The Third Rail

William Manning

20160929

Abstract:

Naming in an internet context has been plagued for years on a conflict between the name of an object and the location of the object. [1] The Domain Name System has been very successful in avoiding many of the problems of naming by the creation of both scalable, ephemeral namespace and a flexible, extensible query/response protocol for publication of the namespace. A primary problem remains in the absence of external validation checking of either the name or the address. These two issues were highlighted in "Toward a Safer and More Secure Cyberspace " [2]. The technical response to provide for validation was the development of the DNSSEC suite of protocols with capabilities to cryptographically sign the data and protect the communications channels. [3-5] Unfortunately, the security attributes of the keys and signatures is subordinate to the canonical label, either the name or the address, and is inextricably bound to the DNS namespace. In the absence of always on, always connected reachability, it is common to have names and addresses cached but without the ability to reach a trust anchor. [6] These design choices have lead to a much less robust and resilient DNS. It has been argued that moving the cryptographic hierarchy outside the DNS namespace would greatly increase the robustness and resilience of the DNS, in essence creating a distributed Certification Authority. [7] The segregation of the DNS cryptospace from the DNS namespace and the DNS addressspace creates a "third rail" which provides more stability and trust than adding the crypto functions to the existing DNS apex. While desirable and useful, the inertia in the creation and maintance of yet another centralized registry is counter to a robust and flexible naming system. Methods for creating a scalable, decomposable naming system that has at least "two-factor" authentication (name and address, address and key, key and name) to validate the third should be the next step. Some work on this has already been undertaken, with projects like "peername" [8] working on decentralized, decomposable naming systems. Having such a system with the triple of name/address/key seems to offer a robust, scalable solution.

[1] RFC 1498, On the Naming and Binding of Network Destinations

[2] https://www.nap.edu/catalog/11925/toward-a-safer-and-more-secure-cyberspace

[3] https://www.ietf.org/rfc/rfc4033.txt

[4] https://www.ietf.org/rfc/rfc4034.txt

[5] https://www.ietf.org/rfc/rfc4035.txt

[6] http://www.internetgovernance.org/2007/04/18/securing-the-root-the-root-of-the-problem-creating-a-trust-anchors/

[7] http://koara.lib.keio.ac.jp/xoonips/modules/xoonips/download.php/KO90001001-20133923-0004.pdf?file_id=92075

[8] https://peername.com/about/