DOI:10.1145/2659899

Article development led by acmqueue
queue.acm.org

Routing security incidents can still slip past deployed security defenses.

BY SHARON GOLDBERG

Why Is It Taking So Long to Secure Internet Routing?

THE BORDER GATEWAY PROTOCOL (BGP) is the glue that holds the Internet together, enabling data communications between large networks operated by different organizations. BGP makes Internet communications global by setting up routes for traffic between organizations—for example, from Boston University's network, through larger ISPs such as Level3, Pakistan Telecom, and China Telecom; then on to residential networks such as Comcast or enterprise networks such as Bank of America.

While BGP plays a crucial role in Internet communications, it remains surprisingly vulnerable to attack. The past few years have seen a range of routing incidents that highlight the fragility of routing with BGP. They range from a simple misconfiguration at a small Indonesian ISP that took Google offline in parts of Asia,[32] to a case of BGP-based censorship that leaked out of Pakistan Telecom and took YouTube offline for most of the Internet,[2] to a routing error that caused a large fraction of the world's Internet traffic to be routed through China Telecom,[6] to highly targeted traffic interception by networks in Iceland and Belarus.[34]

People have been aware of BGP's security issues for almost two decades and have proposed a number of solutions, most of which apply simple and well-understood cryptography or whitelisting techniques. Yet, many of these solutions remain undeployed (or incompletely deployed) in the global Internet, and the vulnerabilities persist. Why is it taking so long to secure BGP?

The answer to this question lies in the fact that BGP is a global protocol, running across organizational and national borders. As such, it lacks a single centralized authority that can mandate the deployment of a security solution; instead, every organization can autonomously decide which routing security solutions it will deploy in its own network. Thus, the deployment becomes a coordination game among thousands of independently operated networks; this is further complicated by the fact that many security solutions do not work well unless a large number of networks deploy them.

Routing Primer

BGP enables networks to route to destination *IP prefixes*. An IP prefix is a set of Internet Protocol addresses with a common prefix that is n bits in length. For example, the set of IP addresses {8.0.0.0, 8.0.0.1, ..., 8.255.255.255} is written as 8.0.0.0/8, where the notation /8 ("slash eight") implies that the first eight bits (the prefix) are common to all addresses in the set (in this case, those beginning with the numeral 8.). IP prefixes can have variable lengths, and the addresses in one IP prefix may

be entirely contained in another IP prefix. For example, the prefix 8.8.8.0/24, which is allocated to Google, is entirely contained in prefix 8.0.0.0/8, which is allocated to Level3; we say that IP prefix 8.0.0.0/8 *covers* IP prefix 8.8.8.0/24.

Longest-prefix-match routing. To decide how to forward an IP packet, an Internet router identifies the *longest* IP prefix that covers the destination IP address in the packet. For example, a packet with destination IP address 8.8.8.8 would be forwarded on the route to the longer 24-bit IP prefix 8.8.8.0/24 rather than to the shorter eight-bit IP prefix 8.0.0.0/8.

Autonomous systems. BGP allows autonomous systems (ASes) to discover routes to destination IP prefixes. ASes are large, autonomous networks operated by different organizations. Each AS is assigned a different AS number (for example, Google [AS 15169], China Telecom [AS 4134], Comcast [AS 7922], Boston University [AS 111], Verizon Wireless [AS 22394 and AS 6167]) and is allocated a set of IP prefixes. An AS is the *origin* for a prefix that is allocated to it.

ASes are interconnected, creating a graph where nodes are ASes and edges are the links between them, as in Figure 1. ASes discover routes to IP prefixes through the AS-level graph via BGP *announcements* they receive from their neighbors. Each BGP announcement contains the AS-level path the neighbor AS uses to reach the destination IP prefix. In Figure 1,[17,41] IP prefix 66.174.161.0/24 is allocated to Verizon Wireless, whose AS 22394 *originates* the prefix into the routing system by sending the following BGP announcement to AS 6167:

22394
66.174.161.0/24

AS 6167 selects the route and forwards all traffic for prefix 66.174.161.0/24 to its neighbor AS 22394. AS 6167 then appends its own name to the path and announces the path to its neighbors AS 2828 and AS 3356 as:

6167, 22394
66.174.161.0/24

Level3's AS 3356 selects the path and announces it onward to its neighbor AT&T AS 7018 as:

3356, 6167, 22394
66.174.161.0/24

This process continues, and the AS-level path to prefix 66.174.161.0/24 propagates through the network.

Business relationships and routing policies. If an AS learns multiple routes to a particular IP prefix, then it chooses a single most-preferred route using its local routing policies. BGP provides ASes with considerable flexibility in how they select their routes. Routing decisions are typically independent of the performance of the route at a given instant; instead, they are based on route length (that is, the number of ASes on the AS-level path) and the price of forwarding traffic to the neighbor that announced the route.

The price of forwarding traffic depends on the *business relationships*[9,19,20] between neighboring ASes. While many business relationships exist, two are particularly relevant here. The first is a *customer-provider* relationship, where the customer AS pays the provider AS to both send and receive traffic; Level3 and Verizon Wireless have a customer-provider relationship, represented by a directed edge in Figure 1 from the customer (Verizon Wireless) to the provider (Level3). The second relevant business relationship is *settlement-free peering*, where two ASes agree to transit each other's traffic for free; Level3 and AT&T have a peering relationship, represented by an undirected edge in Figure 1.

