DNSSEC/DANE: Tools to Encourage Adoption

ICANN53

June 24, 2015

v1

Agenda

- DNSSEC/DANE Adoption
- Object security via S/MIME, a Plugin Library
- DANE Provisioning Portal Proof of Concept

DNSSEC/DANE Adoption – where are we?

- DNSSEC adoption has moved slowly
  - First implementation in 1999 (BIND)
  - .SE is the first signed ccTLD in 2005
  - Root zone signed in 2010

- As of May 2015 (http://www.statdns.com/)

TLD	Domains	Signed
COM	117,111,271	464,541
NET	14,954,083	86,380
ORG	10,523,409	49,703

DNSSEC Adoption – why?

- Many possible obstacles to adoption
  - Awareness outside the DNS community
  - Compelling applications – what can I do with a signed zone?
  - Incomplete deployment (validating resolvers, recursive NS)
  - Tools and infrastructure?

DANE Puts Steam in the DNSSEC Engine

Where is the “killer app” for DNSSEC? DANE makes DNSSEC relevant to the Internet for more than MITM protection.

The world needs an interoperable and easy but trusted way to learn user’s keys without physically meeting them. DANE uses DNSSEC to create a rock solid substrate on which every application can offer real security.

DNSSEC/DANE Adoption – How to make progress?

- Each of the obstacles to adoption deserves attention
- Let's focus on answering one of the objections: are there gaps to fill in the tools and infrastructure?
- DNSSEC/DANE is hard for many to understand – simplified tools and infrastructure can help with this!

Object Security via S/MIME

- S/MIME gives us object security
  - Signing
  - Encryption
- Current proposal in IETF DANE WG for SMIMEA RR type
  - Uses locator based on email address to learn user key
  - Uses TLSA record format and registries
- S/MIME reaches beyond email

Libsmaug, a Plugin Library

Libsmaug is an open source implementation of a library that aims to make object security easy for application developers

- Working code
- Implements one of the proposals for the SMIME RR format
- Built using full featured stub resolver (getdns or libunbound)
- C/C++ shared library
- Encapsulates getDNS, openssl

- https://github.com/verisign/smaug

DANE Provisioning Portal Proof of Concept

Experimental Service to encourage adoption

- Free provisioning web UI and REST API
- Limited RR types (DANE focused)

- Per-RR Authorization
  - Users can change their keys without affecting parent zone

Let's Bring Key Learning to the Internet

- Experiment with libsmaug and send feedback
- Contact dane-provisioning@verisign.com to be notified when the DANE Provisioning Portal Proof of Concept is available
- DANE is more than email – where do you see applications that need interoperable key learning? Let us know.

powered by

VERISIGN™