(R)Evolutionary Bootstrapping of a Global PKI for Securing BGP

Yih-Chun Hu, UIUC
David McGrew, Cisco Systems
Adrian Perrig, CMU / CyLab
Brian Weis, Cisco Systems
Dan Wendlandt, CMU / CyLab

ABSTRACT

Most secure routing proposals require the existence of a global public-key infrastructure (PKI) to bind a public/private key-pair to a prefix, in order to authenticate route originations of that prefix. A major difficulty in secure routing deployment is the mutual dependency between the routing protocol and the establishment of a globally trusted PKI for prefixes and ASes: cryptographic mechanisms used to authenticate BGP Update messages require a PKI, but without a secure routing infrastructure in place, Internet registries and ISPs have little motivation to invest in the development and deployment of this PKI.

This paper proposes a radically different mechanism to resolve this dilemma: an evolutionary Grassroots-PKI that bootstraps by letting any routing entity announce self-signed certificates to claim their address space. Despite the simple optimistic security of this initial stage, we demonstrate how a Grassroots-PKI provides ASes with strong incentives to evolve the infrastructure into a full top-down hierarchical PKI, as proposed in secure routing protocols like S-BGP. Central to the Grassroots-PKI concept is an attack recovery mechanism that by its very nature moves the system closer to a global PKI. This admittedly controversial proposal offers a rapid and incentive-compatible approach to achieving a global routing PKI.

1 INTRODUCTION

The Border Gateway Protocol (BGP) is deployed as the main interdomain routing protocol of the Internet. As described by RFC 1771 all routers in all Autonomous Systems (ASes) are trusted. However, as the Internet has grown, this ubiquitous trust assumption has been proven problematic. For example, in the "AS 7007 incident" one ISP announced short paths to all destinations [10] which caused a wide-spread outage of network connectivity. Clearly, given the importance of the Internet today, we need a more secure routing infrastructure to prevent a single ISP from being able to cause global damage.

Researchers have proposed several protocols to secure BGP [3, 6, 8, 15]. Most of these protocols require that routers authenticate the owner of a network prefix. For example, S-BGP proposes to authenticate prefixes using a PKI that is rooted at IANA [8], as Figure 1 shows.[1] The idea is that IANA is the trusted root of the PKI, and that all participants use IANA's public key to authenticate other certificates regarding prefix ownership. When IANA delegates IP address space to ARIN, it issues a certificate signing ARIN's public key and the IP address space, which indicates that ARIN can rightfully use and delegate those address blocks. Similarly, ARIN will sign AT&T's public key and address space delegation, etc. Some secure routing protocols also need certificates for each AS, which can be achieved through another PKI rooted at IANA, but with certificates binding an AS number to a public key. In this paper, we focus on creating a PKI for verifying route originations, which prevents route hijacks, the most prevalent type of routing attack and misconfiguration on the Internet today. While not discussed in detail, creating a PKI to bind public keys to ASes can benefit from the same "grassroots" approach advocated in this paper.

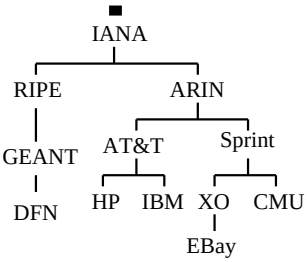

Figure 1: Example prefix PKI structure proposed by S-BGP. IANA is the sole trust root, and each entity in the figure signs the certificate of the entities connected to them from a lower level of the hierarchy. This process mirrors the delegation of IP address space.

S-BGP and soBGP [14] both require a global PKI for AS numbers and prefix ownership in order to provide security guarantees. While S-BGP proposes a PKI with a single root at IANA, soBGP also considers a scenario where a root of trust is formed by large ISPs signing and trusting each other's certificates. The more recent SPV protocol [6] simplifies the PKI requirement slightly by not requiring per-AS certificates, but still needs a global IP address space PKI to authenticate routing announcements.