An AS will almost always avoid forwarding traffic from one neighbor to another if it cannot generate revenue by doing so; for example, China Telecom's AS 4134 in Figure 1 will not carry traffic from its peer, Level3 (AS 3356), to its other peer, AT&T (AS 7018), because neither neighbor pays China Telecom for this service. As such, China Telecom will not send a BGP announcement to AT&T (AS 7018) for the route to the prefix it learned from Level3 (AS 3356) in Figure 1.

This economically motivated behavior[9,19,20] is often generalized as the following *rule of thumb*: AS *a* will typically

Figure 1. Excerpt of the AS-level graph.[17,41]

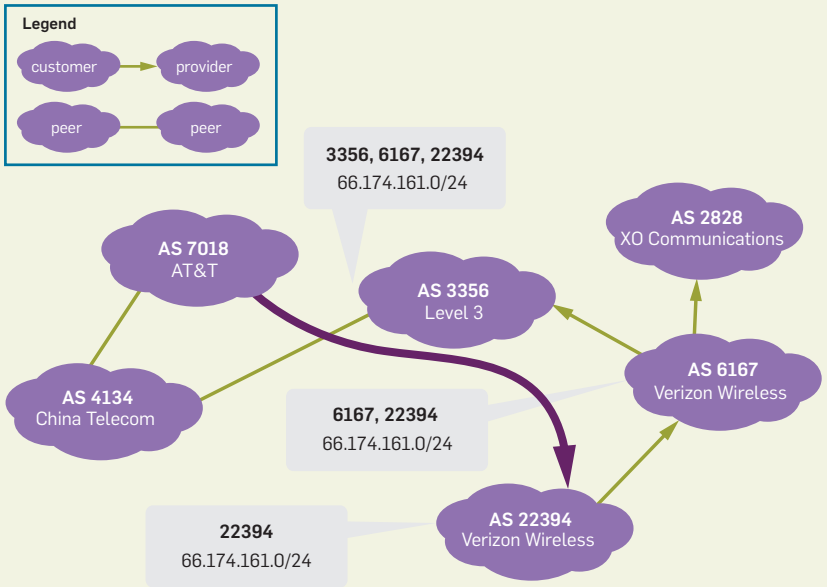
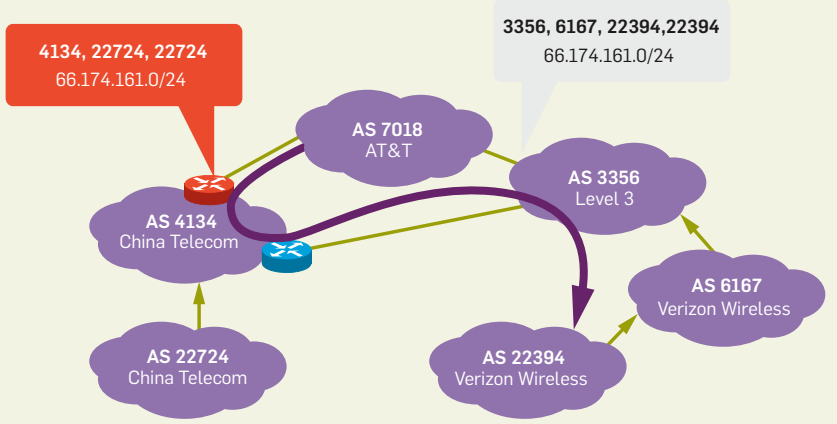


Figure 2. China Telecom hijacks Verizon Wireless.[17]



announce a route to neighboring AS *n* only if: (1) *n* is a customer of *a*; (2) the route is for a prefix originated by *a*; or (3) the route is through a customer of *a*.

Attacks on BGP

BGP was designed in the early 1990s—a simpler time, when the Internet was less contentious. As a result, BGP lacks basic authentication mechanisms, making it highly vulnerable to attack. We illustrate these vulnerabilities using several real-life routing incidents.

Hijacks. BGP lacks mechanisms to authenticate the allocation of IP prefixes to autonomous systems; a prefix hijacker exploits this by originating a prefix that was not allocated to its AS. Hijacks can be classified into two types: *prefix* and *subprefix*.

Prefix hijacks. In a prefix hijack, the hijacking AS originates the exact same prefix as the AS(es) that is legitimately allocated the victim IP prefix. The bogus BGP announcement originated by the hijacking AS will be disseminated throughout the routing system, and the other ASes will use their local policies to choose between routes to the legitimate origin AS(es) and bogus routes originated by the hijacking AS.

For 18 minutes on April 8, 2010, China Telecom launched prefix hijacks for 15% the Internet's prefixes.[6,17] While there is no evidence this incident resulted from anything other than a misconfiguration, it provides an instructive example of a "classic" prefix hijack.[17] Figure 2 shows one of the hijacks: China Telecom's AS 22724 hijacks Verizon Wireless's prefix 66.174.161.0/24. The bogus route originated by AS 22724 propagates through the AS-level graph and is eventually selected by AT&T because it is shorter than the legitimate route originating by Verizon Wireless's AS 22394. Meanwhile, Level3 selects the legitimate route, because it is shorter than the bogus route. Thus, network traffic splits between the hijacking AS and the legitimate origin AS, with the nature of the split depending on routing policies used by individual ASes and the topology of the AS-level graph.

Subprefix hijacks. A far nastier attack, the subprefix hijack can potentially allow the hijacker to intercept 100% of the network traffic destined for the victim IP prefix. In a subprefix hijack, the hijacking AS originates a subprefix of the victim's IP prefix—that is, a prefix that is covered by the victim IP prefix.

