Don't Secure Routing Protocols, Secure Data Delivery

Dan Wendlandt, Carnegie Mellon
Ioannis Avramopoulos, Princeton
David G. Andersen, Carnegie Mellon
Jennifer Rexford, Princeton

1 Introduction

Internet routing and forwarding are vulnerable to attacks and misconfigurations that compromise secure communications between end systems. With networks facing external attempts to compromise their routers [3] and insiders able to commandeer infrastructure, subversion of Internet communication is an ever more serious threat.

Much prior work has proposed to improve communication security with secure interdomain routing protocols (e.g., S-BGP [10] and so-BGP [12]). We argue that solving the problem of secure routing is both harder and less effective than directly solving the core problems needed to communicate securely: end-to-end confidentiality, integrity, and availability. Secure routing protocols focus on providing *origin authentication* and *path validity*, identified as necessary by the IETF to secure BGP [7]. Unfortunately, these properties are both too little and too much:

Secure routing is too little: As we discuss further in §2, secure routing does not completely address the core problems in secure communication. For example, it cannot prevent adversaries on the communication path from eavesdropping or modifying data traffic. Hosts must still use end-to-end cryptography to defend against these attacks. Similarly, secure routing cannot detect or prevent packet loss due to data-plane bugs, misconfigurations, or attacks.

Secure routing is too much: The mechanisms behind secure routing, both cryptographic and administrative, are painfully heavy-weight. They require router hardware upgrades for cryptographic processing, time-consuming maintenance of address registries, and a new public key infrastructure (PKI).

Recognizing that a secure version of BGP will be difficult to deploy, yet provide only limited protection, we ask: what is the best division of labor between end systems (end hosts, or edge routers acting on behalf of end hosts) and the routing infrastructure to provide secure, robust communication? The answer, we argue, is that the routing infrastructure must only provide *availability*, i.e., enable an end system to find a working path to the valid destination as long as such a path exists. End systems can provide confidentiality and integrity as needed.

Following this model, we present Availability Centric Routing (ACR), which is based on three principles:

1. End systems learn multiple paths to a destination.
2. End systems monitor end-to-end integrity and path performance to determine if a path is working.
3. End systems can change paths to find one that works.

By propagating multiple paths per destination instead of one "best path," ACR thwarts an adversary's attempt to prevent a source from hearing a valid path to a destination. Taken together, ACR has several interesting advantages over traditional secure routing schemes:

- Using alternate paths can circumvent data-plane availability threats, such as malicious drops, misconfigured ACLs, link DoS, and transient routing issues.
- Significant gains in resilience are achieved even if only a few interested domains cooperate.
- Adoption is simplified because no address registry, AS-level PKI, or router cryptography is required.
- Performance, usually at odds with security, also benefits from path diversity.

ACR achieves robustness by treating learned routes as possibilities, not certainties. With this approach, control-plane security (e.g., S-BGP) is an *optimization* to help ACR find valid paths quickly by avoiding spurious routes, rather than a requirement for communication security.

2 Threat Model

Reliable Internet communication can be impaired by attackers who compromise routers or by link DoS, failures, bugs, and misconfigurations. In a traditional threat model, attackers can tamper with data or impersonate identities (violate integrity), snoop on traffic (violate confidentiality), or deny service (reduce availability). In this section, we first examine why only the last of these threats—availability—requires support from the routing infrastructure. We then examine in more detail the ways an attacker might attempt to deny availability.

Integrity can be provided end-to-end using well-known cryptographic techniques (Message Authentication Codes) along with shared secret or public key authentication schemes. Data **confidentiality** is similarly easy to protect using encryption. This leaves **availability** as the remaining threat. Unfortunately, cryptography cannot get packets across a path that drops or misdirects all traffic.

Control of a router, legitimate or illegitimate, grants

significant power to compromise communication security in both the control and data planes.

