DNSSEC
Why, how, why now?

Olaf Kolkman (NLnet Labs)
olaf@nlnetlabs.nl
DNS Architecture

As ISP

As 'friend'

secondary

As DNS provider

Registry DB

primary

Provisioning

DNS Protocol

Registrars/Registrants

client

Cache server

http://www.nlnetlabs.nl/

Rabat, Morocco, June 1, 2008
DNS Architecture

- Registrar
- Registrant
- Registry DB
- Inter-server communication
- Cache Poisoning
- Server compromise

DNS Protocol

Provisioning

http://www.nlnetlabs.nl/

Rabat, Morocco, June 1, 2008
Example: Unauthorized mail scanning

- Subject: tenure
- Where?
- There!
- DNS

Astrophysics Mail Server -> DNS -> Central Admin Mail Server
Example: Unauthorized mail scanning

Subject: tenure

Where?

Astrophysics Mail Server

Central Admin Mail Server

Bad Guy

Elsewhere

DNS
voip2voip as an example

_query: 0.5.6.0.2.2.2.0.2.3 1.e164.arpa

SIP URI

SIP negotiation and call setup

voip call: +31 20 222 0650

SIP Server

DNS Server

VOIP

Sip Server

http://www.nlnetlabs.nl/
Slide courtesy: Patrik Fältsröm

Rabat, Morocco, June 1, 2008
voip2voip as an example

Query:
0.5.6.0.2.2.2.0.2.3 1.e164.arpa

SIP call: +31 20 222 0650

http://www.nlnetlabs.nl/
Slide courtesy: Patrik Fältsröm

Rabat, Morocco, June 1, 2008
Why DNSSEC

• Good security is multi-layered
  – Multiple defence rings in physical secured systems
  – Multiple ‘layers’ in the networking world

• DNS infrastructure
  – Providing DNSSEC to raise the barrier for DNS based attacks
  – Provides a security ‘ring’ around many systems and applications
Where Does DNSSEC Come In?

• DNSSEC secures the name to address mapping
• We still need:
  – Routing Security
  – Application Level Security
  – Secure Systems
• Having DNSSEC available may help with the provisioning of say Application security
DNS Architecture

Confidence in outsourcing of DNS

Inter-server communication (although that can be done with TSIG)

Protection against Cache Poisoning not an arms race any longer

Detection of NXDOMAIN replacements

Provisioning

http://www.nlnetlabs.nl/

Rabat, Morocco, June 1, 2008
Application Benefits

• With reasonable confidence perform opportunistic key exchanges
  – SSHFP and IPSECKEY Resource Records

• With DNSSEC one could use the DNS for a priori negotiation of security requirements.
  – “You can only access this service over a secure channel”
Solution
a Metaphor

• Compare DNSSEC to a sealed transparent envelope.
• The seal is applied by whoever closes the envelope.
• Anybody can read the message.
• The seal is applied to the envelope, not to the message.
DNSSEC properties

• DNSSEC provides message authentication and integrity verification through cryptographic signatures
  – Authentic DNS source
  – No modifications between signing and validation
• It does not provide authorization
• It does not provide confidentiality
Other DNS security

• We talked about data protection
  – The sealed envelope technology
  – RRSIG, DNSKEY, NSEC[3] and DS RRss
• There is also a transport security component
  – TSIG
  – Useful for bilateral communication between machines
  – Trivial to deploy today
Methods to prevent Cache Poisoning

\(<\text{Qname, Qclass, Qtype, IP-quad, query-ID}>\)

• Careful matching against all of the above
  - Utilize the maximum amount of variation possible
  - Not predictable

• Qname: 0x20 proposal
  - Qname: Www.ExaMpLE.coM.

• Also, only allowing information in the cache that is related to the question
Wait-a-minute

• Given previous slide: is DNSSEC still needed?
  – Aren’t the methods to prevent cache poisoning sufficient?
    • Yes, prudently written software makes the possibility to poison caches less likely
  – Recognize an arms-race?
    • Only until the next clever trick is announced.
    • DNS is inherently insecure

• The other attack vectors still exist
  – Access to the wire e.g. hijack of DNS server addresses
  – Secondary server access
Status of Deployment

• A sad state of affairs
  - http://secspider.cs.ucla.edu/ reports a little over 10,000 zones signed, only little under 1000 are production zones
  - RIPE Reverse zones
  - .se, .pr, .br and .bg are signed top level domains
  - .uk, .arpa, .org have voiced some form of commitment
  - There is a testbed for the root and a lot of layer 9
Chicken and Egg
Why so little deployment?

• Little deployment means little experience and few tools.
• Little experience and few tools increase the cost of deployment

• Little infrastructure to justify cost of validation
• Little validators to justify the infrastructure
• No short term benefits, only long term
  - No immediate benefit to oneself
Breaking the egg: who and how?

• Deployment by the custodians of the DNS infrastructure: TLD operators and the root
  – Taking responsibility for the public space and act as enablers

• But also at the ISP level, gaining experience

• Providing tools and software

• Sharing Experience
Closing words

• Acting responsible with the network will allow users to keep trusting the network

• Deployment of infrastructure security is one of those measures
  – DNSSEC is a part of the picture, not a magic security bullet (no security tool is)