Unfortunately, setting up such a global PKI is challenging. It requires a significant up-front investment by parties like IANA to manage the private keys, organize outdated and incomplete registries, and issue certificates to ASes. Secondly, all participants need to agree upon and trust a particular root certificate authority (CA); creating a significant point of contention that can stall adoption.

[1] IANA is empowered to allocate address space, but they contract the actual task to ICANN. Thus, while we assume IANA as the logical root of the PKI, this task may well be delegated to another entity.

While these requirements are by no means insurmountable, centralized entities like IANA face little pressure from ISPs to make progress, because no secure routing protocol that requires these certificates has been deployed. This highlights the mutual dependence between the adoption of a new secure routing protocol and the existence of a routing PKI. Stated another way, an AS currently has little demand for an IANA-signed address space certificate, because other ASes do not currently run a routing protocol that chooses routes based on these certificates. Yet operators will not adopt and deploy software for a secure routing protocol if its security benefits depend entirely on a non-existent PKI.

We propose *evolutionary incremental deployment* as a revolutionary approach to bootstrap a secure routing protocol: initially, prefix owners generate and use self-signed certificates, completely without the need for a centralized PKI. As adoption increases, more trusted parties (e.g., tier-1 ISPs) can sign these certificates to resolve any conflicts and provide added robustness for participants, still without requiring the involvement of centralized registries. Finally, driven by a desire to reduce the risk of having distributed points of trust, the system may reach the point where demand for centralized authentication motivates action by actors such as IANA.

In this paper, we study how to overcome this interdependence problem and the lack of incentives for networks to deploy secure routing. We suggest a Grassroots-PKI: an evolutionary approach to deploy a global routing PKI that will enable the deployment of a secure routing protocol. Our goal is to provide a viable deployment path from no security in routing to a highly secure routing infrastructure. We consider the three transitions from no deployment to small deployment, from small deployment to large-scale deployment, and from large-scale deployment to global deployment.

To achieve a viable deployment strategy, we need to provide incentives for ISPs and network administrators to follow each transition. Clearly, the evolutionary approach does not provide as much security as an immediate global deployment of secure routing. However, the evolutionary approach significantly reduces deployment barriers and is strictly better than the absence of routing security. Our approach provides improved security for some networks and worse security for none. If this scheme delayed the adoption of a global secure routing PKI, one could argue that it was detrimental to the greater good. However, quite the opposite is true: the grassroots PKI is specifically designed to hasten the advent of global routing security, by providing powerful incentives to participate in a routing PKI. Specifically, we provide extremely low barriers to joining the PKI, by letting any prefix-owner announce a key. Additionally, we design the deployment path such that when an attacker illegitimately originates a route, the recovery process inevitably moves the routing infrastructure toward a secure global PKI hierarchy. We feel this approach is promising, as it drives a network to be as secure as it needs to be.

2 RELATED WORK

Mechanisms to Authenticate Public Keys:

The most common PKI in use today is managed by corporate CA's like Verisign, who issue public key certificates used by servers for SSL/TLS-enabled protocols like HTTPS. With HTTPS the browser authenticates the server by verifying that the server's public-key is signed by the key of a "trusted root CA". However, due to the large number of online entities that must be verified and cost constraints, CAs can traditionally perform only lightweight identity checks before issuing certificates. In fact, there exists a known case where a hacker obtained a certificate signed for Microsoft [1]. Additionally, because of a focus on usability over security, current web browsers contain root key certificates from over 30 different CA's. Having a large root of trust weakens the security of the overall system, because an attacker that compromises a single CA can forge any web site. This demonstrates that while having many different trust roots eases usability and adoption, it lacks the strong security desirable in a full routing PKI.

More flexible and inexpensive mechanisms for establishing trust without a centralized authority also exist today. The web of trust in pretty-good privacy (PGP) authenticate public keys based on a graph of mutual trust relationships [16]. Unfortunately, the security of such trust paths quickly deteriorates even for extremely small numbers of links [12]. Alternately, the SSH protocol supports a "leap-of-faith" authentication model, in which users accept an unauthenticated key upon first connecting to a server, and use this key to verify all subsequent connections. While it offers no security for the first connection, further communication enjoys significantly improved security and the simplicity of this model is widely recognized as a reason SSH saw quick and widespread adoption.

