The Internet’s crucial role in modern life, commerce, and government underscores the need to study the security of the protocols and infrastructure that comprise it. For years, we’ve focused on endpoint security and ignored infrastructure weaknesses. Recent discoveries and initiatives highlight a simple fact: the core is just as vulnerable as the edge.

In the past few years, attackers have increasingly targeted infrastructure. Internet protests, vigilantism, nation-state attacks, distributed denial of service for hire, public-key infrastructure lapses, and the market for 0-day exploits have shifted our attention to the increased risk in which we place not only our data but also our livelihood. The Internet’s infrastructure, protocols, and processes are therefore getting attention from researchers, not just practitioners.

**Infrastructure Vulnerabilities**

The Internet is one of the world’s largest, most complex human-engineered distributed systems ever devised and deployed. It comprises multiple, often interdependent, subsystems. When an endpoint or user of this massive system is threatened, one or more subsystems are often called on to help contain the threat. However, when Internet subsystems themselves come under fire, how do we manage system threats from the system itself or its otherwise trusted subsystems?

The Internet security community tends to consider only the ramifications of availability or integrity loss at one host or organization at a time. Recently, people have been examining, and in some cases exploiting, vulnerabilities that threaten Internet subsystems—the protocols and equipment that move data around. When these subsystems come under attack, statistics on compromised Secure Shell servers and monetary losses owing to credit card fraud seem almost quaint. When infrastructure is at risk, the upper limits of those statistics are boundless.
In addition, the Internet infrastructure is currently undergoing significant changes. As the available IPv4 address pool winds down, widespread deployment of IPv6 is becoming a reality. Is it any surprise that after one large network provider adopted IPv6, its first inbound email message was spam? More than a decade in the making, the Domain Name System (DNS) root zone was recently signed with DNS Security Extensions. With it generally comes larger DNS answers, which adversaries can use to turn the system against itself in amplification and reflection attacks. The Internet Engineering Task Force’s Secure Inter-Domain Routing working group is trying to bring assurance to Internet routing where currently even relatively simple router configuration errors can mistakenly reroute huge swaths of address space. In summary, the Internet Protocol—the glue that holds the entire system together—is undergoing a major deployment upgrade while two of its biggest core subsystems, DNS and Border Gateway Patrol, are adding some not-so-trivial security mechanisms.

**In This Issue**

This special issue brings together Internet infrastructure security researchers and practitioners—groups that don’t normally overlap. We received several articles on diverse topics including attacks, cryptography, protocol analysis, and policy. At least three expert reviewers from industry or academia reviewed each article. We selected five that focus on IPv6, multinational policy, and wireless protocols.

The recent final allocation from the IPv4 address pool by the Internet Assigned Numbers Authority to the regional registries highlights the inevitable growth of IPv6 address use. Although the base IPv6 specifications are more than a decade old, the Internet security community has paid too little attention to them. Eventual deployment is likely to pose numerous security and operational challenges yet to be discovered. Two articles in this issue examine IPv6 features from a security perspective. “Secure Neighbor Discovery: Review, Challenges, Perspectives, and Recommendations,” by Ahmad AlSa’deh and Christoph Meinel, explores weaknesses in the Neighbor Discovery Protocol (NDP), which is critical to IPv6. Because IPv6 lacks security, researchers have proposed Secure Neighbor Discovery extensions to prevent attacks. The authors provide an overview of this protocol and its deployment challenges. Another article looks at how defenders can use IPv6’s large address space to their advantage. “The Blind Man’s Bluff Approach to Security Using IPv6,” by Matthew Dunlop and his colleagues, explores address hopping as a way to stay ahead of attackers and reviews an IPv6 deployment at an American university.

**Internet-scale security often takes the form of policy, which relies on technological deployments. These technologies face hurdles in interoperability, implementation, and management. Two articles address this subject. In “Is Europe Ready for a Pan-European Identity Management System?,” Sergio Sánchez García, Ana Gómez Oliva, and Emilia Pérez-Belleboni review a multinational identity management system. Challenges remain, but these efforts are growing in importance as policymakers further commit to using the Internet in their key services. Jan Kallberg’s article, “The Common Criteria Meets Realpolitik: Trust, Alliances, and Potential Betrayal,” explores the requirements side by looking at Common Criteria, the complexities owing to its rigid specifications, and complications stemming from rapid technology changes.**

The final article illustrates the continued cat-and-mouse game of protocol security. For many years, various groups have explored Wi-Fi standards and security extensions, and upgrades continue to be made and new weaknesses found. Frederick T. Sheldon and his colleagues’ article, “The Insecurity of Wireless Networks,” looks at recent attacks on 802.11 wireless standards, including the Wi-Fi Protected Access protocol. The authors’ lab work and attack analysis demonstrate the challenges facing Wi-Fi and its increasing ubiquity in the modern “networks of things.”

**We thank the authors of all the submitted articles and the referees who reviewed them. Thanks also to IEEE Security & Privacy editor in chief John Viega for creating this special issue and to Jennifer Stout, Tara Delaney, and the entire IEEE Computer Society Editorial Services staff for their support and guidance from start to finish.**

We hope that you enjoy reading this group of articles as much as we did bringing it together. ■

**Jose Nazario** is a senior manager of security research at Arbor Networks. Contact him at jose@arbor.net.

**John Kristoff** is a researcher at Team Cymru. Contact him at jtk@cymru.com.

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.

**We’re looking for your feedback!**

If you’d like to comment on anything you read in this issue, please email lead editor Kathy Clark-Fisher at kclarkfisher@computer.org.