Perhaps the most famous subprefix hijack occurred on February 24, 2008, when Pakistan Telecom took YouTube offline. The incident[2] began when Pakistani authorities demanded YouTube to be censored within Pakistan. To accomplish this, Pakistan Telecom's AS 17557 launched a subprefix hijack by originating the subprefix 208.65.153.0/24 of YouTube's prefix 208.65.153.0/22 to its customer ASes in Pakistan (for example, Aga Khan University, Lahore Stock Exchange, Allied Bank Pakistan), as in Figure 3.[37,41] This meant traffic destined for YouTube's servers in AS 36561 would instead be forwarded to the *longer* IP prefix originated by Pakistan Telecom's AS 17557, where traffic could then be dropped.

Events took an unexpected turn when Pakistan Telecom's bogus BGP announcement leaked out of Pakistan. PCCW, a large ISP that provides global network connectively to Pakistan Telecom, received the bogus routing announcement, selected the bogus route, and announced it to its own neighbors. Because the bogus route

was for a longer prefix (/24) than the legitimate route (/22), longest-prefix-match routing meant the bogus route was *always* more preferred by the legitimate route, and within minutes, at least two-thirds of the Internet was sending its YouTube traffic to Pakistan.[2] The incident was eventually resolved via manual intervention of network operators at YouTube, PCCW, and other ISPs worldwide.

Detecting hijacks. Prefix hijacks might seem to be easy to detect, just by checking that a particular prefix is originated by more than one AS. A single prefix, however, might be originated by multiple ASes for legitimate reasons (for example, multiple ASes in a disparate part of the AS-level topology might originate a single prefix to reduce latency, so other ASes can get "closer" to the prefix). In some situations, only the legitimate holder of a prefix can be absolutely certain that a prefix is being hijacked. The identification of hijacks using anomaly-detection techniques is an active area of research.[3,21]

Route leaks are a separate class of commonly observed routing incidents.[28] These leaks are especially interesting because they do not involve the announcement of a bogus route. Instead, the perpetrator announces a legitimate route that it is actually using, but announces it to *too many* of its neighbors. The perpetrator is then overwhelmed by a flood of traffic from neighbors that select the leaked route.

Figure 4 illustrates such an incident involving Moratel (AS 23947), a local ISP based in Indonesia.[32,33] Moratel is not designed to transit large volumes of traffic from an international communications provider such as PCCW (AS 3491) to an important content provider such as Google (AS 15169). Per the rule of thumb in the first section, Moratel therefore should not announce its route to prefix 8.8.8.0/24 to its provider PCCW.

On November 6, 2012, however, a misconfiguration at Moratel did just that, "leaking" the route

23947, 15169
8.8.8.0/24

to PCCW. Understanding why this had impact requires knowledge of PCCW's local routing policies. Many routers,[19,20] likely including those in PCCW's AS, are configured to prefer a route through a neighboring customer over one through a neighboring settlement-free peer. By forwarding traffic through its customers, an AS can generate more revenue. As such, PCCW's routers preferred the customer route through Moratel over the usual settlement-free peering route directly to Google's AS 15196. As a result, Moratel received a huge volume of network traffic from PCCW, which quickly took parts of Moratel's network offline and rendered 8.8.8.0/24 unreachable for PCCW and some of its neighbors, including AS 4436.

Impact of routing incidents. Incidents of this type can impact routing in different ways, which can be classified as *blackholes* or *interception*.

Blackhole. In a blackhole, network traffic stops at the perpetrator AS and never reaches its legitimate destination; blackholes happen because BGP routing decisions are typically independent of the instantaneous performance of the route. Blackholes result in network outages that are visible to end users. The Moratel incident is a classic example of a route leak leading to a blackhole. Hijacks can also cause blackholes; the Pakistan Telecom/YouTube incident created a blackhole because all of Pakistan Telecom's neighbors had selected its bogus route,

Figure 3. Pakistan Telecom hijacks YouTube.[2,37,41]