A grassroots PKI will require the ability to merge separate smaller PKIs into a single larger PKI. One of the largest efforts to build a PKI with many administrative entities was the Automotive Network Exchange (ANX) [11]. A central goal of ANX was to bridge trust between the PKIs of the member sites. For the member sites to communicate securely, various ISPs also needed to participate in the PKI. For various reasons, ANX did not fully deploy. One of these reasons seems to be the difficulty in setting up the trust between all of the members simultaneously.

Finally, similar to BGP, securing DNS exhibits a dependency on PKI deployment, because DNSSEC requires a hierarchical PKI mirroring domain name delegation in order to authenticate DNS records. Top-level domains (TLDs) like .com need to publish public keys and sign certificates for sub-domains before that sub-domain can

provide secure DNS responses. To circumvent this dependency, a recent proposal called DNSSEC Lookaside Validation (DLV) [13] permits domain keys to be signed by non-TLD "trust anchors" prior to the existence of a full PKI.

PKIs for Secure Routing:

S-BGP proposes a single PKI root at IANA and a structure that mirrors address delegation. It allows for incremental deployment, but accepts a path as "secure" only if the prefix ownership and AS-path can be completely verified. This requires each AS in the AS-path to have an IANA-rooted certificate before a particular announcement is considered secure. Therefore, S-BGP does not allow for incremental deployment of the authentication infrastructure.

The soBGP effort proposes a PKI that is incremental by nature, where a PKI is generated based on which entities participate and whom the participants choose to trust. However, it recommends no particular structure for that PKI, nor does it provide a design specifically aimed at incentivizing participation in the PKI.

The SPV protocol suggests leveraging identity-based cryptography (IBC) [2] to simplify certificate distribution. SPV uses the prefix as a public key, requiring the prefix owner to contact a root CA to obtain the corresponding private key.[2] However, before any routing information can be authenticated, SPV still requires that all participants trust the global CA, that the CA can identify the legitimate owners of each prefix, and that all participants possess the CA's public key.

3 A Step-wise Approach for Bootstrapping a Routing PKI

Establishing a large PKI for the 20,000+ organizations involved in BGP routing is a daunting challenge, even when compared to initiatives like ANX (mentioned in Section 2) which have struggled with deployment. Moreover, the heterogeneity of entities in the Internet is significant, as ISPs span continents, languages, political ideologies, and cultures and no single entity can mandate a solution. These impediments suggest that the establishment of a PKI will not occur overnight and that individual actors must have strong economic incentives to overcome these barriers to participation. An evolutionary approach to building a global PKI can minimize these hurdles while still achieving strong security as an end result.

In this section, we present a multi-phased, evolutionary approach for establishing a global PKI. We start out assuming an Internet with mutually distrusting entities, with the goal of achieving a global PKI that enables any participant to authenticate any prefix.[3] We suggest two intermediate steps en-route to a full PKI: first, independent simple PKIs based on self-signed certificates; and second, small hierarchies of independent complex PKIs that certify their customers. For each case, we discuss how to reduce the associated security risks while simultaneously providing incentives for adoption. At each step, ASes have strong economic motivation to participate and any successful attacks will automatically drive the infrastructure toward a global PKI. Thus, our evolutionary approach begins with scattered trust points, and culminates in a global PKI with universal trust. Though we share the same final goal as previous routing PKI proposals, this bottom-up approach can greatly accelerate the process.

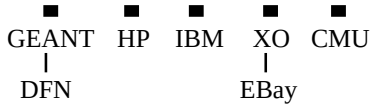

Figure 2: The flat distribution of trust with self-signed certificates. The top five entities are trust roots with self-signed certs, while DFN and EBay has certificates signed by their ISP's self-signed certificate.

