002.
- [75] S. Bellovin and E. Gansner, “Using link cuts to attack Internet routing,” May 2003, draft: <http://www.cs.columbia.edu/smb/papers/reroute.pdf>.
- [76] G. Huston, “BGP AS number exhaustion,” Jun. 2003, nANOG 28.
- [77] —, “Commentary on inter-domain routing in the Internet,” Dec. 2001, rFC 3221.
- [78] S. Bellovin, R. Bush, T. Griffin, and J. Rexford, “Slowing routing table growth by filtering based on address allocation policies,” <http://www.cs.princeton.edu/jrex/papers/filter.pdf>, Jun. 2001.
- [79] T. Griffin and G. Wilfong, “An analysis of BGP convergence properties.” Cambridge, MA, USA: ACM SIGCOMM 1999, Sep. 1999.

- [80] C. Labovitz, A. Ahuja, R. Wattenhofer, and S. Venkatachary, "The impact of Internet policy and topology on delayed routing convergence." Anchorage, AK, USA: IEEE INFOCOM 2001, Apr. 2001.
- [81] H. Chan, D. Dash, A. Perrig, and H. Zhang, "Modeling Adoptability of Secure BGP Protocols," in *Proceedings of ACM SIGCOMM 2006*, Pisa, Italy, Sep. 2006.
- [82] L. Breslau, D. Estrin, K. Fall, S. Floyd, J. Heidemann, A. Helmy, P. Huang, S. McCanne, K. Varadhan, Y. Xu, and H. Yu, "Advances in Network Simulation," *IEEE Computer*, vol. 33, no. 5, pp. 59–67, May 2000.
- [83] J. Cowie, H. Liu, J. Liu, D. Nicol, and A. Ogielski, "Towards Realistic Million-Node Internet Simulations," in *Proceedings of the 1999 International Conference on Parallel and Distributed Processing Techniques and Applications (PTPTA'99)*, Las Vegas, NV, USA, Jun. 2000.
- [84] T. Benzel, R. Braden, D. Kim, C. Neuman, A. Joseph, K. Sklower, R. Ostrenga, and S. Schwab, "Experience with DETER: A Testbed for Security Research," in *Proceedings of the 2nd IEEE Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities (TridentCom 2006)*, Barcelona, Spain, Mar. 2006.
- [85] X. He and C. Papadopoulos, "A framework for incremental deployment strategies for router-assisted services." San Francisco, CA, USA: IEEE INFOCOM 2003, Apr. 2003.
- [86] J. Yu, "Scalable routing design principles," Jul. 2000, rFC 2791.
- [87] V. Stachos, M. Kounavis, and A. Campbell, "SPHERE: A binding model and middleware for routing protocols." Anchorage, AK, USA: Fourth Conference on Open Architecture and Network Programming (OPENARCH 2001), Apr. 2001.
- [88] D. Pei, D. Massey, and L. Zhang, "A framework for resilient Internet routing protocols," UCLA, Tech. Rep., Nov. 2003.
- [89] S. Gorman, R. Kulkarni, L. Schintler, and R. Stough, "Least effort strategies for cybersecurity," <http://arxiv.org/ftp/cond-mat/papers/0306/0306002.pdf>, 2003.
- [90] O. Nordström and C. Dovrolis, "Beware of BGP attacks," *Computer Communications Review*, vol. 34, no. 2, pp. 1–8, Apr. 2004.
- [91] M. Goodrich, "Efficient and secure network routing algorithms," Jan. 2001, provisional patent filing.
- [92] D. Boneh, C. Gentry, H. Shacham, and B. Lynn, "Aggregate and verifiably encrypted signatures from bilinear maps," vol. LNCS 2656. Eurocrypt 2003, 2003, pp. 416–432.
- [93] K. Zhang, "Efficient protocols for signing routing messages." San Diego, CA, USA: ISOC NDSS'98, Mar. 1998.
- [94] M. Bellare and S. Miner, "A forward-secure digital signature scheme," vol. LNCS 1666. Advances in Cryptology - CRYPTO '99 Proceedings, 1999, pp. 431–438.
- [95] E. Cronin, S. Jamin, T. Malkin, and P. McDaniel, "On the performance, feasibility, and use of forward-secure signatures." Washington, DC, USA: ACM CCS'03, Oct. 2003.
- [96] A. Chakrabarti and G. Manimaran, "An efficient algorithm for malicious update detection & recovery in distance vector protocols." Anchorage, AK, USA: IEEE Intl. Conf. on Communications, May 2003.
- [97] I. Avramopoulos, H. Kobayashi, R. Wang, and A. Krishnamurthy, "Highly secure and efficient routing." Hong Kong, PRC: IEEE INFOCOM 2004, Mar. 2004.
- [98] C. Labovitz, A. Ahuja, R. Wattenhofer, and S. Venkatachary, "Resilience characteristics of the Internet backbone routing infrastructure." Boston, MA: Third Information Survivability Workshop, 2000.
- [99] N. Feamster, D. Andersen, H. Balakrishnan, and M. Kaashoek, "Measuring the effects of Internet path faults on reactive routing." San Diego, CA, USA: ACM SIGMETRICS 2003, Jun. 2003.
- [100] V. Padmanabhan and D. Simon, "Secure traceroute to detect faulty or malicious routing." Princeton, NJ, USA: ACM SIGCOMM Workshop on Hot Topic in Networks (HotNets-I), Oct. 2002.
- [101] Z. Mao, J. Rexford, J. Wang, and R. Katz, "Towards an accurate AS-level traceroute tool." Karlsruhe, Germany: ACM SIGCOMM 2003, Aug. 2003.
- [102] R. Perlman, *Interconnections: Bridges, Routers, Switches, and Internetworking Protocols, 2nd Edition*. Reading, MA: Addison Wesley, 1999.
- [103] T. Bates, Y. Rekhter, R. Chandra, and K. D., "Multiprotocol extensions for BGP-4," Jun. 2000, rFC 2858.