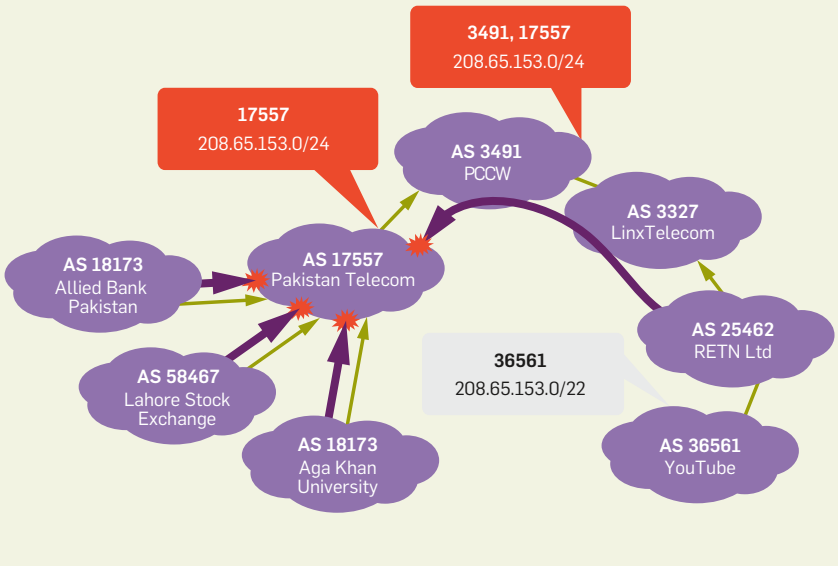
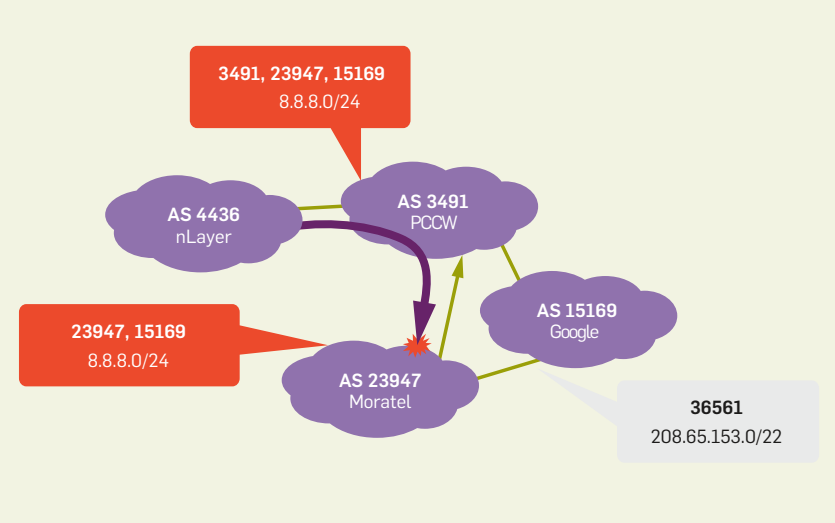
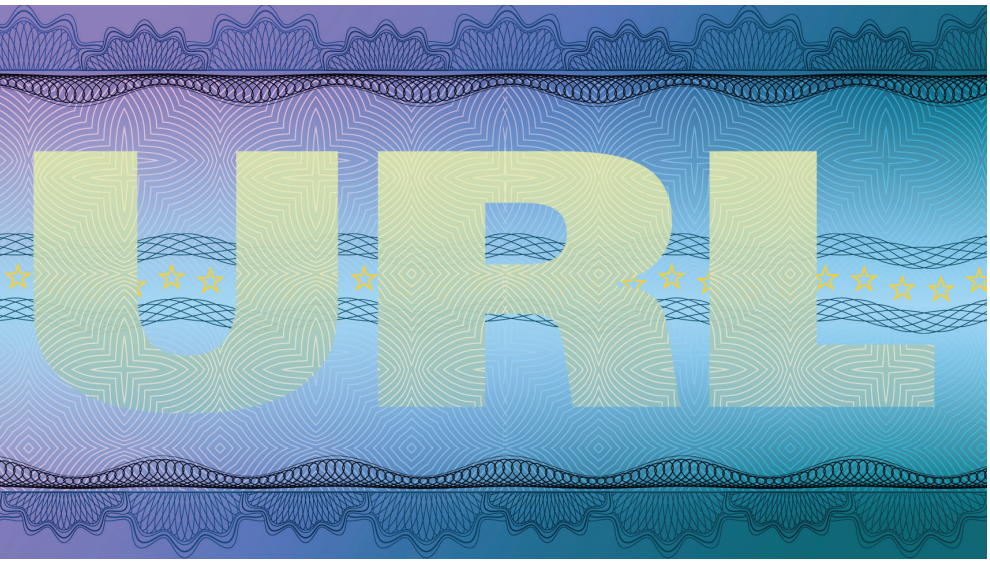


Figure 4. Moratel leaks a route to PCCW.[32,33]





leaving Pakistan Telecom without a working route to YouTube and forcing it to drop traffic for YouTube's prefix.

Interception. Traffic interception occurs when the perpetrator AS intercepts traffic for the victim IP prefix and then silently passes it on to the legitimate origin AS. Interception is invisible to end users. Both route leaks and hijacks can lead to traffic interception, as long as the perpetrator has a working route to the legitimate origin AS and enough network capacity to transit the extra traffic it attracts. The 2010 China Telecom hijack is one example. Figure 2 shows how one of China Telecom's routers announced the bogus hijacked routes to its neighbors, while other China Telecom routers maintained a working route to the legitimate origin of the prefix.[2,17] Traffic then traveled from the hijacking router, through China Telecom's high-capacity network, back out onto the wider Internet, and finally to the legitimate origin AS for the victim IP prefix. Similar incidents were observed last year by Renesys, which reported several short-lived hijacks that caused traffic for targeted IP prefixes to be intercepted by ASes based in Iceland and Belarus.[34]

Defenses

Many of these incidents can be eliminated through security solutions based on simple cryptography or whitelisting techniques. This section looks at these solutions—prefix filtering, RPKI (Resource Public Key Infrastructure), and BGPSEC—and highlights the challenges involved in deploying them on the global Internet.

Prefix filtering is a whitelisting technique used to filter out bogus BGP announcements. It is based on the rule of thumb of the first section, which implies that an AS (for example, Pakistan Telecom in Figure 3) will announce BGP routes to its provider (PCCW) only if those routes are: for its own allocated prefixes; or through its own customers (Aga Khan University, Lahore Stock Exchange, among others). As such, the provider can usually enumerate the small set of IP prefixes that are announced by its customer; that is, the set of IP prefixes allocated to Pakistan Telecom and its customer Pakistani ASes. The provider can therefore keep a *prefix list* of these IP prefixes for each customer and discard BGP announcements from a customer when they are not for prefixes on the list.

Benefit: Prefix filtering is simple and effective. Because a prefix filter is a simple whitelist, it does not usually present a large computational burden to routers. Prefix filtering has been used by various ISPs since the late 1990s and is a highly effective defense against hijacks and leaks perpetrated by customer ASes. Indeed, our research shows if every Internet provider with at least 25 customer ASes were to deploy prefix filters properly, this would prevent at least 48% of the Internet's ASes from launching routing leaks or hijacks.[12] Moreover, if PCCW had properly configured prefix filters in April 2008, the Pakistan Telecom's hijack of YouTube might never have happened. The same is true of the November 2012 Moratel route leak.