3.1 Self-signed Prefix Certificates

The administrative entities controlling authorization (i.e., the Regional Internet Registries (RIRs) or large ISPs) may or may not initially participate in a secure routing PKI. Even if they do, the chain of trust extending from these entities may not follow the existing address authorization infrastructure, because it is likely that some ASes lower in the hierarchy will want to adopt even though entities above them in the delegation chain are not yet participating. Therefore, the PKI for a secure BGP routing infrastructure should be prepared to begin simply, for example, by dealing with several trust roots [9].

We propose a grassroots-PKI, where *anyone* can start disseminating a self-signed certificate for a prefix, drastically lowering the complexity and cost of participation. With no verification process required to claim a prefix, this revolutionary approach has seemingly severe security failures. However, this initially loose structure can rapidly transition to a high-security global PKI because any attack makes the network *more* secure as a result—thus, malicious actors are placed in a quandary where *the best attack strategy may actually be to not attack at all*! Furthermore, as we outline below, simple rules can assure that new vulnerabilities are not introduced into the routing system during this incremental process.

In this stage, an AS may unilaterally decide to sign and announce a key for each of its prefixes without any external coordination, or any ISP may use its own self-signed certificate to delegate prefix ownership to customers. Figure 2 shows an example of small independent trust realms using self-signed certificates.

ASes must simply disseminate these prefix public-key certificates and use the corresponding private key to sign prefixes in routing announcements. *Each key-pair is*

[2] Some people believe that identity-based cryptography obviates the need for a trusted CA, which is unfortunately not the case.

[3] As discussed earlier, a similar "grassroots" concept could also help the adoption of a global AS PKI, if required by the routing protocol.

bound to a single prefix, and that key can only authenticate routing updates associated with that prefix or its sub-prefixes.

Because they are self-signed, these certificates do not imply an endorsement from a centralized authority like IANA that the AS originating the prefix is its legitimate owner. However, these self-signed prefix certificates can be used to authenticate address space delegation between parties within the grassroots-PKI. For example, if a large ISP has a trusted prefix key, it can sign the key of any customer announcing a smaller portion of that address space, indicating that the ISP permits the customer to announce that prefix.

Self-signed certificates are distributed as transitive attributes within the BGP update message, meaning they will be forwarded with route announcements even by ASes that are not yet participating in the secure routing scheme.

The assumption made here is that announcing a self-signed certificate provides security benefits for the early adopters, because BGP routers apply the following list of precedence to decide which BGP prefix/key pairs to trust:

1. **Root-signed:** Prefix that is secured by a certificate chain rooted at IANA.

2. **Trust-anchor-signed:** Prefix with a certificate-chain rooted at a well-respected "trust-anchor", such as a tier-1 ISP, registry, or corporate CA. Such an oligarchy of trusted entities is similar to current web security, where browsers ship with a relatively large list of trusted certificates.

3. **Self-signed:** Prefix signed by a key not associated with a trust anchor. For multiple such certificates, the oldest certificate (date first seen by the router, not date carried in certificate), is preferred. This model is similar to light-weight destination authentication in SSH.

4. **Unsigned:** A prefix in a BGP update as announced on the Internet today.

Note that a BGP router has the highest preference for prefixes certified through trusted entities, which can "overrule" other certificates for the same prefix that are only signed by less well-known entities. The key used by a trust anchor to sign prefix certificates is not itself a prefix key, meaning that a trust anchor can sign prefix keys even if it does not own the associated address space. This flexibility enables quick PKI development despite organizations in the delegation hierarchy that do not yet participate in the PKI. Routers install a trust anchor's public key (used to verify prefix certificates) only if it decides that party is indeed trustworthy.

The policy of preferring older self-signed certificates not only protects the address space of participants from an attacker's unauthenticated route announcement, but it also encourages early adoption because creating a self-signed certificate early (i.e., before an attack) is much easier than later demonstrating prefix ownership to a trust anchor in order to reclaim. By adopting early, an AS achieves a high level of security (an attacker must deceive a trust anchor to be successful) at an extremely low cost.

