DHS Science and Technology Directorate

Secure Protocols for Routing Infrastructure

Relying on an unsecure Internet

The transmission of massive amounts of data on the Internet is dependent upon the Internet Addressing and Routing standards. These standards were designed to be flexible, open, and scalable—more than 2.4 billion people used the Internet in 2012.

However, the standards were not designed to address security, which has created fundamental vulnerabilities in the way the critical functions operate. This leaves global Internet traffic susceptible to disruption and interception. Whether through misconfiguration or malicious attack, email addresses can be faked and Internet traffic can be intercepted or misdirected, both of which endanger the overall stability of the global Internet. While occurrences are not common and can be hard to detect, they do happen and are noticed.

While it has been widely acknowledged within industry and the government that something needs to be done to secure the critical functions of Internet, addressing and routing, tackling this multidimensional problem is challenging. The Internet is a complex, globally-distributed system that is owned and operated by many different parties, and is constantly changing. Additionally, most network operators have very thin margins with long hardware upgrade cycles which require careful attention to ensure approaches are economically viable.

A practical approach

When approaching the complex problem of improving routing security, it is just as important to take into consideration the operational and business constraints of deployment as it is to tackle the technical challenges. Approaches for securing routing and addressing are only useful if they are implemented and deployed. The Department of Homeland Security, Science and Technology Directorate (S&T) Secure Protocols for Routing Infrastructure project has been working directly with industry and academia with the goal of achieving a practical and secure solution. Through a diverse design team, approaches for securing both Internet addresses and routes have been developed that are both practical and incrementally deployable, and are being standardized through the global standards body for the Internet, the Internet Engineering Task Force (IETF).

Internet addresses hierarchically distribute registrars to help ensure that each address is globally unique. The approach taken to secure these addresses includes the use of digital certificates that demonstrate that an organization has been authorized to use a range of addresses. When an address is validated against these certificates, it is easy to discern whether an organization can legitimately use that address.

Global impact

To route information around the globe, it is divided into packets that are passed from one network to another until it reaches its final destination. The routes between networks are discovered and established using the Border Gateway Protocol. Through misconfiguration or malicious action, routes can be altered or misdirected. Building on the address certificates, which are beginning to be deployed, S&T's approach is to have each network along a route add a signature as a routing path is being built. This provides proof for networks that a route passes through, and makes it obvious if a route has been altered or misdirected. It also prevents misconfiguration through the use of address certificates. Routes can only be originated for addresses for which an organization has been authorized.

When deployed, these solutions will provide a more solid foundation upon which the Internet can securely continue to grow. They will provide more certainty about who the user is communicating with and the path that communication is taking. This improves the security of some of the most fundamental aspects of the Internet.

To learn more about Secure Protocols for Routing Infrastructure contact sandt-cyber-liaison@hq.dhs.gov.

2014-11-03