Challenge: Prefix filtering works only on customer links. Prefix filters, however, typically filter BGP announcements only from *customer* ASes; this is because prefix filters are built on the assumption that the filtered AS will announce only a *small* number of IP prefixes to the filtering AS. Prefix filtering is not typically used to filter BGP announcements from providers or settlement-free peers. For example, the 2010 China Telecom incident in Figure 2 could not have been prevented by prefix filtering, since China Telecom announced the bogus route along a settlement-free peering edge between China Telecom (AS 4134) and AT&T (AS 7018).

Challenge: Lopsided incentives. The incentives for deploying prefix filters are somewhat lopsided. For example, the "victims" of the 2008 Pakistan Telecom/YouTube incident were YouTube and all the impacted ASes that could not reach YouTube's hijacked prefix. However, the only AS that could have prevented the incident by using prefix filtering is PCCW itself; deploying prefix filters on the other victim ASes would do nothing to prevent the hijacked route from propagating through the Internet. Thus, the AS deploying the prefix filter (for example, PCCW) does not have particularly strong incentives to do so, other than protecting *the rest of the Internet* from attacks by its *own customers*.

RPKI: Cryptographic origin validation. The issues with prefix filtering have led to the development of many alternative security solutions. The approach that currently has the most traction is the RPKI.[26] Deployed since the start of this decade, the RPKI provides a trusted mapping from allocated IP prefixes to ASes authorized to originate them in BGP. To do this, the RPKI establishes a cryptographic hierarchy of *authorities* that allocate and suballocate IP address space, as well as authorize its use in BGP.

The RPKI is rooted at the RIRs (regional Internet registries). Figure 5 shows how ARIN (American Registry for Internet Numbers) allocates the prefix 8.0.0.0/8 to Level3, which suballocates prefix 8.8.8.0/24 to Google;[5] these allocations are accomplished using cryptographic certificates. The holder of a cryptographic certificate for a prefix can then sign an ROA (route or-

igin authorization) authorizing a prefix (or its subprefix) to be originated in BGP; in Figure 5, for example, Google issues an ROA authorizing its AS 15169 to originate 8.8.8.0/24.

Benefit: Offline cryptography. RPKI does not require any modifications to BGP message formats; nor does it require any cryptography to be performed online during routing. Instead, each day an AS syncs its local cache to the public repositories that store RPKI objects, cryptographically verifies the RPKI objects in its local cache, and pushes the resulting whitelist (mapping IP prefixes and their authorized origin AS(es)) to border routers in its AS.[26]

Benefit: Protection from hijacks. Routers use this whitelist to filter hijacked BGP routes (that is, those with an unauthorized origin AS). For example, in Figure 2 AT&T can use the RPKI to determine the route

3356, 6167, 22394, 22394
66.174.161.0/24

is legitimate; AS 22394 is the origin of the route, and there is ROA in the RPKI of Figure 5 authorizing AS 22394 to originate 66.174.161.0/24. Meanwhile, the route originating at China Telecom's AS 22724 in Figure 2 is bogus, since there is no ROA authorizing AS 22724 to originate 66.174.161.0/24.

Benefit: Effective incentives. The RPKI also avoids the two problems that plague prefix filtering: it can be used to filter BGP announcements made by *any* neighbor (not just neighboring customers), and it avoids lopsided deployment incentives. During the first phase of RPKI deployment, an AS that wants to protect the routes it *originates* can populate RPKI repositories with ROAs for its originated routes. (Today, RPKI contains ROAs for about 4% of the routes announced in BGP.[31]) During the second phase of RPKI deployment, an AS can use RPKI to discard bogus routes, thus protecting the routes it selects. (Currently we are in the very early steps of this phase, with a few ASes worldwide are experimenting with the RPKI-based filtering.)

Challenge: RPKI takedowns and misconfigurations. A key challenge to RPKI deployment stems from abuse of RPKI itself.[5,7,8,30] RPKI is designed as a threat model where BGP is under attack but RPKI is trusted. Can RPKI itself be attacked, misconfigured, or lawfully compelled to misclassify a legitimate BGP route as bogus? (DNS is subject to lawful orders to take down domains;[14,35] could RPKI be used to take down IP prefixes? This has already come up in several court cases.[13,22,29]) Since routers use RPKI to filter bogus BGP routes, then the routers will lose access to the misclassified route. This means RPKI creates a new attack vector that can be used to blackhole routes. These issues are known to the RPKI standards community, and there are ongoing efforts to harden RPKI against this type of abuse through the development of configuration tools[24,31,36] and fail-safe mechanisms;[16,23] it is too early to tell what the outcome of these efforts will be.

Challenge: RPKI can be circumvented. Unfortunately, the RPKI cannot prevent some classes of attacks.

The first is a route leak. The RPKI is designed to detect routes with an unauthorized origin AS, but in a route leak, the perpetrator leaks a legitimate route with an authorized origin AS. For example, even if nLayer (AS 4436) in Figure 4 had been filtering routes based on the RPKI, it would still select the "leaked" Moratel route, since Google is a legitimate origin for prefix 8.8.8.0/24.