Control Plane: An attacker can influence the *global* flow of traffic by falsifying BGP routing information. By announcing a victim's IP prefix or manipulating the AS path, an adversary can draw traffic to its own routers, where it can observe, modify, or drop data and impersonate the destination. An attacker can also prevent a portion of the Internet from hearing the valid route announcement, "black-holing" traffic to the victim. We term the use BGP route announcements to maliciously attract traffic a "control-plane" attack. Secure BGP proposals impede, but do not prevent, attackers from mounting such attacks by providing *origin authentication* and *path validity*. [1]

Data Plane: Despite reducing an attacker's ability to attract traffic, a secure control plane cannot prevent malicious routers or insiders that manage to be on a legitimate communication path from observing, modifying, or misdirecting traffic. Nor does control-plane security protect against link DoS, or misconfigured packet filters. We term these threats "data-plane" attacks. Data plane attacks are particularly troublesome because BGP (secure or not) will not switch away from a "best path" even if it becomes effectively useless for a particular application.

Because control-plane security must still be augmented with end-to-end techniques to guarantee integrity and confidentiality, we argue that *the only property that the control plane must provide is availability*; that is, it must guarantee that a sender will hear about a valid path to the destination if one exists. The control plane *may* provide information regarding what AS paths are likely to be legitimate, but this information is not a requirement for communication security.

A more subtle threat to confidentiality is traffic analysis, which gleans information simply by observing the pattern of communication between hosts even when data is encrypted. Fortunately, traffic analysis is more difficult than simply black-holing traffic, because it requires that the attacker not only be able to intercept traffic, but also to re-inject it to the correct destination. We suspect, but leave for future work, that the use of path selection heuristics as described in §3.4 will make traffic analysis difficult for all but the most well-connected ISPs. In the case of either ACR or a secure BGP, senders in need of strong protection against traffic analysis are best served by techniques like mixnets[6].

A final threat comes from attackers who advertise unallocated or unused address space, as is sometimes done by spammers to avoid IP address blacklists [14]. We do not consider preventing these announcements to be a central requirement for robust routing, because they do not undermine communication security and are only weakly related to the fundamental economic incentives that fuel the spam problem.

[1]For example, secure BGP cannot prevent announcements that attract traffic by violating BGP policy, such as a customer redistributing routes heard from one provider to another.

3 AVAILABILITY CENTRIC ROUTING

The goal of *availability-centric routing* is to enable end systems to communicate securely even if portions of the network infrastructure are controlled by an adversary. ACR uses four components. First, one or more transit ASes act as *availability providers* (APs) that provide the edge with multiple routes for each destination. Second, sources using ACR cryptographically verify the identity of the destination host or network, to confirm that the chosen route reaches the correct destination. Third, ACR end systems securely monitor communication performance; if performance is too poor, for whatever reason (a situation-specific definition), they signal ACR to use a different path. Fourth, the ACR end systems distribute traffic over one or more paths supplied by the AP by applying selection algorithms that quickly identify working paths with high probability.

3.1 Multipath via Availability Providers

To provide path choice in a legacy, single-path BGP environment, ACR includes mechanisms to advertise multiple paths for a single destination and then direct traffic onto these alternate paths. This approach is akin to proposed multipath schemes like MIRO [18]. Availability providers give the network edge access to multiple paths via a (presumably paid) AS-level *deflection service*. End systems can avoid failures by redirecting traffic to different paths.

An availability provider maintains a *route repository* containing all routes learned from BGP peering sessions with neighboring ASes. The repository may be populated by passive BGP sniffers at peering links, or by a BGP monitoring protocol. Customers can request routes on demand from their AP (e.g., if their current path is not working), or subscribe to a feed of paths to particular destinations using either a custom protocol (future work) or the proposed *add-paths* extension to BGP [17].