Accepted certificates/prefix pairs are placed in a local database along with a timestamp indicating when the prefix was first seen at that router. New routers just coming online can be easily be pre-configured with certificates learned by other routers to immediately begin choosing secure routes.

Risk. This approach has two main risks: first, an attacker may use self-signed certificates to try and divert traffic from a legitimate prefix owner, and second, an attacker may compromise one of the trust anchors and issue illegitimate certificates. We explore both possibilities.

Risk 1: Preferring older self-signed certificates prevents an attacker from stealing a prefix that has already been self-signed by its owner. However, an attacker could announce a self-signed certificate before the legitimate owner. Our goal in this case is two-fold: first, make this attack difficult, so that malicious actors do not gain any attack power with a grassroots PKI compared to BGP today. Second, provide a straight-forward mechanism to resolve this conflict that results in an even more secure infrastructure.

To provide the first property of introducing no additional vulnerabilities into the system, a router only accepts a self-signed prefix key if that key has been propagated with every preferred route to that prefix for a set period of time (e.g. 24 hrs.). This simple yet effective heuristic is similar in motivation to PGBGP [7], and builds on the intuition that at any point of time, most Internet routes are correct. Invalid originations for actively-used address space result in outages, which even today are recognized and manually filtered on human timescales of several hours at the most. With this rule, malicious key announcements cannot violate existing security mechanisms like filter lists or make it easier for an attacker to divert traffic. Thus all ASes, even those not participating in a Grassroots-PKI, are no more vulnerable to attacks than they are today.

If an attacker nonetheless successfully has its route and key accepted, we rely on the policy of preferring certificates with a higher trust level as a mechanism for "revoking" the invalid ownership claim. For example, if ISP evil.net is first to issue a self-signed certificate for one of angel.com's prefixes, angel.com can regain control by getting a trust anchor (for example, a tier-1 ISP responsible for providing their transit connectivity) to sign angel.com's prefix key. This makes angel.com's key more trusted than the key from evil.net, and angel.com will quickly reclaim its address space. The required chain of communication largely mirrors today's use of reac-

tionary BGP filters to block invalid routing announcements. However, the major difference is that with a grassroots PKI, the destination now become significantly more resistant to all future attacks, and the overall routing system is one step closer to a global PKI.

A related concern is an attacker's ability to announce a new unsigned sub-prefix of another prefix that is already signed[4]. Without a top-down PKI it is difficult to determine whether this sub-prefix is a valid route from a network not yet participating in the grassroots-PKI, or an attack meant to illegitimately divert traffic. The scheme must either accept and use less-trusted sub-prefixes, introducing significant vulnerability into the system, or reject all more specific prefixes unless they are signed by a key as or more trusted than the prefix they deaggregate. We choose the later, because legitimate sub-prefixes in global routing tables are likely to be IP space obtained by multi-homed customer from one of its upstream ISPs. As a result, sending traffic to the larger prefix will still result in the data being correctly delivered to the sub-prefix owner. If the sub-prefix owner wants its sub-prefix accepted globally as a secure route, it can easily have its upstream delegate that address space by signing the customer's key for the sub-prefix.

Risk 2: While self-signed certificates provide protection against common BGP attacks and misconfiguration, the large number of trust anchors still represents a legitimate vulnerability. Because any trust anchor certificate is preferred over all self-signed certificates, a prefix with only a self-signed certificate is vulnerable to the compromise of any trust anchor. Yet this preference of trust anchors over self-signed certificates is required as part of the attack resolution process described above. Thus, as demand for security increases, destinations will logically desire to have their self-signed certificates be signed by a trust anchor, even if no attack has yet occurred. This leads to our next stage of adoption: independent complex PKIs.

3.2 Independent Complex PKIs

For added robustness, we consider an architecture where islands of domains have their originally self-signed keys certified by one or more entities designated as "trust anchors", thus beginning to form a PKI hierarchy.