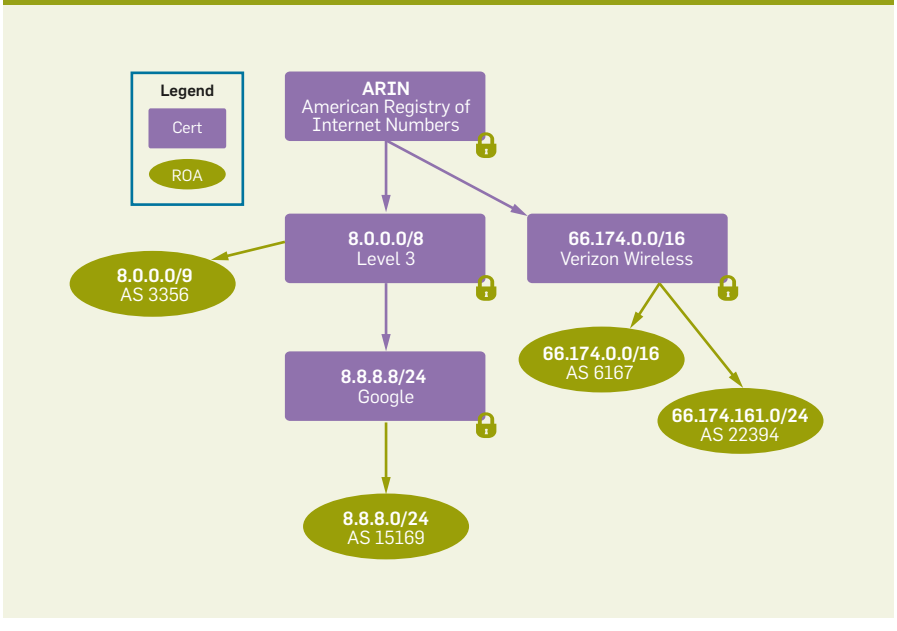
The second is a *path-shortening attack* in which an attacker announces a short bogus path to a prefix that terminates at the authorized origin AS. For example, even if RPKI were fully deployed, China Telecom (AS 4134) could still intercept traffic if it announced the route

4134, 22394
66.174.160.0/24

to AT&T in Figure 2. To see why, notice the route has a legitimate origin AS (AS 22394), but the route is actually bogus: there is no edge between AS 4134 and AS 22394. Thus, even if AT&T used RPKI to filter routes, it would still select the bogus route to China Telecom because it has a legitimate origin AS and is shorter than the legitimate route via Level3.

Fortunately, however, research[1,12,27] suggests fewer ASes are likely to select a leaked or shortened route than one that is subprefix hijacked. During a subprefix hijack, the hijacker exploits longest-prefix-match routing to (potentially) convince *all* of the ASes on the Internet to select the bogus route. Meanwhile, both route leaks and path-shortening attacks do not exploit longest-prefix-match routing. Instead, they cause traffic to split between legitimate routes and the leaked/shortened route, with a majority of the traffic taking legitimate routes;[12,27] the nature of the split is determined by routing policies and the AS-level topology (since ASes closer to the attacker are more likely to select the attacker's route).

Figure 5. Model of a possible future full deployment of the RPKI.[5]



BGPSEC: Cryptographic path validation. The community has considered a number of solutions that can eliminate the attacks that can be launched against the RPKI. Excellent surveys of these solutions are available.[3,21] Here, we focus on BGPSEC, the protocol currently being standardized by the Internet Engineering Task Force (IETF).[25] Building on the RPKI's guarantees that a BGP route has an authorized origin AS, BGPSEC also provides *path validation.*

BGPSEC builds on the RPKI by adding cryptographic signatures to BGP messages. It requires each AS to sign each of its BGP messages digitally. The signature on a BGPSEC message covers (1) the prefix and AS-level path; (2) the AS number of the AS *receiving* the BGPSEC message; and includes (3) all the signed messages received from the previous ASes on the path. For example, in Figure 2, AT&T's AS 7018 would receive the following BGPSEC message from Level3's AS 3356:

$$[66.174.161.0/24 : 7018; 3356; 6167; 22394]_{3356}$$
$$[66.174.161.0/24 : 3356; 6167; 22394]_{6167}$$
$$[66.174.161.0/24 : 6167; 22394]_{22394}$$

where the notation $[m]_A$ means message m signed by AS A. Upon receipt of a BGPSEC announcement, an AS validates the signatures and filters the route if the signatures are invalid.

Benefit: No path-shortening attacks. BGPSEC eliminates path-shortening attacks. In Figure 2, China Telecom (AS 4134) announced the path

4134, 22394
66.174.161.0/24

to AT&T. With BGPSEC, this attack would fail. China Telecom (AS 4134) would not receive the BGPSEC announcement

$$[66.174.161.0/24 : 4134; 22394]_{22394}$$

from Verizon Wireless (AS 22394), since AS 22394 and AS 4134 are not neighbors, and thus could not form a 'shortened' bogus path that passes the digital signature checks required by BGPSEC.

Challenge: Online cryptography. Unlike the solutions discussed thus far, BGPSEC is an *online* cryptographic protocol; routers must cryptographically sign and verify every BGP message they send. This high computational overhead, which could require routers to be upgraded with crypto hardware accelerators, could slow down BGPSEC deployment.

RPKI does not require any modifications to BGP message formats; nor does it require any cryptography to be performed online during routing.