Sources use alternate paths by tunneling packets using IP encapsulation (e.g., L2TPv3 [11]) to *deflection points* in the AP's network. Paths from the route repository include the deflection point IP address, the encapsulation method to use, and a *deflection forwarding identifier*. This tunneling can be performed at line rate by high-end routers [8] and enables decapsulated packets to circumvent normal BGP routing using directed forwarding. Directed Forwarding uses an alternate forwarding table to route packets based on the deflection forwarding identifier included in the encapsulation header. After decapsulation and directed forwarding, subsequent routers forward the packet normally. Access to the deflection ser-

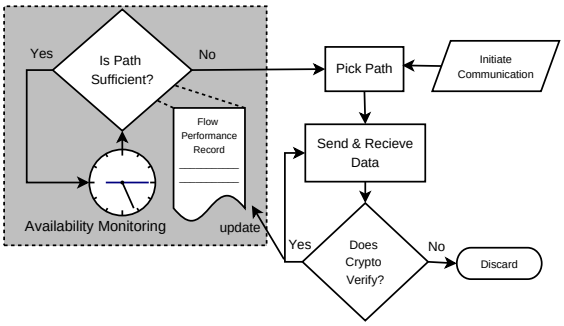

Figure 1: Control-flow of "availability monitoring" in ACR.

vice can be efficiently controlled by light-weight authentication "cookies" such as those found in L2TPv3.

3.2 End-to-End Integrity Check

To work, a path must connect the source to the *correct* destination. ACR allows end systems to authenticate destinations in whatever way they choose, from generic mechanisms such as IPsec or SSL to application-specific approaches like DNSSEC.[2] Many important protocols, including HTTP, SMTP, SSH, and SIP, already support both client and server authentication, and we argue that the majority of important Internet communication *already occurs over secure channels like SSL or IPsec*. Importantly, ACR does not require that all hosts and/or routers participate in a PKI. For example, with HTTPS, clients commonly present no authentication credentials to the server at all, and instead dynamically establish a secret used to verify the integrity of all further packets.

3.3 Availability Monitoring

Detecting availability attacks requires the ability to monitor a network flow and determine if the current path is a usable route.

In the context of Figure 1, consider a general-purpose availability monitor within the TCP stack of an end host using IPSec for end-to-end security. A call to *connect()* causes the path-selection component to select an initial route. TCP sends a SYN packet and sets its retransmission timer. If the timer expires before the SYN/ACK comes back, the monitor records the event and *may* change to an alternate path before retransmitting. Similar monitoring occurs for all data transfered. With TCP, the "flow performance record" consists primarily of state the protocol already keeps to manage reliable delivery, but could be augmented with retransmission or timeout counters to track recent path performance. This record must be reset each time a new path is selected, but no TCP-specific behavior or state is modified. Received packets are verified for integrity using IPsec and are discarded if the check fails, so that paths with adversaries manipulating packets will cause time-outs that result in a path switch.

While this example monitor is simple and general, ACR can work with any type of availability monitoring the edge chooses to employ. In particular, edge routers could use monitoring schemes similar in spirit to Listen [16] or Stealth Probing [4] to detect and switch away from bad paths *on behalf of clients*. Alternately, applications like VOIP clients that already incorporate protocol-specific monitoring could use this information to signal a desire for a different path.

3.4 Path Selection Algorithms

Path selection algorithms should quickly locate working routes, to minimize the time to recover from failures or attacks. These algorithms are triggered by the availability monitors when failures are detected (Figure 1). Path selection algorithms can combine topological information (e.g., AS-paths from insecure BGP) with external knowledge (e.g., known AS connectivity or history of good routes) to select candidate paths. ACR treats this information as *hints*, not truth, because the information may be stale or inaccurate depending on its source. Path selection could explore several paths in parallel to further reduce recovery time at the expense of additional bandwidth. Selection can be assisted by heuristics such as:

Static destination connectivity hints: Destinations that care about availability are likely to know their upstream connectivity. ACR can use this knowledge to give the edge "hints" to quickly identify promising paths. BGP paths that are inconsistent with the connectivity hint from the destination receive lower priority in the path exploration process. Because their consistency is not critical (they affect only priority) static hints can be distributed ahead of time, out-of-band, or via replicated repositories.

Route stability heuristics: Many Internet routes, particularly those to popular destinations, are quite stable [15]. ACR could take advantage historical route information to identify good paths more quickly. Unlike schemes that discard routes that fail historical tests, and so require exceptionally low "false-positive" rates, ACR will still use "anomalous" routes if (and only if) they work correctly end-to-end.

