DNSSEC OUTLINE

I. Introduction

-- The Domain Name System (DNS) is a fundamental (albeit distributed) protocol, critical to the stable and secure operation of the Internet. Hundreds of millions of users rely on DNS every day to convert easy-to-remember and enter names (such as www.uoregon.edu) into numeric IP addresses (such as 128.223.142.71).

-- DNS, left unprotected, is subject to a variety of attacks. One such attack is "cache poisoning." In a cache poisoning attack, an attacker replaces legitimate name-to-number mappings that have been cached on a recursive resolver with incorrect information, potentially resulting in users being misdirected to hostile or untrustworthy alternative destinations.

-- Cache poisoning attacks have been seen in the wild, including at major ISPs (see for example "China Netcom DNS Cache Poisoning," http://securitylabs.websense.com/content/Alerts/3163.aspx from 8/19/2008)

-- Cache poisoning attacks can be defeated using DNSSEC. DNSSEC is a well defined IETF standardized protocol (summary of relevant RFCs: http://www.dnssec.net/rfc), and is supported in many open source and commercial DNS products

-- The only real protocol-level competition to DNSSEC is DNSCurve (http://dnscurve.org/), assumed to be out of scope for this working group.

-- As a hierarchical trust infrastructure, DNSSEC deployment is easiest when the trust anchor "root" has been cryptographically established, and when top level domains also participate. The root ("dot") was signed on July 15th, 2010 (http://www.root-dnssec.org/), and "dot com" was signed March 31st, 2011 (just to mention one of many important TLDs that have now DNSSEC signed their TLDs).

II. Deployment Considerations

-- Some operators may never have experienced a DNS cache poisoning attack; for them, there may be little urgency to deploying DNSSEC, since it would only ameliorate what has largely been a "theoretical" attack to-date.

-- DNSSEC does not ameliorate all security threats to DNS. Many DNS deployments are fraught with other issue that also demand attention (operators should be encouraged to check their DNS with free tools such as http://dnscheck.iis.se/).

-- To be effective, DNSSEC requires adoption by two groups: (a) zone administrators need to sign the DNSSEC zones they manage, and (b) operators of recursive resolvers need to configure their resolvers to verify the DNSSEC status of the queries their resolvers process. Unfortunately, uptake is still relatively low. Because the value to each party depends on the action of the other party, DNSSEC faces a potential "bootstrap" or "chicken-and-egg" race condition: if few zones are signed, there's little point to enabling validation; if few are validating, there's little point to signing one's zone. This is an ongoing challenge.

-- DNSSEC deployment may also be inhibited by the protocol's "failure-signaling" mode: if keys are allowed to expire or a zone is otherwise incorrectly signed, that DNSSEC failure is "signaled" by suppressing the return of results for that zone. That is, if your zone is not correctly signed, your zone will effectively "disappear from the Internet," at least for sites that are doing DNSSEC validation. While this is an example of the DNSSEC protocol performing as intended, this is still obviously a disconcerting event for a zone administrator to experience. (DNSSEC debugging, when failures do occur, is also still something of an arcane art, although Casey Deccio (Sandia)'s http://dnsviz.net/ tool certainly helps).

-- DNSSEC is an example of what some might term a "hidden goodness." That is, when DNSSEC works the way it should, all you get is "an absence of badness," and no one (except the DNS cognoscenti) even knows they're being protected. If may be hard to organizationally prioritize work that no one may notice/care about.

-- DNSSEC is not "end-to-end." That is, DNSSEC validation typically takes place at the ISP's recursive resolver, and not on a stub resolver on the end-user's system. That last hop, between the recursive resolver and the end-user's system, is thus not cryptographically protected.

-- DNSSEC also establishes a trust framework that can be used in potentially commercially disruptive ways. For example, the IETF DANE ("DNS-based Authentication of Named Entities") Working Group has proposed using DNSSEC-signed DNS entries as an alternative to the conventional commercial Certificate Authority Model for SSL/TLS certificates, see http://tools.ietf.org/html/draft-ietf-dane-ops-01