

Tutorial: DNSSEC Deployment

Phil Regnauld and Hervey Allen (Network Startup Resource Center) Abstracts While DNS is, perhaps, one of the most fundamental components of a healthy and safe Internet it is, also, vulnerable to a number of different types of attacks. As the revelation of the Kaminsky Exploit in 2008 showed the traditional DNS trust model leaves this core piece of Internet infrastructure open to potentially devastating attacks.

DNSSEC is an update to the traditional DNS system. DNSSEC uses public-key cryptography to update the DNS trust model to ensure verifiable DNS responses to requests from clients.

In this 1/2 day tutorial we will cover the following:

- * Problems with DNS:

- DNS cache poisoning

- Nameserver hijacking

- * The basics of DNSSEC, one solution available now.

- New DNS Resource Records (DNSKEY, RRSIG, NSEC and NS).

- Two new packet headers (CD, AD)

- * How to sign DNS data:

- KSK and ZSK keys.

- * Operational Aspects:

- Signing the root

- Trust anchors

- DLV and ITAR

- Key management

- Key rollover

- Zone crawling issues

- Available toolsets

- * Registry-registrar aspects:

- EPP or other extensions to support DS records

- Support for authenticated key updates.

- Turning on/off DNSSEC and the impact

- * What isn't solved:

- Man-in-the-middle attacks where everything is spoofed.

- Need to trust the resolver

- DoS attacks

- Data is not encrypted

- * Application side:

- Up-the-stack notification. How do we handle failures?

- Need more info from the stub resolver

- More than one protocol available.

- * Status today

- Root signing discussion (NTIA NOI)

- Signed TLDs include .br, .cz, .gov, .museum, .org, .pr,

- .se, etc.

- * Summary

Attendees will see a hands-on demonstration of securing a zone using DNSSEC. This will include key generation, updating of the zone file, configuration of a forwarding resolver, publishing the zone and verification of the newly signed zone. Step-by-step instructions using a DNSSEC toolset (tbd) will be made available to all attendees.*
Abstracts

- Network Management and NOC Workshop

Hervey Allen (NSRC), Phil Regnauld (NSRC), Chris Evans (Delta-Risk)

- VOIP Deployment Workshop

Jonny Martin (PCH), Vicky Shrestha (PCH), Daniel Griggs (FX Networks)

- Network Security Workshop

Damien Holloway (Juniper Networks), Kunjal Trivedi (Cisco), Merike Kaeo (Doubleshot Security)

- ISP Routing Workshop using IPv4 and IPv6

Gaurab Raj Upadhya(PCH), Amante Alvaran (APNIC), Shankar Vridhagiri

- Advanced Routing - BGP Multihoming with IPv4 and IPv6

Philip Smith (Cisco), Mark Tinka (Global Transit)

- Toward The Internet 2.0
Hiroshi Esaki, Ph.D.

- Advancing the Philippines' Internet Infrastructure
William Torres, Ph.D.

- Integrating IP Wireless Sensor Networks
Patrick Grossetete, Archrock

- Lessons Learnt from the Beijing Olympic Games Website Measurement
Rocky K. C. Chang, The Hongkong Polytechnic University

- A technical demo and overview of .tel
Jim Reid (Telnic)

- BGP IN 2008 - what's changed
Geoff Huston (APNIC)

- IPv6 Traffic levels on Hurricane Electric's backbone
Martin Levy (Hurricane Electric)

- JANET's 40Gbps backbone
Rob Evans (JANET)

- From IPv4 only to v4/v6 Dual Stack
Shin Miyakawa (NTT)

- How to Keep CGNs from Breaking the Internet
Randy Bush (IJJ)

- IPv6 Deployment at IJJ
Yoshinobu Matsuzaki (IJJ)

- Session aware NAT
David Miles (Alcatel-Lucent)

- IANA and DNSSEC at the root
Richard Lamb (IANA)

- IPv6 at Google: lessons learned, state of the art, and the road to deployment
Lorenzo Colitti(Google)

- Euro-IX update
Serge Radovic (Euro-IX)

- IPv6 at Monash University
John Mann(Monash University)

- What can IXPs do for IPv4/IPv6 route exchange?
Takabayashi Takejiro (Japan Internet Exchange Co., Ltd.) and Mawatari Masataka (Co-author)

- What can IXPs do about IPv4 exhaustion?
MAWATARI Masataka (Japan Internet Exchange Co., Ltd.) and TAKABAYASHI Takejiro

- DNS-OARC's Open DNSSEC Validating Resolver
Duane Wessels(DNS-OARC)

- AMS-IX Update
Cara Mascini(AMS-IX)

- DNSSEC in 6 minutes
Joao Damas (ISC)

- NIXI - Internet Exchanges in India
Amitabh Singhal,NIXI
- IPv6 - IPv4 Co-Existence: IETF Report
Jari Arkko, Ericsson Research, IETF
- Rogue DNS servers - a case study
Feike Hacquebord,Trend Micro