Path ranking and selection can be handled by an end host, an edge router, or even the AP to simplify the functionality at the edge network.

4 ACR WITH LIMITED DEPLOYMENT

In the long term, we envision ACR being used with a globally deployed multipath protocol like MIRO[18]. Yet we demonstrate in §5 that deployment by even a single tier-1 ISP provides customer ASes significant availability improvements in the face of routing attacks.

However, "legacy providers" still running single-path BGP complicate the limited deployment scenario. For

[2] Note that because encryption is not required for integrity, it is needed only if the application requires confidentiality.

example, if a destination D has only a single (legacy) provider P, and P believes and propagates a false route for D, no availability provider would be able to reach D. Therefore, ACR, when deployed at limited locations, requires additional light-weight control-plane countermeasures (simple BGP filters, see §5) to prevent such control-plane availability attacks. Before evaluating the resilience of limited ACR deployment we cover two issues related to using ACR in a legacy environment.

Resisting sub-prefix hijacks: With BGP, an attacker can announce a sub-prefix more specific than a legitimate advertisement. This attack is highly effective because the sub-prefix propagates to all ASes and all routers will forward traffic to the more specific sub-prefix. In ACR, if a destination D is not directly connected to its AP, packets sent by the AP to D via a legacy provider P may be misdirected to an attacker if P believes the attacker's sub-prefix.

To counter this attack, a sequence of legacy providers between D and the AP must not believe the attacker's sub-prefix. ACR ensures this by emulating "flat addressing" using /24's, which is the longest prefix most ISPs will accept (i.e., it cannot be sub-prefix hijacked). In the example above, D can announce its prefixes as /24's to P, so that P will not divert packets. P can safely aggregate the /24's before announcing them to peers or customers, and must announce the longer-prefixes only to one upstream provider. This chain terminates at a tier-1 provider, who is directly connected to other AP's and thus assures that there is a complete path from any AP to D that cannot be sub-prefix hijacked. Effectively, upstream providers accept a moderate increase in routing table size to increase availability for their customers, while the global routing table size remains unaffected.[3]

CIDR addressing, the root cause of sub-prefix hijacks, is also troublesome for other proposals for secure routing. For example, sub-prefixes in forwarding tables can lead to discrepancies between control and forwarding plane paths, lessening the benefit of a verified BGP AS-Path. Similarly, prefix aggregation significantly complicates origin authentication. While we propose an incremental measure for dealing with CIDR above, ultimately we feel that a more sound architectural choice is to move toward a flat addressing model for the Internet.

Resisting deflection point hijacks: A BGP hijack could also block a subscriber from reaching its AP's deflection points if the subscriber's direct upstream provider did not support ACR.[4] Fortunately, the number of deflection point prefixes would be quite small, and they are found within stably connected core networks. These properties facilitate "defensive filters" that explicitly deny route announcements for special destinations on all but a few peering sessions.

[3] We have heard from operators that announcing smaller subnets into the global routing table to resist sub-prefix attacks is not uncommon today. ACR offers similar protection but without polluting global tables.

[4] This customer would have an incentive to switch to an ACR-speaking ISP, but we also believe that customers can benefit from using a "remote" (i.e., non-first-hop) availability provider (§6).

5 EVALUATION

We explore the effectiveness of ACR and its countermeasures in the context of today's Internet. In our evaluation, each path may contain at most one deflection point and only a few ASes offer deflections. Our experiments examine ACR's performance against an attacker who announces an IP prefix that belongs to a victim network.

Method: We run simulations on an AS-level graph based on July 2006 RouteViews data with AS relationships inferred using Gao's algorithm [9]. The route selection policy prefers customer-learned routes over peer-learned routes, and prefers provider-learned routes the least, with ties broken using AS-Path length. Each trial has one legitimate AS and a set of attacking ASes that all announce the same prefix. We vary the number of malicious ASes, performing 100 trials for each configuration.