As mentioned above, the resolution of routing attacks creates a certification chain from a trust anchor to the legitimate prefix owner. Additionally, security conscious prefix owners are likely to preemptively have their prefix keys signed by trust anchors to gain improved attack robustness. ISPs will also gain a competitive advantage if they offer customers a certificate path to a trust anchor. In the course of this process, the trust anchors essentially become the roots of smaller hierarchical PKIs. Figure 3 shows an example, where the formerly self-signed clusters from Figure 2 are collected and authenticated by three different trust anchors.

[4]The announcement of a super-prefix is not a security concern, because IP forwarding will prefer the more specific valid route

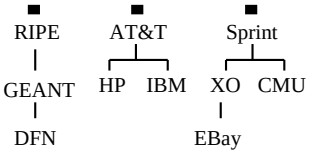

Figure 3: Three independent complex PKIs, each with a trust anchor at its root. Trust hierarchy does not necessarily mirror address delegation.

Risk. This approach has two main risks. First, operational confusion may occur during the transition from the primary use of self-signed certificates to independent complex PKIs. Who is qualified to be a trust anchor? Who decides if a trust anchor should be removed because of bad security practices? Similar to the inclusion of trusted keys in a browser, community consensus will play a powerful role in handling such issues. ISP operational organizations (e.g., NANOG) will be able to develop policies, likely placing trust in organizations already allocated significant responsibility for running core network infrastructures.

Second, the many trust anchors at the root of independent PKIs are still a vulnerability, as compared to full-time CA's, these organizations likely spend less money on and have less experience with roles like validating the identity of a prefix owner and protecting the private signing key from compromise. Prefix owners can achieve additional robustness either by having their key signed by multiple trust anchors or by the most trusted of entities, IANA. Either option is a viable path toward reaching the third and final stage: global PKI.

3.3 Global PKI

With the existence of many independent complex PKIs, we have clearly overcome the mutual dependence cited earlier as a key stumbling block to deployment of a full routing PKI. The existence of a number of trust anchors will provide an incentive for the establishment of a smaller root of trust. Each trust anchor can offload a considerable administrative burden onto the new trust root, and at the same time reduce its security exposure. This economic incentive is important, since any entity assuming the burden of acting as a trust root brings upon themselves a considerable liability. We believe either IANA or a small number of the most well-respected trust anchors will fill this role. There are two likely scenarios for a global PKI: cross-certification or consolidation under a single-rooted hierarchy.

3.3.1 Cross-certification

Large ISPs at the root of independent complex PKIs may be willing to cross-certify each other on the basis of existing business relationships. But in the eyes of some, direct cross-certification "turns the hierarchy of trust into

the spaghetti of doubt, with multiple certificate paths possible from leaf to roots ..." [4]. With cross-certification any given BGP participant may find it difficult to known where trust is coming from, or how reliable that trust is.

An alternative to direct cross-certification is the use of a Bridge Certification Authority (BCA) [5]. A BCA is a CA trusted by all of the smaller PKI roots to mediate trust between them. Each PKI root cross-certifies once with the BCA, and trusts that the BCA will correctly mediate policy and trust the various roots. Any mutually trusted entity could become the BCA in a secure BGP, but IANA may be the most natural choice. Note that as a bridge IANA would not actually require a PKI under it.

Risk. ANX used the Bridge CA architecture, and experienced organizational difficulties due to the number of administrative entities. Similar political complexities may render a BCA infeasible for secure BGP.

3.3.2 Single-Rooted Hierarchy

If IANA and the RIRs agree to participate in a routing PKI, then ISPs and other trust anchors may be willing to graft their root into a Single Rooted Hierarchy [5]. Much like the BCA case, the existence of independent trust anchors creates both management and security incentives to move toward a single root. Additionally, once certificates become a key part of the routing protocol, centralized address space delegators like IANA will be more willing to participate because they could gain power over wayward address owners by denying them a new certificate.

Risk. Single-rooted hierarchies have difficulties if the root key needs to be revoked. The approach of a single-rooted hierarchy for a secure BGP has the remote, yet real, risk that route authorizations for the entire Internet become invalid, causing a breakdown of interdomain routing because no secure routes can be found.