Challenge: The transition to BGPSEC. All the security solutions considered here face the challenge that each AS will decide whether or not to deploy them based on their own local business objectives. This challenge is particularly acute with BGPSEC, because an AS cannot validate the correctness of an AS-level path (and therefore filter bogus routes) unless all the ASes on the path have applied their signatures to the message. This means the security benefits of BGPSEC apply only after *every* AS on the path has deployed BGPSEC. This is in stark contrast to the other two solutions discussed here—prefix filtering and RPKI—where only the AS doing the filtering needs to deploy the security solution. This creates a chicken-and-egg problem; the security benefits of BGPSEC apply only after a large number of ASes have deployed BGPSEC, but there is little security incentive for anyone to be the first to deploy BGPSEC.

There are a number of ways around this chicken-and-egg problem. One idea is that a set of early-adopter ASes would deploy BGPSEC (for example, for regulatory compliance, because of subsidies, or for public-relations purposes) and then trigger a cascade of BGPSEC deployment.[4,10] One argument in favor of deploying BGPSEC is that because BGPSEC necessarily influences routes selection, an AS that has deployed BGPSEC could attract more revenue-generating traffic from its customers that prefer to select BGPSEC-secured routes. Our simulation results suggest these economic incentives, along with several other conditions, can create a cascade that leads to BGPSEC adoption at a majority of ASes on the Internet. [10]

Beyond economic incentives, however, is the question of what security benefits are provided during the transition to BGPSEC, when some ASes have adopted it but others have not. The answer is, unfortunately, less positive. Given the routing policies

that are likely to be most popular[11] during the transition to BGPSEC, our recent work argues that BGPSEC can provide only meager improvements to security over what is already possible with the RPKI.[27] This is because ASes may prioritize economic considerations over security concerns. For example, given a choice between an *expensive*, BGPSEC-secured route through a provider and a *cheap*, *insecure* BGP route through a customer, an AS might choose the cheap, insecure path. Thus, even ASes that have deployed BGPSEC can suffer from *protocol downgrade attacks*, where an attacker convinces them to select a bogus path instead of a legitimate BGPSEC-secured path.

Conclusion

Today we live in an imperfect world where routing-security incidents can still slip past deployed security defenses, and no single routing-security solution is a panacea against routing attacks. Research suggests, however, the combination of RPKI with prefix filtering could significantly improve routing security; both solutions are based on whitelisting techniques and can reduce the number of ASes that are impacted by prefix hijacks, route leaks, and path-shortening attacks. There are still several deployment challenges to overcome, since prefix filtering is limited by lopsided deployment incentives, while RPKI introduces a new dependence on centralized authorities.

This article has concentrated on protocol-based attacks on BGP. Recent research[38,39] and media revelations[15,18,40] indicate routers themselves could be compromised in a manner that circumvents *protocol-based* defenses such as prefix filtering, RPKI, and BGPSEC. Thus, while we continue to make progress toward protocol-based defenses for routing security, the next frontier of routing security could very well be hardening the software and hardware used in Internet routers.

Acknowledgments

Thanks to my collaborators on the research I have drawn upon here: Kyle Brogle, Danny Cooper, Phillipa Gill, Shai Halevi, Ethan Heilman, Pete Hummon, Alison Kendlar, Robert Lychev, Aanchal Malhotra, Leonid Reyzin, Jennifer Rexford, Michael Schapira, and Tony Tauber. This work has been funded by the NSF (1017907), Cisco, and the Sloan Foundation.

Related articles on queue.acm.org

What DNS is Not
Paul Vixie
http://queue.acm.org/detail.cfm?id=1647302

The Network is Reliable
Peter Bailis and Kyle Kingsbury
http://queue.acm.org/detail.cfm?id=2655736

Splinternet Behind the Great Firewall of China
Daniel Anderson
http://queue.acm.org/detail.cfm?id=2405036