Result 1: A single tier-1 availability provider significantly increases routing robustness compared to stubs using either single-path BGP or intelligent multi-homing. Figure 2 charts the average reachability of the legitimate destinations versus the number of attacking ASes. The bottom line (Single-Path BGP) shows the average success rate of all stub ASes in reaching the destination using normal BGP. We simulate intelligent multihoming by testing all stub ASes with exactly five providers to see if any of their five BGP-learned routes are valid.[5] The availability providers for the Tier-1 AP data include all ten ISPs commonly thought to not purchase transit from another ISP, and makes the reasonable assumption that these ISPs offer deflections on all BGP-learned paths. The results indicate the average success rate for these any end system that is able to use just one of the tier-1 APs.

While intelligent multihoming sources can select from multiple paths, *only a tier-1 availability provider exposing multiple BGP-learned paths to the same destination provides strong resilience to hijacks*. ACR works so well because topology and the common BGP policy of preferring customer-learned routes forces an attacker to be "local" (a customer of all of a destination's providers) to prevent the AP from hearing a legitimate announcement.

Result 2: ACR's availability benefits can be further improved using easily-deployed BGP filtering local to the victim. As shown in Figure 2, adversaries are sometimes assigned to local ASes, reducing the Tier-1 AP success rate to 95% with many attackers (e.g., second from

[5] A selection intended to capture stubs that have invested significantly in network availability.

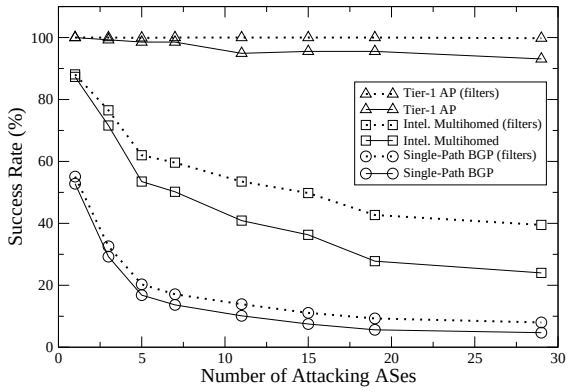

Figure 2: Success rate of sources reaching a hijacked destination when using different degrees of path diversity.

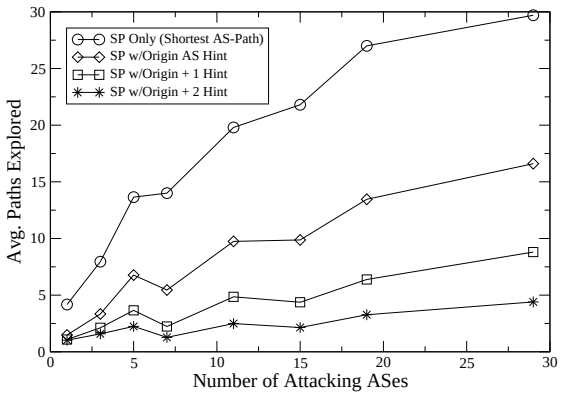

Figure 3: Number of routes explored before finding a valid forwarding path.

top line, far right). To defeat these adversaries, legacy ISPs can employ a tactic already common among large providers today: filtering routes from customers to accept only prefixes that the customers own and have registered. As a result, these filters block malicious advertisements by other customers. Unlike filtering to protect the legacy BGP system (which must be performed globally), these filters need only be applied locally by some of the valid destination's transit providers. The results of applying such filtering at the ISPs between the tier-1 AP and the destination are shown by the "filters" lines. The results show that *filters provide complete protection with a tier-1 AP, but provide only incremental benefit for intelligent multi-homing or single-path BGP*.

Result 3: The time to find a valid route is reasonable in the face of many adversaries, and simple connectivity hints from the destination further speed the process. Figure 3 shows the average number of paths a source must explore, averaged over all Tier-1 APs, without the benefits of destination filtering. The *Origin AS Hint* case assumes that the source knows the correct AS originating the prefix being probed, while *Origin + x Hint* indicates knowledge of all upstream providers up to x hops from the origin (see §3.4). Note that by not incorporating historical knowledge of working routes this analysis represents a scenario significantly more challenging than the likely common case.