4 CONCLUSION

The deployment of a global PKI needed for secure routing is not sufficiently incentivized to overcome operational barriers to development and adoption. Contrary to current top-down PKI proposals, we suggest a grassroots PKI, representing a more realistic deployment path that will facilitate development of a global routing PKI and the deployment of secure routing. By accepting an imperfect level of security, but creating incentives for improved robustness, we construct a global PKI through incrementally staged deployment. At no point do we introduce new vulnerabilities, and attacks against legacy security weaknesses result in a strictly more secure network that is closer to our goal of a global PKI. We anticipate that our (r)evolutionary PKI deployment mechanism will encourage a dialog in the secure routing community to consider alternative PKI deployment strategies.

5 ACKNOWLEDGMENTS

This research was supported in part by CyLab at Carnegie Mellon under grant DAAD19-02-1-0389 from the Army Research Office, and grant CT-0433540 from the National Science Foundation, and by a gift from Cisco.

We would like to thank Jennifer Rexford for interesting discussions and feedback, and the anonymous reviewers for their insightful suggestions.

REFERENCES

[1] MS01-017: Erroneous VeriSign-Issued Digital Certificates Pose Spoofing Hazard. `http://support.microsoft.com/kb/293818`.

[2] D. Boneh and M. Franklin. Identity-based encryption from the Weil Pairing. In *Advances in Cryptology — CRYPTO '2001*, pages 213–229, 2001.

[3] G. Goodell, W. Aiello, T. Griffin, J. Ioannidis, P. McDaniel, and A. Rubin. Working around BGP: An incremental approach to improving security and accuracy in interdomain routing. In *Proceedings of NDSS 2003*, February 2003.

[4] P. Gutmann. PKI: It's not dead, just resting. *Computer*, 35(8):41–49, August 2002.

[5] P. Hesse and D. Lemire. Managing interoperability in non-hierarchical public key infrastructure. In *Proceedings of Network and Distributed System Security Symposium, 2002*, February 2002.

[6] Yih-Chun Hu, Adrian Perrig, and Marvin Sirbu. SPV: Secure path vector routing for securing BGP. In *Proceedings of ACM SIGCOMM 2004*, September 2004.

[7] Josh Karlin, Stephanie Forrest, and Jennifer Rexford. Pretty good BGP: Improving BGP by cautiously adopting routes. In *Proc. International Conference on Network Protocols*, November 2006.

[8] S. Kent, C. Lynn, J. Mikkelson, and K. Seo. Secure border gateway protocol (S-BGP) — real world performance and deployment issues. In *Proceedings of NDSS 2000*, pages 103–116, February 2000.

[9] John Linn. Trust models and management in public-key infrastructures. Available at `http://citeseer.ist.psu.edu/linn00trust.html`.

[10] S. A. Misel. Wow, AS7007! NANOG mail archives, `http://www.merit.edu/mail.archives/nanog/1997-04/msg00340.html`, 1997.

[11] Robert Moskowitz. History of the bca concept and other bca efforts, April 2000. Available at `http://csrc.nist.gov/pki/twg/Archive/y2000/presentations/twg-00-15.pdf`.

[12] Michael K. Reiter and Stuart G. Stubblebine. Authentication metric analysis and design. *ACM Transactions on Information and System Security*, 2(2):138–158, 1999.

[13] S. Weiler. Dnssec lookaside validation (dlv), draft-weiler-dnssec-dlv-01.txt. Technical report, IETF, June 2006.

[14] B. Weis, ed. Secure origin BGP (soBGP) certificates. Internet-Draft, July 2004. Work in progress. Available at `http://www.watersprings.org/pub/id/draft-weis-sobgp-certificates-02.txt`.

[15] R. White. Deployment considerations for secure origin BGP (soBGP), draft-white-sobgp-bgp-deployment-01.txt. Draft, IETF, June 2003.

[16] Philip R. Zimmermann. *The Official PGP User's Guide*. MIT Press, Cambridge, MA, USA, 1995. ISBN 0-262-74017-6.