References

1. Ballani, H., Francis, P. and Zhang, X. A study of prefix hijacking and interception in the Internet. In *Proceedings of the ACM SIGCOMM 2007 Conference*, 265–276.
2. Brown, M. Pakistan hijacks YouTube. Renesys blog; http://www.renesys.com/blog/2008/02/pakistan_hijacks_youtube_1.shtml.
3. Butler, K., Farley, T. McDaniel, P. and Rexford, J. A survey of BGP security issues and solutions. In *Proceedings of the IEEE 98*, 1, (2010), 100¬–122.
4. Chan, H., Dash, D., Perrig, A. and Zhang, H. Modeling adoptability of secure BGP protocol. In *Proceedings of the ACM 2006 SIGCOMM Conference*, 279–290.
5. Cooper, D., Heilman, E., Brogle, K., Reyzin, L. and Goldberg, S. On the risk of misbehaving RPKI authorities. In *Proceedings of the 12th ACM Workshop on Hot Topics in Networks* (2013).
6. Cowie, J. China's 18-minute mystery. Renesys blog, 2010; http://www.renesys.com/blog/2010/11/chinas-18-minute-mystery.shtml.
7. FCC Communications Security, Reliability and Interoperability Council III (CSRIC). Secure BGP deployment. *Communications and Strategies*; (2012); http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRICIII_9-12-12_WG6-Final-Report.pdf.
8. FCC Communications Security, Reliability and Interoperability Council, Working Group 6. Secure BGP deployment, final report, 2013.
9. Gao, L., Rexford, J. Stable Internet routing without global coordination. *IEEE/ACM Transactions on Networking 9*, 6 (2001), 681–692.
10. Gill, P., Schapira, M. and Goldberg, S. Let the market drive deployment: A strategy for transitioning to BGP security. In *Proceedings of the ACM SIGCOMM 2011 Conference*, 14–25.
11. Gill, P., Schapira, M. and Goldberg, S. A survey of interdomain routing policies. *ACM SIGCOMM Computer Communication Review 44*, 1 (2013), 28–34.
12. Goldberg, S., Schapira, M., Hummon, P. and Rexford, J. How secure are secure interdomain routing protocols? In *Proceedings of the ACM SIGCOMM 2010 Conference*, 87–98.
13. Goldman, E. Sex.com–An update. Technology and Marketing Law blog, 2010; http://blog.ericgoldman.org/archives/2006/10/sexcom_an_updat.htm.
14. Government Printing Office. H.R.3261 - Stop Online Piracy Act, 2011.
15. Greenwald, G. How the NSA tampers with US-made Internet routers. *The Guardian* (May 12, 2014); http://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden.
16. Heilman, E., Cooper, D., Reyzin, L. and Goldberg, S. From the consent of the routed: Improving the transparency of the RPKI In *Proceedings of the ACM SIGCOMM 2014 Conference*.
17. Hiran, R., Carlsson, N. and Gill, P. 2013. Characterizing large-scale routing anomalies: a case study of the China Telecom incident. In *Passive and Active Measurement*. Springer, Berlin Heidelberg, 2013, 229–238.
18. Horchert, J., Appelbaum, J. and Stöocker, C. 2013. Shopping for spy gear: Catalog advertises NSA toolbox. *Der Spiegel* (Dec. 29, 2013); http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html.
19. Huston, G. Interconnection, peering and settlements, Part I. *Internet Protocol Journal 2*, 1 (1999). Cisco.
20. Huston, G. Interconnection, peering and settlements, Part II. *Internet Protocol Journal 2*, 2 (1999). Cisco.
21. Huston, G., Rossi, M. and Armitage, G. Securing BGP: a literature survey. *IEEE Communications Surveys and Tutorials 13*, 2 (2011), 199–222.
22. Internet Governance Project. M.L. Mueller. In important case, RIPE-NCC seeks legal clarity on how it responds to foreign court orders; http://www.internetgovernance.org/2011/11/23/in-important-case-ripe-ncc-seeks-legal-clarity-on-how-it-responds-to-foreign-court-orders/.
23. Kent, S. and Mandelberg, D. Suspenders: a fail-safe mechanism for the RPKI. Internet Engineering Task Force, 2014; http://tools.ietf.org/html/draft-kent-sidr-suspenders-01.
24. LACNIC Labs. RPKI looking glass; www.labs.lacnic.net/rpkitools/looking_glass/.
25. Lepinski, M., ed. BGPSEC protocol specification. IETF Network Working Group, 2014; http://tools.ietf.org/html/draft-ietf-sidr-bgpsec-protocol-05.
26. Lepinski, M. and Kent, S. RFC 6480: an infrastructure to support secure Internet routing. Internet Engineering Task Force, 2012; http://tools.ietf.org/html/rfc6480.
27. Lychev, R., Goldberg, S. and Schapira, M. BGP security in partial deployment. Is the juice worth the squeeze? In *Proceedings of the ACM SIGCOMM 2013 Conference*, 171–182.
28. McPherson, D., Amante, S., Osterweil, E. and Mitchell, D. eds. Draft. Route leaks and MITM attacks against BGPSEC. IETF Network Working Group, 2013; http://tools.ietf.org/html/draft-ietf-grow-simple-leak-attack-bgpsec-no-help-03.
29. Miller, R. Court ruling: Israeli and US terrorism victims now "own" Iran's Internet. Joshuapundit blog (June 25, 2014); http://joshuapundit.blogspot.com/2014/06/court-ruling-israeli-and-us-terrorism.html.
30. Mueller, M. and Kuerbis, B. Negotiating a new governance hierarchy: an analysis of the conflicting incentives to secure Internet routing. *Communications and Strategies 81* (2011), 125–142.
31. National Institute of Standards and Technology. RPKI deployment monitor; http://www-x.antd.nist.gov/rpki-monitor/.
32. Paseka, T. Why Google went offline today and a bit about how the Internet works. Cloudflare blog (Nov. 6, 2012); http://blog.cloudflare.com/why-google-went-offline-today-and-a-bit-about.
33. PeeringDB. 2014; https://www.peeringdb.com/.
34. Peterson, A. Researchers say U.S. Internet traffic was re-routed through Belarus. That's a problem. *Washington Post* (Nov. 20, 2013).
35. Piscitello, D. Guidance for preparing domain name orders, seizures and takedowns. Thought paper. ICANN (Mar. 2012).
36. RIPE Network Coordination Centre. RPKI validator; http://localcert.ripe.net:8088/trust-anchors.
37. RIPE Network Coordination Centre. YouTube hijacking: A RIPE NCC RIS case study. RIPE NCC Blog, 2008; http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study.
38. Schuchard, M., Thompson, C., Hopper, N. and Kim, Y. Taking routers off their meds: why assumptions of router stability are dangerous. In *Proceedings of the Network and Distributed System Security Symposium*. 2012.
39. Schuchard, M., Thompson, C., Hopper, N. and Kim, Y. 2013. Peer pressure: exerting malicious influence on routers at a distance. In *IEEE 33rd International Conference on Distributed Computing Systems*, 2013, 571–580.
40. Storm, D. 17 exploits the NSA uses to hack PCs, routers and servers for surveillance. *ComputerWorld* (Jan. 3, 2014); http://blogs.computerworld.com/cybercrime-and-hacking/23347/17-exploits-nsa-uses-hack-pcs-routers-and-servers-surveillance.
41. Wang, L., Park, J., Oliveira, R. and Zhang, B. Internet AS-level topology archive; http://irl.cs.ucla.edu/topology/.

Sharon Goldberg is an assistant professor of computer science at Boston University.