Without external topology information, ACR explores paths based only on their AS-path length. ACR must test a few paths per attacker before finding a working path, which we feel is not unreasonable. However, guiding path selection with some prior knowledge of topology is more efficient, requiring probing only a few paths even for large numbers of attackers. The topology hints force an adversary to pad its AS path to include the correct topology, which makes the path longer and less attractive to the shortest AS-path heuristic. Using these heuristics, ACR helps reduce outages to short "hiccups" in connectivity experienced while it explores new paths.

6 DEPLOYABILITY

ACR emphasizes low barriers to adoption: ACR simplifies deployment because it does not require cryptographic hardware in routers and because the functionality needed for path deflections is already widely available. Robustness for applications already using SSL or IPSec could be deployed immediately, with no dependence on an AS-level PKI and address ownership registries.

ACR benefits from backward compatibility: Changing a critical part of the Internet infrastructure raises stability and reliability concerns. Because ACR runs alongside BGP, not as a replacement, operators can evaluate it on operational networks without the need for a parallel test infrastructure. Additionally, failures within ACR are isolated from BGP. As a result, unlike many secure replacements for BGP, legitimate use or misconfiguration of ACR is unlikely to result in worse reachability than is provided by legacy BGP, because the single-path legacy BGP route is still available for use.

ACR provides well-incentivized deployment: We envision deflection services being offered in two ways. First, core networks can offer deflections to their directly-connected transit customers. This could give an ISP a competitive advantage: customers will receive improved resilience against attacks and gain the ability to select paths that perform better.

The second deployment scenario is to offer a remote deflection service to ASes that are not direct transit customers. This service would enable customers of legacy ISPs to gain many of ACR's benefits. This remote deflection service is more technically challenging to offer, but as §5 showed, even deployment by a single large ISP can provide greatly improved attack resilience. An AP can offer remote deflection service more cheaply than normal transit service because (1) availability customers do not need a physical router port and (2) a tier-1 AP also re-

ceives more overall transit revenue because of increased traffic entering its network for deflections. As a result, stubs with both types of providers need not be "double-charged" for their connectivity.

7 Related Work

ACR is similar in spirit to seminal work performed by Perlman [13]. Secure routing has been pursued extensively in academia and industry; due to space constraints, we refer the interested reader to a recent survey of BGP security research [5]. ACR's path selection can benefit from secure routing protocols, but remains effective without them.

Popular current approaches for robust routing use overlay networks [2] or multi-home the edge [1]. While these techniques improve availability against many failures, we know of no studies that examine their resilience to deliberate routing attacks. Our evaluation suggests that they cannot withstand powerful adversaries that use BGP to globally disrupt routes to a destination.

Many clean-slate source-routing architectures either do not address security (e.g., NIRA [19]), or conflict with operational practices (e.g., feedback based routing [21]) by requiring the disclosure of routing policies often guarded today by non-disclosure agreements.

Recent work on router-level deflections [20] offers a complementary technique that provides finer-grained path diversity, but with less source control over how packets are deflected; ACR could leverage such techniques to help avoid adversaries within an AS.

8 Conclusion

ACR demonstrates that communication security can be achieved *without* securing the routing protocols. Because properties such as confidentiality and integrity can, and often already are, provided end-to-end by applications requiring strong security, this paper argues that availability is the only property that the routing system must provide. Availability, we believe, is better achieved by lightweight, incentive-compatible mechanisms to expose multiple paths to the network edge than by heavyweight secure routing techniques.

By recognizing that many applications today already require and use end-to-end security, ACR presents a novel and compelling point in the routing security design space. ACR demonstrates that robust routing and forwarding are in fact achievable given building blocks already common on the Internet today, and that the adoption of these mechanisms can occur in a well-incentivized and incremental way. Because ACR also provides strong protection from data-plane adversaries and failures, we believe its principles are a worthwhile addition to the routing security toolbox, regardless of whether a secure version of BGP is eventually deployed.

