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.