Acknowledgments

The Dept. of Homeland Security helped to fund this work with HSARPA grant 1756303 and a graduate fellowship for Dan Wendlandt. Special thanks to Adrian Perrig, Nick Feamster, our anonymous reviewers, and many others whose comments greatly improved this work.

References

[1] A. Akella, J. Pang, B. Maggs, S. Seshan, and A. Shaikh. A comparison of overlay routing and multihoming route control. In *Proc. ACM SIGCOMM*, Aug. 2004.

[2] D. G. Andersen, H. Balakrishnan, M. F. Kaashoek, and R. Morris. Resilient Overlay Networks. In *Proc. 18th ACM Symposium on Operating Systems Principles (SOSP)*, pages 131–145, Oct. 2001.

[3] Arbor Networks. Arbor networks: Infrastructure security survey. http://www.arbornetworks.com/sp_security_report.php, 2006.

[4] I. Avramopoulos and J. Rexford. Stealth probing: Efficient data-plane security for IP routing. In *Proc. USENIX Annual Technical Conference*, May/June 2006.

[5] K. Butler, T. Farley, P. McDaniel, and J. Rexford. A survey of BGP security. Technical Report TD-5UGJ33, AT&T Labs, June 2004.

[6] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Comm. of the ACM*, 4(2), February 1981.

[7] B. Christian and T. Tauber. *BGP Security Requirements*. IETF, Apr. 2006. Internet Draft: draft-ietf-rpsec-bgpsecrec-06.txt.

[8] P. Francios and O. Bonaventure. An evaluation of IP-based fast reroute techniques. In *Proc. CoNEXT'05*, 2005.

[9] L. Gao. On inferring autonomous system relationships in the Internet. *IEEE/ACM Trans. Netw.*, 9(6):733–745, 2001.

[10] S. Kent, C. Lynn, and K. Seo. Secure border gateway protocol (S-BGP). *IEEE JSAC*, 18(4):582–592, Apr. 2000.

[11] J. Lau, M. Townsley, and I. Goyret. Layer two tunneling protocol - version 3 (L2TPv3). RFC 3931, IETF, Mar. 2005.

[12] J. Ng. *Extensions to BGP to Support Secure Origin BGP (soBGP)*. IETF, Apr. 2004. Internet Draft: draft-ng-sobgp-extensions-02.txt.

[13] R. Perlman. Network layer protocols with byzantine robustness. Technical Report TR-429, MIT LCS, Oct. 1988.

[14] A. Ramachandran and N. Feamster. Understanding the Network-Level Behavior of Spammers. In *Proc. ACM SIGCOMM*, 2006.

[15] J. Rexford, J. Wang, Z. Xiao, and Y. Zhang. BGP routing stability of popular destinations. In *Proc. ACM SIGCOMM Internet Measurement Workshop*, Nov. 2002.

[16] L. Subramanian, V. Roth, I. Stoica, S. Shenker, and R. Katz. Listen and Whisper: Security mechanisms for BGP. In *Proc. Symposium on Networked System Design and Implementation*, Mar. 2004.

[17] D. Walton, A. Retana, and E. Chen. *Advertisement of Multiple Paths in BGP*. IETF. Internet Draft: draft-walton-bgp-add-paths-05.txt, Expired August 2006.

[18] W. Xu and J. Rexford. MIRO: Multi-path interdomain routing. In *Proc. ACM SIGCOMM*, Sep. 2006.

[19] X. Yang. NIRA: A New Internet Routing Architecture. In *ACM SIGCOMM Workshop on Future Directions in Network Architecture*, Aug. 2003.

[20] X. Yang, D. Wetherall, and T. Anderson. Source selectable path diversity via routing deflections. In *Proc. ACM SIGCOMM*, 2006.

[21] D. Zhu, M. Gritter, and D. Cheriton. Feedback based routing. In *Proc. HotNets-I*, Oct. 2002.